Global Information Assurance Certification Paper

SANS GIAC Certified Firewall Analyst Practical Assignment

GCFW Version 1.8

By:

Fabio Cerniglia Saitta
October 14, 2002

Index

Introduction

GIAC Enterprises is an e-business company, which deals in the online sale of fortune cookie sayings. GIAC Enterprises business is related to information that travels on the network. Business depends on IT infrastructure: availability and security are the main goal to produce business. The equation is simple: system down → no e-business → no business.

There are a lot of situations that can compromise system availability and security, concerning information management, system management, people which use information and IT devices, … but also weather conditions, wars, - don't forget 11th September 2001 -, and so on. In all of these, security is always a key word. Security, security, security…. What can I do? It depends on what I want to do and how many money I have to spend.

GIAC Enterprises said that security is the first priority, because a breech in the security can easily cause the company to loose income and even fail altogether. Armed with these basic tenets GIAC Enterprises is ready to invest whatever is required to keep their systems and networks secure. In the following paragraphs, I will illustrate the analysis of business process and the design of network security architecture.

Assignment 1 – Security Architecture

GIAC Enterprises is a new e-business company and employs approximately 70 people. It relies heavily on their business partners for the translation and the reselling of their product and on their suppliers for the creation of the fortune cooking sayings.

IT infrastructure has been developed according to the following criteria:

1. **Standardization**: they use few hardware platforms and operating systems: Intel based machine using Microsoft Windows 2000 as PC and servers, CISCO or 3Com as network equipments (router, switch, hub, …). IT support staff will gain some important benefit from the choice of identical platforms, because they will not be forced to find patches for many hardware or OS combinations.
2. **User training and skill upgrading**: every user must know, at different level, depending on what he have to do and what he have to use, the instruments used to perform his activities
3. **Scalability**: if I need more workstations or if I have to add new servers o new applications, I don't have to redesign the IT architecture
4. **Availability**: for each critical component is available a spare system, backup are scheduled on regular basis and tapes are store in a distinct

safe place, recovery process has been defined and tested, antivirus protection is running and update on all systems.

The network structure has been designed to satisfy their business need, but it is time to re-evaluating their entire network architecture to improve security and maintain business "on-line".

Business Operation Model

The business operation model of GIAC Enterprises uses the following actors:

1. GIAC Enterprises employees
2. GIAC Enterprises mobile sales force and teleworkers
3. Partners
4. Suppliers
5. Customers

GIAC Enterprises employees (internal users) connect to the network via the GIAC intranet, have access to all our required resources and need access to Internet for web browsing or ftp download for software updates. Every GIAC Enterprises employee has a badge, a personal identification code, a personal UserID and password. Each employee is responsible to protect such data. Two different groups of internal users have been defined with different permissions: general user and IT technical user. Some of IT technical users are responsible for maintenance of systems and network equipments and they are the only people which have administrative authorities, know administrator passwords, are allowed into the server farm room, which is in a safety, controlled and secured place. Restriction will be based on the individual policies that are associated with the task assigned.

GIAC Enterprises mobile sales forces and teleworkers are people traveling or employees working in a place outside. They, using the TCP/IP suite of protocol, get into the network from either external remote locations or their home, with access to the public internet, and are able to use the same resources as they were physically in the office, inside GIAC. GIAC Enterprises mobile sales forces and teleworkers use a laptop computer, provided by GIAC Enterprises. The laptops will be pre-loaded with corporate licensed software, VPN client software, antivirus and personal firewall software. VPN client software is configured for secure and encrypted communication with the corporate VPN services, located on the DMZ Firewall. Authentication is required using personal UserID and password. Antivirus and personal firewall software should protect laptops from computer viruses and Trojan horse software (they are internet connected!!!). This solution helps us to protect the GIAC intranet when mobile users do connect back inside the DMZ.

The partners translate the fortunes and resell them. We use a secure VPN tunnel between GIAC firewall and their terminating network equipment. The partners use web services to connect to the fortune data. The access will be controlled through authentication procedure, using UserID and password.

The suppliers access GIAC network through VPN connections, using a secure tunnel. They have much the same access to GIAC Enterprises like partners and access is controlled through authentication procedure, using UserID and password.

We assume that GIAC management has established a business agreement with his partners and suppliers. It means that we have a trusted working relationship with them, but, obviously, each company realize the prudence of restricting access to an as need basis and of securing and filtering content.

The Customers are world wide located and purchase GIAC fortune cookie sayings online via our web server. Their access must be secure and made available at all time, 24 hours per day, 7 days per week. HTTPS will be used anytime sensitive or secure information needs to be transmitted over the network. The SSL logic is built into the application environment and the server certificates will be purchased from a certification authority, like Verisign.

You will find a detailed description of the protocol and the ports used in the assignment 2, where are illustrated the policy we are implementing to secure network architecture.

GIAC Enterprises Network Design

The network design will leverage a defense in depth. It is recognized that everyone (employees, partners, suppliers) are sharing the burden to maintain the integrity of the network and its data. A security team will be employed to maintain and structure the security of the GIAC network.

I will remind some general security rules, not strictly related to the network design, but if any company should adopt them to protect his assets:

- Unauthorized use of equipment is not allowed
- All data on the network are considered property of the company
- Access to data on the GIAC Enterprises network is restricted to authorized users
- All connection into the GIAC network must be logged, monitored and analyzed.
- Server farm, network equipments and uninterruptible power source (UPS) must be housed in a rack, which must be securable, located in a protected safety room, with limited access and controlled by alarm system.

- Access to the IT server room is controlled through use of special ID Smart card that will be issued to authorized IT technical staff only.
- The operating systems must be hardened following manufacturer guidelines and any available reference materials.
- Systems must be patched on regular basis, unless there is vulnerability in the operating system or service running on the machine. They must be aware of any problems (especially that concerning vulnerabilities) as soon as the rest of community is, because IT technical staff must monitor the vendor web sites and any other relevant web sites containing security warning or relevant issue.
- Vendor-supplied defaults for system passwords and other security parameters are not allowed
- GIAC IT technical staff must keep track of all hardware and software changes, so that this information is readily available in case of problems.
- All device configurations must be maintained in separate and encrypted file, stored off-site
- Appropriate plans must be defined to regularly test security systems and processes
- Disaster recovery procedures must be defined, tested and updated as needed

In my network design, a layered approach will be taken when connecting the various information assets and network appliances, with a strong focus on securing all hosts and systems. All unnecessary services and ports will be eliminated on each host or network device in an effort to minimize potential vulnerability. Multiple layers make it that much harder for a bad guy to attack GIAC environment. A multi-layer security architecture will help to mitigate the overall risks GIAC Enterprises is exposed to and allow for a greater chance of containing security breaches or at least slowing them down, before the intruder can damage efficiency of information assets.

In the network diagram shown in fig. 1 you can see four layers, which respectively are named: public domain, unsecured perimeter zone, demilitarized zone (DMZ) and GIAC intranet.

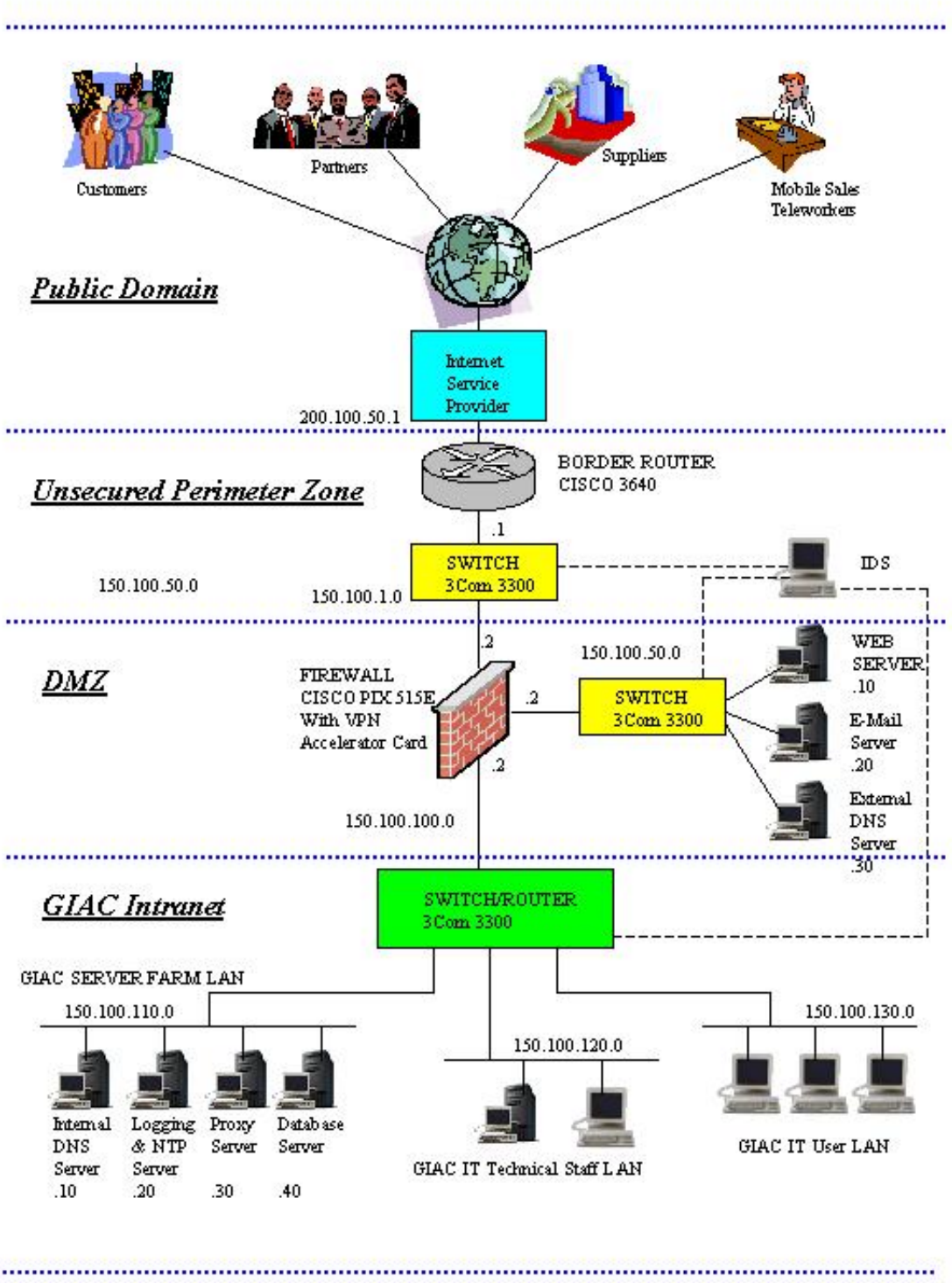


Figure 1

I will briefly illustrate their characteristics.

- Public domain: this is the public network that is freely available to everyone. It is out of GIAC Enterprise control. It is considered to be totally insecure.

- Unsecured perimeter zone: it is insecure because it is placed outside of the firewall. Their components are the most visible targets to the outside world and are directly in the line of fire. The perimeter is the first line of defense and it is assumed that it is possible the perimeter can be compromised in some way.

- Demilitarized zone (DMZ): it is a buffer zone between the insecure networks outside of the organization and GIAC Enterprises internal protected network. All the equipments are located in a safety place, protected by alarm system. In the DMZ we put only the minimum amount of devices and services as is necessary to satisfy the business requirements. These devices are protected by GIAC firewall against the hostilities coming from the internet but run services that are publicly accessible. This produces some degrees of vulnerability.

- GIAC intranet: it is the most secured and trusted zone. All the employees connect to the GIAC intranet where are hardware, software and information vital to the GIAC Enterprises' business. The GIAC intranet is the most protected area from access by threats from outside the company. It does not mean that it is 100% secure, but we have to secure it as much as possible.

While designing secure network architecture, we decided to make it simple, because simplicity in design is important to keep the maintenance as low as possible and reduce errors produced by human variable.

To reduce downtime due to hardware or software failure, some critical components (border router, firewall, switch, some of the server) will be maintained in duplicate, to allow for a quick replacement.

For the purpose of this assignment, I will suppose that the Internet Assigned Numbers Authority (IANA) has assigned the class B network (150.100.0.0) to GIAC Enterprises. Using a subnet mask of 255.255.255.0, I am able to split the network address assigned into 254 networks, each with 254 hosts.

It should not be a real case, but I think that the main goal of the assignment is to illustrate the criteria I follow to secure network architecture.

Using public addressing for GIAC Enterprises network, I do not need to use Network Address Translation (NAT). I have to use NAT in the networks if they use private addresses and need to connect to the internet, because private

addresses are not routable over the internet. NAT main function is to hide private addresses and translate them into public addresses.

Sometimes, many people consider private addressing a security feature, because it becomes more difficult to discover real IP addresses assigned to resources located in the internal network.

The following table reports the IP addressing scheme I will use:

Zone	Device/Segment	IP Address	Subnet Mask
Public Domain	Border Router	200.100.50.1	255.255.255.255
Unsecured Perimeter Zone	Border Router	150.100.1.1	255.255.255.0
DMZ	Firewall (router) Firewall (DMZ) Firewall (intranet) Web Server E-Mail Server External DNS Server	150.100.1.2 150.100.50.2 150.100.100.2 150.100.50.10 150.100.50.20 150.100.50.30	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0
GIAC Intranet	GIAC Server Farm LAN Internal DNS Server Logging & NTP Server Proxy Server Database Server GIAC IT Technical Staff LAN GIAC IT User LAN	150.100.110.0 150.100.110.10 150.100.110.20 150.100.110.30 150.100.110.40 150.100.120.0 150.100.130.0	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0

Table 1

In the following pages, I will illustrate the components used and their function.

Components used in the GIAC Enterprises Network design

The border router connects GIAC Enterprises network directly to ISP, by a dedicated E2 Line (2Mbps). Border router is the first line of defense in our layered security approach. The main functions and security issues we have to address are:

- To deny unwanted protocols, services and ports or, if you prefer, – and it is better –, to allow only wanted protocols, services and ports (first rule in security is: deny every things that is not explicitly allowed)
- Packet filtering at the perimeter (to prevent IP spoofing, some DOS attacks and to block other types of attacks before they reach the firewall)
- To disable some abilities like icmp redirects, unreachable response messages, directed broadcasts or proxy-arp
- To provide access control list that limits access to the router itself and filters packets based on source and destination IP address or ports, in order to clear off most of the noise or unwanted traffic
- To deny incoming traffic from private IP networks (RFC 1918), that do not route across the internet, or illegal IP addresses
- To deny incoming traffic from multicast address o reserved address (class E)
- To allow inbound access to web server
- To allow inbound and outbound e-mail and DNS services
- To allow secure transactions and encrypted communications
- To allow established internal TCP connections to pass
- To allow internally initiated ICMP or UDP
- To allow GIAC intranet user access to internet
- To send log messages to logging server

The border router is a Cisco 3640 running Cisco IOS 12.2. The router processor memory has 128 MB DRAM and 32 MB flash memory. We fully load the router processor memory because more memory improves throughput and reduce degradation due to DOS attacks. The processor type is 100 MHz IDT R4700 RISC. As modular solutions the Cisco 3600 series have the flexibility to meet both current and future connectivity requirements.
Cisco components are familiar to IT technical staff that is favorably impressed with the excellent technical support provided by Cisco Systems and with the reference materials available on Cisco's web site (http://www.cisco.com). More details about Cisco 3600 series are available on the Cisco's web site, starting from http://www.cisco.com/en/US/products/hw/routers/ps274/index.html .

A firewall is a system (hardware, software, or both, working in concert) that divides intranet from outside network. It is a single point of access between a local network and any outside foreign network. Some rules (access control policy) define what types of information are allowed to flow between the two networks. Using a firewall, it is possible to protect network and information from intruders. A firewall must deny all traffic not specifically permitted.

The firewall selected is the Cisco PIX 515E, running firmware version 6.2. The Cisco PIX 515E Firewall intended for small-medium business and enterprise environment, provided up to 188 MBps of firewall throughput with the ability to handle as many as 125000 simultaneous sessions. Certain models includes stateful high-availability capabilities, as well as integrated support for 2000 IPSec tunnels. It is a hardware-based firewall and it should be faster than a software-based firewall. Another important consideration is that it is not susceptible to attacks on the underlying operating system because it has only firmware and no operating system.

The firewall will be also used as the termination point for VPN services. If we want to offload this work from the firewall's main processor, we should take the Cisco VPN Accelerator Card, a specialized card with its own processor, memory and software, optimized to handle intensive IPSec encryption/decryption.
The use of VPN accelerator card will increase the performance of both the firewall and VPN services. You can find more information about Cisco PIX 515 Firewall or IOS software in the Cisco web site at the following URL:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html
http://www.cisco.com/en/US/products/sw/iosswrel/index.html

A DNS Server provides a useful way to access internet resource by mapping the resource name to the IP address, because it easy to know or remind a name instead of an IP address.
The GIAC Enterprises network design includes two DNS Server, because I follow a split approach. The external DNS Server only maintains entries related to devices and services that are publicly accessible. The internal DNS Server is available to people connected to the internal network and provides conversion between name and IP address for hosts and devices on the GIAC intranet.
To implement DNS, I will use Berkeley Internet Name Domain (BIND) version 9.2.1. Zone transfers between the internal DNS and the external DNS server is not allowed, to prevent crackers from mapping out internal network, if the external DNS server has been compromised.

The WEB server uses Microsoft Internet Information Services 5.0 (IIS) on a Microsoft Windows 2000 server. The database server is separate from the web server, thus even if the web server is compromised, the database is always secured inside the intranet. In the web server all unnecessary software has been removed, all the patches to the software (especially patches to protect against hostile browsers) have to be applied, software such as e-mail, FTP, TFTP, telnet is not enabled. The firewall should disallow FTP, TFTP, telnet and every request on any port not specifically configured for incoming requests. Detailed description on Internet Information Services 5.0 can be found on the following Microsoft web page: http://www.microsoft.com/windows2000/technologies/web/default.asp.

The mail server is used for electronic mail that enters or exists in the GIAC network via the internet. I selected a Microsoft Windows 2000 server, running Microsoft Exchange 2000 with SP2, because in Microsoft Exchange 2000 it is possible to find some useful built in security feature, like virus scanning or disabling of executable attachments. It is important to notice that an e-mail server uses specific TCP/IP ports that are well known to hackers. For more information on the Microsoft Exchange 2000 server, you can look the following web site: http://www.microsoft.com/exchange/default.asp.

The Log Server provides a centralized repository for log files, reporting access, changes, failures and intrusion into network devices and services. The log files come from routers, switch, firewall, proxy servers, web server and any other system where activities are logged. The log must be monitored and analyzed periodically, because they are the way by which it is possible to discover possible problems or attacks. The Log Server will also act as the Network Time Protocol (NTP) server to synchronize time in all other devices on GIAC network.

The proxy server runs on a Microsoft Windows 2000 server with SP2 and uses Microsoft ISA Server. The proxy server has many functions. It is used as a gateway for all traffic between the intranet and the internet, as a caching device for serving up web pages, saving bandwidth usage on internet lines. The most important function is that a proxy server is able to scan the payload of packets and compliments firewall (that only scans IP header). If you need to know more details on Microsoft ISA Server, look at the following page on Microsoft web site: http://www.microsoft.com/isaserver/.

On each segment, the devices are connected via a 3Com Superstack Switch 3300. It has 24 ports 10/100 BaseT Ethernet. It is possible to define one port as a monitoring port, allowing it to see traffic flowing on other switch ports. A switch can distinguish traffic on the network directed to different segment, reducing bandwidth occupation on each segment. The switch in the GIAC Intranet needs to route packets between the LAN segments defined and uses the routing capabilities given by the 3Com Superstack Switch Layer 3 Module. The 3Com Superstack Switch 3300 is not the latest model available from 3Com, but they were available on customer site. Look the 3Com web site for more information at the following URL: http://www.3com.com.

Intrusion Detection System (IDS), like Snort 1.8.7 sensor (see the web site http://www.snort.org), will be used to watch the traffic on the network, forwarding what it sees to the logging server for further analysis. The IDS sensor logs provide an important means of detecting unusual, unexpected or illicit activity on a network segment. While they are often located behind the firewall component, it is helpful to have them placed in the various segments of the overall network, when troubleshooting or analyzing attacks against the network. It is not necessary to have a sensor at every point, it is only necessary to be able to plug to each network segment as desired. IDS are connected to the monitoring ports

on the 3Com Superstack 3300 switches. The interface card itself is not assigned an IP address and is put into promiscuous mode, enabling it to listen, but not respond. Since there is no assigned IP address, the NIC can be connected to any segment at any time as desired.

All the equipments listed above will employ, if available, a redundant power supply and will be plugged into a different electrical circuit.

Finally, I will draw your attention on an important matter: guidelines and documents regarding to security issue should be accurately checked to avoid any known potential vulnerability.

Assignment 2 – Security Policy and Tutorial

In the assignment 2, the security policies defined to secure GIAC Enterprises network will be illustrated. I will also report a tutorial regarding some information on how you can customize your router, starting from a scratch device. I will not describe all the steps you have to complete to gain a full configuration, because you can find it on Cisco documentation, but will try to explain what is important to know to accomplish this task and our goals.

Border Router Configuration

Describing GIAC Enterprises network architecture, I stated that the border router is the first defense against any outside attack. This is obviously true, but it is true if we have to configure the router to do what we want it do: it must be the first defense for GIAC Enterprises network. It means that we have to configure the router so that appropriated statements cover all the securing issue, illustrated in the assignment 1.

The border router configuration can be divided in the following steps:

1. General configuration
2. Interfaces configuration
3. Access control list definition

In the following paragraphs, I will describe each of the four steps.

<u>General configuration</u>

The main purpose of the general configuration is to define router general characteristics, to disable unwanted services, to set up a login banner and to specify logging capabilities.

COMMAND	DESCRIPTION
hostname fd01k02	To set up our hostname. It is important to use hostname that aren't explicitly related to GIAC Enterprises reality to prevent every external identification attempt. Use innocuous name.
Service timestamps debug datetime localtime Service timestamps log datetime localtime	To enable the services that will time stamp all log and debug activity in the log
service password-encryption enable secret <password>	To store passwords using highest level encryption possible (usually MD5 hash) and to set up the password to be used to get to configuration mode on the router
no snmp-server	To disable simple network monitoring protocol (SNMP). Hackers should use it to find the devices on the network and their status. It is vulnerable to attack.
no service tcp-small-server no service udp-small-server	To disable services that run on port number less than 20. This services include: echo, discard, daytime, chargen
no ip finger	To disallow finger protocol requests. Hackers should use it to acquire a list of users that are logged in to a host.
no ip unreachables	To block all ICMP host unreachable messages
no ip redirects	To deny all ICMP redirects messages
no ip directed-broadcasts	To discard all packets targeting the broadcast address (use it to defend against smurf attacks)
no ip http server	To discard any ip datagram containing this option by disabling web administration interface of the router. We use command line. The router web server should be used for DOS attacks.
no ip bootp server	To discard any ip datagram containing this option by disabling bootp. Not used outside the protection of the firewall.
no ip proxy-arp	To discard any ip datagram containing this option by disabling arp.

no cdp run	To disable Cisco Discovery Protocol (CDP). We do not have any Cisco routers connected to this device.
no ip source-route	To discard any ip datagram containing this option by disabling ip source routing, that is a way to specify the path a packet uses to travel between hosts. IP source routing should be used to spoof the IP address of a valid host.
banner login ^C GIAC Enterprises Network Unauthorized access is prohibited. ^C	Warning message to inform that is better not to try to access the system, if not authorized
logging on logging 150.100.110.20 no logging console	To enable logging capabilities and to send all of our logs to the logging server (150.100.110.20), without write log messages to console
Ntp server 150.100.110.20	To define the ip of the ntp server
Line console 0 Password 7 <password> Login Exec timeout 10 0 Access-list 5 deny all Line vty 0 4 Access class 5 in	To allow logins only on the console for administrative purpose, we define an access list for the virtual terminals
IP domain-name Giacnetwork.com	To define the domain name this router is part of
IP nameserver 150.100.110.10	To provide the IP address of the DNS server
AAA new-model AAA authentication login GIACnet tacacs+ enable AAA authentication enable GIACnet tacacs+ enable AAA accounting exec default stop-only tacacs+ AAA accounting commands 0 defaults start-stop tacacs+ AAA accounting commands 1 defaults start-stop tacacs+ AAA accounting commands 15 defaults start-stop tacacs+ AAA accounting system default start-stop tacacs+ Enable password 7 <password>	To authenticate the user logging in to the router via a tacacs server. The AAA accounting commands provides system level information about commands entered at different privilege modes to the log file.
Tacacs-server host 150.10.110.20 key <password>	To identify the IP address of the tacacs server

Interface configuration

In the interface configuration are described the properties of the interfaces used.

COMMAND	DESCRIPTION
Interface serial0 Ip address 200.100.50.1 255.255.255.255 Ip access-group 101 in Ip access-group 102 out No ip redirects No ip unreachables No ip directed-broadcast No ip proxy-arp No cdp	To define the serial line to the ISP. Some services are explicitly disabled. There are defined the access lists to be applied to the interface for the inbound and outbound traffic.
Interface ethernet0 Ip address 150.100.1.1 255.255.255.0 No mop enabled No ip redirects No ip unreachables No ip directed-broadcast No ip proxy-arp No cdp	To define the ethernet interface. Some services are explicitly disabled.
Interface loopback0 Ip address 150.100.2.1 255.255.255.255 No IP directed-broadcasts	To define the loopback interface

Access control list definition

Access control lists provide basic traffic filtering capabilities and can be configured for all routed network protocol to filter the packets of that protocol as the packets pass through a router. If we do not define any access control list (ACL), the router will forward all traffic. Access control lists are used to specify what specific traffic must be allowed and what must be denied. The router examines each packet to determine whether to forward or drop the packet, based on the criteria specified within the access list. One of the most important reasons to configure access list is to provide security for your network. To provide traffic filtering, we have to create an access list definition and to apply the access list to an interface. It is possible to create one access list to filter inbound traffic and one access list to filter outbound traffic. When creating an access list, we define criteria that will be applied to each packet processed by the router. Typical criteria in access lists are source or destination address, protocol of the packet, port used.

There are various types of access control list:

- standard access list,
- extended access list

- reflexive access list.

The standard access list is defined by a number between 1 and 99, looks only at the source IP address and is the fastest acl because consumes less cpu cycles.

A number between 100 and 199 identifies the extended access list. It checks source IP address, destination IP address, the protocol, the port in the case of TCP or UDP, the ICMP type and the TCP flags on a packet. Extended access list can also be referred to by a name.

The reflexive access list is referred to only by a name and can also maintain a state table, in addition to all of the features of the extended access list. It is the most cpu demanding access control list.

The order of the rules in an ACL is very important because the ACLs are executed in a top-down line-by-line fashion: the first rule that applies to a packet examined is the only rule that will be applied. To save CPU time, we can move up rules that are used more often than others. If you try to speed-up your router moving up the rules most used, be careful that you respect the specifications: a packet that must be denied should not become permitted!!!

Every ACL list is closed by a "deny all" rule, therefore any traffic not explicitly allowed is automatically denied.

The format of the extended access list command is described in the "Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2" (http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800873a2.html), from where I take the following information:

To define an extended IP access list, use the extended version of the **access-list** global configuration command. To remove the access lists, use the **no** form of this command.

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]

For ICMP, you can also use the following syntax:

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

For IGMP, you can also use the following syntax:

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

For TCP, you can also use the following syntax:

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*]

For UDP, you can also use the following syntax:

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*]

Syntax Description

Access-list-number	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
dynamic *dynamic-name*	(Optional) Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.
timeout *minutes*	(Optional) Specifies the absolute length of time, in minutes, that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide.*
Deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword. Some protocols allow further qualifiers described below.
source	Number of the network or host from which the packet is being sent

	There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0. Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0.64 would be valid.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines."
Tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
Log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
log-input	(Optional) Includes the input interface and source MAC address or VC in the logging output.
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the section "Usage Guidelines."
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines."
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and

	range (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines." TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

For our purpose, two access control lists will be defined:

- The ACL 101 is used to control the inbound traffic on the serial interface
- The ACL 102 is used to control the outbound traffic on the serial interface

COMMAND	DESCRIPTION
Access-list 101 deny ip 150.100.0.0 0.0.255.255 any log	To deny packets that are sourced with GIAC IP address in order to prevent spoofing.
Access-list 101 deny ip 10.0.0.0 0.255.255.255 any log Access-list 101 deny ip 172.16.0.0 0.15.255.255 any log Access-list 101 deny ip 192.168.0.0 0.0.255.255 any log	To deny traffic to the addresses listed as reserved for private networks in RFC 1918.
Access-list 101 deny ip 127.0.0.0 0.255.255.255 any log	To deny packets using the loopback address
Access-list 101 deny ip 224.0.0.0 7.255.255.255 any log	To deny packets with a multicast address
Access-list 101 deny ip 240.0.0.0 0.255.255.255 any log	To deny packets with a

	reserved class E address
Access-list 101 deny ip 255.0.0.0 0.255.255.255 any log	To deny packets using a broadcast address
Access-list 101 deny ip host 0.0.0.0 any log	To deny any packets without an IP address
Access-list 101 deny icmp any any host-unreachable	To deny ICMP host unreachable messages
Access-list 101 deny icmp any any redirect	To block any potential packet that may be associated to IP spoofing attack
Access-list 101 permit tcp any any established log	To allow traffic related to an established tcp session
Access-list 101 permit tcp any host 150.100.50.10 eq 80 log Access-list 101 permit tcp any host 150.100.50.10 eq 443 log Access-list 101 permit tcp any host 150.100.50.10 eq 21 log	To allow http, shttp and ftp traffic to the web server
Access-list 101 permit tcp any host 150.100.50.10 gt 1023 established log	To allow established ftp traffic to ports number greater than 1023 on the web server
Access-list 101 permit tcp any host 150.100.50.20 eq 25 log Access-list 101 permit tcp any host 150.100.50.20 eq 110 log	To allow smtp and pop3 traffic to the mail server
Access-list 101 permit udp any host 150.100.50.30 eq 53 log Access-list 101 permit tcp any host 150.100.50.30 eq 53 log	To allow DNS queries to reach external DNS Server
Access-list 101 deny ip any any log	This is the final rule for ACL 101: it discards all the packets not otherwise permitted.
Access-list 102 deny icmp any any log	To block any outbound ICMP traffic
Access-list 102 permit ip 150.100.0.0 0.0.255.255 any log	To allow only traffic originated from GIAC network
Access-list 102 deny ip any any log	This is the final rule for ACL 102: it discards all the packets not otherwise permitted.

Tutorial: what is important to know to configure a router

The tutorial will analyze some characteristics of the IOS software used by router, looking from the point of view of the network engineer that has to put inside the router all the command and information to let the router itself to work properly and according to the policies defined.

I suppose that I am working with a new routed, not configured before. (If it is not true, you can destroy the configuration inside the router and start again as it was a scratch router.) I suppose also to performing the configuration tasks using the command line interface (CLI).

To gain access to the router, you have to connect an asynchronous terminal (a console) to the console port of the router, using the proper cable. I use a laptop running Microsoft Windows XP Professional and one of the available asynchronous terminal emulator, like Hyperterminal. You have to set up the connection profile, according to the following value:

- Baud rate: 9600
- Data bits 8
- Stop bits: 1
- Parity: none
- Flow Control: none

Before starting, I will point your attention on the facts that the command line interface is divided into many different modes and that the commands available to you at any given time depend on the mode you are currently in.

When you log in to the command line interface, you are in "User Exec" mode: in this environment only a limited subset of commands are available to you. In "User Exec" mode you can show some general information or use some generic commands, but cannot customize or change the configuration. The prompt that characterizes the "User Exec" mode is: router>. To exit from the "User Mode", type "logout".
When you are in "User Exec" mode, typing the keyword "enable" and providing the right password (if one has been defined), gain the access to the "Privileged Exec" mode, where are actually available the levels from 0 to 15. In "Privileged User" mode, using the default level (that is 15), you can issue any command. The prompt of the "Privileged User" mode is: router#.
If you want to set or modify the router configuration, you have to get into the "Global Configuration" mode, typing the keyword "configure terminal", available when you are in "Privileged User" mode. The prompt for the "Global Configuration" mode is: router(config)#.

The following table summarizes the command mode described above:

Command Mode	***Access Method***	***Prompt***	***Exit Method***
User Exec	Log in	Router>	Use the "logout" command
Privileged Exec	From the User Exec, use the "enable" command	Router#	To return to User Exec mode, use the "disable" command

Global Configuration	From the Privileged Exec, use the "configure terminal" command	Router(config)#	To return to the Privileged Exec mode use the "end" or "exit" command or press Ctrl-Z

Table 2

The previous table was taken from the "Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2" that you can find in: (http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ff9.html)

You have to remind that most commands are one-time commands and are not saved if the software reboots. If you make changes to the running configuration, do not forget to save it to the startup configuration, if you do want not to loose any item or parameter modified.
Use the "copy running-config startup-config" command to save any configuration changes to the startup configuration.
I have to notice that after initializing the router hostname, the word "Router" in the prompt will be replaced by the hostname.

To begin the router configuration, we have to get into the "Global Configuration" mode. From here, we can input all the command according to what I have described in the previous pages. Sometimes, and especially when you have to type all the access list command, it should be better to use a simple user-friendly editor like wordpad and then transfer that to the router using a cut and paste method or (it more professional) using a file transfer (TFTP). When you have finished, do not forget to save the configuration, before rebooting the router.

To close this brief tutorial, I wish to spend few words about the help capabilities provides by the Cisco IOS Software. It is a very powerful help and very easy to use. There is only a "keyword" to remind, if you need helps: it is "?".

For example:

- If you need to know the list of available command, enter a simply a question mark
- To complete a command keyword, enter a few known characters followed by a question mark
- For a list of option or other keyword to be used with a command, enter the command followed by a blank and a question mark

CISCO PIX Firewall configuration

The access control lists defined for the Cisco PIX firewall follow rules that are quite similar to the border router one: top down flow, implied deny all at the end of the list.

I do not list the entire configuration but will report only the commands as necessary to cover specific requirements of the present assignment. The Cisco web site (http://www.cisco.com/en/US/products/sw/secursw/index.html) contains a lot of documentation regarding Pix firewall software and some specific articles covering aspects on securing firewall.

I will use the same table layout used to illustrate Cisco border configuration.

COMMAND	DESCRIPTION
Hostname fw01r03	To assign a host name to the firewall
Enable password <password> encrypted	To set and encrypt password for the configuration and administrative functions of the firewall
Passwd <password> encrypted	To set an encrypted telnet password
IP address outside 150.100.1.2 255.255.255.0 IP address dmzone 150.100.50.2 255.255.255.0 IP address giacnet 150.100.100.2 255.255.255.0	To assign IP address to each interface
Interface ethernet0 100full Interface ethernet1 100full Interface ethernet2 100full	To set speed and mode of operation of each interface
Nameif ethernet0 outside security0 Nameif ethernet1 dmzone security50 Nameif ethernet2 giacnet security100	To assign a name to each Ethernet interface and to define the security level of the interface
Mtu outside 1500 Mtu dmzone 1500 Mtu giacnet 1500	To set a MTU of 1500 on all interfaces
Fixup protocol FTP 21 Fixup protocol HTTP 80 Fixup protocol ILS 389 Fixup protocol RSH 514 Fixup protocol SMTP 25 Fixup protocol SQLNET 1521 Fixup protocol SIP 5060 Fixup protocol SKINNY 2000 Fixup protocol RTSP 554	To define port assignment and to enable application inspection for the protocols specified.
AAA-server Giac-tech protocol tacacs+ AAA-server (giacnet) host 150.100.110.20	'AAA' statements set tacacs+ as the

AAA authentication telnet console Giac-tech AAA authentication SSH console Giac-tech	authentication protocol and give the IP address of the tacacs+ host. They also set access verification for certain services to the firewall console.
Telnet 150.100.120.0 255.255.255.0 SSH 150.100.120.0 255.255.255.0	To set telnet and SSH access to the firewall as coming from the GIAC IT Technical Staff LAN
Floodguard enable	Enables the Flood Defender to protect against flood attacks
NAT (giacnet) 0 0.0.0.0 NAT (dmzone) 0 0.0.0.0	Disables network address translation on our inside interfaces since we have NIC-registered addresses. It also requires that traffic initiates from an inside host unless explicitly given by a STATIC statement.
Static (DMZ, outside) 150.100.50.10 150.100.50.10 netmask 255.255.255.255 Static (DMZ, outside) 150.100.50.20 150.100.50.20 netmask 255.255.255.255 Static (DMZ, outside) 150.100.50.30 150.100.50.30 netmask 255.255.255.255	To define static mapping for the DMZ hosts that need to be contacted by the outside world.
Route outside 0.0.0.0 0.0.0.0 150.100.1.1 1 Route DMZ 150.100.50.0 0.0.0.255 1 Route giacnet 150.100.0.0 0.0.255.255 150.100.100.3 1	To define static routes for faster and more secure routing of packets.
Access-list inbound permit TCP any host 150.100.50.30 eq 53 Access-list inbound permit UDP any host 150.100.50.30 eq 53	To allow all DNS requests to reach external DNS server.
Access-list inbound permit TCP any host 150.100.50.10 eq 80 Access-list inbound permit TCP any host 150.100.50.10 eq 443 Access-list inbound permit TCP any host 150.100.50.10 eq 21	To allow access to our web server using http, shttp and ftp.
Access-list inbound permit TCP any host 150.100.50.20 eq 25 Access-list inbound permit TCP any host 150.100.50.20 eq 110	To allows smtp and pop3 traffic to reach the email server.
Access-list inbound permit TCP any host 150.100.110.30 eq 80 Access-list inbound permit TCP any host 150.100.110.30 eq 443	To permit http and shttp traffic to get to the internal proxy servers.
Access-list outbound permit TCP host 150.100.110.30 any eq 80 Access-list outbound permit TCP host 150.100.110.30 any eq 443 Access-list outbound permit TCP host 150.100.110.30 any eq 21 Access-list outbound permit TCP host 150.100.110.30 any eq 25 Access-list outbound permit TCP host 150.100.110.30 any eq 110	To allow the proxy server access using http, shttp, ftp, smtp and pop3.
Access-list outbound permit TCP host 150.100.110.40	Let the database server

150.100.50.10 any	communicate with the web server.
Access-list outbound permit TCP 150.100.120.0 255.255.255.0 150.100.50.0 255.255.255.0 any Access-list outbound permit ICMP 150.100.120.0 255.255.255.0 150.100.50.0 255.255.255.0 any	To allow hosts on the GIAC IT Technical LAN to access all devices in the DMZ
Access-list outbound permit TCP 150.100.130.0 255.255.255.0 150.100.50.0 255.255.255.0 any Access-list outbound permit ICMP 150.100.130.0 255.255.255.0 150.100.50.0 255.255.255.0 any	To allow hosts on the GIAC IT User LAN to access all devices in the DMZ
Access-list outbound permit TCP 150.100.120.0 255.255.255.0 150.100.1.0 255.255.255.0 any Access-list outbound permit ICMP 150.100.120.0 255.255.255.0 150.100.1.0 255.255.255.0 any	To allow hosts on the GIAC IT Technical LAN to access all devices in the perimeter zone.
Access-list dmzout permit TCP host 150.100.50.10 any eq 80 Access-list dmzout permit TCP host 150.100.50.10 any eq 443 Access-list dmzout permit TCP host 150.100.50.10 any eq 21	To allow the web server access using http, shttp or ftp.
Access-list dmzout permit TCP host 150.100.50.20 any eq 25 Access-list dmzout permit TCP host 150.100.50.20 any eq 110	To allow the mail server access using SMTP and pop3.
Access-list dmzout deny TCP host 150.100.50.30 150.100.0.0 255.255.0.0 eq 53 Access-list dmzout deny UDP host 150.100.50.30 150.100.0.0 255.255.0.0 eq 53	To deny the external DNS server access to the intranet using domain.
Access-list dmzout permit TCP host 150.100.50.30 any eq 53 Access-list dmzout permit UDP host 150.100.50.30 any eq 53	To allow the external DNS server all other access using domain.
Access-group inbound in interface outside	This statement binds the ACL “inbound” to the outside interface and applies to incoming traffic.
Access-group outbound in interface giacnet	This statement binds the ACL “outbound” to the giacnet interface and applies to incoming traffic.
Access-group dmzout in interface dmzone	This statement binds the ACL “dmzout” to the dmzone interface and applies to incoming traffic.

VPN Configuration

In the present network design, customers, partners and suppliers join GIAC Enterprises network using VPN. Partners and suppliers use a site-to-site connection, while customers use remote access functionality. In a site-to-site VPN connection, the traffic between the two sites flows through VPN devices. It is a good for a many to many access. Partners and suppliers have a permanent tunnel set up to connect their internal network to GIAC network. In this case, there is transparent access between their networks and our own, filtered only by any rules that has been defined on our firewall and theirs. Remote VPN access is used by customers and involves single devices accessing a VPN concentrator (in our case the PIX 515) that grant access to remote resources. IP Security Protocol (IPSec) will be implemented in the remote access configuration and will allow secure access to the remote users possessing Cisco VPN Client. IPSec comprises Internet Key Exchange (IKE) standards as well as secure data transfer standards: Authenticating Header (AH) and Encapsulating Security Payload (ESP). For our VPN, we have selected to use ESP, because provides data confidentially by encrypting data portion of the packet.

Now I will illustrate how to configure the PIX firewall to interoperate with a CA (Verisign Private Certificate Services) and obtain a certificate.

1.Configure the PIX firewall hostname:

Hostname fw01r03

2.Configure the PIX Firewall domain name:

domain-name Giacnetwork.com

3.Generate the PIX Firewall RSA key pair

ca generate rsa key 1024

4.Define a Certification Authority.

ca identify giacnetwork.verisign.com 200.201.202.203

(I suppose that giacnetwork.verisign.com is the CA name assigned by Verisign and 200.201.202.203 is the IP address of the CA)

5.Configure the parameters of communication between the PIX firewall and the certification authority:

ca configure giacnetwork.verisign.com ca 1 20 crloptional

6.Authenticate the CA by obtaining its public key and its certificate:

ca authenticate giacnetwork.verisign.com

7.Request signed certificates from your CA for your PIX firewall:

ca enroll giacnetwork.verisign.com <password> serial ipaddress
(before entering this command, you have to contact CA administrator because he must authenticate GIAC firewall manually, before granting its certificate.)

8.Verify that the enrollment process was successful using the command:

show ca certificate

9.Save the keys, certificates and CA configuration to flash memory

ca save all
write memory

Next step is to enable and configure Internet Key Exchange (IKE).

1.Enable IKE

isakmp enable outside

2.Define an IKE policy

isakmp policy 10 auth rsa-sig

3.Create an access list to define the traffic to protect

access-list 50 permit ip 150.100.1.0 255.255.255.0 100.100.1.0 255.255.255.0

4.Configure a transform set that defines how the traffic will be protected

crypto ipsec transform-set harder esp-3des esp-sha-hmac

5.Create a crypto map entry

crypto map giacsupp10 10 ipsec-isakmp

6.Assign the access list previously defined to the crypto map entry

crypto map giacsupp10 10 match address 50

7.Specify the peer to which the IPSec protected traffic will be forwarded

crypto map giacsupp10 10 set peer 147.148.149.150

(I suppose that 147.148.149.150 is the outside IP address of the firewall in the supplier's site)

8.Specify which transform sets are allowed for this crypto map entry

crypto map giacsupp10 10 set transform-set harder

9.Specify security association lifetime

crypto map giacsupp10 10 set security-association lifetime seconds 3600

10.Apply the crypto map to the outside interface, where the IPSec traffic will be evaluated

crypto map giacsupp10 interface outside

11.Specify that IPSec traffic is implicitly trusted

sysopt connection permit-ipsec

GIAC Partners and Suppliers must setup their VPN device configuration to match the rules reported above.

Finally, I will describe the setup procedure for configuring the CISCO VPN Client, on laptop of GIAC remote sales people and teleworkers. All the steps required are clearly described in the "Cisco PIX Firewall and VPN Configuration Guide Version 6.2", from where I take the customization example reported here. (see: http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a00800eb49b.html
and
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb72d.html#xtocid22)

The example has been modified according to the environment defined in the present assignment.

Follow these steps to configure the Cisco Secure VPN Client version 1.1:

Step 1 Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Security Policy Editor**.

Step 2 Click **Options**>**Secure**>**Specified Connections**.

Step 3 In the Network Security Policy window, click **Other Connection** and click **Non-Secure** in the panel on the right.

Step 4 Click **File**>**New Connection**. Rename New Connection. For example, **GIACNET**.

Step 5 Under **Connection Security**, click **Secure**.

Step 6 Under **Remote Party Identity and Addressing,** set the following preferences in the panel on the right:

a. ID Type—Click **IP address**.

b. Enter the IP address of the internal host within the PIX Firewall unit's internal network to which the VPN Client will have access. Enter **150.100.50.3**.

c. Click **Connect using Secure Gateway Tunnel**.

d. ID Type—Click **IP address**.

e. Enter the IP address of the outside interface of the PIX Firewall. Enter **150.100.1.2**

Step 7 In the Network Security Policy window, click the plus sign beside the GIACNET entry to expand the selection, and click **My Identity**. Set the following preferences in the panel on the right:

a. Select Certificate—Click **None**.

b. ID Type—Click **IP address**.

c. Port—Click **All**.

d. Local Network Interface—Click **Any**.

e. Click **Pre-Shared Key**. When the Pre-Shared Key dialog box appears, click **Enter Key** to make the key field editable. Enter **cisco1234** and click **OK**.

Step 8 In the Network Security Policy window, expand Security Policy and set the following preferences in the panel on the right:

a. Under **Select Phase 1 Negotiation Mode, c**lick **Main Mode**.

b. Select the **Enable Replay Detection** check box.

Leave any other values as they were in the panel.

Step 9 Click **Security Policy**>**Authentication (Phase 1)**>**Proposal 1** and set the following preferences in the panel on the right:

a. Authentication Method—Click **Pre-shared Key**.

b. Encrypt Alg—Click **Triple DES**.

c. Hash Alg—Click **MD5**.

d. SA Life—Click **Unspecified** to accept the default values.

e. Key Group—Click **Diffie-Hellman Group 1**.

Step 10 Click **Security Policy**>**Key Exchange (Phase 2)**>**Proposal 1** and select the following values in the panel on the right:

a. Select the **Encapsulation Protocol (ESP)** check box.

b. Encryption Alg—Click **Triple DES**.

c. Hash Alg—Click **SHA-1**.

d. Encapsulation—Click **Tunnel**.

Step 11 Click **File**>**Save Changes**.

The VPN Client is now activated.

Assignment 3 – Verify the Firewall Policy

GIAC management asked us to conduct a technical audit of GIAC's primary firewall in order to verify that the policies are correctly enforced and to identify any potential vulnerability that may exist within the network design.
The technical audit will be conduct in cooperation with GIAC IT technical staff people. Together we will use a project management approach to define all the aspects involved: planning, execution, control, risk analysis, resource, costs, and deliverables.

Plan the technical audit.

To plan the technical audit we have to:

- Describe the technical approach we will use to assess the firewall
- Include consideration as what shift or day we would do the assessment
- Estimate costs and level of effort
- Identify risks and considerations, specifying how the will be addressed

Technical approach to assess the firewall.

The main goal of the present technical audit is to verify that the policies implemented in the firewall work, as we want they work. It means that GIAC Enterprises business model, the GIAC security policies and the rules used by the firewall are our starting point, because it should be not true that the firewall customization satisfies all the security policies defined to accomplish, in a safety manner, the GIAC business needs. For example, if a policy is defined but is out of right order, the firewall does not work, as we should expect. In the same manner, auditing the firewall policy we can find a service that is available while it should be unavailable or a service that is unavailable while it should be available. Obviously, if we have done a good work, the number of such situation should be as low as possible, ideally zero.

To test the firewall policies, we have to work on different network (internet, DMZ network, GIAC intranet), pointing server or service that we have to reach through the firewall.

The audit must check that all the required item defined in the security policy are satisfied. To do this, based on what we define the firewall should do, we have to prepare a checklist that we use to verify what really happens.

In the checklist, for each item, you will find four fields:

- the first field is the test number;
- the second one describes the check we have to perform;
- the third one describes the desired result;
- the forth one is the result of the real test: it may be “OK” if the result matches the expectation, or may contain the description of the difference between the real situation and what I expected.

The checklist used to audit the GIAC’s primary firewall is reported in the paragraph describing how the audit is conducted.

Define what we have to do while conducting the technical audit is important because we can select what kind of instruments we need to use. Usually it is sufficient to have a network port scanner, a sniffer and to use the data available, provided by the IDS o stored in the log server. I will give more detailed information on which instruments I will use, when I will describe how the audit is conducted.

Resources, schedule and costs

A team will conduct the audit: our security technical consulting works together with GIAC IT technical staff. The people selected to apply in this job are: John Smith (Technical Security Manager), Mark Cooper (Senior IT Network Administrator) and David Bush (IT Consulting). They are very happy to work in this activity, because it is an excellent opportunity to verify and, sometimes, to improve their knowledge.

The technical audit will be conducted during main business hours. Three days have been scheduled to perform the audit: the first day is used to define a plan that will be submitted to GIAC management for approval, during the second day we will conduct the tests, the last day is reserved to analyze the results and to prepare audit report for the GIAC management.

We estimate that the total cost of the technical audit of GIAC's primary firewall will be less than € 10.000,00.

Risks and other considerations

It is important to inform GIAC management and GIAC IT technical staff on the implicit risks involved with conducting the audit. The risks include the possibility that, while conducting the tests, some systems should offer poor performance, may hang, crash or become unavailable or damaged. It means that GIAC IT technical staff must provide all the guarantees regarding backup availability and efficiency of disaster recovery procedures. If we need to use them, we must be sure that they work properly.

Another consideration is related to system resources and bandwidth: they should be heavily stressed during the audit. We should try to affect the business operations of GIAC Enterprises as less as possible and will inform the management when the test related to the technical audit will be finished.

Conduct the technical audit

Regarding to the technical audit of GIAC's primary firewall in order to verify that the policies are correctly enforced, the following checklist has been defined:

Test	Description	Desired result	Test result
1	Verify that the Cisco Pix firewall has been installed using the latest firmware and that all security issue about Cisco Pix firewall have been correctly investigated and any recommendation has been applied.	Cisco Pix firewall uses the latest firmware. All known security recommendations has been analyzed and, if necessary, applied	
2	Verify that the mail server in the DMZ	The smtp and pop3 services	

	zone is accessible from the internet, using the services enabled	on the mail server are accessible from the internet	
3	Verify that the mail server in the DMZ zone is not accessible from the internet, using the services not enabled	Any other service, distinct from smtp and pop3, is unavailable on the mail server	
4	Verify that the external DNS server in the DMZ zone is accessible from the internet, using the services enabled	The domain services (tcp/53 and udp/53) on the external DNS server are accessible from the internet.	
5	Verify that the external DNS server in the DMZ zone is not accessible from the internet, using the services not enabled	Any other service, distinct from tcp/53 or udp/53, is unavailable on the external DNS server	
6	Verify DNS effectiveness	Verify that a DNS query from internet, regarding a host located in the DMZ zone, will resolve name and IP address, while no name resolution is obtained for hosts in the GIAC intranet	
7	Verify that the web server in the DMZ zone is accessible from the internet, using the services enabled	The http, shttp and ftp services on the web server are accessible from the internet.	
8	Verify that the web server in the DMZ zone is not accessible from the internet, using the services not enabled	Any other service, distinct from http, shttp or ftp, is unavailable on the web server	
9	Verify that the mail server in the DMZ zone is accessible from the GIAC intranet, using the services enabled	The smtp and pop3 services on the mail server are accessible from the GIAC intranet	
10	Verify that the web server in the DMZ zone is accessible from the GIAC intranet, using the services enabled	The http, https and ftp services on the web server are accessible from the GIAC Intranet.	
11	Verify that user in the GIAC intranet can use http to navigate in the internet	Using a browser, be able to connect to a generic URL, like http://www.cisco.com outside GIAC network	
12	Verify that remote user connecting via VPN can access GIAC network	Connect to the GIAC Network and browse GIAC web homepage, using the laptop, where all the software has been properly customized, like that provided to sales people	
13	Control reconnaissance exposition (DNS, ICMP message, SNMP,…)	GIAC servers and network devices does not provide critical network information to external sources	
14	Verify logging facility effectiveness	The logs contain the appropriate traffic information and record any	

		scan activity detected	
15	Verify that the firewall is located in a safety alarmed room, mounted in a rack key locked, and that the access is limited to authorized GIAC IT technical user	The firewall must be located in a safety-alarmed room, mounted in a rack key locked. The door of the room must be locked. The access to the alarmed room is limited only to authorized GIAC IT technical users. They use a smart cart and a personal ID Code to unlock the door.	
16	Verify that the logon console is password protected and check the list of users authorized to modify the firewall configuration	Logon to the firewall is password protected. Only selected GIAC IT Technical users are authorized to admin firewall	
17	Verify that a copy of the firewall configuration is stored encrypted in a safety place	Control that a stored encrypted copy of the firewall configuration exists in a safety place	
18	Verify potential weakness, checking the last report available of the twenty most critical internet security vulnerabilities (see the web site http://www.sans.org/top20/)	Potential vulnerabilities has been removed	

Before starting the audit, the checklist is submitted to GIAC management for any required approval.

To conduct the technical audit of GIAC's primary firewall in order to verify that the policies are correctly enforced, we will essentially use nmap 3.0, a free tool that can be downloaded from the web site http://www.insecure.org/nmap . We will use nmap 3.0 from command line, but sometimes the graphical interface should be more impressive and easy to use. I report a brief description of the tool, as I have found on the web:

> "Nmap (that means Network Mapper) is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways 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 runs on most types of computers, and both console and graphical versions are available".

Nmap will be used to look for hosts behind the firewall, to find open ports and to try to guess what operating system is being run on the host we find.

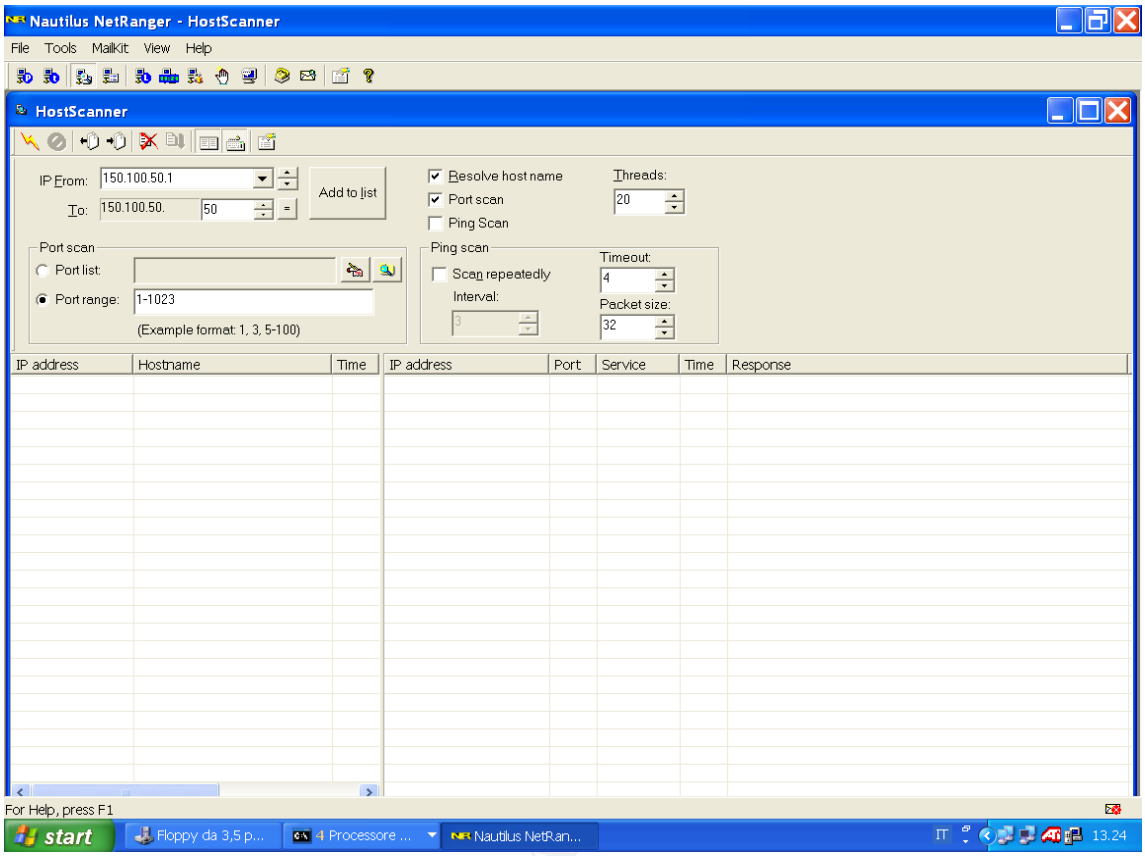
The main options and flags available when using nmap, as are visualized issuing the command nmap without options or parameters, are:

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

For more information on nmap options and usage, read the document available at the following web site: http://www.insicure.org/nmap_documentation.html.

Another nice network tool is Nautilus Netranger version 3.02, provided by Nautilus Digital. It is a tool very easy to use, with a graphical interface, and runs on Microsoft Windows 2000/XP, so that it should be proposed to GIAC IT Technical Staff as a first aid instrument, when they want control their network. Nautilus Netranger includes a lot of network tool: host scanner (to pingscan or portscan hosts or networks), ping, traceroute, lookup (to obtain information using DNS), finger, whois, netinfo, and so on. You can find more information about Nautilus Netranger on the Nautilus Digital web site: http://www.nautidigital.com .

The follow picture shows how Nautilus Netrange hostscanner looks like:



The tools (nmap and netranger) has been installed in a laptop that can be easily plugged in to the switch placed in the perimeter zone or in to the one placed in the dmz zone or in the GIAC intranet, because we have to run our tests, acting from different network. Sometimes we try to compare the results given by the two tools (they must be equal, but if they were different it is time to open our eyes to investigate the reasons of the difference).

To run some of the test reported on the checklist, I will use commands generally available as part of operating system like ping, nslookup or netstat. I suppose that such commands are well known and do not speak more about them. Nslookup will be use to test DSN server functionality.

To exploit vulnerabilities, I suggest use the tool Nessus, available from http://www.nessus.org. Nessus is another port scanner, running in Unix environment. Nessun can detect what are the server running on a given port and is very useful to discover vulnerabilities: it is able to tell you how the vulnerabilities could be exploited.

In our case, using nmap, the command used to run a port scan on the ipaddress aaa.bbb.ccc.ddd. is:

```
nmap  -v –P0  -sS   aaa.bbb.ccc.ddd
```

For example, if we have to run the test to check which TCP ports are open on the mail server in the DMZ zone, acting from the GIAC IT technical lan, I should issue the following command:

```
nmap –v  -P0  -sS  150.100.50.20
```

The output of the previous command is

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (150.100.50.20) appears to be up ... good.
Initiating SYN Stealth Scan against  (150.100.50.20)
Adding open port 25/tcp
Adding open port 110/tcp
The SYN Stealth Scan took 1 second to scan 1601 ports.
Interesting ports on  (150.100.50.20):
(The 1599 ports scanned but not shown below are in state: closed)
Port       State      Service
25/tcp     open       smtp
110/tcp    open       pop3

Nmap run completed -- 1 IP address (1 host up) scanned in 10 seconds
```

The output shows that: host 150.100.50.20 exists and is alive, the tcp/25 port (smtp) and tcp/110 port (pop3) are opened, and others TCP ports are closed. It matches the policy we have defined.

If I issue the same command, but acting from the internet (i.e. outside the firewall), the output provided is:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (150.100.50.20) appears to be up ... good.
Initiating SYN Stealth Scan against  (150.100.50.20)
Adding open port 25/tcp
Adding open port 110/tcp
The SYN Stealth Scan took 1 second to scan 1601 ports.
Interesting ports on  (150.100.50.20):
(The 1599 ports scanned but not shown below are in state: filtered)
Port       State      Service
25/tcp     open       smtp
110/tcp    open       pop3

Nmap run completed -- 1 IP address (1 host up) scanned in 10 seconds
```

The output looks like similar, but you should notice the difference: in the first output, the line starting with "(The 1599 ports scanned but not shown …" shows a state of "closed", while the second one reports a state of "filtered". It is right and it is important. It means that:

- in the first case, nmap was able to get from the mail server the information about the state of the TCP ports not opened (they are "closed")

- in the second one, nmap cannot get specific information from the mail server, about the state of the TCP ports not opened, because the IP packets using TCP ports distinct from tcp/25 and tcp/110 are blocked by the firewall, according to the defined policies.

Using the Syn Stealth scan, nmap is able to show filtered TCP port. You can get the same information about filtered TCP ports, using an ACK scan.
In a Syn Stealth scan, a TCP connection with a remote host is initiated by sending the initial Syn. If the packet crosses the firewall and the remote host responds with a Syn/Ack (TCP port opened), it is possible to quickly shutdown the connection, because we have get all the information we desire. For this reason the scan is named "stealth".

Evaluating the audit

The result of the tests is reported in the checklist sheet.

Test	Description	Desired result	Test result
1	Verify that the Cisco Pix firewall has been installed using the latest firmware and that all security issue about Cisco Pix firewall have been correctly investigated and any recommendation has been applied.	Cisco Pix firewall uses the latest firmware. All known security recommendations has been analyzed and, if necessary, applied	Cisco Pix firewall is running firmware vers. 6.2 Any suggested recommendation has been applied. ***OK***
2	Verify that the mail server in the DMZ zone is accessible from the internet, using the services enabled	The smtp and pop3 services on the mail server are accessible from the internet	Accessible from the internet are the following ports: Tcp 25 Tcp 110 ***OK***

3	Verify that the mail server in the DMZ zone is not accessible from the internet, using the services not enabled	Any other service, distinct from smtp and pop3, is unavailable on the mail server	Ports not used are filtered by the firewall ***OK***
4	Verify that the external DNS server in the DMZ zone is accessible from the internet, using the services enabled	The domain services (tcp/53 and udp/53) on the external DNS server are accessible from the internet.	Accessible from the internet are the following ports: Tcp 53 Udp 53 ***OK***
5	Verify that the external DNS server in the DMZ zone is not accessible from the internet, using the services not enabled	Any other service, distinct from tcp/53 or udp/53, is unavailable on the external DNS server	Ports not used are filtered by the firewall ***OK***
6	Verify DNS effectiveness	Verify that a DNS query from internet, regarding a host located in the DMZ zone, will resolve name and IP address, while no name resolution is obtained for hosts in the GIAC intranet	Web server resolved. Logging Server not resolved ***OK***
7	Verify that the web server in the DMZ zone is accessible from the internet, using the services enabled	The http, shttp and ftp services on the web server are accessible from the internet.	Accessible from the GIAC Intranet are the following ports: ftp 21 http 80 shttp 443 ***OK***
8	Verify that the web server in the DMZ zone is not accessible from the internet, using the services not enabled	Any other service, distinct from http, shttp or ftp, is unavailable on the web server	Ports not used are filtered by the firewall ***OK***
9	Verify that the mail server in the DMZ zone is accessible from the GIAC intranet, using the services enabled	The smtp and pop3 services on the mail server are accessible from the GIAC intranet	Accessible from the GIAC intranet are the following ports: Tcp 25 Tcp 110 ***OK***

10	Verify that the web server in the DMZ zone is accessible from the GIAC intranet, using the services enabled	The http, https and ftp services on the web server are accessible from the GIAC Intranet.	Accessible from the GIAC intranet are the following ports: ftp 21 http 80 shttp 443 ***OK***
11	Verify that user in the GIAC intranet can use http to navigate in the internet	Using a browser, be able to connect to a generic URL, like http://www.cisco.com, outside GIAC network	We are able to browse Cisco home page. ***OK***
12	Verify that remote user connecting via VPN can access GIAC network	Connect to the GIAC Network and browse GIAC web homepage, using the laptop, where all the software has been properly customized, like that provided to sales people	After user authentication, we are able to browse GIAC home page ***OK***
13	Control reconnaissance exposition (DNS, ICMP message, SNMP,…)	GIAC servers and network devices does not provide critical network information to external sources	Test passed. ***OK***
14	Verify logging facility effectiveness	The logs contain the appropriate traffic information and record any scan activity detected	The logs have been reviewed. They contain scanning activities and appropriate traffic information. ***OK***
15	Verify that the firewall is located in a safety alarmed room, mounted in a rack key locked, and that the access is limited to authorized GIAC IT technical user	The firewall must be located in a safety-alarmed room, mounted in a rack key locked. The door of the room must be locked. The access to the alarmed room is limited only to authorized GIAC IT technical users. They use a smart cart and a personal ID Code to unlock the door.	Test passed. ***OK***
16	Verify that the logon console is password protected and check the list of users authorized to modify the firewall configuration	Logon to the firewall is password protected. Only selected GIAC IT Technical users are authorized to admin firewall	Test passed. ***OK***
17	Verify that a copy of the firewall configuration is stored encrypted in a safety place	Control that a stored encrypted copy of the firewall configuration exists	Test passed. ***OK***

		in a safety place	
18	Verify potential weakness, checking the last report available of the twenty most critical internet security vulnerabilities (see the web site http://www.sans.org/top20/)	Potential vulnerabilities has been removed	Test passed. ***OK***

As you can see, the policies defined in the GIAC's primary firewall are correctly enforced. It is a good result.

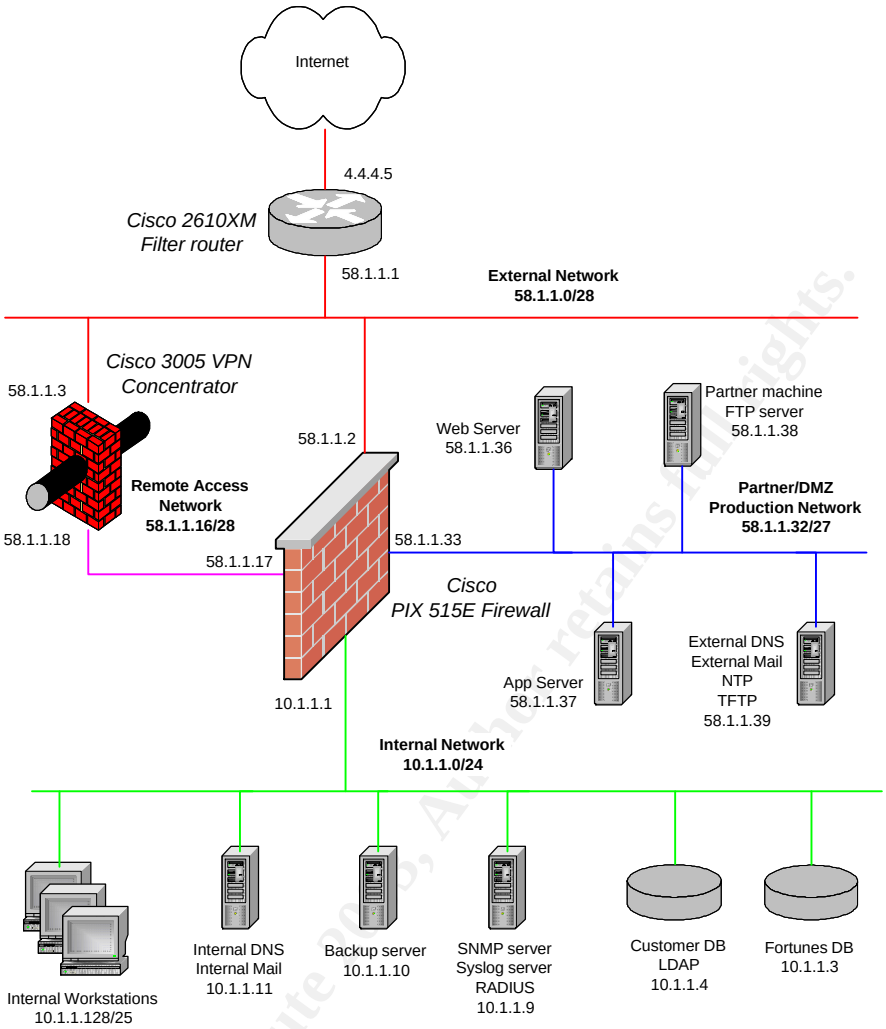
This is our new starting point, because now we have to discover any improvements or re-design architecture to preserve or increase IT security.

Analyzing the audit results and reviewing the GIAC Network design, we should make the following recommendations:

1. Review GIAC IP addressing to explore the use of NAT in order to hide GIAC IP address to the internet
2. Duplicate some critical resource that should compromise your business, like web server, mail server, database server, …).
3. Use two different links from GIAC Network to internet, through two different ISP
4. Activate solutions able to improve general availability, clustering web server or mail server or any other critical server, or using high availability feature that you can find in some of the recently announced network devices (router, firewall, switch)
5. Use a secondary firewall to protect more the servers and/or the hosts in the GIAC Intranet. It is a good practice to use multiple manufacturing while selecting the devices to use in a network design in order to minimize the effects related to any single vulnerability. We suggest Firewall-1 from Checkpoint Software, as secondary firewall.

Assignment 4 – Design under Fire

For my "Design under fire", I selected the network design proposed by Steve Keifling , posted on June 5,2002, that can be found in the following web page http://www.giac.org/pratical/Steve_Keifling_GCFW.doc. Looking at the following picture, you can see that the firewall used in the Steve Keifling 's network design is a Cisco PIX 515E with four network interfaces.



Attack against to the firewall

For the purpose of the present assignment, I suppose that I do not know the Steve Keifling 's network design. One of the tasks needed to attack a firewall is to discover as much details as possible on my target. When I start the discovery process, the only information I know is the URL of GIAC Enterprises's web site: it is www.giac.com. It is not enough, but it is sufficient to begin my effort.

To conduct the reconnaissance task, I begin to navigate the GIAC web site, as I were a normal customer looking for fortune cookie sayings, but my interests are really concerned to other information I can find there, like names, telephone numbers, locations, contact point, organization structure an so on. For example, I will try to edit the html source code of their web pages where some developers should leave details about IP addresses, operating systems, type of web server engine and so on.

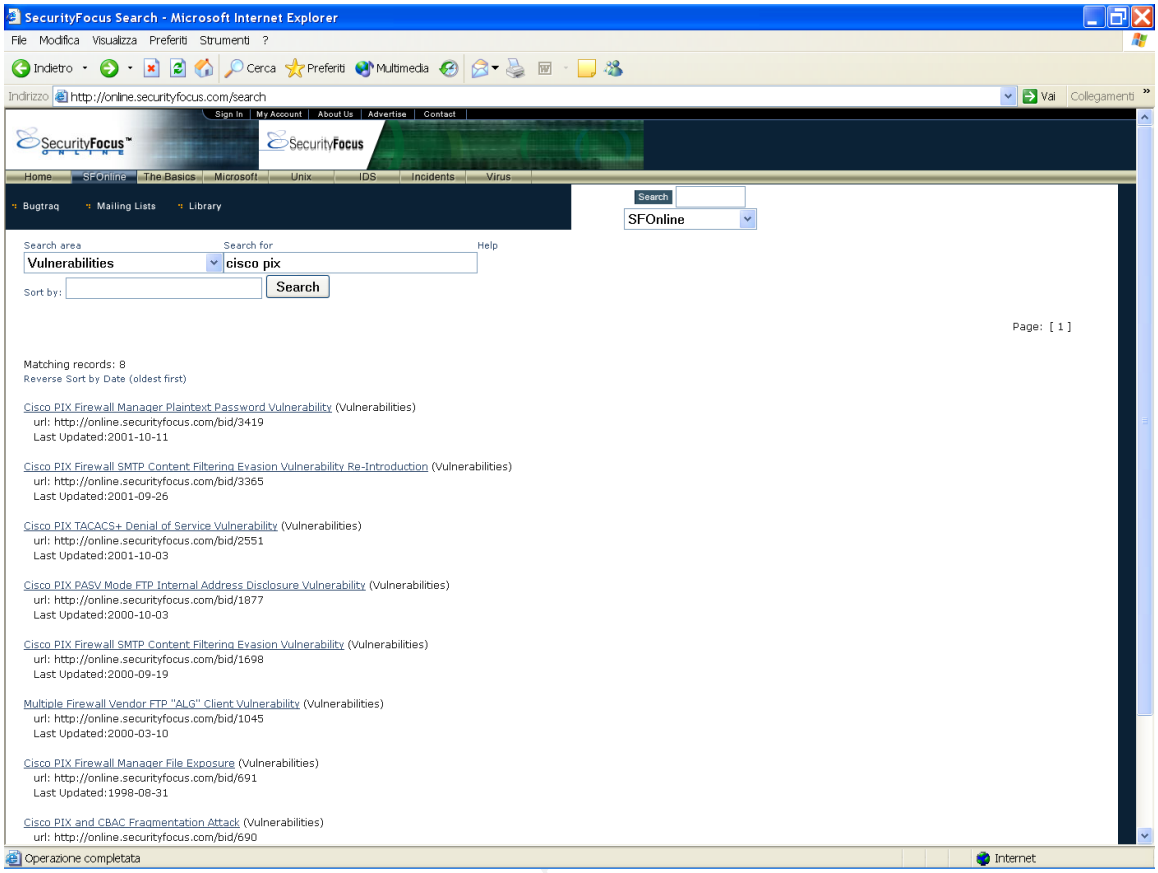
Next step is to explore GIAC network, using some common commands, like nslookup, traceroute, or tool like nmap, available from http://www.insecure.org/nmap. While exploring GIAC network, it is important to employ as much stealth as possible, because I do not want to raise alarms on GIAC IT network administrator, leaving that my suspicious activity is detected by IDS o reported in the security log. To do this, I initially will try to explore what I thing it is generally available, using services or ports that should be enabled and not blocked by the firewall. For example, to gather more information on the web site, if I use nmap, I try the following command, using TCP port 80 (http):

```
Nmap –v –sS –O –p 80 –v www.giac.com
```

When I know the IP address of the web site, I can use the command traceroute to map out something about GIAC's network layout, discovering the border router and the firewall. Now I am ready to gather more information about my target, the firewall, and the most useful tool is again nmap. Step by step, I can increase my knowledge of the GIAC firewall, so that I know it is a Cisco Pix 515 Firewall, I know its IP address, I know which are the ports opened and so on. When I have sufficient information, I begin to search in the Internet for known vulnerability and tools that can exploit it. First, I look into the Cisco web site (http://www.cisco.com), pointing my attention to documents as the PIX firewall software release notes or the Cisco PSIRT (product Security Incident Response Team) advisories. Next, I connect to the web site of specialized organizations that provide a lot of up to date information about bugs and weakness in software and hardware. Here are some of the sites I search:

- http://www.cert.org
- http://www.sans.org/newlook/digests
- http://www.securityfocus.com
- http://cve.mitre.org

The following screen shot of a Securityfocus web page contains the results obtained searching Cisco Pix Vulnerabilities.



I have analyzed the details of the known vulnerabilities, but new Cisco PIX firewall version 6.2 contains all the necessary patches and update to remove them. I think that patches and any update are installed in to the GIAC firewall: the vulnerabilities that I have found should be inappropriate to attack the firewall.

Searching the Cisco web site, I found a field notice reporting a bug detected in Cisco PIX 515 and 506. You can see the problem description of the bug on the page http://www.cisco.com/warp/public/770/fn15490.shtml. It states that:

"Some PIX 515 systems will hang and become unresponsive, typically triggered by higher traffic throughput level. …. This failure occurs regardless of the PIX OS version installed."

The problem symptoms are:

"When the PIX hangs, all interfaces stop passing traffic and the console port becomes unresponsive. No crash or stack trace is seen on the console port, and the system does not reboot on its own. The only way to return the unit to operation is by manually resetting the power."

The problem affects the equipments that have been manufactured before October 2001.
The workaround is to reduce the traffic throughput level to the point where the hang does not occur.
The solution of the problem is to replace the failed hardware.

I do not know when GIAC has introduced the firewall in his network, but October 2001 is not too far…. I will try to hang the GIAC firewall.

To conduct the attack against the GIAC firewall, I have to increase the traffic throughput, flowing the firewall, above the level point where the hang occur.
I can use a DDoS (Distributed Denial of Service) tool to attack the firewall. A Distributed Denial of Service (DDoS) uses multiple systems to attack simultaneously the target, in a coordinated fashion. My favorite Distributed Denial of Service (DDoS) tool is Tribe Flood Network 2000 (TFN2K), available from http://packetstormsecurity.org. I will use 50 compromised cable modem/DSL systems – the same that I will use next to conduct a DDoS attack – that will send a TCP SYN flood attack against the web server on port 80, through the firewall. If you put the IP address of the 50 compromised cable modem/DSL system in a file (killer_list.txt), you can use the following command to launch the attack against the firewall:

```
tfn –f ./killer_list.txt –c5 –i 58.1.1.36 –p 80
```

Does the Cisco PIX firewall hang? To control what happens, I use nmap to scan ports on the DNS server and on the web server. I know the ports opened in the DNS Server and in the web server, but I will use the nmap scan only to verify if my data are able to flow through the firewall. If I do not receive the right answer to the scan, it means that the attack was successfully.

Denial of Service attack

A Denial of Service (DoS) attack makes unavailable services or networks by consuming their resources or making them fail. Network DoS is more dangerous because it compromises all the resource behind the network link.
My denial of service attack will try to saturate the WAN link connecting ISP to the GIAC border router, to deny legitimate customers or employees the online services provided by GIAC Enterprises. I suppose that the link connecting GIAC network to the ISP is a T1 line (1,54 Mbps). If I use 50 compromised cable modem/DSL hosts, I can overwhelm the T1 bandwidth providing a minimum sustained data rate of 30 Kbps for each of the compromised cable modem/DSL systems. It should be easily achieved, because the line rate of cable modem/DSL hosts is usually in the hundreds of Kbps throughput range.

I will use the DDos tools TFN2K, available from http://packetstormsecurity.org, to attack against the GIAC router ip address. The file killer_list.txt contains the IP address list of my 50 compromised cable modem/DSL systems that will send a mixed flood (UDP/TCP/ICMP) against to the GIAC router ip address 58.1.1.1, when I execute the following command:

```
tfn –f ./killer_list.txt –c8 –l 58.1.1.1
```

By overwhelming the WAN link connecting ISP to the GIAC border router, the legitimate users are locked out or become frustrated by very long response time.

There is no easy way to prevent DDoS attacks. They should be stopped as close to the source as possible. The countermeasures that can be put into place to mitigate the attack are:

- Ask the ISP to place an intrusion detection system at ISP site, to detect and block any suspicious traffic from offending IP addresses to GIAC network
- Apply anti spoofing rules at the network boundary
- Set up on the border router the appropriate rate limit for SYN or ICMP packets
- Enable detection of unsolicited ICMP echo replies or unusually high traffic levels
- If available, enable SYN-flood protection on the firewall
- Make available backup network devices (essentially another border router and another firewall), configured with “external” IP addresses distinct from that normally used, to enable a different path to connect GIAC network to the ISP. (You should need to have another route path to GIAC network defined in the ISP router). If a DoS attack occurs, you can power off the compromised border router and/or internal firewall and activate the backup devices. Such countermeasure does not prevent DoS attacks, but can help to mitigate their effects, limiting services unavailability, because now the attacker does not known the new IP address and have to discover it again.
- Increase ISP WAN link to mitigate the problem
- Maintain the practice of monitoring, testing, reviewing and improving the network security

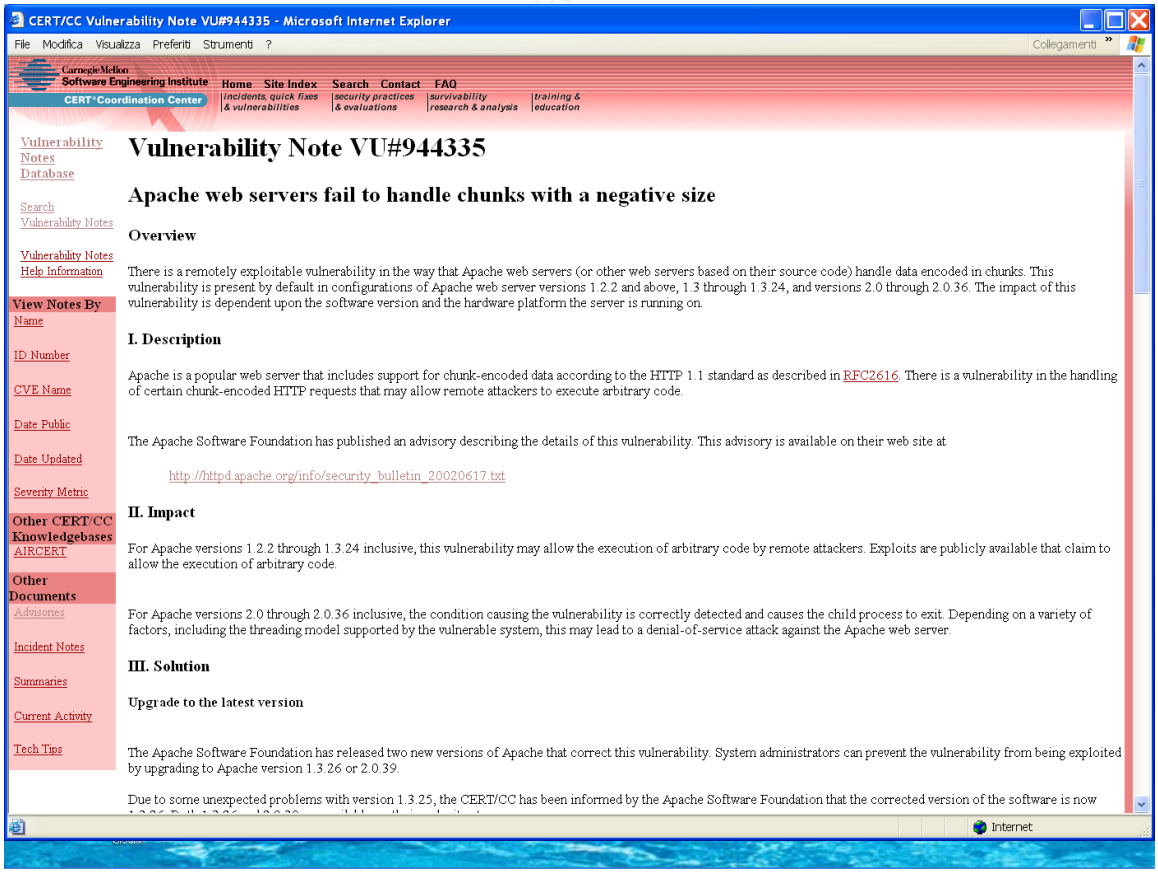
Other suggested methods to prevent distributed denial of service attacks are reported in the following documents:
“Strategies to protect against Distributed Denial of Services (DDoS) Attack”, that you can find in Cisco web site, at the following URL address:
http://www.cisco.com/warp/public/707/newsflash.html
or
“Denial of service Attack – DDOS, SMURF, FRAGGLE, TRINOO”
that you can find in Infosyssec web site, at the following URL address:
http://www.infosyssec.com/infosyssec/secdos1.htm
or

"Help Defeat Denial of Service Attacks: Step-by-Step"
that you can find in SANS Institute web, at the following URL address:
http://www.sans.org/dosstep/index.htm.

Attack plan to compromise an internal system through the perimeter system.

I will illustrate the plan to compromise an internal system through the perimeter system. While I was thinking about what internal system I wish to compromise, I received a mail with the latest news about critical internet security vulnerabilities. I read the document "The Twenty Most Critical Internet Security Vulnerabilities", that you can find in the site http://www.sans.org/top20, updated on 7th October 2002, and found some interesting information about Apache Web Servers vulnerabilities. It is a great idea to compromise the GIAC web server, because – do not forget it – GIAC is an e-business company.

I was attracted by the vulnerability affecting Apache Web Servers, identified as CERT Advisory CA-2002-17 and described by vulnerability note VU#944335: Apache Web servers fail to handle chunks with a negative size. I report a screen shoot taken from the web at http://www.kb.cert.org/vuls/id/944335.



I know that Apache web server running in GIAC network is version 2.0.36, because it is one of the information gathered during the reconnaissance task.

It means that, as reported in the documentation, "the condition causing the vulnerability is correctly detected and causes the child process to exit", but "… this may lead a denial-of service attack against the Apache web server". It is not too hard to set up an environment where some compromised systems send to the GIAC web server a flood of appropriate chunk-encoded http requests. It is again a DDoS attack.

I am quite confident that the attack should be successfully, because http can flow from the internet to the web site, but I will compromise the web server if the bandwidth of the wan link to ISP and the throughput of the network devices involved (border router and the firewall) are able to sustain so intensive http traffic.

To remove the vulnerability, the Apache web server should be upgraded to the latest version available.

References

Books

Simson Garfinkel and Gene Spafford
Practical unix and Internet security
O'Reilly and Associates, 1996.

Joel Scambray, Stuart McClure, George Kurtz
Hacking Exposed, 3th Edition
McGraw-Hill, 2001

Stephen Northcutt, Donald McLachlan and Judy Novak
Network Intrusion Detection: An Analyst's Handbook, 2nd Edition
New Riders Publishing, 2000

Web sites

Cisco web site:
http://www.cisco.com

Cisco 3600 series multiservice platforms:
http://www.cisco.com/en/US/products/hw/routers/ps274/index.html

Cisco IOS Software:
http://www.cisco.com/en/US/products/sw/iosswrel/index.html

Cisco PIX 500 Series Firewalls
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/index.html

Microsoft web site:
http://www.microsoft.com

Microsoft: Web and Application Services
http://www.microsoft.com/windows2000/technologies/web/default.asp

Microsoft Exchange Server:
http://www.microsoft.com/exchange/default.asp

Microsoft Internet Security & Acceleration Server
http://www.microsoft.com/isaserver/

3Com web site :
http://www.3com.com

Snort : the Open Source Network Intrusion Detection System
http://www.snort.org

Cisco IOS Software Release 12.2
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/ps4032/index.html

Cisco IOS IP Command Reference, Volume 1 of 3 : Addressing and Services, Release 12.2
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800873a2.html

Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ff9.html

Cisco Security and VPN Software :
http://www.cisco.com/en/US/products/sw/secursw/index.html
Cisco PIX Firewall and VPN Configuration Guide Version 6.2
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a00800eb49b.html

Configuring VPN Client Remote Access: Cisco Secure VPN Client Version 1.1
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb72d.html#xtocid20

SANS/FBI: The Twenty Most Critical Internet Security Vulnerabilities
http://www.sans.org/top20/

nmap
http://www.insecure.org/nmap

nmap documentation
http://www.insecure.org/nmap/nmap_documentation.html

Nautilus netranger
http://www.nautidigital.com

Nessus
http://www.nessus.org

Keifling S., GCFW Practical Assignment
http://www.giac.org/pratical/Steve_Keifling_GCFW.doc

CERT Coordination Center web site
http://www.cert.org

SANS Institute security digests
http://www.sans.org/newlook/digests/

SecurityFocus web site
http://www.securityfocus.com

Common Vulnerabilities and Exposures web site
http://cve.mitre.org

Cisco Field Notice: PIX 515 and 506 Hang
http://www.cisco.com/warp/public/770/fn15490.shtml

Tribe Flood Network 2000 (TFN2K)
http://packetstormsecurity.org

Strategies to Protect Against Distributed Denial of Service (DdoS) Attacks
http://www.cisco.com/warp/public/707/newsflash.html

Infosyssec: Denial of service Attack – DDOS, SMURF, FRAGGLE, TRINOO
http://www.infosyssec.com/infosyssec/secdos1.htm

SANS Institute: Help Defeat Denial of service Attack: Step-by-Step
http://www.sans.org/dosstep/index.htm

CERT/CC Vulnerability note VU#944335
http://www.kb.cert.org/vuls/id/944335