Global Information Assurance Certification Paper

SANS GIAC

Firewall, Perimeter Protection, and VPNs

GCFW Practical Assignment
Version 1.5
For SANS Darling Harbour Conference in Sydney

Submitted by:
Marek Krawus,
April 2001,

In partial fulfilment of the GCFW certification requirements.

TABLE OF CONTENTS

Objectives

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams wit h explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- *Customers (the companies that purchase bulk online fortunes);*
- *Suppliers (the authors of fortune cookie sayi ngs that connect to supply fortunes);*
- *Partners (the international partners that translate and resell fortunes).*

Architecture Overview

GIAC Enterprises has been enjoying steady grow for some time now. The fortune cookie sayings bussines is on the rise, in line with growing numbers of customers, suppliers and business partners. The company has successfully completed the merge with its former competitor. For GIAC Enterprises, the Internet becomes a vital means of doing business with it partners. This emphasises the need to open external access to the company network for a several group of external users, each of them with different access requirements. The business needs however must not compromise or weaken the network security requirements. Data and services accessibility by users, both external and internal, has to be matched by adequate network resistance to intrusion.

The proposed architecture follows well -known principles of security [Zwicky 00] - namely a choke point, defence in depth, and diversity of defence. The choke point is represented by the combination of the border router and the f irewall #1. Any traffic, both inbound and outbound must traverse these security components. The approach is that the more sensitive data the more layers of protection constitutes the defence in depth principle. The network design satisfies the requirement that traffic between any two security zones must pass through at least one firewall. Using firewall technology from different vendors facilitates the diversity of defence concept. The mix of hardware types, operating systems, and firewall software has bee n chosen to make the differences as wide as practical.

Network Segmentation

GIAC Enterprises network is divided into five distinctive security domains, as it is illustrated on Fig. 1. The segmentation reflects security requirements imposed by corporate se curity policy.

The **screened subnet** is the home for information and services offered by GIAC to an unauthenticated audience in a controlled way. This comprises access to the web service, name resolution, and the external mail hub. The screened subnet has a highest level of exposure to the external environment. It has a private address of 10.10.0.0/24. Firewall #1 controls access to this subnet.

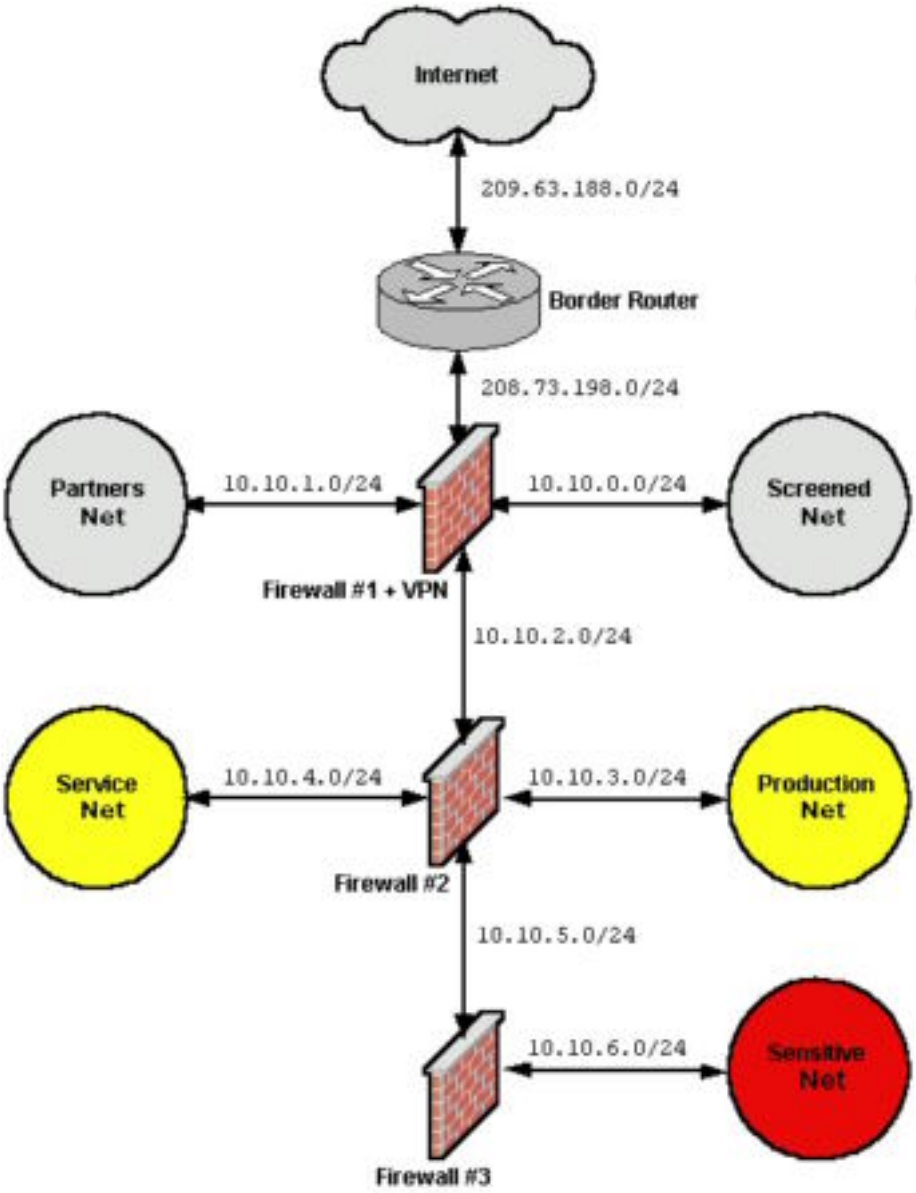

Figure 1. GIAC Enterprises basic architecture

The **partners subnet** contains servers accessible to authenticated external collaborators, such as business partners, suppliers, salesmen on the road, and also employees of the recently acquired company. This category of users connects to GIAC network by means of LAN -to-LAN VPN. In this case, the remote partner's network perimeter becomes GIAC Enterprises network perimeter. The partner's security weakness becomes GIAC Enterprises' own. As the external collaborator security policies are not to the highest standards yet, the network connections from these sources are confined to the designated partners network. This subnet address is 10.10.1.0/24. Access to it is controlled by Firewall #1.

The **service subnet** accommodates hosts providing vital services to the rest of the internal network, such as: NTP Server, Syslog Server, Internal DNS Server, Backup Server, Authentication Server. Connections from / to this subnet follow very strict rules and are based on an individual service basis. Its address is 10.10.4.0/24. Firewall #2 manages access to this subnet.

The **production subnet** comprises Customer Support, Quality Management, and Research and Development sections. Its allocated address is 10.10.3.0/24. This subnet houses, among others, the Production DB Server, File Server, Proxy Server. Traffic between the production subnet and other subnets is under Firewall #2 control.

The **sensitive subnet**, 10.10.6.0/24, contains information critical to GIAC Enterprises survival such as finance and client data and is the home for Human Resources, Finance, Marketing, Strategic Planning sections. Access to this subnet is controlled by Firewall #3.

Key Security Architecture Components

The core of the security architecture is composed of the border router and three firewalls.

A Cisco 3620 with Cisco IOS Release 12.1(5)YB2 has been chosen as the **router** facing Internet. An IP address 209.63.188.99 has been allocated to its external, serial interface while 208.73.198.1 is the IP address of the internal (ethernet) interface. While routing remains its main job, the border router contributes to the defence of the network perimeter by performing a basic filtering and protecting the next layer of defence, the outermost firewall [Brenton 01]. The security enforcing ACLs sanitize traffic traversing the router:

- Block traffic with invalid source addresses (private addressing space)
- Discard traffic with broadcast and multicast source addresses
- Deny spoofed traffic (inbound packets with internal source addresses and outbound packets with source addresses other then internal)
- Drop source routing
- Limit ICMP traffic

Firewalls create several layers of security and separate subnets with different security requirements. All firewall machines operate at the application level.

The outermost firewall (**Firewall #1**) is based on Cisco PIX 525 appliance. It has been chosen for a couple of reasons. The appliance is based on proprietary, real-time, embedded operating system. This greatly reduces the risks associated with general-purpose operating systems. The Cisco's Adaptive Security Algorithm provides stateful security for all TCP/IP session while maintaining a high throughput. Adaptive Security obeys several default rules ([CisPIXcfg 00], page 1-3):

- No packet can traverse the PIX firewall without a connection and state;
- Connections, or states from a higher security interface to a lower security interface (outbound) are allowed, except those specifically denied by access control list;
- Connections, or states form a lower security interface to a higher security interface (inbound) are denied, except those specifically allowed;
- All ICMP packets are denied unless specifically permitted;
- All attempts to circumvent the previous rules are dropped and logged.

The Adaptive Security also pays attention to the security of UDP based communication. UDP packets are handled in the manner similar to TCP, i.e. "connection" state information is created when a UDP packet is sent from the inside network. Response packets resulting from this traffic are accepted if they match the "connection" state information. This information is delated from memory after a short period of inactivity.

The PIX firewall is rich in features increasing security of internal servers, e.g. ActiveX blocking, Java filtering, DNS guard, flood defender. It comes with a VPN card and runs Cisco Secure PIX Firewall Version 5.3 software. PIX fully supports the implementation of IPsec suite of protocols (IKE, AH, ESP), which allows compatibility with broad range of VPN devices from different vendors. The firewall has four interfaces and provides NAT. The first interface is connected to the border router and has public address 208.73.198.254. The second interface (10.10.0.254) is connected to the screened network, the third (10.10.1.254) to the partners network, and the fourth interface (10.10.2.254) is facing inside network. Additionally, the firewall provides an IDS capability.

The second firewall (**Firewall #2**) is the Sun Microsystems solution. The SunScreen 3.1 firewall is installed on the Netra T1 200 server with Trusted Solaris 8 Operating Environment. The purpose of this firewall is to isolate the inner segments of the corporate network from screened and partners subnets where the controlled external connections are allowed. It creates an additional barrier for attackers, both external and internal trying get access to restricted services and hosts. The firewall has four interfaces managing traffic between outer (10.10.2.1), inner (10.10.5.254), production (10.10.3.254), and service (10.10.4.254) parts of the corporate network. No NAT is performed.

Checkpoint Firewall-1 running on an Intel-based platform and Red Hat Linux 7 composes the third firewall (**Firewall #3**). It further separates the sensitive subnet from the rest of the corporate network. Addresses of external and internal interfaces are 10.10.5.1 and 10.10.6.254 respectively. No NAT is running on this firewall.

Network Access for Business Associates

This section describes the access method allowed for each group of GIAC Enterprises business associates.

Employees accessing corporate network from the Remote Office
Due to the recent merge, these employees have created a new category of users accessing corporate network resources. They are able to access services provided on the partners subnet using LAN-to-LAN VPN created between the Remote Office perimeter firewall and Firewall #1 (Cisco PIX 525) on the GIAC Enterprises network perimeter. The access to the DB and FTP servers is based on the username/password authentication.

Customers (the companies that purchase bulk online fortunes)
This category of business associates uses the https to the Web server. The authentication is based on an assigned username/password. Upon a successful authentication customers are able to retrieve data that pertain to them. The requested data is delivered from the External DB Server located on the partners network.
(Refer to [Kossakowski 00] for an excellent paper on securing public web servers).

Suppliers (the authors of fortune cookie sayings that connect to supply fortunes)
The access method is similar to that the Remote Office employees adopt. An IPsec tunnel is established between supplier's network perimeter and Firewall #1. Then the new fortunes are uploaded to the FTP server (access to which is based on username/password authentication). Finally, the new bunch of fortune cookie sayings is moved to the production DB server to undergo Quality Assurance checking and final approval (in this case the communication is initiated from the production network).

Partners (the international partners that translate and resell fortunes)
Partners reach the GIAC Enterprises corporate network via LAN-to-LAN VPN terminated on Firewall #1. Then the External DB server located on partners network offers fine-grained access control to fortunes that pertain to each partner.

Travelling salesmen.
The Cisco Secure VPN Client, version 1.1 is installed on a salesman's laptop. This allows establishing a remote-access VPN between a laptop and the Firewall #1. Then access to the DB and FTP servers on the partner network is allowed. Authentication is based on username/password.

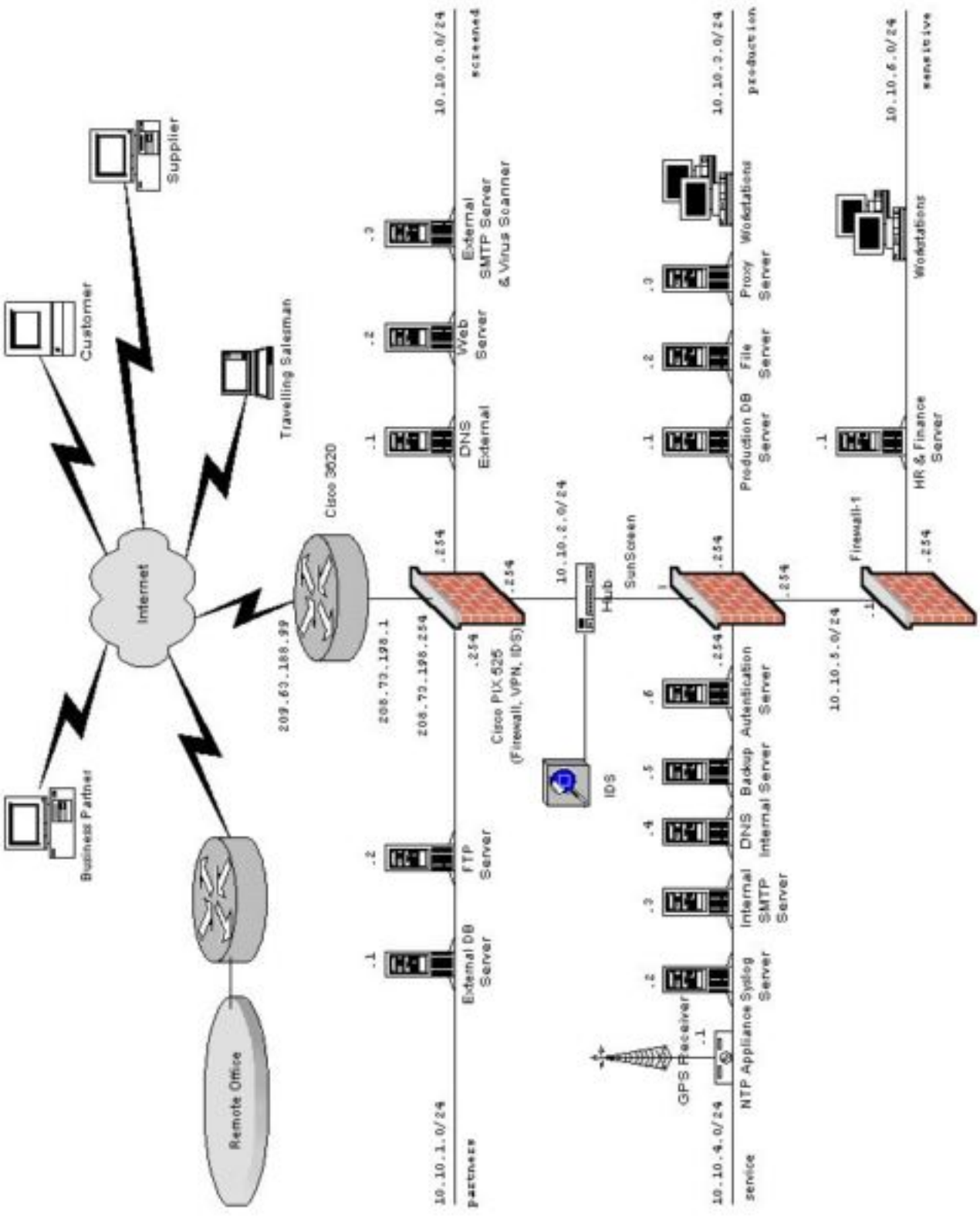

Figure 2. GIAC Enterprises network diagram

General public and prospect customers
GIAC Enterprises provides also publicly available company Web site that is accessible via http. This site contains information intended to the prospect customers. No authentication is required.

Critical Services

The following section briefly describes the architecture of critical services provided by the GIAC Enterprises corporate network (see Fig. 2). From the network security point of view it is recommended that each network service be on a dedicated, single-purpose host where possible. The detailed configuration of each server will not be provided, as this is beyond the scope of this assignment. Generally speaking, all servers must be hardened, patched, and unused services switched off. Service processes should be executed in an chrooted environment where possible.

NTP
Core network operations like file management, certificate management, and event logging depend on a reliable server synchronisation. For this purpose a dedicated TimeVault NTP Time Server equipped with GPS antenna synchronises time on the corporate network. Network Time Protocol operates on the UDP port 123.

DNS
The split DNS model is adopted. The Internal DNS server located on the service subnet resolves queries from the entire corporate network. It provides authoritative answers about internal hosts (including those on the screened and partners networks), and does all recursive DNS lookups.
The External DNS server has only publicly accessible servers listed in its zone file (External SMTP server, Web server, and itself). This server allows queries from the Internet. It does not permit recursion and allows zone transfers to the slave server provided by ISP only.

Mail and Virus Scanning
The electronic mail delivery system consists of two servers: the External SMTP Server located on the screened subnet and the Internal SMTP Server located on the service subnet. Both are Unix systems running Sendmail version 8.12.0.Beta5 with all security features enabled (e.g. preventing unauthorised relaying). The external server (TCP port 25) accepts incoming mail for valid addresses within GIAC Enterprises domain and then runs virus scanning and attachment sanitizing software (AMaViS). Signature files for virus-scanning software are updated frequently from trusted sources. The external and the internal SMTP servers exchange email using UUCP over a SSH link. The internal server always initialises the connection. Finally, mail is delivered to workstations by POP3. The POP3 communication between the internal server and workstations is encrypted by SSH tunnels.

Web
The webserver provides both an open access (via http) and account access (via SSL/https). The former type of access is intended for marketing purposes while the later one is used by customers. Each customer has unique username and password allocated to him/her. The web server provides access to relevant data for authenticated users. Data is supplied from the External DB server located on the partners subnet by means of netsql queries. The authoritative copy of the Web site content is maintained on the File Server located on the production subnet. The contents are synchronized (the authoritative copy is uploaded to the Web server) using rsync over SSH tunnel. This transfer procedure utilizing an encrypted connection is initiated from the File server.

FTP
External users (reaching the corporate network via VPN) are allowed to upload and download files based on their username/password authentication. File transfers between the FTP Server and the File Server (located on the production subnet) are performed over a secure SCP connection initiated from the production subnet.

External DB Server
The Oracle server accepts queries from the Web server and users coming over encrypted VPN connections. Data on the server is updated from the Internal DB server. Connection is always initiated from the production network. Information on the server is stored in an encrypted form.

Intrusion Detection
The intrusion detection facility consists of two independent nodes. The first node is located on Firewall #1 and utilizes the embedded PIX firewall IDS capability. The log messages are sent to the Syslog server located on the service subnet. The second node, running Snort, is located on the subnet 10.10.2.0/24 and listens to the traffic between Firewall #1 and Firewall #2. This IDS server is configured in receiving only stealth mode and stores log messages locally. In addition to the primary task of detecting signs of intrusions IDS systems help to verify the router filters and Firewall #1 security policy.

Syslog
This central log server collects syslogs from the entire corporate network: border router, firewalls, IDS, servers. No outbound connection is allowed (please see Eric Hines' paper [Hines 00] for details on on a remote log server configuration). Log messages are analysed by Swatch. Alert events are displayed on the console and trigger SMS messages.

Corporate IT Security Policy

The defence of the corporate IT infrastructure can't depend solely on the few components creating the perimeter, namely the border router and the outermost firewall. Any perimeter can be penetrated sooner or later, leaving the corporate network at the mercy of attackers. This is one of the reasons why the internal defence must be built and maintained as if the parameter did not exist. The other reasons are the internal attacks. While a strong emphasis is put on securing the corporate network resources against the external attacks, much less attention is paid to threats originating from the inside. According to Sun Microsystems [Sun 99] in 1999, 78% of the companies that took part in the *1998 CSI/FBI Computer Crime and Security Survey,* reported insider abuse. Similar data is unveiled by Blank [Blank 00]:

> *Experts say insider hacking represents about 70% of all malicious attacks and causes $1 billion in damages each year to U.S. businesses.*

The problem is of a global nature. Anne Robbins [AAP 00] from Australian Information Security Evaluation Program said there had been many recent publicised cases of hackers attacking computer systems and websites from the outside, but breached security from within seemed to be a bigger problem.

> *"Federal police and consulting agencies estimate 30 to 80 per cent of computer crime is carried out by employees in their own networks," she said. "We have spent an awful lot of time putting locks on the doors but it's the people with the keys that are causing the problems."*

This environment requires a response to corporate network security comprise issues related to host hardening, backups, physical security, access management, integrity management, auditing and logging, and personnel security. All these subjects are comprehensively covered in [Garfinkel 96] among others. Checklists for both Unix [AusCERT 95] and Windows NT [AusCERT 00] servers are good compact references pertaining to a site security policy. The CERT/CC website provides useful documents highlighting the process of securing network servers [Allen 00] and complementary to it security issues relating to day-to-day operation of servers [Kochmar 98], [Firth 97]. A security policy concerning workstation machines is provided in [Simmel 99].
The GIAC Enterprises IT Security Policy follows recommendations provided by the above-mentioned publications.

Objective

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- *Border Router*
- *Primary Firewall*
- *VPN*

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (a s appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E - Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split -horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP -based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. *The service or protocol addressed by the ACL or rule, and the r eason these services might be considered a vulnerability.*
2. *Any relevant information about the behavior of the service or protocol on the network.*
3. *The syntax of the ACL, filter, rule, etc.*
4. *A description of each of the parts of the filter.*
5. *An explanation of how to apply the filter.*
6. *If the filter is order -dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)*
7. *Explain how to test the ACL/filter/rule.*

Be certain to point out any tips, tricks, or "gotchas".

Border Router Configuration

As has been emphasized in [Brenton 01] a border router is the first layer of defe nce. It works together with an

external firewall, but these two devices play a different role in the defence of the network perimeter. As a router's primary job is to route, its ACL should not replicate an entire firewall rulebase. In contrast to a firewall, a router's default action is to pass all traffic, then deny only specific services or IPs. However, by blocking source routing, controlling ICMP traffic, blocking private addressing, and preventing spoofing, it can contribute to the perimeter defence as well as to the protection of an external firewall.
Cisco document [CisImpSec 01] provides a good overview about basic approach to the router security.
A detail, comprehensive ACL for the border router can be found in [Thomas 01] or [Keeney 98]. However, in these examples, denying traffic is the default action (the last statement in the respective access lists) for both ingress and egress filters, which makes the behaviour of the router similar to the function of a packet filtering firewall. Winters [Winter s 00] provides an excellent source of information on a router security policy. His paper thoroughly explains a rationale behind each filer rule used. The border router considered by Winters meant to play a role of a firewall. This assumption means complex filters. In our case, the router will perform only a basic, rudimentary filtering leaving the most of the job to the external firewall (Firewall #1). The configuration of the border router will then comprise the highlighted below steps.

For the purpose of this assignment the following addresses will be assumed:

Router External Interface	209.63.188.99/24
Router Internal Interface	208.73.198.1/24
Firewall External Interface	208.73.198.254/24
Screened Network	10.10.0.0/24
Firewall Screened Network Interface	10.10.0.254/24
External DNS Server	10.10.0.1/24
External WWW Server	10.10.0.2/24
External SMTP Server	10.10.0.3/24
NTP Server	10.10.4.1/24
Log Server	10.10.4.2/24

Ingress ACL on external interface

```
! Deny RFC 1918 addresses
! Class A: 10.0.0.0 -10.255.255.255
! Class B: 172.16.0.0 -172.31.255.255
! Class C: 192.168.0.0 -192.168.255.255
! They can't be coming from outside of corporate network in good
! faith. It usually indicates some malicious behaviour, including
! denial of  service.
!
!
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
!
! Deny the loop-back address 127.0.0.1 for the reasons as above.
!
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
!
! Deny packets with multicast and broadcast addresses
! Class D: 224.0.0.0 -239.255.255.255
! Class E: 240.0.0.0 -255.255.255.255
!
access-list 100 deny ip 224.0.0.0 31.255.255.255 any log
access-list 100 deny ip 255.0.0.0 0.255.255.255 any log
!
! Deny packets without ip addreses. They are usually purposely crafted.
!
access-list 100 deny ip host 0.0.0.0 any log
!
! Deny incoming packets claiming that they have our internal
```

```
! source addresses. This is a cl assical spoofing attempt.
!
access-list 100 deny ip 208.73.198.0 0.0.0.255 any log
!
! Permit otherwise
!
access-list 100 permit ip any any
!
! End of access-list 100
```

In global configuration mode, apply the following commands to the external interface:

```
interface Serial0/0

! Assign address to the interface
!
ip address 209.63.188.99 255.255.255.0
!
! Don't propagate smurf attacks.
!
no ip directed-broadcast
!
! Don't send unreachables. It is a well -known method to map out
! our network.
!
no ip unreacha bles
!
! Disable ntp. It is not secure to allow ntp traffic coming from the
! Internet to synchronize time on the corporate network. (at least
! coming from not authenticated and trusted servers). Time
! manipulation can help to break other protocols. F  or this reason
! we use internal NTP server.
!
ntp disable
!
! Apply the access list 100 to traffic going into the interface
! (from the Internet towards the corporate network)
!
ip access-group 100 in
```

Egress ACL on internal interface

```
! Allow packets  with source addresses belong to
! our internal network.
!
access-list 101 permit ip 208.73.198.0 0.0.0.255 any
!
! Deny any other outbound traffic. Packet with source
! address other then the internal network could indicate
! two serious problems: leaked  Network Address Translation,
! or purposely crafted packet originated from an internal,
! compromised host. Log and analyze.
!
access-list 101 deny ip any any log
!
! End of access-list 101
!
```

From global configuration mode:

```
interface FastEthernet0/0
!
! Assign address to the internal interface
ip address 208.73.198.1 255.255.255.0
!
! Apply the access list 101 to traffic going into the interface
! (from the corporate network towards the Internet)
!
ip access-group 101 in
```

Router hardening

```
! Force password encryption, so it would never be displayed,
! or printed out in clear -text.
!
service password-encryption
!
! Use an improved encryption algorithm to protect a password.
!
enable secret <PASSWORD>
!
! Disable minor TCP services such as echo, chargen,   discard
! and daytime. These services have no legitimate reasons to traverse
! the border router.
!
no service tcp-small-servers
!
! Disable minor UDP services such as echo, chargen, and discard.
! These services have no legitimate reasons to traverse t  he border
! router.
!
no service udp-small-servers
!
! Disable IP source routing. This does not allow source  -routed packets
! to pass through the router thus reducing a chance of spoofing.
! Source-routing allows a packet to force router to craft a path   back
! to the point of origin of this packet. This could allow a hacker to
! guide return traffic wherever he wish.
!
no ip source-route
!
! Disable the Finger protocol. The Finger can provide a potential
! hacker with a list of the users currently using   the router.
! The information displayed includes the processes running on the
! system, the line number, connection name, idle time, and terminal
! location.
!
no service finger
!
! Disable the BOOTP service.
!
no ip bootp server
!
! Don't allow the rout er to be configured from the browser interface.
!
no ip http server
```

```
!
!  SNMP is a big security concern (see i.e. [Winters 00]).
!
no snmp
!
! Disable the propagation of On -Demand Routing (ODR) stub routing
! information via Cisco Discovery Protocol (CDP ). Anyone with a CDP
! capable device can collect data from our router.
!
no cdp run
!
! Use a local NTP server on internal network. The NTP server real IP
! address of 10.10.4.1 is translated to 208.73.198.6 by Firewall #1.
!
ntp source ethernet0/0
ntp update-calendar
ntp server 208.73.198.6
!
! Add warning banner. It helps to prosecute hackers.
!
banner motd ^C
Unauthorized access is prohibited.

^C
```

Disable remote access to the router

Access to the router is permitted from the console only. Log any a ttempt to access telnet on the router.

```
!
! Access list to log any attempt to telnet the router.
!
access-list 1 deny any any log
```

Apply the above list to the telnet vtys.

```
line vty 0 4
      access-class 1 in
```

Enable logging

The following commands turn on the syslog logging on the router and send the log messages to the internal log server (the syslog server real IP address of 10.10.4.2 is translated to 208.73.198.5 by Firewall #1). Logging to the console is disabled. Log messages appear on the console make d ifficult to edit and enter commands. It is important since the access to the router is permitted from the console only.

```
no logging console
logging 208.73.198.5
logging on
```

Enable the timestamps for logging. By default timestamps are off. It will help t racing syslog messages.

```
Service timestamps log datetime msec localtime
```

External Firewall Configuration

The Firewall #1 is the next line of the defence. It does the most of filtering. For the incoming traffic, it allows services from very specific hosts and ports. It also permits selected services to be reached on Internet from

specific internal hosts. However, the firewall imposes the lockdown rule, which means that the final rule on any rulebase drops all packets.
For the detail information on the PIX firewall configuration please see [CisPIXcfg 00]. The Cisco web site also provides a number of real-life examples on PIX firewall based perimeter defence solutions together with appropriate firewall's commands (rulebases) [CisPIXTips 01].

Each firewall's interface is named and its security level assigned with the *nameif* command. The inside interface has always the highest security level at 100 and the outside has always 0. The perimeter interfaces can have a unique number between 1 and 99. It is possible, however, to completely isolate two perimeter interfaces from each other by assigning the same security level to them. The *ip address* command specifies an IP address for the given interface. The *route* statement provides the address of the default (border) router.
The PIX firewall provides several commands to facilitate communication between interfaces. The *nat* command lets users on a higher security level interface start connections to a host on any lower security interface. The *global* command defines a pool of global addresses to be used on a lower security level interface in order to provide an IP address for each outbound connection. The *outbound* command creates filters for outgoing packets from the PIX firewall. It requires use of the *apply* command to activate filters.
The communication in the opposite direction (from lower to higher security level interface) is enabled by *static* and *conduit* commands. The *static* command maps an inside host to a global address for access by outside user. The *conduit* command identifies what services can be accessed from a global address. The PIX firewall processes the *conduit* command statements in the order they are entered into configuration.
An alternative way of creating an access list is provided by *access-list* command. Then the *access-group* command binds a created access list to an interface. The access list is applied to traffic inbound to an interface. The use of *access-group* command overrides the *conduit* or *outbound* command statements for the specified interface.

Initial firewall configuration

Change the command line prompt.
```
hostname giacfirewall
```

Assign security levels to interfaces.
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 screened security40
nameif ethernet3 partners security60
```

Identify speed, duplex mode, and MTU for each interface.
```
interface ethernet0 100basetx
interface ethernet1 100basetx
interface ethernet2 100basetx
interface ethernet3 100basetx
mtu outside 1500
mtu inside 1500
mtu screened 1500
mtu partners 1500
```

Assign addresses to interfaces.
```
ip address outside 208.73.198.254 255.255.255.0
ip address inside 10.10.2.254 255.255.255.0
ip address screened 10.10.0.254 255.255.255.0
ip address partners 10.10.1.254 255.255.255.0
```

Enable Adaptive Security Algorithm for selected application protocols.
```
fixup protocol ftp strict 21
fixup protocol http 80
fixup protocol https 443
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

Disable failover feature

```
no failover
```

Enable Flood Defender

```
floodguard enable
```

Disable RIP (Routing Information Protocol) which is enabled by default. Some security concerns are always linked with dynamic routing. The default, static route is used.

```
no rip inside passive
no rip inside default
no rip outside passive
no rip outside default
no rip screened passive
no rip screened default
no rip partners passive
no rip screened default
```

Set the outside default route to the border router

```
route outside 0.0.0.0 0.0.0.0.0 208.73.198.1 1
```

Associate real (internal) IP addresses of some servers with their names. It makes the configuration file easier to read .

```
name extdns 10.10.0.1
name webserver 10.10.0.2
name extsmpt 10.10.0.3
name ftpserver 10.10.1.2
name extdbserv 10.10.1.1
name logserver 10.10.4.2
name ntpserver 10.10.4.1
name intdns 10.10.0.4
```

The IP address of security administrator workstation.

```
Name secadm 10.10.4.7
```

The IP address of GIAC's DNS slave server maintained by the ISP.

```
name ispdns 209.63.188.10
```

Enable logging to the internal syslog server. Use level 5 (notifications) and facility20 (LOCAL4). Facility 20 is a default. Set time stamps. Do not degrade PIX firewall performance – dump only level 2 (critical) messages on the console.

```
logging on
logging timestamps
logging console critical
logging trap notifications
logging host inside l ogserver
```

Allow remote console access via SSH from a security administrator's workstation.

```
ssh secadm 255.255.255.255 inside
```

Rules of access from a higher security level interfaces to a lower security level interfaces.

Network address translation (NAT) is performed for packets leaving the outside interface. The fine -grained access from the internal subnets (production, service and sensitive) to the Internet as well as from the inside interface to the partners and screened subnets is controlled by Firewal l #2 and Firewall #3.

Allow internal users to initiate connections to lower security interfaces, namely outside, screened and partners. In order to facilitate this policy the nat command is used.

```
nat (inside) 1 0 0
```

Allow servers on screened subnet start connections to the Internet.

```
nat (screened) 1 0 0
```

Give access to the partners interface for users on the inside interface. This global command statement lets selected inside users (as configured on Firewall #2) access the External DB server and the FTP server.

```
global (partners) 1 10.10.1.50 -10.10.1.199 netmask 255.255.255.0
```

Give access to the screened interface for users on the inside interface. This global command statement lets selected inside users (as configured on Firewall #2) access to the WebServer, External DNS server, and the External SMTP server.

```
global (screened) 1 10.10.0.50 -10.10.0.199 netmask 255.255.255.0
```

Specify a pool of addresses on the outside interface to which the hosts defined in the above NAT statements will be translated.

```
global (outside) 1 208.73.198.20 -208.73.198.253 netmask 255.255.255.0
```

Rules of access from a lower security level interfaces to a higher security level interfaces.

Allow any untrusted host on the Internet to connect to selected servers on the screened network. Firstly, the static command is used to create an one-to-one permanent mapping. Then, the conduit command defines allowed connections, based on both port and protocol.

```
static (screened,outside) 208.73.198.2 extdns netmask 255.255.255.255
static (screened,outside) 208.73.198.3 webserver netmask 255.255.255.255
static (screened,outside) 208.73.198.4 extsmtp netmask 255.255.255.255
```

Define, using the conduit command, which hosts can connect on which ports to the external DNS server, WEB server, and the external Mail server.

```
!--- allow zone transfer between external DNS and the slave server
conduit permit tcp host 208.73.198.2 eq domain ispdns
!— allow DNS queries from Internet
conduit permit udp host 208.73.198.2 eq domain any
!— allow access to the Web server for both http and https
conduit permit tcp host 208.73.198.3 eq www any
conduit permit tcp host 208.73.198.3 eq 443 any
!-- permit incoming mail connections to the external SMTP server
conduit permit tcp host 208.73.198.4 eq smtp any
```

Allow servers on screened and partners networks to access the syslog, internal DNS and NTP servers on the internal interface

```
static (inside,screened) 10.10.0.10 logserver netmask 255.255.255.255
static (inside,screened) 10.10.0.20 intdns netmask 255.255.255.255
static (inside,screened) 10.10.0.30 ntpserver mask 255.255.255.255
static (inside,partners) 10.10.1.10 logserver netmask 255.255.255.255
static (inside,partners) 10.10.1.20 intdns netmask 255.255.255.255
static (inside,partners) 10.10.1.30 ntpserver mask 255  .255.255.255

conduit permit udp host 10.10.0.10 eq syslog 10.10.0.0 255.255.255.0
conduit permit udp host 10.10.0.20 eq domain 10.10.0.0 255.255.255.0
conduit permit udp host 10.10.0.30 eq ntp 10.10.0.0 255.255.255.0
conduit permit udp host 10.10.1.10 eq  syslog 10.10.1.0 255.255.255.0
conduit permit udp host 10.10.1.20 eq domain 10.10.1.0 255.255.255.0
```

```
conduit permit udp host 10.10.1.30 eq ntp 10.10.1.0 255.255.255.0
```

Allow the border router to send logs to the syslog server

```
static (inside,outside) 208.73. 198.5 logserver netmask 255.255.255.255
conduit permit udp host 208.73.198.5 eq syslog 208.73.198.1
255.255.255.255
```

Permit the border router to access the NTP server

```
static (inside,outside) 208.73.198.6 ntpserver netmask 255.255.255.255
conduit permit udp  host 208.73.198.6 eq ntp 208.73.198.1 255.255.255.255
```

Permit netsql queries from the Web server on screened subnet to the External DB server on partners subnet

```
static (partners,screened) 10.10.0.40 extdbserv netmask 255.255.255.255
conduit permit udp hos t 10.10.0.40 eq netsql host 10.10.0.2
```

VPN Architecture

This section describes the configuration of LAN -to-LAN VPN for access by remote office employees, supplies and partners. In this scenario the IPSec/VPN Tunnel is created without a Certification Auth ority (CA). The Internet Key Exchange (IKE) will use the authentication method based on pre -shared keys. Pre -shared keys are hardcoded locally in the peers IPSec configuration. The pre -shared keys approach is cheaper to implement. However it does not scale well with a growing network and increasing number of IPSec peers. RSA signatures are another available solution but it requires use of a CA to facilitate authentication.

The IPSec configuration involves several steps in order recommended by Cisco ([Cis PIXIPSec 00] p. 1 -4):

1. IKE;
2. IPSec;
3. (Optional) IKE Extended Authentication – applies only for configuring user authentication for remote VPN clients;
4. (Optional) IKE Mode Configuration – applies only for configuring dynamic IP addressing for remote VPN clients.

A detailed documentation on PIX firewall VPN solutions can be found in [CisPIXIPSec 00] (available online).

The PIX firewall VPN encrypts traffic between IPSec peers. By default, all packets, including IPSec protected, that traverse the PIX firewall are subjected to blocking as specified by the inbound conduit, outbound list, or the interface access -list. Optionally, the *sysopt connection permit -ipsec* command can be configured to enable IPSec packets to bypass these ingress and egress blocking rules a nd be evaluated directly by the crypto map access list.

IPSec packets that are destined to an IPsec tunnel are selected by the crypto map access list bound to the outgoing interface. The *access-list* commands with the *permit* keyword create access list on the basis of source and destination address. The IPSec access list is created for the traffic leaving the interface (outbound direction). However, the same list is applied in the reverse direction to traffic entering the PIX firewall from the VPN tunnel, with the exception that the source and destination addresses are reversed. In this case, if an unprotected packet matches a permit entry in a particular (reversed) access list associated with an IPSec crypto map, that packet is silently dropped. This behav iour could cause problems when the *any* keyword is used in the crypto access list (assuming that *the sysopt connection permit -ipsec* command is in use). The *permit any any* statement means that all outbound traffic will be subject to protection by VPN and be sent to the peer. On other hand, at the same time a VPN expects all inbound traffic be protected. As a result, all inbound packets that lack IPSec protection will be dropped. That is why Cisco discourages the use of the *any* keyword in the crypto access lis ts

PIX firewall supports two security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides data origin authentication, connectionless integrity, protection against reply attacks, but

does not encrypt data payload. For this reason it may be used where encryption algorithms (DES, Triple DES) are not available. EPS offers payload encryption and limited traffic flow confidentiality in addition to all features provided by AH.
Security protocols, algorithms and other parameters applied for encrypting packets between IPSec peers constitute a security association. Internet Security Association and Key Management Protocol (ISAKMP) is the protocol defining a framework within which a security association is negotiated. IKE protocol automates process of this negotiation and performs it according to a combination of security parameters defined in IKE policy. These parameters comprise encryption algorithm (des or 3des), hash algorithm (sha or md5), authentication method (rsa-sig or pre-share), Diffie-Hellman group identifier (1 for 768-bit Diffie-Hellman or 2 for 1024-bit Diffie-Hellman), and security association's lifetime (number of seconds).
Multiple IKE policies can be created for an IPsec peer, each with a different combination of parameter values, and marked with a unique priority number (1 being the highest priority). If no policy is specified, the PIX firewall will use the default policy containing the default parameters of des for the encryption algorithm, sha for the hash algorithm, rsa-sig for the authentication method, 1 for the Diffie-Hellman group identifier, and 86,400 for the security association's lifetime. This default policy is always set to the lowest priority.
IKE polices must be created at each IPSec peer. IKE negotiation attempts to find a matching policy with the highest priority. Matching polices must contain all the same parameter values but the security association's lifetime.

For the purpose of this assignment the following addresses will be assumed:

Peer VPN IPSec Device in Remote Office	210.99.99.99/24
R&D Network in Remote Office	10.2.2.0/24
Peer VPN IPSec Device in Partner Office	205.20.30.40/24
Production Network in Partner Office	192.68.100.0/24
Peer VPN IPSec Device in Supplier Office	202.4.12.240/24
File server in Supplier Office	172.30.50.2

The following steps must be completed in order to establish LAN-to-LAN VPN Tunnel.

1. Configure IKE policy

Identify the policy and assign its priority:
```
isakmp policy 22
```

Specify the encryption algorithm:
```
isakmp policy 22 encryption 3des
```

Specify the hash algorithm:
```
isakmp policy 22 hash sha
```

Specify the authentication method:
```
isakmp policy 22 authentication pre-share
```

Specify the Diffie-Hellman group identifier:
```
isakmp policy 22 group 2
```

Specify the security association's lifetime:
```
isakmp policy 22 lifetime 86400
```

2. Configure IKE Pre-Shared Keys

Specify the pre-shared key. Use a unique key for each peer. The same pre-shared key must be configured at both the GIAC PIX firewall and its peer.

```
isakmp key <remoteofficekey> address 210.99.99.99
isakmp key <partnerkey> address 205.20.30.40
isakmp key <supplierkey> address 202.4.12.240
```

3. Configure IPSec crypto access -list

Create an access list to protect traffic from/to External DB Server (10.10.1.1) to/from R&D network in Remote Office (10.2.2.0/24):

```
access-list 110 permit ip host 10.10.1.1 10.2.2.0 255.255.255.0
```

Create an access list to protect traffic from/to FTP Server(10.10.1.2) to/from file R&D network in Remote Office(10.2.2.0/24):

```
access-list 110 permit ip host 10.10.1.2 10.2.2.0 255.255.255.0
```

Create an access list to protect traffic from/to External DB Server (10.10.1.1) to/from Production Network in Partner Office (192.68.100.0/24):

```
access-list 120 permit ip host 10.1 0.1.1 192.68.100.0 255.255.255.0
```

Create an access list to protect traffic from/to FTP Server (10.10.1.2) to/from file server in Suplier Office:

```
access-list 130 permit ip host 10.10.1.2 host 172.30.50.2
```

4. Configure transform set

Create a transform set to define how the traffic will be protected:

```
crypto ipsec transform -set giacset1 esp-des esp-md5-hmac
crypto ipsec transform -set giacset2 ah-sha-hmac esp-des esp-sha-hmac
```

5. Configure IPSec map

Create a crypto map entry for Remote Office with the se quence number of 10. The lower the sequence number the higher the priority:

```
crypto map remoteffice 10 ipsec -isakmp
```

Assign an access list to a crypto map entry:

```
crypto map remoteffice 10 match address 110
```

Specify the remote IPSec peer (VPN appliance in t he Remote Office):

```
crypto map remoteffice 10 set peer 210.99.99.99
```

Associate a crypto map entry with allowed transform sets:

```
crypto map remoteoffice 10 set transform -set giacset1
```

Apply a crypto map set to the outside interface:

```
crypto map remoteoffice in terface outside
```

Create a crypto map entry for Partner

```
crypto map partner 20 ipsec -isakmp
crypto map partner 20 match address 120
crypto map partner 20 set peer 205.20.30.40
crypto map partner 20 set transform -set giacset1 giacset2
crypto map partner inte rface outside
```

Create a crypto map entry for Supplier

```
crypto map supplier 30 ipsec -isakmp
crypto map supplier 30 match address 120
crypto map supplier 30 set peer 202.4.12.240
crypto map supplier 30 set transform -set giacset1 giacset2
crypto map supplier  interface outside
```

6. Enable IPSec traffic to be implicitly trusted .

Enable packets that have been processed by IPSec to bypass the conduit, outbound list, and interface access -list checks . By default, all packets, including IPSec protected, that travers e the PIX firewall are subjected to blocking as specified by inbound conduit, outbound list, or interface access -list.

```
sysopt connection permit -ipsec
```

Objectives

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. *Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.*
2. *Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.*
3. *Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.*

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

Planing the Assessment

The Primary Firewall is the most important element of GIAC Enterprises network and is critical to company's business activities. Any interruption to network services could result in financial loses and damages to company image. This is a significant restraint we must take into consideration during the planning phase of the assessment. A conventional security evaluation may be able to determine whether the firewall is configured properly and IDS detects scanning and spoofing attacks properly. But it does not answer the question whether the firewall will actually resist and survive Denial of Services (DoS) attack. Only a simulated attack can answer this question. Can we go that far with our assessment?

The assessment will consists of three phases:

1. information gathering and non impact checking;
2. penetration testing which would have a potential impact on network performance or could perhaps bring the network down, firewall configuration tune up.
3. final checking of the firewall configuration.

Phases one and three will be performed during normal business hours. As phase two could result in a network outage, the time of the testing must be synchronized with the period when network services are least utilized. Mid-weekend, in particular very early Sunday morning seems to be a preferable time. All business partners, vendors, and suppliers must be notified in advance about the timing and possible disruption of the network services and VPN access.
I would recommend not mentioning a firewall penetration test in information for the business associates. Rather scheduled system maintenance should be given as a reason behind the service disruption.

The estimated cost of the assessment includes only a security auditor fee. All software tools used in the test are freely available. I estimate t he amount of time to implement the assessment would be: 2 days for phase one, one day for phase two and one day for phase three. The hourly rate will be $150, which yields $4800 as a total cost of the assessment.
Before entering the implementation phase of the assessment we must obtain an official approval signed by Senior Management to conduct the audit. This document must specify persons and resources to be engaged in the audit, its scope and time, and must acknowledge a potential risk of interruption to network services.

Implementing the Assessment

Phase one is perform during standard business hours. We execute the following:

- check the physical security of the firewall, its location, physical access to the firewall and its console, connection to UPS;
- identify who is responsible (have passwords) for the firewall maintenance;
- collect and review all relevant documentation such as Security Policy, firewall configuration and maintenance procedures, change control procedures, firewall logbook, network diagrams , password policy;
- verify and assess administrative connectivity to the firewall from the internal network;
- identify the operating system level and patch level;
- check for latest security advisory pertaining to the firewall software version on a manufacture r's Web site, review the latest security flaws in this software posted on SecurityFocus, SANS, CERT Web sites, scan archives of relevant mailing lists and discussion groups;
- review syslog records originating from the firewall and IDS in order to determinat e a standard traffic pattern and determinate possible irregularities;
- use ***show*** commands to review firewall's configuration;
- compare the current firewall's configuration against mentioned above local security policy and vendor recommended patches and adviso ries, record differences;
- review syslog records originated from the firewall and IDS in order to determinate a standard traffic pattern and determinate possible irregularities;
- prepare a workstation, connect it outside GIAC Enterprises perimeter, install n map, nemesis, and teardrop tools on this workstation;
- install nmap on an internal workstation.

Phase two of the assessment starts at 3 am Sunday morning and the following steps are performed:

- use nmap tool to discover open ports on any firewall interface .;
- compare the list of open ports with those intended to be open according to the security policy.

The tool we use for scanning is nmap version 2.53. This free utility delivers a very comprehensive list of scanning methods. The most common options are:

```
nmap V. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all -around TCP scan)
* -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 r emote 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.micros oft.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/-oM <logfile> Output  normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '  -' for stdin
* -S <your_IP>/ -e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88 -90.*.*'
```

We use nmap to map the entire port range for TCP and UDP on internal interface:

```
nmap -sT -p1- -P0 10.10.2.254

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )

Interesting por ts on (10.10.2.254 ):

(The 65533 ports scanned but not shown below are in state: closed)

Port       State       Service

22/tcp    open         ssh

Nmap run completed  -- 1 IP address (1 host up) scanned in 397 seconds



nmap -sU -p1- -P0 10.10.2.254

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )

Interesting ports on (10.10.2.254):

(The 65534 ports scanned but not shown below are in state: closed)

Port       State       Service

123/udp    open        ntp

Nmap run completed  -- 1 IP address (1 host up) scanned in 344 seconds
```

There should be only one TCP port open: 22/tcp – ssh access for administrative purposes, and one UDP port open: 123/udp – ntp allowing time synchronisation with the internal ntp s erver.
Similar scans against other three interfaces performed from appropriate networks should show all ports closed.

```
nmap -sT -p1- -P0 10.10.0.254

nmap -sU -p1- -P0 10.10.0.254

nmap -sT -p1- -P0 10.10.1.254

nmap -sU -p1- -P0 10.10.1.254
```

```
nmap -sT -p1- -P0 208.73.198.254

nmap -sU -p1- -P0 208.73.198.254
```

In the next step we will run the scan against servers available from the Internet. From the outside run:

```
nmap -sT -p1- -P0 208.73.198.x

nmap -sU -p1- -P0 208.73.198.x
```

where x = 2 for External DNS server, x = 3 for Web server, x = 4 for External DNS server, x = 5 for Syslog server. All ports but providing appropriate services documented in the security policy (which in turn is implemented by the firewall rulebase) should be filtered. Again, the IDS logs should show the scanning warnings.
If we have enough time, and sufficient disk space on the Syslog server, we can try to run similar scan against the whole range of allocated addresses 208.73.198.0/24

```
nmap -sU -p1- -P0 208.73.198.0/24
```

in order to fully test the firewall rule base concerning the external interface.

Finally, we can test the firewall resistance against a simulated SYN-flooding and IP fragment style attacks. A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a web site, or accessing external e-mail sever. In order to perform a SYN-flooding simulation, the *nemesis-tcp* tool is employed is described in [Smith 01]. One can use *nemesis* to generate finely crafted packets by specifying parameters at the link, network and transport layers of the TCP/IP protocol suite.
Another form of assault is IP fragment style attack. Discussed in [RFC 1858], it exploits vulnerabilities in the packet reassembly code of specific IP stack implementations regarding tiny fragments or overlapping fragments. A teardrop tool can be used in order to perform an attack simulation.

In the final third phase the following steps can be performed:

- apply vendor recommended patches (if any);
- correct discrepancies between the current security policy and the firewall configuration (if any).

Perimeter Analysis

The perimeter security can be improved in several ways.

The border router can be configured as a first line of defence against TCP SYN-flooding and protect the firewall (which is also a VPN security gateway and a IDS) against this type of DoS attacks. The IOS TCP *intercept* feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. The TCP intercept can operate in either active intercept mode or passive watch mode. The default is intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt. If the number of incomplete connections exceeds a given threshold, TCP intercept switches into aggressive mode. In this mode, the software actively intercepts each incoming connection request (SYN) and responds on behalf of the server with a SYN-ACK, then waits for an ACK from the client. When that ACK is received, the original SYN is sent to the server and the software performs a three-way handshake with the server. When this is complete, the two half-connections are joined.

The following commands tune up TCP intercept parameters and enable the IOS to intercept packets:

```
! By default, the router still manages a connection for 24 hours
! after no activity. Allow 60 seconds only for inactive connectio  ns.
!
ip tcp intercept connection -timeout 60
!
! Keep half-open sockets for 10 seconds only. By default, the
! software waits for 30 seconds for a watched connection to reach
! established state before sending a Reset to the server.
!
ip tcp intercept wa tch-timeout 10
!
! Set the threshold for stopping aggressive mode. Allow 600
! connection requests per minute (default 900).
!
ip tcp intercept one -minute low 600
!
! Sets the threshold for triggering aggressive mode (above 900
! connection requests per  minute). Default value is 1100.
!
ip tcp intercept one -minute high 900
!
! Finally, define extended IP access list (190 in our case), causing
! the software to intercept all TCP packets traversing the router
!
access-list 190 permit tcp any any

ip tcp intercept list 190
```

The behaviour of the IOS' TCP intercept feature under the simulated attack can be monitored with the following commands:

```
! Display incomplete connections and established connections.
show tcp intercept connections
! Display TCP intercept  statistics.
show tcp intercept statistics
```

The IP Frag Guard feature can be used to protect a PIX firewall against an IP fragment style attack. This feature is disabled by default. It operates on all interfaces in the PIX firewall and cannot be selecti vely enabled or disabled by interface. The IP Frag Guard is enabled by a command:

```
sysopt security fragguard
```

A teardrop-specific syslog messages notifying of any fragment overlapping and small fragment offset anomalies should be logged during the simulate d IP fragment style attack.

Other suggested improvements are related to the network architecture. As Web servers are always among the most favourite hacking targets I would suggest implementing a WWW reverse proxy server. In this case, there will be no di rect unauthenticated traffic to the Web server. Furthermore, I would split the secure (https) and general access (http) Web servers and house them on separate hosts.
Figure 3 illustrates suggested amendments to the network architecture.

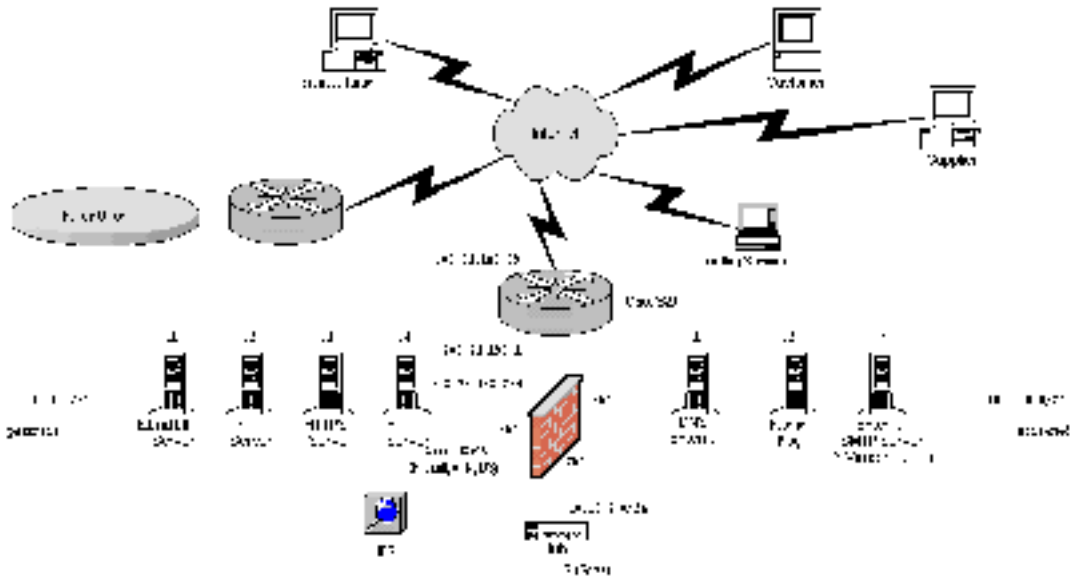

Figure 3. Improvements to network architecture

Objectives

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. *An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.*
2. *A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.*
3. *An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.*

***Note:** this is the second time this assignment has been used. The first time, a number of students came up with magical "hand-waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.*

For the purpose of this assignment I have chosen the network designed by Dominique Galland (Fig. 4). The practical is available at: http://www.sans.org/y2k/practical/Dominique_Galland_GCFW.zip

Attack Against the Firewall

This practical specifies no details regarding the brand and version of each perimeter defence component. The only information unveiled is the name of the firewall software used to create the external firewall, namely CheckPoint Firewall-1. No version is specified, neither an operating system the firewall is installed on. I assume the Firewall-1 version used is 4.0 or 4.1. These last two versions of the Firewall-1 are known for vulnerabilities. One of them is *Check Point Firewall-1 Fragmented Packets DoS Vulnerability* (bugtraq id 1312: http://www.securityfocus.com/bid/1312). Lance Spitzner comprehensively explains this flaw in his paper *"FW-1 IP Fragmentation Vulnerability"* available at http://www.rootshell.com/archive-j457nxiqi3gq59dv/200006/fw1ipfrag.txt.html. By sending illegally fragmented packets directly to or routed through Check Point Firewall-1, it is possible to force the firewall to use 100% of available processor time logging these packets. As result the firewall system locks up and even may also crash, depending on OS type. The Firewall-1 rulebase cannot prevent this attack and it is not logged in the firewall logs. The jolt2 tool (http://www.securityfocus.org/data/vulnerabilities/exploits/jolt2.c) can be used to facilitate the attack. Both Check Point Software Firewall-1 4.1 prior SP2 and Check Point Software Firewall-1 4.0 prior SP6 are vulnerable.

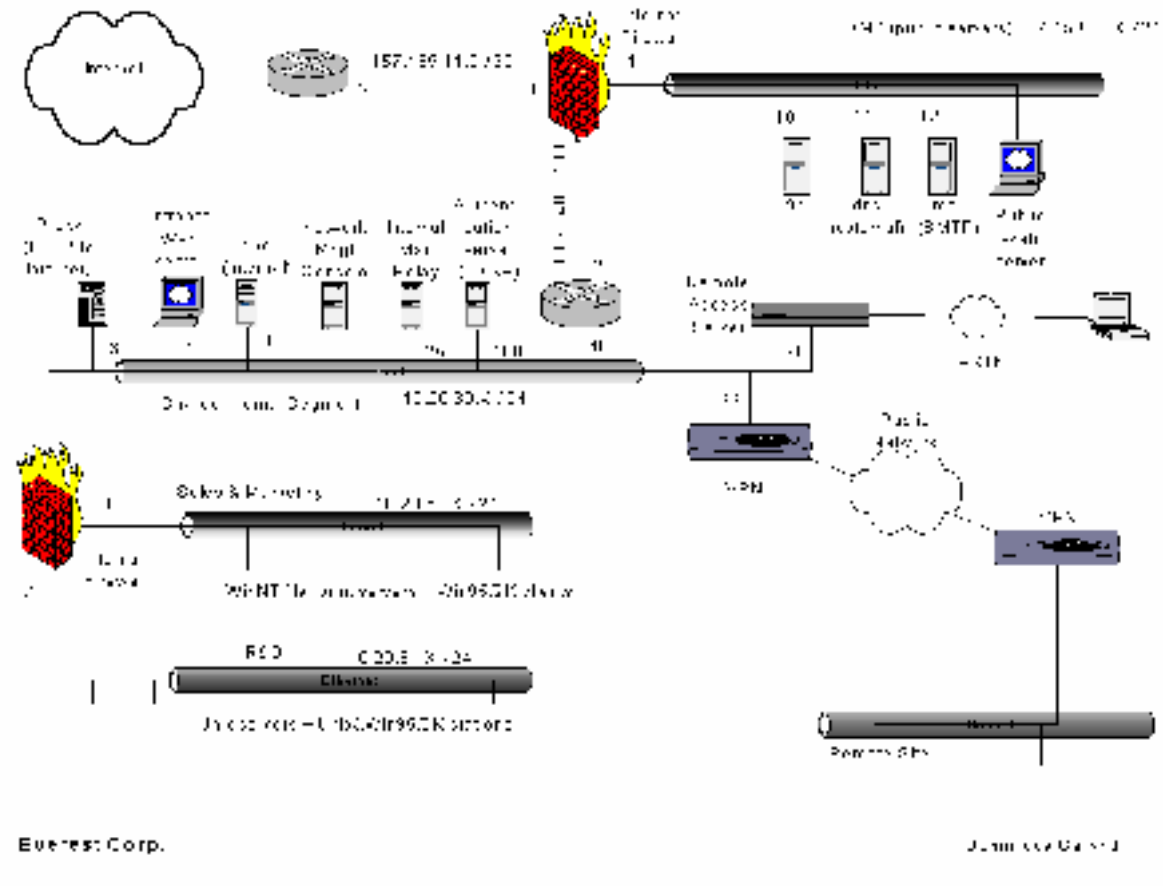

Figure4. Design under fire

Disabling Firewall-1 kernel logging is a short-term solution to the problem. In this way some CPU cycles will be saved. However, this action stops logging any fire wall kernel events. In order to disable the console logging type the following command at the FireWall -1module:

```
fw clt debug -buf
```

The long term solution comprises all the following:

- install the latest patches for the operating system. Most operating s ystem have recently released patches that help protect against fragment attacks;
- install CheckPoint latest Service Pack for Firewall -1;
- run an IDS service (e.g. Snort). The network architecture under review has no any IDS module installed;
- block the IP fra g attacks at the border router.

Denial of Service Attack

Joel Scambray et al. [Scambray 01] provides the good overview of DDoS attacks. The tool chosen to facilitate the DDoS assault is TFN2K. This new generation DDoS tool is more sophisticated then its predecessors. Its set of feature is designed to make detection difficult and includes [Barlow 00]:

- randomised communication from the master to the agent via TCP, UDP, or ICMP;
- completely silent daemon on clients – all control communication is unidirectional;
- encrypted traffic from master to agents;
- decoy packets sent to random IP numbers.

Target may be attacked with a TCP/SYN, UDP, ICMP/PING, or Broadcast PING (Smurf) packet flood. Clients may also be instructed to randomly alternate between all four styles of attack.

The countermeasures against the TFN2K attacks are twofold. On one hand we must prevent our systems from being used as agents (zombies), on other hand we need to protect out systems from DDoS attacks. In this assignment we focus on the latter part of the defence only. In the network under review, measures to block spoofed addresses on the border router and block all ICMP traffic on the firewall are taken. However there is no explicit statement that a countermeasure against a TCP SYN flood has been applied on the router or on the firewall. If the border router is a Cisco then the tcp intercept facility should be enabled (for details please see: Assignment 3 in this paper). As far as the firewall is concerned, the Firewall-1 has SYNDefender Gateway serving the same purpose. SYNDefender Gateway tracks the handshaking process between a client and a server and resets connection attempts if there is no ACK from the client within a certain period of time.
The recommended settings for SYNDefender would be:

- Timeout: 10 seconds
- Maximum sessions: 5000
- Display warning messages: YES (enabled).

Compromising an Internal System

There are four public servers shown on the DMZ. Yet again, no information regarding software used to facilitate these servers has been supplied. Research regarding vulnerabilities in most popular FTP (wu-ftpd), DNS (bind), mail (Sendmail), and Web server (Apache) software yields dozens of exploits to be used in order to perform attacks on these servers. The following web sites:

http://www.securityfocus.org
http://www.hideaway.net
http://securiteam.com
http://rootshell.com/beta/exploits.html

are among the most popular for this kind of information.
Lets look at some recent vulnerabilities pertaining to the above-mentioned software which are exploitable by a remote user:

Apache

- 2001-03-13: Apache Artificially Long Slash Path Directory Listing Vulnerability

  This vulnerability makes it possible for a malicious remote user to launch an information gathering attack, which could potentially result in compromise of the system. This vulnerability affects all releases of Apache previous to 1.3.19

- 2000-12-06: Apache Web Server with PHP 3 File Disclosure Vulnerability

  By requesting a specially crafted URL by way of php, it is possible for a remote user to gain read access to a known file that resides on the target host.
  Successful exploitation of this vulnerability could lead to the disclosure of sensitive information and possibly assist in further attacks against the victim.

Bind

- 2001-01-29: ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability

  Version 8 of BIND contains a overflow that may be exploitable to remote attackers. Due to a bug that is present when handling invalid transaction signatures, it is possible to overwrite some memory locations with a known value. If the request came in via the UDP transport then the area partially overwritten is a stack frame in named. If the request came in via the TCP transport then the area practically overwritten is in the heap and overwrites malloc's internal variables. This can be exploited to execute shellcode with the privileges of named (typically root).

- 2000-11-01: Multiple Vendor BIND 8.2.2 -P5 Denial of Service Vulnerability

  A Denial of Service exists in current implementations.
  The problem occurs in the Compressed Zone Transfer (ZXFR) functionality of BIND. A default installation of BIND does not support the transfer of compressed zone files. However, daemon that allows zone transfers and recursive queries will crash if queried for a compressed zone transfer that is not in the nameserver cache. This could result in a name resolution Denial of Service for all users and systems depending upon nameservers using the affected software.

Sendmail

- 1999-12-22: Sendmail ETRN Denial of Service Vulnerability

  There is a low-bandwidth dos vulnerability in Sendmail 8.9.3. When a client connects to the sendmail smtpd and sends an ETRN command to the server, the server fork()s and sleeps for 5 seconds. If many ETRN commands are sent to a server, it is possible to exhaust system resources and cause a denial of service or even a reboot of the server.

Wu-ftpd

- 2000-06-22: Wu-Ftpd Remote Format String Stack Overwrite Vulnerability

  Washington University ftp daemon (wu-ftpd) is a very popular unix ftp server shipped with many distributions of Linux and other UNIX operating systems. Wu-ftpd is vulnerable to a very serious remote attack in the SITE EXEC implementation. Because of user input going directly into a format string for a *printf function, it is possible to overwrite important data, such as a return address, on the stack. When this is accomplished, the function can jump into shellcode pointed to by the overwritten eip and execute arbitrary commands as root. While exploited in a manner similar to a buffer overflow, it is actually an input validation problem. Anonymous ftp is exploitable making it even more serious as attacks can come anonymously from anywhere on the internet.

The Check Point Firewall-1 Fast Mode TCP Fragment Vulnerability opens another way to facilitate a remote attack against an internal host. This security flaw is documented at http://www.securityfocus.com/bid/2143.
The "Fast Mode" option may allow an attacker to bypass access control restrictions and access certain blocked services. Fast Mode is a setting that turns off analysis of packets in TCP sessions after the TCP 3-way handshake has completed for speed-critical services. In spite of the fact that a fast mode is disabled by default, it is likely enabled for such a speed-critical services as a public web server or FTP server.
Thomas Lopatic provides the full explanation of the exploit in his paper *Fastmode Vulnerability in VPN-1/FireWall-1 4.1 SP2. Advisory #3,* available on-line at: http://www.dataprotect.com/fw1.
Generally speaking, if we are able to use fast mode to get access to an allowed single TCP service (e.g. http, TCP port 80), all TCP services on the same machine become accessible. That means, for example, that a service in the DMZ opened to the Internet may give access to all services in the DMZ for the attacker from the Internet. And if an administrator has opened a service in the intranet to the DMZ (suppose the web server needs to access a DBMS), all services in the intranet may become accessible to the DMZ. Thus, an attacker might be able to work his way from the Internet through the DMZ to the intranet. Demonstration source code that exploits this vulnerability is available at: http://www.dataprotect.com/fw1/fm.c.

This issue has been completely fixed in Firewall -1 version 4.1 SP3 and version 4.0 SP8. The suggested immediate workaround is to turn off the fast mode option in the rules where it is being used.

REFERENCES

[AAP 00] AAP. *Hacking comes from the inside, computer expert warns*. John Fairfax Holdings Ltd, 15 February 2000. Available at: http://www.it.fairfax.com.au/breaking/20000215/A19865_-2000Feb15.html

[Allen 00] Allen, Julia. et al. *Securing Network Servers*. (CMU/SEI-SIM-010). Pittsburgh, Pa.: Software Engineering Ins titute, Carnegie Mellon University, 2000.
Available at: http://www.sei.cmu.edu/pub/documents/sims/pdf/sim010.pdf

[AusCERT 95] *UNIX Computer Security Checklist (Version 1.1).* Australian Computer Emergency Response Team, Brisbane. 1995. Available at: ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist

[AusCERT 00] *Windows NT Configuration Guidelines*. Australian Computer Emergency Response Team, Brisbane. 2000 . Available at:
http://www.auscert.org/Information/Auscert_info/Papers/win_configuration_guidelines.html

[Barlow 00] Barlow, Jason. Thrower, Woody. *TFN2K - An Analysis*, Axent Security Team, 10 February 2000. Available on line: http://packetstorm.securify.com/distributed/TFN2k_Analysis.htm.

[Blank 00] Blank Dennis. *When the Hacker Is on the Inside*. Business Week Online. 13 December 2000. Available at: http://www.businessweek.com:/print/bwdaily/dnflash/dec2000/nf20001213_253.htm?content

[Brenton 01] Brenton, Chris. *Advanced Perimeter Protection and Defence*. SANS Darling Harbour 2001, pp 11-58

[CisNetSec 01] *Network Security Policy: Best Practices White Paper*. Cisco Systems Inc. 2001.
Available at: http://www.cisco.com/warp/public/126/secpol.html

[CisImpSec 01] *Improving Security on Cisco Routers*. Cisco Systems Inc. 2001
Available at: http://www.cisco.com/warp/public/707/21.html

[CisIOSdoc 01] *Cisco IOS Release 12.1 Documentation*. Cisco Systems Inc. 2001
Available at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/index.htm

[CisIOScfg 01] *Cisco IOS Security Configuration Guide, Release 12.1.* Cisco Systems Inc. 2001. Available at:
http://www.cisco.com/univercd/cc/td/doc/product/softwa re/ios121/121cgcr/secur_c/index.htm

[CisPIXcfg 00] *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3.* Cisco Systems Inc. 2000
Available at: http://www.cisco.com/univercd/cc/td/doc/produ ct/iaabu/pix/pix_v53/config/index.htm

[CisPIXIPSec 00] *IPSec User Guide for the Cisco Secure PIX Firewall Version 5.3*. Cisco Systems Inc. 2000
Available at: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/ipsec/index.htm

[CisPIXTips 01] *Pix Tech Tips*. Cisco Systems Inc. 2001
Available at: http://www.cisco.com/warp/public/110/index.shtml#pix

[Firth 97] Firth, Robert, et al. *Detecting Signs of Intrusion* (CMU/SEI-SIM-001). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1997. Available at:
http://www.sei.cmu.edu/pub/documents/sims/pdf/sim001.pdf

[Fithen 99] Fithen, Wiliam. et al. *Deploying Firewalls*. (CMU/SEI-SIM-008). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1999.
Available at: http://www.sei.cmu.edu/pub/documents/sims/pdf/sim008.pdf

[Garfinkel 96] Garfinkel, Simson. Spafford, Gene. *Practical UNIX and Internet Security, Second edition.* Sebastopol: O'Re illy & Associates, Inc., 1996

[Hines 00] Hines, Eric. *Complete Reference Guide to Creating a Remote Log Server* . Aug. 14 2000. Available at: http://www.hideaway.net/Server_Security/Library/General/gentxts/secure -remotelogserver -howto.txt

[Keeney 98] Keene y Frank. *Screening Router Access List* . 30 December 1998. Available at: http://pasadena.net/cisco/secure.html

[Kochnar 98] Kochmar, John. et al. *Preparing to Detect Signs of Intrusion* (CMU/SEI-SIM-005). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1998. Available at: http://www.sei.cmu.edu/pub/documents/sims/pdf/sim005.pdf

[Kossakowski 00] Kossakowski, Klaus -Peter. Allen, Julia. *Securing Public Web Servers* . (CMU/SEI-SIM-011). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 2000. Available at: http://www.sei.cmu.edu/pub/documents/sims/pdf/sim011.pdf

[Lopatic 00] Lopatic, Thomas. McDonald, John. Song, Dug. *A Stateful Inspection of FireWall -1*. Center for Information Technology Integration University of Michigan, 2000. Available at: http://www.dataprotect.com/bh2000

[RFC 1858] Ziemba, G. Reed, D. Traina, P. *Security Considerations for IP Fragment Filtering* . Request for Comments: 1858. October 19 95. Available at: http://rfc.net/rfc1858.html

[Scambray 01] Scambray, Joel. McClure, Stuart. Kurtz, George. *Hacking Exposed: Network Security Secrets & Solutions. 2nd Edition* . Berkeley, CA, Osborne/McGraw -Hill, 2001. pp. 459 -506.

[Simmel 99] Simmel, Derek. et al. *Securing Desktop Workstations* (CMU/SEI-SIM-004). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1999. Available at: http://www.sei.cmu.edu/pub/documents/sims/pdf/sim004.pdf

[Smith 01] Smith, Nicholas. *Choking on Naptha. TCP/IP Network Denial of Service Vulnerabilities* . Available at: http://www.sans.org/y2k/practical/Nicholas_J_Smith_GCIH.html

[Sun 99] *Protecting From Within. A Look at Intranet Security Policy and Management* . Sun Microsystems, Inc, Palo Alto, Ca, 1999. Available at: http://www.sun.com/software/white -papers/wp -security -intranet/protectingfromwithin.pdf

[Thomas 00] Thomas Rob. *Secure IOS Template Version 2.2* , 19 December 2000 Available at: http://www.cymru.com/~robt/Docs/Articles/secure -ios -template -22.html

[Winters 00] Winters Scott. *Top Ten Blocking Recommendations Using Cisco ACLs. Securing the Perimeter with Cisco IOS 12 Route rs.* August 15 2000. Available at: http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm

[Zwicky 00] Zwicky, Elizabeth D. Cooper, Simon. Chapman, Brent D. *Building Internet Firewalls, Second Edition*. Sebastopol: O'Reilly & Associates, Inc., 2000. pp 59 – 72.