Firewalls, Perimeter Protection & VPNs

GIAC Certified Firewall (GCFW) Analyst Practical Assignment

Version 1.5e

Delvin Nelson

1. GIAC Enterprises – An Overview

GIAC Enterprises expects to earn $200 million in online sales of fortune cookie sayings in Year 2001. GIAC Enterprises recently completed a merger with Cookie.Com in an attempt to grab market share and gain valuable intellectual property. The merger necessitated a redesign of the security architecture for the GIAC Enterprises network. The merger prompted a renewed focus on providing remote access for customers, suppliers and partners. In order to keep up with the security architecure redesign, the existing GIAC Information Security policy was revised and is provided below.

GIAC Information Security Policy

The GIAC Information Security Policy was used to design the security architecture diagram and has been updated to accommodate external connections in section VIII.

I. Purpose of the Policy:

Electronic commerce is a highly competitive and lucrative market. GIAC Enterprises systems and intellectual property are of immense value to its' internal stakeholders, customers, suppliers, partners as well as competitors. GIAC computer systems and intellectual property must be protected from both intentional and unintentional computer fraud, misuse and abuse. Thus, an information security policy is required to address all potential forms of fraud, misuse and abuse.

II. Underlying Security Principles:

- Confidentiality - All data must be protected from unauthorized access.
- Availability – All data must be accessible.
- Integrity – All data must be unaltered and authentic.

III. Access Control:
Access to GIAC systems and information must be strictly controlled. Access control measures must be implemented and logging must be enabled on all systems.

IV. Host Security:
Security patches, hot-fixes and service packs will be installed on all Internet-connected systems and host systems as soon as possible to thwart compromise. Administrative reviews of system logs must be made regularly and often to enable swift discovery and handling of mistakes, abuse, and intrusion attempts. Each system in the De-Militarized Zones (DMZ) must be limited to have only one function. In other words, all unnecessary services must be disabled. This enables the communications to be limited to specific protocols/ports and allows the systems to be hardened more effectively.

V. Network Security:

Security will be employed in layers – also called “Defense in Depth”. Defense in Depth emphasizes multiple layers of security. Each layer must have some type of logging and alerting mechanism in order to notify security personnel of a possible compromise of any layer. The GIAC Enterprises network systems will use private IP addresses per RFC 1918 and these addresses will be translated into Internet routable addresses at the firewall. The GIAC Enterprises network will limit the information provided about systems, the network and services. Examples of this activity include registering only required DNS hosts and dropping packets rather than responding that a particular service is not provided.

VI. Physical Security:

Physical access to all systems must be commensurate with the highest level of data residing on that system. For example, laptops storing sensitive data must be locked when not in use. All servers must be kept in locked areas.

VII. Risk Management

It is often impossible to provide total security for all situations. Risk management requires a careful evaluation of security requirements. Risks to information resources must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected. An example of risk management activities is the requirement to review new vulnerability announcements on a daily basis.

VIII. External Access Requirements - NEW

GIAC Enterprises must provide access for several customers, suppliers and partners.

- Customers - Customers are required to connect via web browsers utilizing Secure Socket Layer (SSL) with the strongest key encryption allowed by US export control laws. Special customers may also be provided the RaptorMobile VPN client.

- Suppliers - Suppliers are required to connect to the GIAC Main firewall using the RaptorMobile VPN client. The RaptorMobile client establishes an IPSec encrypted session to allow the suppliers to share data with GIAC Enterprises.

- Partners – Partners are also required to connect to the GIAC Main firewall utilizing the RaptorMobile VPN client. The VPN is configured to use the strongest key encryption allowed by U.S. export control laws.

Diagram 1: GIAC Enterprises Security Architecture

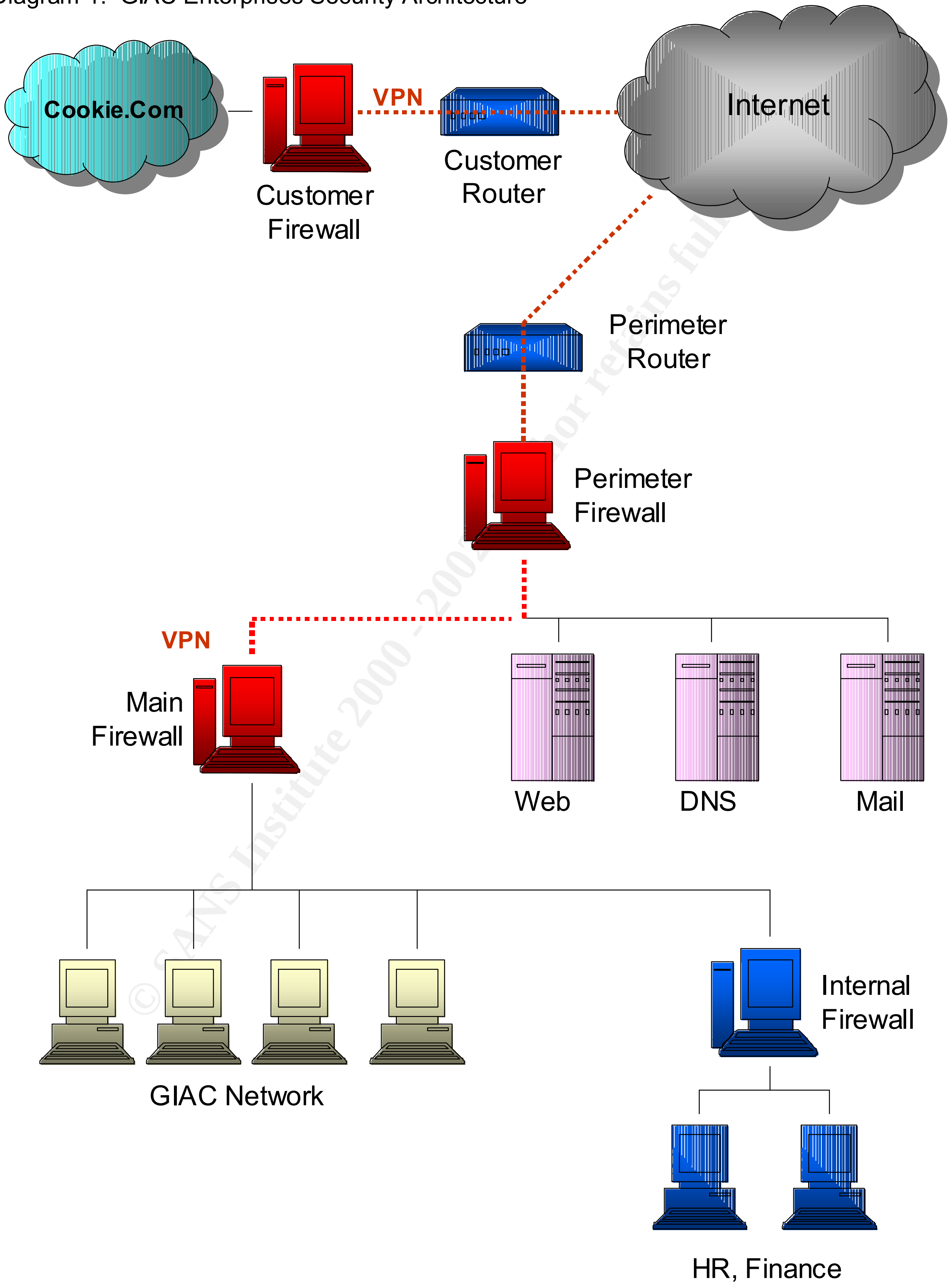


Diagram Description

GIAC Enterprises Perimeter router

System	OS/Software Version
Cisco Router 7204	IOS 12.1

The primary function of the router is to route traffic. However, this router is also used to block certain types of traffic. The border router will provide an initial screen of traffic destined for the GIAC Enterprises network. Some filtering is performed by this perimeter router to reduce the load on the perimeter firewall by denying traffic originating from private Internet addresses, by controlling ICMP traffic and by blocking protocols not used on GIAC Enterprises' external network such as Netbios and Ident. In addition to decreasing the perimeter firewall processing, the screening will also minimize the number of entries in the firewall logs.

GIAC Enterprises Perimeter Firewall

System	OS/Software Version
Intel Pentium 4	FreeBSD, IP Filters, version 3.4.16

The perimeter firewall is also used to further screen traffic destined for the server network and to GIAC Enterprises' main firewall. For example, only HTTP traffic is permitted to go to the web server, SMTP traffic to the mail server, DNS traffic to the DNS server, etc. The traffic filtering process is intended to protect the servers from attacks on ports other than the intended service port.

The IP Filters firewall is installed on a robust Intel based system with two network interfaces running FreeBSD as the operating system. FreeBSD is a freeware UNIX operating system that is well regarded for strong security. The IP Filters firewall will be configured as a bridge (i.e., no IP address). Hence, the firewall is invisible to unauthorized "sniffers" on the network so that makes it quite difficult to target. However, the disadvantage of not having an IP address is that firewall configuration can only be done via the console.

All perimeter firewall functions are to be handled by the IP Filters software. IP Filters is also freeware software that not only serves as a packet-filtering firewall but also provides the ability to retain state information on communication sessions. To illustrate how stateful firewalls can enhance security, consider an internal system establishing a TCP connection session through the firewall. The first packet will contain a synchronize (SYN) flag to start the session. A server outside the firewall responds with a packet containing a synchronize (SYN) and an acknowledgement (ACK) flag. Because the firewall has an entry in its' state tables for the initial connection request, it can only allow a response to the request from the contacted host. At the same time a telnet request from the contacted host would be denied because no established session exists.

Besides the advantage of minimal budget requirements, FreeBSD and IP Filters were selected for their performance. Thus, the firewall will provide high-speed connections for existing customers, suppliers and partners.

Server Systems

Systems	OS/Software Version
Web server – Sun Ultra 10	Solaris 2.8, Apache HTTP (latest version)
Intel Pentium 4	FreeBSD, Sendmail (latest version)
Intel Pentium 4	FreeBSD, BIND (latest version)

As part of GIAC Enterprises' "Defense in Depth" policy, these server systems are configured very securely (i.e., hardened) even though they are protected by a firewall and are located in the DMZ. Each system has one primary function and all unnecessary services have been removed. The latest versions of the software have been installed along with all security hot-fixes, patches. All systems are required to have integrity-checking software (e.g., ESM, Tripwire) installed.

GIAC Main Firewall

System	OS/Software Version
Sun Ultra 60	Solaris 2.8, Raptor 6.5 (w/PowerVPN)

GIAC Enterprises' main firewall, which will protect the business network, is a proxy firewall. Proxy firewalls are considered more secure than either packet-filtering firewalls or stateful firewalls because it combines the capabilities of both types. For example, proxy firewalls examine the source and destination IP addresses and ports like a packet-filtering firewall. Furthermore, proxy firewalls also maintain information about the state of a communication session like a stateful firewall. Thus, a proxy firewall contains information about the application itself and provides an "air gap" between the two networks. This means that a proxy firewall can detect different services running on well-known ports.

By design, the proxy firewall (Raptor) is located behind the stateful (IP Filters) firewall. This design will provide enhanced protection because hackers will have to exploit vulnerabilities for two different types of firewalls.

Symantec acquired Axent in July 2000. Since the acquisition, the Axent Raptor firewall has been renamed Symantec Enterprise Firewall, version 6.5. Similarly, the PowerVPN software has been renamed Symantec Enterprise VPN. However, I will use the Raptor name to prevent confusion. Symantec does have a new product called VelociRaptor, version 1.1 but it is a very new (untested) product.

Since the firewall actually performs the functions of the “proxied” services, it is slower than other types of firewalls. Also, there are only a limited number of proxies that have been designed for a firewall. Communications on other than the well-known services do not have proxies and therefore cannot be secured to the same level.

GIAC Network Systems and Internal Subnet Systems

Systems	OS/Software Version
Intel Pentium systems	Windows 2000, SP2
Intel Pentium systems	Windows NT 4.0, SP 6a
UNIX	Solaris 2.8 w/latest security patches

All GIAC systems must have anti-virus software installed and virus signatures must be updated regularly. All systems on the GIAC internal network are also routinely scanned for vulnerabilities. GIAC users must either accept one of several company standard configurations that are maintained by the systems administrators or take responsibility for timely implementation of security hot-fixes and patches that are recommended by the security staff.

GIAC Internal Firewall

System	OS/Software Version
Intel Pentium 4	FreeBSD, IP Filters, version 3.4.16

An internal firewall will be installed for internal departments with confidential information (e.g., Human Resources, Finance). According to a recent study, internal personnel are responsible for many of the computer security incidents experienced at small and large companies.

The configuration of the internal firewall will be similar to that of the GIAC perimeter firewall although external access from within the sensitive network will not be as stringently controlled.

Assignment 2 – Provide a Security Policy

Border Router Policy

The function of the border router is to route traffic. The perimeter defense begins at the border router so Access Control Lists (ACLs) may be used to allow or deny traffic through the router. Here is the set of ACLs implemented on the GIAC border router. Comments are provided to describe each ACL or group of ACLS following the Cisco router syntax.

```
ROUTER#sho run
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
service password-encryption
```

Comment: The running configuration on the router is displayed by typing the command ‘show run’. The IOS version is displayed. The ‘service timestamps’ command configures the system to provide a timestamp for all debugging and logging entries. The ‘service password-encryption’ command is used to ensure that the password will be encrypted.

```
hostname ROUTER
enable secret 5 %0&~dNc*t*(#21xxxxxxxx/
```

Comment: The hostname is specified. The next line is a very important line. The ‘enable secret’ command means that the router will require a password to enter privileged mode. The number 5 indicates the type of encryption used for the password and the rest of the line is the encrypted password.

```
no ip subnet-zero
```

Comment: The next configuration line turns off the ability to use subnet zero. This is used to eliminate any potential for having both a network and a subnet with the same IP addresses.

```
no ip source-route
```

Comment: This command will deny all source-routed packets. Hackers may exploit the ability to specify the route a packet will take rather than rely on the router to route the packet. Source routed packets are denied by the main firewall but it is good to stop them at the router also.

```
no ip finger
```

Comment: Disable finger to prevent querying of current connections on the router.

```
ip domain-name GIAC.com
ip name-server 9.9.9.9
```

Comment: The domain name and the name server are defined.

```
no ip bootp server
no ip http server
no cdp run
```

Comment: Always remember to disable unnecessary services on the router. Disabling the HTTP server will prevent a potential Denial Of Service attack. For additional information, refer to http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml
Note: The Cisco HTTP service was also vulnerable to the Code Red worm. CDP (Cisco Discovery Protocol) allows devices to share basic configuration information so it must be disabled.

```
snmp-server community secret RO
```

Comment: Remember to secure Simple Network Management Protocol (SNMP) with a community name other than the default names (i.e., public or private).

```
interface FastEthernet0/0
 ip address 9.9.9.194 255.255.255.192
 ip access-group 101 in
 full-duplex

interface FastEthernet1/0
 ip address 9.9.9.2 255.255.255.192
 ip access-group 102 in
 full-duplex
```

Comment: Specify the interface information including connection type, port number, IP address, filter list number (access-group) and duplex type.

```
ip classless
```

Comment: Configure the router to forward packets that are destined for the subnets of any networks that are directly connected.

```
ip route 0.0.0.0 0.0.0.0 <ISP Router IP>
```

Comment: The default route is established.

```
access-list 101 deny  udp any any eq netbios-dgm log
access-list 101 deny  udp any any eq netbios-ns log
access-list 101 deny  udp any any eq netbios-ss log
access-list 101 deny  ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny  ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny  ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny  ip 9.9.9..0 0.0.0.63 any log
access-list 101 deny  ip 9.9.9.64 0.0.0.63 any log
access-list 101 deny  ip 9.9.9.128 0.0.0.63 any log
```

Comment: Here we begin the extended access list number 101. ACL 101 is applied to the interface that is attached to the Internet. Deny unnecessary Netbios traffic and traffic from all private/registered and non-routable Internet IP addresses.

```
access-list 101 deny icmp any any
```

Comment: Deny all ICMP traffic (i.e., SYN floods) from the Internet.

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

Comment: If traffic is not denied by any previous Access Control List, allow it with the preceding syntax.

```
access-list 102 permit ip 9.9.9.0 0.0.0.63 any
access-list 102 deny  ip any any log
```

Comment: This is the extended access list number 102. ACL 102 is applied to the interface connected to the GIAC Enterprises service network. Allow any traffic from the service network. Deny any packets on the inside interface that do not originate from the service network (e.g., spoofed addresses).

```
banner motd ^C ************************************************
*                                                              *
*    GIAC Enterprises Inc.                                     *
*                                                              *
*    WARNING!!!!                                               *
*         Unauthorized Access is strictly prohibited           *
*         All access attempts are logged.                      *
*        Unauthorized Access is against the law and            *
*        will be prosecuted.                                   *
*                                                              *
****************************************************************
^C
```

Comment: Be sure to insert an intimidating banner for those who stumble upon the router.

```
line con 0
password 7 972190B14C3Z480MC2P
login
transport input none

end
```

Comment: Finally, the last 4 lines configure the router to be managed from the console. A password is required. The “7” is the encryption type and the remainder of the line is the encrypted password. Based on this configuration, the router can only be managed from the console.

Additional Cisco router specific to IOS version 12.1 is available at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/

GIAC Enterprises Perimeter Firewall

IP Filters is somewhat unique because it takes the last rule that satisfies the criteria for the packet and performs the desired operation. IP Filters rules are implemented using keywords. A brief description of some IP Filters keywords are provided below:

- **Block/pass** – The first word in each rule that describes the action to be taken on the packet that satisfies the rule criteria. Obviously, "Block" is used to deny and "pass" is used to allow a packet to proceed.
- **In/out/all** – Next, in/out/all describes the type of packet that is allowed or denied. "In" denotes a packet coming into the firewall, "out" denotes an outgoing packet, and "all" is both. (Note: "in" and "out" are not specific to any interface)
- **On xl0** – This denotes the interface that the rule applies to. The interfaces described below are xl0 and xl1.
- **Quick** – The quick keyword is used to discontinue reading the rule base for applicable rules and perform the operation on the packet. This word cancels out the use-last-rule-that-applies algorithm of the firewall.
- **Proto** – IP Filters can filter all IP traffic. The "proto" keyword is used to indicate any of the common IP protocols (e.g., TCP, UDP, etc.).
- **From** – The "from" keyword enables the firewall to limit packets by source. The source can be a hostname or even a network.
- **To** – The "to" keyword similar to the "from" keyword enables the firewall to examine the destination of the packet.
- **Log** – The "log" keyword is used to specify logging of a packet that satisfies the rule (block or pass). Logging is not automatic with IP Filters. A third party tool is required to view the logs.
- **Group** – This keyword identifies the group for rule applicability. The group keyword provides flow control within the rule set.
- **Keep state** – This parameter allows the firewall to retain state information.

To configure a system to run IP Filters the following items must be accomplished:

- set ipfilter=YES in /etc/rc.conf

Reminder: The kernel must be compiled with option IPFILTER turned on:

- set net.inet.ip.forwarding=1 in /etc/sysctl.conf

The rules in the file /etc/ipf.rules are then used to configure the firewall.

The IP Filters rules are provided per group according to the interface and destination.

The firewall groups established are:

- Group 10 – Incoming packets from the Internet (interface xl0) to GIACnet are examined.
- Group 15 – Incoming packets from the Internet to the server network in the DMZ.
- Group 20 – Incoming packets from the interior of the bridging firewall (interface xl1).

Outgoing packets to the Internet are passed without examination. These packets are examined when entering the firewall. Again, outgoing packets on the inside interface of the firewall are also passed. Packets on the local host interface (lo) are allowed.

This will be the rule set top-level decision tree. Interface xl0 is the interface to the perimeter router and on to the Internet. Interface xl1 is the interface to the service network.

```
Block in log quick on xl0 from any to 9.9.9.0/24 all head 15
Block in log quick on xl0 all head 10
Pass in quick on xl1 all head 20
Pass out quick on xl0 all
Pass out quick on xl1 all
Pass in quick on l0 all
```

Rule Group 10

Comment: The following rules are part of group 10. These rules are the basic rules for examining traffic coming in from the Internet. The first two rules block all packets from the Internet with IP options set (first rule) and packets that are fragmented (second rule).

```
block in log quick all with ipopt group 10
block in log quick all with frag group 10
```

Comment: Deny any rules coming from the Internet with the IP addresses of the service network (i.e., spoofed packets).

```
block in log quick from 9.9.9.0/24 to any group 10
```

Comment: Deny any other spoofed packets and log the packets. Tip: monitor the logs because the packets should have been blocked at the perimeter router.

```
block in log quick from 255.255.255.255/32 to any group 10
block in log quick from 0.0.0.0/32 to any group 10
block in log quick from 127.0.0.0/8 to any group 10
block in log quick from 10.0.0.0/8 to any group 10
block in log quick from 172.16.0.0/12 to any group 10
block in log quick from 192.168.0.0/16 to any group 10
block in log quick from any to 255.255.255.255/32 group 10
block in log quick from any to 0.0.0.0/32 group 10
block in log quick from any to 127.0.0.0/8 group 10
block in log quick from any to 10.0.0.0/8 group 10
block in log quick from any to 172.16.0.0/12 group 10
block in log quick from any to 192.168.0.0/16 group 10
```

Rule Group 20

The following rules are part of the second group. These packets are coming in from the inside interface via the service network. This rule allows communication attempts from inside GIACnet (i.e., originate from the GIACnet proxy firewall). The “keep state” keyword means that only sessions initiated inside will be allowed to receive responses.

```
pass in quick proto tcp port all flags S keep state group 20
```

Comment: UDP connections from DNS are also allowed.

```
pass in quick proto udp from any to any port = dns keep state group 20
```

Rule Group 15

Comment: Rule Group 15 is specifically set for packets from the Internet destined for the server network. The same concerns apply as in Rule Group 10. The following rules are duplicated from group 10.

```
block in log quick all with ipopt group 15
block in log quick all with frag group 15

block in log quick from 9.9.9.0/24 to any group 15

block in log quick from 255.255.255.255/32 to any group 15
block in log quick from 0.0.0.0/32 to any group 15
block in log quick from 127.0.0.0/8 to any group 15
block in log quick from 10.0.0.0/8 to any group 15
block in log quick from 172.16.0.0/12 to any group 15
block in log quick from 192.168.0.0/16 to any group 15
block in log quick from any to 255.255.255.255/32 group 15
block in log quick from any to 0.0.0.0/32 group 15
block in log quick from any to 127.0.0.0/8 group 15
block in log quick from any to 10.0.0.0/8 group 15
block in log quick from any to 172.16.0.0/12 group 15
block in log quick from any to 192.168.0.0/16 group 15
```

Comment: Allow Internet requests to the server systems according to port number.

```
pass in quick proto tcp from any to 1.2.3.6 port = http group 15
pass in quick proto tcp from any to 1.2.3.7 port = smtp group 15
pass in quick proto tcp from any to 1.2.3.2 port = ftp group 15
```

Comment: Allow Internet requests to the firewall for VPN. Port 50 is used for Encapsulation Security Payloads (ESP).

```
pass in log quick proto udp from any to 1.2.3.2 port = 500 group 15
pass in log quick proto tcp from any to 1.2.3.2 port = 50 group 15
```

Comment: Allow UDP requests to the DNS server.

```
pass in log quick proto udp from any to 1.2.3.9 port = 53 group 15
```

Comment: Requests to ports other than standard system service should be blocked and logged (e.g., log HTTP requests to the mail server). In the following example, the "flags" keyword is used to have the firewall examine the TCP/IP packet flags.

```
block in log level local0.warn quick proto tcp all flags S/SA group 15
block in log level local0.warn quick proto tcp all flags SA/SA group 15
block in log level local0.warn quick proto tcp all flags SAFRPU group 15
```

GIAC Enterprises Main Firewall

The firewall that protects the GIAC Enterprises network is a Raptor, version 6.5, proxy firewall. As mentioned above, the proxy firewall is very secure because it can filter the packets on source/destination ports and IP address, maintain state information and verify the application data at layer 7 of the OSI model. The Raptor firewall being used to protect GIACnet is running the latest version of the Raptor software (excluding the new VelociRaptor product). All authorization rules have the following elements:

- Source – the originator of the packet and the interface in its' path (i.e., named IN and OUT).
- Destination – the intended destination of the packet.
- Action – any actions such as permit or deny.
- Services and protocols – there are three types of services/protocols
    - Plain services/protocols – self-explanatory
    - Services/protocols with additional settings such as FTP
    - Services/protocols with no pre-defined proxy

Optional rule elements include:

- Scope – similar to VPN tunnel rules
- Time – a setting to control connections by time or day of the week
- User or User groups – intended for rules requiring authentication
- Data scanning – specify whether the application payload is examined
- Thresholds – specify a level at which an alert is generated

Before creating rules in the Raptor firewall, setup the network and user components. Examples of network components for Raptor include networks, subnets, specified hosts, and domains.

The Raptor firewall operates with the default mode of denying all connections except those that are specifically allowed. The rules are evaluated on a "best fit" basis for each connection attempt so the rule that best fits a packet is the one that is applied. Similar to other firewalls, the evaluation criterion is to match specific rules first followed by the more general rules. If case of a tie, Raptor will default to a deny rule if one exists. If not, Raptor will apply the most restrictive rule.

An example of the Raptor rule-ranking process -- ranking is done first by service and next by source and destination. The ranking of source and destination is performed first by hosts, then by subnets and finally by interface. The interface parameter is a new feature on Raptor version 6.5.

The following generic labels will be used in the rule set description process. Note: The GIAC Enterprises network diagram does not display an internal DNS server.

- GIAC-net - all the systems in GIAC Enterprises' 192.168 internal network.
- Universe – a Raptor provided label for all network entities.
- Service – for the systems on the service network
- GIAC-Int – the inside interface to the firewall.
- Out-Int - the outside interface to the service network and Internet
- Serv-mail – the service network mail system
- GIAC-mail – GIAC Enterprises' internal mail server
- GIAC-DNS – internal DNS server
- Serv-DNS – the service network DNS system

The following format will be used to present the GIAC proxy firewall rules. Raptor's rule maintenance window is similar. Raptor handles mail and DNS in a unique fashion so there are few rules required to handle such traffic.

TYPE	IN	SRC	DEST	OUT

HTTP Setup

The first rule we will create is to allow GIAC employees to use the World Wide Web.

TYPE	IN	SRC	DEST	OUT
Allow	GIAC-Int	GIAC-Net	Universe	Out-Int

This rule is for the Hyper Text Transfer Protocol (HTTP) service. When this protocol is specified, additional prompts require further information. At this point, HTTPS may be allowed and ports selected. Standard ports (443 & 563) are recommended. Other application-type choices may be selected:

- allow FTP protocol conversion
- allow Gopher Protocol conversion
- allow DCOM over HTTP

There is an option to restrict specific URLs or filename extensions. Restricting HTTP traffic by either URL or filename extension is not recommended because you must then maintain a table of allowed URLs or filename extensions. This type of activity quickly becomes an administrative nightmare.

FTP Setup

The next rule we will create is to allow GIAC employees to FTP out to the Internet.

TYPE	IN	SRC	DEST	OUT
Allow	GIAC-Int	GIAC-Net	Universe	Out-Int

This rule is for the File Transfer Protocol (FTP) service. At this point, FTP "Puts" and/or "Gets" may be configured.

SMTP Setup

The Simple Mail Transfer Protocol (SMTP) service is configured next. Raptor has an SMTP server application proxy. The server supports transparent addressing and checks all traffic entering and leaving the domain for known sendmail vulnerabilities. To set up the mail proxy, use the "Configure Mail Menu" option. The resulting window requests the IP address of the GIAC internal mail server. Do not select the button to "allow all internal hosts out". This means the Raptor mail proxy will only allow the GIAC internal mail server to talk to the service network mail server and vice versa. GIAC Enterprises has elected to not utilize Raptor's anti-spam measures since the mail servers already disallow SMTP forwarding. The resulting mail rules are listed below.

TYPE	IN	SRC	DEST	OUT
Allow	<ANY>	Universe	GIAC-mail	<ANY>
Allow	<ANY>	GIAC-mail	Universe	<ANY>

Since we are using an external forwarding mail system we will further refine this rule to authorize only communications between the external and internal mail servers. The new rules look like this:

TYPE	IN	SRC	DEST	OUT
Allow	Out-Int	Serv-mail	GIAC-mail	GIAC-Int
Allow	GIAC-Int	GIAC-mail	Serv-mail	Out-Int

DNS Setup

Domain Name Service (DNS) is configured next. Raptor provides what appears to be a fairly strong DNS proxy solution in the firewall. The problem with this solution is that it will violate the GIAC Enterprises policy of one primary service on one system. Raptor does not use BIND for DNS on the firewall but it still may have similar vulnerabilities. For this reason, a system on the service network will be used for DNS.

TYPE	IN	SRC	DEST	OUT
Allow	GIAC-Int	GIAC-DNS	Serv-DNS	Out-Int
Allow	Out-Int	Serv-DNS	GIAC-DNS	GIAC-Int

These rules allow the GIAC internal DNS server to pass unknown requests to the service network DNS server. The service network DNS server can then respond back to the GIACnet DNS system. To configure this communication we will use a Generic Service Passer (GSP) on Raptor. The GSP will use a UDP protocol with the standard port number 53 for DNS.

Remote Firewall Management

The firewall is configurable to allow remote management from systems other than the console. However, care must be taken to minimize the number of administrators who can manage the firewall because only one person can have read/write access to the firewall at a time.

Raptor's Remote Management Console (RMC) is used to communicate with the firewall using 3DES for domestic use or DES for international use. An RMC configured for domestic use can manage an international firewall but a RMC configured for international use cannot manage a domestic firewall.

The RMC communicates with the Raptor firewall via ports 416, 418, and 481. Filters have been installed on the firewall so that it does not listen for connections on these port numbers from the external interface. This configuration meets the GIAC Information Security policy network security requirements (i.e., reduce the probability of stumbling upon vulnerabilities from an external perspective). All firewall management must be done from GIACnet or on the console.

Remote management functions are configured via two commands at the firewall console.

- rempass – this command establishes the password for remote management.
- setremote – this command enables management access from a specific remote system.

Raptor provides remote management client software for both Solaris systems and Windows NT systems. The remote management client software is free with the purchase of the Raptor firewall software.

VPN Client

The RaptorMobile VPN client allows individuals to utilize an encryption client on a desktop or laptop system to establish a VPN over the Internet. This type of connection is an ideal solution for customers, suppliers and partners.

The steps required to establish a RaptorMobile secure tunnel include:

- Defining network entities – systems and subnets that the VPN will access
- Defining the local gateway entity – firewall's external interface and security parameters
- Defining the VPN policy – type of encapsulation, type of encryption algorithm, type of data integrity algorithm, etc.
- Defining the secure tunnel

- Configuring the RaptorMobile client

Network entities – A single system is set up on GIACnet inside the firewall to receive shared customer, supplier and partner data. Because name resolution can be an issue with the mobile clients, only one system is configured to receive the shared data. The firewall will be the local VPN endpoint and IPSec/IKE is selected as the VPN policy. Also, because GIACnet utilizes non-routable IP addresses, network address translation will be utilized for the VPN.

Here is an example of the firewall rules for this VPN.

TYPE	IN	SRC	DEST	OUT
Allow	Out-Int	Universe	Supplier-host	GIAC-Int
Allow	GIAC-Int	GIAC-Net	Universe	Out-Int

The user entity setup on the firewall requires:

- Phase 1 ID – a value for first level key negotiations (the user will be prompted for a password)
- A shared secret (optional) that is entered both on the firewall and in the RaptorMobile client; or,
- A user certificate – an authentication device bound to identifying information called a distinguished name as defined by the X.509 standard

The phase 1 ID is a unique name provided to each supplier by GIAC administrators. For simplicity, GIAC Enterprises will use a shared secret configuration and not a certificate. For greater security all customers, suppliers and partners will be assigned a SecureID card to use with Raptor's extended authentication.

Ike_default_crypto_strong will be used as one of the pre-configured VPN policies that come with Raptor. This policy uses the IPSec/IKE encapsulation protocol. Because we are translating the IP address we will pass the traffic through the Raptor proxies. For the data integrity algorithm, SHA1 was selected since it is regarded as more secure. And finally, 3DES was selected as the primary encryption preference and regular DES as the secondary preference.

Assignment 3 – Audit Your Security Architecture

At a minimum, a process for security assessments should include the following:

- All assessment procedures must be documented and readily available.
- Internal processes must be established to audit compliance to the GIAC Enterprises Information Security policy.
- Security assessments must be conducted on a regular basis.
    - It is recommended that all Windows systems be assessed at least monthly.
    - All non-Windows systems must be assessed on a quarterly basis.
- Third-party vendors will be contracted to complete a comprehensive assessment on a quarterly basis subject to budget limitations. Security assessments are expensive. Based on my work experience, a single web application assessment may cost as much as $25,000 per web site.
- Assessments must be scheduled during non-business hours.

There are three areas that need to be assessed in any security architecture. Security assessment requirements may vary dependent upon the types of systems in each area.

External Systems

Included in the assessment of external systems are the border router, firewalls, and any potential backdoors to the network such as analog phone lines. Several tools will be used to accomplish this assessment as outlined in the tools section. Specifically, we will be looking for open ports, and authentications issues. A manual audit of the logging functionality will be required. These tests will be performed to assess all vulnerabilities as well as audit the level of compliance to established GIAC policies.

Systems in the De-Militarized Zone (DMZ)

DNS, Web and Mail servers are situated in the DMZ. The security assessment in the DMZ area will focus on detecting any configuration flaws on these servers. The assessment will also identify any unnecessary services that are active. A test of the firewall from the DMZ area will be conducted to check that only ports allowed are those outlined in the policy. A manual check of logging activity is necessary for all devices in the DMZ.

Internal Systems

Even if the GIAC Enterprises network has a crunchy outer shell, the interior is most likely soft and chewy. Thus, the GIAC Information Security policy explicitly states that all hosts on the internal network will be scanned to identify system vulnerabilities and unnecessary services. A custom ISS scan policy is required to audit compliance to the standard security configuration established for GIAC host systems. A tedious manual audit to verify overall compliance to the “need-to-know” policy will be assessed on an annual basis. It is a conceded that Social engineering is 100% effective and thus will not be tested.

Tools to assess External Systems:

- ISS Internet Scanner 6.1 – ISS will be used to scan for open ports and to scan hosts/devices in the DMZ and internal network.
  http://www.iss.net
- Network Associates CyberCop Scanner
  http://www.nai.com/
- Nmap - This tool will be used to probe for unauthorized open ports/services.
  http://www.insecure.org/nmap/

Tools to assess Systems in the DMZ:

- Whisker.pl – a perl script used to check for CGI vulnerabilities on web servers; also useful for identification of web servers and versions.
  http://www.wiretrip.net/rfp
- Sam Spade – This web site provides tools used to query information from the DNS servers.
  http://www.samspade.org
- Security scanners already listed above (Internet Scanner, CyberCop, nmap).

Tools to assess Internal Systems:

- Security scanners already listed above.
- LC3 – used to crack Windows NT & Windows 2000 passwords
  http://www.atstake.com/research/lc3/index.html
- Crack – used to crack Unix passwords
  http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=Crack

GIAC Enterprises Tool of Choice: ISS Internet Scanner, version 6.1

The ISS Internet Scanner is one of many tools that may be used to scan the systems in the three areas. A thorough security assessment requires the use of at least two different tools in order to provide better detection of vulnerabilities. Other tools include: Network Associates CyberCop and the freeware Nessus scanner.

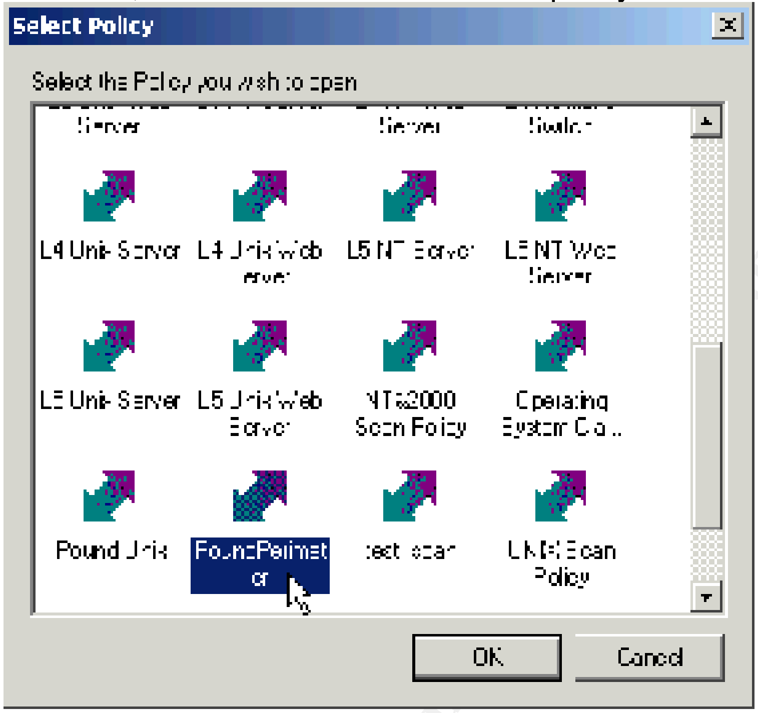
Note: ISS Internet Scanner 6.2 was released within the past week but extensive testing is required before using the new version in a production environment.

ISS Internet Scanner 6.1 is a user-friendly tool especially for day-to-day security scanning. Internet Scanner contains default policies and the capability to create custom polices to suit the GIAC Enterprises network. Repeat scans using the same scan policies may be used to generate trend analysis charts. Regular scanning per the security assessment process is highly recommended to keep up with newly identified system vulnerabilities.

The following section will describe the step-by-step procedures for running a simple scan using ISS Internet Scanner. ISS does provide adequate documentation for new users so a thorough review of the documentation is required. The ISS Internet Scanner must be configured correctly, preferably on a system designated for scanning purposes.

Regardless of security scanner product, each must be updated with the latest vulnerability checks. For example, ISS Internet Scanner uses an update mechanism called X-PressUpdate. This is a critical step similar to updating virus definitions for anti-virus software.

The first step is to gather information regarding the target systems (i.e., IP addresses, host names, etc). Next, start up the Internet Scanner software. The software provides a "wizard" to walk novice users through the required steps. For example, there is a prompt to select a default policy or a custom policy for servers by operating system. For this scan, a "PoundPerimeter" custom policy has been created.



Navigating through the wizard prompts is relatively easy. When finished responding to the prompts, an ISS session window will appear. From the tool menu bar, select Scan. That is it. The scanner will start pounding away at the target hosts. It is very important that all Denial of Service and Buffer Overflow attacks be disabled unless if pre-scan coordination has been planned. Intrusion detection software will be tested extensively too so those monitoring such activity logs should be contacted prior to the scans.

The scan would be conducted during non-business hours or during scheduled downtime since the scans may affect the performance of the scanned systems and may result in inadvertent and unintended denial of service. After the scan is completed, reports may be generated to view all the discovered vulnerabilities, services running, standard configuration discrepancies and local accounts on that machine.

A sample entry from an ISS report is shown below.

Vulnerability Name	**Severity**
Back Orifice 2000 allows complete remote administrative control of compromised ~	High

Description:
Back Orifice 2000 is a remote administration tool, or 'trojan horse,' designed to allow the remote operation of infected Windows 9x and Windows NT machines. This program was designed with stealth in mind, and as such is very difficult to detect with scanning, cleansing, and intrusion detection tools.
Fix
Contact your anti-virus vendor for updates to allow the automatic cleanings of systems infected with Back Orifice 2000.

IP Address	DNS Name	Additional Info	More Info	Session ID
xxx.xxx.xxx.xxx	test_system	Port 54321		118

At this point, the difficult work begins. All vulnerabilities must be closely examined in the ISS report. The security scanners are notorious for generating multiple false detections.

This type of security assessment using commercial and freeware scanners will need to be performed for the three target areas. Again, it is highly recommended to use a mixture of tools to provide the best coverage of vulnerabilities.

Analysis and Recommendations:
After the implementation phase of the security assessment is complete, all the reports from all the different tools must be combined to produce a report containing a list of all vulnerabilities. The ISS Internet Scanner uses a ranking scale of high, medium and low to categorize the vulnerabilities. However, GIAC Enterprises security administrators have developed their own definitions for high, medium and low-risk vulnerabilities.

- High: Any vulnerability that allows an attacker to gain immediate access into a machine, to gain admin/superuser access, or to bypass a firewall.
- Medium: Any vulnerability that provides information, degrades performance, or has a high potential of giving system access to an intruder.
- Low: Any vulnerability that provides information that could potentially lead to a compromise.

A security assessment of the GIAC Enterprises perimeter security architecture revealed the following vulnerability. The perimeter devices are vulnerable to a Distributed Denial of Service (DDOS) attack. According to the CERT Advisory CA-1999-17, the following actions should be taken to reduce the risk from a distributed DOS (DDOS) attack:

- Implement network ingress filtering in accordance with RFC-2267.
- Perform egress filtering (i.e., only allow valid internal addressing out)
- Block incoming broadcast addresses
- Turn off directed broadcast capability
- Block private and reserved addresses
- Block unused ports and those known to be associated with DDOS attacks

Assignment 4 – Design Under Fire

The network design chosen for the attack is:
http://www.sans.org/y2k/practical/Alexander_Usenko_GCFW.doc

Firewall Attack

Mr. Usenko stated in his documentation "The platform (hardware, firmware and operating system) hosting the firewall should be hardened by applying the latest vendor supplied/recommended patches/service packs and disabling all non-required services."

However, as most experienced security professionals know, applying patches/services packs on a regular basis is a challenging task for most system administrators. A quick search at the CheckPoint FireWall-1 technical support web site revealed a number of serious vulnerabilities.

- GUI Buffer Overflow – September 19, 2001
- Format Strings Vulnerability – July 11, 2001
- RDP Communication Vulnerability – July 9, 2001
- Denial of Service reported on RealSecure Network Sensor – March 12, 2001
- Fast Mode Vulnerability – December 18, 2000
- Potential Security Issues Recently Identified in FireWall-1 – July 26, 200
- IP Fragmentation DoS Vulnerability – June 6, 2000

A hot-fix for the most recent vulnerability (GUI Buffer Overflow) was released by CheckPoint but the odds are pretty good that the system administrator has not applied the patch yet. According to CheckPoint's sanitized summary, the GUI Buffer Overflow vulnerability is described as follows:

> "An issue exists in VPN-1/FireWall-1 Management Server running on Windows NT or Windows 2000. A malicious administrator (me) can exploit a buffer overflow condition in the GUI authentication code to potentially impair management station functionality or to execute code."

A search of the major hacking/security web sites did not reveal any known exploits (yet). However, CheckPoint FireWall-1 is plagued by a well-known authentication vulnerability. According to the write-up available at:
http://packetstormsecurity.org/0001-exploits/checkpoint-fw1.vuln.txt

> "The basic authentication used in Checkpoint FW-1 used inside/outbound and outside/inbound allows unlimited attempts to authenticate without a timeout or disconnect between unsuccessful attempts. To make matters worse, the attempt at authentication will let you know if you have the wrong username before you are allowed to enter in the password. The exploit is trivial, grind away at user names until you hit one that works and then grind away at passwords with the username you just found until you find one that works."

Therefore, there are many avenues of attack to target the firewall.

Denial of Service Attacks

A well-placed Trojan will easily compromise fifty cable/DSL modem systems. The Trojans could be mass-mailed to unsuspecting victims who are without updated anti-virus signatures. Since Mr. Usenko's web servers are not protected by a firewall, a simple flood of TCP SYN, UDP or ICMP packets with spoofed IP's may be aimed at the web servers. A newbie hacker would most likely attempt a denial of service just to see what happens. Some load balancing systems provide a SYN flood defense (e.g., Cisco LocalDirector). By only allowing a certain rate of SYNs or a certain number of connections that are half-opened, load balancing systems are configured to close the connections after a certain threshold has been reached. Cisco Local Director is configurable to block ICMP and UDP packets. Another security measure to protect the web servers is to place them in a DMZ. Then, the firewall could be easily configured to prevent denial of service attacks. Once compromised, the unprotected web servers could be used as a launch point to target other systems in the vicinity.

Attack to Compromise Internal Systems

For an attack to succeed in compromising the internal systems, the target of choice is the web server because of its' accessibility. Mr. Usenko did not specify the web server type nor did he specify the version. Fortunately (or unfortunately for Mr. Usenko), there are tools such as whisker.

```
./whisker.pl -h www.giac.com
-- whisker / v1.4.0+SSL / rain forest puppy / www.wiretrip.net --

= - = - = - = - = - =
= Host: www.giac.com
= Server: Microsoft-IIS/5.0
```

Whisker identifies the web server as running Microsoft's Internet Information Services (IIS), version 5.0. Given the recent phenomenon of the Code Red, Code Red 2 and Nimda worms, any decent hacker would run the various URL commands through Mr. Usenko's unprotected web servers to determine if the backdoor Trojan is still present. If not, there are plenty of IIS vulnerabilities. For example, the following command may be used to exploit the MS IIS UTF Directory Traversal and Remote Command Execution Vulnerability:
http://target/Scripts/..%u0025u005c..u0024u005cWINNT/system32/cmd.exe?/c+dir+c:

Once a web server is compromised, it will be a trivial matter of loading malicious code on the server to be downloaded via web browser vulnerabilities. The Nimda worm used this type of exploit to propagate.

List of References:

Books:
Axent Technologies, Inc., (Nov. 2000) Raptor Firewall and PowerVPN V6.5 Configuration Guide for Solaris.

The SANS Institute, SANS Authors (Apr. 2001) Firewalls, Perimeter Protection and Virtual Private Networks training manuals.

Websites:
CERT CA-1999-17: Denial of Service Tools
http://www.cert.org/advisories/CA-1999-17.html

Cisco IOS Security Configuration Guide, Release 12.1.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/

Cisco IOS HTTP Server Query Vulnerability from Cisco (Oct. 2000)
http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml

Conoboy, Brendan & Fichtner, Erik (July, 2001) IP Filter Based Firewalls: HOWTO
http://www.obfuscation.org/ipf/ipf-howto.txt

EEye Digital Security – Code Red Advisory
http://www.eeye.com/html/Research/Advisories/AL20010717.html

Firetower, Inc., (2000) Raptor-to-Cisco IPSEC VPN
http://www.firetower.com/faqs/vpn/ciscovpn-static-ciscoside.html

Packetstorm – CheckPoint FireWall Vulnerabilities
http://packetstormsecurity.org/0001-exploits/checkpoint-fw1.vuln.txt

SANS GCFW Practicals:
http://www.sans.org/y2k/practical/Alexander_Usenko_GCFW.doc

Symantec Security Response Center – Nimda worm information
http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html

Symantec Enterprise Security – Firewalls & VPN product information
http://enterprisesecurity.symantec.com/content/productlink.cfm#2