Global Information Assurance Certification Paper

GIAC Enterprises Network Security Architecture

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment
Version 1.8 (revised September 10, 2002)

SANS Institute Track 2:
Firewalls, Perimeter Protection and VPNs

Capitol SANS
Washington, D.C.
October 19-23, 2002

Terry Hasford

March 2003

Table of Contents

ABSTRACT **5**

ASSIGNMENT 1 – SECURITY ARCHITECTURE

1.1. Company Overview **6**
1.2. Assumptions **6**
1.3. Network Security Strategies **7**
1.4 Business Relationships and Access Requirements **7**
1.5 Network Security Architecture for GIAC Enterprises **8**
1.5.1 Network Design Overview **8**
1.5.2 IP Address Allocation Table **9**
1.5.3 Network Address Translation (NAT) Table **10**
1.5.4 Network Perimeter Design **10**

ASSIGNMENT 2 – SECURITY POLICIES

2.1 Overview **16**
2.2 Router Security Policy **17**
2.2.1 Router Ingress Filtering **19**
2.2.2 Router Egress Filtering **23**
2.3 Primary Firewall Security Policy **24**
2.3 Virtual Private Network Security Policy **30**
2.4 Host-Gateway VPN Tutorial **33**
2.5 Tips, Tricks, and Potential Problems **36**
2.6 Secondary Firewall **36**
2.7 Host Hardening **37**

ASSIGNMENT 3 – AUDIT SECURITY INFRASTRUCTURE

3.1 Primary Firewall Audit Plan **38**
3.2 Primary Firewall Audit Procedures **42**
3.2.1 Auditing From the Internet **44**
3.2.2 Auditing From the Service Network **47**
3.2.3 Auditing From the Internal LAN **47**
3.2.3 Auditing From the Secure LAN **49**
3.3 Primary Firewall Audit Evaluation and Recommendations **50**

Table of Contents
(continued)

ASSIGNMENT 4 – DESIGN UNDER FIRE

4.1 Attack Against the Firewall **51**
4.1.1 Patricia Siow's Network Diagram **52**
4.1.2 Check Point FireWall-1 Documented Vulnerabilities **53**
4.1.3 Attack Scenario **55**
4.2 Denial of Service Attack **55**
4.3 Attack Through the Perimeter **57**

CONCLUSION **58**

APPENDICES

Appendix A – GIAC GCFW Certification Paper Requirements **60**

REFERENCES **64**

List of Figures

Figure 1 – GIAC Enterprises Network (Page 16)
Figure 2 – Cisco Secure VPN 1.1 Client Security Policy Editor (Page 35)
Figure 3 – GIAC Enterprises Firewall Audit Network (Page 40)
Figure 4 – Nmap Windows v1.3.1 screen shot (Page 45)
Figure 5 – Patricia Siow's GIAC Network (Page 56)

List of Tables

Table 1 – GIAC Enterprises IP Address Allocation Table (Page 10)
Table 2 – GIAC Enterprises Network Address Translation (NAT) Table (Page 10)
Table 3 – GIAC Enterprises IKE Policy for the Cisco PIX Firewall VPN (Page 32)

List of Pictures

Picture 1 – Cisco PIX 515 Firewall (Page 11)

Abstract

This is a Global Information Assurance (GIAC) Certified Firewall Analyst (GCFW) Practical Assignment paper, which is submitted to fulfill one of the requirements for GCFW certification. The practical has four separate requirements.

The first section of the paper satisfies the first practical requirement by describing the business operations of a fictitious enterprise named GIAC Enterprises (GIACE) and detailing a network security architecture to protect its business operations. GIAC Enterprises is in the business of selling fortune cookie sayings over the Internet. Access requirements and restrictions for GIACE customers, suppliers, partners, remote workers, and internal workers are defined and discussed.

The second section of the paper satisfies the second practical requirement by defining a security policy for GIAC Enterprises based upon the network security architecture detailed in section one of the paper, and provides a tutorial on setting up IPSec Host-to-Gateway Virtual Private Network (VPN) connections.

The third section of the paper describes the conduct of a technical audit of GIAC Enterprises' primary firewall to verify the firewall policy and provides an evaluation of the audit results, which satisfies the third practical requirement.

The fourth and final section of the paper satisfies the final practical requirement by detailing three different attack scenarios against the network design described in a previously posted GCFW Practical Assignment paper.

See Appendix A – GIAC GCFW Certification Paper Requirements for detailed GIAC GCFW practical assignment paper instructions and requirements.

Assignment 1 - Security Architecture
Define Network Security Architecture

1.1 COMPANY OVERVIEW

GIAC Enterprises is a commercial enterprise employing approximately three hundred personnel at its corporate headquarters in Birmingham, Alabama. GIAC Enterprises' sole source of income is from the online Internet sales of fortune cookie sayings from its web site, www.giacenterprises.com. Every dollar GIACE spends on network security is one dollar less for profits, salaries, bonuses, and stock dividends. The GIACE Board of Directors wants GIACE to act as a "good Internet citizen" but they do not want the company to go bankrupt doing it. The company nets a profit of approximately $10,000,000 a year. GIACE's annualized expenditures for network security are $500,000 for hardware, software, personnel costs and training costs. The GIACE Board of Directors considers the network security costs as money well spent since it protects their Internet business operation, which is the sole source of GIACE's income, and protects the reputation of their company.

1.2 ASSUMPTIONS

- Telnet is not allowed on the network. Secure Shell (SSH) is used in its place.

- FTP is not allowed on the network. The Secure Copy Protocol (SCP) via Secure Shell is used in instead.

- Internal modems are not allowed on the network and are removed before systems are placed on the network.

- All GIACE personnel undergo a background check prior to assuming their positions and periodically thereafter.

- Windows-based operating systems are allowed on the network only if there is a strong business case for their presence. The goal is to limit the types of operating systems on the network to Unix/Linux variants (except for the firmware-based Cisco router and firewall operating systems), which limits the types of operating system vulnerabilities that can be exploited.

1.3 NETWORK SECURITY STRATEGIES

GIAC emphasizes the following security strategies as guidelines in implementing its network security policies (the book Building Internet Firewalls[1] was used as a source and reference):

- **Explicit Deny** - Everything not explicitly allowed is denied access.

- **Least Privilege** - Only the minimum access required to function is granted.

- **If Not Used Then Not Available** – Any system accounts, applications, etc… that are not used are removed, if possible, instead of simply being disabled. Internal modems are removed from systems if they are not required.

· **Defense in Depth** - Defensive components and measures are staggered so that multiple defensive layers must be penetrated in order to exploit the network.

· **Choke Point** - All traffic is funneled through the border router and one or two firewalls.

· **Diversity of Defense** - The two firewalls are from different vendors and use different operating systems. Network-based and host-based defensive measures are employed.

· **Weakest Link** - Any vulnerable access point in the network defenses can be used to breach network defenses.

1.4 BUSINESS RELATIONSHIPS AND ACCESS REQUIREMENTS

GIACE Customers - The customers of GIAC Enterprises are fortune cookie producers and companies that sell/service vending machines that sell fortune sayings. Customers purchase the fortune sayings online in bulk from GIACE at wholesale prices. Customers are permitted access to the GIAC web server via the HTTP protocol (port 80) to browse the website and the SSL protocol (Secure Sockets Layer/https - port 443) to submit purchase order and financial information. Customers also are permitted access to the GIACE mail server via the SMTP protocol (port 25) to transmit email. Any individual on the Internet (unless they are blocked at the GIACE border router) is allowed this level of "public" access to the GIACE network.

1 Chapman, D. Brent and Zwicky, Elizabeth D. Building Internet Firewalls, O'Reilly & Associates, Inc., Sebastopol, CA 1995. 45-54.

GIACE Suppliers - The suppliers of GIAC Enterprises are companies and individuals that author the fortune sayings and sell them to GIAC Enterprises at wholesale prices. In addition to public access, the suppliers are permitted access via any IPSec-compatible VPN software to upload the fortune sayings to the GIACE database via IPSec (UDP port 500) and Encapsulating Security Protocol (ESP) (protocol 50).

GIACE Partners - GIAC Enterprises partners are companies and individuals that translate the fortune sayings from their original language into the languages that the customers desire to purchase. This allows GIAC Enterprises to buy fortune sayings in almost any language and sell them in almost any language format. In addition to public access the partners are permitted access via any IPSec-compatible VPN software to upload and download the fortune sayings to and from the GIACE database via IPSec (UDP port 500) and ESP (protocol 50). The partners download the fortune sayings using SQL Net Client (TCP port 1521) via VPN tunnel.

GIACE On-Site Employees - In addition to public access**,** all GIAC on-site employees at the GIAC corporate headquarters are permitted access to the GIACE mail server, web server, and DNS servers. GIAC database administrators are permitted access to the database server via Secure Shell (port 22).

GIACE Mobile Sales Force and Teleworkers – In addition to public access that all the sale force and teleworkers have, at present two GIAC teleworkers who perform database administration tasks are permitted access to the GIACE Database Server on the Secure LAN via VPN tunnel utilizing IPSec (port 500) and ESP (protocol 50) via Cisco Secure VPN Client 1.1 software.

1.5 Network Security Architecture for GIAC Enterprises

1.5.1 Network Design Overview:

The GIACE corporate headquarters operates a network which is divided into three sub-networks. These networks are located behind the border router and firewalls and will include a Service Network, a Secure Local Area Network (LAN), and an Internal (LAN). The Service Network provides a location for the SMTP Mail server, the external DNS server, and the Web server that customers connect to in order to purchase fortunes online via the Internet. The Secure LAN is protected by a border router and two firewalls and it stores the most valuable GIAC data, the customer information and fortune sayings.

1.5.2 IP Address Allocation:

Note: In order to avoid using assigned Internet IP addresses in this practical assignment, a combination of lower-case letters and numbers are used to represent the external IP addresses for GIACE systems/interfaces, GIACE Remote Workers, GIACE Suppliers, and GIACE Partners:

Example: bbb.bbb.bbb.1 – the IP address provided for GIACE network use by GIACE's ISP and assigned to the external interface of the GIACE border router.

Private IP addresses (RFC 1918) are used for the host IP addresses for the GIACE Services Network, Secure LAN, and Internal LAN.

1.5.2 IP Address Allocation Table:

IP Address	Subnet Mask	Description
bbb.bbb.bbb.1	255.255.255.224	Border Router External Interface
aaa.aaa.aaa.1	255.255.255.0	Border Router Internal Interface
aaa.aaa.aaa.2	255.255.255.0	Primary Firewall External Interface
192.168.3.1	255.255.255.0	Primary Firewall Interface to Service Network
192.168.3.2	255.255.255.0	SNORT IDS Workstation (IDS-1)
192.168.3.3	255.255.255.0	External Mail Server
192.168.3.4	255.255.255.0	External DNS Server
192.168.3.5	255.255.255.0	Web Server
192.168.3.6	255.255.255.0	NTP Server
192.168.4.1	255.255.255.0	Primary Firewall Inside Interface
192.168.4.2	255.255.255.0	SNORT IDS Workstation (IDS-2)
192.168.4.254	255.255.255.0	Secondary Firewall External Interface
192.168.5.1	255.255.255.0	Secondary Firewall Interface to Internal LAN
192.168.6.1	255.255.255.0	Secondary Firewall Interface to Secure LAN
192.168.6.2	255.255.255.0	SNORT IDS Workstation (IDS-3)
192.168.6.3	255.255.255.0	Internal Mail Server
192.168.6.4	255.255.255.0	Internal DNS Server
192.168.6.5	255.255.255.0	Log Server
192.168.6.6	255.255.255.0	Security Administration Workstation
192.168.6.7	255.255.255.0	Database Server
ccc.ccc.ccc.0	255.255.255.0	Remote User Network
ddd.ddd.ddd.0	255.255.255.0	Partner Network
eee.eee.eee.0	255.255.255.0	Supplier Network
fff.fff.fff.1	255.255.255.0	DNS Server of GIACE's ISP
ggg.ggg.ggg.1	255.255.255.5	Trusted Internet Stratum 2 Time Server

Table 1 - GIAC Enterprises IP Address Allocation Table

1.5.3 Network Address Translation table:

Device	Internet Global IP	Internal Local IP
External Mail Server	aaa.aaa.aaa.3	192.168.3.3
External DNS Server	aaa.aaa.aaa.4	192.168.3.4
Web Server	aaa.aaa.aaa.5	192.168.3.5
Time Server	aaa.aaa.aaa.6	192.168.3.6
Log Server	aaa.aaa.aaa.10	192.168.6.5
Database Server	aaa.aaa.aaa.12	192.168.6.7

Table 2 – GIAC Network Address Translation (NAT) Table

Network Address Translation (NAT) is implemented at the Cisco PIX 515E Firewall to deter mapping of GIACE's internal network by outside entities.

1.5.4 Network Perimeter Design

Border Router

GIACE's border router is a Cisco 2650 Router with two 10/100BaseT Ethernet ports and two integrated WIC slots, running Cisco IOS 12.1. The Cisco 2650 Router's modular architecture allows integration with 70 different network modules and interfaces to accommodate network expansion.[2]

The Cisco 2600/3600/3700 Series VPN Module installed on the router provides up to 10 times the performance over software-only encryption by offloading the encryption processing from the router central processing unit (CPU).[3] Cisco provides extensive and high quality online and hardcopy documentation on its networking products, as well as 24-hour technical support that has an excellent reputation.

The border router is a hardened system designed for security services to survive on the edge of a network acting as a static packet filter which examines each network packet entering and leaving the GIAC network. In order to protect the

2 "Cisco 2600 Series Multiservice Platforms"
http://cisco.com/en/US/products/hw/routers/ps259/index.html
3 "Virtual Private Network Modules for Cisco 1700, 2600, 3600, and 3700 Series"
http://cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a008008875.html

border router and the GIAC network against denial of service attacks originating from the Internet, it is configured with a TCP Intercept feature. The TCP Intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks (which occur when a hacker floods a server with a barrage of requests for connection, in a denial of service attack).[4]

Primary (External) Firewall

Picture-1 Cisco PIX 515 Firewall[5]

GIACE uses a Cisco PIX Firewall as its primary firewall. The Cisco PIX 515E Firewall is a stateful filtering firewall designed to be used by small-to-medium businesses, providing 188 Mbps of clear text throughput and providing up to 125,000 simultaneous sessions, up to 2000 IPSec tunnels and up to six 10/100 Fast Ethernet interfaces.[6] "Hardware-based firewalls like the PIX (which store their security-designed operating systems in firmware) typically boot faster than their OS-dependent counterparts, do not experience boot-time errors, and are simpler to upgrade."[7] The Cisco PIX firewalls have been assigned Common Criteria Evaluation Assurance Level 4 (Methodically Designed, Tested and Reviewed) evaluation status.

GIAC Enterprises' Cisco PIX 5151E "Unrestricted" software license (515E-UR) model adds a hot-standby capability (if needed), additional interfaces, and increased VPN performance to the features of the "515E" model. The Cisco PIX 515E (UR) model uses OS Release 6.2(1) and PIX Device Manager 2.0(1),

---

4 "New Features in Release 11.3"
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/rn113m/rn113mft.htm - xtocid63
5 Cisco PIX Firewall (Photo)
http://cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html
6 "Cisco Pix Firewalls"
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/index.shtml
7 "Firewall Comparison: Checkpoint Firewall-1 and Cisco PIX"
http://www.roble.com/docs/fw1_or_pix.html

hardware-based VPN acceleration with 168-bit Triple DES IPSec which has a VPN throughput of 63 Mbps. The firewall is setup as a screened host firewall utilizing the Cisco router for initial packet filtering. The firewall has three active Ethernet interfaces.

Virtual Private Network (VPN) Gateway

VPNs are used for secure encrypted communication from the GIAC mobile workers, GIAC teleworkers, GIAC partners, GIAC suppliers and the GIAC corporate network, with the GIAC primary firewall (Cisco PIX 515E) acting as the VPN gateway.

GIACE's Cisco PIX 515E Firewall is a full-featured VPN gateway that can securely transport data over public networks using site-to-site and remote access VPN applications via 56-bit Data Encryption Standard (DES) or 168-bit Triple DES (3DES), utilizing an integrated hardware-based VPN Accelerator Card (VAC) delivering up to 63 Mbps throughput and 2,000 IPSec tunnels.[8]

External DNS Server

For security purposes GIACE utilizes a split-DNS system.

The external Domain Name System (DNS) server allows GIACE customers, suppliers, partners, and employees to access resources by entering a host name instead of an IP address. The external DNS server holds only the host names and IP addresses of devices on the service network. DNS resolution is provided by GIACE's DNS server and the ISP's DNS server which serves as a secondary DNS server for GIACE. GIACE's DNS server is non-authoritative and only provides name resolution using cached records. GIACE's DNS server relays DNS lookup requests that it cannot resolve to the ISP's DNS servers.

GIACE's external DNS server uses the latest version of Berkeley Internet Name Domain (BIND Version 9.2.1 as of this writing) to implement the DNS protocols. The external DNS server was hardened using procedures outlined in the white paper "Running the BIND9 DNS Server Securely" by Sean Boran (**http://www.boran.com/security/sp/bind9_20010430.html**) as a guide.

Web Server

The GIAC Sun ONE Web Server runs on the Solaris 9 Operating System which includes a SunScreen 3.2 Firewall for host-based protection. The web server uses TrendMicro InterScan VirusWall to scan for malicious programming content

8 "Cisco PIX 515E Firewall**"**
http://cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html

in Internet transactions. "InterScan VirusWall provides high-performance, comprehensive Internet gateway protection against viruses and malicious code".[9]

The GIACE web server is configured to process customer purchase requests, charge their credit cards for the purchase price, retrieve the desired fortunes from the Oracle Database Server, and forward the fortunes to the customer. Secure Sockets Layer (port 443) is used for encryption of the order process and transfer of the fortune sayings.

External Mail Server

The GIACE external mail server uses a Solaris 9 Operating System with the latest version of Sendmail (Sendmail 8.12.7 as of this writing) as its mail server. TrendMicro InterScan VirusWall is used to scan for infected email. The Solaris 9 Operating System has its own integrated host based firewall, SunScreen 3.2 Firewall. The external mail server is used to relay mail to and from the GIACE internal mail server.

Secondary (Internal) Firewall

GIAC Enterprises uses IPFilter on Open BSD (v 3.0) as a secondary firewall, which provides additional layered protection to the internal network. The secondary firewall is not normally susceptible to the same type of attacks that would work on the primary (Cisco PIX) firewall.

Time Server

Accurate time synchronization of all hosts is critical to the proper operation of the VPN and analysis of system logs. The time server uses the Network Time Protocol (NTP) Version 3 (described in RFC 1305) on UDP port 123 to periodically synchronize its time with a calibrated Internet time server in order to provide the correct time to GIAC hosts. The optional Data Encryption Standard (DES) made available with NTP Version 3 is utilized to provide added security.

(Note: The United States Naval Observatory maintains a list of NTP servers available to the public at their website **http://tycho.usno.navy.mil/ntp.html**. According to established "protocol", prior coordination should be made with an administrator of an Internet time sever before configuring your time server to use it for time synchronization.)

Network-Based Intrusion Detection Systems

The GIAC network utilizes three Dell Workstations with the RedHat LINUX Operating System version 8.0, and the latest version of the open-source

---

9 "Internet Gateway Products"
http://www.trendmicro.com/en/products/gateway/overview.htm

freeware Snort (Snort version 1.9.0 as of this writing) as network-based intrusion detection systems.

Internal Mail Server

The internal mail server provides mail service to the GIAC network, retrieving mail from the external mail server and forwarding mail to the external mail server. The internal mail server uses a Solaris 9 Operating System with the latest version of Sendmail (Sendmail 8.12.7 as of this writing) as its mail server. TrendMicro InterScan VirusWall is used to scan for infected email. The Solaris 9 Operating System has its own integrated host based firewall, SunScreen 3.2 Firewall.

Internal DNS Server

The internal DNS server provides hostname-to-ip address resolution for GIAC resources on the GIACE Internal LAN and Secure LAN. The internal DNS server is configured to forward queries that it cannot resolve to external name server. As a security measure, DNS zone transfers between the internal and external DNS servers are not allowed.

Log Server

The log server provides a central location for all GIAC servers and hosts to forward their system log information. The log server uses an Open BSD 3.1 operating system with all unnecessary services turned off.

Security Administration Terminal

The security administration terminal provides a location for the GIAC network administrators to manage the network via Secure Shell (SSH) connection. The security administration terminal also uses an Open BSD 3.1 operating system with all unnecessary services turned off.

Database Server

The GIAC database server runs Oracle 9i Database software on a Sun Fire V480 server with the Solaris 9 Operating System which includes a SunScreen 3.2 Firewall for host-based protection. GIACE suppliers and partners have accounts on the database to add and retrieve data as part of normal business operations, via VPN tunnel. A backup is made of the database each night.

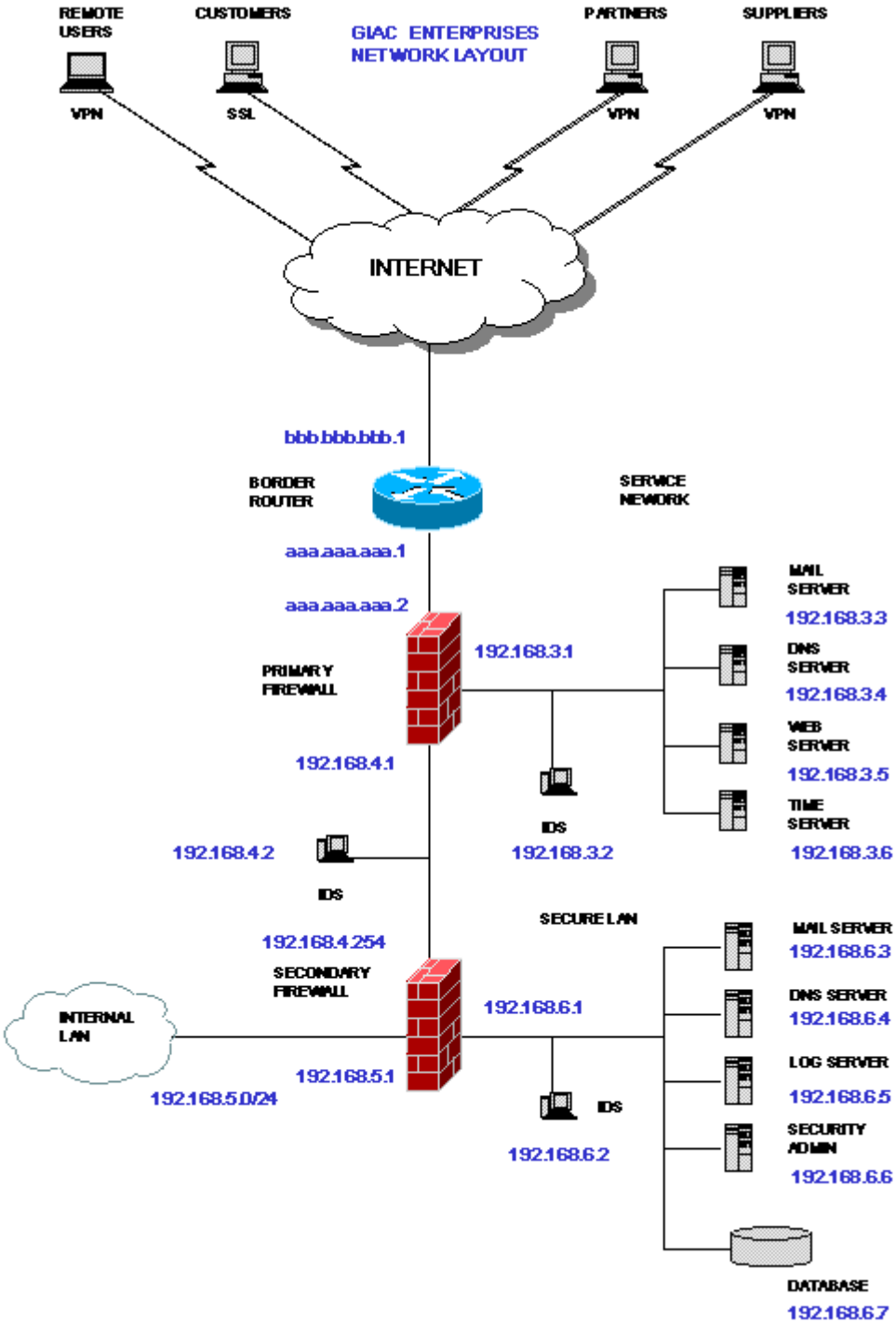


Figure 1 - GIAC Enterprises Network

Assignment 2 - Security Policies: Router Security Policy

2.1 OVERVIEW

The GIAC Enterprises border router serves the dual purposes of routing traffic to and from the Internet and also providing first-line of defense for the network for incoming traffic and last-line of defense for outbound traffic from inside the GIACE network. Using extended router access lists, the border router filters traffic coming to and leaving the GIACE network using port number, source IP address, destination IP address, and type of traffic as parameters. This provides a layer of security and relieves the internal network from handling unnecessary traffic.

By default, out-of-the-box, routers normally allow everything and firewalls block everything. Access Control Lists are used to specifically define what the router will allow and block. Commands in Cisco Router Access Control Lists are executed starting at the top of the list, with each command being processed until a match is found. After a match is found the remaining commands in the list are ignored. As added security measure, Cisco has designed their routers so there is an implicit unseen "deny all" command automatically placed as the last command in all Cisco Access Control Lists which denies access to any traffic that is not matched by any of the previous commands in the list. However an actual "deny all" command should still be entered as the last command in the list so that any rejected traffic can be logged, since the implicit "deny all" command does not cause anything to be logged.

Use of extended access control lists allows a finer granularity of control over the traffic than standard access control lists. The command syntax formats for the Cisco access-list command for router extended access control lists are[10]:

IP

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

10 "Configuring IP Access Lists"
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

ICMP

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

TCP

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

UDP

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

2.2 ROUTER SECURITY POLICY

The "NSA/SNAC Router Security Configuration Guide" at **http://www.nsa.gov/snac/index.html,** and the white paper Improving Security on Cisco Routers at **http://www.remainsecure.com/whitepapers/routers/aclcisco.htm** were used as references for the router policy.

General Router Configuration and Hardening

! To set the router host name

hostname giac-r1

! The normal Cisco encryption for the secret password (Encryption Method 7) is reversible and susceptible to attack. To set the enable password using the stronger Message Digest 5 (MD5) encryption algorithm for the secret password

enable secret 5 <enable_password>

! To encrypt the password stored in the configuration file

service password encryption

! Cisco IOS offers multiple management connection modes. To strengthen security the console port will be the only port used for management of the GIAC border router. To require local login to the router:

line console 0
transport input none[11]

! To create a banner which will be shown to anyone connecting to the router[12].
! It is important that unauthorized users be informed that they are not permitted
! access, in case legal action is taken. This is the electronic equivalent of a "No
! Trespassing" sign.

banner login ^
This system is the property of GIAC Enterprises.
Only GIAC Enterprises employees may access this system.
Disconnect IMMEDIATELY if you are not an authorized user!
Unauthorized use will be MONITORED, RECORDED and PROSECUTED!
^

! To disable proxy arp responses

no ip proxy-arp

! To disable Cisco Discovery Protocol

no cdp run

! To disable unnecessary services

no snmp server
no service finger
no ip http server

! To prevent mapping of the GIACE network using ICMP Host Unreachable messages

no ip unreacheables

---

11 "Router Security Configuration Guide"
http://www.nsa.gov/snac/index.html
12 "Essential IOS Features Every ISP Should Consider"
http://www.grift.com/

! To deter spoofing of internal network addresses:

no ip source-route

! To prevent the router from participating in DDOS attacks

no ip directed-broadcast
no ip redirects

! To disable standard TCP network services of echo, chargen, etc… that use TCP ports with numbers less that 23, which can be used for DOS attacks

no service tcp-small-servers

! To disable standard TCP network services of echo, chargen, etc…that use UDP ports less than 23, which can be used for DOS attacks

no service udp small servers

! To setup and start logging system message log severity 7 messages and below to the GIAC syslog server:

logging buffered 10000
logging trap debugging
logging aaa.aaa.aaa.10
set logging severity 7

! To specify the time server IP address

ntp source Ethernet0/0
ntp server aaa.aaa.aaa.6

! To enable time stamping of log entries

service timestamps debug datetime localtime show timezone msec
service timestamps log datetime localtime show timezone msec

! To turn on TCP Intercept mode in order to defend against TCP SYN-Flooding:

ip tcp intercept list 101
ip tcp intercept mode intercept

Router Ingress Filtering – External Interface Access Control List

Cisco 2600 Router Access Control List 101 for Inbound Traffic

! To remove the extended Cisco Access Control List number 101 if it already exists

no access-list extended 101

! The commands below create and configure the Cisco 2600 Router Access Control List 101 for inbound network traffic from the Internet Service Provider (ISP) via the router's serial interface (serial 0).

interface serial 0

! To create extended access control list 101

ip access-list extended 101

! Since some applications require the use of "packet too big" messages,
! those messages will be allowed

access-list 101 permit icmp any any packet-too-big

! To filter in-bound traffic from sources with private IP addresses and the loopback address (127.0.0.0)[13]

access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.0.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any

! To deny access to inbound traffic from sources using Internet Assigned Numbers Authority (IANA) Reserved IP Addresses

access-list 101 deny ip 1.0.0.0 0.255.255.255 any
access-list 101 deny ip 2.0.0.0 0.255.255.255 any
access-list 101 deny ip 5.0.0.0 0.255.255.255 any
access-list 101 deny ip 7.0.0.0 0.255.255.255 any
access-list 101 deny ip 23.0.0.0 0.255.255.255 any
access-list 101 deny ip 27.0.0.0 0.255.255.255 any
access-list 101 deny ip 31.0.0.0 0.255.255.255 any
access-list 101 deny ip 36.0.0.0 0.255.255.255 any
access-list 101 deny ip 37.0.0.0 0.255.255.255 any
access-list 101 deny ip 39.0.0.0 0.255.255.255 any

---

13 "Cisco Router Configuration Options"
http://www.uniforum.chi.il.us/slides/ddos/sld019.htm

```
access-list 101 deny ip 41.0.0.0 0.255.255.255 any
access-list 101 deny ip 42.0.0.0 0.255.255.255 any
access-list 101 deny ip 58.0.0.0 0.255.255.255 any
access-list 101 deny ip 59.0.0.0 0.255.255.255 any
access-list 101 deny ip 60.0.0.0 0.255.255.255 any
access-list 101 deny ip 70.0.0.0 0.255.255.255 any
access-list 101 deny ip 71.0.0.0 0.255.255.255 any
access-list 101 deny ip 72.0.0.0 0.255.255.255 any
access-list 101 deny ip 73.0.0.0 0.255.255.255 any
access-list 101 deny ip 74.0.0.0 0.255.255.255 any
access-list 101 deny ip 75.0.0.0 0.255.255.255 any
access-list 101 deny ip 76.0.0.0 0.255.255.255 any
access-list 101 deny ip 77.0.0.0 0.255.255.255 any
access-list 101 deny ip 78.0.0.0 0.255.255.255 any
access-list 101 deny ip 79.0.0.0 0.255.255.255 any
access-list 101 deny ip 83.0.0.0 0.255.255.255 any
access-list 101 deny ip 84.0.0.0 0.255.255.255 any
access-list 101 deny ip 85.0.0.0 0.255.255.255 any
access-list 101 deny ip 86.0.0.0 0.255.255.255 any
access-list 101 deny ip 87.0.0.0 0.255.255.255 any
access-list 101 deny ip 88.0.0.0 0.255.255.255 any
access-list 101 deny ip 89.0.0.0 0.255.255.255 any
access-list 101 deny ip 90.0.0.0 0.255.255.255 any
access-list 101 deny ip 91.0.0.0 0.255.255.255 any
access-list 101 deny ip 92.0.0.0 0.255.255.255 any
access-list 101 deny ip 93.0.0.0 0.255.255.255 any
access-list 101 deny ip 94.0.0.0 0.255.255.255 any
access-list 101 deny ip 95.0.0.0 0.255.255.255 any
access-list 101 deny ip 96.0.0.0 0.255.255.255 any
access-list 101 deny ip 97.0.0.0 0.255.255.255 any
access-list 101 deny ip 98.0.0.0 0.255.255.255 any
access-list 101 deny ip 99.0.0.0 0.255.255.255 any
access-list 101 deny ip 100.0.0.0 0.255.255.255 any
access-list 101 deny ip 101.0.0.0 0.255.255.255 any
access-list 101 deny ip 102.0.0.0 0.255.255.255 any
access-list 101 deny ip 103.0.0.0 0.255.255.255 any
access-list 101 deny ip 104.0.0.0 0.255.255.255 any
access-list 101 deny ip 105.0.0.0 0.255.255.255 any
access-list 101 deny ip 106.0.0.0 0.255.255.255 any
access-list 101 deny ip 107.0.0.0 0.255.255.255 any
access-list 101 deny ip 108.0.0.0 0.255.255.255 any
access-list 101 deny ip 109.0.0.0 0.255.255.255 any
access-list 101 deny ip 110.0.0.0 0.255.255.255 any
access-list 101 deny ip 111.0.0.0 0.255.255.255 any
access-list 101 deny ip 112.0.0.0 0.255.255.255 any
access-list 101 deny ip 113.0.0.0 0.255.255.255 any
```

access-list 101 deny ip 114.0.0.0 0.255.255.255 any
access-list 101 deny ip 115.0.0.0 0.255.255.255 any
access-list 101 deny ip 116.0.0.0 0.255.255.255 any
access-list 101 deny ip 117.0.0.0 0.255.255.255 any
access-list 101 deny ip 118.0.0.0 0.255.255.255 any
access-list 101 deny ip 119.0.0.0 0.255.255.255 any
access-list 101 deny ip 120.0.0.0 0.255.255.255 any
access-list 101 deny ip 121.0.0.0 0.255.255.255 any
access-list 101 deny ip 122.0.0.0 0.255.255.255 any
access-list 101 deny ip 123.0.0.0 0.255.255.255 any
access-list 101 deny ip 124.0.0.0 0.255.255.255 any
access-list 101 deny ip 125.0.0.0 0.255.255.255 any
access-list 101 deny ip 126.0.0.0 0.255.255.255 any

! To deny in-bound traffic with source IP addresses of the GIACE internal network:

access-list 101 deny ip aaa.aaa.aaa.0 0.0.0.255 any

! To permit access to the GIACE web server from the Internet

access-list 101 permit tcp any host aaa.aaa.aaa.5 eq 80

! To permit access to the GIACE external mail server from the Internet

access-list 101 permit tcp any host aaa.aaa.aaa.3 eq 25

! To permit access to the GIACE DNS server from the Internet:

access-list 101 permit udp any host aaa.aaa.aaa.4 eq 53

! To permit DNZ zone transfers between the GIACE DNS server and the DNS server (IP address fff.fff.fff.1) of GIACE's Internet Service Provider

access-list 101 tcp host fff.fff.fff.1 host aaa.aaa.aaa.4 eq 53

! To permit the GIACE Time Server to retrieve time information from a trusted Internet Stratum Time Server (IP address ggg.ggg.ggg.1)

access-list 101 udp host ggg.ggg.ggg.1 host aaa.aaa.aaa.6 eq 123

! To allow IPSec VPN traffic from GIACE remote users (ccc.ccc.ccc.0/24), partner (ddd.ddd.ddd.0/24) and supplier (eee.eee.eee.0/24)

access-list 101 permit esp ccc.ccc.ccc.0 255.255.255.255 host aaa.aaa.aaa.12 eq 500

access-list 101 permit esp ddd.ddd.ddd.0 255.255.255.255 host aaa.aaa.aaa.12 eq 500

access-list 101 permit esp eee.eee.eee.0 255.255.255.255 host aaa.aaa.aaa.12 eq 500

access-list 101 permit udp ccc.ccc.ccc.0 255.255.255.255 host aaa.aaa.aaa.12 eq isakmp

access-list 101 permit udp ddd.ddd.ddd.0 255.255.255.255 host aaa.aaa.aaa.12 eq isakmp

access-list 101 permit udp eee.eee.eee.0 255.255.255.255 host aaa.aaa.aaa.12 eq isakmp

! To deny access to any other traffic not specifically listed earlier in the access list and have it logged

access-list 101 deny ip any any log

! To apply the access list to the interface access group

interface s0
ip access-group 101 in

Router Egress Filtering – Internal Interface Access Control List

! The commands below create and configure the Cisco 2600 Router Access Control List 102 for outbound network traffic from the GIAC internal network to the Internet Service Provider (ISP) via the router's Ethernet interface (ethernet 0).

! To remove the extended Cisco Access Control List number 102 if it already exists

no access-list extended 102

Cisco 2600 Router Access Control List 102 for Outbound Network Traffic

ip access-list extended 102

! To allow IP access from any internal hosts to the Internet

access-list 102 permit ip aaa.aaa.aaa.0 0.0.0.255 any

! To allow internal applications to send "packet-too-big" messages to Internet hosts

access-list 102 permit icmp aaa.aaa.aaa.0 0.0.0.255 packet-too-big

! To deny access to the Internet from traffic with a source IP address not in the GIAC corporate network – in order to prevent spoofing of IP addresses inside the GIAC network[14] and to block any traffic not specifically permitted by rule

access-list 102 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 log

! To activate the outbound access list on the Ethernet interface[15]

interface e0
ip access-group 102 out

! To terminate session

exit

Assignment 2 - Security Policies:
Primary Firewall Security Policy and Virtual Private Network Configuration

---

2.3 Primary Firewall SECURITY POLICY

GIACE uses a Cisco PIX 515E Firewall in it screened subnet firewall design to provide defense in depth and also more granular control over traffic than the router can provide.

An example PIX configuration from the Cisco web site at **http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm** was used as the template for the configuration of the GIAC Cisco PIX 5151E Firewall.[16] The command line interfaces of the Cisco PIX Firewall and

---

14 "Info on configuring a Cisco access list to filter IP"
http://www.mtiweb.com/isp/ciscoacc.html http://www.mtiweb.com/isp/ciscoacc.html
15 "Info on configuring a Cisco access list to filter IP"
http://www.mtiweb.com/isp/ciscoacc.html http://www.mtiweb.com/isp/ciscoacc.html
16 "Basic Firewall Configuration"
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm

Cisco Router Internetwork Operating System (IOS) are identical in both structure and appearance.[17]

! To set the host name for the GIAC primary firewall

hostname giac-fw1

! To set the domain name

domain-name giacenterprises.com

! To configure an encrypted password for access to command mode

enable password enable_password encrypted

! To assign IP addresses to the three PIX interfaces used

ipaddress outside aaa.aaa.aaa.2
ipaddress svc 192.168.3.1
ipaddress inside 192.168.4.1

! To set the speed for the PIX interfaces

interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto

! To assign names and security levels to the three PIX 515E interfaces

nameif ethernet0 outside security 0
nameif ethernet1 svc security 50
nameif ethernet2 inside security 100

! To ensure the Cisco Floodguard protection is turned on (it is on by default)

floodguard enable

! To set the logging host and turn on firewall syslog message logging at Level 7 (Debugging) - logging is off by default):

logging host 192.168.6.5
logging on
logging trap 7

! To set default routes

17 Cisco Security Bible, Rajesh Kumar Sharma, Hungry Minds, Inc, New York, NY, 2002, p. 292

route outside 0.0.0.0 0.0.0.0 aaa.aaa.aaa.2
route svc 0.0.0.0 0.0.0.0 192.68.3.1
route inside 0.0.0.0 0.0.0.0 192.68.4.1

! To set the maximum transmission unit (MTU) to 1500 octets for each interface used

mtu outside 1500
mtu svc 1500
mtu inside 1500

! To configure fixup protocol for needed protocols

fixup protocol smtp 25
fixup protocol domain 53
fixup protocol http 80
fixup protocol ntp 123
fixup protocol ssl 443
fixup protocol sqlnet 1521

! To disable protocol fixup for protocols not used in the GIAC network

no fixup protocol ftp 21
no fixup protocol telnet 23
no fixup protocol rsh 514
no fixup protocol h323 1720
no fixup protocol sip 5060

To configure the "inbound" access list for the external interface

! Rule 1 to allow DNS lookup info to reach the external DNS server

access-list inbound permit udp any host 192.168.3.4 eq domain

! Rule 2 to allow access to the GIAC web server via HTTP

access-list inbound permit tcp any host 192.68.3.5 eq www

! Rule 3 to allow access to the GIAC web server via SSL

access-list inbound permit tcp any host 192.68.3.5 eq 443

! Rule 4 to allow SMTP traffic to reach the external mail server

access-list inbound permit tcp any host 192.68.3.3 eq smtp

! Rule 5 to allow the border router to send syslog data to the log server

access-list inbound permit udp host aaa.aaa.aaa.1 aaa.aaa.aaa.10 eq 514

! Rule 6 to deny and log everything else

access-list inbound deny tcp any any log

To configure the "svcout" access list for the Service Network interface

! Rule 1 to allow the web server access using HTTP

access-list svcout permit tcp host 192.68.3.5 any eq www

! Rule 2 to allow the web server access using SSL

access-list svcout permit tcp host 192.68.3.5 any eq 443

! Rule 3 to allow the web server access to the database server using SQLNet

access-list svcout permit tcp host 192.68.3.5 192.168.6.7 255.255.255 eq 1521

! Rule 4 to allow the mail server access using SMTP

access-list svcout permit tcp host 192.68.3.3 any eq smtp

! Rule 5 to allow the External DNS Server access to the internal DNS server

access-list svcout udp host 192.68.3.4 host 192.68.6.4 eq domain

! Rule 6 to allow the external DNS Server access to the GIACE ISP DNS Server (IP Address fff.fff.fff.1) using domain

access-list svcout permit udp host 192.68.3.4 fff.fff.fff.1 255.255.255.255 eq domain

! Rule 7 to allow the external DNS server all other access using domain

access-list svcout permit udp host 192.68.3.4 any eq domain log

! Rule 8 to allow the Service Network hosts to send logs to the GIACE log server on the Secure LAN

access-list svcout permit udp 192.68.3.0 255.255.255.0 192.168.6.5 255.255.255.255 eq 514

! Rule 9 to allow Secure Shell (SSH) communication between Service Network hosts and Internal LAN hosts

access-list svcout permit udp 192.68.3.0 255.255.255.0 192.168.5.0 255.255.255.0 eq 22

! Rule 10 to allow Secure Shell (SSH) communication between the Service Network and the Secure LAN

access-list svcout permit udp 192.68.3.0 255.255.255.0 192.168.6.0 255.255.255.0 eq 22

! Rule 11 to deny everything else

access-list svcout deny tcp any any

To configure the outbound access list for the inside interface

! Rule 1 to allow mail transfer between the internal and external mail servers

access-list outbound permit tcp host 192.168.6.3 192.168.3.3 eq 25

! Rule 2 to allow the Security Administration workstation access to the GIACE network via Secure Shell (port 22)

access-list outbound permit tcp host 192.168.6.6 any eq 22

! Rule 3 to allow everyone on the Internal Network access to the Internet via HTTP

access-list outbound permit tcp host 192.168.3.5 any eq www

! Rule 4 to allow everyone on the Internal Network access to the Internet via HTTPS

access-list outbound permit tcp host 192.168.3.6 any eq SSL

! Rule 5 Allow the database server to communicate with the web server

access-list outbound permit tcp host 192.168.6.7 192.168.3.5 eq 1521

! Rule 6 to allow Secure Shell (SSH) communication between the Internal LAN and the Service Network

access-list outbound permit tcp 192.68.5.0 255.255.255.0 192.168.6.0 255.255.255.0 eq 22

! Rule 7 to deny everything else

access-list svcout deny tcp any any log

! To bind the inbound Access Control List to the outside interface

access-group inbound in interface outside

! To bind the outbound Access Control List to the intranet interface

access-group outbound in interface intranet

! To bind the svcout Access Control List to the svc interface

access-group svcout in interface svc

! To set IP addresses to be used for Network Address Translation (NAT)

global (outside) 1 aaa.aaa.aaa.64-aaa.aaa.aaa.254
nat (inside) 1 0.0.0.0 0.0.0.0
nat (svcout) 1 0.0.0.0 0.0.0.0

! To assign NAT'ed hosts public IP address to enable external systems to communicate with them

static (svcout,outside) aaa.aaa.aaa.3 192.168.3.3 netmask 255.255.255.255 0 0

static (svcout,outside) aaa.aaa.aaa.4 192.168.3.4 netmask 255.255.255.255 0 0

static (svcout,outside) aaa.aaa.aaa.5 192.168.3.5 netmask 255.255.255.255 0 0

static (svcout,outside) aaa.aaa.aaa.6 192.168.3.6 netmask 255.255.255.255 0 0

static (svcout,outside) aaa.aaa.aaa.10 192.168.6.5 netmask 255.255.255.255 0 0

static (inside,outside) aaa.aaa.aaa.12 192.168.6.7 netmask 255.255.255.255 0 0

! To specify a static route

route outside 0.0.0.0 0.0.0.0 aaa.aaa.aaa.2 1

Assignment 2 - Security Policies: Virtual Private Network Security Policy

---

2.4 VPN SECURITY POLICY

The primary firewall is also used as the VPN Gateway for GIACE. Cisco VPN is based upon IPSec (Internet Protocol Security). GIAC uses host-to-gateway VPN connections for remote users (mobile users and telecommuters) and gateway-to-gateway VPN connections for extranet connections to partners, and suppliers. The Cisco PIX 5151E Firewall serves as the VPN endpoint for the Cisco Secure VPN 3000 Client software installed on the remote users' hosts and the VPN client software of the partners and suppliers hosts. The partners, suppliers, and remote users are able to use any IPSec-compliant VPN client to communicate with the GIAC network. GIAC remote users have Cisco Secure VPN Client v1.1 software installed on their hosts. The IPSec Encapsulating Security Payload (ESP) protocol is mandated to insure the VPN traffic is encrypted while it is on the Internet.

GIACE uses Internet VPNs to encrypt communication with GIAC remote employees who have Cisco Secure VPN Client 3000 software installed on their systems. GIACE uses extranet VPNs with its partners and suppliers who can use any VPN software as long as it is conforms to IPSec open VPN standards. In this regard the only requirement that GIACE has of its partners and suppliers is that connections to its network have be via VPN. Pre-shared symmetric encryption/decryption keys are used.

GIAC IKE Policy for the 515E PIX Firewall[18]

Parameter	GIAC PIX VPN Server	Client
Encryption algorithm	3des	3des
Message integrity algorithm	sha	sha
Peer Authentication method	pre-shared key	pre-shared key
Key exchange parameters	1024-bit D-H Group 2	1024-bit D-H Group 2
IKE SA lifetime	86,400	86,400
Peer IP Address	192.68.2.2	(various)

Table 3 - GIAC IKE Policy for the Cisco PIX 515E Firewall VPN

! Virtual Private Network Configuration of the PIX 515E Firewall
! This configuration is for point-to-point VPN connections using IPSec with pre-shared cryptographic keys. (Note: An example from the book "Cisco Secure PIX Firewalls" was used as a guide for the firewall VPN configuration.[19])

! To specify that traffic from the GIAC Corporate Network to GIAC remote users be encrypted

access-list VPN1 permit 192.68.0.0 255.255.0.0 ccc.ccc.ccc.0 255.255.0.0 log

! To specify that traffic from the GIAC Corporate Network to GIAC partners be encrypted

access-list VPN2 permit 192.68.0.0 255.255.0.0 ddd.ddd.ddd.0 255.255.0.0 log

! To specify that traffic from the GIAC Corporate Network to GIAC suppliers be encrypted

access-list VPN3 permit 192.68.0.0 255.255.0.0 eee.eee.eee.0 255.255.0.0 log

! To create an access list to be used by the nat 0 command below so that NAT is not performed on IPSec traffic

access-list VPN4 permit 192.68.0.0 255.255.0.0 ccc.ccc.ccc.0 255.255.0.0 log

access-list VPN4 permit 192.68.0.0 255.255.0.0 ddd.ddd.ddd.0 255.255.0.0 log

18 Cisco Secure PIX Firewalls, edited by David W. Chapman and Andy Fox, Cisco Press, Indianapolis, IN, Mar 2002, p. 203
19 Cisco Secure PIX Firewalls, Edited by David W. Chapman Jr. and Andy Fox, Cisco Press, March 2002, pages 228-229

access-list VPN4 permit 192.68.0.0 255.255.0.0 eee.eee.eee.0 255.255.0.0 log

! To configure a global address pool

global (outside) 1 aaa.aaa.aaa.64-aaa.aaa.aaa.254 netmask 255.255.255.0

! To disable Network Address Translation inside the VPN tunnel

nat (inside) 0 access-list VPN4
nat (inside) 1 192.68.0.0 255.255.0.0 0 0

! To permit IPSec traffic to bypass access list rules

sysopt connection permit-ipsec

crypto ipsec transform-set giac-fw1 esp-3des

! To use ISAKMP to establish Phase 1 Security Association to the GIAC remote users

crypto map VPN 10 ipsec-isakmp
crypto map VPN 10 match address VPN1
crypto map VPN 10 set peer ccc.ccc.ccc.0 255.255.255.0
crypto map VPN 10 set transform-set giac-fw1

! To use ISAKMP to establish Phase 1 Security Association to the GIAC partners

crypto map VPN 20 ipsec-isakmp
crypto map VPN 20 match address VPN2
crypto map VPN 20 set peer ddd.ddd.ddd.0 255.255.255.0
crypto map VPN 20 set transform-set giac-fw1

! To use ISAKMP to establish Phase 1 Security Association to the GIAC suppliers

crypto map VPN 30 ipsec-isakmp
crypto map VPN 30 match address VPN3
crypto map VPN 30 set peer eee.eee.eee.0 255.255.255.0
crypto map VPN 30 set transform-set giac-fw1

! To bind the crypto map to operate on the outside interface

crypto map VPN interface outside

! To bind IKE to operate on the outside interface

isakmp enable outside

! To set pre-shared keys for peers (GIAC remote users, partners and suppliers)

isakmp key 16543789 address ccc.ccc.ccc.0 255.255.255.0
isakmp key 22309867 address ddd.ddd.ddd.0 255.255.0.0
isakmp key 37401234 address eee.eee.eee.0 255.255.0.0

! To use IP addresses to identify crypto peers

isakmp identity address

! To set ISAKMP policy parameters

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy group 2
isakmp policy lifetime 86400

Assignment 2 - Security Policies: VPN Tutorial

2.3 Host-Gateway VPN Tutorial

This tutorial provides a step-by-step procedure for setting up the Cisco Secure VPN Client Version 1.1 for a host-to-gateway VPN connection. This procedure is used to configure the laptop computers used by GIACE's remote employees to connect remotely to the GIAC network PIX Firewall via encrypted VPN connection. The setup steps for this tutorial were excerpted from an article "Configuring the Cisco Secure VPN Client Version 1.1", at the Cisco web site, **http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/config/bascInt.htm - 20537.**

Step 1 - To start the Cisco Secure VPN Client Version 1.1 graphical user interface, click the **Start** button then select **Programs** from the Start menu then **Cisco Secure VPN Client** then **Security Policy Editor**.

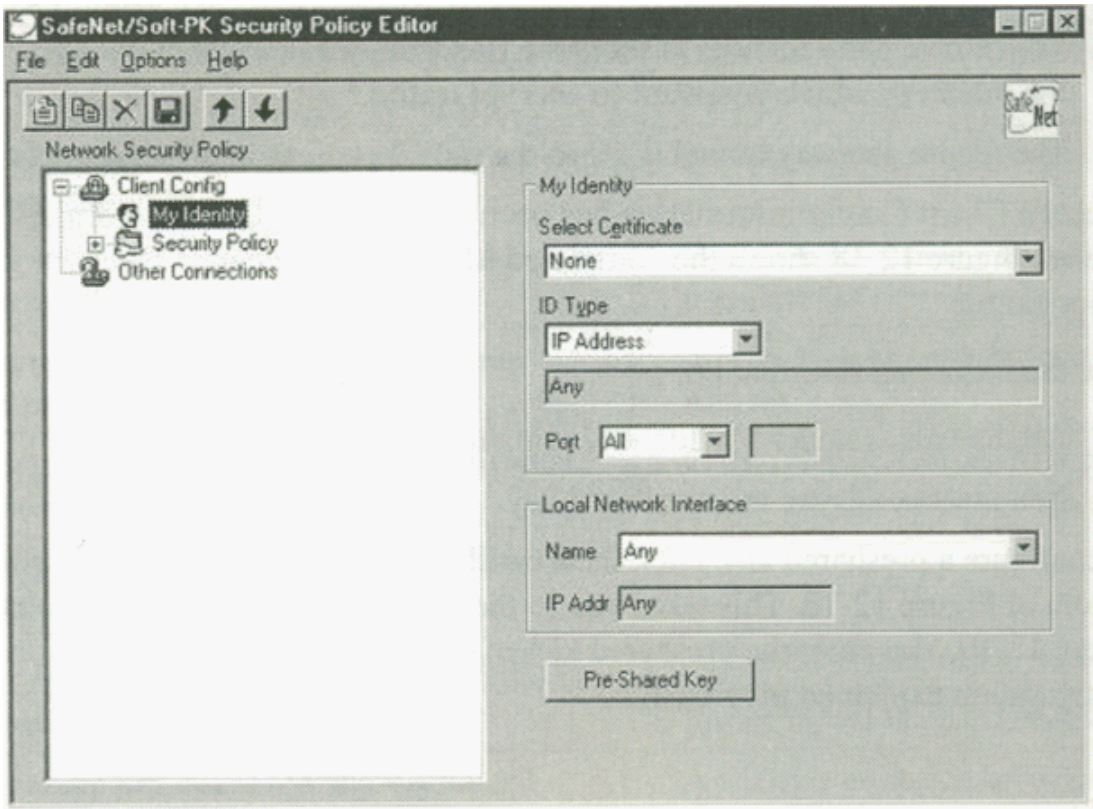


Figure 2 – Cisco Secure VPN 1.1 Client Security Policy Editor

Step 2 - Click **Options** then **Secure** then **Specified Connections**.

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

Step 4 - Click **File** then **New Connection**. Type in a name for the new connection, **GIACE**.

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

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

- For *ID Type* click **IP address**.
- Enter the IP address of the internal host within the PIX Firewall unit's internal network to which the VPN client will have access, the database server, IP address **aaa.aaa.aaa.12**.
- Click **Connect using Secure Gateway Tunnel**.

- For *ID Type* Click **IP address**.

- Enter the IP address of the outside interface of the PIX Firewall, **aaa.aaa.aaa.2.**

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

- Select Certificate Click **None**.

- For *ID Type* Click **IP address**.

- For *Port* Click **All**.

- For *Local Network Interface* Click **Any**.

- Click **Pre-Shared Key**. When the Pre-Shared Key dialog box appears, click **Enter Key** to make the key field editable. Enter **16543789** (the pre-shared key of the GIACE PIX Firewall VPN configuration) and then click **OK**.

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

- Under **Select Phase 1 Negotiation Mode** click **Main Mode**.

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

Leave any other values as they were in the panel.

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

- For *Authentication Method* Click **Pre-shared Key** (to match the GIACE PIX Firewall setting).

- For *Encryption Algorithm* click **Triple DES** (to match the GIACE PIX Firewall setting).

- For *Hash Algorithm* click **SHA-1** (to match the GIACE PIX Firewall setting).

- For *Security Association Life* type in **86,400** (to match the GIACE PIX Firewall setting).

- For Key Group click **Diffie-Hellman Group 2** (to match the GIACE PIX Firewall setting; GIACE security policy requires the use of Diffie-Hellman Group 2 (1024-bit) keys because they provide higher security that Diffie-Hellman Group 1 (512-bit) keys).

Step 10 - Click **Security Policy** then **Key Exchange (Phase 2)** then **Proposal 1** and select the following from the choices in the panel:

- Select the **Encapsulation Protocol (ESP)** check box.
- For *Encryption Algorithm* click **Triple DES**.
- For *Hash Algorithm* click **SHA-1**.
- For *Encapsulation* click **Tunnel**.
- For *Security Association Life* click **Unspecified** (directs the Client to use the SA life specified by the GIACE PIX Firewall).

Step 11 - Click **File** then **Save Changes**.

The VPN client is now configured to open VPN connections to the GIACE Cisco PIX Firewall over the Internet.

Assignment 2 - Security Policies: VPN Tutorial
Tips, Tricks, & Potential Problems

· The **sysopt connection permit-ipsec** command configured the Cisco PIX 515E Firewall to permit all IPSec traffic to bypass access list rules. This means that if someone is able to subvert the security of the VPN the firewall will allow them access. Therefore, maintaining the security of VPN access is of paramount importance. GIACE requires users connecting to the GIACE network via VPN to have a VPN key and network password in order to obtain access.

2.5 Secondary Firewall

GIACE uses an Open Berkley Software Distribution (BSD) Operating System 3.1 with IPFilter firewall software (Open BSD + IPF 3.1) for its secondary (internal) firewall. Open BSD is designed with security as the primary consideration and is considered to be a very "hardened" operating system as is. The secondary

firewall provides an additional layer of defense from network attack from the Internet and also provides access control to and from the Internal LAN and Secure LAN. The IPFilter firewall can be configured to identify and filter specific traffic patterns that perhaps the Cisco PIX firewall could not segregate. Unlike the Cisco PIX Firewalls (and most other firewalls) IPFilter scans all the rules of its rulebase before making a decision on allowing or disallowing traffic.

A white paper "IP Filter Based Firewalls HOWTO", written by Brendan Conoboy and Erik Fichtner (**http://www.obfuscation.org/ipf/ipf-howto.txt**) was used a reference for the secondary firewall configuration.

2.6 Host Hardening

The focus on security is from the inside (desktop computer) out (border router). The host operating system and applications are the last line of defense in the defense in depth strategy. The following measures were taken to "harden" hosts in order to lessen/remove vulnerabilities:

- Unneeded services/ports are turned off.
- Only the remote users hosts are allowed internal modems.
- Remote users and teleworkers have McAfee host-based anti-virus protection and host-based ZoneAlarm personal firewalls on their systems.
- Each system has a strong operating system, account, and application passwords set.
- All company business email is encrypted.
- Secure Shell Version 2 (SSHv2) is installed on systems to replace Telnet.
- All systems not acting as mail servers have Sendmail not running in daemon mode.
- All systems not acting as DNS servers have BIND removed.
- System patches are routinely monitored and kept current.
- All systems have warning banners stating that use is restricted to authorized personnel only.

Assignment 3 – Audit Security Infrastructure: Plan the Audit

3.1 Primary Firewall Audit Plan

After obtaining written approval of their audit plan from GIAC management, GIAC network security personnel conducted a technical audit of its primary firewall (Cisco PIX 515E) in order to verify that the firewall is functioning as intended and network traffic flow is in compliance with the GIAC security policy. An additional objective of the firewall audit was to identify any network security problems or weaknesses.

GIAC personnel scheduled the conduct the audit of the GIAC primary firewall (Cisco PIX 5151E) beginning at 1:00 a.m. on a Saturday morning in order to allow approximately forty-eight hours before the start of the next business day to recover from any problems encountered. Occasionally the process of performing a security test on a system will cause the system to crash particularly when denial of service attacks are simulated. GIACE's Internet Service Provider was given notice of the firewall audit and its time period and an announcement that the network would be down for maintenance during that time period was sent to customers, suppliers, partners, and GIACE personnel. A full backup of all GIACE user and system data was scheduled and completed just prior to the start of the firewall audit.

The methodology of the audit was to connect the laptop to several points on the network, to simulate scans (using the Nmap network mapping tool) from the Internet, the service subnet, and the internal network while running the Tcpdump utility on the IDS workstations in order to capture the traffic allowed to pass through the firewall. The tools that GIAC network security personnel used to perform the security audit were downloaded from trusted sources and verified as authentic using MD5 checksums.

It was estimated that a total of twenty-four man-hours would be required to plan, conduct, and evaluate the primary firewall audit. The monetary cost of the audit was the labor cost since no new equipment was needed and the Nmap software was obtained free of cost from the Internet. The labor cost was estimated to be approximately $2,500.

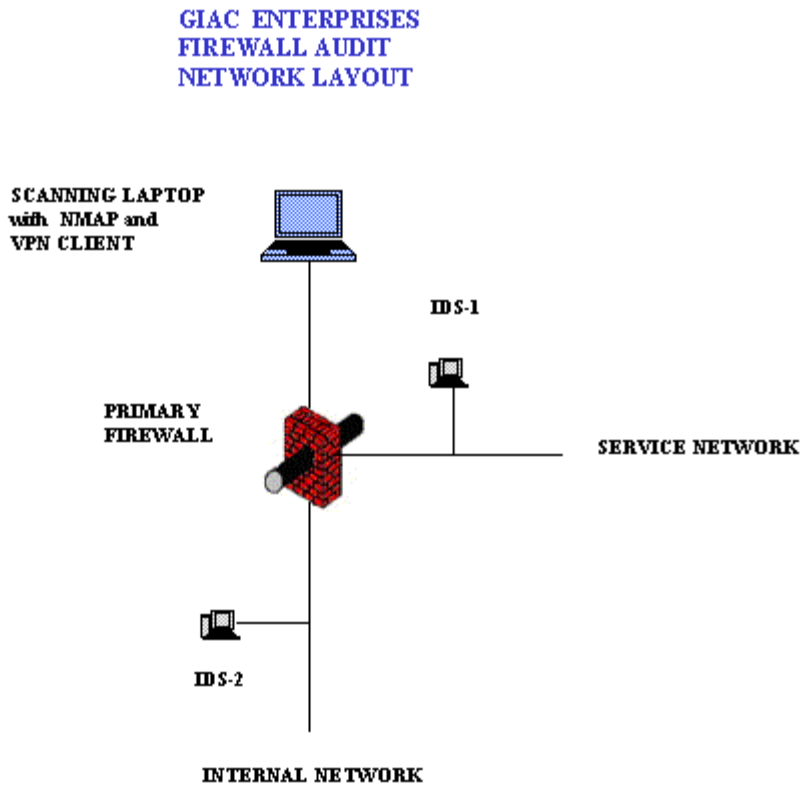


Figure 3 - GIAC Enterprises Test Network

Cisco PIX Firewall Vulnerabilities

GIAC network security personnel conducted a search for information concerning Cisco PIX Firewall vulnerabilities and found the following:

Source of Information:
http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml

Cisco bug ID CSCdu47003
Cisco PIX Firewall SIP Protocol Bugs Let Remote Users Deny Service

Multiple Cisco products contain vulnerabilities in the processing of Session Initiation Protocol (SIP) INVITE messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for SIP and can be repeatedly exploited to produce a denial of service.

Affected Cisco PIX Firewalls: PIX Firewall running software versions with SIP support, beginning with version 5.2(1) and up to, but not including versions 6.2(2), 6.1(4), 6.0(4) and 5.2(9).

Fix: This vulnerability is repaired in Cisco Secure PIX Software versions 5.2.9, 6.0.4, 6.1.4, and 6.2.2 and later.

Source of Information:
http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml

Cisco bug ID CSCdu47003
Cisco PIX Firewall SIP Protocol Bugs Let Remote Users Deny Service

Multiple Cisco products contain vulnerabilities in the processing of Session Initiation Protocol (SIP) INVITE messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for SIP and can be repeatedly exploited to produce a denial of service.

Affected Cisco PIX Firewalls: PIX Firewall running software versions with SIP support, beginning with version 5.2(1) and up to, but not including versions 6.2(2), 6.1(4), 6.0(4) and 5.2(9).

Fix: This vulnerability is repaired in Cisco Secure PIX Software versions 5.2.9, 6.0.4, 6.1.4, and 6.2.2 and later.

Source of Information:
http://www.cisco.com/warp/public/707/SSH-scanning.shtml

Security Advisory: Scanning for SSH Can Cause a Crash

"Vulnerability allows an attacker to send an overly large packet to the SSH daemon, causing the Cisco device to either consume all CPU cycles, or reboot."

Affected Cisco PIX Firewalls: PIX Firewalls supporting SSH are affected.

Fix: Install an applicable fixed software release.

Source of Information:
http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml

Cisco Bug ID CSCdu47003
Cisco Secure PIX Firewall SMTP Filtering Vulnerability

"Vulnerability allows an attacker to by-pass PIX "mailguard" feature, allowing attacker to execute blocked SMTP commands."

Affected Cisco PIX Firewalls: PIX Firewall versions 6.0(1), 5.2(5) and 5.2(4) that provide access to SMTP Mail services are at risk.

Fix: Install the applicable fixed software release.

Source of Information:
http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml

Cisco Bug ID CSCdt92339
Cisco PIX Firewall Authentication Denial of Service Vulnerability

"Vulnerability allows an attacker to consume all PIX AAA authentication resources, causing a denial of service condition by preventing additional users from authenticating and logging in."

Affected Cisco PIX Firewalls: PIX Firewall versions 4.0 up to and including 4.4(8), 5.0(3), 5.1(3), 5.2(2), and 5.3(1) with configurations using AAA authentication are at risk..

Fix: Install the applicable fixed software release.

Assignment 3 – Audit Security Infrastructure: Conduct the Audit

3.2 Primary Firewall Audit Procedures

(Note: Lance Spitzner's excellent white paper "Auditing Your Firewall Setup"[20] was used as a reference for this section of the practical.)

Audit Tools

GIAC network security personnel used a laptop computer with the open source network exploitation tool and security scanner Nmap (Network Mapper) Security Scanner 3.0 (written by "Fyodor", which was downloaded from **http://insecure.org/nmap/**) and NmapWin 1.3.0 (a native Windows-32 front-end GUI for Nmap developed by Jens Vogt), which was downloaded from **http://www.insecure.org/Nmap/Nmap_download.html**, installed to generate test traffic which consisted of port scans. The Nmap tool provided as output reports indicating whether the ports scanned were open, closed, filtered, or unfiltered. The Tcpdump sniffer applications on the Intrusion Detection System workstations were used to log test traffic that was allowed through the primary firewall. This allowed GIAC network security personnel the opportunity to view the packets allowed by the firewall and correlate that information with the firewall access control settings.

20 "Auditing Your Firewall Setup"
http://www.spitzner.net/audit.html

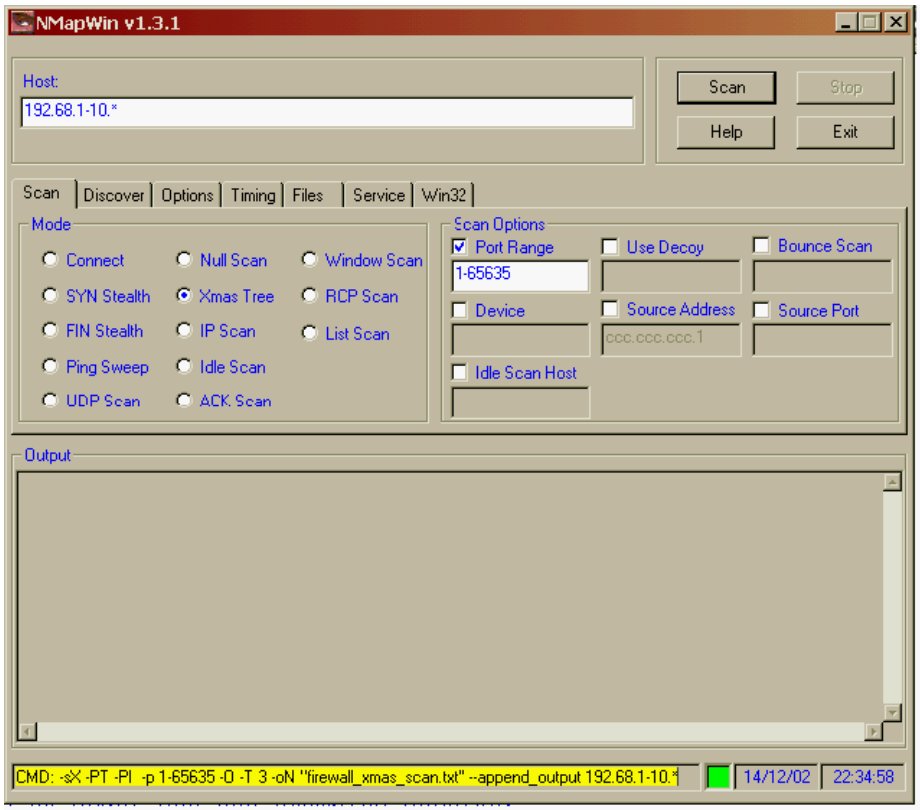


Figure 4 – Nmap Windows v1.3.1 example screen shot

Nmap Options - The "Nmap Network Security Man Page" at **http://www.insecure.org/Nmap/data/Nmap_manpage.html** lists the options that can be used with Nmap):

-oN	Indicates the output file name follows
-O	Nmap attempts to identify operating system
-p	Indicates the port(s)/port ranges to scan
-P0	Do not try to ping hosts before scanning them
-sF	Stealth FIN mode
-sS	TCP SYN scan
-sU	UDP port scan
-sX	Stealth Xmas Tree mode
-T 3	Specifies "Polite" mode which reduces network load

Tcpdump Utility -The Tcpdump version 3.6.1 network monitoring utility was used on the intrusion detection system hosts for the duration of the audit to collect the traffic from the audit computer that was allowed by the primary firewall. Some of the Tcpdump options:

-i <interface_name> : listen to interface interface_name, such as eth0

-n : list numeric addresses and port numbers

-w : write output to file (instead of the standard output which is the default)

The command executed was of the format "**tcpdump –i eth0 host <ip_address> –n -w <text_file_name>**", which provided very very verbose output to the designated text output file without attempting to convert IP addresses to host names[21] . The command executed to read the saved files was of the format "**tcpdump –r <text_file_name>**".

3.2.1 Auditing From the Internet

Ping Firewall

First, the audit laptop (IP address ccc.ccc.ccc.10) was connected to the Internet Service Provider (ISP) interface of the primary firewall and the Ping utility was used to ping the external firewall's external interface:

ping aaa.aaa.aaa.2

Pinging aaa.aaa.aaa.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Ping statistics for aaa.aaa.aaa.2:
Packets: Sent = 4, Received = 0, Lost = 4 <100% packet loss>,

The ping test of the firewall was not successful.

Run Nslookup

In order to verify that the primary firewall does not allow DNS Zone transfers with a request to enumerate all domain records was made[22]:

>nslookup
Default Server ns.example.net

---

21 The SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs course manual 2.5, 2002. 110.
22 The SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs course manuals 2.3, 2002. 202.

>ls –d giacenterprises.com
******* Can't list giacenterprises.com: Query refused

The attempt at a DNS Zone transfer was not successful.

Scan the Firewall External Interface

The audit laptop (IP address ccc.ccc.ccc.10) was connected to the external interface of the primary firewall and an Nmap scan was conducted to determine open ports/services using the following Nmap commands:

TCP SYN Scan

nmap -sS -PO -p 1-1024 -O -T 3 -oN "pixoutsidesyn.txt" aaa.aaa.aaa.2

TCP UDP Scan

nmap -sU -PO -p 1-1521 -O -T 3 -oN "pixoutsideudp.txt" aaa.aaa.aaa.2

Nmap scan results:

Since the Cisco Pix Firewall has its ports in stealth mode, the scan did not reveal any ports listening on the firewall, as expected.

Scan the Service Network From the Internet

Next, an Nmap scan was conducted to determine open ports/services on the Service Network using the following Nmap commands:

TCP SYN Scan

nmap -sS -PO -p 1-1521 -O -T 3 -oN "int-svc-syn.txt" aaa.aaa.aaa.3-6

TCP UDP Scan

nmap -sU -PO -p 1-1024 -O -T 3 -oN "int-svc-udp.txt" aaa.aaa.aaa.3-6

Nmap scan results:

Device	IP Address	Port	Service
Mail Server	aaa.aaa.aaa.3	25/tcp	SMTP
DNS Server	aaa.aaa.aaa.4	53/udp	DNS
Web Server	aaa.aaa.aaa.5	80/tcp	HTTP
Web Server	aaa.aaa.aaa.5	443/tcp	HTTPS

Pertinent Snort Portscan Log Entries on IDS-1:

Feb 25 01:36:36 ccc.ccc.ccc.10 -> aaa.aaa.aaa.3 SYN **S*****
Feb 25 01:36:36 ccc.ccc.ccc.10 -> aaa.aaa.aaa.5 SYN **S*****

Feb 25 01:41:36 ccc.ccc.ccc.10 -> aaa.aaa.aaa.4 UDP

PIX Firewall Inbound Access List Rules Tested:

Rule 1 to allow DNS lookup requests to reach the external DNS server, Rule 2 to allow access to the GIAC web server via HTTP, Rule 3 to allow access to the GIAC web server via SSL, Rule 4 to allow SMTP traffic to reach the external mail server, and Rule 5 to deny everything else, were verified.

Scan the Secure LAN From the Internet

Next, an Nmap scan was conducted to determine open ports/services on the Secure LAN using the following Nmap commands:

TCP SYN Scan

nmap -sS -PO -p 1-1024 -O -T 3 -oN "int-secure-syn.txt" 192.168.6.1-7

TCP UDP Scan

nmap -sU -PO -p 1-1521 -O -T 3 -oN "int-secure-udp.txt" 192.168.6.1-7

Nmap scan results:

No responses received.

Pertinent Snort Portscan Log Entries on IDS-2:

No entries.

PIX Firewall Inbound Access List Rules Tested:

Rule 6 to deny everything else was verified.

3.2.2 Auditing From The Service Network

Next, the audit laptop was connected to the Service Network, temporarily replacing the web server.

Scan the Secure LAN From the Service Network

Nmap scans were conducted, spoofing the web server IP address (192.168.3.5) as the source address, to determine open ports/services on the Secure LAN using the following Nmap commands:

TCP SYN Scan

nmap -sS -PO -p 1-1024 -O –S 192.168.3.5 -T 3 -oN "svc-secure-syn.txt" aaa.aaa.aaa.8-12

TCP UDP Scan

nmap -sU -PO -p 1-1521 -O –S 192.168.3.5 -T 3 -oN " svc-secure-udp.txt" aaa.aaa.aaa.8-12

Nmap scan results:

Device	IP Address	Port	Service
Database Server	aaa.aaa.aaa.7	1521/tcp	SQLNET

Snort Portscan Log Entries on IDS-2:

Feb 25 02:46:36 192.168.3.5 -> aaa.aaa.aaa.12 SYN **S*****
Feb 25 02:46:36 192.168.3.5 -> aaa.aaa.aaa.12 UDP

PIX Firewall svcout Access List Rules Tested:

Rule 3 to allow the web server to access the database server via SQLNET

3.2.3 Auditing From the Internal LAN

Next, the audit laptop was connected to the Internal LAN.

Scan the Service Network From the Internal LAN

Nmap scans were conducted to determine open ports/services on the Service Network using the following Nmap commands, spoofing an unassigned Internal LAN IP address (192.168.5.130):

TCP SYN Scan

nmap -sS -PO -p 1-1024 -O –S 192.168.5.130 -T 3 -oN "internal-svc-syn.txt" aaa.aaa.aaa.3-6

UDP Scan

nmap -sU -PO -p 1-1521 -O –S 192.168.5.130 -T 3 -oN "internal-svc-udp.txt" aaa.aaa.aaa.3-6

Nmap scan results:

Device	IP Address	Port	Service
Mail Server	aaa.aaa.aaa.3	25/tcp	SMTP
Mail Server	aaa.aaa.aaa.3	22/tcp	SSH
DNS Server	aaa.aaa.aaa.4	22/tcp	SSH
DNS Server	aaa.aaa.aaa.4	53/udp	DNS
Web Server	aaa.aaa.aaa.5	22/tcp	SSH
Web Server	aaa.aaa.aaa.5	80/tcp	HTTP
Web Server	aaa.aaa.aaa.5	443/tcp	HTTPS
Web Server	aaa.aaa.aaa.5	1521/tcp	SQLNET
Time Server	aaa.aaa.aaa.6	22/udp	SSH
Time Server	aaa.aaa.aaa.6	123/udp	NTP

Pertinent Snort Portscan Log Entries on IDS-1:

Feb 25 03:16:36 192.168.5.130 -> aaa.aaa.aaa.3 SYN **S*****
Feb 25 03:16:36 192.168.5.130 -> aaa.aaa.aaa.4 SYN **S*****
Feb 25 03:16:36 192.168.5.130 -> aaa.aaa.aaa.5 SYN **S*****
Feb 25 03:16:36 192.168.5.130 -> aaa.aaa.aaa.6 SYN **S*****

Feb 25 03:20:36 192.168.5.130 -> aaa.aaa.aaa.4 UDP
Feb 25 03:21:36 192.168.5.130 -> aaa.aaa.aaa.5 UDP

PIX Firewall outbound Access List Rules Tested:

The outbound access list Rule 6 to allow all hosts on the Internal Network access to any host via HTTP, Rule 4 to allow everyone on the Internal Network access

to any host via HTTPS, and Rule 7 to allow Secure Shell connections from the Internal LAN to the Service Network, were verified.

3.2.4 Auditing From the Secure LAN

Next, the audit laptop was connected to the Secure LAN.

Scan the Service Network From the Secure LAN

Nmap scans were conducted to determine open ports/services on the Service Network using the following Nmap commands, spoofing the database server IP address (192.168.6.7), using the "-S" option of Nmap to specify the source address to use during the scans:

TCP SYN Scan

nmap -sS -PO -p 1-1024 –O -S 192.168.6.7 -T 3 -oN "svc-secure-syn.txt" aaa.aaa.aaa.3-6

UDP Scan

nmap -sU -PO -p 1-1521 –O -S 192.168.6.7 -T 3 -oN "svc-secure-udp.txt" aaa.aaa.aaa.3-6

Nmap scan results:

Device	IP Address	Port	Service
Mail Server	aaa.aaa.aaa.3	25/tcp	SMTP
DNS Server	aaa.aaa.aaa.4	53/udp	DNS
Web Server	aaa.aaa.aaa.5	80/tcp	HTTP
Web Server	aaa.aaa.aaa.5	443/tcp	HTTPS
Time Server	aaa.aaa.aaa.6	123/udp	NTP

Pertinent Snort Portscan Log Entries on IDS-1:

Feb 25 04:10:20 192.68.6.7 -> aaa.aaa.aaa.3 SYN **S*****
Feb 25 04:10:20 192.68.6.7 -> aaa.aaa.aaa.5 SYN **S*****

Feb 25 04:16:09 192.68.6.7 -> aaa.aaa.aaa.4 UDP
Feb 25 04:16:09 192.68.6.7 -> aaa.aaa.aaa.6 UDP

PIX Firewall outbound Access List Rules Tested:

Rule 5 to allow the database server to connect to the web server using SQLNet

Additional Audit Tests Conducted

· Using a VPN account and an Oracle Database account setup for the test an attempt was made to access the GIACE Service Network, Internal LAN, and Secure LAN via a VPN tunnel connection from the Internet. These tests were successful and verified the firewall rule to allow VPN traffic to bypass firewall access controls "sysopt connection permit-ipsec" and also verified that the VPN settings are functional. Examination of the TCPDUMP log file on IDS-2 verified that the VPN tunnel traffic was encrypted.

- An encrypted test email was sent from a host on the Internal LAN to the Internet. This email was successfully received and a review of the TCPDUMP log on IDS-2 verified that the email was encrypted and that network address translation was functioning properly on the primary firewall.

Assignment 3 – Audit Security Infrastructure: Evaluate the Audit

---

3.3 Primary Firewall Audit Evaluation and Recommendations

Review of the Nmap scan results, the Snort Portscan logs and the Tcpdump output files of the three IDS systems, and the primary firewall logs indicated that the security audit of GIACE's primary firewall demonstrated that the primary firewall filtered the test traffic in compliance with GIACE's security policy.

The security architecture assessment of the primary firewall was successful and did not reveal any significant problems or weaknesses. The firewall rules were validated for proper functioning.

The auditors listed the following suggestions to improve the overall security posture of the organization:

- Periodically conduct a complete and comprehensive audit of the entire GIACE network

- Create a disaster recovery plan to prepare for failure. Create an incident handling standard operating procedure that lists detailed instructions to follow during and after a security breach occurs.

- Currently the GIACE router, primary firewall, and secondary firewall are "single points of failure" for the network. Adding a second firewall to the network setup as a hot standby (Cisco calls this "failover") configuration would add redundancy to the network configuration and increase reliability. The Cisco PIX 515E "Failover" (PIX 515E-FO) model is designed for use with a PIX 515E-UR in a failover configuration. Similarly, having a second Cisco router, second IPFilter firewall, and second web server available would also increase network redundancy and reliability.

- Encryption of fortune sayings and other sensitive data would add another layer of defense to the network security posture.

- Emphasize organization and user security awareness. Stress that security is in the organization's and everyone's best interests. Emphasize that everyone has a stake in the company – attacks against the company are attacks against everyone. Fight apathy – use the team approach. The fortune sayings are the lifeblood of the company and generate everyone's salary, bonuses, profits and must be protected.

Assignment 4 – Design Under Fire: Attack Against the Firewall

---

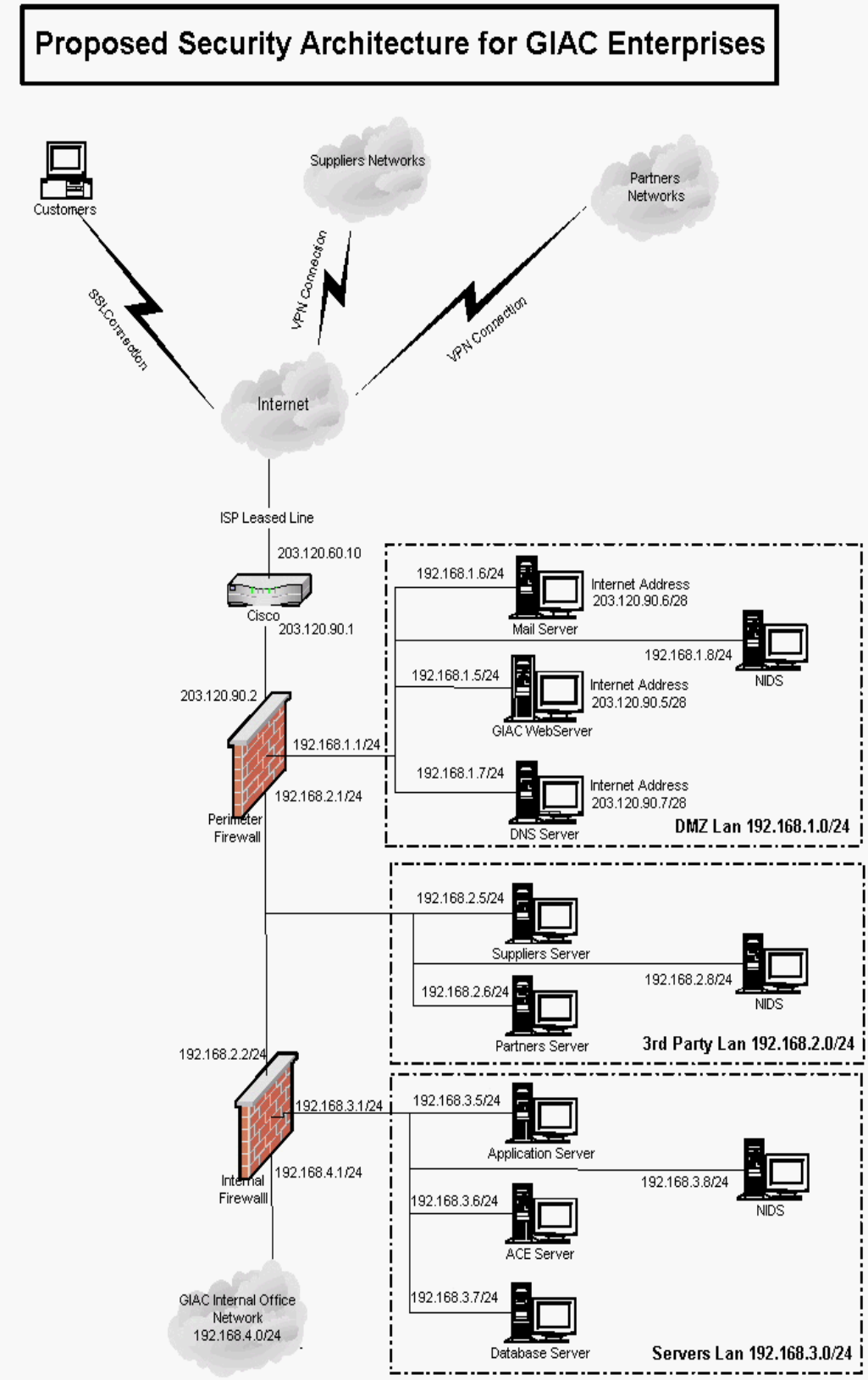
4.1 Attack Against the Firewall

The last portion of this GCFW practical assignment involves reaching and designing postulated attacks against the network layout described in a previously posted GCFW practical assignment. The attacks are an attack against the primary firewall, a denial of service attack against the network, and an attack against a chosen internal system from the perimeter.

4.1.1 Patricia Siow's Network Diagram

The network design of Patricia Siow's practical at **http://www.giac.org/practical/Patricia_Siow_GCFW.zip** was chosen as the network to attack. Patricia (GIAC Certified Firewall Analyst #0324) designed her network using a Cisco 3620 Router as the border router and a Check Point Firewall-1 4.1 built on a Sun machine running Solaris 8 for her primary firewall. Patricia's network design was chosen because it contains a Check Point Firewall-1, which is widely used and extensively evaluated, providing abundant research material.

Patricia Siow's Network Diagram (Figure 5):



4.1.2 Check Point FireWall-1 Documented Vulnerabilities

Checkpoint FW-1 Limited-IP License Vulnerability[23]

Check Point FireWall-1 version 4.1 running on Solaris version 2.x and possibly other Unix platforms is vulnerable to a denial of service attack if using a limited-IP license, due to a vulnerability in the license manager. A remote attacker can send a large number of spoofed packets to the internal interface of the firewall. If the packets include more spoofed source IP addresses than the IP address limit of the firewall license, the console sends a license violation message listing all of the IP addresses counted by the licensing manager. If a very large number of spoofed packed are sent, it causes the console to send a new warning message before the previous message is finished. This can consume 100% of the CPU resources on the console device, and significantly slow down the system.

Checkpoint FW-1 Fragmented Packets DoS Vulnerability[24]

Check Point Firewall-1 4.0 and 4.1 are subject to an IP fragment-driven denial of service vulnerability. A stream of illegally large IP fragments routed to or through the firewall can force the firewall CPU to use all of its processing power to log the packets. The FireWall-1 rule base cannot prevent this attack and it is not logged in the firewall logs. This issue is resolved by installing Firewall-1 4.1 service pack 2.

Checkpoint FW-1 Fast Mode Option Vulnerability[25]

If any firewall rules include the "Fast Mode" option, Check Point Firewall-1 and VPN-1 will incorrectly allow unauthorized connection attempts to hosts that should be restricted. CERT Vulnerability Note VU#446689. A feature called "Fast Mode" (or "FASTPATH"), included in Check Point FireWall-1 and VPN-1 is designed to improve performance in older versions of these products. Unfortunately, a system with this feature

---

23 "Firewall-1 Limited-IP License Denial of Service"
http://www.iss.net/security_center/static/5966.php

24 "Checkpoint FW-1 Fragmented Packets DoS Vulnerability**"**
http://www.safermag.com/html/safer26/dos/19.html

25 "Check Point FireWall-1 allows fragmented packets through firewall if Fast Mode is enabled"
http://www.kb.cert.org/vuls/id/446689

enabled in any rules may not adequately protect systems from specially malformed TCP fragment packets. The Fast Mode feature is disabled by default. Specifically, an intruder can make unauthorized connection attempts to hosts they know the IP address for.

Checkpoint FW-1 Port 259 (RDP) Vulnerability[26]

Vulnerability Note VU#310295 Check Point VPN-1/FireWall-1 version 4.0 & 4.1 may allow an intruder to pass traffic through the firewall on port 259.

Firewall-1 and VPN-1 include support for RDP, but do not provide adequate security controls for RDP data. By adding a faked RDP header to typical UDP traffic, any content can be passed to port 259 on any host on either side of the device. An attacker who exploits this vulnerability can build a tunnel to bypass the firewall and pass traffic to and from arbitrary hosts on either side of the firewall on port 259.

Checkpoint FW-1 Username Guessing Vulnerability[27]

During the course of regular testing, NTA Monitor discovered two serious flaws in Checkpoint Firewall-1, giving rise to both username guessing and sniffing issues.

Firstly, affected versions permit remote users to determine if a Firewall username is valid without having to know the associated password, enabling hackers to guess valid usernames using a dictionary attack. In tests of the flaw conducted by NTA Monitor, it took 2 minutes 30 seconds to check 10,000 usernames at a rate of 67 guesses per second using only 10% of a 2 Mbps leased line. The guessing rate is mostly limited to by the Firewall CPU rather than by the Internet link speed. In effect, this means that companies using a hi-spec firewall server increase the speed at which an attacker can guess passwords.

In addition, VPN usernames are passed in the clear without encryption, allowing anyone who is able to sniff network traffic between VPN clients and the Firewall to observe usernames in transit. The flaws exploit the Internet Key Exchange (IKE) encryption scheme and affect all Checkpoint Firewall-1 systems of 4.0 or above.

The biggest problem is that it is not necessary to send a password to obtain a reply from the Firewall. Given that both users and system

26 "RDP Communications Issue"
http://www.checkpoint.com/techsupport/alerts/rdp_comms.html
27 "NTA Monitor Discover Check Point FW-1 Flaw"
http://www.nta-monitor.com/news/checkpoint.htm

administrators often chose weak passwords, it is likely that any attacker will be able to guess at least one password and thus gain access to the VPN - and from there most configurations easily allow full access to the company's resources.

4.1.3 Attack Scenario

Any of the above listed Check Point FW-1 vulnerabilities could possibly be utilized to gain access to the network that the firewall is protecting if the appropriate safeguards are not in place. Since Patricia's firewall uses Solaris 8 as its base operating system, Solaris 8 vulnerabilities could also be used to attack the firewall. The longer the amount of time that has passed since a vulnerability has been announced, the more likely a patch has been created and applied to correct the problem. A determined hacker dedicated to gaining access to GIACE's network could possibly have more up-to-date information on GIACE's network security posture that GIACE's network security personnel. A hacker could exploit an announced security flaw before a patch to guard against it is created or applied, even if patch administration is kept up-to-date.

I conducted a Internet search of exploits for Check Point FW-1 or Solaris 8 vulnerabilities and found a website that boasts a proof of concept C Language script that could be used to exploit the Checkpoint FW-1 Port 259 (RDP) Vulnerability (described above). By default, Check Point FW-1 firewalls allow Check Point RDP packets on UDP Port 259 to pass through the firewall. The source C code is available for reference at **http://www.inside-security.de/uploads/media/fw1_rdp_poc.c**.

I chose to simulate an attempt to exploit the Port 259 (RDP) Vulnerability on Patricia's firewall. The command to execute the exploit (my compiled version of the C Language program is named fw_1rdp_poc) on my SuSE Linux 7.1 system is:

./fw_1rdp_poc www.xxx.yyy.zzz 259 203.120.90.2

www.xxx.yyy.zzz is the spoofed source IP address
259 is the spoofed source port
203.120.90.2 is the IP address of Patricia's firewall (obtained from Internet research)
(the destination port is hard-coded in the program to be UDP Port 259)

The fw_1rdp_poc program creates crafted UDP packets that appear to be Check Point RDP packets to UDP Port 259 on Patricia's firewall, which are allowed access by default on an un-patched firewall. However, the attack was not successful, indicating that Patricia had either applied the proper patch (Check Point SP5) or applied one of several hot fixes to remove the vulnerability.

Assignment 4 – Design Under Fire: Denial of Service (DOS) Attack

4.2 Denial of Service Attack

(Note: A U.S. Department of Energy Computer Incident Advisory Capability (CIAC) Information Bulletin, title **"**K-037: "mstream" Distributed Denial of Service Tool", **http://ciac.llnl.gov/ciac/bulletins/k-037.shtml**, was used a reference for the following "mstream" simulated attack scenario.)

A distributed client-server DDoS tool named "mstream", a distributed handler-agent tool designed to enable use of multiple Internet-connected systems to perform packet flooding DDOS attacks against Internet target host(s), was chosen for the "simulated" Distributed Denial of (DDoS) attack against Patricia's network, using fifty compromised "zombie" cable modem/DSL systems**.**

My mstream network is comprised of my system running the mstream client, ten of my compromised systems acting as mstream "handlers", and 40 of my compromised systems acting as mstream "agents". My system send traffic to the handler systems via unencrypted TCP Port 6723. My handler systems send traffic to their agent systems via UDP Port 7983 and receive traffic back from their handler systems via UDP Port 9325. (Note: The ports are configurable. The default ports are listed.)

After logging in to each handler system to begin an attack against www.giacenterprises.com (used as an example) for 600 seconds, I issue the command:

stream www.giacenterprises.com 600

Upon receiving the command each handler system resolves the hostname www.giacenterprises.com to an IP address and transmits the following command to each of the four agent systems that it handles (203.120.90.5, the IP address for the web server in Patricia's network design, is used for this example):

mstream /203.120.90.5: 203.120.90.5/600

The attack floods the www.giacenterprises.com system with 40-byte TCP Acknowledge (ACK) packets with forged random IP addresses sent to random ports designed to slow down the target system as www.giacenterprises.com tries to return TCP Reset (RST) packets and tie up network resources as network routers try to return ICMP Host Unreachable messages.

I issue the command "quit" to my mstream handler systems to close the connections.

Countermeasures for the DDOS Attack

- Use Aggressive TCP on border router – Patricia's network design includes a Cisco 2610 border router configured with TCP Intercept mode set to protect against TCP SYN-Flood attacks.

- Reject in-bound subnet-directed broadcast traffic at the network perimeter.

- Increase the network bandwidth.

- Implement IPv6, which provides protocol authentication functionality to deter spoofing of the origin of Internet packets.[28]

Assignment 4 – Design Under Fire:

Compromise an Internal System Through a Perimeter System

4.2 Attack Through the Perimeter

SCENARIO 1 -The GIAC public web server is a good choice as the perimeter system to compromise in order to gain access to the internal network. The web server is the most vulnerable part of an e-commerce business since it allows public access, processes input from the public, and sends output to the public. The router and firewall allow public access via http to the web server. There are a myriad of exploitation tools available to use to probe for vulnerabilities in and penetrate Internet web servers. Once compromised, the web server can be used as a stepping-stone to gain access to the remainder of the network.

An outstanding tool that can be used to scan web servers for vulnerabilities is the freeware Whisker common gateway interface (CGI) scanner created by "Rain Forest Puppy". The current Whisker version 2.1 can be downloaded from his web site at **http://www.wiretrip.net/rfp/p/doc.asp/i5/d21.htm** Whisker was designed so that its scans are as "stealthy" as possible and the scans are specifically configured to avoid recognition by intrusion detection systems.

28 "Author of Web Attack Tool Speaks" **http://zdnet.com.com/2100-11-518461.html?legacy=zdnn**

Once Whisker has been installed, a scan of Patricia's web server (IP address 203.120.90.5) can be performed with the following command:

#perl whisker.pl -v -s scan.db -h 203.120.90.5

The –v option specifies verbose output.
The –s option specifies the script database file (the default is scan.db).
The –h option specifies scan a single host.
203.120.90.5 is the IP address of Patricia's web server.

The prospects for success of this type of attack are very good, as demonstrated by the many Internet web server hacks that have occurred, many against businesses and institutions that were thought to have very secure networks.

Defending against this type of attack involves constant vigilance by everyone in the organization. Software patches for all operating systems and applications must be kept up-to-date. If the network defenses are compromised, a plan of action must be in place that can be implemented immediately (at any time of day) to minimize the consequences.

SCENARIO 2 - Social engineering is also a good choice as a way to compromise a network through a perimeter system. Exploiting the vulnerabilities of people may sometimes be easier than exploiting computer network software and hardware vulnerabilities. An example of this is "piggy-backing" behind someone who has access to an entrance by following them through the door after they have opened it. Another social engineering example is calling on the phone and coaxing/deceiving users or administrators to reveal helpful sensitive network information over the phone.

Defending against social engineering attacks requires that people be aware of such attacks and have the commitment to thwart and report them.

SCENARIO 3 - An attacker could use a war dialer to search for unprotected modems on the network. This would allow the attacker to bypass all of the network-based security measures.

This type of attack can be defended against by creating and strictly enforcing an organization security policy forbidding the use of individual computer modems inside the network. Another countermeasure is for the organization to conduct periodic scans for the presence of the modems.

Conclusion:

Operating a computer network today, especially one which connects to other networks such extranets and/or the Internet, is a serious responsibility. Network security is a dynamic ever-changing continuum. There will always be a balance

between the use and productivity of computer networks and the security of those networks. The costs of network security measures have to be weighed against the threat and consequences of not utilizing the security measures. The threat will always be there and the threat. People get better at breaking network security every day. But people also get better at defending networks every day. So it is always a matter of evaluating the possibility of the threat targeting a specific organization or person, estimating the possible consequences, and taking weighed measures to reduce the threat and minimize the consequences.

Just as a chain is only as strong as its weakest link, a security architecture is only as secure as its weakest element.

Appendix A – GIAC GCFW Certification Paper Requirements

Assignment 1 - Security Architecture: Requirements

Define a network security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings.
Your architecture must consider access requirements (and restrictions) for:

- Customers (Companies or individuals that purchase bulk online fortunes)
- Suppliers (Companies that supply GIAC Enterprises with their fortune cookie sayings)
- Partners (International companies that translate and resell fortunes)
- GIAC Enterprises employees located on GIAC Enterprise's internal network
- GIAC Enterprises mobile sales force and teleworkers

You must explicitly define how the business operations of GIAC Enterprises will take place. How will each of the groups listed above connect to or communicate with GIAC Enterprises? How will GIAC Enterprises employees access the outside world? What services, protocols, or applications will be used?
Defining access requirements and the reasoning for those requirements is critical to this assignment. If you have not thought through how this access will take place, you will not be able to adequately define your security policy and ACLs/rulesets later in the paper.

In designing your architecture, you must include the following components:

- Filtering Router(s)
- Firewall(s)
- VPN(s)
- An IP addressing scheme (use known non-routable addresses your policies will be graded taking them into account.)

Your architecture may also include the following optional components if they are appropriate to your design:

- Internal firewalls (Are internal firewalls appropriate for additional layered protection; to segment internal networks…?)
- Additional secure remote access (Is additional remote access – other than the VPN – required by administrators, salespeople, telecommuters…?).
- Intrusion detection systems

You must include a diagram or set of diagrams that shows the layout of GIAC Enterprise's network and the location of each component listed above. You must provide the specific brand and version of each perimeter defense component

used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.
The network can be as complex or as simple as you like as long as it meets the functional requirements that you define according to the guidelines given above. The important thing is not how elaborate your network is, but that your design actually works.

You must justify the appropriateness of your design. Is it both technically reasonable and financially feasible? Are you building a $1000 fence to contain a $100 horse? You may provide a cost or bill of materials if you wish.

Assignment 2 - Security Policies: Requirements

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

- Border Router(s)
- Primary Firewall(s)
- VPN(s)

You may optionally include policy for other devices (i.e., - internal firewalls).
By "policy" we mean the specific set of ACLs, ruleset, or IPSec policy for that device – **not** corporate or organizational policy (though note that organizational policy may dictate the specific ACLs or ruleset in effect).

For each component, be sure to consider the access requirements for customers, suppliers, partners, remote users, and internal users that you defined in Assignment 1. The policies you define must accurately reflect those business needs as well as appropriate security considerations.

You must include the complete policy (meaning explicit ACLs, Ruleset, IPSec policy, etc.) in your paper. It is not enough to simply state "I would include ingress and egress filtering..." The policies may be included in an Appendix if doing so will help the "flow" of the paper (clearly state if this is the case).

For each rule in all policies, you must include the general purpose of the rule and why it is important.

You must also include a discussion of the order of the rules, and why order is (or is not) important.

For one of the three security policies defined above, you must create a clearly labeled & separate tutorial on how to implement the policy. This tutorial is in addition to the full policy for that device / function. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information to clarify your instructions. Be certain to include a general explanation of the syntax or format of the ACL, filter, or rule for your device, as well as a general explanation of how to apply a given ACL, filter, or rule.

Be certain to point out any tips, tricks, or potential problems.

Assignment 3 – Audit Security Infrastructure: Requirements

You have been asked to conduct a technical audit of GIAC's primary firewall in order to verify that the policies are correctly enforced as described in Assignments 1 and 2. To conduct the audit, you will need to:

- Plan the audit.
  - Describe the technical approach you will use to assess the firewall.
  - 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 and how they are addressed.
  - Remember the goal is to verify the firewall policy not perform a vulnerability assessment.

- Using the approach you described conduct the audit.
  - Demonstrate how you validated that the primary firewall is actually implementing GIAC Enterprise's security policy.
  - Be certain to include the tools and commands used. Include screen shots in your report if possible.
  - It is essential that you are actually verifying the firewall policy instead of auditing or vulnerability assessing other network devices.

- Evaluate the audit. Based on your assessment (and referring to data from your assessment):
  - Provide an analysis of the audit results.
  - Make recommendations for improvements or alternate architectures.
  - **Supportive 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 you must annotate/explain the output.

Assignment 4 – Design Under Fire: Requirements

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 **GCFW practical** posted in the previous **6 months** and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Research and design the following three types of attacks against the architecture:

1. An attack against the firewall itself.

- Research and describe a vulnerability that has been found for the type of firewall chosen for the design.
- Design an attack based on the vulnerability.
- Explain the results of running that attack against the firewall.

2. A denial of service attack.

- Subject the design to an attack from 50 compromised cable modem/DSL systems.
- 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 and explain your reasons for choosing that target.
- Describe the process to compromise the target.

Your attack information should be detailed – include the specifics of how the attack would be carried out. Do not simply say "I would exploit the vulnerability described in Vendor Security Bulletin XXX". What commands would you use to carry out the attack? Are exploit tools or scripts available on the Internet? What additional steps would you need to take prior to conducting the attack (reconnaissance, determining internal network layout, determining valid account name…)? Would any of your methods be noticed (log files, IDS…)? What "stealth" techniques could you employ to avoid detection? What countermeasures would help prevent your attack from succeeding?

If it is possible to carry out the attack on a test system, include screen shots, log files, etc. as appropriate to illustrate your methods.
In designing your attacks, keep the following in mind:

- The attack should be **realistic.** The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

- The attack should be **reasonable.** The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should **not** assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)

- You must supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.

The attack does not necessarily have to succeed. If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.

List of References

[1] Chapman, David W. and Fox, Andy (Editors) Cisco Secure PIX Firewalls, Indianapolis, Cisco Press, 2002. 203, 228-229.

[2] "Cisco 2600 Series Multiservice Platforms" **http://cisco.com/en/US/products/hw/routers/ps259/index.html** (15 FEBRUARY 2003)

[3] "Virtual Private Network Modules for Cisco 1700, 2600, 3600, and 3700 Series" **http://cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a0080088750.html** (15 FEBRUARY 2003)

[4] "New Features in Release 11.3" **http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/rn113m/rn113mft.htm - xtocid63** (31 DECEMBER 2002)

[5] Cisco PIX 515 Firewall photo – courtesy of the Cisco website: **http://cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html** (28 FEBRUARY 2003)

[6] "Cisco PIX Firewalls" URL: **http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/index.shtml** (31 DECEMBER 2002)

[7] "Firewall Comparison: Checkpoint Firewall-1 and Cisco PIX" URL: **http://www.roble.com/docs/fw1_or_pix.html** (31 DECEMBER 2002)

[8] "Cisco PIX 515E Firewall" **http://cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html** (20 FEBRUARY 2003)

[9] "Internet Gateway Products" **http://www.trendmicro.com/en/products/gateway/overview.htm** (31 DECEMBER 2002)

[10] "Configuring IP Access Lists" **http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml** (23 FEBRUARY 2002)

[11] "Router Security Configuration Guide" URL: **http://www.nsa.gov/snac/index.html** (31 DECEMBER 2002)

[12] "Essential IOS Features Every ISP Should Consider" URL: **http://www.grift.com/** (25 FEBRUARY 2003)

List of References (continued)

[13] "Cisco Router Configuration Options" URL: **http://www.uniforum.chi.il.us/slides/ddos/sld019.htm** (31 DECEMBER 2002)

[14] "Info on configuring a Cisco access list to filter IP" URL: **http://www.mtiweb.com/isp/ciscoacc.html** (31 DECEMBER 2002)

[15] "Info on configuring a Cisco access list to filter IP" URL: **http://www.mtiweb.com/isp/ciscoacc.html** (31 DECEMBER 2002)

[16] "Basic Firewall Configuration" URL: **http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm** (31 DECEMBER 2002)

[17] Cisco Security Bible, Rajesh Kumar Sharma, Hungry Minds, Inc, New York, NY, 2002, p. 292

[18] Cisco Secure PIX Firewalls, edited by David W. Chapman and Andy Fox, Cisco Press, Indianapolis, IN, Mar 2002, p. 203

[19] Cisco Secure PIX Firewalls, edited by David W. Chapman and Andy Fox, Cisco Press, Indianapolis, IN, Mar 2002, pages 228-229

[20] Spitzner, Lance. "Auditing Your Firewall Setup", URL: **http://www.spitzner.net/audit.html** (18 FEBRUARY 2003)

[21] The SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs course manual 2.5, 2002. 110.

[22] The SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs course manual 2.3, 2002. 202.

[23] "Firewall-1 Limited-IP License Denial of Service" **http://www.iss.net/security_center/static/5966.php** (18 FEBRUARY 2003)

[24] "Check Point FW-1 Fragmented Packets DoS Vulnerability" **http://www.safermag.com/html/safer26/dos/19.html** (18 FEBRUARY 2003)

[25] "Check Point FireWall-1 allows fragmented packets through firewall if Fast Mode is enabled" **http://www.kb.cert.org/vuls/id/446689** (18 FEBRUARY 2003)

List of References (continued)

[26] "RDP Communications Issue" URL: **http://www.checkpoint.com/techsupport/alerts/rdp_comms.html** (31 DECEMBER 2002)

[27] "NTA Monitor Discovers Check Point FW-1 Flaw" URL: **http://www.nta-monitor.com/news/checkpoint.htm** (20 FEBRUARY 2003).

[28] Lemos, Robert. 9 Feb 2000. "Author of Web Attack Tool Speaks" URL: **http://zdnet.com.com/2100-11-518461.html?legacy=zdnn** (31 DECEMBER 2002).

GIAC GCFW Practicals used as general references:

Siow, Patricia. May 2002. "GCFW Practical Assignment Oct. 2002" URL: **http://www.giac.org/practical/Patricia_Siow_GCFW.zip** (20 FEBRUARY 2003)

Chan, William. Oct 2002 "SANS GIAC Certification GCFW Practical Assignment" URL: **http://www.giac.org/practical/William_Chan_GCFW.pdf** (20 FEBRUARY 2003)

Poer, Geoff. Jan 2, 2003 "Cause Cookies Aren't Cheap!" URL: **http://www.giac.org/practical/GCFW/Geoff_Poer_GCFW.pdf** (20 FEBRUARY 2003)

Matusiewicz, Joe. Jan 2003 "GCFW Practical Assignment " URL: **http://www.giac.org/practical/GCFW/Joe_Matusiewicz_GCFW.pdf**

Pogue, Matt. Nov 19, 2002. "GCFW Practical Assignment" URL: **http://www.giac.org/practical/Matt_Pogue_GCFW.doc** (20 FEBRUARY 2003)