



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Firewalls, Perimeter Protection, and VPNs

**GCFW Practical Assignment  
Version 1.5e**

**Practical Assignment for SANS Rocky Mountain 2001**

**Stephen Goldman**

## Table of Contents

Assignment 1 – Security Architecture	3
1. Overview	3
1.1 Border Router	3
1.2 Customer Access	3
1.3 Partners and Supplier Access	3
1.4 Traveling/Remote User Access	3
1.5 Firewall and VPN server	5
1.6 Web Server	5
1.7 Corporate E-mail	5
1.8 Domain Name Server	5
1.9 Intrusion Detection System	6
Network Design - Figure 1	7
Assignment 2 – Security Policy	8
2. Security Policy	9
2.1 Configuration and Hardening of Border Router	9
2.2 Network Address Translation Configuration	12
2.3 Border Router ACL lists	13
2.4 Primary Firewall	16
2.5 VPN Server	19
Assignment 3 - Assessment	21
3.1 Planning the Assessment	21
3.2 Implementing the Assessment	25
3.3 Recommendation	25
Assignment 4 – Design Under Fire	27
4.1 Firewall Attack	28
4.2 Denial of Service Attack	29
4.3 Internal System Attack	30
References	32

## Assignment 1 – Security Architecture

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

You must consider and define access for:

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

### 1. Overview

In today's world of ready accessibility to the Internet and the proliferation of GUI based tools, hackers do not need to be as knowledgeable as they once were. Programs and tools are easily downloaded from various websites that allow you to scan other networks, probe for weaknesses, and exploit them without knowing much, if any thing about the TCP/IP protocol stack and networking in general. Today programs exist that will quickly generate email virus and worms, which then can be sent out to bring down whole networks. GIAC Enterprise network is being designed to minimize these ever-growing threats of cyber space attacks. Using the analogy of the medieval castles, we are building many walls and layers that will slow down the attackers long enough so we can proactively react.

Our first layer of defense will be the border router. This will provide packet filtering to eliminate noise and unwanted traffic from the network. The next layer will be the external firewall that will guard the DMZ, GIAC service network and Virtual Private Network (VPN) services for the company's partners, suppliers and remote users. The last layer is the internal firewall that protects the companies database servers and the internal network.

To further protect and hide GIAC hosts and workstations that do not need visibility on the internet, Network Address Translation (NAT) will be implemented to utilize private IP address (RFC 1918) on the internal network. GIAC Enterprises has obtained from it's Internet Service Provider (ISP) a block of 14 IP addresses (x.y.z.1 – x.y.z.14) to be used for Internet access. The first 9 IP addresses will be statically assigned to hosts, while the last 5 are allocated for the NAT pool. Access control lists will be used to limit the internal hosts from receiving address translations. This will be further discussed in the next section.

## **1.1 Border Router**

The CISCO 3640 router is the first level of defense for our network. This particular router is designed for medium to large size offices and has the horsepower to support GIAC current and future needs. Utilizing access control lists on the inbound and outbound paths of the interfaces, the router will strip away-unwanted traffic based on protocol leaving the firewall to handle what is left. In addition to performing the basic routing and packet filtering for GIAC network, the router will also be functioning as the NAT server for the network. The router will have the latest version of the IOS software installed, which at the time of this paper version 12.2.1b. Updates will be made when needed to patch future vulnerabilities.

## **1.2 Customer Access (Reverse Proxy Server)**

For any normal e-business, a web server needs to be accessible by the outside world to allow customers access to the site and more importantly to purchase the services or products in a secure manner. Money is what keeps the company in business, and without a secure way for customer to purchase the products, the company will not survive. A Reverse Proxy Server (RPS) will be used as the access point for all customer interactions. The purpose of a RPS is to appear as the actual webserver to the outside world and provide protection to the true webserver. When the customer makes a request, the proxy receives it and relays the request to webserver, which is protected behind the firewall. The webserver then sends the results back through the firewall to the proxy, which in turn relays it back to the customer.

## **1.5 Partners and Supplier Access**

Since the suppliers and partners are the source of GIAC business, it is important to maintain tight security on the information flowing between these sources. For this reason, all connectivity will be handled through a Virtual Private Network (VPN) server. For smaller offices without a VPN server, access will be handled in the same way remote users are. Similar to the customer access, once a secure connection is made, the partners or suppliers will connect to their perspective web servers via a RPS to carry out their business.

## **1.6 Traveling /Remote User Access**

For remote and traveling users that need access to GIAC internal network, access will be made via the Internet (ISP, Cable modem, DSL) to the corporate VPN server. The client machines will run Checkpoint VPN-1 SecureClient software version 4.1 with the latest service pack (at the time of this paper sp4 is the latest)

<http://www.checkpoint.com/products/vpn1/secureclient.html>.

SecureClient allows GIAC's VPN Policy Server to download its security policy to the remote client ensuring proper configuration. This will prevent hackers from taking advantage of insecure remote machines' VPN connections into the GIAC network.

### **1.7 Firewall and Virtual Private Network (VPN) Server**

GIAC is utilizing two stateful firewalls on their network, one acting as the external firewall and the other as the internal firewall. Separate vendors firewall products are used for additional level of complexity and security to the network. This method ensures that if the first firewall is compromised, the same techniques can not be used on the second firewall.

For the external firewall and VPN server, GIAC will be using Checkpoint Firewall-1 / VPN-1 server installed on a Nokia IP530 with the Luna VPN accelerator card for added performance <http://www.checkpoint.com/opsec/platforms/nokiaip530.html>. An integrated firewall and VPN solution was picked because it offers centralized management, unified audit logs, and access control for all traffic.

The Cisco PIX 515 Firewall system will be used for the internal firewall. It will be running PIX version 6.0 software. When updates and patches are released, they will be installed to keep the software current.

With both firewalls installed on appliances, this will eliminate the vulnerability inherent in a commercial Operating System (OS) such as Windows NT or Unix. The appliance OS is already hardened, removing most of the vulnerabilities.

### **1.6 Web Server**

The corporate web servers are all SSL enabled with both 128bit and 40bit certificates to handle international security issues if applicable. The web servers are installed on Redhat 7.1 servers with the latest security patches running apache web services. All transactions will be done via the https protocol (443/TCP). Web servers are only accessible via their reverse proxy servers. Data displayed for the users comes from SQL data queries made to the enterprise database server.

### **1.7 Corporate E-mail**

Today, a common method of communications and information exchange takes the form of email. Email is a major source of security holes, it can be used to transport viruses and other types of malicious programs. Email also can be used to commit corporate espionage. To patch these holes and vulnerabilities, a mail proxy running MailMarshal ver 4.2 by Marshal Software (<http://www.marshalsoftware.com>) will be used. With the use of the Mail Proxy, all incoming/outgoing messages will be tested for content of worms/viruses, and also search for internal company information to prevent fortunes from being sent out via email.

### **1.8 Domain Name Server (DNS)**

DNS is a distributed database that is used to maintain a translation between IP addresses and host names, and visa versa. The Internet depends on IP address, but people do not

remember numbers as well as they remember names. Because humans do not use IP addresses, but rather names, the DNS does the translation and allows us to access the hosts. To protect against DNS poisoning, we will be using split-split horizon DNS. The external-external DNS will be located in the DMZ network and will be the only DNS to have UDP port 53 accessible to the internet and contain the bare minimum information about GIAC network. The external-internal DNS will be accessible only for the service network and the internal DNS will function as the internal network DNS. Both of the external DNSs are running on Redhat 7.0 with up to date security patches. The internal DNS is running on Windows NT 4.0 SP6a and appropriate hot fixes. Since DHCP is utilized on the internal network, a separate WINS server is installed in conjunction with the DNS.

### **1.9 Intrusion Detection System**

Once the firewalls and routers have been setup for the network, we need to be able to provide checks and balances to ensure that no unwanted traffic is entering the network. This is the job of Intrusion Detection Systems (IDSs). They are placed on the network and passively monitor and log all TCP/IP traffic. The logs for the systems on GIAC network will all be stored on the corporate logging server located on the service network. Systems installed with Redhat 7.1 running tcpdump will be used for this task. As the company grows and funds become more available, these systems will be replaced with Cisco's Intrusion Detection System appliances.

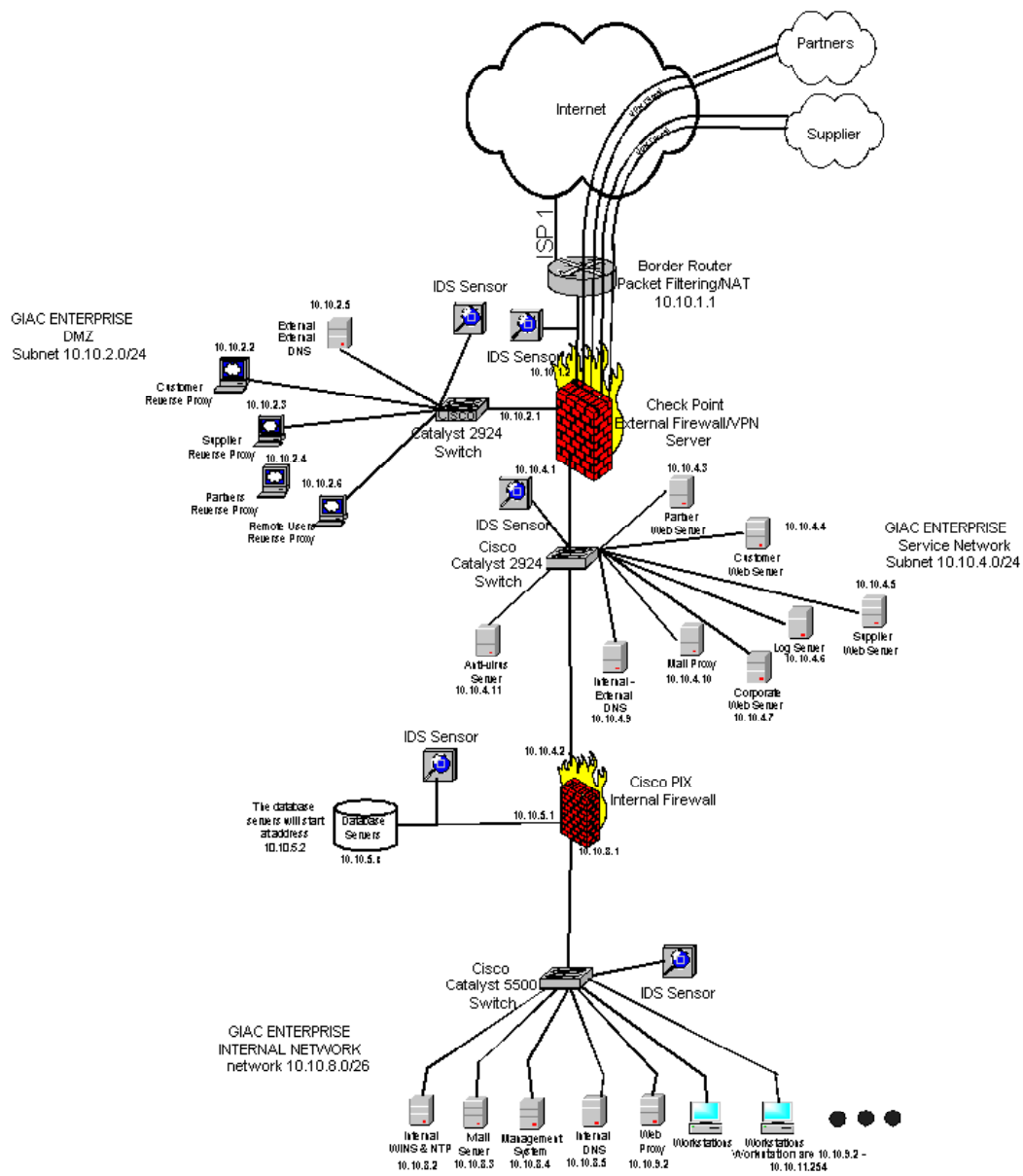


Figure 1



## Assignment 2 – Security Policy

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

- Border Router
- Primary Firewall
- VPN

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

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

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

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

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

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

## 2. Security Policy

In this sections we will discuss the configuration of the border router, primary firewall and VPN server utilized on this network. A basic understanding of CISCO IOS software is assumed. Once you have connected to the router, you must enter the *enable mode* in order to configure the IOS. This is accomplished by entering *enable* at the command line, and then when prompted, entering the enable password.

Before the border router and firewall can be configured, the rules for the security policy must properly defined. They are as follow

- Harden Operating System
- Deny all common spoofing and denial of service attacks.
- Deny all common vulnerabilities
- In order to protect against DNS poisoning, split-split horizon DNS technique will be implemented.
- Network Address Translation is utilized to help hide internal systems
- Limit direct access to the following internal hosts: border domain DNS, customer reverse proxy server, mail proxy server and VPN server.
- Corporate web servers will be accessible only from the reverse proxy servers (Customer, Partner, and Supplier), internal web proxy server and the corporate management hosts.
- Access to the corporate database is limited to the corporate management hosts and web servers.
- All e-mail inbound and outbound will pass through the mail relay host to verify content and check for viruses.
- All traffic will pass through corporate firewall.
- Internal devices with address of 10.10.8.x and 10.10.5.x will not be translated by the NAT. These devices are switches, hubs and internal use only servers and hosts that do not need to access the Internet.

### 2.1 Configuration and Hardening of Border Router (CISCO 3640)

The first issue that needs to be addressed before any access control lists can be created, is to first ensure that the underlying operating system has been harden. This entails the removing or disabling of services that are not needed and can cause potential security holes.

#### 2.1.1 Administrative Access

The router has five virtual terminals that allow users to connect via telnet sessions to the router. In order to prevent any unauthorized access, an access-list will be applied to all of the VTY interfaces, along with a password. This access-list will granted telnet access only to the GIAC management host for security purposes. Configuration can also be achieved through the console port on the router.

```
CISCO-3640(config)# access-list 5 permit 10.10.8.4 255.255.255.255
CISCO-3640(config)# line vty 0 4
CISCO-3640 (config-line)# access-class 5
```

```
CISCO-3640 (config-line)# session-timeout 45
CISCO-3640 (config-line)# exec-timeout 45 0
CISCO-3640 (config-line)# password #####
CISCO-3640 (config-line)# login
```

### **2.1.2 SNMP (RFC 1157)**

Simple Network Management Protocol (SNMP) is used to both gather information about a network device and has the capability to modify various parameters. Because of the several vulnerabilities that exist with this protocol, SNMP is disabled on the router.

```
CISCO-3640(config)# no snmp-server
CISCO-3640(config)# no snmp-server location
CISCO-3640(config)# no snmp-server contact
```

### **2.1.3 Loose Source Routing**

Loose Source Routing allows you to specify a list of routers that a packet must traverse in getting to its destination. This service should be disabled.

```
CISCO-3640(config)# no ip-source route
```

### **2.1.4 Password Encryption**

By default, passwords saved in the configuration file are in clear text mode. Cisco provides a command that will display the passwords encrypted. This is not fool proof in that the encryption used at this level can be cracked.

```
CISCO-3640(config)# service password-encryption
CISCO-3640(config)# enable secret
```

### **2.1.5 TCP and UDP Diagnostic Ports**

Cisco by default has various TCP and UDP diagnostics ports enabled which can be exploited to cause a Denial of Service (DOS) by causing excessive CPU utilization. These services should be disabled.

```
CISCO-3640(config)# no service udp-small-servers
CISCO-3640(config)# no service tcp-small-servers
```

### **2.1.6 Limiting ICMP**

ICMP packets can be used to gather information about the internal network. The two global settings are turned off thus preventing malicious directed broadcasts from causing DoS and from giving out information based on error messages. Access-lists will be used to block all other ICMP traffic.

```
CISCO-3640(config)# no ip direct-broadcast
CISCO-3640(config)#no ip unreachable
```

### **2.1.7 Disable Finger, Bootp, Cisco Discover Protocol (CDP) and HTTP Services**

Hackers can possibly gain information about your network by use finger. This service should be disabled. Bootp and HTTP are not utilized and should be disabled. CDP should be disabled because it can be used to aid in the discovery other network devices.

```
CISCO-3640(config)# no service finger
CISCO-3640(config)# no ip bootp
CISCO-3640(config)# no ip http
CISCO-3640(config)# no cdp run
```

### **2.1.8 Logging**

Select Access Control List (ACL) rules that are critical to the security of the system need to be logged. In order to be able to examine the information in the files at some later date, they need to be stored on a remote host. The following command will save the log files to the networks logging server.

```
CISCO-3640(config)# service timestamps log datetime msec localtime show-timezone
CISCO-3640(config)# logging 10.10.4.6
CISCO-3640(config)# logging console emergencies
CISCO-3640(config)# logging trap debug
```

### **2.1.9 Network Time**

In order for the system logs to be of some worth, all of the systems on the network need to be time synchronized to allow you to correlate the logs from different systems. An internal timeserver has been configured on the GIAC network. It can be a security issue to receive time synchronization from unknown outside sources.

```
CISCO-3640(config)# ntp update-calendar
CISCO-3640(config)# ntp server 10.10.8.2
```

### **2.1.10 Warning Banner**

A warning banner needs to be displayed every time someone connects to the system. The banner would state that it is unlawful to access the system without authorization. This is more for legal reasons than anything else.

```
CISCO-3640(config)# banner motd ^C
CISCO-3640(config)# Warning: Unauthorized access is not allowed.
CISCO-3640(config)# ^C
```

### **2.1.11 TCP Intercept Mode**

TCP intercept protects the TCP server from the TCP SYN-flooding DoS attack. If this

attack occurs the server is flooded with requests for connections with unreachable return addresses. TCP intercept helps prevent the attack by intercepting SYN packets that match an access list. The router establishes the connection with the client, if successful it establishes the connection to the server and then joins the two together. If the connection with the client is not established, it times out, and is discarded. This protects the server while still allowing valid requests. For more detail information, visit [http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur\\_c/scprt3/scdenial.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/scdenial.htm)

```
CISCO-3640(config)# ip tcp intercept list 101
CISCO-3640(config)# access-list 101 permit tcp any x.y.z.0 0.0.0.15
```

## 2.2 Network Address Translation (NAT) Configuration

The Cisco 3640 router supports NAT and will be implemented on the border router. This allows GIAC to hide most of its internal network from the world, adding an additional layer of security and protection. GIAC received the subnet x.y.z.0/28 from the local ISP, giving then routable ip addresses of x.y.z.1 through x.y.z.14. The first 9 address will be used for static mappings and the last 5 will be used for the NAT pool.

The following is the configuration for the Cisco 3640 and NAT services

### ! Ethernet connection to GIAC network

```
Interface ethernet 0
description connection to External Firewall
ip address 10.10.1.1 255.255.255.0
no ip directed-broadcast
ip nat inside
ip Access-group 130 in
```

!

### ! Serial connection to ISP

```
Interface serial 0
Description Connection to ISP
ip address x.y.z.1 255.255.255.240
no ip directed-broadcast
ip nat outside
Description Access list for ingress and egress explained in section 2.3
ip Access-group 110 out
ip Access-group 120 in
```

### ! Define Dynamic NAT pool

```
ip nat translation timeout 86400
ip nat translation tcp-timeout 86400
ip nat translation udp-timeout 300
ip nat translation dns-timeout 60
ip nat translation finrst-timeout 60
ip nat pool giac x.y.z.10 x.y.z.15 prefix 28
```

### ! Assigning access-list that defines rules for NAT translations

ip nat inside source 15 pool giac overload

**! Static for Customer Reverse Proxy Server**

ip nat inside source static 10.10.2.2 x.y.z.2

**! Static for VPN Server (Firewall)**

ip nat inside source static 10.10.1.2 x.y.z.3

**! Static for DMZ DNS server, all incoming ports are mapped to port 53**

ip nat inside source static 10.10.2.5 x.y.z.4 53

**! Static for Mail Proxy**

ip nat inside source static 10.10.4.10 x.y.z.5

**! Static for Internal Web Proxy Server**

ip nat inside source static 10.10.9.2 x.y.z.6

**!Access list for defining what internal private address will be translated by the NAT**

access-list 15 permit 10.10.2.0 0.0.0.255

access-list 15 permit 10.10.3.0 0.0.0.255

access-list 15 permit 10.10.4.0 0.0.0.255

access-list 15 permit 10.10.9.0 0.0.0.255

access-list 15 permit 10.10.10.0 0.0.0.255

access-list 15 permit 10.10.11.0 0.0.0.255

## 2.3 Border Router ACL lists (CISCO 3640)

Now that we have hardened the baseline OS and configured the NAT, we will now define the inbound packet filtering rules. Order of the Access Control List (ACL) is important for various reasons. The ACL is read sequentially from top to bottom, once a match is found the search is stopped and the action stated is executed. For this reason, the order that the rules are entered becomes important. The rules that will apply most often should be placed closer to the top of the ACL, followed by the next most frequent rule.

Doing a *Show Access-list 110* at the command line will display the list along with the number to matches each rule has. Based on this, the order of the access-list can be revised and thus optimized. You will still want to keep the spoofing address on the top of the list for protection.

### 2.3.1 Ingress ACL on Border Router Interface S0 (CISCO 3640)

This is the ACL that controls the filtering for packets coming into GIAC network from the Internet.

**! Deny RFC 1918 addresses (Spoofed Addresses)**

Access-list 110 deny ip 10.0.0.0 0.255.255.255 any log

Access-list 110 deny ip 172.16.0.0 0.31.255.255 any log

Access-list 110 deny ip 192.168.0.0 0.0.255.255 any log

Access-list 110 deny ip 224.0.0.0 31.255.255.255 any log

Access-list 110 deny ip 127.0.0.0 0.255.255.255 any log

Access-list 110 deny ip host 0.0.0.0 any log

**! Deny GIAC internal address from the outside of the router**

Access-list 110 deny ip x.y.z.0 0.0.0.240 log

**! Allow UDP access to external-external DNS**

Access-list 110 permit tcp any host x.y.z.4 eq 53 log

Access-list 110 deny tcp any any eq 53 log

**! Allow access to Mail Proxy**

Access-list 110 permit tcp any host x.y.z.5 eq 25 log

Access-list 110 deny tcp any any eq 25 log

**! Allow access to VPN Server**

Access-list 110 permit 50 any host x.y.z.3 log

Access-list 110 permit 51 any host x.y.z.3 log

Access-list 110 permit udp any host x.y.z.3 eq 500 log

Access-list 110 deny 50 any any log

Access-list 110 deny 51 any any log

Access-list 110 deny udp any any eq 500 log

**! Allow http and https access to customer proxy server**

Access-list 110 permit tcp any host x.y.z.2 eq 80 log

Access-list 110 permit tcp any host x.y.z.2 eq 443 log

**! Allow https and https access to internal web proxy for established connections**

Access-list 110 permit tcp any host x.y.z.6 eq 80 established log

Access-list 110 permit tcp any host x.y.z.6 eq 443 established log

**! Deny all other http and https access**

Access-list 110 deny tcp any any eq 80

Access-list 110 deny tcp any any eq 443

**! Blocking Telnet Services**

Access-list 110 deny tcp any any telnet log

**! Allow ping to S0 interface on Border deny all other ICMP traffic**

Access-list 110 permit icmp any host x.y.z.1 eq echo log

Access-list 110 deny icmp any any log

**! Blocking NetBIOS traffic**

Access-list 110 deny tcp any any range 135 139 log

Access-list 110 deny udp any any range 135 139 log

Access-list 110 deny tcp any any eq 445 log

Access-list 110 deny udp any any eq 445 log

**!Blocking SUNRPC , Xwindows and NFS**

Access-list 110 deny upd any any eq 111 log

Access-list 110 deny tcp any any eq 111 log

Access-list 110 deny tcp any any range 6000 6255 log

Access-list 110 deny upd any any eq 2049 log

Access-list 110 deny tcp any any eq 2049 log

Access-list 110 deny upd any any eq 4045 log

Access-list 110 deny tcp any any eq 4045 log

**! Allow all established tcp traffic, deny all other**

Access-list 110 allow tcp any any established log

Access-list 110 deny tcp any any log

**! Allow all other traffic. Needed because of Cisco explicit deny**

Access-list 110 permit ip any x.y.z.0 255.255.255.240 log

**!Deny everything else**

Access-list 110 deny ip any any

### **2.3.2 Egress ACL of Border Router Interface S0 (CISCO 3640)**

This is the ACL to control the filtering of packets leaving GIAC network.

**!Deny RFC 1918 addresses (Spoofed Addresses)**

Access-list 120 deny ip any 10.0.0.0 0.255.255.255 log

Access-list 120 deny ip any 172.16.0.0 0.31.255.255 log

Access-list 120 deny ip any 192.168.0.0 0.0.255.255 log

Access-list 120 deny ip any 224.0.0.0 31.255.255.255 log

Access-list 120 deny ip any 127.0.0.0 0.255.255.255 log

Access-list 120 deny ip host any 0.0.0.0 log

**! Allow email traffic from mail proxy**

Access-list 120 permit tcp host x.y.z.5 any eq 25 log

**! Allow access from VPN Server**

Access-list 120 permit ip host x.y.z.3 any log

**! Allow http and https access from customer proxy server**

Access-list 120 permit tcp host x.y.z.2 any eq 80 established log

Access-list 120 permit tcp host x.y.z.2 any eq 443 established log

**! Allow https and https access from internal web proxy**

Access-list 120 permit tcp host x.y.z.6 any eq 80 log

Access-list 120 permit tcp host x.y.z.6 any eq 443 log

**!Allow Norton Anti-virus server to FTP out to get updates**

Access-list 120 permit tcp any any eq ftp log

Access-list 120 deny tcp any any eq ftp

**! Allow ping from S0 interface on Border**

Access-list 120 permit icmp host x.y.z.1 any eq echo

**! Allow DNS UDP queries out**

Access-list 120 permit tcp any any eq 53 log

**! Blocking NetBIOS traffic**

Access-list 120 deny tcp any any range 135 139 log

Access-list 120 deny udp any any range 135 139 log

Access-list 120 deny tcp any any eq 445 log

Access-list 120 deny udp any any eq 445 log

**!DENY all other traffic**

Access-list 120 deny ip any any log

### **2.3.3 Ingress ACL of Border Router Interface E0 (CISCO 3640)**

On the Ethernet 0 interface of the router an ACL will be applied that will only allow certain hosts to pass, blocking all others. This is based on the private IP addresses since they have not been translated by the NAT yet.



**!Allow only internal address ranges that are allowed out to the internet**

**! External-external DNS**

Access-list 130 permit upd host 10.10.2.5 any eq 53

**! Internal-external DNS**

Access-list 130 permit upd host 10.10.4.9 any eq 53

**!Customer RPS**

Access-list 130 permit tcp host 10.10.2.2 any eq 80

Access-list 130 permit tcp host 10.10.2.2 any eq 443

**!Corporate Web Proxy Servcer**

Access-list 130 permit tcp host 10.10.9.2 any eq 80

Access-list 130 permit tcp host 10.10.9.2 any eq 443

**!Deny all other http and https requests out**

Access-list 130 deny tcp any any eq 80 log

Access-list 130 deny tcp any any eq 443 log

**!SMTP mail relay**

Access-list 130 permit tcp host 10.10.4.10 any eq 25

**!VPN Server**

Access-list 130 permit ip host 10.10.2.1 any log

**! Allow Norton Anti-Virus server FTP access**

Access-list 130 permit tcp host 10.10.????? any eq ftp log

**! Users Workstations**

Access-list 130 permit ip 10.10.9.0 255.255.255.0 any log

Access-list 130 permit ip 10.10.10.0 255.255.255.0 any log

Access-list 130 permit ip 10.10.11.0 255.255.255.0 any log

Access-list 130 deny ip any any log

### 2.3.4 “Gotcha’s”

Since all ICMP packets are filtered at the router for all internal address, the ability to ping from internal devices out to the Internet or visa versa is disabled. The only system that has this capability is the router. This becomes important to remember when connectivity issues are in question.

### 2.3.5 Testing the Router

From an external host, attempt to telnet, ping, finger the router and internal hosts.

Utilizing the nmap utility, a scan of both TCP and UDP would be performed against the x.y.z.0/28 network to verify that only the hosts with the associated ports permitted by the ACL are visible. The IDS located on the network is connected to interface Ethernet 0 of the router and will be monitored for results along with the router logs.

*Nmap -sT x.y.z.0/28*

*Nmap -sU x.y.z.0/28*

## 2.4 Primary Firewall (Checkpoint Firewall-1)

The primary firewall for GIAC will be protecting the DMZ, VPN server and the service network. The following is the security policy that will be used for the configuration of the

firewall. The format for the Checkpoint Firewall-1 rule base is .

#### **2.4.1 Firewall Rules**

Rule #: Order number for the policy, starting with 1.

Source: An object designating the source of the IP packet (an individual host, IP subnet or network)

Destination: An object designating the destination of the IP packet (a individual host, IP subnet or network).

Service: Defines the transport protocol and port to filter on (TCP, UDP, etc...)

Action: Defines what should be done to the packet (accept, deny, reject, drop, etc...)

Track: What type of logging should be done if any (long, short, alert, etc...)

© SANS Institute 2000 - 2005, Author retains full rights.

Firewall - Firewall-1 Security Policy								
File Edit View Manage Policy Window Help								
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Net-Admin	Any	FireWall1 telnet http https ftp tftp	accept	Long	Firewall-1	Any	Admin Workstation
2	Any	Firewall-1	NBT	reject		Firewall-1	Any	Reject Netbios traffic to Firewall
3	Any	VPN-Server	IPSEC	accept	Long	Firewall-1	Any	Traffic to VPN Server
4	Any	Firewall-1	Any	drop	Long	Firewall-1	Any	Block all traffic to firewall
5	Any	Cust_RPS	http https	accept	Long	Firewall-1	Any	Permit Traffic to Customer Web Site
6	Internal	DMZ-DNS	domain-udp	accept	Long	Firewall-1	Any	Allow UDP DNS queries to External-External DNS from Internet only
7	DMZ-DNS Service-DNS	Internal	dns	accept	Long	Firewall-1	Any	Allow DNS servers to Query both UDP, TCP to the internet
8	Internal	SendMail	smtp	accept	Long	Firewall-1	Any	Allow Internet SMTP servers access to GIAC SMTP server
9	SendMail	Internal	smtp	accept	Long	Firewall-1	Any	Allow GIAC SMTP server access out for port 25
10	Antivirus_Server	Any	ftp	accept	Long	Firewall-1	Any	Allow Antivirus server to FTP updates down
11	VPN-Server	Cust_RPS Partners_RPS Remote-Users_RPS	https	accept	Long	Firewall-1	Any	Allow VPN users access to RPS's
12	Cust_RPS	Cust_Web	https http	accept	Long	Firewall-1	Any	Allow Customer RPS to communicate with Customer Web Server
13	Partners_RPS	Part_Web	https	accept	Long	Firewall-1	Any	Allow Partner RPS to communicate with Partner Web Server
14	Supplier_RPS	Sup_Web	https	accept	Long	Firewall-1	Any	Allow Supplier RPS to communicate with Supplier Web Server
15	Remote-Users_RPS	GIAC_Webserver	https	accept	Long	Firewall-1	Any	Allow remote users RPS to communicate with GIAC Web Server
16	Web-Proxy	Internal	http https	accept	Long	Firewall-1	Any	Allow internal Web Proxy Server access to Internet
17	Border-Router Firewall-1 VPN-Server IDS-DMZ IDS-Router	Log_Server	syslog	accept	Long	Firewall-1	Any	Allow systems to send logging information to Log Server
18	Internal	Internal	Any	drop	Alert	Firewall-1	Any	Alert if Non-Internal host attempt to Internal host
19	Any	Any	Any	drop	Long	Firewall-1	Any	Deny anything else

Figure 2

Rule #1: Before we lock down the firewall, we must first allow GIAC network management station access to the firewall and all other hosts on the network utilizing the following protocols (firewall, telnet, ftp, tftp, http, and https). This is done to allow remote configuration.

Rule #2: Netbios is extremely chatty, and thus we will reject this. Because we are rejecting this and not dropping it, this will cause a RST to be sent to the host closing the connection instead of having it timeout. As suggested from SANS, we are not logging this traffic for it would quickly fill our logs.

Rule #3: Allow outside traffic to the VPN Server. The source is presently set to any. It would be preferable to have defined source address, but since some users utilize ISP that provide DHCP address, it may not be feasible.

Rule #4: Drops any traffic destined for the firewall. No other hosts should be communicating directly to the firewall.

Rule #5: Since customers will be accessing GIAC network via the Customer reverse proxy server, access will be granted for the protocols http and https (port 80 & 443) from the any source.

Rule #6: Allow non-internal hosts (Internet) access to the external-external Domain Name Server for UDP DNS queries. Internal hosts will not be accessing the external-external DNS to protect them from DNS poisoning.

Rule #7: Allow external-external and internal-external DNS access to non-internal network for both UDP and TCP port 53.

Rule #8: Allow SMTP traffic (email) from the Internet access to the mail relay server located on the service network.

Rule #9: Allow SMTP traffic from the mail relay server out to the Internet.

Rule #10: Allow Anti-Virus Server FTP services to download latest virus patterns from designated FTP download site.

Rule #11: Allow VPN server to the Supplier, Partners, and remote users Reverse Proxy Server on 443/TCP.

Rule #12: Allow customer's Reverse Proxy Server to access corresponding web servers.

Rule #13: Allow partner's Reverse Proxy Server to access corresponding web servers.

Rule #14: Allow supplier's Reverse Proxy Server to access corresponding web servers.

Rule #15: Allow remote user's Reverse Proxy Server to access corresponding web servers.

Rule #16: Allow internal web proxy server access to port http and https for all

destinations.

Rule #17: Allow all servers to send log information to logging server located on service network.

Rule #19 Drop and alert us for any non-internal hosts attempting to access internal hosts.

Rule #20 Lastly, everything else will be dropped.

#### **2.4.2 “Gotcha’s”**

Because we are limiting access to our external-external DNS server to only UDP, we are taking the chance that some DNS queries will fail since the max size of the packet can only be 512 bytes.

#### **2.4.3 Testing Firewall**

Running nmap utility to test the firewall. The test will verify what can be seen from one segment to the other. From the DMZ segment, the VPN, service and router segments will be checked. From the router segment, the VPN, DMZ and service segment is tested and from the service segment all others will be tested.

#### **2.5 VPN Server**

GIAC partners and suppliers will be making all connections to the GIAC’s network through a IPsec VPN tunnel. IPsec is a set of security protocols that allows for the encryption of data in a secure format. The first parameter of IPsec that needs to be determined is the security protocol that defines how the packet will be encrypted. The two choices provided under IPsec are Authentication Header (AH) and Encapsulating Security Payload (ESP). AH only encrypts the head information of the packet, leaving the payload in plain text. This protects the destination, but leaves the data accessible to being sniffed. ESP on the other hand encrypts the payload data of the packet. GIAC will be implementing ESP tunneling to provide the integrity and confidentiality of information.

In order for communication to occur between two IPsec nodes, the Security Association (SA) must be established. This is accomplished through the Internet Key Exchange (IKE) protocol. The ISAKMP method will be used to perform IKE for GIAC enterprise. SHA and MD5 message authentication are available with 3DES (168bit) encryption. Because of international laws dealing with encryption, the VPN server may need to be configured to accept lower IPsec encryption.

Remote clients will be configured with Checkpoint VPN-1 SecureClient to ensure that the corporate security policies adhered to on the remote client workstation. Secure Client will additionally protect the VPN tunnel against hackers who may compromise the remote machine.

Additionally, PKI certificates will be issued to both the partners and suppliers to ensure

additional data security and users authentication when accessing GIAC web servers. All connections will be made utilizing https.
















No.	Source	Destination	Service	Action	Track
1	 Partner@Any	 Partners_RPS	 https	 Client Encrypt	 Long
2	 Supplier@Any	 Supplier_RPS	 https	 Client Encrypt	 Long
3	 Remote_User@Any	 Remote-Users_RSP	 https	 Client Encrypt	 Long

Figure 3

Selecting Encrypt in the action column for the VPN connections we can edit the various VPN's properties.

Key Management: ISAKMP/OAKLEY  
 Encapsulation: Encryption + Data Integrity (ESP)  
 Encryption Algorithm: 3DES  
 Data Integrity: MD5 and SHA

Telecommuters and small offices without VPN servers:

We will be using Secure Remote to facilitate our client to site VPNs. On the firewall side we need to create users accounts and define the authentication method to be used. With Checkpoint Secure Client, rules will be verified and configure if necessary the remote users machine encryption policy.

### **Assignment 3 - Audit Your Security Architecture**

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

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

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

#### **3.1 Planning the Assessment**

The purpose of assessing the GIAC network is to verify that the router and firewall are properly configured to protect GIAC network by allowing only authorized network traffic. Because of potential impact on network performance, and possibly some host systems, written approval from GIAC Corporate must first be signed in order to run the audit against the GIAC network. Any security holes will be identified with corresponding fixes if possible.

Since GIAC is a 7/24 shop, a suitable time must be determined that will least affect customer access. To determine the timeframe of least usage, we must analyze the transaction logs from both the database server and the customer web server to develop a usage trend. After studying the trend, it was determined that the optimum time to perform the audit is between the hours of 12:01 am and 5:00 am Sunday morning. Suppliers and partners will be informed of the down time so business is least effected. No posting will be made to the general public because it may invite unwanted hackers to the site.

Because of the potential but unlikely event of a system crashing or any other unforeseen problems from the various tests, in addition to the audit team, a system administrator for each host and system engineers need to be present. To estimate the potential costs of this assessment, we need to tally the overtime pay for 5 hours for each of the system engineers and administrators. Additional money will be needed to pay for the two weeks needed to compile the data and create the final report.

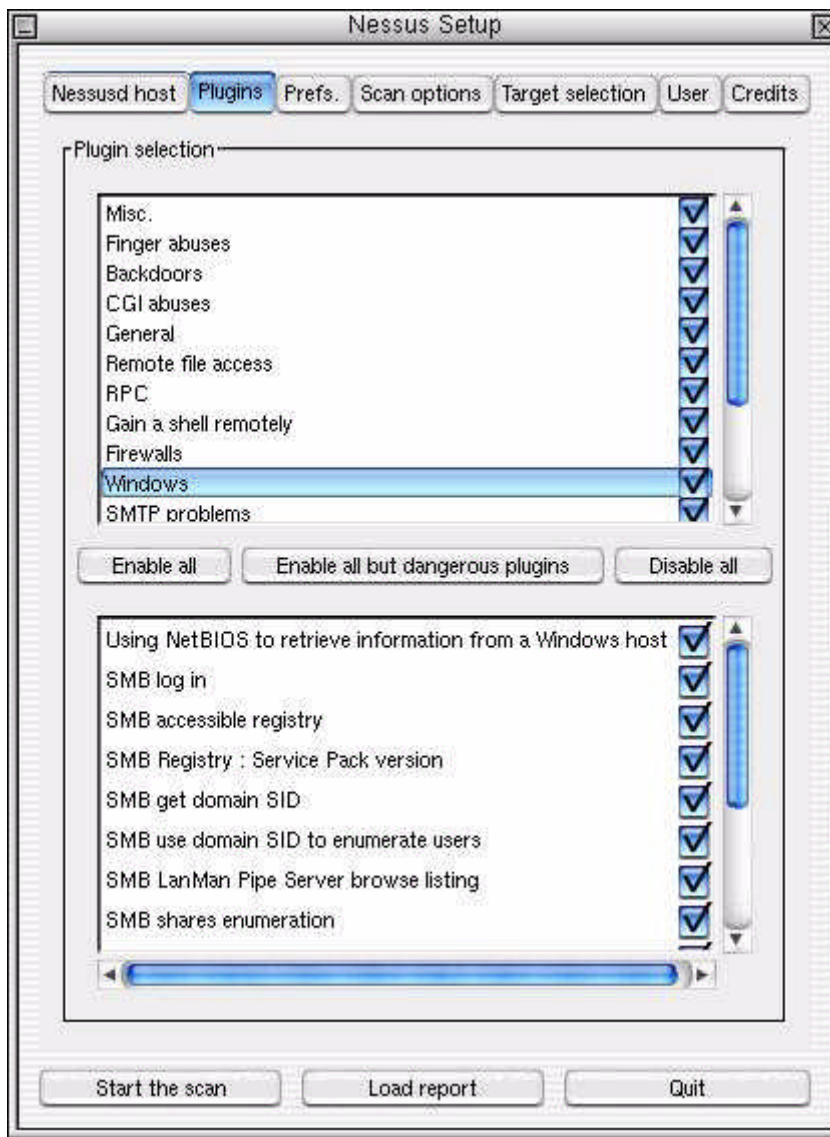
A laptop installed with Red Hat 7.0 with the latest security patches will be used to perform the internal audit. Utilizing a laptop allows the flexibility of moving from one network segment to another without the need to transport heavy and bulky equipment. Additional testing will be performed from a machine located outside of GIAC network to test the routers ACL's and firewall rules against an outside source.

The software that will be used to perform various tests against GIAC network will be Nessus and tcpdump. The nmap utility along with various DNS tools will not be used because they are incorporated in the Nessus program as plug-ins. Nessus (<http://www.nessus.org>) is a free security scanner to audit remote networks for various vulnerabilities. The software utilizes a plug-in architecture, that is each security test is written as a external plug-in and can individually added, thus allowing you to customize your testing. Updates are done on a daily basis and can easily be downloaded from their website. Nessus tests vulnerabilities on standard and non-standard ports, has good reporting features and provides you with a fix to any potential security holes it finds.

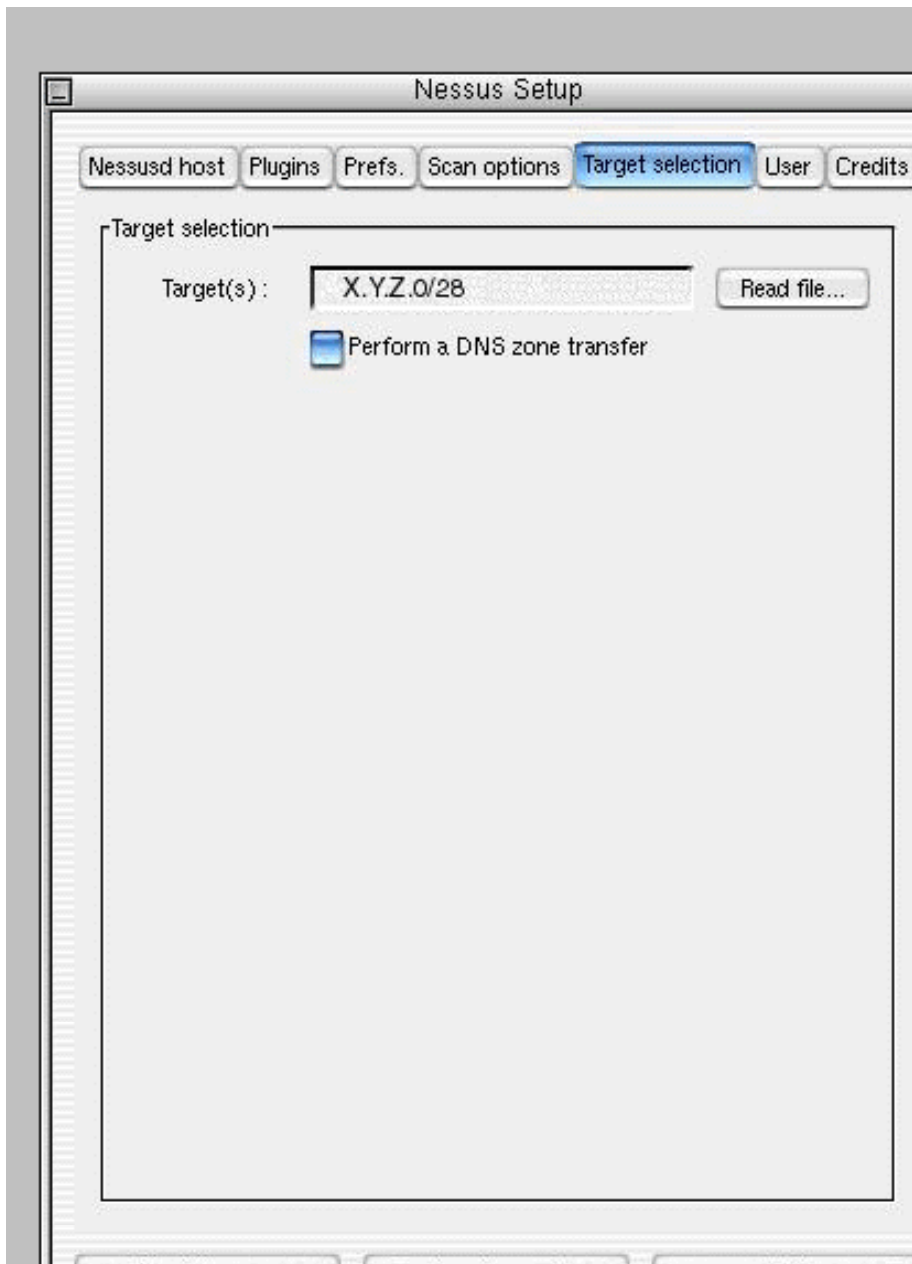
Nessus has two parts, sever and client. The server runs on a unix host while the client can be installed on either a unix or windows host. In our case both will be installed on the same system. Once the server is installed the client then needs to be configured to select which of the tests will be performed.

© SANS Institute 2000 - 2005, All rights reserved.





Note: One of the tests performed by Nessus is a Denial of Service attack test. This is a touchy and sensitive issue in the use of this test. The potential of systems crashing is a likely possibility. It was determined after meeting with management that this test would not be performed at this time. Later, in a lab situation, separate hosts will be similarly configured as the various live systems. The DoS attacks will then be run against the test hosts. In case of a system crash, they can be reloaded and appropriate fixes can then be determined. Once done, the live systems will be updated accordingly.



Targets can be specified either by individual host addresses or by the IP subnet. Note that a DNS transfer option is available. This will be selected when testing GIAC DNS servers to verify that the transfer is denied.

TCPdump program, which is currently running on the companies IDS systems, will be used to verify that no unexpected network traffic is traversing the network. Additionally, we will verify that the traffic that is intended to be encrypted actually is.

### 3.2 Implementing the Assessment

The assessment will start from outside the GIAC network. This will be accomplished by establishing a dial up connection with the local ISP. The workstation will utilize the Nessus program to port scan the subnet x.y.z.0/28, attempting to discover any potential vulnerability, and verifying that only allowed hosts with associated ports are visible. Additionally, we will also test the DNS to verify that zone transfers access lists are properly configured, allowing no zone transfers to non-authorized DNS.

From each network segment, the workstation will run testing against all the other segments, checking for vulnerabilities and verifying the ACLs and firewall rules. Any variation to this will be documented in the assessment report along with appropriate steps to correct the problem.

All hosts will be inspected to verify that they have the latest security patches available for the respective operating system and that the anti-virus software is up to date. Additionally, the individual hosts OS will be checked to verify that they have been hardened. Appropriate white papers and tools are available from the respective OS manufacturers (Redhat and Microsoft) for this issue.

The mail relay host will be tested to verify that it is properly configured to quarantine all email that contain viruses in addition to attachments ending in either \*.vbs or \*.exe, since these are the vehicles that are utilized to carry viruses. Additionally, the relay host will be checked to ensure that anti-spamming features are enabled.

Once the router and firewall ACL's have been tested and verified, the next set of tests to be run will be directed toward user's security. Since the internal systems are Windows NT servers, the systems user password will be checked for ease of cracking. The L0phtCrack program (<http://www.atstake.com/research/lc3/index.html>) will be utilized to perform password auditing on the corporate NT accounts. All accounts that the passwords were cracked will be locked until the effected user can be notified to change their password problem.

### 3.3 Recommendations

Once the assessment was performed and all of the logs were compiled for examination. No major problems were noted, but some minor configuration issues were noted.

The Nessus software did bring to light that some of the corporate server did not contain all the necessary security patches that were previously thought to have. The needed patches were applied to these systems. It was found that no logbook existed for each server that specified what and when patches were installed. It is recommend that such a log book be created and that a designated person be tasked to daily check security sites for new patches and vulnerabilities to ensure that the systems are well protected.

Additionally, it was found that FTP protocol was allowed out of the GIAC network with out any limitations to the destination. Since the only requirement for ftp within the network was for the anti-virus server to download updates to the virus detention pattern file, it would be prudent to restrict FTP destination to the Symantec FTP site. The modifications to both the router egress and the firewall ACL would be the following:

Router ACL modification:

Access-list 120 permit tcp any {ip address for Norton Anti-virus ftp site} eq ftp log

Firewall rule modification:



The corporate NTP server was located on the internal network. This server is to provide the time for the entire network to ensure that all of the system logs are all time synchronized. The external firewall was missing the rule to allow the NTP protocol to the internal network. It may be more secure to move the NTP server from the Internal network to the Service network. This is corrected by adding the following rule.



GIAC utilizes IDS's through its network for the purpose of detecting possible intrusions. The task of analyzing the various logs from these systems takes very qualified individuals and is additionally very labor intensive. It may be cost effective to take this function and outsource it to a managed security services provider (MSSP).

## Assignment 4 - Design Under Fire

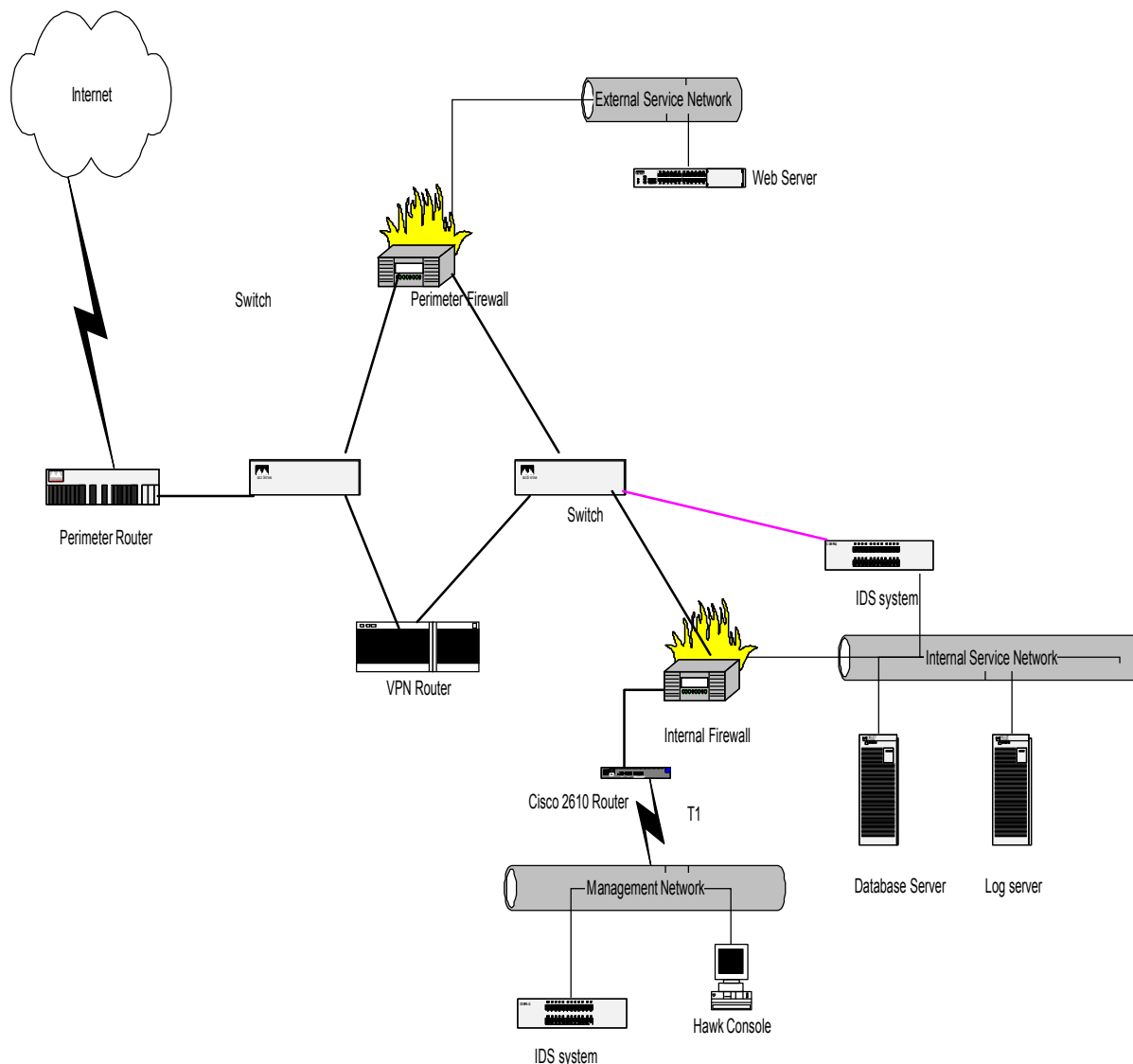
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

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

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

© SANS Institute 2000 - 2005, Author retains full rights.

The network design that was selected for the attacks is Tamara Bowman  
[http://www.sans.org/y2k/practical/Tamara\\_Bowman\\_GCFW.doc](http://www.sans.org/y2k/practical/Tamara_Bowman_GCFW.doc). Below is the network design.



#### 4.1 Firewall Attack

Tamara is using a Cisco Pix 525 with IOS ver 5.3(1) for her external firewall with SSH being used for a secure telnet session. A quick search of Cisco website finds a multiple SSH vulnerability with this configuration. The weakness in the SSH protocol that allows the possibility to insert arbitrary commands into an established SSH session, and retrieve information which can be helpful in a brute force key recovery.

The SSH vulnerabilities actually consists of three separate vulnerabilities and as described

on Cisco web site (<http://www.cisco.com/warp/public/707/SSH-multiple-pub.html>) they are as follows:

1. CRC-32 integrity checks vulnerability: This attack is only successful if an attacker possess one or two known ciphertext/plaintext pairs. According to the document describing the vulnerability, this is not difficult due to the fact that very session starts with a greeting screen, which is fixed, and which can be determined. The hacker must be able to sniff the session and collect the corresponding ciphertext. This allows the hacker to insert arbitrary commands in the session, once it has been established.
2. Traffic analysis: For this vulnerability, you must be able to capture packets. The exact length of the password used for login authentication is exposed and can significantly help an attacker in guessing the password using the brute force attack.
3. Key recovery in SSH protocol: Once again the attacker must to sniff the SSH session and be able to establish a connection to the SSH server. This could lead to the compromise of the session key. Once the session key is determined, the attacker can proceed to decrypt the stored session using any implementation of the crypto algorithm used, revealing all information in an unencrypted form.

#### **4.2 Denial of Service Attack. (DoS)**

Denial of Service attacks come in many different forms. The objective of the attack is to deny the end user of some sort of service. This could be anything from access to files (data), to a particular system, or to the Internet. One method is to make a system or resource unavailable by causing it to fail and roll over. This could be accomplished by exploiting known vulnerabilities in the underlining operating system, or causing the resources to be used up so that the system crashes, shuts down or reboots. Another form is to degrade the performance of the system or network to a point were it becomes painfully slow and unusable. Yet, another is to break into a system and destroy, or modify data that makes it unusable to the end user.

For the ICMP type DoS attacks, the most efficient method of prevention this do block all ICMP packets at the boundary router. As describe in section 2.1.11, the router can additionally be configured to help prevent the TCP SYN attacks by enabling TCP Intercept mode. This will intercept the packets and wait until the three-way handshake is done before allowing the connection to the designated host.

Knowing that the boarder router is Cisco 7505 running IOS 12.0(5), a little research is done to find any exploits that could be used against the router to cause a DoS attack. Two attacks were discovered to cause the router to crash.

The first to be discovered as described on Cisco's web site (<http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml>) concerns the HTTP service. In the

configuration of the router there was no command to disable this service, we are going to assume that it is enabled. By browsing to the url of the router: <http://<router-ip>/%%>, this will cause the router to halt and reload. If this is done on a continuous basis, the router will continue to roll over and deny and inbound and outbound traffic to pass. The fix for this is to upgrade the IOS to version 12.2 or greater, disable http service, or applying an access-list to prevent access to port 80 on the router.

The next attack is a telnet handling option vulnerability. As described at Cisco web site (<http://www.cisco.com/warp/public/707/iostelnetopt-pub.shtml>), there exists a defect in the IOS software that will cause the router to unexpectedly reload when being scanned for two Unix based vulnerabilities with security scanners. This happens when the scanning program is asserting the Telnet ENVIRON option, #36, before the router indicates that it is willing to accept it, and thus causes the router to reload. When done on a repeated basis, this will cause a DoS attack. The fix is to upgrade to software greater or equal to version 12.0 (8)

### **4.3 Internal System Attack**

Before any attack on internal systems can be performed, the hacker must first interrogate the network in an attempt to determine what the server's operating system is. This can be accomplished with such tools as nmap. The new version has a GUI interface and is extremely easy to run. Since the internal configuration is already known, this enables us to attack the system with less effort.

The operating system that Tamara used through the network is Sun Solaris. Searching the Internet, multiple vulnerabilities were found that would allow us to gain root access to the operating system. On this is accomplished, other systems can be compromised and allowing us access to the internal firewall, database server along with the log server. Once the log server has been compromised, the logs can be deleted to cover up our tracks.

To begin, we must break into the network in order to compromise the internal systems. Going on the assumption that since all of the systems are running Solaris, the DNS server probably is running the same OS. Bind has always been plagued with security holes and researching this, some were found <http://www.cert.org/advisories/CA-2001-02.html>. Once root access is gained, the DNS can be used as a launch point to compromise the other systems. The next three vulnerabilities can be used to accomplish this task. Since the internal firewall is running on top of Solaris, we should be able to do the same thing to it.

The first vulnerability that we will exploit is the Simple Network Management Protocol (SNMP) to Desktop Management Interface (DMI) Mapper Daemon (SNMPXDMID). As stated in Cert Advisory CA-2001-05 (<http://www.cert.org/advisories/CA-2001-05.html>) this daemon is susceptible to a buffer overflow, which could allow an intruder to gain root level access. Once this is achieved, the system can be used to leap frog to other hosts; sensitive internal corporate data could be extracted, and in this case fortune cookies sayings and more important, customers credit card information. Steps to prevent this are to turn off DMI and to remove all permissions from the daemon.



The next vulnerability exists in Solaris remote printing process. As stated in Cert CA-2001-26 (<http://www.cert.org/advisories/CA-2001-26.html>), this process is also vulnerable to a buffer overflow that could lead to a local or remote root compromise, allowing the intruder to crash the printer process and gain root level access. Steps to prevent this are to disable the print server, enable the noexec\_user\_stack tunable, and to block access to 515/tcp at the router and firewall.

The third vulnerability that was found exists in the sadmind program that uses RPC to remotely perform distributed system administration operations. As stated in vulnerability note VU#28934 (<http://www.kb.cert.org/vuls/id/28934>), a buffer overflow can overwrite the stack pointer running inside of the sadmind process and allow the intruder to execute arbitrary code with root level privileges. Steps to prevent this are to install latest patches for this vulnerability, and to harden the system. If this function is not needed, then sadmind should be disabled. If the function is needed, the security level to authenticate requests should be set to Strong. In addition, the access should be blocked for port 111/tcp & udp at the router and firewalls.

© SANS Institute 2000 - 2005, Author retains full rights.

## References:

The SANS Institute: Track 2 – Firewalls and Intrusion Detection. Volume 2.1 – 2.5  
(Rocky Mountain SANS)

Cisco IOS Software Command Summary, Release 11.1, San Jose, CA: Cisco Systems, Inc

## Web Sources:

Esperanza Lopez-Wilkin. “Managed Security Services: an IDS solution”, May 20, 2001  
URL: <http://www.sans.org/infosecFAQ/intrusion/mss.htm>

Check Point Resource Library – URL: <http://cgi.us.checkpoint.com/rl/resourcelib.asp?state=2#VPN>

Network Computing article about firewall comparisons. URL:  
<http://www.networkcomputing.com/shared/printArticle?article=nc/1106/1106f1full.html&pub=nwc>

Nessus scanner – URL: <http://www.nessus.org>

Cisco product information and configuration guides – URL: <http://www.cisco.com>

Other Security Sites Utilized. URL:

<http://www.sans.org>  
<http://infosec.navy.mil>  
<http://www.cert.org>  
<http://www.cisco.com>  
<http://www.sun.org>