# 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 permited without express written permission.

# GIAC LevelTwo Firewalls, Perimeter Protection, and VPNs

Practical Assignment
for Capitol SANS

Submitted by:

Dennis Webb

February 20, 2001

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

# Table of Contents


**INTRODUCTION** ..... **3**

**ASSIGNMENT 1 – SECURITY ARCHITECTURE** ..... **3**

CISCO 3620 ROUTER ..... 3
AXENT RAPTOR FIREWALL WITH POWERVPN ..... 5
AXENT RAPTORMOBILE ..... 5
ISS REALSECURE NETWORK SENSOR ..... 6

**ASSIGNMENT 2 – SECURITY POLICY** ..... **6**

CISCO 3620 ..... 7
Router Commands ..... 7
Access Lists ..... 8
Tip, Tricks, and Gotchas ..... 10
AXENT RAPTOR FIREWALL WITH POWERVPN ..... 10
Firewall Rule Base ..... 11
Tip, Tricks, and Gotchas ..... 13
VPN ..... 13

**ASSIGNMENT 3 – AUDIT YOUR SECURITY ARCHITECTURE** ..... **14**

PLANNING THE ASSESSMENT ..... 14
IMPLEMENT THE ASSESSMENT ..... 15
CONDUCT A PERIMETER ANALYSIS ..... 18

**ASSIGNMENT 4 – DESIGN UNDER FIRE** ..... **19**

FIREWALL ATTACK ..... 20
DENIAL OF SERVICE ATTACK ..... 20
INTERNAL SYSTEM COMPROMISE ..... 21

**REFERENCES** ..... **22**



© SANS Institute 2000 - 2002, Author retains full rights.

## Introduction

GIAC Enterprises is an Internet startup company that is in the business of selling fortune cookie sayings online. In today's economy, e-business is a growing industry full of promise, but new dotcom companies are being viewed with trepidation from investors. While GIAC Enterprises expects to earn $200 million yearly, it is anticipated that the initial budget will be tight. It is also anticipated that the initial Information Technology department will be staffed by only a few members, therefore management considerations must also be taken into account as the security architecture of the network is defined. These assumptions are carried throughout the assignments that follow.

## Assignment 1 – Security Architecture

GIAC Enterprises will gain its revenue from it online customers. The customers will access GIAC Enterprises public Internet web servers on the Service network and perform their transactions online. Therefore, Internet access must be fast or the companies that buy bulk online fortune cookie sayings will look elsewhere for their purchases. GIAC Enterprises must also cater to their suppliers and partners with different access methods. The suppliers who write the fortune cookie sayings will access the web servers located on the Extranet network. GIAC Enterprises' partners that translate and resell the fortune cookie sayings will be allowed VPN access to the Extranet network. With these differing access methods in mind, it is apparent that the overall security architecture for GIAC Enterprises must be strong, but still stay within the means of the initial operating budget constraints. Figure 1 illustrates the security architecture for the perimeter defense and the layout of the network. *(Axent Technologies has recently merged with and become a wholly-owned subsidiary of Symantec Corporation. For purposes of this document Axent will be used to refer to the vendor of the security products.)*

### *Cisco 3620 Router*

The Cisco 3620 router will be the border router and provide connectivity from the GIAC Enterprises' network to the Internet community. The Cisco 3620 will be implemented with a number of filters in place to block unwanted Internet traffic from ever getting to the Axent Raptor Firewall. With this in mind, the router has to have the horsepower to execute the defined ACLs without becoming a traffic bottleneck itself. The Cisco 3620 has an 80 MHz RISC processor, which will supply this horsepower. The router will not be implemented with the Firewall Feature Set. This would add additional overhead to the router and duplicate the functions provided by the Axent Raptor Firewall. The router will be directly connected to the Universe interface of the firewall via a crossover cable. This eliminates the possibility of any device being added to the GIAC Enterprises' network that is outside of the firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

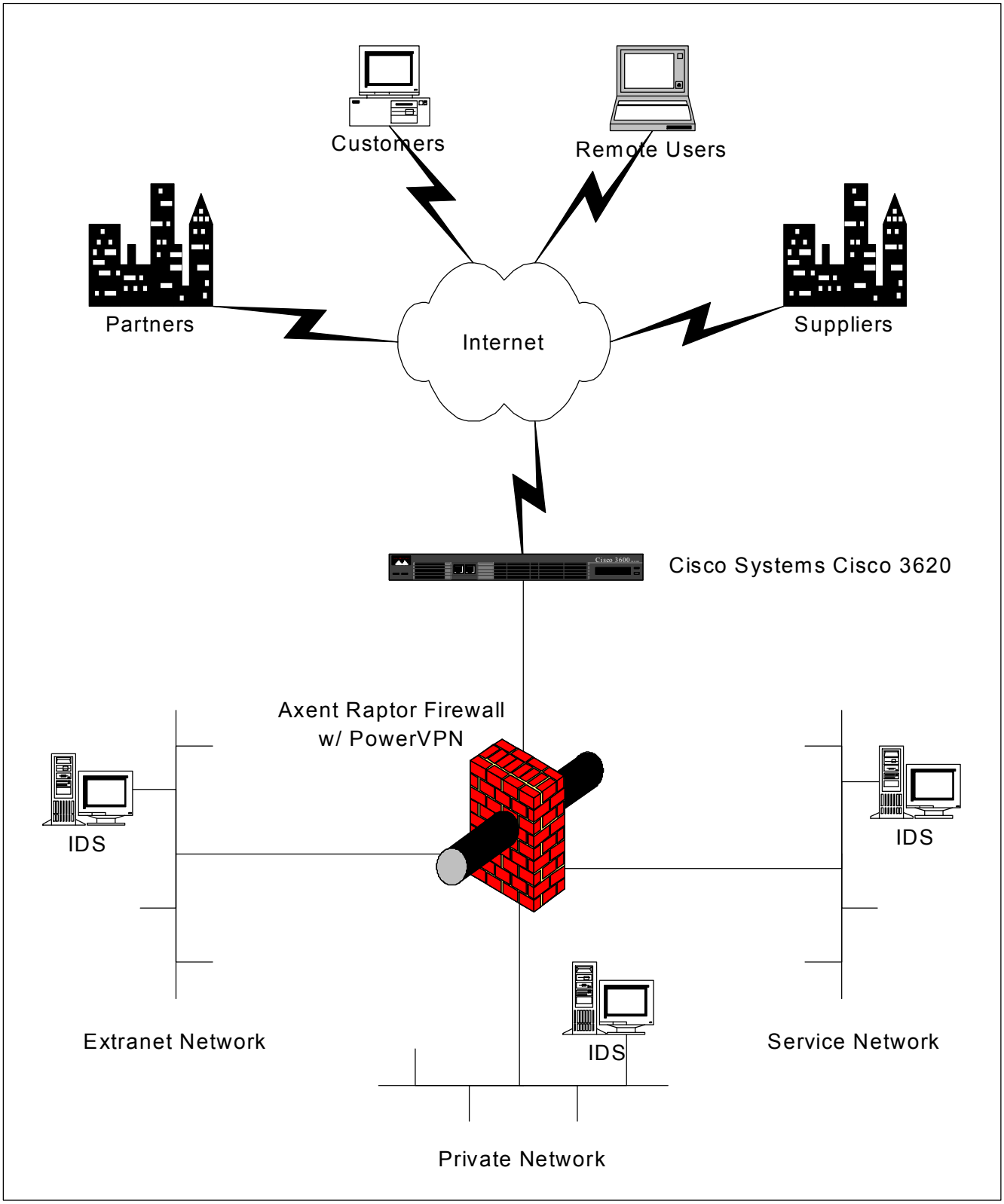


**Figure 1 - GIAC Enterprises Security Architecture**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

### *Axent Raptor Firewall with PowerVPN*

The core of the security architecture for GIAC Enterprises is an Axent Raptor Firewall with PowerVPN. The current version is 6.5. The Axent product will control many of the services required by the GIAC Enterprises design – including perimeter protection, VPN access to partners, secure remote access, protection of the private network – while conforming to the budgetary and management constraints. Raptor Firewall implements application proxy technology to scan packets through all seven layers of the OSI model. Raptor Firewall will operate as the network address translation (NAT) device in the GIAC Enterprises network. The PowerVPN option allows for VPN connections to remote offices and users utilizing standards-based encryption – IPSec, X.509, LDAP, and Triple DES.

Due to the knowledge of the administrators, Raptor Firewall will be run on a Microsoft Windows NT platform. It can be either Windows NT 4 Workstation or Server. Raptor Firewall automatically hardens the Windows operating system and utilizes an internal "vulture" program to disable any services that are not explicitly permitted to be running. If NT Server is installed, Raptor Firewall will turn off the unneeded services and essentially turn it into NT Workstation.

The server hardware must be robust in order to handle the demand placed upon it from the Raptor Firewall software. It will contain a fast processor and a large amount of memory. The internal hard drives will also be implemented in a RAID 5 array for fault tolerance and sufficient capacity for storing log files. The firewall will have four network interface cards installed to create four separate networks. These are the Universe, Service, Extranet, and Private. The Universe network is the connection between the border router and the firewall. The Service network will contain the public web servers and other public accessible devices. The Extranet network will contain the web servers and devices accessible by GIAC Enterprises' suppliers and partners. The Private network is GIAC Enterprises' internal network. The Service, Extranet, and Private networks will implement switch technology. While this does produce more efficient use of the available bandwidth, the switches can also control passive attacks since each port operates as its own collision domain. If at any time performance demands it and the budget is available, a second Raptor Firewall can be installed utilizing Radware's Fireproof hardware to load balance traffic across the two firewalls.

### *Axent RaptorMobile*

Secure remote access for GIAC Enterprises employees will be allowed via use of Axent's RaptorMobile software. RaptorMobile is a VPN client that provides secure connections from remote laptops and desktops across the Internet to the Raptor Firewall running PowerVPN. RaptorMobile is IPSec compliant and supports both exportable DES and Triple DES encryption protocols. Any GIAC Enterprises remote user that has access to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the Internet and has the client software installed will have secure access back to the headquarters' network. This includes field staff who travel internationally to work with existing partners or recruit new ones. RaptorMobile also includes a personal firewall, which will further protect the integrity of the data traversing the VPN connection. RaptorMobile licenses come bundled with the Raptor Firewall with PowerVPN thus providing secure remote access within GIAC Enterprises' limited budget. Management over network access is controlled at the Raptor Firewall console through the same interface as the firewall itself, easing the administrative burden on the IT staff. As GIAC Enterprises grows and the security needs and budget change, there are additional products and services that can be added to the network. The authentication method for secure remote access can be strengthened to support the use of tokens. These can be hard or soft tokens depending on the needs of the security policy.

### *ISS RealSecure Network Sensor*

Intrusion detection systems (IDS) will play an important role in the GIAC Enterprises network. Since the organization's lifeline is Internet access, the integrity of the network cannot be compromised. Network intrusion detection will be utilized on the three network segment protected by the firewall – Service, Extranet, and Private – to examine the packets traversing these networks and identify unauthorized access, misuse, and abuse by both external hacker and internal saboteurs. Internet Security Systems' RealSecure Network Sensor will be running on a dedicated workstation on each of the three networks. A third party product was chosen over Axent's own NetProwler product to introduce diversity into the security architecture. The use of too many products from a single vendor can lead to a security hole that crosses all security devices and an opening for a hacker to exploit.

## Assignment 2 – Security Policy

Once the security architecture for GIAC Enterprises is designed, it must be configured correctly during the implementation phase to yield the maximum security benefit. To do so, security policies should be written that incorporate the correct balance between access and security for GIAC Enterprises to be protected and profitable. GIAC Enterprises complete security policy should contain at least the following topics:

- Usage Policy Statements
- System Backups
- Anti-Virus Programs
- Incident Handling and Response
- Audits
- Confidentiality

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The sections below discuss the security policies for the Cisco 3620 router, Axent Raptor Firewall, and PowerVPN configurations. Figure 2 names the interfaces on the firewall and the network addresses to be used by each network.

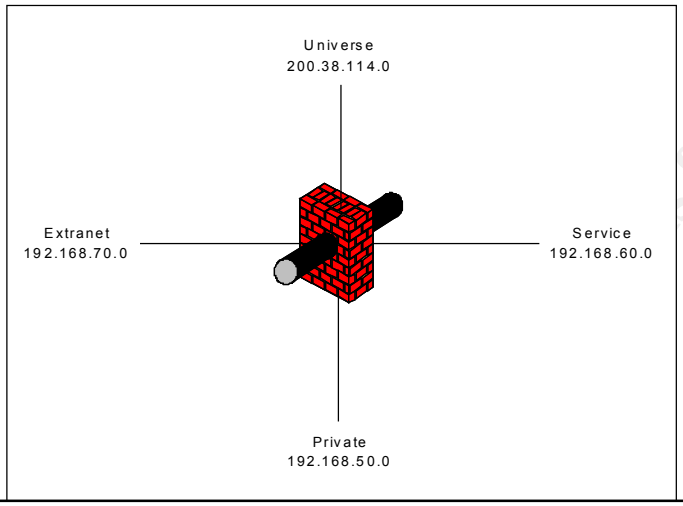


**Figure 2 -- Interface Names and IP Addressing**

### *Cisco 3620*

The Cisco 3620 router is the connection point to the Internet and therefore, should be configured as the first layer of perimeter defense for the GIAC Enterprises network. Access to it should be secured and access through it should be limited. The router's security policy should not constrain the router, but compliment the firewall. By default, the router allows all traffic to pass through it.

*Router Commands*

The following table shows the commands to enter to secure the Cisco router and a description of what each command does.

| Command | Description |
|---|---|
| line console 0<br>login<br>password 4Access | Configure the case-sensitive password "4Access" for console access to the router. By default, there is no password. |
| enable secret giac-ent | Configure the password "giac-ent" for privileged mode access to the router. |
| service password-encryption | Stores passwords in an encrypted manner so anyone performing a write terminal and show |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

| | |
|---|---|
| | configuration will not be able to see passwords in clear text. |
| line vty 0 4<br>login<br>password 4remote | Configure the password "4remote" for telnet access to the router on the maximum five virtual terminal ports. |
| banner login | Insert a banner that informs unauthorized users that their use is in fact unauthorized and unlawful. |
| no service udp-small-servers<br>no service tcp-small-servers | The small services – echo, chargen, and discard – are disabled by default in Cisco IOS 12.0 and later, but it doesn't hurt to ensure they are disabled. If enabled, they can contribute to releasing DNS information to an attacker. |
| no service finger | Disable the finger service, which could be used to find out which users are logged into a network device. |
| no ntp enable | Unless Network Time Protocol is to be used, it is an unneeded service that could be used as a path of penetration. |
| no cdp running<br>no cdp enable | Cisco Discovery Protocol allows any system on a directly connected segment to learn that the router is a Cisco device, determine the model number, and the IOS version being run. |
| no ip source-route | IP source routing is almost never used for legitimate purposes and can sometimes be used to transport packets to parts of the network from which they should be blocked. |
| no ip directed-broadcast | Directed broadcasts can be used to multiply the power of denial-of-service attacks and should be disabled on any interface where they're not actually needed. |
| no snmp | Unless GIAC Enterprises actually plans to use the information provided by SNMP, the service should be disabled. If enabled, it should be governed by access lists and inobvious community names. |
| no ip http<br>no ip bootp | Disable unused server services. |
| no ip unreachables | Prevents the router from distributing information based on ICMP error messages. |

*Access Lists*

Access lists are packet filters that define a set of criteria used by the Cisco router when it examines the packets passing through its interfaces. The router uses these lists to determine whether to forward the packet or block it based on the rules defined in the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

access lists. All routed protocols can be controlled in this way, with separate access lists for each type of protocol. One point to remember here is the Cisco 3620 router is not the firewall and should not be configured with extensive access lists that will make it a bottleneck in the flow of packets. Access lists need to be created carefully to avoid. They compare packets using top-down processing so as soon as a match is found, the packet is handled accordingly. Also, there is an implicit deny all statement at the end. The following access lists should be configured for GIAC Enterprises.

Anti-spoofing is especially critical on any interface that faces the Internet. Anything not explicitly assigned to the internal net is assumed to be on the Internet, but under no circumstances should any system accept internal source addresses on packets originating outside the internal network. Anti-spoofing entails checking that incoming packets do not have source addresses that claim to be from GIAC Enterprises own network, reserved loopback addresses, unregistered addresses (RFC 1918), multicast addresses, or the source address is left blank. Such packets are always the result of a deliberate attack or a misconfiguration. The following ingress filter should be applied to the serial port of the Cisco 3620 router.

```
interface serial 0
        ip access group 101 in

access-list 101 deny ip 192.168.50.0 0.0.0.255 any          Deny internal addresses
access-list 101 deny ip 192.168.60.0 0.0.0.255 any          Deny internal addresses
access-list 101 deny ip 192.168.70.0 0.0.0.255 any          Deny internal addresses
access-list 101 deny ip 127.0.0.0 0.255.255.255 any         Deny Loopback
access-list 101 deny ip 0.0.0.0 0.0.0.0 any                 Deny Blank
access-list 101 deny ip 10.0.0.0 0.255.255.255 any          RFC 1918 Private Network
access-list 101 deny ip 172.16.0.0 0.15.255.255 any         RFC 1918 Private Network
access-list 101 deny ip 192.168.0.0 0.0.255.255 any         RFC 1918 Private Network
access-list 101 deny ip 224.0.0.0 31.255.255.255 any        Deny Multicast
access-list 101 deny ip 255.255.255.255 255.255.255.255     Deny Broadcast
access-list 101 permit ip any any
```

Access list 102 controls what packets can be received from the private Ethernet interface and forwarded on to the serial interface to go out the Internet. It is important to check that the IP packets coming from the GIAC Enterprises network have source addresses consistent with the network. This precaution avoids spoofed addresses from being transmitted from the internal network and problems that could be caused by accidental misconfiguration. The following egress filter should be applied to the Ethernet port of the Cisco 3620 router.

```
interface ethernet 0
        ip access group 102 in

access-list 102 permit tcp 200.38.114.0 0.0.0.255 any       Public Address
access-list 102 deny ip any any log-input
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The log-input at the end of the deny statement will log any packet that is sent with a source address other than the ones permitted and will add the MAC address of the device that sent the packet. This information will be necessary to follow up and trace why this activity is occurring.

*Tip, Tricks, and Gotchas*

The following are points that should be kept in mind by GIAC Enterprises administrative personnel regarding the Cisco 3620 router implementation.

- Service password-encryption for the router is helpful, but it is a simple Vingenere cipher and can be easily compromised and should not be considered secure.

- Use enable secret to set the privileged mode password, instead of enable password, because it uses MD5 for password hashing.

- Do not distribute the router configuration file because the service password-encryption can be broken and enable secret is subject to dictionary attacks.

- It is always important to stay on top of software updates and fixes. Cisco IOS software is no different. Cisco posts its security advisories and other security information at http://www.cisco.com/warp/public/707/advisory.html. GIAC Enterprises administrators should visit this site regularly.

- Applying access lists on a Cisco may have a performance impact. GIAC Enterprises administrators should monitor the CPU and Memory usage before and after applying the filters to determine any impact. This can be done by using the show proc cpu command.

- Never change the access lists on the router interface you are using to configure the router. Either remove the access-group first or configure the router via the serial console interface. If you do not remove the access-group from the interface first, you will cause a momentary outage while installing the new access list and may disable all traffic through the interface if you make an error (plus inadvertently disconnect your telnet terminal session from which configuration changes are being made.)

### *Axent Raptor Firewall with PowerVPN*

Since GIAC Enterprises' business depends on the Internet, it is critical to align the security access with business needs. Since the requirements of the e-commerce system are not currently known, the security policy for the firewall will have to follow what traffic is expected to sustain customer relations, supply chain management, and partner collaboration.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

*Firewall Rule Base*

By default, no traffic is permitted in or out of any interface on the Raptor Firewall when it is initially installed. Ports must be opened and rules assigned in order for packets to pass through the firewall. Once the interfaces have been named, the security policy for the firewall portion of the Raptor Firewall is described in the following steps.

1. **Universe access to the Service network:** Allow anyone on the Internet to connect to the public web server on the Service network at internal IP address 192.168.60.6 and public IP address 200.38.114.6. This scenario allows outside users both unsecure and secure access to view GIAC Enterprises' web pages and download (via HTTP) files that the company has posted for outside availability. The firewall is providing the translation of the IP address. Also, allow all systems to send mail to the GIAC Enterprises mail server located on the Service network at IP address 192.168.60.5.

| Service | Port | In Via | Out Via | Source | Destination |
|---|---|---|---|---|---|
| http | 80 | Universe | Service | any | 192.168.60.6 |
| https | 443 | Universe | Service | any | 192.168.60.6 |
| smtp | 25 | Universe | Service | any | 192.168.60.5 |

2. **Universe access to the Extranet network:** Suppliers will be allowed unsecure and secure access to the web server on the Extranet network. Prior to access, suppliers will have to authenticate with an id and password to the firewall. Access is through a different URL than the public web server.

| Service | Port | In Via | Out Via | Source | Destination |
|---|---|---|---|---|---|
| http | 80 | Universe | Extranet | any | 192.168.70.6 |
| https | 443 | Universe | Extranet | any | 192.168.70.6 |

3. **Universe access to the Private network:** No direct access is allowed from the Internet to the private network.

4. **Service network access to the Private network:** No access to the Private network is allowed to originate from the Service network.

5. **Service network access to the Extranet network:** No access to the Extranet network is allowed to originate from the Service network.

6. **Service network access to the Universe network:** The mail server is the only device on the Service network that is allowed to send traffic to the Internet.

| Service | Port | In Via | Out Via | Source | Destination |
|---|---|---|---|---|---|
| smtp | 25 | Service | Universe | 192.168.60.5 | any |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7. **Extranet network access to the Private network:** No access to the Private network is allowed to originate from the Extranet network.

8. **Extranet network access to the Service network:** The Extranet network is allowed both unsecure and secure access to the web server on the Service network. This allows GIAC Enterprises' partners and suppliers to access the public web pages after they have authenticated to the firewall.

| Service | Port | In Via | Out Via | Source | Destination |
|---|---|---|---|---|---|
| http | 80 | Extranet | Service | 192.168.70.6 | 192.168.60.6 |
| https | 443 | Extranet | Service | 192.168.70.6 | 192.168.60.6 |

9. **Extranet network access to the Universe network:** No access to the Internet is allowed to originate from the Extranet network.

10. **Private network access to the Service network:** Allow unsecure and secure access from the Private network to the public web server for viewing, testing, and updating web pages. Allow inside users to connect to the mail server to pick up their mail and to Telnet to it for administration.

| Service | Port | In Via | Out Via | Source | Destination |
|---|---|---|---|---|---|
| http | 80 | Private | Service | any | 192.168.60.6 |
| https | 443 | Private | Service | any | 192.168.60.6 |
| ftp | 21 | Private | Service | any | 192.168.60.6 |
| smtp | 25 | Private | Service | any | 192.168.60.5 |
| telnet | 23 | Private | Service | any | 192.168.60.5 |

11. **Private network access to the Extranet network:** Allow unsecure and secure access from the Private network to the partner and supplier web server for viewing, testing, and updating web pages.

| Service | Port | In Via | Out Via | Source | Destination |
|---|---|---|---|---|---|
| http | 80 | Private | Extranet | any | 192.168.70.6 |
| https | 443 | Private | Extranet | any | 192.168.70.6 |
| ftp | 21 | Private | Extranet | any | 192.168.70.6 |

12. **Private network access to the Universe network:** Allow inside users to connect to certain services on the public Internet. Some access to the Internet will be blocked that is deemed non-business related in an effort to free up Internet bandwidth for customers. AOL Instant Messenger traffic is allowed as a communication tool between GIAC Enterprises employees and remote users, with the knowledge that it will be used for private use only.

| Service | Port | In Via | Out Via | Source | Destination |
|---|---|---|---|---|---|
| http | 80 | Private | Universe | any | any |
| https | 443 | Private | Universe | any | any |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

| | | | | | |
|---|---|---|---|---|---|
| ftp | 21 | Private | Universe | any | any |
| tftp | 69 | Private | Universe | any | any |
| AOL IM | 5190 | Private | Universe | any | any |
| ping | 9595 | Private | Universe | any | any |
| telnet | 23 | Private | Universe | any | any |

The Raptor Firewall collects detailed information on all connections and connection attempts to the firewall and classifies each entry as either Information, Notice, Warning, Error, Alert, Critical, or Emergency. Initially the firewall should be set to capture all events and possibly scaled to capture all events but Information entries in the future in an effort to keep the log files manageable. Log files should be retained for as long as disk space warrants, but at least three months.

*Tip, Tricks, and Gotchas*

The following are points that should be kept in mind by GIAC Enterprises administrative personnel regarding the Raptor Firewall implementation.

- Firewall logs should be routinely reviewed in order to identify unwanted activity from any interface on the firewall. The firewall logs can be ported to Microsoft Access and other applications, such as Telemate.Net Software's NetSpective product, to ease the review process.

- The web server located in both the Service and Extranet networks should be secured as much as possible. Since GIAC Enterprises is a Microsoft Windows shop, both the Windows operating system and the IIS hosting software need to be reviewed. Microsoft, as well as many other sites, offer white papers on performing this operation. In conjunction with this, the latest service packs and hot fixes should also be diligently applied.

- GIAC Enterprises may want to consider the installation of a content blocking software to filter out access to objectionable web sites. Many products on the market perform this function including WebNOT and SurfControl.

- GIAC Enterprises may also want to consider the installation of software to protect and manage the content of the SMTP e-mail. This software can scan for viruses and block certain e-mail from reaching the mail server.

### *VPN*

VPN access is granted in two ways in the security architecture for GIAC Enterprises. The first is via VPN-to-VPN connections with partners since PowerVPN is IPSec compliant. The second is via RaptorMobile to remote users.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

PowerVPN allows the creation of a secure gateway of the remote firewall. This is configured with IKE enabled and a shared secret is created. This enables a two-part authentication when the VPN tunnel is built. Within Raptor Mobile, a policy is created specifying Triple DES encryption. This is done to enable a high level of encryption since the VPN tunnel could be active for a long period of time. The policy is passed up to the proxy on the firewall to allow rules to be established regarding the use of the VPN tunnel. Once the VPN tunnel is established, partners will be allowed http, https, and ftp access to the Extranet network.

The same process is followed for creating VPN connectivity for remote users, with the installation of the RaptorMobile client on their workstations. Again IKE is implemented. Remote users authenticating and establishing a VPN tunnel with RaptorMobile are the packets allowed to travel from the Universe network to the Private network.

## Assignment 3 – Audit Your Security Architecture

A security assessment is an overt study to locate security vulnerabilities, with the goal of studying the current security environment and identifying improvements to secure the systems. Since the GIAC Enterprises security architecture has yet to be implemented, and the equipment is not available to create a prototype network, the system audit presented in the following sections is design only. The audit can not be implemented at this time to create actual data or screen shots. The system audit is an extremely important part of the overall security policy and should be performed at least twice a year or when major security architecture changes occur.

### *Planning the Assessment*

The goal of this security assessment is to validate the security of the Cisco 3620 router and the Axent Raptor Firewall (as they will be configured according to the security policy detailed under Assignment 2.) In order to perform this assessment, full cooperation from GIAC Enterprises will be required, including network access, network diagrams, and all information pertaining to existing security policies. The security assessment will be performed in three stages – outside inspection of the GIAC Enterprises network, physical inspections of the current systems, and the utilization of industry standard software tools to scan the border router and firewall.

The assessment should begin from outside GIAC Enterprises. This means attempting to gain as much information as possible posing as a complete outsider to the network. This simulates the activity a hacker would be performing. This can stage of the assessment can be performed at any time, except for probes, which should be conducted during off hours, as to not disrupt e-commerce traffic to the public web server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Once on-site at GIAC Enterprises, an inspection of the perimeter security devices, the border router and firewall, will be performed in an attempt to identify any vulnerabilities. The inspections will not disrupt either device and can be performed during normal working hours. Discussions will be held with GIAC Enterprises administrators in an effort to detail security policies and practices currently in use. These discussions are an attempt to uncover potential vulnerabilities that would not be disclosed in either the inspection or by use of software tools.

A scan of the existing network will be performed to discover security vulnerabilities and to identify which parts of the network are most susceptible to unauthorized access and denial of service. In this security assessment, the border router and firewall will be scanned from both outside and inside the GIAC Enterprises' network using industry software tools. Scanning the networks from the outside shows how the network looks to an external attacker. It also shows what the router and firewall are allowing outsiders to see and access. Scanning the network internally shows which parts of the network can be exploited internally or by an external attacker who has gained local network access.

Precautions will be taken to ensure GIAC Enterprises does not see any disruptions during business hours. During the implementation of the security assessment, scans and probes of the router and firewall will be planned in advance. This will be done to prevent shutting or slowing down access to the GIAC Enterprises' network for customers, suppliers, and partners, or in case any destructive scans are executed. Prior to any activity occurring on the border router, the running configuration will be saved. This is to prevent the loss of any changes that have been made to the router and not currently saved. If, for any reason, the router were to be restarted prior to saving the changes, GIAC Enterprises could temporarily lose access to the Internet. As stated previously, Internet access is mandatory for revenue to be generated.

It is estimated it will take between 80 and 90 hours to complete this security assessment project, including a presentation and review of the final document. At the standard rate of $175.00 per hour, the total investment for the project will be between $14,000.00 and $15,750.00.

### *Implement the Assessment*

Implementation of the security assessment will be performed in the three stages outlined above. Outside inspection of the network is stage 1. Performing DNS zone transfers is one step to gain as information the GIAC Enterprises network. This can be accomplished by using Sam Spade. Sam Spade is a comprehensive package of tools that run under Microsoft Windows. A few of the tools and what they accomplish are as follows:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

| Tools | Description |
|---|---|
| DNS zone transfer | This asks a DNS server for all the information it has about a domain. It automatically finds the authoritative servers for a domain and will query one or all of them. |
| whois | Ask a whois server who owns a domain name. Sam Spade will usually ask the right whois server automatically, or you can query a particular server. Whois queries for .com/.net/.org addresses are directed to the correct registrar automatically. |
| dig | A more advanced DNS query tool. Dig asks a DNS server for all the information it has about a host. |
| nslookup | Find the IP address from a hostname, or vice-versa. |
| SMTP relay check | This checks whether a mail server is secure. It attempts to send email back to yourself via somebody else's email server (one which you're not supposed to have access to). Hopefully it'll fail, but if it doesn't the mail server is open to all sorts of abuse and the administrator needs to secure it. |

Analyzing the data received from Sam Spade could yield a complete map of the network devices, along with a few glaring security holes that need to be filled.

Once information has been gathered from outside of GIAC Enterprises, the second step is to go on-site and perform an inspection of the border router and firewall. A detailed review of the configurations and log files will be accomplished during this stage.
As discussed previously, before any actions are taken on the Cisco 3620 router, the running configuration will be saved. Access to the router will be tested via the console port and telnet to confirm nonprivileged mode passwords have been created. Logging will be turned on, on the workstation accessing the router in order to capture the screen prints for future analysis. Once the password for privileged mode has been acquired, the command **show running-config** will be executed to obtain a detailed listing of the current configuration of the border router. This will be compared to the list of services that should be turned off as detailed in Assignment 2. It will also yield the current version of IOS software on the router. Each access list will also be reviewed using the **show access-lists xxx** command, where xxx represents the number assigned to the list when it was created. This will also display the number of matches each statement in the access list has made. These are displayed in parentheses after the statement. A **show interface nn** command, where nn is the interface identification, will also be executed to determine if the interface is configured correctly. The log file will also be examined for packets that were denied access by the egress filtering on the Ethernet interface.

Inspection of the firewall will include a physical inspection of the interface connections, especially the connection to the border router. This should be via a crossover cable to eliminate the possibility of any devices being placed outside the firewall. Further inspection of the Raptor Firewall will be conducted to determine the version of the operating system and the Axent software, if any services have been configured to be

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

allowed to run by the vulture program, and if any other applications have been load on the firewall. The firewall logs will be reviewed and copied for further analysis.

The primary method to review the security of the router and firewall will be conducted in stage 3 of the security assessment through the use of scanning tools. There are a number of good port scanning tools available today. These include commercial products – such as NAI's CyberCop Scanner, ISS' SafeSuite, and Cisco's Secure Scanner – and freeware products – such as Nmap and SATAN. The primary analysis software to be used in this security assessment is Axent's NetRecon product. NetRecon is a network vulnerability assessment tool that discovers, analyzes and reports holes in network security. NetRecon achieves this by conducting an external assessment of network security by scanning and probing services on the network. NetRecon reenacts common intrusion or attack scenarios to identify and report network vulnerabilities. It supports Windows NT, NetWare, Unix and Cisco routers. Because it runs under Windows NT, it can make use of any available network protocol to penetrate any type of system on the network. A few of it features and benefits are as follows.

| **Feature** | **Benefit** |
|---|---|
| Discover network vulnerabilities | • Finds out where your network is open<br>• Probes nearly all network devices (including servers, workstations, routers, web servers, and firewalls)<br>• Checks for common ways to break into networks |
| UltraScan Technology | • Executes vulnerability objectives in parallel<br>• Provides immediate visual results while scanning<br>• Simultaneously feeds results from one objective into others resulting in a quicker, deeper security probe<br>• Uses multiple network protocols, not just IP, to find network resources (e.g., NetWare) |
| Intuitive Windows GUI | • Provides an easy-to-use Windows NT interface that lets you quickly install and check for vulnerabilities<br>• Allows you to perform network vulnerability probes from your own workstation or notebook<br>• Graphically displays progress and results in real-time |
| Automatically discovers nodes in the network | • Automatically finds network systems, devices, and subnets that can be accessed<br>• Ensures thorough coverage<br>• Tells you which nodes are running ESM and Intruder Alert |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

| | |
|---|---|
| Select portions of network to analyze | • Selectively targets certain sections of the network<br>• Checks as much or as little of the network as you wish |
| Network vulnerability report | • Creates an HTML report detailing security concerns which can be viewed using any browser<br>• Includes expert advice on vulnerabilities discovered |

NetRecon will be run in three different modes. A light scan will be run during business hours, since it utilizes very little bandwidth as it mainly identifies network resources. A medium will be run after hours as it searches for a wide range of vulnerabilities, and therefore, consumes more bandwidth. A heavy scan will be performer over a weekend as this performs a deep search for vulnerabilities, attempts to crack encrypted passwords, and use the information gathered from one system to attack other systems.

### *Conduct a Perimeter Analysis*

A comprehensive analysis of the information gathered above will be performed to determine the extent of the GIAC Enterprises security vulnerabilities and to determine the implications of the vulnerabilities disclosed. A final security report will be produced. The document will provide a summary of the vulnerabilities classified by their severity. Also included will be a recommendations document designed to limit the potential exposure of the GIAC Enterprises' network in an effort to create a secure environment for the e-business activity. A formal presentation will be made to present and review the findings.

The current version of the border router will be investigated to determine what security vulnerabilities exist for it and what patches/updates are available from Cisco and should be applied. The findings from the show access-lists command on the border router will be used to optimize the order of the statement. It is important to remember that Cisco routers use a top down approach to evaluate packets against the access lists in use. The more statements a packet has to be processed against, the more resources used within the router. The statements should be ordered in descending order of the number of matches that have been made.

The information gathered on the Raptor firewall will be analyzed to make the firewall more secure. As with the Cisco router, the software itself will be investigated for any version upgrades, patches/updates, and any known vulnerabilities. Sites such as SANS, CERT, CVE, and Razor will be used for this analysis. The service pack level on the Windows operating system will also be investigated. Careful attention will be given to the current Windows service pack supported by the Raptor Firewall software.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The output from NetRecon will also be analyzed in detail. NetRecon discovers vulnerabilities, but does not correct them. The corrections to the vulnerabilities discovered will be included in the final report and presentation to GIAC Enterprises.

It must be understood that a security assessment is different from a penetration test, which is a covert test. It provides a snapshot of vulnerabilities that exist at the time the assessment occurs. Accordingly, future changes in configurations or permissions could open up entirely new security holes. Also, vulnerabilities in operating systems and applications are being identified constantly and these too represent future vulnerabilities not covered under this security assessment.

## Assignment 4 – Design Under Fire

The practical chosen for this assignment was written by Janice Southerland from the SANS NS2000 Monterey conference. It can be found at the following URL www.sans.org/y2k/practical/janice_southerland_GCFW.doc. Figure 3 contains Ms. Southerland's network design.

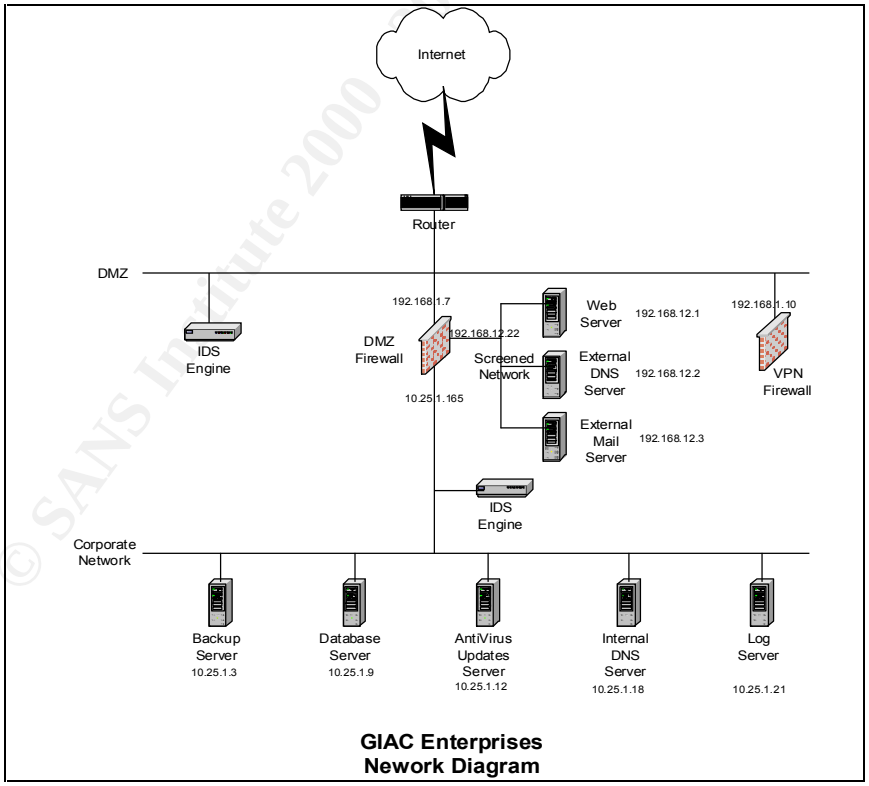


**Figure 3 - Janice Southerland Network Design**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

### *Firewall Attack*

The firewall in use in this network design is CheckPoint's Firewall-1 version 4.1. Research on web sites, including SANS, CERT, and CVE, yielded a number of vulnerabilities with Firewall-1 version 4.1. The current service pack for v 4.1 is SP3. If no service packs have been applied, the firewall is particularly vulnerable. Without service pack 2, Firewall-1 is vulnerable to the following attacks:

- SMTP Security Server Denial-of-Service
- IP Fragmentation Denial-of-Service
- One-Way Connection Enforcement Bypass
- FTP Connection Enforcement Bypass
- Retransmission of Encapsulated Packets
- OPSEC Authentication Vulnerability
- Getkey Buffer Overflow

The SMTP Security Server Denial-of-Service vulnerability can be exploited by sending a rapid stream of invalid SMTP commands to the SMTP Security Server. This would raise the CPU load on the firewall and disable mail delivery. Other traffic is reported to be able to continue to be processed, but if the CPU load can be increased enough, the firewall will begin to operate erratically and affect all traffic. If the single firewall in this network design can be crippled, access to and from the network will be crippled.

### *Denial of Service Attack*

Denial of Service (DOS) attacks overrun web sites with streams of packets. In the case of a Distributed Denial of Service attack, the stream of packets is coming in from multiple locations. A hacker plants a daemon, an automatic utility program that runs in the background of a computer, on numerous computers and later sends a trigger for the daemon to begin operating. The daemon then begins to send a flood TCP SYN, UDP, or ICMP packets to an unsuspecting host. The amount of traffic generated is more than the host can handle and it essentially shuts down. In 2000, this was done to a number of highly publicized web sites. UPD floods are what brought down Yahoo and Amazon.

Most firewalls today include measures to repel denial of service attacks, and, coupled with intrusion detection systems can terminate the unwanted connections before they can shut down communications. In the case of this design, if 50 compromised systems were to send a large stream of TCP SYN, UDP, or ICMP packets to the network (and especially if they were IP fragments) the firewall could be crippled if it did not have the latest CheckPoint service pack, at least SP2, installed.

To mitigate this attack from happening, the latest service pack, hot fixes, and security updates should be applied to both the Firewall-1 software and the underlying operating system.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

### *Internal System Compromise*

An attack plan to compromise an internal system through the perimeter would target the web server on the Screened network. The reason the web server has been chosen is because it is already accessible from the internet by the fact it is a public web server. Typically, the security of the web server operating systems are overlooked by administrators. The attack plan would be to gain access to the operating system level of the web server and then run software like l0phtcrack to crack the logins and passwords. These same passwords would then be used against the router and firewall in an attempt to gain access and modify the access rules. If the access rules can be modified, access to the private network and the hosts located on it. If this plan did not work, but the web server operating system could be compromised, access from it to the private network may be available.

© SANS Institute 2000 - 2002, Author retains full rights.

# References


**Print Media**

Axent Technologies, Inc., e-Security: Enabling e-Business. 1999.

Axent Technologies, Inc., NetRecon – Installation and Getting Started Guide. 2000.

Axent Technologies, Inc., Raptor Firewall Reference Guide. 2000.

Briney, Andy, *"First Rate Security."* Information Security. January 2001.

Stevens, W. Richard, TCP/IP Illustrated, Volume 1. Addison-Wesley, Boston, MA. 1994.

Syngress Media, Inc., Cisco Certified Design Associate Guide. Osborne/McGraw Hill, Berkeley, CA. 2000.

**On-Line Articles**

*Building a Perimeter Security Solution with the Cisco Secure Integrated Software,* http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm

*Cisco Anti-Spoof Egress Filtering,* http://www.sans.org/dosstep/cisco_spoof.htm

*Deploying Firewalls,* http://www.cert.org/security-improvement/modules/m08.html

*Increasing Security on IP Networks,* http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

*Improving Security on Cisco Routers,* http://www.cisco.com/warp/customer/707/21.html

*Potential Security Issues in VPN-1/FireWall-1,* http://www.checkpoint.com/techsupport/alerts/list_vun.html#FTP_Connection

*Network Security Policy: Best Practices White Paper,* http://www.cisco.com/warp/customer/126/secpol.html

*RFC 2196 – Site Security Handbook,* ftp://ftp.isi.edu/in-notes/rfc2196.txt


© SANS Institute 2000 - 2002, Author retains full rights.

**On-Line Sites**

www.axent.com

www.cert.org

www.checkpoint.com

www.cisco.com

www.cve.mitre.org

www.microsoft.com

www.mimesweeper.com

www.radware.com

www.razor.bindview.com

www.samspade.org/ssw/

www.sans.org

www.surfcontrol.com

www.telemate.com

© SANS Institute 2000 - 2002, Author retains full rights.