



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

Eric Mroczka

SANS Baltimore 2001

Table of contents

| | |
|---|----|
| Overview | 4 |
| Assignment 1: Security Architecture | 5 |
| 1.0 Corporate Assumptions | 5 |
| 1.1 Customers | 6 |
| 1.2 Suppliers | 6 |
| 1.3 Partners | 6 |
| 1.4 Security Architecture Diagram | 7 |
| 1.5 Security Architecture Component Description | 8 |
| 1.5.1 Border Router | 8 |
| 1.5.2 External Firewall | 8 |
| 1.5.3 Internal Firewall | 8 |
| 1.5.4 VPN Hardware | 8 |
| 1.5.5 External DNS | 8 |
| 1.5.6 Mail Relay Server | 9 |
| 1.5.7 IDS Sensors | 9 |
| 1.5.8 Internal DNS | 9 |
| 1.5.9 Mail Server | 10 |
| 1.5.10 Syslog Server | 10 |
| 1.5.11 Proxy Server | 10 |
| 1.5.12 Reverse-Proxy Server | 10 |
| Assignment 2: Security Policy | 11 |
| 2.1 Overview | 11 |
| 2.1.1 Sample Security Policy | 11 |
| 2.1.2 Common types of Network Attacks | 12 |
| 2.1.3 Packet Filtering - A Technical Overview | 13 |
| 2.1.4 Packet Filtering | 14 |
| 2.2 Traffic Rules | 14 |
| 2.3 Cisco Basic Command Modes | 17 |
| 2.4 Border Router | 18 |
| 2.5 External Firewall | 26 |
| 2.6 VPN Hardware | 27 |
| 2.6.1 Client Configuration | 30 |
| 2.7 Internal Firewall | 30 |
| Assignment 3 | 33 |
| 3.1 Planning the Assessment | 33 |
| 3.2 Implementing the Assessment | 34 |
| 3.3 Conduct a perimeter analysis | 36 |
| Assignment 4 | 37 |
| 4.1 An attack against the firewall itself | 38 |
| 4.2 A denial of service attack | 38 |
| 4.3 An attack plan to compromise an internal system | 39 |
| References | 40 |

Figures and Tables:

| | |
|--|----|
| Figure 1: Security Architecture Diagram | 6 |
| Table 1: Cisco Basic Command Modes | 17 |
| Table 2: Creating Standard Access-Lists | 19 |
| Table 3: Creating Extended Access-Lists | 19 |
| Table 4: External Firewall Rules | 26 |
| Figure 2: Cisco VPN 3000 Concentrator Series Manager Screen-Shot | 27 |
| Figure 3: Cisco VPN 3000 Concentrator Series Manager Screen-Shot | 28 |
| Figure 4: Cisco VPN Authentication, Encryption and IKE selection screen-shot | 28 |
| Figure 5: Cisco VPN Configuration Screen-Shot | 29 |
| Table 5: Cisco VPN filter configuration/traffic flow rules | 30 |
| Figure 6: nmap Screen-shot #1 | 34 |
| Figure 7: nmap Screen-shot #2 | 34 |

© SANS Institute 2000 - 2002, Author 1

Overview

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.

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

Assignment 3 - Audit Your System 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.
2. Implement the assessment.
3. Conduct a perimeter analysis.

Assignment 4 - Design Under Fire

Select a network design from any previously posted GCFW practical (<http://www.sans.org/giactc/gcfw.htm>) and paste the graphic into your submission.

1. Plan an attack against the firewall itself.
2. Describe the countermeasures that can be put into place to mitigate the DOS attack.
3. Describe the process to compromise a target.

Security Architecture

1.0 Corporate Assumptions

While no budgetary constraints have been given for this project, the fact that GIAC Enterprises is defined as a growing Internet start-up company does not mean that we have an unlimited amount of money. Still, this provides a clean slate in which to implement proper security policies and procedures. In other words, we can do things right from the start.

Therefore, we will balance the type and cost of the components we build into our design to give us good security while not breaking the bank. Since we are not sure what the future growth rate of the company will be our design will allow the remaining components to be upgraded in future years as the company reaches and maintains a profit. This is taken into account so that we do not find ourselves designed into a corner!

Our corporate security policy will use these principles:

1. Be a good Internet neighbor.
2. Keep things simple.
3. Always error on the side of security.
4. Whenever possible avoid forcing the customers to use special software to access resources.
5. Everything is explicitly denied unless required/allowed.
6. Explicitly define all default values. In other words, never assume that the default value is what is published in the manual and that it will remain that way with future upgrades.
7. To keep the network as secure as possible with the available resources.
8. Provide security at each layer corresponding to the TCP/IP stack
9. Provide security for each component of the security architecture.
10. Perform security audits at least twice per year.
11. During security audits, always check the security of our partners and suppliers as well. Insist that they perform audits as often as we do. A chain is only as strong as its weakest link.

Access to all data on the GIAC Enterprises LAN by home users, remote offices, and other business partners will be done via an encrypted VPN solution.

Access to the customer web site and supplier web site will be done over the Internet using encryption via Secure Sockets Layer (SSL).

Purchases made by our customers will be handled either via a corporate purchase order, a credit card, or a company check.

Because we will be allowing purchases via credit cards we will adopt [VISA's Cardholder Information Security Program \(CISP\)](#) requirements. They are listed as follows:

1. Install and maintain a working network firewall to protect data accessible via the Internet.
2. Keep security patches up-to-date.
3. Encrypt stored data.
4. Encrypt data sent across open networks.
5. Use and regularly update anti-virus software.
6. Restrict access to data by business "need to know."
7. Assign a unique ID to each person with computer access to data.
8. Don't use vendor-supplied defaults for system passwords and other security parameters.
9. Track access to data by unique ID.
10. Regularly test security systems and processes.

Two additional requirements pertain to administrative and physical security issues:

11. Maintain a policy that addresses information security for employees and contractors.
12. Restrict physical access to cardholder information.

1.1 Customers

In order to make things easy for the customers we will not require them to set-up a VPN connection with us in order to access the customer web site. However, in order to keep the transactions secure, access to the customer web site will be done using an SSL encrypted connection.

1.2 Suppliers

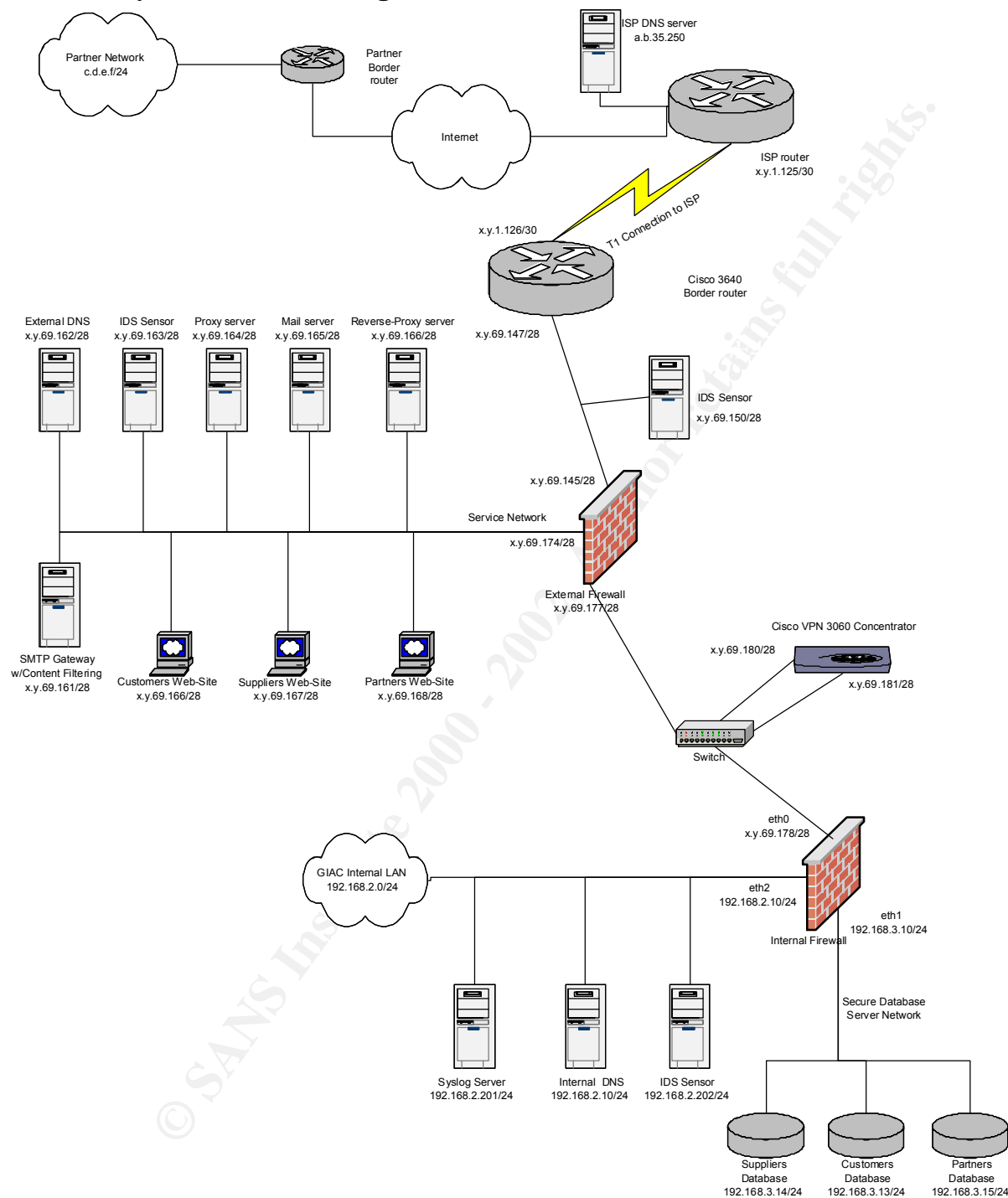
All suppliers will need to set-up a VPN solution in order to gain access to the necessary resources on the GIAC LAN. The VPN solution will use IPSec.

All suppliers will be required to have a firewall and some level of security in place to help prevent attacks coming into the GIAC LAN thru the encrypted VPN tunnel.

1.3 Partners

All business partners will need to set-up a VPN solution in order to gain access to the GIAC LAN. All partners will be required to adhere to the same security principles that GIAC Enterprises uses. This is to help prevent an attacker from coming into the GIAC LAN thru an encrypted VPN tunnel from a Partner network.

1.4 Security Architecture Diagram



1.5 Security Architecture Component Description

1.5.1 Border Router

[Cisco 3640 border router](#)
running IOS v12.0.

Our Border router needs to be able to handle the load of the traffic going between the GIAC network and the rest of the outside world. We want one that not only does the job but also has enough horsepower and provides enough growth capacity for the future. Lastly, this device will be our first line of defense by providing basic ingress and egress filtering.

1.5.2 External Firewall

Nokia IP440 with [CheckPoint Firewall-1](#)

The firewall will be set-up to deny everything except the specific addresses and ports that the security policy calls for. The FW-1 will be patched to the latest service level.

1.5.3 Internal Firewall

PC running [Linux](#)
[V2.4.7 kernel](#)
[NetFilter](#)

The primary function of the Internal Firewall is to provide a more granular control over the traffic it passes. This server will be hardened to bastion host level.

1.5.4 VPN Hardware

[Cisco VPN 3060 Concentrator](#)

Because there are a large number of business partners and remote users we need a large, scaleable VPN solution. The Cisco VPN 3060 Concentrator is a VPN platform designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) and up to 5000 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and non-redundant configurations are available. The Cisco VPN 3000 Client is provided at no additional charge and includes unlimited distribution licensing.

1.5.5 External DNS Server

PC running [Linux](#)
[V2.4.7 kernel](#)
[BIND v9.1.3](#)

We are using a split-DNS design. Our external DNS server will be hardened to bastion host level and will be configured as a Master (Primary) DNS server. We will configure

the server to run only essential services. Our ISP will host slave DNS servers. This server provides the first portion of our split-DNS design. It will also be configured to allow lookups to be forwarded from the Internal DNS server only.

1.5.6 Mail Relay Server

PC running [Linux](#)
[MailSweeper for SMTP v4.2](#)

The Mail Relay Server will be running MailSweeper for SMTP v4.2 from Baltimore Technologies. This server will be hardened to bastion host level. We will configure MailSweeper to:

- Scan all messages with an Anti-Virus scanner
- Block all Visual Basic Script (.VBS) files-both incoming and outgoing.
- Block all messages whose mime-types do not match.
- Block all HTML formatted messages that use script tags
- Deny relaying from any external mail server.

We will also change the SMTP server's banner in order to disguise the true identity of our SMTP server.

1.5.7 IDS Sensors

PC running [Linux](#)
[Snort v1.8p1](#)

Our IDS Sensors are placed throughout our network infrastructure. Their primary job is to provide real-time network traffic knowledge as well as payload based attack detection. Another function of our IDS sensors is to provide a way to check the configuration of our firewalls and border router. All of these servers will be hardened to bastion host level.

1.5.8 Internal DNS

PC running [Linux](#)
[BIND v9.1.3](#)

This server provides the Internal portion of our split-DNS design. This server holds the "family jewels" and as such, any external DNS servers will not be allowed to query it. Because it will not be doing zone transfers with any DNS servers in the outside world, this server will also be set-up as a Master (Primary) server. This server will be configured to forward any DNS queries that it cannot answer to the external DNS server. This server will also be hardened to bastion host level.

1.5.9 Mail Server

[Microsoft Windows 2000](#)
[Microsoft Exchange Server 2000](#)

This server will be running Microsoft Exchange 2000 (with Service Pack 1) on top of Microsoft Windows 2000 (with Service Pack 2). Also, the latest available OS patches and hot fixes will be installed.

1.5.10 Syslog Server

PC running [Linux](#)
external tape drive

This server will be running a syslog daemon. The logs files will be checked on a daily basis.

1.5.11 Proxy Server

[Microsoft Windows 2000](#)
[Microsoft ISA Server 2000](#)

This server will be running a proxy service that will help protect and filter web access requests from the GIAC network. This server will have all of the latest available service packets and hotfixes applied.

1.5.12 Reverse-Proxy Server

PC running [Linux](#)
[Squid Proxy Cache software v2.4](#)

This server will be running a proxy service that will help protect the data on the actual web servers. It will be the machine that the users actually communicate with. It makes the requests to the actual web server on behalf of the user.

Security Policy

2.1 Overview

Defining a security policy is a critical first element in building a proper and secure enterprise network. It provides a common point of reference for all employees to adhere to, and provides rules by which the company's technology and information assets are governed.

A security policy must not only show what the framework is for the companies security and network infrastructure, but also be properly documented to show the thought behind the policy.

2.1.1 Sample Security Policy¹

GIAC Enterprises relies heavily on the application of information technology for the effective management of their fortune cookie sayings business. Rapid and continuing technical advances have increased the dependence of GIAC Enterprises on information systems. The value of GIAC Enterprises information, software, hardware, telecommunications, and facilities must be recognized by senior staff as a critical resource, and be protected through a company security program.

Basic GIAC Enterprises Policy - Assumptions

- Automated information and information resources are strategic and vital assets. These assets require a degree of protection equal to their value. In order to do this measures shall be taken to protect these assets against accidental or unauthorized disclosure, modification or destruction, as well as to assure the security, reliability, integrity and availability of information.
- The protection of assets is the responsibility of all company employees, both permanent and contract.
- Access to GIAC Enterprises information resources must be strictly controlled. GIAC Enterprises owned information resources are to be used only for official GIAC Enterprises purposes.
- All corporate information should be considered sensitive and confidential. It must be protected from unauthorized access or modification. Data which is essential to critical GIAC Enterprises functions, must be protected from loss, contamination, unauthorized modifications or destruction.
- Risks to information resources must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected, considering value to both the GIAC Enterprises and a potential intruder.

¹ Sample template policy provided by Chris Brenton during SANS Baltimore conference.

- The integrity of data, its source, its destination, and processes applied to it must be assured. Changes, alterations and distribution of data must be made only in authorized and acceptable ways.
- Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.
- Security awareness and training of employees is one of the most effective means of reducing vulnerability to errors and fraud and must be continually emphasized and reinforced at all levels of management. All individuals must be accountable for their actions relating to information resources. Information security programs must be responsive and adaptable to changing vulnerabilities and technologies affecting information resources.
- Management must ensure adequate separation of functions for tasks that are susceptible to fraudulent or unauthorized activity.
- All GIAC Enterprises personnel are expected to be intolerant of computer security violations and report them immediately.

2.1.2 Common Types of Network Attacks

In general, firewalls are intended to protect network resources from several kinds of attacks:

- *Passive Eavesdropping/Packet Sniffing*—An attacker uses a packet sniffer to gather sensitive information from data streams between two sites or to steal username/password combinations, either on a private carrier or a public network.
- *IP Address Spoofing*—An attacker pretends to be a trusted computer by using an IP address that is within the accepted range of IP addresses for an internal network.
- *Port Scans*—An active method of determining to which ports on a network device a firewall is listening. After attackers discover the "holes" in a firewall, they can concentrate on finding an attack that exploits the applications that use those ports.
- *Denial-of-Service Attack*—Differs from other types of attack because, instead of seeking access, the attacker attempts to block valid users from accessing a resource or gateway. This blockage can be achieved through SYN flooding a network resource to exhaustion through using half-open sessions (sending TCP packets with the SYN bit set from a false address) or by crafting packets that cause a resource to perform incorrectly or crash.
- *Application-Layer Attack*—This attack can be in various forms—from exploiting weaknesses in server software to accessing hosts by obtaining the permission of the account that runs an application. For example, an attacker might use Simple Mail Transfer Protocol (SMTP) to compromise hosts that run older versions of sendmail using undocumented commands in the sendmail application.
- *Trojan horse*—In this attack the user is induced to run a malicious piece of software by being misled into believing it is something other than what it really is. More advanced application-layer attacks exploit the complexity of new technologies such as HTML, Web browser functionality, and the Hypertext

Transfer Protocol (HTTP). These attacks include Java applets and ActiveX controls to pass harmful programs across a network and load them via user Web browsers.

2.1.3 Packet Filtering-a Technical Overview

Packet filtering is a process that enables a router to implement a security policy based on identifiable attributes within each packet. Cisco IOS software has a set of access control options that can be used to filter packets. These options can be applied to inbound or outbound packets on any interface, and they add minimal latency to packets going through the host. This type of policy enforcement can stop many of the problems caused by unwanted intrusions from the public side. Packet filters can be "stateless"; that is, they do not consider TCP session state, while still providing acceptable security for many environments.

Cisco routers generally do not maintain any information about the state of a session (for traffic traversing the box). A router will normally cache pertinent portions of a header so that subsequent packets can be fast-switched, but it will not keep track of items such as:

- How long ago was the last packet in this session transmitted?
- Are the sequence/acknowledgment numbers climbing as expected?
- Was the session initiated from the inside or outside?
- Is the session still open or has it been closed?
- What port or ports are the return data channels using?

In general, stateless packet filtering provides less scrutiny than filters that examine session states. However, because a stateless packet filter does less processing than other technologies (such as proxy servers), it is also the fastest firewall technology available, and is often implemented in perimeter hardware solutions such as routers. Cisco routers contain features that provide several levels of standard, stateless packet filtering:

- *Standard access lists and static extended access lists*—Provide basic traffic-filtering capabilities. Configurable criteria describe which packets should be forwarded and which should be dropped, based upon each packet's network-layer information. For example, one can block all User Datagram Protocol (UDP) packets from a specific source IP address or address range. Some extended access lists can also examine transport-layer information to determine whether to forward or block packets.
- *Lock and Key (dynamic access lists)*—Provide traffic filtering with the ability to allow temporary access through the firewall for certain individuals. These individuals must first be authenticated by a username/password mechanism (usually through an attached authentication server such as a TACACS+, Remote Authentication Dial-In User Services (RADIUS), or a Kerberos server). Upon user authentication, the firewall opens to allow traffic through for the associated host.

Upon logout, the firewall closes the temporary opening. This scenario provides tighter, user-based control at the firewall.

2.1.4 Packet Filtering²

Each of the fields within IP and TCP headers contain information that can be processed by the router. The portions that are usually examined for filtering are:

- IP destination address
- IP source address
- IP protocol field
- TCP source port
- TCP destination port
- TCP flags field
 - SYN alone for a request to open a connection
 - SYN/ACK for a connection confirmation
 - ACK for a session in progress
 - FIN for session termination

Various combinations of matching (or not matching) these fields can be used to support a policy. For example, if the policy were preventing SMTP sessions initiated from IP host 10.1.1.10 with a destination address of 12.2.2.12, then the packet filter would discard packets that have:

- IP destination address = 12.2.2.12
- IP source address = 10.1.1.10
- IP protocol = 6 (for TCP)
- Destination port = 25 (for SMTP)

The other fields generally do not need to be considered, although adding a check "ACK bit not set" would guard against the connection being a non-SMTP connection initiated outgoing from port 25, for example.

2.2 Traffic rules

The first thing we need to do is define what traffic we are going to allow in and out of our network via our border router. I have listed the types of traffic we should allow below. This list can be modified as the business needs change, but this provides a good starting point. It also provides a good set of rules to fall back on when someone wants to have other traffic in from the outside world.

Traffic allowed in from the outside (coming from our ISP):

- SMTP (TCP/25) to our mail relay server (x.y.69.161).
- DNS queries (UDP/53) to our External DNS server (x.y.69.162).

² Cisco Systems, Inc. [Packet Filtering](#).

- Web (TCP/80 and SSL/443) to x.y.69.164 and x.y.69.166.
- VPN traffic (IPSec) to x.y.69.181.

Traffic allowed out from our network (going to our ISP):

- SMTP (TCP/25) from our mail relay server (x.y.69.161) to any SMTP server.
- DNS queries (UDP/53) from our External DNS server (x.y.69.162).
- DNS zone transfers (TCP/53) from x.y.69.162 to a.b.35.250.
- Web (TCP/80 and SSL/443) from x.y.69.164 and x.y.69.166.
- VPN traffic (IPSec) from x.y.69.181.

Next, we need to define the traffic allowed in and out of the various interfaces on the External Firewall.

Traffic allowed into the firewall (*coming from the Border Router*):

- SMTP (TCP/25) to our mail relay server (x.y.69.161).
- DNS queries (UDP/53) to our External DNS server (x.y.69.162).
- DNS zone transfers (TCP/53) to x.y.69.162 to a.b.35.250.
- Web (TCP/80 and SSL/443) to x.y.69.164 and x.y.69.166.
- VPN traffic (IPSec) to x.y.69.181.

Traffic allowed out from the firewall (*going to the Border Router*):

- SMTP (TCP/25) from our mail relay server (x.y.69.161) to any SMTP server.
- DNS queries (UDP/53) from our External DNS server (x.y.69.162).
- DNS zone transfers (TCP/53) from x.y.69.162 to a.b.35.250.
- Web (TCP/80 and SSL/443) from x.y.69.164 and x.y.69.166.
- VPN traffic (IPSec) from x.y.69.181.

Traffic allowed into the firewall (*coming from the service network*):

- SMTP (TCP/25) from our mail relay server (x.y.69.161).
- DNS queries (UDP/53) from our External DNS server (x.y.69.162).
- DNS zone transfers (TCP/53) from x.y.69.162 to a.b.35.250.
- Web (TCP/80 and SSL/443) from x.y.69.164 and x.y.69.166.
- VPN traffic (TCP/80) from x.y.69.180 to x.y.69.167 or x.y.69.168.
- SQLnet traffic from x.y.69.166 to the CustomersDB (192.168.3.13).
- SQLnet traffic from x.y.69.167 to the SuppliersDB (192.168.3.14).
- SQLnet traffic from x.y.69.168 to the PartnersDB (192.168.3.15).

Traffic allowed out from the firewall (*going to the service network*):

- SMTP (TCP/25) to our mail relay server (x.y.69.161) to any SMTP server.

- DNS queries (UDP/53) to our External DNS server (x.y.69.162).
- DNS zone transfers (TCP/53) to x.y.69.162 from a.b.35.250.
- Web (TCP/80 and SSL/443) to x.y.69.164 and x.y.69.166.
- VPN traffic (TCP/80) from x.y.69.167 or x.y.69.168 to x.y.69.180.
- SQLnet traffic to x.y.69.166 from the CustomersDB (192.168.3.13).
- SQLnet traffic to x.y.69.167 from the SuppliersDB (192.168.3.14).
- SQLnet traffic to x.y.69.168 from the PartnersDB (192.168.3.15).

Traffic allowed into the firewall (*coming from the internal firewall/VPN*):

- DNS queries (UDP/53) to our External DNS server (x.y.69.162) from our Internal DNS server.
- Web (TCP/80 and SSL/443) to our Proxy Server (x.y.69.164).
- VPN traffic (TCP/80) to the Supplier Web Server or Partner Web Server.
- VPN traffic (IPSec) to our Suppliers or Partners.
- SQLnet traffic to x.y.69.166 from the CustomersDB (192.168.3.13).
- SQLnet traffic to x.y.69.167 from the SuppliersDB (192.168.3.14).
- SQLnet traffic to x.y.69.168 from the PartnersDB (192.168.3.15).

Traffic allowed out from the firewall (*going to the internal firewall/VPN*):

- DNS queries (UDP/53) from our External DNS server (x.y.69.162) to our Internal DNS server.
- Web (TCP/80 and SSL/443) from our Proxy Server (x.y.69.164).
- VPN traffic (TCP/80) from the Supplier Web Server or Partner Web Server.
- VPN traffic (IPSec) from our Suppliers or Partners.
- SQLnet traffic from x.y.69.166 to the CustomersDB (192.168.3.13).
- SQLnet traffic from x.y.69.167 to the SuppliersDB (192.168.3.14).
- SQLnet traffic from x.y.69.168 to the PartnersDB (192.168.3.15).

Last, we should define the traffic our Internal Firewall will allow:

Traffic allowed into the firewall (*coming from the external firewall/eth0*):

- DNS queries (UDP/53) to our External DNS server (x.y.69.162) from our Internal DNS server.
- Web (TCP/80 and SSL/443) to our Proxy Server (x.y.69.164).

Traffic allowed out from the firewall (*going to the external firewall/eth0*):

- DNS queries (UDP/53) from our External DNS server (x.y.69.162) to our Internal DNS server.
- Web (TCP/80 and SSL/443) from our Proxy Server (x.y.69.164).

Traffic allowed into the firewall (*coming from the Internal LAN/eth2*):

- DNS queries (UDP/53) to our External DNS server (x.y.69.162) from our Internal DNS server.
- Web (TCP/80 and SSL/443) to our Proxy Server (x.y.69.164).

Traffic allowed out from the firewall (*going to the Internal LAN/eth2*):

- DNS queries (UDP/53) from our External DNS server (x.y.69.162) to our Internal DNS server.
- Web (TCP/80 and SSL/443) from our Proxy Server (x.y.69.164).

Traffic allowed into the firewall (*coming from the Database network/eth1*):

- SQLnet traffic to x.y.69.166 from the CustomersDB (192.168.3.13).
- SQLnet traffic to x.y.69.167 from the SuppliersDB (192.168.3.14).
- SQLnet traffic to x.y.69.168 from the PartnersDB (192.168.3.15).

Traffic allowed out from the firewall (*going to the Database network/eth1*):

- SQLnet traffic from x.y.69.166 to the CustomersDB (192.168.3.13).
- SQLnet traffic from x.y.69.167 to the SuppliersDB (192.168.3.14).
- SQLnet traffic from x.y.69.168 to the PartnersDB (192.168.3.15).

2.3 Cisco Basic Command Modes³

Table 1 summarizes the main command modes of the Cisco IOS software.

| Command Mode | Access Method | Prompt | Exit Method |
|----------------------|---|-----------------|---|
| User EXEC | Log in. | Router> | Use the logout command. |
| Privileged EXEC | From user EXEC mode, use the enable EXEC command. | Router# | To exit back to user EXEC mode, use the disable command. To enter global configuration mode, use the configure terminal privileged EXEC command. |
| Global configuration | From privileged EXEC mode, use the configure terminal privileged EXEC command. | Router(config)# | To exit to privileged EXEC mode, use the exit or end command or press Ctrl-Z . |

³ Cisco Systems, Inc. [Using the Command Line Interface](#)

| | | | |
|-------------------------|--|--------------------|--|
| | | | To enter interface configuration mode, enter an interface configuration command. |
| Interface configuration | From global configuration mode, enter by specifying an interface with an interface command. | Router(config-if)# | To exit to global configuration mode, use the exit command. To exit to privileged EXEC mode, use the exit command or press Ctrl-Z . To enter subinterface configuration mode, specify a subinterface with the interface command. |

2.4 Cisco 3640 Border Router

Our border router is our first line of defense. It is at this point that we begin to filter out basic stuff that we don't want our firewall to deal with. This includes basic ingress and egress filtering. Then we'll add a few more filters to block out most of the other stuff we don't even want to consider letting into our network.

First let's define an access list, it's format, and how to apply it. "An access list is a sequential collection of permit and deny conditions that apply to IP addresses. The Cisco IOS software tests addresses against the conditions in an access list one by one. The first match determines whether the software accepts or rejects the address. Because the software stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the software rejects the address."⁴

Standard IP access lists use source addresses for matching operations.

Extended IP access lists use source and destination addresses for matching operations, and optional protocol type information for finer granularity of control.

A more detailed set of instructions can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm#xtocid420214

To create a standard access list, use the following commands in global configuration mode:⁵

⁴ Cisco Systems, Inc. [Filtering IP Packets Using Access Lists](#)

⁵ Cisco Systems, Inc. [Creating Standard and Extended Access Lists Using Numbers](#)

Table 2: Creating Standard Access-Lists

| | Command | Purpose |
|---------------|---|--|
| Step 1 | Router(config)# access-list <i>access-list-number</i> remark <i>remark</i> | Indicates the purpose of the deny or permit statement. |
| Step 2 | Router(config)# access-list <i>access-list-number</i> { deny permit } <i>source</i> [<i>source-wildcard</i>] [log] or Router(config)# access-list <i>access-list-number</i> { deny permit } any [log] | Defines a standard IP access list using a source address and wildcard. or Defines a standard IP access list using an abbreviation for the source and source mask of 0.0.0.0 255.255.255.255. |

To create an extended access list, use the following commands in global configuration mode:⁶

Table 3: Creating Extended Access-Lists

| | Command | Purpose |
|---------------|---|---|
| Step 1 | Router(config)# access-list <i>access-list-number</i> remark <i>remark</i> | Indicates the purpose of the deny or permit statement. |
| Step 2 | Router(config)# access-list <i>access-list-number</i> { deny permit } <i>protocol</i> <i>source</i> <i>source-wildcard</i> <i>destination</i> <i>destination-wildcard</i> [precedence precedence] [tos <i>tos</i>] [established] [log] | Defines an extended IP access list number and the access conditions. Specifies a time range to restrict when the permit or deny statement is in effect. Use the log keyword to get access list logging messages, including violations. Use the log-input keyword to include input interface, source MAC address, or VC in the logging output. |

⁶ Cisco Systems, Inc. [Creating Standard and Extended Access Lists Using Numbers](#)

| | | |
|------------------------------|---|--|
| <p>Step 2 (cont).</p> | <p> log-input] [time-range <i>time-range-name</i>]</p> <p>or</p> <p>Router(config)#access- list <i>access-list-number</i> {deny permit} <i>protocol any any</i> [log log-input] [time-range <i>time-range-</i> <i>name</i>]</p> <p>or</p> <p>Router(config)#access- list <i>access-list-number</i> {deny permit} <i>protocol/host</i> <i>source host destination</i> [log log-input] [time- range<i>time-range-name</i>]</p> <p>or</p> <p>Router(config)#access- list <i>access-list-number</i> [dynamic <i>dynamic-name</i> [timeout <i>minutes</i>]] {deny permit} <i>protocol source</i> <i>source-wildcard</i> <i>destination destination-</i> <i>wildcard</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [established] [log log-input] [time-range <i>time-range-name</i>]</p> | <p>Or</p> <p>Defines an extended IP access list using an abbreviation for a source and source wildcard of 0.0.0.0 255.255.255.255, and an abbreviation for a destination and destination wildcard of 0.0.0.0 255.255.255.255.</p> <p>Or</p> <p>Defines an extended IP access list using an abbreviation for a source and source wildcard of <i>source</i> 0.0.0.0, and an abbreviation for a destination and destination wildcard of <i>destination</i> 0.0.0.0.</p> <p>Or</p> <p>Defines a dynamic access list. For information about lock-and-key access, refer to the "Configuring Traffic Filters" chapter in the <i>Cisco IOS Security Configuration Guide</i>.</p> |
|------------------------------|---|--|

After you create an access list, you place any subsequent additions (possibly entered from the terminal) at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

Tip Cisco routers run their IOS commands from a copy of the start-up configuration. This copy is made whenever the router is powered on. As long as you do not save your changes to the start-up configuration you can always reboot the router to get it back to the working state it was in before you messed it up.

Gotcha When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end. Further, with standard access lists, if you omit the mask from an associated IP host address access list specification, 0.0.0.0 is assumed to be the mask.⁷

Gotcha When creating an access list you must pay attention to which interface you are creating them for and which direction they are supposed to work on. Applying inbound rules as outbound rules will have negative affects on your Internet connectivity. The same holds true for outbound rules being incorrectly applied as inbound rules.

The border router ingress access list will be configured to block local loopback addresses, multicast traffic, broadcast traffic and other private address traffic as defined in [RFC 1918](#).

We are going to define a numbered extended access list for the inbound side of the Serial 0 interface on the router. Our inbound side access list will be number 101. The following ACL's should be entered into our router, in Global configuration mode, in the order given, as access lists are processed in the order that they are entered:

These first two ACL's are at the top of the list to help speed up processing of sessions that have already been established:

```
GIAC-Border(config)#access-list 101 permit tcp any any established
GIAC-Border(config)#access-list 101 permit udp any any
```

The next set of ACL's allow SMTP and HTTP (Normal and Encrypted) traffic thru:

```
GIAC-Border(config)#access-list 101 permit tcp any host x.y.69.161 eq smtp
GIAC-Border(config)#access-list 101 permit tcp any host x.y.69.166 eq 80
GIAC-Border(config)#access-list 101 permit tcp any host x.y.69.167 eq 80
GIAC-Border(config)#access-list 101 permit tcp any host x.y.69.168 eq 80
GIAC-Border(config)#access-list 101 permit tcp any host x.y.69.166 eq 443
GIAC-Border(config)#access-list 101 permit tcp any host x.y.69.167 eq 443
GIAC-Border(config)#access-list 101 permit tcp any host x.y.69.168 eq 443
```

⁷ Cisco Systems, Inc. [Creating Standard and Extended Access Lists Using Numbers](#)

This set of ACL's will allow DNS queries and zone transfers thru:

```
GIAC-Border(config)#access-list 101 permit udp any host x.y.69.162 eq 53
GIAC-Border(config)#access-list 101 permit tcp host a.b.35.250 host x.y.69.162 eq 53
```

These ACL's block out some traffic that we don't want to be bothered with:

These per RFC 1918:

```
GIAC-Border(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any
GIAC-Border(config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any
GIAC-Border(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any
GIAC-Border(config)#access-list 101 deny host 0.0 0.0
```

The local loopback address should not be seen on any network:

```
GIAC-Border(config)#access-list 101 deny ip 127.0.0.0 0.255.255.255 any
```

We don't want to see any multicast traffic:

```
GIAC-Border(config)#access-list 101 deny ip 224.0.0.0 31.255.255.255 any
```

We should never see broadcast traffic on the internet:

```
GIAC-Border(config)#access-list 101 deny ip 255.0.0.0 0.255.255.255 any
```

Deny all of the private non-routable address groups:

```
GIAC-Border(config)#access-list 101 deny ip 169.254.0.0 0.0.255.255 any
GIAC-Border(config)#access-list 101 deny ip 240.0.0.0 31.255.255.255 any
GIAC-Border(config)#access-list 101 deny ip 248.0.0.0 31.255.255.255 any
```

We do not have a need to use any of the login services (i.e. ftp, telnet, exec, lpd), so let us block all of those:

```
GIAC-Border(config)#access-list 101 deny tcp any any range ftp telnet
GIAC-Border(config)#access-list 101 deny tcp any any range exec lpd
```

We do not any sunrpc or nfs running to/from the internet, so block them:

```
GIAC-Border(config)#access-list 101 deny udp any any eq sunrpc
GIAC-Border(config)#access-list 101 deny tcp any any eq sunrpc
GIAC-Border(config)#access-list 101 deny udp any any eq 2049
GIAC-Border(config)#access-list 101 deny tcp any any eq 2049
GIAC-Border(config)#access-list 101 deny udp any any eq 4045
```

```
GIAC-Border(config)#access-list 101 deny tcp any any eq 4045
```

We do not need NetBios going in and out either, so block all of it:

```
GIAC-Border(config)#access-list 101 deny tcp any any 135
GIAC-Border(config)#access-list 101 deny udp any any 135
GIAC-Border(config)#access-list 101 deny udp any any range 137 138
GIAC-Border(config)#access-list 101 deny tcp any any eq 139
GIAC-Border(config)#access-list 101 deny tcp any any eq 445
GIAC-Border(config)#access-list 101 deny udp any any eq 445
```

We should also block the X-Windows ports:

```
GIAC-Border(config)#access-list 101 deny tcp any any range 6000 6255
```

We have no need for LDAP access to/from our network, so block that out too:

```
GIAC-Border(config)#access-list 101 deny tcp any any eq 389
GIAC-Border(config)#access-list 101 deny udp any any eq 389
```

We should not see our public IP addresses coming in from the internet, so deny them:

```
GIAC-Border(config)#access-list 101 deny ip x.y.69.144 0.0.0.240 any
GIAC-Border(config)#access-list 101 deny ip x.y.69.160 0.0.0.240 any
GIAC-Border(config)#access-list 101 deny ip x.y.69.176 0.0.0.240 any
```

Permit only type 0 (Echo Reply) and type 8 (Echo Request) ICMP packets through. Both of these are important debugging aids:

```
GIAC-Border(config)#access-list 101 permit icmp any x.y.69.144 0.0.0.15 echo
GIAC-Border(config)#access-list 101 permit icmp any x.y.69.144 0.0.0.15 echo-reply
```

Last, we deny everything else. Cisco access lists by default deny anything that does not match any of the rules. However, placing this last rule on the list helps us to see that everything else is denied:

```
GIAC-Border(config)#access-list 101 deny ip any any
```

Now that we have all of our inbound rules defined let us apply them to the interface that we designed them for (i.e. Serial 0).

To activate the rules we need to go into the interface configuration mode for the Serial 0 interface on the Cisco router and enter the following instructions:

```
GIAC-Border(config-if)#ip access-group 101 in
```


Now let us define our Egress filter rules. For this we will once again use a numbered extended access list. These rules are also entered in Global configuration mode. We will use access list number 102 for our outbound filter on Serial 0:

The first ACL is here to help speed up processing of sessions that have already been established:

```
GIAC-Border(config)#access-list 102 permit tcp any any established
```

The next set of ACL's allow SMTP and HTTP (Normal and Encrypted) traffic thru:

```
GIAC-Border(config)#access-list 102 permit tcp host 209.69.100.146 any eq smtp
```

```
GIAC-Border(config)#access-list 102 permit tcp any any eq 80
```

```
GIAC-Border(config)#access-list 102 permit tcp any any eq 443
```

This set of ACL's will allow DNS queries and zone transfers thru:

```
GIAC-Border(config)#access-list 102 permit udp any any eq 53
```

```
GIAC-Border(config)#access-list 102 permit host x.y.69.162 tcp host a.b.35.250 eq 53
```

```
GIAC-Border(config)#access-list 102 permit icmp x.y.69.144 0.0.0.15 any
```

Last, we deny everything else.

```
GIAC-Border(config)#access-list 102 deny ip any any
```

Now that we have all of our outbound rules defined let us apply them to the interface that we designed them for (i.e. Serial 0).

To activate the rules we need to go into the interface configuration mode for the Serial 0 interface on the Cisco router and enter the following instructions:

```
GIAC-Border(config-if)#ip access-group 102 in
```

Now all of our Ingress and Egress rules are in place. Next, we need to secure the router by making sure certain services are disabled and that the rest of the configuration is done correctly. First let's start by defining a default static route. This is done in Global configuration mode. This route tells the router where to send the traffic that it does not have a route to.

```
GIAC-Border(config)#ip route 0.0.0.0 0.0.0.0 x.y.1.125
```

By using a static route we reduce the chances of getting route poisoning in our router.

Next we will remove the capability to telnet into the router. We are setting up the router this way because we are on-site with it and we have no need to access the router across a network. The first line defines a standard access list that deny's everything. The next line gets us into line configuration mode. The last two lines apply the standard access list to the virtual terminals numbered 0 thru 4.

```
GIAC-Border(config)#access-list 10 deny any
GIAC-Border(config)#line vty 0 4
GIAC-Border(config-line)#access-group 10 in
GIAC-Border(config-line)#access-group 10 out
```

Next, we should turn off a lot of services that we do not need on the router.

```
GIAC-Border(config)#no snmp
GIAC-Border(config)#no snmp-server location
GIAC-Border(config)#no snmp-server contact
GIAC-Border(config)#no snmp-server enable traps
GIAC-Border(config)#no ip source-route
GIAC-Border(config)#service password-encryption
GIAC-Border(config)#enable secret
GIAC-Border(config)#no service tcp-small-servers
GIAC-Border(config)#no service udp-small-servers
GIAC-Border(config)#no service finger
GIAC-Border(config)#no service pad
GIAC-Border(config)#no cdp run
GIAC-Border(config)#no ip http server
GIAC-Border(config)#no ip bootp server
GIAC-Border(config)#no service dhcp
GIAC-Border(config)#no ip domain-lookup
```

Now we need to turn off a few more services that are applied to the Serial 0 Interface.

```
GIAC-Border(config-if)#no ip unreachable
GIAC-Border(config-if)#no ip direct-broadcast
GIAC-Border(config-if)#no ip redirects
```

Let's display a warning banner on all incoming accessible links that clearly states that only authorized personnel should access the router.

```
GIAC-Border(config)#banner motd "Authorized Personnel Only!!!"
GIAC-Border(config)#banner exec "Now entering User EXEC mode. Authorized
Personnel Only!!!"
GIAC-Border(config)#banner incoming "Authorized Personnel Only!!!"
GIAC-Border(config)#banner login "Authorized Personnel Only!!!"
```

2.5 External Firewall

The rules used by FW-1 are processed much like the Cisco Border Router. They are processed from the top down and we should put the most commonly used rules at the top of the list to help reduce CPU cycles.

Table 4: External Firewall Rules

| Rule # | Source | Destination | Service | Action | Track |
|--------|-------------------|--------------------|------------|--------|-------|
| 1 | Fw_admin | Firewall | firewall-1 | Accept | Log |
| 2 | Any | Firewall | NBT/ident | Reject | |
| 3 | Any | Firewall | any | Drop | Log |
| 4 | Any | ReverseProxyServer | http80 | Accept | Log |
| 5 | Any | ReverseProxyServer | http443 | Accept | Log |
| 6 | Any | ExternalDns | udp53 | Accept | Log |
| 7 | ExternalDns | ISPDns | tcp53 | Accept | Log |
| 8 | Any | MailRelayServer | smtp | Accept | Log |
| 9 | Partners | VPN | IPSEC | Accept | Log |
| 10 | Suppliers | VPN | IPSEC | Accept | Log |
| 11 | VPN | SupplierWebServer | 80 | Accept | Log |
| 12 | VPN | PartnerWebServer | 80 | Accept | Log |
| 13 | InternalDns | ExternalDNS | udp53 | Accept | Log |
| 14 | InternalMachines | ProxyServer | http80 | Accept | Log |
| 15 | InternalMachines | ProxyServer | http443 | Accept | Log |
| 16 | CustomerWebServer | CustomerDB | sqlnet | Accept | Log |
| 17 | SupplierWebServer | SupplierDB | sqlnet | Accept | Log |
| 18 | PartnerWebServer | PartnerDB | sqlnet | Accept | Log |
| 19 | LoggingMachines | LoggingServer | udp514 | Accept | Log |
| 20 | Any | Any | Any | Drop | Log |

Breakdown of what the rules are doing:

- Rule #1 This allows authorized machines to connect to the firewall to manage it. This is very important.
- Rule #2 This blocks all NetBIOS/indent traffic. The firewall adds to our Defense in Depth by backing up the Border Router, which is also blocking this traffic.
- Rule #3 Whenever anyone else tries to talk directly to the firewall; it drops the traffic and logs it.
- Rule #4 Allow outside users access to the Reverse Proxy Server via tcp port 80. This gives our Customers a front-end to access their web-server through.
- Rule #5 Allow outside users access to the Reverse Proxy Server via tcp port 443. This gives our Customers a front-end SSL encrypted access to their web-server.
- Rule #6 Allow outside users to query our External DNS server.
- Rule #7 Allow our External DNS server to perform zone transfers with our ISP's DNS server.

- Rule #8 Allow outside mailservers to communicate with our Mail Relay Server via tcp port 25.
- Rule #9 Allow our partners to access the VPN device on our network.
- Rule #10 Allow our suppliers to access the VPN device on our network.
- Rule #11 Allow the VPN to send traffic to the Suppliers Web Server.
- Rule #12 Allow the VPN to send traffic to the Partners Web Server.
- Rule #13 Allow our Internal DNS server to forward requests that it can not resolve to our External DNS server.
- Rule #14 Allow our Internal machines to talk to the Proxy Server for outbound HTTP connections via tcp port 80.
- Rule #15 Allow our Internal machines to talk to the Proxy Server for outbound HTTP connections via tcp port 443.
- Rule #16 Allow the Customer Web Server to communicate with the Customer Database Server.
- Rule #17 Allow the Supplier Web Server to communicate with the Supplier Database Server.
- Rule #18 Allow the Partner Web Server to communicate with the Partner Database Server.
- Rule #19 Allow any logging machine to communicate with the central logging server.
- Rule #20 Drop all other packets and log them.

2.6 Cisco VPN 3060 Concentrator

In setting up the VPN Concentrator we must choose an authentication method. The Concentrator can use either a RADIUS server, an NT Domain, a RSA SecurID or an internal list. For this case I have chosen to use an internal list. While it is very likely that we will have a NT Domain in our network, it has been my experience that allowing the users to have the same password for accessing the internal network resources and accessing the network remotely creates a security concern. By using an internal list, the user will have to maintain a separate, and hopefully, different password than what is used on the internal resources.

Figure 2: Cisco VPN 3000 Concentrator Series Manager Screen-Shot

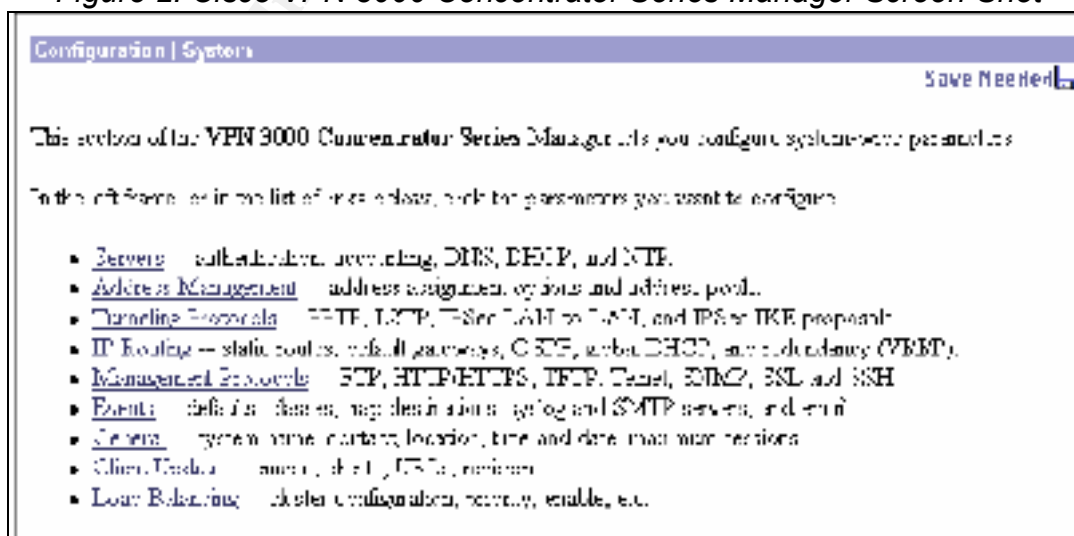
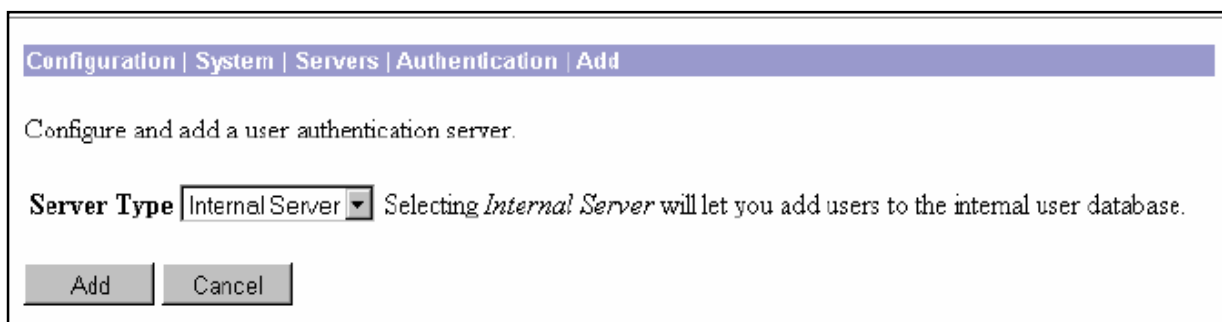


Figure 3: Cisco VPN Server Type Selection Screen-Shot

Configuration | System | Servers | Authentication | Add

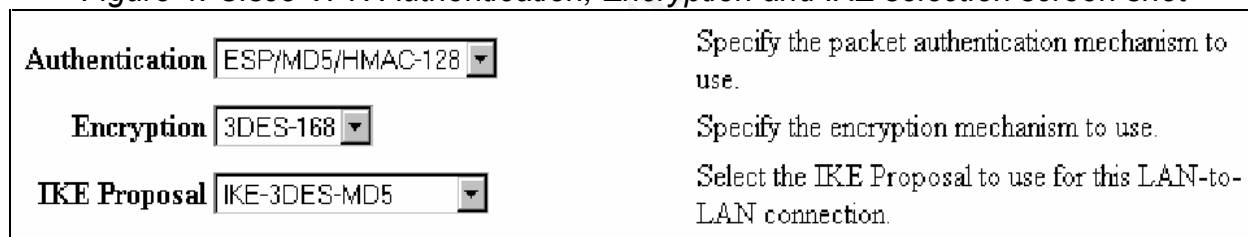
Configure and add a user authentication server.

Server Type Internal Server Selecting *Internal Server* will let you add users to the internal user database.

Add Cancel

I have chosen to use IPSec as the encryption protocol. We will require the IPSec protocol to be configured because we have decided to deploy Cisco's VPN Concentrator client software to all remote access users.

A "Peer" connection is a remote-access client or another secure gateway. When establishing the tunnel using IPSec, the two peers negotiate Security Associations (SA) that will govern authentication, encryption, encapsulation, key management, etc. I have chosen ESP-MD5-HMAC-128 as the authentication algorithm and 3DES-168 as the encryption algorithm. Both of these are the most secure selection available.

Figure 4: Cisco VPN Authentication, Encryption and IKE selection screen-shot

| | | |
|-----------------------|------------------|--|
| Authentication | ESP/MD5/HMAC-128 | Specify the packet authentication mechanism to use. |
| Encryption | 3DES-168 | Specify the encryption mechanism to use. |
| IKE Proposal | IKE-3DES-MD5 | Select the IKE Proposal to use for this LAN-to-LAN connection. |

In the illustration below I have selected 3DES for the type of encryption this group will be required to use. Note that I have also declined the ability to use Split Tunneling. The internal database is also shown as the authentication method selected for the base group configuration.

Figure 5: Cisco VPN Configuration Screen-Shot

Configuration | User Management | User Group

General | IPSec | IPsec/VPN

IPSec Parameters

| Attribute | Value | Description |
|------------------------------|-----------------------------|--|
| IPSec SA | IPsec SA | Select the IPSec Security Association assigned to this group. |
| IKE Peer Identity Validation | Not required by certificate | Select whether or not to validate the identity of the peer using the peer's certificate. |
| ECB Encapsulation | <input type="checkbox"/> | Check to enable the use of IKE Encapsulation for users of this group. |
| Reauthentication on Rekey | <input type="checkbox"/> | Check to reauthenticate the peer on an IKE (Phase-1) rekey. |
| Tunnel Type | Remote Access | Select the type of tunnel for this group. Update the Remote Access parameters below as needed. |

Remote Access Parameters

| | | |
|--------------------|--------------------------|--|
| Group Lock | <input type="checkbox"/> | Lock the users into this group. |
| Authentication | Internet | Select the authentication method for users in this group. |
| IPComp | None | Select the method of IP Compression for members of this group. |
| Mode Configuration | <input type="checkbox"/> | Check to initiate the exchange of Mode Configuration parameters with the client. This may be checked if version 2.0 (or earlier) of the Cisco Client is being used by members of this group. |

Mode Configuration Parameters

| | | |
|----------------------------------|--------------------------|--|
| Banner | | Enter the banner for this user. |
| Allow Password Storage on Client | <input type="checkbox"/> | Check to allow the IPSec client to store the password locally. |
| Split Tunneling Network List | None | Select the Network List to be used for Split Tunneling. |
| Default Domain Name | | Provide the default domain name given to users of this group. |
| IPSec through NAT | <input type="checkbox"/> | Check to allow the IPSec client to operate through a firewall using NAT via UDP. |
| IPSec through NAT UDP Port | 4001 | Provide the UDP port to be used for IPSec through NAT (4001 - 4015). |

Apply Cancel

Here's where I select the type of encryption for this group

Here's where the Authentication method is selected.

The is where I have chosen to NOT allow Split tunneling

The 3060 uses a filter to determine whether to forward or drop a data packet coming through it. The filter examines the data packet according to one or more rules (direction, source address, destination address, ports, and/or protocol), which determine whether to forward, apply IPSec and forward, or drop the packet. As with the Cisco Border Router, the VPN concentrator examines the rules in the order they are arranged in the filter. Therefore place the more specific rules higher in the order and the general rules lower in the order.

Filters are applied to Ethernet interfaces, and thus govern all traffic through an interface. Filters are also applied to groups and users, and thus govern tunneled traffic through an interface. The table below represents the VPN filter configuration of how traffic flows for remote access.

Table 5: Cisco VPN filter configuration/traffic flow rules

| Filter Rule | Direction | Protocol | Source Address | Destination Address | Source Port | Destination Port | Action |
|--------------|-----------|----------|----------------|---------------------|-------------|------------------|-------------|
| HTTP In | In | TCP | 0.0.0.0 | 0.0.0.0 | 0-65535 | 80 | Forward/Log |
| HTTP Out | Out | TCP | 0.0.0.0 | 0.0.0.0 | 80 | 0-65535 | Forward/Log |
| HTTPS In | In | TCP | 0.0.0.0 | 0.0.0.0 | 0-65535 | 443 | Forward/Log |
| HTTPS Out | Out | TCP | 0.0.0.0 | 0.0.0.0 | 443 | 0-65535 | Forward/Log |
| IPSec-ESP In | In | ESP | 0.0.0.0 | 0.0.0.0 | IPsec | IPsec | IPSec/Log |

2.6.1 Client Configuration

With the VPN Concentrator configured, the next part is to configure the VPN access client. The IPSec client connects to the VPN Concentrator via a group name and password, and then the system authenticates a user via a username and password. Encryption and authentication options have been configured on the 3060 Concentrator, which requires remote users to negotiate the specified setting to be able to obtain remote access. For maximum security, we will not allow password storage (caching) on the client; users must enter their password each time they wish to access the VPN. For complete instructions on how to install the client software, please see the [Client Concentrator documentation](#).

2.7 Internal Firewall

We'll start setting up our Internal Firewall rules on our Linux PC running IPTables. But what exactly are IPTables? To start, you need to know how the firewall treats packets that are leaving, entering, or passing through your computer.

There is a chain for each of these: Any packet entering your computer goes through the INPUT chain. Any packet that your computer sends out to the network goes through the OUTPUT chain. Any packet that your computer picks up on one network and sends to another goes through the FORWARD chain. The chains are only half of the story.

Next you set up certain rules in each of these chains that decide what happens to packets of data that pass through them. For instance, if your computer was to send out a packet to www.sans.org to request an HTML page, it would first pass through the OUTPUT chain. The kernel would look through the rules in the chain and see if any of them match. The first one that matches will decide the outcome of that packet. If none of the rules match, then the policy of the whole chain will be the final decision maker. Then whatever reply SANS sent back would pass through the INPUT chain.

So let's start with manipulation of certain IP addresses. Suppose you wanted to block all packets coming from 24.10.10.1. First of all, -s is used to specify a source IP or DNS name. So from that, to refer to traffic coming from this address, we would use this:

```
iptables -s 24.10.10.1
```

But that doesn't tell what to do with the packets. The -j option is used to specify what happens to the packet. The most common three are ACCEPT, DENY, and DROP. It is obvious what ACCEPT does. DENY sends a message back that we are not accepting connections. DROP just totally ignores the packet. If we are really suspicious about this certain IP address, we would probably prefer DROP over DENY. So here is the command with the result:

```
iptables -s 24.10.10.1 -j DROP
```

But the computer still will not understand this. There is one more thing we need to add and that is which chain it goes on. You use -A for this. It just appends the rule to the end of whichever chain you specify. Since we want to keep the computer from talking to us, we would put it on INPUT. So here is the entire command:

```
iptables -A INPUT -s 24.10.10.1 -j DROP
```

This single command would ignore everything coming from 24.10.10.1.

So, with this in mind we will start setting up our Internal Firewall rules by defining the default actions. They are defined to drop all packets that enter the firewall. We will grant access to the connections that we want to allow.

```
iptables -p In DROP  
iptables -p Out DROP  
iptables -P Forward DROP
```

Next, we are going to set up a rule to block all NULL packets:

```
iptables -A In -p tcp --tcp-flags ALL NONE -j DROP  
iptables -A Forward -p tcp --tcp-flags ALL NONE -j DROP
```

Now we are going to set up a rule to block all packets that have all of their flags set (also known as Christmas packets).

```
iptables -A Input -p tcp --tcp-flags ALL ALL -j DROP  
iptables -A Forward -p tcp --tcp-flags ALL ALL -j DROP
```

Now we need to allow the traffic from our Customer, Supplier and Partner Web Servers across to their respective DB servers.

```
iptables -t nat -A PREROUTING -i eth0 -s x.y.69.166 -dport sqlnet -j DNAT --to \\\n192.168.3.13  
iptables -t nat -A PREROUTING -i eth0 -s x.y.69.167 -dport sqlnet -j DNAT --to \\\n192.168.3.14
```



```
iptables -t nat -A PREROUTING -i eth0 -s x.y.69.168 -dport sqlnet -j DNAT --to \
192.168.3.15
```

We also need to make sure that the traffic can get back from the DB servers to the appropriate Web Server.

```
iptables -t nat -A PREROUTING -i eth1 -s 192.168.3.13 -dport sqlnet -j DNAT --to \
x.y.69.166
iptables -t nat -A PREROUTING -i eth1 -s 192.168.3.14 -dport sqlnet -j DNAT --to \
x.y.69.167
iptables -t nat -A PREROUTING -i eth1 -s 192.168.3.15 -dport sqlnet -j DNAT --to \
x.y.69.168
```

Now we need to allow access from the GIAC Internal LAN to the rest of the network, according to our security policy.

```
iptables -t nat -A PREROUTING -i eth2 -s 192.168.2.0/24 -dport 80 -j DNAT --to \
x.y.69.164
iptables -t nat -A PREROUTING -i eth2 -s 192.168.2.0/24 -dport 25 -j DNAT --to \
x.y.69.165
iptables -t nat -A PREROUTING -i eth2 -s 192.168.2.0/24 -dport 53 -j DNAT --to \
x.y.69.162
iptables -t nat -A PREROUTING -i eth0 -dport 514 -j DNAT -o eth2 --to 192.168.2.201
```

Much more information can be learned about setting up iptables by searching <http://www.google.com> with the words iptables or netfilter.

Auditing the Security Architecture

3.1 Planning the assessment

For our network audit we want to test each layer of the perimeter defenses independently. This includes testing our border router, our external firewall, our internal firewall and our DNS servers (both internal and external). The purpose of this is to validate each layer of the defense structure. Therefore, we start on the outside and work our way in. The last item to check would be our logs to verify that they detected the audit.

Most of the testing we will be doing will not be destructive or disruptive in nature. However, we want to make certain that we can call off the audit if it turns up any major problems. Therefore, all of the contact numbers for the security team, the network admin team, and the help desk will be made available for the duration of the audit. Most of the work will be done during the evening hours to minimize the risks to the network and to GIAC's customers. We have allocated 8 man-hours per segment for auditing. This puts our total estimate at 32 man-hours.

Before any testing can be done we will gather information by performing an on-site visit. We will check for the following items:

- An up-to-date copy of the Information Security Policy.
- A current network diagram.
- After reviewing the current copy of the Information Security Policy, we will tour the facility and verify that everything adheres to that policy.
- A current copy of the firewall configuration rule-set.
- A current copy of the border router configuration rules.
- Check all of the network defense components to verify that they are physically secure.

We would also begin to do data reconnaissance by utilizing various tools:

- Nslookup or [sam spade](#): use these tools to query the DNS servers. Also attempt to do a zone transfer.
- Whois: query against the Internic whois database ([whois.networksolutions.com](#), [whois.internic.net](#) and [whois.arin.net](#)). Gather contact information, IP network information and domain information.
- [Netcat](#): Gather any banner information that you can.

Last, we need to obtain written authorization from GIAC Enterprises management team.

3.2 Implementing the assessment

We'll start our assessment by using a popular scanning tool called [nmap](#). We will perform the TCP SYN stealth port scan against the firewall. The screen shot below shows the command line and it's results:

Figure 6: nmap Screen-Shot #1

```

C:\GCFW\nmap -v -s -P0 192.168.1.45

Starting nmap v. 2.53 by igmp@Egy.com
Egy Digital Security : http://www.Egy.com/
Learn on nmap by igmp@Egy.com : http://www.Egy.com/nmap/

Initiating SYN Stealth Scan against 192.168.1.45
Adding TCP port 25 (state open).
Adding TCP port 53 (state open).
Adding TCP port 80 (state open).
Adding TCP port 443 (state open).

The SYN scan took 14 seconds to scan 1328 ports.
Involving ports on 192.168.1.45:
Port      State      Service
25/tcp    filtered   smtp
53/tcp    filtered   domain
80/tcp    filtered   http
443/tcp   filtered   https

nmap run completed - 1 IP address (1 host) scanned in 35 seconds
C:\GCFW>
  
```

Here you see the only TCP ports nmap found available.

As we can see the only open TCP ports are port 25, 53, 80 and 443. According to our security policy, this is what we should expect to see. Good! Next we perform a UDP scan as shown below:

Figure 7: nmap Screen-Shot #2

```

C:\GCFW\nmap -v -u 192.168.1.45

Starting nmap v. 2.53 by igmp@Egy.com
Egy Digital Security : http://www.Egy.com/
Learn on nmap by igmp@Egy.com : http://www.Egy.com/nmap/

Port 192.168.1.45 appears to be up & going.
Initiating FIN, NULL, UDP, or Xmas Stealth Scan against 192.168.1.45
The UDP or stealth FIN, NULL, XMAS scan took 113 seconds to scan 1443 ports.
Involving ports on 192.168.1.45:
Port      State      Service
53/udp    open       domain
All 1443 scanned ports on 192.168.1.45 were filtered

nmap run completed - 1 IP address (1 host) scanned in 118 seconds
C:\GCFW>
  
```

Here you can see the only UDP port that nmap could find.

This shows exactly what we should expect to see, only UDP port 53 open. Next, we would perform the same scans from within the network and verify the results against our security policy for outbound ports.

Then, we would check our audit logs and verify that the logs reported the scans taking place.

Last, we will need to audit all of the VISA security requirements and verify that we are complying with the requirements. Auditing for each of the requirements will be done as follows:

1. Perform the complete assessment on the network as previously described.
2. Randomly check several hosts/servers and verify that their Operating Systems are patched completely and properly.
3. Use tools like grep (Unix) and find (Windows) to verify that the database servers are storing the data in encrypted format.
4. Use packet sniffing to verify that critical data going across any open network is encrypted.
5. Randomly check the version and anti-virus data files on several hosts/servers. Be sure to include the SMTP Relay Server in this audit. Verify that all are running with the most current software revision and latest anti-virus definitions. Last, verify that all systems are set up on a centralized, automated update system.
6. Randomly check users permissions while they are logged into the network. Compare results with documented permissions/guidelines. Verify that passwords are globally set to expire as per company password lifetime policy.
7. Obtain a copy of all usernames. Verify that each user has there own account. Randomly check several of the user accounts and verify that they have been used recently.
8. Using a map of the network and an equipment list, login to each component with the default username and password. Also, obtain a copy of the password file and run [l0phtcrack](#) against it.
9. Obtain a copy of audit logs. Verify that each audit record has a user id attached to it.
10. Divide the entire security infrastructure into 5 pieces. Schedule an audit of 1 piece per month for the next five months. On the 6th month, perform a complete security audit.
11. Retrieve latest copy of the Information Security Policy. Review the policy and update where necessary. Distribute a reminder to all employees and contractors once per year. Verify that human resources has the latest copy to show/explain to new/terminated employees.
12. Check physical security of all servers and verify that access is restricted to authorized personnel only. Verify off-site tape rotation logs and authorized access lists. Confirm that all off-site tapes are stored in a secure off-site location.

3.3 Conduct a perimeter analysis

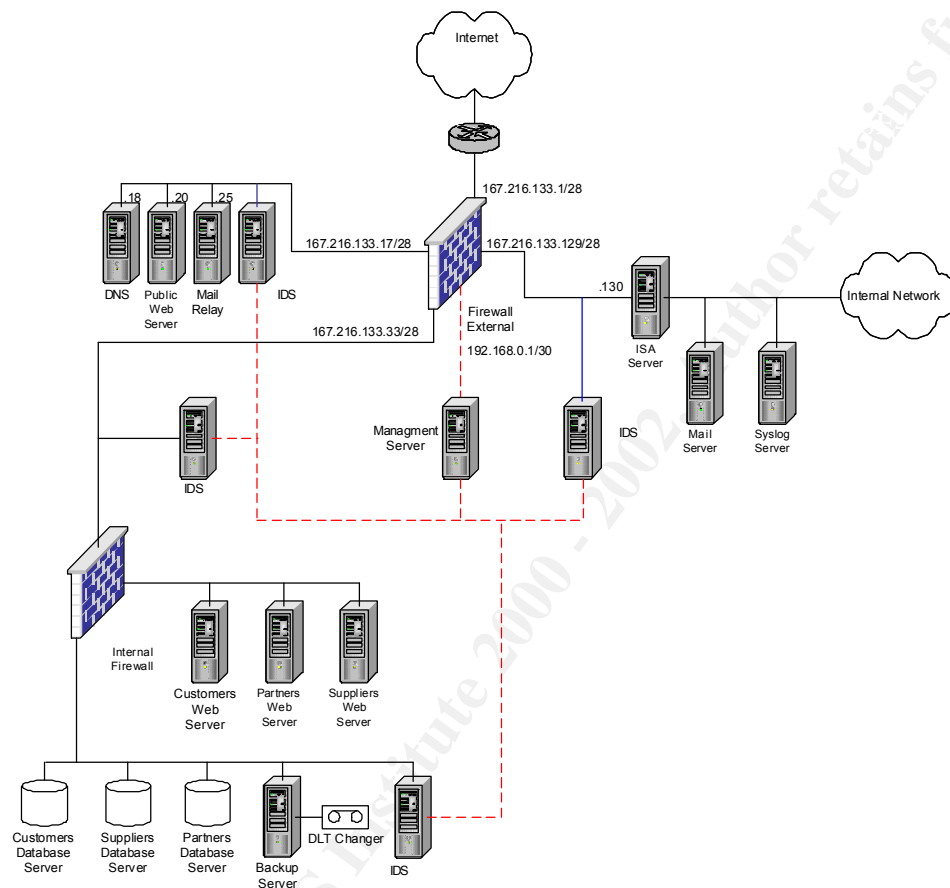
In reviewing the recent assessment I would make the following recommendations for improvement:

1. The Internet connectivity for both customers and employees is a shared connection. This creates the potential for having the employees hog the bandwidth on this shared connection, intentionally or otherwise. Therefore the Internet connection for the Customers web site should be split off and put on it's own connection. The Suppliers and Partners connections can remain on the same connection that the employees use.
2. The border router is set-up properly and currently in good working order. We could increase traffic security by adding another layer of defense to our perimeter. To do this, we would modify the current extended access lists to include reflexive access lists nested within them. This would give the border router stateful-inspection capability and add on to the layer of defense that the external firewall provides.
3. Set up a system to automatically rotate and archive all log files for future reference and data analysis.
4. Define a baseline on all critical systems, including but not limited to all servers, routers and firewalls. Define a policy to compare the baselines with actual system performance on a regular basis.
5. Set-up a time server to synchronize all of the clocks on the servers and most importantly the IDS sensors and syslog server.
6. Move the reverse-proxy server to it's own service network. This would help isolate it from the rest of the machines on the service network, just in case it gets compromised.

Design Under Fire

Choosing a target

I have chosen the GCFW practical done by Davey Rance, which can be found at http://www.sans.org/y2k/practical/Davey_Rance_GCFW.doc



Mr. Rance's architecture breakdown is as follows (taken directly from his practical):

Border Router

Cisco 3640 running IOS version 12.1.03

The Border router's main function is to route packets to and from the Internet and the internal networks. It will also provide a base security filter including ingress and egress. The connection to the Internet is via a 2 Mbit serial link.

External Firewall

Cisco PIX 525 Running IOS version 5.3(1)

IPSec Hardware VPN Accelerator Card (VAC) 4 Port network card

The External Firewall will terminate the VPN connections for incoming customers, partners and suppliers. Implementing the main security policy as defined by GIAC and protecting the internal firewall and servers from DOS attacks where possible. The security policy of the firewall will be to DENY everything with the exception of specific ports and IP addresses that allow users to access servers.

4.1 An attack against the firewall itself

Mr. Rance's design is utilizing a Cisco PIX firewall 525 running IOS v5.3(1) with a IPSec Hardware VPN Accelerator Card. A search for known vulnerabilities on Cisco PIX firewalls was done by checking www.securityfocus.com. No known vulnerabilities were found against the Cisco PIX with this version of IOS running.

A search at www.google.com using keywords "Cisco PIX 5.3 vulnerability" turned up the following item: http://www.opennet.ru/base/sco/988181601_1697.txt.html. The link notes an item sent to securityfocus back in March of 2001 regarding several vulnerabilities in the Cisco PIX firewall running IOS 5.3(1).

One of the vulnerabilities documented shows a problem with the PIX not properly checking for spoofing when SSH is enabled. While Mr. Rance's practical does not indicate the status of the SSH port of the firewall he does indicate that the logs from his DNS server, Public Web Server and Mail Relay Server will be pulled to the syslog server via SSH. This means the SSH traffic will have to go through the PIX firewall. While none of this is conclusive, it would lead me to at least try this attack against the firewall. If the attack succeeds it would at least give me the ability to attack the firewall on the SSH port. The writing of the above mentioned document is not clear on what the outcome would be of this attack method.

A message posted at <http://archives.linuxbe.org/arch051/0992.html> shows Cisco's response to the above-mentioned document. It indicates, for this particular attack, that the problem has been resolved with the defect ID CSCdt02132, which is available via an interim version of the Cisco IOS v5.3 software. The PIX will verify the permission status with the SSH list before replying to a TCP connection setup.

4.2 A denial of service attack

The goal of a DOS attack is to deny valid users access to the resources available at the target site. In this case we would be denying GIAC's customers, suppliers, partners and remote workers access to the entire GIAC Enterprises network. Utilizing the 50 compromised cable modem/DSL systems I would launch an attack by sending a flood of large UDP packets at the external firewall interface (167.216.133.1).

At this point I would recommend changing the Ingress filters on the border router to drop the packets immediately. However, once this is done there is nothing preventing

the attack from being changed to attack the external side of the border router itself. Because there is only a 2 Mbit serial link to the Internet in Mr. Rance's design it would be flooded with this bogus traffic very easily. Please note, for more good reading on this type of attack I would recommend reading about the attack on the grc.com network at <http://grc.com/dos/grcdos.htm>. I do not agree with everything in the details of the attack on grc, but it does document this type of DOS attack very well.

The best countermeasure that we can implement at this point would be to change the Ingress filters on the border router. If this type of attack is aimed at the external border router interface, then there is very little that can be done with the current network design. To prevent this type of situation we would need to split the connection to the Internet and utilize 2 or more connections to the Internet. We would have to implement a load balancing solution to allow outside users to connect to our network via whichever link is least used.

4.3 An attack plan to compromise an internal system

For this I have decided to attack Mr. Rance's Public Web Server. The web server is already open to the Internet via ports 80 and 443. Although Mr. Rance has indicated that all appropriate patches and hotfixes have been applied I would attempt to run the IIS 5.0 Printer ISAPI Buffer Overflow exploit against it. This is a relatively new exploit, being discovered on May 1, 2001 by Riley Hassell of [eEye Digital Security](http://www.eeye.com). I would hope to get in before the GIAC security team has a chance to apply the appropriate hotfix. As was recently shown by the Code Red Worm and the number of vulnerable IIS systems available on the Internet, it stands to reason that I would have a good chance of using such a recently discovered vulnerability successfully. The reason I choose to attack this server is that it provided a relatively easy target because of the frequent flaws found in Microsoft products. Especially those related to running IIS services.

The process involved in attacking the system is as follows. I would craft an HTTP .print request containing approximately 420 bytes in the 'Host:' field. Once sent to the Public Web Server it would cause a buffer overflow error in inetinfo.exe. Typically a web server would stop responding in a buffer overflow condition; however, once Windows 2000 detects an unresponsive web server it automatically performs a restart of the Internet services. The restart then allows the malicious code to run at system level context with administrative rights and permissions. This attack would give me full control of the Web Server.

References:

1. ARIN database available at: <http://www.arin.net/whois/>
2. Arthiabah, Kofi "GIAC Firewall and Perimeter Protection Practical Assignment for Parliament Hill". Available at http://www.sans.org/y2k/practical/Kofi_Arthiabah.zip
3. Baltimore Technologies plc. Mimesweeper for SMTP v4.2. Available at: <http://www.us.mimesweeper.com/products/msw4smtp/default.asp>
4. BIND DNS software. Available at <http://www.isc.org/products/BIND/>
5. Brenton, Chris. "2.2 Firewalls 101: Perimeter Protection with Firewalls". Baltimore: SANS Institute, May 14th, 2001.
6. Brenton, Chris. "2.3 Firewalls 102: Perimeter Protections and Defense, In-Depth". Baltimore: SANS Institute, May 15th, 2001.
7. Brenton, Chris. "2.4 VPNs and Remote Access". Baltimore: SANS Institute, May 16th, 2001.
8. Brenton, Chris. "2.5 Network Design and Performance". Baltimore: SANS Institute, May 17th, 2001.
9. Brenton, Chris. "FUBAR Computer Use Policy Template". Baltimore SANS Conference, May 15th, 2001
10. Brown, Matthew "GIAC Training and Certification SANS 2001 New Orleans GCFW Practical". Available at http://www.sans.org/y2k/practical/Matthew_Brown_GCFW.zip
11. CERT/CC Advisories available at: <http://www.cert.org/>
12. CheckPoint Firewall-1. Available at: <http://www.checkpoint.com/products/firewall-1/index.html>
13. Cisco Systems, Inc. "Building a Perimeter Security Solution with the Cisco Secure Integrated Software". Available at http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/tech/firew_wp.htm. Posted on September 17th, 2000.
14. Cisco Systems, Inc. [Cisco 3640 border router](#)
15. Cisco Systems, Inc. [Cisco VPN 3060 Concentrator](#)

16. Cisco Systems, Inc. "Cisco 3060 VPN Client Configuration". Available at: [Client Concentrator documentation](#).
17. Cisco Systems, Inc. "Using the Command Line Interface". Available at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt1/fcui.htm#15788. Posted April 28th, 1999.
18. Cisco Systems, Inc. Packet Filtering. Available at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/pcprt1/1cfip.htm#xtocid420214
19. CyberCop Scanner available at: <http://www.nai.com>
20. General UNIX hardening suggestions compiled by CERT: http://www.cert.org/tech_tips/unix+configuration_guidelines.html
21. Gibson, Steve "The Strange Tale of the Denial of Service Attacks against GRC.COM" Available at: <http://grc.com/dos/grcdos.htm>. Posted on July 4th, 2001.
22. Internet search engine google.com available at www.google.com
23. l0phtcrack v3.0: <http://www.atstake.com/research/lc3/index.html>
24. Linux Operating System. Available at <http://www.linux.org/>
25. Linux Kernel v2.4.7 available at <http://www.kernel.org/>
26. Martin, Daniel "GIAC Certified Firewall Analyst Practical". Available at http://www.sans.org/y2k/practical/Daniel_Martin_GCFW.doc
27. Microsoft "Microsoft Security Bulletin MS01-023 - Unchecked Buffer in ISAPI Extension Could Enable Compromise of IIS 5.0 Server" Available at: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-023.asp>. Posted on May 1st, 2001.
28. Microsoft Windows 2000 Server. Available at <http://www.microsoft.com/windows2000/serverf/default.asp>
29. Microsoft Exchange Server 2000. Available at <http://www.microsoft.com/exchange/default.asp>
30. Microsoft ISA Server 2000. Available at <http://www.microsoft.com/proxy>

31. Napier, Lisa "Re: Cisco PIX Security Notes *Vendor Response*". Available at: <http://archives.linuxbe.org/arch051/0992.html>. Posted on March 16th, 2001.
32. Natcat. Available at: <http://www.atstake.com/research/tools/index.html>
33. Netfilter. Available at <http://netfilter.samba.org/>
34. NetSonar available at: <http://www.cisco.com/warp/public/778/security/netsonar/>
35. Network Mapper (Nmap) available at: <http://www.insecure.org/nmap>
36. Olree, Kevin "GIAC Level 2: Firewall, Perimeter Protections and VPNs". Available at http://www.sans.org/y2k/practical/Kevin_Olree_GCFW.doc
37. PentaSafe Security available at: <http://www.pentasafe.com/>
38. Pietrosanti, Fabio "Cisco PIX Security Notes". Available at: http://www.opennet.ru/base/sco/988181601_1697.txt.html. Posted on March 9th, 2001
39. Pincock, Corey "Secure Windows Initiative Trail by Fire: IIS 5.0 Printer ISAPI Buffer Overflow". Available at: <http://www.sans.org/infosecFAQ/win2000/trial.htm>. Posted on June 7th, 2001.
40. Rance, Davey "Firewalls, Perimeter Protection and VPNs. GCFW Practical Assignment". Available at http://www.sans.org/y2k/practical/Davey_Rance_GCFW.doc
41. RFC 1918 : <http://rfc.fh-koeln.de/rfc/html/rfc1918.html>
42. Rounthwaite, Matt "GIAC Enterprises Security Architecture Assignment". Available at http://www.sans.org/y2k/practical/Matthew_Rounthwaite_GCFW.zip
43. SAINT available at: <http://wwdsilx.wwdsi.com/saint/>
44. Sam Spade available at: <http://samspade.org/ssw>
45. SANS Institute available at: <http://www.sans.org>
46. Security Focus/bugtraq available at: <http://www.securityfocus.com/>
47. Silvia, Tara "SANS GIAC Firewalls, Perimeter Protection and Virtual Private Networks". Available at http://www.sans.org/y2k/practical/Tara_Silvia_GCFW.zip
48. Snort. Available at: <http://www.snort.org/>

49. Squid Proxy caching software v2.4 for Linux. Available at <http://www.squid-cache.org/>
50. WHOIS database available at: <http://www.networksolutions.com>
51. [VISA's Cardholder Information Security Program \(CISP\)](#)

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