GCFW Practical

Arthur Lee
GCFW Practical
Version 4.1

Date: March 18,
2005

Table of Contents

List of Figures

1. Future state of security technology

1.1 Topic: Attacks from the parking lot

Focus: Intrusion detection and analysis on wireless networks: what makes it different? Compare and contrast wireless attacks, and attackers, to their wired counterparts.

1.2 Abstract / Summary

A major problem with wireless technology is a lack of centralized management and standards. Any access point, no matter what model or make, provides potential entry into an organization’s network. It is this rogue factor that separates wireless from its wired counterpart in this environment. Wireless networking also falls under the same issues that wired networks have, as they also rely on common layer three and above protocols (i.e., TCP/IP). However, the physical layer carries additional concerns and may be detected using tools such as wireless intrusion detection systems; with this in mind, access controls, policy, attack methodology will also differ. The best way for a proper defense is to develop a “virtual machine” concept to the defense-in-depth strategy, which includes strong policies and possible network admission control technologies.

1.3 Whitepaper

In 2003, three men were convicted of compromising a wireless access point at a local Lowe’s hardware store, giving them an opportunity to steal customer credit card numbers nationwide (Poulsen). In 2004, a man was convicted of using unsecured residential access points to send pornographic, unsolicited bulk emails (Weiss). These are just two publicized cases of wireless access abuse. Both incidents were the first of its kind.

These incidents demonstrate the ease in which an attacker may gain access to a network using a simple laptop and wireless card. In comparison to its wired counterpart, there are differences in the way wireless handles access control, deployment, as well as attack methodology. While the use of wireless needs a strict policy and possible network admission technologies, it needs to be included as just a mere component in the overall scope. That is, the corporate network needs to be considered a virtual machine, and its security architecture treated as such. Defense-in-depth is the crucial element.

<u>Intrusion Detection and Analysis</u>

To begin, let's take a look at intrusion detection and analysis on a *wired* network. This involves capturing packets from the wire directly. Most network intrusion detection systems (NIDS) will typically capture traffic between Open Systems Interconnection (OSI) layers two and seven, that is, between the datalink and application layers (CyberGuard). For simplicity's sake, this will be a packet capture and signature match.

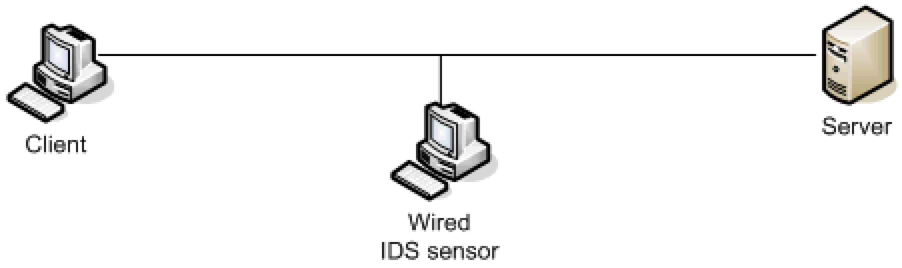

Figure 1: IDS on a wired network

Now, intrusion detection from a *wireless* perspective is an extension of that of the wired network. Computers on a wireless network will require TCP/IP capability, and hence a traditional NIDS would be able to detect traffic from this aspect. Thus, wired IDS sensors within the enterprise would continue to be useful in this regard.

However, there is the *physical* aspect of wireless networking. That is, you have communication passing through the air. As such, additional equipment is necessary to detect this type of communication (NetworkChemistry).

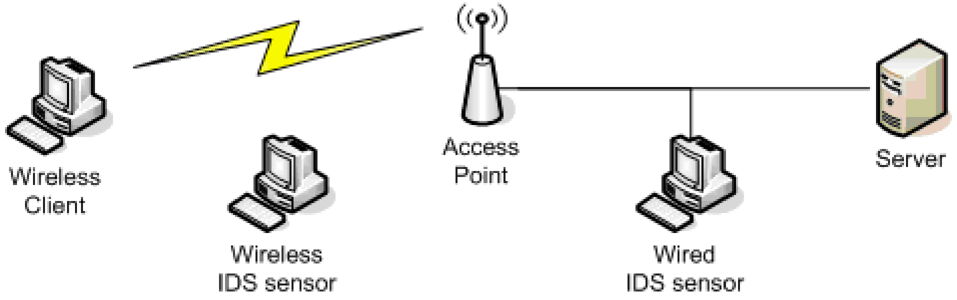

Figure 2: IDS on a wireless (and wired) network

There are two basic methods to detect wireless networks. The first is Active Probing. This is an easy method for detection, as active probing uses "probe request frames on each channel where it is able to detect wireless activity … When an AP comes within range of the client, and receives a probe request frame it will typically respond with a [detectable] probe response frame" (Wright). The second method is RF Monitoring (RFMON). This is a passive mode of detection, where it "will be able to capture all RF signals on the channels to which it is configured to listen" (Wright).

Attackers and Access Control

Access control in a traditional wired network is quite straightforward. That is, attacks must occur directly on the wire. Security architecture reflects this, as an emphasis is placed on points of entry into the network (i.e., border router/perimeter firewall, VPN concentrators, and so forth), but certainly isn't limited to this. Attaching a machine directly into a corporate network is rather difficult, as entry to a physical building may be required, and even further, data center access (as opposed to general user LAN access) may be restricted to select personnel. As such, attacks on a traditional wired network will be on OSI layers two through seven (i.e., port scans, TCP/IP response/stimulus, buffer overflows against remote services, etc.).

Access control in a wireless network is quite a different story. As mentioned, wireless communication also relies on common OSI layer three and above protocols, such as TCP/IP. However, wireless technology brings a large risk to the enterprise for a number of reasons.

Any wireless access point is a possible entry point into the enterprise network. An access point may be placed anywhere in the environment and create a bridge into the organization. No longer does someone need physical access to the building. An employee may place his own personal access point, purchased from any department store, into his cubicle and introduce unwanted guests, regardless of his or her intentions. Another employee may have an AP at home and VPN into his or her corporate network. This creates another point of entry. Finally, a poorly configured laptop with wireless may actually *create* an access point, with an ad hoc (computer to computer) configuration (Metz). This is especially problematic, as many laptops are configured to automatically associate with a known (by SSID name) access point within range (Verton).

Standards for encrypting wireless traffic between wireless peers (i.e., access point to wireless client) have also been in question. Wired Equivalency Protocol (WEP), which was popular on many earlier access points, is "rife with security weaknesses and vulnerabilities" (Cohen). Other encryption protocols are available; however, standards are only recently being implemented by the Wi-Fi Alliance, as well as the National Institution of Standards (Cohen). In 2004, a project called the "World Wide War Drive" discovered that out of 228,537 volunteer-detected access points, 140,890 had no encryption enabled, and 71,805 were using their default Service Set Identity (SSID) names; in fact, 62,859 access points were using no encryption *and* default SSIDs (World Wide War Drive).

Hence, a wireless attacker has an easier attempt at being anonymous than his wired counterpart, as he may simply drive around with a laptop, wireless card, and scanner, seeking preferably unsecured access points that are preferably broadcasting their default SSID (Lazarikos). This is exactly what the aforementioned "warspammer" did to commit his crime (Weiss).

The Path Forward

In looking to mitigate some of the risks associated with wireless technology, we need to adopt a “virtual machine” concept to the defense-in-depth strategy. Wireless technology remains only a small component of the overall security architecture. The traditional defense-in-depth strategy needs to serve the purpose of the organization as an entity.

What do we mean by virtual machine concept? A traditional virtual machine refers to an abstraction of a hypothetical machine giving the illusion that the user has access to the entire underlying machine (Tanenbaum, 2). We can take this concept and apply it to the security architecture of the organization as a whole. That is, we will apply the singular machine abstraction to a number of machines and/or networks, with its own level of access control, with its own security policies, and so forth.

To begin, the organization itself has a role, whether it is a service provider, research facility, or fortune cookie phrase reseller. Now, consider the organization’s enterprise network as a single, virtual machine. We can apply the first layer of access controls based on this concept. We can also apply security policies to this concept, which would affect all users of this virtual machine.

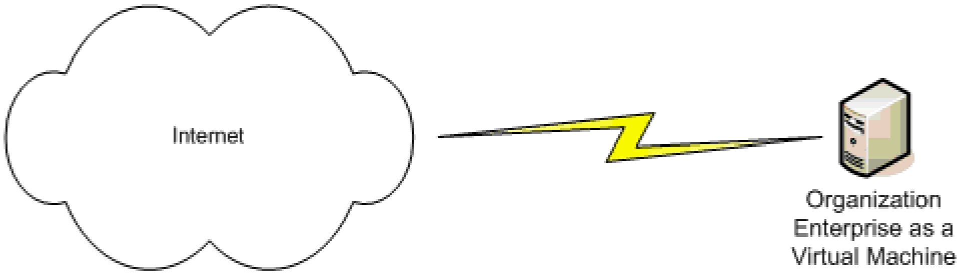

Figure 3: The enterprise as a virtual machine

Looking into the organization, each department can, in turn, be treated as a separate, virtual machine. For example, accounting and payroll may be a virtual machine, with access controls separate from that of other departments. Human resources may be another virtual machine. Each of these entities would have its own security policies which affect its own processes, transactions, usage, and so forth.

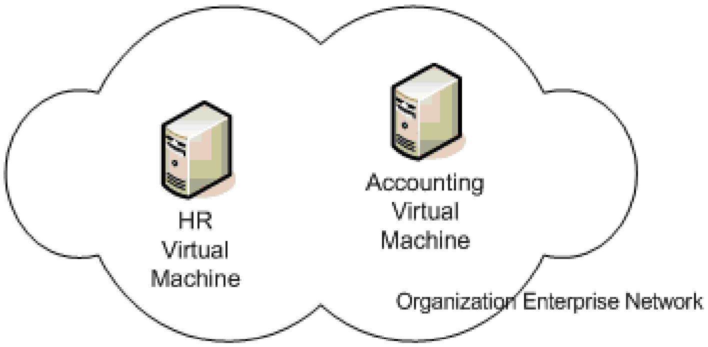

Figure 4: Functionality of departments within the enterprise as virtual machines

We can take this virtual machine concept and apply this to further levels within the organization. This may be from a server itself, to the application, to even process isolation and protected memory. Thus, the defense-in-depth strategy is given a virtual entity at each layer of security.

With wireless technology, we can segregate into a number of virtual machines. For example, we can have a virtual machine consisting of access points in the environment on a separate network, with its own level of access control and security policies. We can extend user-accessible networks within the company as a separate user virtual machine. Additionally, we can extend VPN users as another separate virtual machine.

In extending the defense-in-depth strategy to a virtual machine concept, we can mitigate risk from one virtual machine to another, as well as focus on the functionality of each. In this sense, we can apply this to *both* wired and wireless technologies using the same architectural methodology. Access control and policy would be first based on the purpose of the virtual machine (i.e., purpose of the department), and secondly based on the technology. By using this concept, security is focused to the business, and not the other way around.

Network admission technologies should also be explored, which would facilitate and extend the virtual machine concept. This is fairly new technology, developed by a handful of vendors, which would restrict (or quarantine) a machine until a minimum level of security standards are met. This may be applied to both wired and wireless machines.

A few vendors that have developed network admission products are Cisco, Checkpoint (formerly Zone Labs), and Sourcefire. Most of these products require some sort of agent installed on the machine in question. This agent will scan for a number of settings, from a minimum level of software versions, antivirus signature versions, and so forth. A central server will handle authorization, and then choose to grant access to the network, or to quarantine the machine until appropriate measures have been taken (Cisco).

In Conclusion

While there are many differences between wired and wireless networks, many problems arise from rogue access points, poor management, and weak policies. These issues extend beyond the scope of traditional, "wired" TCP/IP concepts and present challenges in the network infrastructure. However, by implementing the defense-in-depth strategy to "virtual machines" in the enterprise, a consistent and business-relevant approach may be taken to secure the enterprise.

2. Security Architecture (GIAC Enterprises)

2.1 Abstract / Summary

With increasing security threats reported in the news, GIAC Enterprises has decided to review and document its security architecture. Its goal is not only to ensure that current operations present a layered security approach, but that costs are justified and relevant to business needs. This paper defines and details those findings, with regard to business and security functions. Several issues will be presented, from network architecture, access controls and requirements, to defense-in-depth and business needs.

2.2 Introduction

GIAC Enterprises is a small, fifty-person staffed business, which sells fortune cookie phrases to customers worldwide. Its head office, which employs 38 people, is located in Chicago, Illinois. Four satellite offices, each employing three people each, are geographically located in New York, London, Hong Kong, and Seoul. Sales are conducted entirely via the Internet through the GIAC Enterprises primary website, with a separate Business Services website serving Supplier and Partner functions.

2.3 Access Requirements

Access controls and requirements are defined according to role, as this is crucial to the security architecture. The below will detail groups that interact with GIAC Enterprises, the purpose of their interaction, as well as what access controls in place per group.

2.3.1 Customers

Customers consist of individuals or organizations that purchase bulk fortunes from GIAC Enterprises. For ease of use, orders are placed on the GIAC Enterprises primary website. From here, customers can specify amount, category of fortune, shipping address, as well as billing information. These transactions occur via HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) as a web application with a SQL database (which is hosted on a separate server internally). Customers may also contact the company via phone/fax, postal mail, or email. Orders may only be placed via the website. No further access is required or given.

Source	Destination	Port(s)/Protocol	Description
Customer	GIAC Enterprises SMTP server	25/tcp (SMTP)	Means for customers to email the company

Customer	GIAC Enterprises primary web server	80/tcp (HTTP), 443/tcp (HTTPS)	Customer access to the primary web server to view catalog, place and check existing orders

Is this sufficient for business purposes? Yes, as most modern web browsers are SSL-capable and secure, and this provides an easy means to place orders into the database. Additionally, inquiries may be placed via phone, fax, postal mail, or email.

2.3.2 Suppliers

Suppliers supply the actual fortune phrases to GIAC Enterprises. The supply companies can either bulk ship finished fortunes, or submit electronic versions. Regardless of the approach, transactions are completed via GIAC Enterprises Business Services website (separate from the primary) over HTTPS with same SQL database as above. Suppliers may also contact the company via phone/fax, postal mail, or email, although transactions are strictly web-based. Suppliers do not need further access to GIAC Enterprises.

Source	**Destination**	**Port(s)/Protocol**	**Description**
Supplier	GIAC Enterprises SMTP server	25/tcp (SMTP)	Means for suppliers to email the company
Supplier	GIAC Enterprises Business Services web server	80/tcp (HTTP), 443/tcp (HTTPS)	Supplier access to the Business Services web server to submit fortunes or view/update information

Is this sufficient for business purposes? Yes, for the same reasons as customer communication. The process by which suppliers transact to GIAC Enterprises is very similar, albeit through a different web server. Additionally, any further communication may occur via phone, fax, email, or postal mail.

2.3.3 Partners

Partners of GIAC Enterprises are companies that translate and resell fortunes. They are located globally, and perform translations based on market area. As such, partners may purchase fortunes at a special rate, receive the fortunes electronically, and perform translations at their respective offices. These transactions are over the Business Services website via HTTPS. Partners may also contact the company through phone/fax, postal mail, or email, although transactions are strictly web-based. Although they are partners, further access to GIAC Enterprises is restricted.

Source	Destination	Port(s)/Protocol	Description
Partner	GIAC Enterprises SMTP server	25/tcp (SMTP)	Means for partners to email the company
Partner	GIAC Enterprises Business Services web server	80/tcp (HTTP), 443/tcp (HTTPS)	Partner access to the Business Services web server to download fortunes or view/update information

Is this sufficient for business purposes? Yes, for the same reasons above as customer communication. Again, this process is very similar, and in fact easier, as order and delivery are entirely via HTTPS. Further communication means (phone, email, etc.) are available as well.

2.3.4 Employees

GIAC Enterprises' employees on the internal user network need a minimal level of access to conduct business. All orders and transactions are checked and modified via internal web server (HTTPS-enabled), which communicates with the SQL database server. They would need access to the Internet (web access via squid proxy) to view information (such as websites for partners and competitors), as well as be able to send and receive email to other employees, customers, partners, suppliers, and the general public, via mail server. As such, employees on the internal network would need to be able to resolve addresses on the Internet, as well as internally. Additionally, employees would need to place and receive communication via phone/fax and postal mail. Finally, employees would be required to sign an acceptable use policy, stating that all company resources would be used for business purposes only.

Source	Destination	Port(s)/Protocol	Description
Internal employees	GIAC Enterprises mail server	1352/tcp (NOTES)	Means for email communication to customers, suppliers, partners, other employees, as well as the general public
Internal employees	GIAC Enterprises internal DNS server	53/udp (DNS)	Allow name resolution for internal and external addresses

Internal employees	GIAC Enterprises internal web server	80/tcp (HTTP), 443/tcp (HTTPS)	Employee access to the internal web server to check or modify order information
Internal employees	Proxy server	12333/tcp (SQUID)	Employee access to proxy server for access described in next line
Proxy server	Internet web servers	80/tcp (HTTP), 443/tcp (HTTPS)	Proxy server access to partner, supplier, and competitor websites (for business purposes only)

Is this sufficient for business purposes? Yes, as employees' network access would not only need to communicate to the GIAC Enterprises web server, but also be able to view partners and competitors. DNS (Domain Name Service) would also be required for proper name resolution. Finally, communication via phone/fax, email, and postal mail would be required.

2.3.5 Sales Force/Remote Employees

The Sales Force travel frequently, and often need access from their laptop at a remote, unspecified, location. They may only access the GIAC Enterprises internal web server via VPN (Virtual Private Network), using a Cisco VPN client. They also need to be able to phone, and send both email and postal mail.

Remote Users in the satellite offices are connected via VPN through a Cisco PIX 501 firewall deployed at each location. Their responsibilities are similar to those of employees at the main office. That is, they need to access both the GIAC Enterprises as well as external websites (suppliers, partners, competitors, etc.). They also need to be able to send and receive email via mail server, as well as place calls, faxes, and send postal mail. Finally, they need to be able to resolve addresses, both internally and externally. Just as with the central office, all employees are required to sign an acceptable use policy, stating that all company resources would be used for business purposes only.

Source	**Destination**	**Port(s)/Protocol**	**Description**
Remote employees and Sales force via VPN	GIAC Enterprises mail server	1352/tcp (NOTES)	Means for email communication to customers, suppliers, partners, other employees, as well as the general public

Remote employees and Sales force via VPN	GIAC Enterprises internal DNS server	53/udp (DNS)	Allow name resolution for internal and external addresses
Remote employees and Sales force via VPN	GIAC Enterprises internal web server	80/tcp (HTTP), 443/tcp (HTTPS)	Employee access to GIAC Enterprises internal web server to query or submit sales information
Remote employees and Sales force via VPN	Proxy server	12333/tcp (SQUID)	Employee access to proxy server for access described in next line
Proxy server	Internet web servers	80/tcp (HTTP), 443/tcp (HTTPS)	Proxy server access to partner, supplier, and competitor websites
Remote employees and Sales force via VPN	GIAC Enterprises Firewall/VPN	500/udp (ISAKMP)	Means for key negotiation for VPN establishment
Remote employees and Sales force via VPN	GIAC Enterprises Firewall/VPN	IP 50 (ESP)	Remote VPN access

Is this sufficient for business purposes? Yes, as off-site employees need a similar level of network access as those of their on-site counterparts.

2.3.6 General Public

The general public of GIAC Enterprises needs to simply be able to view the primary website and send email. They may also need to be able to send postal mail, and phone or fax the company. They do not need further access to GIAC Enterprises.

Source	**Destination**	**Port(s)/Protocol**	**Description**
General public	GIAC Enterprises SMTP server	25/tcp (SMTP)	Means for general public to email the company
General public	GIAC Enterprises primary web server	80/tcp (HTTP)	Establish web presence, and display information, as well as present means to contact company

Is this sufficient for business purposes? Yes, as the general public needs to only be able to view information via the web, and send inquiries to the company via email, phone, fax, or postal mail.

2.4 Architecture Components

The overall design of GIAC Enterprises security architecture was based on the principle of defense-in-depth. The network has been segmented into distinct, separate functional units, with access controls between each. Additionally, access controls have been placed on servers themselves, adding a further level of defense. All of these measures will be discussed in further detail.

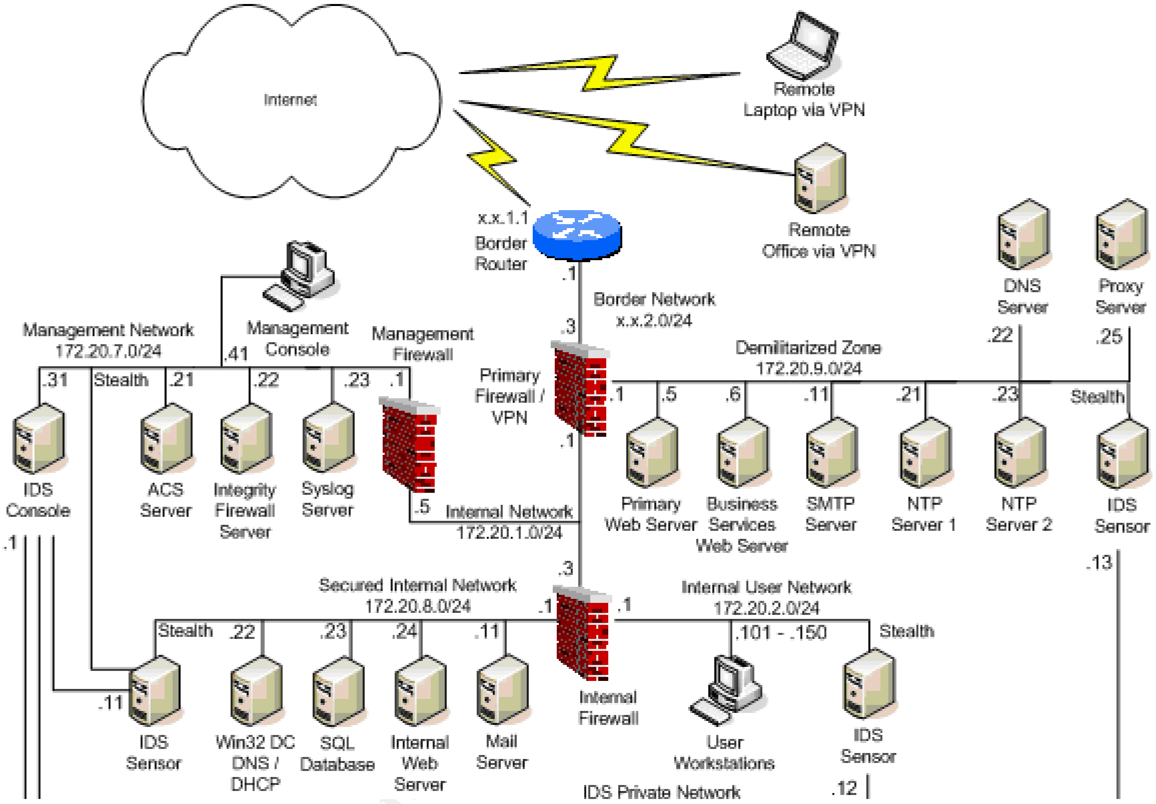

Figure 5: GIAC Enterprises Architecture

2.4.1 IP addressing scheme

The RFC 1918 compliant IP addressing schemes of: 172.20.0.0 and 172.21.0.0 were used for all internal addresses with the exception of the private IDS network, which uses the IP addressing scheme of: 192.168.0.0 (also RFC 1918 compliant). Each of these networks, in turn, has been broken into separate, CIDR 24-bit addresses. Please see Appendix 5.1 for full GIAC Enterprises address list.

Networks are listed as follows:

172.20.1.0/24	Primary network (Chicago)
172.20.9.0/24	Demilitarized zone (Chicago)
172.20.8.0/24	Secured internal network (Chicago)

172.20.7.0/24	Management network (Chicago)
172.20.2.0/24	Internal user network (Chicago)
192.168.1.0/24	IDS Private network (Chicago)
172.21.5.0/24	VPN client users
172.21.1.0/24	Remote office (New York)
172.21.2.0/24	Remote office (London)
172.21.3.0/24	Remote office (Hong Kong)
172.21.4.0/24	Remote office (Seoul)

2.4.2 Border Router

The first layer of security along the perimeter lies with the border router. This is connected to the Internet via T1 and performs initial packet filtering. These are rudimentary rules and measures to serve as a first line of defense, as well as offload some of the work from the firewall. Access rules for this device are applied per network interface and are described in Appendix 5.1. The border router is a Cisco 2621XM running IOS version 12.3. With regard to business purposes, this is more than adequate. The Cisco 2621XM is a decently priced router with filtering capabilities, and technical support is easy to obtain.

Certain basic provisions have been put in place to harden security on the router itself. This is separate from the access lists, which will be described later.

- Disable unnecessary services (i.e., tcp/udp small-servers, bootp, http, finger)
- Disable unnecessary features (i.e., cdp, service config, domain lookup)
- Disable IP Directed Broadcasts and Proxy ARP
- Enable SYN Protection with TCP Intercept

2.4.3 Firewalls (and the networks they protect)

A number of firewalls provide layered protection, from behind the border router, throughout the GIAC Enterprises network, as well as on servers themselves. The defense-in-depth strategy stretches far with this architecture, and is quite secure. Two different kinds of firewalls are used: Cisco PIX (http://www.cisco.com/) and NetFilter/IP Tables (http://www.netfilter.org/) on Linux. The separate vendors allow the avoidance of common vulnerabilities.

Primary Firewall and Demilitarized Zone

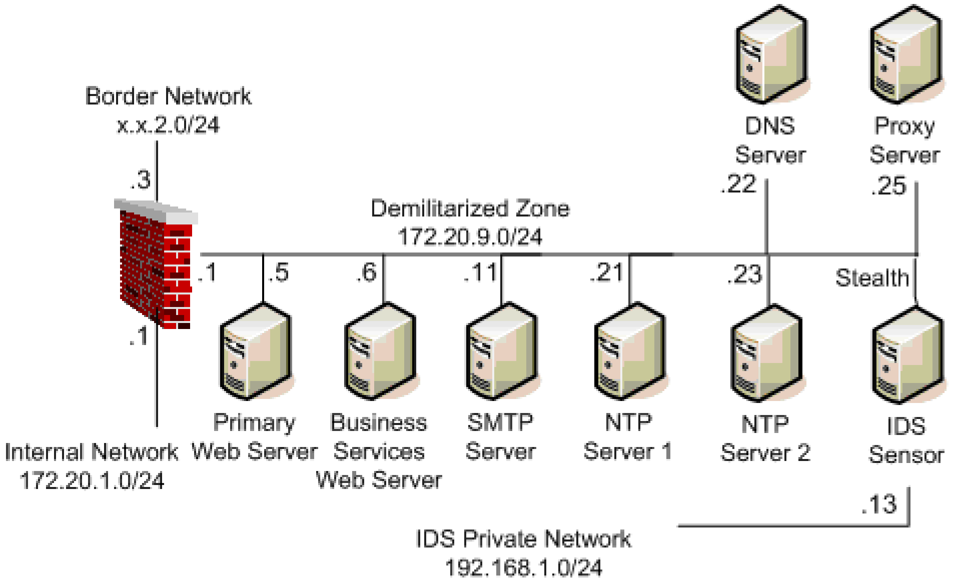

Figure 6: Primary Firewall and DMZ

Directly behind the border router resides the primary firewall. While the border router provides the first line of defense with initial filtering, the primary firewall performs the bulk of the work, performing stateful inspection on traffic coming through the firewall. The primary firewall is a Cisco PIX 515E, running PIX OS 6.3(3). It is equipped with three interfaces, restricting traffic between the external and internal networks, and demilitarized zone (DMZ). Access rules are applied per interface. See Section 3 for Access Table and Appendix 5.2 for access control list.

Primary Firewall

- Hardware: Cisco PIX 515E, three 10/100 Ethernet
- OS: PIX OS 6.3(3)

Demilitarized Zone (DMZ)

Primary web server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
  - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Apache 2.0.51-2.7
  - Running as unique, non-privileged user in a chroot jail
  - HTML files owned by non-privileged user
  - Using mod_headers module to disable HTTP server header
  - Full audit of CGI scripts
  - Disable Server Side Includes (SSI)
  - Using robots.txt file (Disallow / for all User-Agent) to disable archive.org (and other web spider) scans.

Business Services web server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet

- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Apache 2.0.51-2.7
    - Running as unique, non-privileged user in a chroot jail
    - HTML files owned by non-privileged user
    - Using mod_headers module to disable HTTP server header
    - Full audit of CGI scripts
    - Disable Server Side Includes (SSI)
    - Using robots.txt file (Disallow / for all User-Agent) to disable archive.org (and other web spider) scans.

SMTP server

- Hardware: HP DL140, 3.2GHz/1Gb RAM, one 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Sendmail 8.12.11-4.6
    - Running as unique, non-privileged user using smrsh
    - Strip outbound mail headers
    - Relay local network only

Primary NTP server

- Hardware: HP DL140, 3.2GHz/1Gb RAM, one 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Ntpd 4.2.0-7
    - Do not permit external time servers to query or modify service
    - Do not permit local clients to modify service

Secondary NTP server

- Hardware: HP DL140, 3.2GHz/1Gb RAM, one 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Ntpd 4.2.0-7
    - Do not permit external time servers to query or modify service
    - Do not permit local clients to modify service

DNS server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Bind 9.2.3-13
    - Running as non-privileged user in chroot jail
    - No recursive queries
    - Version information changed in configuration file
    - No access to root DNS servers
    - Restricted zone transfers, with logging
    - Provides only external service addresses (no internal)

Proxy server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
  - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Squid 2.5-STABLE6
  - Running as unique, non-privileged user in a chroot jail
  - Only valid, internal IP addresses are allowed.
  - Running on non-standard port: 12333/tcp.

IDS sensor

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, two 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
  - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Snort 2.3 and SnortCenter Agent
  - Stealth interface listening in DMZ
  - Management interface on private IDS network to IDS console

Internal Firewall and Networks

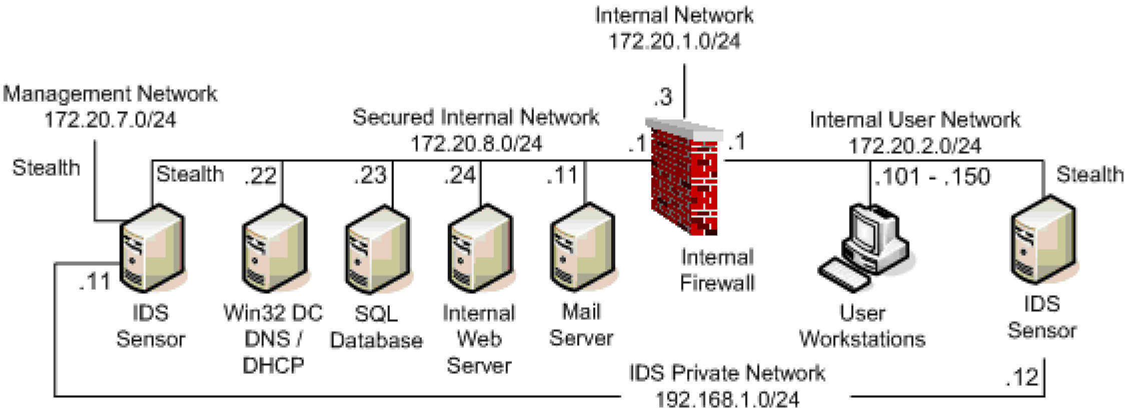

Figure 7: Internal Firewall and Networks

An internal firewall secures internal servers, including the SQL database, which stores mission-critical data (customer, supplier, and partner information, as well as fortunes). This provides an additional level of protection, should the attacks come from the inside (i.e., compromise of the primary firewall, discontented employees, etc.). The internal firewall is a NetFilter/IP Tables Linux machine (HP DL320/G2), performing stateful inspection and running RedHat Enterprise 3. Update 4 has been applied, and critical fixes are updated regularly. Additionally, the operating system has been hardened, running only necessary components, utilizing TCP Wrappers, as well as BastilleLinux (http://www.bastille-linux.org/). The internal firewall is equipped with three network interfaces, restricting traffic between the internal network, the internal user network, and the secured internal network. Access rules are applied per interface.

Internal Firewall

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, three 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
  - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux

Secured Internal Network

SQL Database server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
  - Secured with: NetFilter/IP Tables, TCP Wrappers
- Running: MySQL Database Server 4.1.7
  - Running as unique, non-privileged user in chroot jail
  - Authentication required (no password-less accounts)
  - Disabled anonymous access
  - Example tables and databases removed

Internal web server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
  - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Apache 2.0.51-2.7
  - Running as unique, non-privileged user in a chroot jail
  - HTML files owned by non-privileged user
  - Using mod_headers module to disable HTTP server header
  - Full audit of CGI scripts
  - Disable Server Side Includes (SSI)

Win32 Domain Controller

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: Windows Server 2003
  - Secured with: Minimal service and policy configuration
- Running: Active Directory Services (including DNS and DHCP)
  - DNS:
    - Queries allowed by internal networks only
    - Provides internal addresses and external via forwarding
  - DHCP:
    - Enabled for Internal User Network only

Mail server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: Windows Server 2003
  - Secured with: Minimal service and policy configuration
- Running: Lotus Notes 6.5

IDS sensor

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, three 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
  - Secured with: NetFilter/IP Tables, TCP Wrappers
- Running: Snort 2.3 (two instances, each on a separate NIC) and SnortCenter Agent

  - Stealth interface listening in Secured Internal Network
  - Stealth interface listening in Management Network
  - Management interface on private IDS network to IDS console

Internal User Network

IDS sensor

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, two 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
  - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: Snort 2.3 and SnortCenter Agent
  - Stealth interface listening in Internal User Network
  - Management interface on private IDS network to IDS console

User workstations

- Hardware: Various HP and IBM Intel desktops
- OS: Microsoft Windows XP SP2 (firewall disabled)
  - Secured with: Symantec Antivirus software and Check Point Integrity Agent (personal/distributed firewall)

Management Firewall and Network

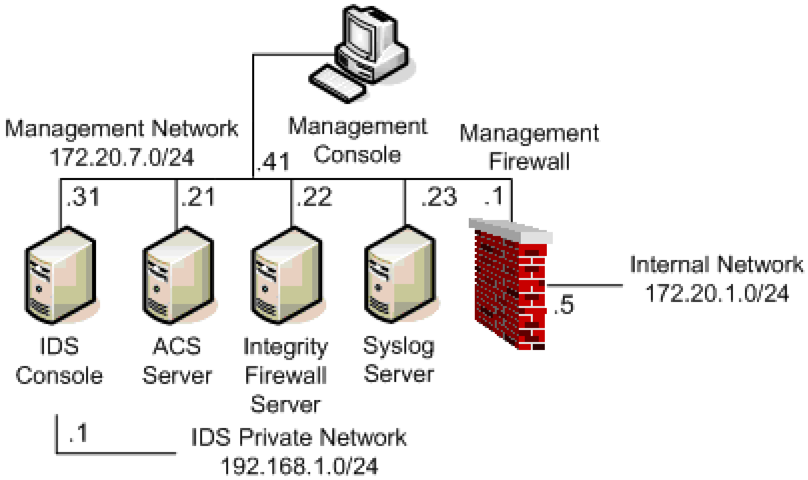

Figure 8: Management Firewall and Network

The management network is also protected by a Linux NetFilter/IP Tables machine in a similar setup, albeit with two interfaces only. This separates the management network from the internal network. The firewall's tasks involve passing minimal types of traffic to and from the management network (syslog, NTP, RADIUS, TACACS+, SMTP, and Check Point Integrity). No further access is defined.

Management Firewall

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, two 10/100 Ethernet

- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux

Management Network

Syslog server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, one 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: syslogd 1.4.1 and Psionic LogSentry 1.1 for alerting
    - Specify individual logs for external syslogs for analysis
    - Additionally, have a consolidated "master" syslog for LogSentry alerting

ACS server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: Windows Server 2003
    - Secured with: Minimal service and policy configuration
- Running: Cisco ACS 3.3.2
    - RADIUS authentication for laptop VPN users
    - TACACS+ authentication for remote office VPN

Personal/Distributed Firewall Server

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, 10/100 Ethernet
- OS: Windows Server 2003
    - Secured with: Minimal service and policy configuration
- Running: Check Point Integrity 5.0

IDS console

- Hardware: HP DL360/G2, 3.6GHz/2Gb RAM, two 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux
- Running: SnortCenter 1.0-RC1
    - With SSL support
    - With ACID plug-in
- Running: Apache 2.0.51-2.7
    - Running as unique, non-privileged user in a chroot jail
    - HTML files owned by non-privileged user
    - Using mod_headers module to disable HTTP server header
- Running: MySQL Database Server 4.1.7
    - Running as unique, non-privileged user in chroot jail
    - Authentication required (no password-less accounts)
    - Disabled anonymous access
    - Sample tables and databases removed
    - Local access only

Management console

- Hardware: HP dc 5000, 2.6GHz/1Gb RAM, one 10/100 Ethernet
- OS: RedHat Linux Enterprise 3 Update 4
    - Secured with: NetFilter/IP Tables, TCP Wrappers, BastilleLinux

Both the Cisco PIX 515E and NetFilter/IP Tables are a good business choice for a number of reasons. The PIX 515E is a decently priced firewall, capable of three interfaces, decent technical support, as well as having a similar command set to Cisco IOS. NetFilter/IP Tables is included with the license cost of RedHat Enterprise Linux, and is a versatile firewall with powerful capabilities. Additionally, it has the wide-spread support of the open-source community, and troubleshooting can range from placing a call with RedHat to doing a simple Google search. Finally, diversifying platforms for firewall tasks also reduces the risk of a single vulnerability for one platform; that is, a single PIX vulnerability won't compromise the entire network.

2.4.4 VPN(s)

Virtual Private Networking (VPN) is handled through the Primary Firewall (Cisco PIX 515E), terminating IPSec VPN connections for both laptop users and remote offices. Laptop users use the Cisco VPN Client, while remote offices each use a Cisco PIX 501. Authentication is handled via Cisco ACS server (which resides in the Management Network), RADIUS for laptop users and TACACS+ for remote offices. Encryption is handled via 256-bit Advanced Encryption Standard (AES). This solution works for GIAC Enterprises, as it leverages features in existing hardware for a fairly light amount of traffic (mainly mail and web).

Remote offices

- Hardware: Cisco PIX 501, internal and external 10/100 interfaces
- OS: PIX OS 6.3(3)

Laptop users

- Hardware: IBM Intel ThinkPad T41
- OS: Microsoft Windows XP SP2 (firewall disabled)
  - Secured with: Symantec Antivirus software and Check Point Integrity Agent (personal/distributed firewall)
  - Cisco VPN Client 4.6

2.4.5 Network-Based IDS Sensors

The snort (http://www.snort.org/) network intrusion detection system is deployed throughout the GIAC Enterprises network. Sensors are placed in the DMZ, the secured internal network, the management network, as well as the internal user network. It is important to understand and establish a baseline of normal traffic for each of these networks in the event of an intrusion, incorrect network configuration, or network-based viruses.

Snort 2.3 is used, with SnortCenter 1.0-RC1 (http://users.pandora.be/larc/) with ACID (http://www.cert.org/kb/acid/) plug-in for sensor management. Both sensors and IDS console run on RedHat Enterprise 3 with Update 4, security updates, and

BastilleLinux applied. The IDS console is placed in the management network, with SSL encryption between itself and the snort sensors. All sensors and console run on HP DL320/G2 machines.

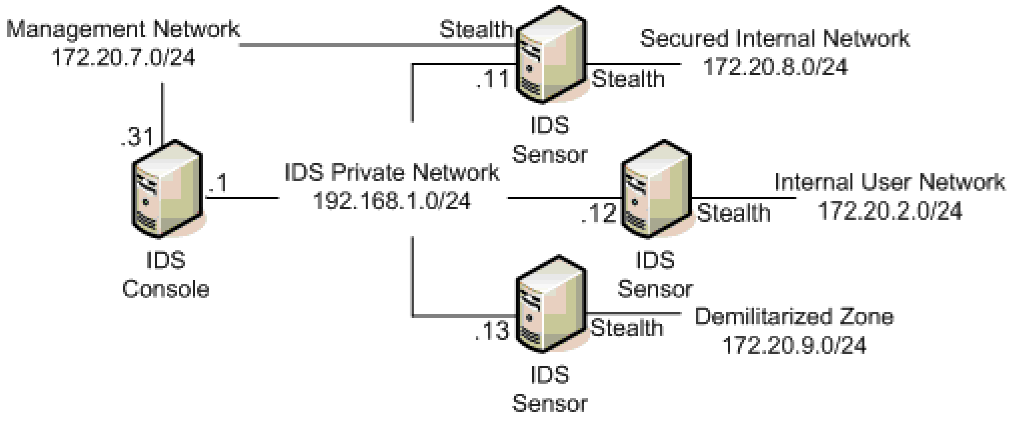

Figure 9: Network IDS Architecture

For the most part, one instance of snort per interface is running on each machine, with the SnortCenter Agent. An exception to this is the sensor that is monitoring both the management and secured internal networks (with separate snort instances on separate interfaces). This makes sense, as the network traffic is substantially less than that of the DMZ or internal user network.

All sensor interfaces are running in "stealth mode," without a defined IP address. Each of these interfaces is connected to a SPAN port in their respective network segments. Finally, each sensor has an additional interface attached to a private network to communicate with the management console. The diagram above displays that architecture.

This is a good choice for the business, as Snort is one of the most popular IDS systems today, and has world-wide support from the open source community. Monetary costs for IDS lie in server hardware and RedHat licensing, which is manageable for GIAC Enterprises.

2.4.6 Additional Components

Antivirus: Each workstation and laptop is installed with Symantec Antivirus (http://www.symantec.com/), which protects it against viruses, worms, trojans and the like. Since GIAC Enterprises is a small company, Office Packs have been purchased rather than the full-blown Enterprise Suite. This is sufficient for the business in regard to functionality and cost.

Backups: Data availability is very important to GIAC Enterprises, as the entire business relies on stored information (fortunes). As such, backups are performed daily on critical servers, namely the Syslog, SQL database, Windows 2003 Domain

Controller, Mail, and web servers. The Linux servers use a straight *tar* to tape, while the Windows machines use Veritas BackupExec (http://www.veritas.com/). Firewall configurations are backed up after every configuration change. Tapes are also stored offsite. This is sufficient for business purposes, as backup and recovery time is relatively quick. The cost for this solution is very manageable and its return on investment is immediate.

Host Firewalls (and TCP Wrappers): Each Linux server within GIAC Enterprises (i.e., Web, SQL database, DNS, NTP) utilizes host firewalls (NetFilter/IP Tables, same as the internal firewalls). Servers are also hardened, running only necessary components, and implementing TCP Wrappers. Each machine restricts which IP addresses have access to valid services, and deny everything else. This provides a further layer of defense to complement the server's respective network firewall.

Personal/Distributed Firewalls: Each workstation and laptop in the enterprise is secured with a Check Point (formerly Zone Labs) Integrity Agent. This is configured to work in two ways: 1) to serve as a personal firewall against malicious attackers, worms, and viruses, and 2) serve as a policy control agent (that is, outbound traffic may be restricted by application, as well as TCP/IP ports). This not only provides restriction of file sharing and instant messaging (IM) programs, but also unknown programs as well (i.e., viruses, worms, and trojans). Additionally, Integrity can check for version information for these programs, as well as virus definition files. If the policy should fail, the workstation or laptop is denied access to the network until the violations are corrected. Only known, corporate-approved applications are allowed access. Management is via the Check Point Integrity server which resides in the Management Network. Cost is relatively inexpensive, and is per agent. Firewall rules are intact, even if not connected to the GIAC Enterprises network. This fits the organization nicely, and protects it from rogue malware, as well as illegal file sharing.

System integrity: System integrity for Linux servers is checked via integrit (http://integrit.sourceforge.net/), which handles checking of file attributes, such as checksum, timestamp, inode, etc. The system is scanned initially to create a baseline. Further scans are compared to this baseline to detect changes to the system. Additionally, chkrootkit (http://www.chkrootkit.org/) is run periodically to detect unauthorized files and malware on the system.

2.4.7 Summary: Implementing Defense-in-depth

To summarize, we can see a distinct layered implementation in looking at the security architecture for GIAC Enterprises. Not only are company assets protected by the Border Router and primary firewall, but also through multiple in-line firewalls, network intrusion detection systems, as well as local firewalls and system hardening. This security serves and complements the business, and isn't designed to hinder or confound it.

Each layer is distinct and purposeful:

- Border Router performing initial ingress/egress packet filtering
- Primary Firewall
- Internal Firewall
- Management Network Firewall
- Separate vendors for firewalls to avoid common vulnerabilities
- Protected network segment architecture
- Virtual Private Network (VPN)
- Network Intrusion Detection System (IDS)
- Local firewalls
- System hardening
- System integrity detection
- Distributed personal firewall on user workstations
- Antivirus
- Controlled and monitored outbound web access via proxy server
- Data availability via backups

3. Router and Primary Firewall Policies

3.1 General Security Stance

With communications needs defined earlier for customers, suppliers, partners, and such, we can establish a security policy for the perimeter; that is, the Border Router and Primary Firewall.

Coming into GIAC Enterprises, the Border Router will handle initial packet filtering and mitigate reconnaissance, denial of service, and filter critical service ports, as well as illegitimate traffic. The Primary Firewall, in turn, will allow identified services to be accessed (for example, the web server), and filter everything else. This utilizes the router to handle static packet filtering and offload some of the processing on the firewall.

Coming out of GIAC Enterprises, the converse occurs. That is, the Primary Firewall will allow identified services to reach their destination, and filter everything else. The Border Router will take this remaining traffic, and also mitigate reconnaissance, denial of service, and so forth.

The concept of defense-in-depth works here at the perimeter, as each device complements each other nicely.

3.2 Border Router Access Control Lists

Ingress Filtering: The first section details the security policy as it applies to the external interface of the Border Router. These are rules that deal with traffic coming into the GIAC Enterprises network from the outside. This is critical, as the Border Router serves as the first line of defense against hacks and scans. This will handle initial filtering and restrict particular types of traffic. The remainder will go through and be handled by the perimeter firewall (and in turn, will be handled by internal firewalls, system access controls, and so forth).

The order is important, as more frequently used traffic will be towards the top to optimize performance; that is, it will have to go through less lines of the access list, saving processing time on the router.

Traffic rules for internal addresses on external interface:

These rules will tackle loopback, broadcast, multicast, RFC 1918 reserved, as well as APIPA (Automatic Private IP Addressing) addresses. This will protect against denial of service (DOS) attacks, as incoming traffic to the router should be from valid (and external) addresses.

Source	**Destination**	**Port (Protocol)**	**Action**	**Interface**	**Description**
127.0.0.0/8	Any	IP	Deny	External	Deny loopback traffic
224.0.0.0/8	Any	IP	Deny	External	Deny multicast traffic
10.0.0.0/8	Any	IP	Deny	External	Deny RFC 1918 reserved traffic
172.16.0.0/12	Any	IP	Deny	External	Deny RFC 1918 reserved traffic
192.0.2.0/24	Any	IP	Deny	External	Deny TEST-NET traffic
192.168.0.0/16	Any	IP	Deny	External	Deny RFC 1918 reserved traffic
169.254.0.0/16	Any	IP	Deny	External	Deny APIPA / RFC 3330 reserved traffic

Traffic rules for unassigned addresses:

These rules perform a similar task to the previous list. These IP addresses have not been assigned and are reserved by the Internet Assigned Numbers Authority (IANA); as such, traffic with a source address from this list would not be valid.

Source	**Destination**	**Port (Protocol)**	**Action**	**Interface**	**Description**
0.0.0.0/8	Any	IP	Deny	External	IANA Reserved
1.0.0.0/8	Any	IP	Deny	External	IANA Reserved
2.0.0.0/8	Any	IP	Deny	External	IANA Reserved
5.0.0.0/8	Any	IP	Deny	External	IANA Reserved
7.0.0.0/8	Any	IP	Deny	External	IANA Reserved
23.0.0.0/8	Any	IP	Deny	External	IANA Reserved
27.0.0.0/8	Any	IP	Deny	External	IANA Reserved
31.0.0.0/8	Any	IP	Deny	External	IANA Reserved
36.0.0.0/8	Any	IP	Deny	External	IANA Reserved
37.0.0.0/8	Any	IP	Deny	External	IANA Reserved

39.0.0.0/8	Any	IP	Deny	External	IANA Reserved
41.0.0.0/8	Any	IP	Deny	External	IANA Reserved
42.0.0.0/8	Any	IP	Deny	External	IANA Reserved
60.0.0.0/8	Any	IP	Deny	External	IANA Reserved
73.0.0.0/8	Any	IP	Deny	External	IANA Reserved
74.0.0.0/8	Any	IP	Deny	External	IANA Reserved
75.0.0.0/8	Any	IP	Deny	External	IANA Reserved
76.0.0.0/8	Any	IP	Deny	External	IANA Reserved
77.0.0.0/8	Any	IP	Deny	External	IANA Reserved
78.0.0.0/8	Any	IP	Deny	External	IANA Reserved
79.0.0.0/8	Any	IP	Deny	External	IANA Reserved
89.0.0.0/8	Any	IP	Deny	External	IANA Reserved
90.0.0.0/8	Any	IP	Deny	External	IANA Reserved
91.0.0.0/8	Any	IP	Deny	External	IANA Reserved
92.0.0.0/8	Any	IP	Deny	External	IANA Reserved
93.0.0.0/8	Any	IP	Deny	External	IANA Reserved
94.0.0.0/8	Any	IP	Deny	External	IANA Reserved
95.0.0.0/8	Any	IP	Deny	External	IANA Reserved
96.0.0.0/8	Any	IP	Deny	External	IANA Reserved
97.0.0.0/8	Any	IP	Deny	External	IANA Reserved
98.0.0.0/8	Any	IP	Deny	External	IANA Reserved
99.0.0.0/8	Any	IP	Deny	External	IANA Reserved
100.0.0.0/8	Any	IP	Deny	External	IANA Reserved
101.0.0.0/8	Any	IP	Deny	External	IANA Reserved
102.0.0.0/8	Any	IP	Deny	External	IANA Reserved
103.0.0.0/8	Any	IP	Deny	External	IANA Reserved
104.0.0.0/8	Any	IP	Deny	External	IANA Reserved
105.0.0.0/8	Any	IP	Deny	External	IANA Reserved
106.0.0.0/8	Any	IP	Deny	External	IANA Reserved
107.0.0.0/8	Any	IP	Deny	External	IANA Reserved
108.0.0.0/8	Any	IP	Deny	External	IANA Reserved
109.0.0.0/8	Any	IP	Deny	External	IANA Reserved
110.0.0.0/8	Any	IP	Deny	External	IANA Reserved
111.0.0.0/8	Any	IP	Deny	External	IANA Reserved
112.0.0.0/8	Any	IP	Deny	External	IANA Reserved
113.0.0.0/8	Any	IP	Deny	External	IANA Reserved
114.0.0.0/8	Any	IP	Deny	External	IANA Reserved
115.0.0.0/8	Any	IP	Deny	External	IANA Reserved
116.0.0.0/8	Any	IP	Deny	External	IANA Reserved
117.0.0.0/8	Any	IP	Deny	External	IANA Reserved
118.0.0.0/8	Any	IP	Deny	External	IANA Reserved
119.0.0.0/8	Any	IP	Deny	External	IANA Reserved
120.0.0.0/8	Any	IP	Deny	External	IANA Reserved
121.0.0.0/8	Any	IP	Deny	External	IANA Reserved
122.0.0.0/8	Any	IP	Deny	External	IANA Reserved
123.0.0.0/8	Any	IP	Deny	External	IANA Reserved
173.0.0.0/8	Any	IP	Deny	External	IANA Reserved
174.0.0.0/8	Any	IP	Deny	External	IANA Reserved
175.0.0.0/8	Any	IP	Deny	External	IANA Reserved
176.0.0.0/8	Any	IP	Deny	External	IANA Reserved
177.0.0.0/8	Any	IP	Deny	External	IANA Reserved

178.0.0.0/8	Any	IP	Deny	External	IANA Reserved
179.0.0.0/8	Any	IP	Deny	External	IANA Reserved
180.0.0.0/8	Any	IP	Deny	External	IANA Reserved
181.0.0.0/8	Any	IP	Deny	External	IANA Reserved
182.0.0.0/8	Any	IP	Deny	External	IANA Reserved
183.0.0.0/8	Any	IP	Deny	External	IANA Reserved
184.0.0.0/8	Any	IP	Deny	External	IANA Reserved
185.0.0.0/8	Any	IP	Deny	External	IANA Reserved
186.0.0.0/8	Any	IP	Deny	External	IANA Reserved
187.0.0.0/8	Any	IP	Deny	External	IANA Reserved
189.0.0.0/8	Any	IP	Deny	External	IANA Reserved
190.0.0.0/8	Any	IP	Deny	External	IANA Reserved
197.0.0.0/8	Any	IP	Deny	External	IANA Reserved
223.0.0.0/8	Any	IP	Deny	External	IANA Reserved
225.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
226.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
227.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
228.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
229.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
230.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
231.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
232.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
233.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
234.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
235.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
236.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
237.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
238.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
239.0.0.0/8	Any	IP	Deny	External	Deny IANA multicast
240.0.0.0/8	Any	IP	Deny	External	IANA Reserved
241.0.0.0/8	Any	IP	Deny	External	IANA Reserved
242.0.0.0/8	Any	IP	Deny	External	IANA Reserved
243.0.0.0/8	Any	IP	Deny	External	IANA Reserved
244.0.0.0/8	Any	IP	Deny	External	IANA Reserved
245.0.0.0/8	Any	IP	Deny	External	IANA Reserved
246.0.0.0/8	Any	IP	Deny	External	IANA Reserved
247.0.0.0/8	Any	IP	Deny	External	IANA Reserved
248.0.0.0/8	Any	IP	Deny	External	IANA Reserved
249.0.0.0/8	Any	IP	Deny	External	IANA Reserved
250.0.0.0/8	Any	IP	Deny	External	IANA Reserved
251.0.0.0/8	Any	IP	Deny	External	IANA Reserved
252.0.0.0/8	Any	IP	Deny	External	IANA Reserved
253.0.0.0/8	Any	IP	Deny	External	IANA Reserved
254.0.0.0/8	Any	IP	Deny	External	IANA Reserved
255.0.0.0/8	Any	IP	Deny	External	IANA Reserved

Block critical services:

Certain services, such as HTTP access to the primary web server are needed by the public. However, there are many services that aren't needed and should be filtered. The below identifies and mitigates critical common services.

Source	Destination	Port (Protocol)	Action	Interface	Description
Any	Any	135 to 139 / tcp	Deny	External	Deny Microsoft NetBIOS traffic
Any	Any	135 to 139 / udp	Deny	External	Deny Microsoft NetBIOS traffic
Any	Any	445/tcp	Deny	External	Deny Microsoft SMB traffic
Any	Any	161 to 162 / udp	Deny	External	Deny SNMP traffic
Any	Any	69/tcp	Deny	External	Deny TFTP traffic
Any	Any	514/udp	Deny	External	Deny Syslog traffic
Any	Any	6000 to 6255 / tcp	Deny	External	Deny X Windows traffic

ICMP rules:

Using tools that utilize ICMP (i.e., ping, hping2, etc.) are common and easy ways to gain information about a network. These simple rules can reduce this risk.

Source	Destination	Port (Protocol)	Action	Interface	Description
Any	Any	ICMP echo request	Deny	External	Deny ICMP echo requests, to restrict reconnaissance scans
Any	Any	ICMP redirect	Deny	External	Deny ICMP redirect traffic
Any	Any	ICMP mask-request	Deny	External	Deny ICMP mask requests, to restrict topological reconnaissance

Apply rules:

Now we permit everything else inbound on the external interface of the Border Router, as long as it is to the GIAC Enterprises network (everything else will be denied). The traffic will then be handled by the Primary Firewall (and in turn, other access control methods).

Source	Destination	Port (Protocol)	Action	Interface	Description
Any	GIAC Enterprises Network x.x.2.0/24	IP	Allow	External	Allow legitimate traffic that hasn't been filtered thus far to the GIAC Enterprises network
Any	Any	IP	Deny	External	Deny everything else

Egress Filtering: This next section details the security policy as it applies to the internal interface. These are rules that deal with traffic coming out of the GIAC Enterprises network from the inside. While egress rules may be thought of as less important than ingress, they are still very critical as the Border Router also serves as the last line of defense for the company. As with the above, order is important, as more frequently used traffic will be towards the top to optimize performance.

Block critical services:

It is good practice to restrict services on the host itself, or even through the firewalls the traffic may pass. However, it is better to have a defense-in-depth strategy and apply this further. The below are the same critical services that are filtered inbound. We need to filter them outbound to prevent information and access leakage.

Source	Destination	Port (Protocol)	Action	Interface	Description
Any	Any	135 to 139 / tcp	Deny	Internal	Deny Microsoft NetBIOS traffic to the Internet
Any	Any	135 to 139 / udp	Deny	Internal	Deny Microsoft NetBIOS traffic to the Internet
Any	Any	445/tcp	Deny	Internal	Deny Microsoft SMB traffic to the Internet
Any	Any	161 to 162 / udp	Deny	Internal	Deny SNMP traffic to the Internet
Any	Any	69/tcp	Deny	Internal	Deny TFTP traffic to the Internet
Any	Any	514/udp	Deny	Internal	Deny Syslog traffic to the Internet

ICMP rules:

As with ICMP ingress rules, using tools that utilize ICMP (i.e., ping, hping2, etc.) are common and easy ways to gain information about a network. These simple rules can also reduce this risk.

Source	Destination	Port (Protocol)	Action	Interface	Description
Any	Any	ICMP echo reply	Deny	External	Deny ICMP echo replies to the Internet
Any	Any	ICMP unreachable	Deny	External	Deny ICMP unreachables to the Internet

Apply rules:

Now we permit everything else outbound on the internal interface of the Border Router. Only traffic that has originated from GIAC Enterprises will be allowed outbound. The remainder will be denied. This will mitigate denial of service attacks that may originate from the company.

Source	Destination	Port (Protocol)	Action	Interface	Description
GIAC Enterprises Network x.x.2.0/24	Any	IP	Allow	Internal	Allow legitimate traffic that hasn’t been filtered thus far to the Internet
Any	Any	IP	Deny	Internal	Deny everything else

3.3 Primary Firewall Security Policy

External Interface: The first section details the security policy as it applies to the external interface. These are rules that deal with traffic coming into the GIAC Enterprises network from the outside (that is, through the Border Router). The order is important. More frequently used traffic will be towards the top to optimize performance (usage is determined by a "show access-list" command on the PIX); it will have to go through less lines of the access list, saving processing time on the firewall. As such, incoming email and DNS queries will be first, followed by web traffic. VPN and Border Router traffic will follow last. The last line of this configuration is important and cannot be moved. Finally, audits of access-list usage will be reviewed on a regular basis – rule order may be modified as such.

Note: Publicly accessible servers have public IP addresses, which have a static translation to internal addresses. See Appendix 5.2 for translations.

Source	**Destination**	**Port (Protocol)**	**Action**	**Interface**	**Description**
Any	SMTP server x.x.2.58 (172.20.9.11)	25/tcp (SMTP)	Allow	External	Allow outside hosts to send email to GIAC Enterprises with the external IP of x.x.2.58
Any	DNS server x.x.2.60 (172.20.9.22)	53/udp (DNS)	Allow	External	Allow DNS server to answer queries for external service names and addresses with the external IP of x.x.2.60
Any	Primary web server x.x.2.50 (172.20.9.5)	80/tcp (HTTP)	Allow	External	Allow outside hosts to view primary website via HTTP with the external IP of x.x.2.50
Any	Primary web server x.x.2.50 (172.20.9.5)	443/tcp (HTTPS)	Allow	External	Allow customers to view primary website via HTTPS with the external IP of x.x.2.50
Suppliers and partners	Business Services web server x.x.2.56 (172.20.9.6)	80/tcp (HTTP)	Allow	External	Allow suppliers and partners to access Business Services website via HTTP with the external IP of x.x.2.56
Suppliers and partners	Business Services web server x.x.2.56 (172.20.9.6)	443/tcp (HTTPS)	Allow	External	Allow suppliers and partners to access Business Services website via HTTPS with the external IP of x.x.2.56
Remote offices and VPN clients	Primary firewall	500/udp (ISAKMP)	Allow	External	Means for key negotiation for VPN establishment
Remote offices and VPN clients	Primary firewall	IP 50 (ESP)	Allow	External	Remote VPN access
Border router x.x.x.1	Primary NTP server 172.20.9.21	123/udp (NTP)	Allow	External	Allow Border router to synchronize time to primary NTP server

Border router x.x.1.1	Secondary NTP server 172.20.9.23	123/udp (NTP)	Allow	External	Allow Border router to synchronize time NTP to secondary NTP server
Border router x.x.1.1	Syslog server 172.20.7.23	514/udp (SYSLOG)	Allow	External	Allow Border router to send logs to syslog server
Any	Any	All	Deny	External	Deny all other access into the GIAC Enterprises network.

Demilitarized Zone (DMZ) Interface: This next section details the security policy as it applies to the DMZ interface. These are rules that deal with traffic from the GIAC Enterprises DMZ network. As with the above, the order is important, as more frequently used traffic will be towards the top to optimize performance. As such, email and DNS queries will be first, followed by web traffic. Syslog traffic will follow last. Again, the last line must remain as the last.

Source	**Destination**	**Port (Protocol)**	**Action**	**Interface**	**Description**
SMTP server 172.20.9.11	Internal mail server 172.20.8.11	1352/tcp (LOTUSNOTES)	Allow	DMZ	Allow email from the DMZ SMTP server to the internal mail server
SMTP server 172.20.9.11	Any	25/tcp (SMTP)	Allow	DMZ	Allow email to be sent from the SMTP server to the Internet
DNS server 172.20.9.22	Any	53/udp (DNS)	Allow	DMZ	Allow DNS server to query Internet names/addresses
Primary NTP server 172.20.9.21	Public NTP Stratum 2 server	123/udp (NTP)	Allow	DMZ	Allow primary NTP server to synchronize to external Stratum 2 server
Secondary NTP server 172.20.9.23	Public NTP Stratum 2 server	123/udp (NTP)	Allow	DMZ	Allow secondary NTP server to synchronize to external Stratum 2 server
Primary web server 172.20.9.5	SQL database server 172.20.8.23	3306/tcp (MYSQL)	Allow	DMZ	Allow web server to communicate with SQL database server
Business Services web server 172.20.9.6	SQL database server 172.20.8.23	3306/tcp (MYSQL)	Allow	DMZ	Allow web server to communicate with SQL database server
DMZ servers 172.20.9.0/24	Syslog server 172.20.7.23	514/udp (SYSLOG)	Allow	DMZ	Allow DMZ servers to send logs to syslog server
Proxy server 172.20.9.25	Any	80/tcp (HTTP)	Allow	DMZ	Allow proxy server to access web content via HTTP
Proxy server 172.20.9.25	Any	443/tcp (HTTPS)	Allow	DMZ	Allow proxy server to access web content via HTTPS
Any	Any	All	Deny	DMZ	Deny all other access from GIAC Enterprises DMZ.

Internal Interface: This last section details the security policy as it applies to the internal interface. These are rules that deal with traffic internal to the company to either the DMZ or Internet. As with both of the above policies, the order is important, as more frequently used traffic will be towards the top to optimize performance. As such, incoming email and DNS queries will be first, followed by web traffic. VPN and Border Router traffic will follow last. Similarly, the last line must remain as the last.

Source	Destination	Port (Protocol)	Action	Interface	Description
Internal mail server 172.20.8.11	SMTP server 172.20.9.11	25/tcp (SMTP)	Allow	Internal	Allow outbound email from the mail to the SMTP server
Servers and firewalls behind primary firewall	Primary NTP server 172.20.9.21	123/udp (NTP)	Allow	Internal	Allow servers and firewalls to synchronize time with primary NTP server
Servers and firewalls behind primary firewall	Secondary NTP server 172.20.9.23	123/udp (NTP)	Allow	Internal	Allow servers and firewalls to synchronize time with secondary NTP server
Internal DNS (Win2003 DC) server 172.20.8.22	DNS server 172.20.9.22	53/udp (DNS)	Allow	Internal	Allow internal DNS server to query external DNS server for Internet names/addresses
User workstations 172.20.2.101 - 150	Primary web server 172.20.9.5	80/tcp (HTTP)	Allow	Internal	Allow internal users access to the primary web server via HTTP
User workstations 172.20.2.101 - 150	Primary web server 172.20.9.5	443/tcp (HTTPS)	Allow	Internal	Allow internal users access to the primary web server via HTTPS
User workstations 172.20.2.101 - 150	Business Services web server 172.20.9.6	80/tcp (HTTP)	Allow	Internal	Allow internal users access to the Business Services web server via HTTP
User workstations 172.20.2.101 - 150	Business Services web server 172.20.9.6	443/tcp (HTTPS)	Allow	Internal	Allow internal users access to the Business Services web server via HTTPS
User workstations 172.20.2.101 - 150	Proxy server 172.20.9.25	12333/tcp (SQUID)	Allow	Internal	Allow workstations to connect to the proxy server to browse the web
Any	Any	All	Deny	Internal	Deny all other access from GIAC Enterprises DMZ.

4. References

Analysis Console for Intrusion Databases. Analysis Console for Intrusion Databases.

2005. <http://www.cert.org/kb/acid/>.

Bastille Linux. Bastille Linux. 2005. <http://www.bastille-linux.org>.

Cisco. Cisco. 2005. <http://www.cisco.com>.

Cohen, Alan. Why standards are important for wireless security. SC Magazine. Feb 07 2005. <http://www.scmagazine.com/features/index.cfm?fuseaction=featureDetails&newsUID=28be92c1-15dc-4332-9024-4a5b4589de7e>.

Dens, Stefan. SnortCenter. SnortCenter. 2005. <http://users.pandora.be/larc/>.

Help Defeat Denial of Service Attacks: Step-by-Step. SANS Institute. Mar 23 2003. <http://www.sans.org/dosstep/index.php>.

HP Proliant Systems. Hewlett Packard. 2005. <http://h18004.www1.hp.com/products/servers/platforms/>.

Integrit. The Integrit Project. 2005. <http://integrit.sourceforge.net>.

Integrity. Checkpoint. 2005. <http://www.checkpoint.com>.

Internet Protocol V4 Address Space. Internet Assigned Numbers Authority. Jan 27 2005. <http://www.iana.org/assignments/ipv4-address-space>.

Lazarikos, Demetrios. My summer of war driving. ComputerWorld. Nov 10 2004. <http://www.computerworld.com/securitytopics/security/story/0,10801,97352,00.html>.

Metz, Cade. The Trouble with Wireless. PC Magazine. Apr 19 2004. <http://www.pcmag.com/article2/0,1759,1570246,00.asp>.

Murilo, Nelson, and Steding-Jessen, Klaus. Chkrootkit. Chkrootkit. 2005. <http://www.chkrootkit.org>.

Network Admission Control. Cisco. 2005. <http://www.cisco.com/en/US/netsol/ns466/netqa0900aecd800fdd6f.html>.

Network Troubleshooting: A Complex Process Made Simple. CyberGuard. 2005. <http://www.cyberguard.com/news_room/Security_Articles/Network_Troubleshooting.html>.

Noonan, Wesley J. Hardening Network Infrastructure. Emeryville, CA: McGraw-Hill, 2004.

Osipov, et al. Cisco Security Specialist's Guide to PIX Firewalls. Rockland, MA: Syngress, 2002.

Poulsen, Kevin. Warspammer guilty under new federal law. Security Focus. Sep 29 2004. <http://www.securityfocus.com/news/9606/>.

RedHat Enterprise Linux. RedHat. 2005. <http://www.redhat.com>.

RFC 1918: Address Allocation for Private Intranets. Network Working Group. Feb 1996. <http://rfc.net/rfc1918.html>.

SANS Institute. Defense in Depth. 2004.

SANS Institute. TCP/IP for Firewalls. 2004.

Snort. Snort. 2005. <http://www.snort.org>.

Symantec. Symantec. 2005. <http://www.symantec.com>.

Tanenbaum, Andrew S. Structured Computer Organization. Upper Saddle River, NJ: Prentice Hall, 1999.

Weiss, Todd R. Hacker in Lowe's case sentenced to nine years. ComputerWorld. Dec 17 2004. <http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,98355,00.html>.

Welte, Harald, et al. NetFilter. 2005. <http://www.netfilter.org>.

Wireless LANs: Defending the Wireless Airwaves. NetworkChemistry. 2004. <http://www.networkchemistry.com/news/whitepaper.pdf>.

World Wide War Drive 4. World Wide War Drive. 2004. <http://www.worldwidewardrive.org/>.

Wright, Joshua. Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection. Polar Cove. 2003. <http://www.polarcove.com/whitepapers/layer2.htm>.

Veritas. Veritas. 2005. <http://www.veritas.com>.

Verton, Dan. 'War Drive' Reveals New York's Hidden Security Flaws. ComputerWorld. Sep 06 2004. <http://www.computerworld.com/mobiletopics/mobile/technology/story/0,10801,95709,00.html>.

5. Appendix

5.1 GIAC Enterprises IP address list

172.20.1.0/24	Primary network (Chicago)
	.1 – Primary firewall interface
	.3 – Internal firewall interface
	.5 – Management firewall interface
172.20.9.0/24	Demilitarized zone (Chicago)
	.3 – Primary firewall interface
	.5 – Primary web server
	.6 – Business Services web server
	.11 – SMTP server
	.21 – Primary NTP server
	.22 – DNS server
	.23 – Secondary NTP server
	.25 – Proxy server
172.20.8.0/24	Secured internal network (Chicago)
	.1 – Internal firewall interface
	.11 – Internal mail server
	.22 – Win2003 Domain Controller (internal DNS, DHCP)
	.23 – SQL database server
	.24 – Internal web server
172.20.7.0/24	Management network (Chicago)
	.1 – Management firewall interface
	.21 – ACS server
	.22 – Check Point Integrity server
	.23 – Syslog server
	.31 – Intrusion detection console
	.41 – Management console
172.20.2.0/24	Internal user network (Chicago)
	.1 – Internal firewall interface
	.101 - 150 – User workstations (allocated via DHCP)
192.168.1.0/24	IDS Private network (Chicago)
	.1 – IDS console
	.11 – IDS sensor (secured internal network, management network)
	.12 – IDS sensor (internal user network)
	.13 – IDS sensor (DMZ network)
172.21.5.0/24	VPN client users
	.101 - 150 – Address pool
172.21.1.0/24	Remote office (New York)
172.21.2.0/24	Remote office (London)
172.21.3.0/24	Remote office (Hong Kong)

5.2 GIAC Enterprises Static IP Translations

x.x.2.50	→ 172.20.9.5	Primary web server
x.x.2.56	→ 172.20.9.6	Business Services web server
x.x.2.58	→ 172.20.9.11	SMTP server
x.x.2.60	→ 172.20.9.22	DNS server