



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

John C. Ash
GCFW Practical Version 4.0

August 2004

Securing the GIAC Enterprises Network

© SANS Institute 2004, Author retains full rights.

Summary

The GIAC Corporation is a distributor of premium fortune cookie sayings. Over the years they have seen their business grow from a small operation to a medium sized business employing many additional employees.

In addition to growing financially and personnel wise, the reliance on computers has also grown over the years. Currently GIAC has a firm reliance on their computers and the data stored on them.

This document is designed to describe the great lengths they have taken to ensure their network and the computers contained within it are kept as secure as possible. While no computer or network is completely secure, a balance of security and accessibility was strived for.

© SANS Institute 2004, Author retains full rights.

Assignment #1

The Wireless Warehouse Project

(Wireless Network Integration, Practical Assignment Wishlist Feb 5, 2004)

GIAC Enterprises recently diversified into the fortune cookie manufacturing. To facilitate this, a new warehouse and manufacturing facility will be opened next door to the GIAC Enterprises corporate headquarters. Because of the special situations involved with the operation of the warehouse, GIAC has decided to utilize a wireless LAN (WLAN) in this facility.

The warehouse will need access to the network from several mobile devices. These include the following;

- Wireless tablets. These devices will be used in the forklifts that move the products around the warehouse. These devices are manufactured by Glacier Computers. They are Intel Pentium based machines running Windows XP. They are mounted on the forklifts, and allow the operators to effectively track the movements of the product from the point they enter the storage facility, until they are loaded on the trucks for shipment. Touch screens and custom designed web applications make this procedure easy on the operators.
- Hand scanners. These devices will be used in the inventory process. These scanners are Intel based embedded PC's running Windows XP as well.

With any project of this magnitude, a complete risk assessment was done. The risks were defined and evaluated, and mitigation strategies were decided upon. This report was then provided to management for their evaluation. The following risks were defined.

- Confidentiality – The data residing on GIAC's network is considered confidential. Various types of data are stored on the various servers at GIAC. These include payroll data, customer information, order information, accounts payable and receivable, and employee information. Any unauthorized disclosure of this information could pose severe consequences to GIAC.
- Integrity – GIAC relies heavily on its data. If an attacker had access to change or corrupt the data, it could prove disastrous to GIAC. Such things as changing or deleting customer's orders, tampering with employee and payroll records, or manipulating the accounts payable system to send payments that are not valid are all situations that GIAC has considered.
- Availability – GIAC relies on their data for the day-to-day operation of the company. Any disruption in the availability of the data impacts their ability to deliver their product. Such disruptions whether due to equipment failure, accident, or willful destruction must be eliminated.

With these risks in mind, GIAC came up with the following specific situations that may occur with a wireless LAN, and the problems associated with them.

- Sniffing – Sniffing is the act of unauthorized “listening in” on the traffic on the network. There are many products that can facilitate this, including Ethereal, Airosniff and NetStumbler. The following security situations are associated with unauthorized sniffing of GIAC.
 1. Data confidentiality can be compromised if someone sniffing the network is able to read the traffic. Since confidential data is passed over the airways, it's essential that a high degree of encryption is used to ensure that any data received through sniffing is unreadable to the potential hacker.
 2. Sniffing can lead to other compromises. For example, sniffing can simply be reconnaissance designed to learn enough about the network to lead to further attacks.
 3. Passive wireless sniffing can be very difficult to detect. However, some events can be detected, and used for wireless intrusion detection.¹
- Unauthorized Access – Unauthorized access is when an individual or group of individuals gains access to services or information for which they were not authorized. This unauthorized access can take the following forms;
 1. Simple access to the network – This is when an attacker gains access at the network level. The attacker gains an IP address on the network, but does not yet have access to any server or other network resource. This may simply be someone accessing the network to use its resources (free Internet access for example), or may simply be one step in a greater attack on the network.
 2. Denial of Services – Someone who has gained unauthorized access to the network may use this access to run denial of services attacks from within the corporate network. These attacks can slow down or completely disrupt access to network resources for legitimate transactions.
 3. Server Compromise – Often the next step for someone who has gained access to the network is to try to gain unauthorized access to a server. There are several reasons that an attacker would do this. Some of these are;
 - Backdoors – An attacker would load software on a server that would allow him to access the server in the event the security flaw that allowed him his access is closed.
 - Data Compromise – An attacker may change or delete data located on the server. This could spell disaster for any organization, such as GIAC, that relies heavily on their data.
 - Denial of Service – The attacker may simply cause the server to fail, thus disrupting the business operations.
 - Further Attacks – The attacker may attempt to use the server to gain further access. For example, key logging may be used on the

¹ Intrusion Detection on Wireless Network; David Dobrotka; [www.sans.org](http://www.sans.org/resources/idfaq/wireless_ids.php);
http://www.sans.org/resources/idfaq/wireless_ids.php

server to capture usernames and passwords for the administrators. Armed with this information and attacker could gain further access to other network resources.

Now that we have enumerated the risks involved with the WLAN, lets take a look at the various security measures that exist to help mitigate these risks. We'll discuss the most popular means of securing the wireless network, and then decide which method should be employed in our wireless implementation.

- **SSID – The Service Set Identifier.** The SSID was originally intended solely as a way to identify one wireless network from another. By default, most Wireless Access Points (AP's) broadcast beacon frames containing the SSID every few seconds. If we turn off these beacon frames, a small amount of additional security can be gained. Because it's very easy to get the SSID through other methods, this is a small step in securing the network. However, choosing a random SSID and disabling the beacon frames is still a good idea.
- **MAC Address Filtering –** MAC address filtering is a great way to secure the network from casual intrusions. With this feature, each access point has a list of the MAC addresses of devices which are authorized to communicate with the access point. This is a great start, however, a dedicated attacker could sniff the network for MAC addresses that are communicating on the network, and modify their OS to send out the stolen address in place of their own.
- **WEP – Wired Equivalency Protocol (WEP)** is a weak encryption technique that utilizes a 40 bit encryption key. There are several short comings with WEP however.² Because of the weak RC4 cipher and because WEP does not provide any method to exchange keys among stations leaves WEP as a poor choice for the security of wireless networks.
- **WEP2 –** Originally pioneered by Lucent under the name of WEP Plus, WEP2 extends the encryption key from 40 bit to 104 bits. This however provides little additional security because it still uses the same RC4 ciphers of original WEP.³ The larger key length only provides a moderate amount of security from brute force attacks, and nothing from the attacks on the RC4 cipher itself.
- **Key Rotation –** Key rotation is very important with wireless communications. Because of the weak nature of WEP, attackers can break the encryption in a short amount of time. Because of this, it's important to change the keys often. By the time an attacker breaks the encryption key, a new key has been put into use. Some products only allow the broadcast keys to be automatically rotated. While this is of some use, it's much more secure to rotate both keys.
- **WPA – WiFi Protected Access.** WPA is a temporary standard to enable administrators to start securing their wireless installations until the newer 802.11i standard is ratified. This standard has several components which we'll look at separately.

² 802.11 WEP: Concepts and Vulnerability; Jim Greier; WI-Fi Planer [Internet]; <http://www.wi-fiplanet.com/tutorials/article.php/1368661>

³ Wireless Security Blackpaper; Trey "Azariah" Dismukes; Ars Technica [Internet]; <http://arstechnica.com/paedia/w/wireless/security-3.html>

- First, WPA uses 802.1X authentication protocol. 802.1X allows users to authenticate to the wireless network by means of a RADIUS server.⁴ If you do not have a RADIUS server available for this, it is still possible to use 802.1X by using a preshared key instead. This allows only authenticated users access to the network. Clients that are unable to authenticate via the RADIUS server or preshared key will not be allowed to communicate on the network until they authenticate.
- Key Management – One of the biggest shortcomings of the WEP Protocol is the use of static keys. Even if the keys were manually changed periodically, there was a major investment in time as each access point and client would need to be manually updated with the new key. WPA adds the use of Temporary Key Integrity Protocol (TKIP). TKIP is required under WPA where WEP was optional under standard WiFi. The TKIP protocol has many functions.⁴ First, it determines the keys to be used, and verifies the clients security configuration. Second, it is responsible for changing the unicast encryption key for each frame. Lastly, it establishes the starting key for each client using a preshared key.
- Replay Protection⁵ – WPA extends the protection from replay attacks by implementing a method called *Michael*. Michael specifies a new algorithm that calculates an 8bit encrypted Message Integrity Code (MIC). The MIC ensures the frame has not been tampered with. In addition, Michael provides protection from standard replay attacks.
- 802.11i – The recently ratified 802.11i standard improves on WPA. In addition to everything in the WPA specification, 802.11i includes AES encryption. AES is currently the algorithm of choice for the U.S. Government, and is considered very secure.
- Wireless Intrusion Detection – Due to the nature of wireless networks, special intrusion detection methods should be used to detect and prevent attacks. Several products such as AirDefense Guard, and Snort-Wireless exist. I believe due to the nature of wireless networks it is even more important to employ effective IDS technologies in these networks.

⁴ WPA wireless security offers multiple advantages over WEP; Brien M. Posey MCSE; TechRepublic [Internet]; <http://techrepublic.com.com/5100-6265-5060773.html>

⁵ Overview of the WPA Wireless Security Update in Windows XP; Microsoft [Internet]; <http://support.microsoft.com/default.aspx?scid=kb;en-us;815485#7>

Now that we know what techniques are available to us, we should try to decide what methods we should use to secure the planned wireless network.

First, it should be remembered that defense in depth requires us to layer our defenses. With this in mind, here are my recommendations on how we should proceed with securing the integration of the wireless network located in the new warehouse into our current wired LAN.

First, the placement of the devices is extremely important. The warehouse is a large building, and will require several wireless access points to provide complete coverage. Three access points installed in the ceiling of the warehouse will provide sufficient coverage.

A site survey was performed to determine the how far the signals reached outside the building. Power levels on the access points were modified to limit the distance outside the warehouse the signal was present. Since the warehouse is located on a fairly remote location, surrounded only by the GIAC headquarters and the GIAC employee parking lots it should be slightly harder for an attacker to launch and attack without being physically detected. However, since attackers can possibly be persons who are trusted to be in the area or even employees this is only one step in our overall strategy.

The physical connection to the wired network is also critical. Implementation of this project will see the following changes in the design of the current network.

- An additional interface will be added to the firewall, and an additional DMZ Zone will be created for wireless access devices.
- The firewall ruleset will be modified to allow access to the application servers from the wireless devices. Since the only applications required for these devices are web based applications housed on the internal Application Server, traffic will be limited to port 80 and 443 traffic to the specific IP address of the application server.

This design allows us to leverage the use of the firewall in protecting the rest of the network from the wireless access devices. If one of these devices were compromised, the only access to the rest of the network would be web traffic to the application server. This greatly reduces the risk to the rest of the network.

Final Recommendations

There are considerable risks involved with using a wireless local area network (WLAN) for the new warehouse project. However, with proper configuration and security measures, the risks can be mitigated, and a design that is free from unacceptable risks implemented. To this end, here is how I believe the WLAN should be created and implemented for this project.

First, Cisco wireless access points will be purchased. These state-of-the-art devices support the latest security methods. Furthermore, since the company has already

standardized with Cisco equipment, the staff is already quite familiar with Cisco, their products, and support personnel.

Next, an additional zone will be created in the firewall to physically connect the WLAN to. This zone will have no access to the network until the WLAN has been implemented, secured, and evaluated by a third party to ensure its security. Separating the wireless network into their own zone on the firewall is an important security step. In the event that someone does gain unauthorized access to the wireless network, we limit their ability to gain access to the wired network by using the firewall to restrict the traffic that is allowed to travel between these networks.

Then, a Microsoft Windows 2000 server will be installed in the WLAN subnet, and configured as a RADIUS Server. This server will handle the authentication of the wireless devices. This server will have the OS hardened to help prevent any unauthorized access to the server.

The access points will use WPA with 802.1X authentication to the RADIUS server. While 802.11i seems to hold great promise for the future, it was felt that the greater level of encryption offered by AES was not warranted in this installation.

Also, the access points will have a unique SSID made up of randomly generated characters, and be configured to not broadcast the SSID.

MAC address filtering will not be used in this installation. It's felt that using 802.1X for client authentication is sufficient. Manually entering the MAC addresses into each access point would complicate the setup, and provide little in the way of extra security.

WEP, WEP2, and Key Rotation will not be utilized in this installation in favor of the WPA standards that surpass these older standards.

The various wireless IDS products should be evaluated, and the one that best fits our needs should be purchased and implemented.

Once all these security measures are implemented a third party should be employed to test the security of the network. Any failures in security should be identified and corrected prior to actual use. Once certified by the third party, the firewall rules should be changed to allow access to the wired network.

Despite all the extra work involved in creating and implementing the wireless network, I believe the convenience of wireless access in our warehouse will make the operation work more effectively and efficiently, and will be cost justified in the end.

Assignment #2

Background

GIAC Corp is the leading provider of Fortune Cookie Sayings. Recently, a deal was signed with The Global Fortune Cookie Company, an international maker of fortune cookies that would make GIAC Corp. their primary supplier. Because of this growth, GIAC decided to make some changes to the way they do business.

Previously, GIAC had writers employed in-house who would write sayings, and store them in a Microsoft Access database. Customers would then purchase these databases, and they would be shipped on CD to the customer.

With the expected growth involved with this new contract some changes were necessary. First, a connection to the Internet was established to allow easy real-time communications with their customers. Second, outside writers were commissioned to supply sayings when the workload for the internal writers becomes too much. An Oracle database server was added to house all their sayings, and keep track of other things, such as order status, and customer contact information.

This document will demonstrate the security measures taken by GIAC Corp. in creating a secure computing infrastructure.

Parties Involved

The connection to the Internet allowed GIAC Corp. to communicate securely with many different parties. These include;

Customers

GIAC Corp. uses a custom web site to communicate with their customers. Customers can sign in to this secure website, and download the exact number of sayings they wish to buy. Customers maintain their contact and payment information on this site also, and can review their past purchase history.

Suppliers

With the dramatic increase in demand, GIAC has decided to employ outside writers to supplement their in-house writing staff. The outside suppliers communicate with GIAC via an "extranet". This custom website is tailored specifically to their needs. This allows them to connect to the GIAC servers, sign-in, and upload their sayings via a secure web site.

Partners

GIAC Corp. has several international partners that translate their sayings and resell them in other countries. These partners access the data directly from their

own portion of the extranet. This allows them to have immediate access to the most current sayings.

GIAC Employees

The GIAC employees access the data via their own local LAN network. This is an Ethernet network running 100 mbps over category 6 UTP cabling. The category 6 cabling will allow for easy migration to Gigabit ⁶Ethernet should more bandwidth become desirable.

GIAC Mobile Sales

GIAC Corp. has a very aggressive mobile sales force. These salespeople travel the world in an attempt to bring GIAC's product to the largest possible audience. This traveling sales force must keep in touch with the main office. They use an Internet connection, and VPN software to do this.

The Public

GIAC Corp. maintains a standard WWW server accessible to the public. This site is used to distribute literature on the products and services that GIAC produces. It also has news and information on the company that potential investors may find of use. Because this is non-secure information meant for general public knowledge, no encryption is necessary on these pages.

Equipment

Several pieces of equipment will be utilized in securing this network. Following is the equipment to be used, as well as the functions they will perform.

External Router

A Cisco 2620 router was chosen as the device of choice for the external router. The external router is the first line of defense from an external attack. As a result, the router has a default deny rule that drops all traffic not absolutely necessary. It also has anti-spoofing rules to protect from spoofing attacks, and egress filtering to ensure that GIAC Inc. is a good Internet neighbor. ¹

Firewall Software

GIAC Inc. has chosen the Checkpoint Firewall-1 NG with Application Intelligence, as their firewall software of choice. Firewall-1 is a leader in firewall software.⁷ The features of Firewall-1, such as Stateful Inspection, and SmartDefense will enable GIAC Corp to run their business over the internet, free from unacceptable risks.

Firewall Hardware

⁶ Mike Chapple, Security Policy Tips, Egress Filtering, TechTarget.com [online], URL: http://whatis.techtarget.com/tip/0,289483,sid14_gci883409,00.html. (June 2004).

⁷ Checkpoint Firewall-1, Mistral Internet [Online]. URL: <http://www.mistral.co.uk/products/security/firewalls-firewall1.asp>. (June 2004).

GIAC has standardized their operation on Dell hardware. As such, a Dell 2650 Server was chosen as their hardware platform. This server will have a single 2.8Ghz Pentium Processor; 4 GB of RAM, and a RAID array in excess of 100 GB. This will allow sufficient storage space for software, as well as a generous partition for the storage of logs.

Firewall Operating System

This server will be running Checkpoint's Secure Platform⁸ operating system. Secure Platform is a hardened version of Linux, distributed by checkpoint specifically to run their products. The easy web enabled administration features as well as the robust functionality and stable performance of this Operating System will serve GIAC Corp well.

Internal Router

A Cisco 2621 was chosen to serve as the Internal Router for GIAC. This router will be configured with two Ethernet connections, which will connect the internal network to the firewall. Filtering will also be done on this router to increase the security of our internal systems.

Hubs

Several hubs are provided where necessary. These hubs will allow the IDS sensor to capture packets at strategic places throughout the network. All of these hubs will be 8 port unmanaged Netgear 10/100 hubs.

Core LAN Switch

GIAC already had a Cisco 6509 LAN Switch as their core LAN Switch. This platform provides plenty of performance and is greatly expandable, allowing for future growth. As such, this switch will serve the purpose for this exercise and will not be replaced.

IDS Software

Snort 2.0 IDS was chosen as the Intrusion Detection System. The IDS will have several sensors monitoring several points around the network.

IDS Hardware

The Snort IDS system will be running on a Dell 2650 server. This server will be running Fedora Core 2 as its Operating System, and will feature three network interface cards. The low cost of this product paired with it's high degree of functionality make it the perfect choice for our IDS system

Cisco VPN 3005

The VPN Solution will utilize a Cisco VPN 3005 concentrator. This device will allow up to 100 simultaneous VPN connections. This should be more than

⁸ Secure Platform, CheckpointSoftware [Online]. URL: <http://www.checkpoint.com/products/secureplatform/index.html>. (June 2004).

enough for the near future, and will allow for the secure communications between GIAC and authorized outside entities.

Antivirus Software

The Symantec Antivirus 8.1 Corporate Edition was chosen as the Antivirus Solution for GIAC Corp. This suite of applications includes a WWW and SMTP proxy as well as desktop and server antivirus applications.

Budgetary Considerations

Despite the necessity for an environment free from unacceptable risks, it was also necessary to keep the costs down. Because of this, GIAC chose to use free software whenever prudent. The Snort IDS for example gives the corporation a robust Intrusion Detection System for very little expenditure. Also, since GIAC already has employees that are somewhat familiar with the maintenance and configuration of Linux, it was decided to use Linux as the operating system on the IDS Server as well as a version of Linux (Secure Platform) on the Firewall itself.

Also, it was decided to connect the VPN 3005 to the Internet via a DSL Link. This not only provides a cost effective solution for remote access, but also has some security advantages because the DSL IP address does not show up as an address associated with this organization. It is not distinguishable from a DSL address in use at someone's home.

Servers to be used

GIAC Corp will use several servers to accomplish their Internet connectivity goals. These are the various servers and their function in the GIAC Corporation.

- WWW – WebServer. This is the main web server for GIAC's publicly accessible web pages. This is a Windows 2000 server running Internet Information Server as its HTML Service. The server has 2 virtual directories. These are for the main web site and one for the secure web site. The Extranet is secured by a Verisign Certificate.
- SMTP Proxy – This server that is used for receiving scanning and transferring inbound emails to the Exchange server on the internal network. This is a Windows 2000 Server running Symantec Antivirus for SMTP Gateways Version 3.1.0
- Log Server – The Log Server is a Linux machine running Fedora Core 2. This server primarily runs a syslog daemon that accepts outside connections from the routers and other network equipment. It also has an apache web server running on it that allows administrators from within the internal network to access the log files via some custom built web pages.
- Database Server – This is a Windows 2000 Server running the Oracle 9i Database software. This server is accessed directly by the clients on the internal network, as well as the WWW Server in the DMZ. However, for

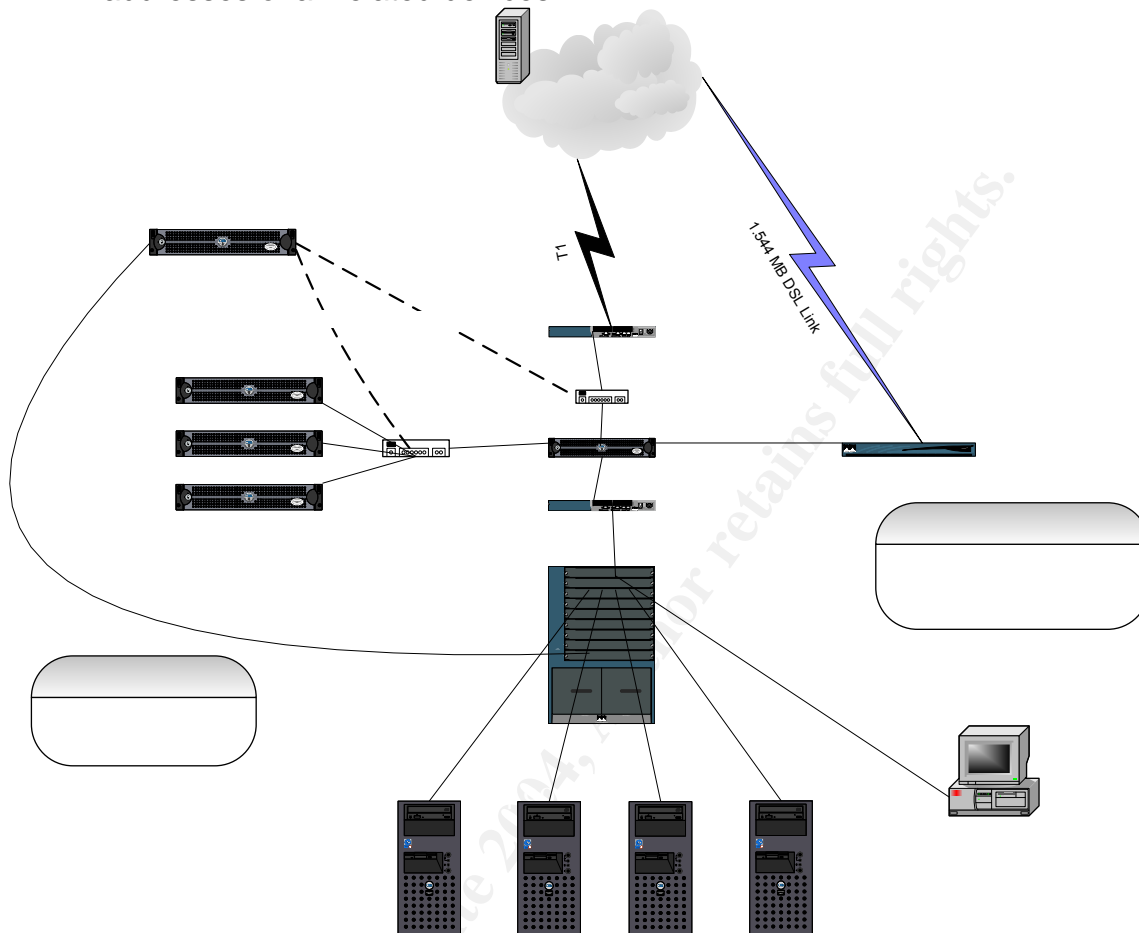
security reasons, we've changed the port that is used to connect to the Oracle server to port 7890.

- Exchange Server – This is a Windows 2000 Server machine running Microsoft Exchange 2000. This server processes inbound emails from the SMTP proxy server, sends outbound emails to the Internet, and accepts connections from clients on the internal network.
- Proxy Server – This is a Windows 2000 Server machine running Symantec Web Security 3.0.⁹ This server accepts connections from the client computers on the internal network. Then it retrieves the pages from the internet, and scans them for viruses as well as for content. The pages are then passed back to the client computer.
- Windows Domain Controller – This is a Windows 2000 Server configured as a domain controller. It uses Active Directory to manage the user and group information for the internal domain. Group Policies are used extensively by the Systems Administrator to enforce security policies throughout the domain. This server also has the Symantec Antivirus Corporate Software on it. This server serves as the Antivirus Server, and pushes out the AV updates as necessary. It is set to check for new updates every 4 hours.
- SNORT IDS – This is a Server running Fedora Core 2 as well as the Snort 2.0 IDS Software. This server has three network cards

⁹ Symantec Web Security, Symantec [Online], URL:
<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=60>

Network Layout

The following is a logical representation of the network layout including the IP addresses of all related devices.



As you can see the network is split into 4 separate security zones connected by the firewall. These zones are;

- Internal – This zone is the main network for GIAC Corp. This is where the majority of the employees and servers are located.
- VPN – This zone houses the Cisco VPN 3005, and is used for communications to outside entities. As such, it has some degree of trust and connectivity to the internal zone.
- DMZ – This is the zone that houses all the externally accessible servers. This zone has some degree of trust and connectivity to the internal network.
- External – This zone consists of devices directly connected to the Internet. This is the least trusted zone. – Notice there is no direct connections to the Internal Zone from the External Zone!

The following IP Addressing scheme was used.

No IP Address

Network	IP Address	Net Mask
Internal Network	192.168.0.0	255.255.255.0
DMZ Network	10.0.1.0	255.255.255.0
Public IP Addresses	123.45.67.65	255.255.255.240
Admin VPN Network	10.10.0.32	255.255.255.224
Sales VPN Network	10.10.0.64	255.255.255.224

Traffic bound for the Internet Zone is restricted to only the services necessary to complete the employees' jobs. All other traffic to the Internet is restricted.

Allowed services include the following;

- HTTP – Employees access outside web servers via a proxy server running Symantec's Web Security application. This proxy server retrieves any requested external web pages, and scans them for viruses and inappropriate material.
- SMTP – GIAC Corp utilizes an exchange server for all its email requirements. Clients transmit email to the exchange server, and the exchange server sends the email out to the internet using the SMTP protocol.
- DNS – GIAC Corp's ISP hosts all of GIAC Corp's Internet DNS and MX records. A DNS service running on the Windows Domain Controller allows for resolution of internal addresses. Should the request be for an outside address, the server forwards the request out to the ISP's DNS Server, or to a root server on the Internet.

Port / Service	Source	Destination
HTTP	Proxy Server	Anywhere
HTTPS	Proxy Server	Anywhere
SMTP	Exchange Server	Anywhere
DNS	Domain Controller	Anywhere
Telnet	Management Station	Routers

Traffic bound to the DMZ is allowed to take place for the following purposes;

- HTTP – Anyone on the Internet can get to the WWW Server using port 80. This allows the general public access to the public website. The public website is used to publish marketing materials, investor information, and contact information.
- HTTPS – Anyone on the Internet is allowed to contact the Extranet site on the WWW Server. This will take them to the login screen for the extranet. Only authorized partners have been given an Extranet password. These people can then sign into the secure website using their username and password. Once signed in, the partners can access the custom designed website.

- SMTP – Any site on the internet has the ability to send email to the email proxy via the SMTP service. This server then scans the email for viruses, illegal content (such as executable programs or scripts), and spam, and processes the message accordingly. If the email passes all these tests, it is then relayed to the Exchange server on the internal network. Since all email is accepted by the SMTP Proxy and then relayed to the internal network, at no time does an external server access an internal server directly.
- Syslog – The routers forward log messages to the log server via Syslog. This server records those messages into a log file for later analysis by the Network Administrator
- HTTP – The Management Station uses custom designed web pages to view the log files stored on this server.

Port / Service	Source	Destination
HTTP	Anywhere	WWW
HTTPS	Anywhere	WWW
SMTP	Anywhere	SMTP Proxy
Syslog	Routers	Log Server
HTTP	Management Station	Log Server

Inbound traffic into the internal network is limited to the following services.

- Database Traffic - The web server in the DMZ contacts the database within the internal network. This enables the server to use real live data to create dynamic web pages. The GIAC programmers have created several web applications for the GIAC Corp Extranet that allow partners secure access to the data. For security reasons, the standard Oracle ports are not used for this communication. Instead, Oracle is listening on port 7890. Since this port is non standard port, should an attacker run a network scan from within the DMZ, it would not show a port open that is easily identifiable as an Oracle port, thus denying the attacker one small piece of information about the systems on the inside.
- SMTP Traffic – SMTP Traffic from the SMTP Proxy Server in the DMZ to the Exchange server in the internal network is allowed. This allows email to be routed to the internal Exchange server after it has been scanned for viruses and spam.

Port / Service	Source	Destination
DB Traffic - Port 7890	WWW	Database Server
SMTP	SMTP Proxy	Exchange Server

VPN Traffic is traffic originating from users connected to the VPN 3005. Such users are divided into two separate groups based on their login credentials. These groups are as follows.

Administrators – Administrators use the VPN connection to remotely manage the network. Because GIAC Corp relies heavily on its network for the operation of its business, uptime is very important. The use of VPN for administrators allows them the flexibility to make changes at off hours, or to respond to issues more quickly. This access takes the following form:

- Access to the Exchange Mail Server – Administrators use the Outlook Web Access portion of the Microsoft Exchange Server to connect to their email from a standard web browser. This allows them to read and respond to emails from anywhere they can get an Internet connection.
- Telnet – Administrators can use telnet to connect to the routers to make configuration changes. This allows them to respond to security issues, as well as make any operational changes that may be necessary. Telnet itself is not a very secure protocol. The current setup of the routers prohibited the use of SSH however. A future upgrade will include more memory and a more robust IOS package for these routers allowing us to use SSH. To mitigate the insecurities with Telnet, we've limited access to the telnet services on these routers to just the management station and the VPN group for the administrators. These limitations are done at the firewall level as well as on ACL's on each of the routers. Since there is no access to these services from anywhere outside of these locations the likelihood that the routers could be compromised is minimal.
- Terminal Services – Administrators use Microsoft's Terminal Services as a way to remotely connect to their servers. This feature gives them the ability to work on one of these servers much like they were physically at that machine.
- Proxy – Administrators may occasionally have to connect to the internet while connected to the corporate network via VPN. Because of this, we allow them to connect to the Proxy Server using port 8080.

Port / Service	Source	Destination
HTTPS	Admin VPN	Exchange Server
Telnet	Admin VPN	Routers
Terminal Services	Admin VPN	Internal Network
Proxy Port - 8080	Admin VPN	Proxy Server

Mobile Sales Staff – The Mobile Sales Staff uses the VPN connection for several purposes. These purposes are as follows;

- The Sales Staff connects to their email via Outlook Web Access using port 443. This allows them to effectively stay in touch while they are out of the office.
- The Mobile Sales Staff also uses the Internet for research, and access it while they are connected to the VPN through the proxy server. Thus, access to the Proxy Server from their VPN group must be allowed.
- The Mobile Sales Staff also uses a custom written application loaded on their laptop computers to connect to the Oracle Database. This access is granted to port 7890, which Oracle has been instructed to listen on.

Port / Service	Source	Destination
HTTPS	Sales VPN	Exchange Server
Proxy Port - 8080	Sales VPN	Proxy Server
Oracle Port - 7890	SALES VPN	Oracle Server

Defense in depth

Several key components of the security design don't deal directly with the network, but are still critical in creating a secure environment for our network, and the data carried on it.

- Physical Security – All routers, switches, firewalls and servers will be housed in the GIAC Corp Computer Room. This room is secured with an electronic access control system that allows access to only authorized personnel. Members of the IT Staff are the only people authorized for access to this room. Power to the server room is supplied by a large capacity UPS which is backed up a natural gas generator. The server room has sufficient fire suppression equipment and cooling equipment to protect all equipment in this room
- Policies and procedures – GIAC Corp has evaluated its policies and procedures, and deemed them to be adequate. Review of these is beyond the scope of this document.
- Patch Management Procedures – GIAC has extensive procedures in place for patching their systems from vulnerabilities as they are released.
- Vulnerability Scanning / Penetration Testing – GIAC is assessed by an outside security consultant every quarter, and also when significant changes to the firewall and routers have been made. The results of these tests are evaluated, and any necessary changes are made. The results and any changes made to correct problems are then reported to the management of GIAC Corp for their review. If significant changes are made to correct any problems found, an additional scan may be requested to verify the completeness of the corrective actions.

© SANS Institute

Assignment #3

For this section, we'll look at the ruleset that was put in place on the firewall. Please refer to the ruleset located on page 22.

Firewall-1 processes the ruleset in a top-down manner. This means that when a packet is received, it's first compared to the first rule in the ruleset. If it matches this rule, the appropriate action is taken immediately. If the rule does not meet the criteria of the first rule, the packet is then compared with the next rule. This procedure continues until the packet matches a rule, or it falls to the end of the list, in which case it's dropped.

Since the rules are applied in a top-down manner, the first rule we define allows access to the firewall from the management station. This ensures that no matter what rules follow, we'll always be able to contact the firewall from the management station to make corrections. Should this rule be further down the list, a rule above it may block access to the firewall, and we would not be able to make any further changes. Also, you should note that the track option on this rule is set to "log". Anytime someone connects to the firewall we want the access to show in the firewall logs.

We split the rest of the rules up into sections. The sections have no real effect other than organization. We've decided to organize our rules based on traffic. This allows us to quickly find the rule we need without looking through every rule in the ruleset. Because of the top-down processing style of CheckPoint though, it should be kept in mind that the first rule that matches the packet will decide the action taken, despite what section it is in.

Splitting the rules into sections also makes management easier. If we need to disable all access to the network for the mobile sales team, we can quickly do this by disabling each rule in their section.

The next set of rules is designed to allow access to the internet from internal devices. The following rules were defined;

- The firewall accepts packets from the Proxy Server destined for anywhere using the HTTP and HTTPS protocols. This allows the Proxy Server to retrieve web pages from the internet on behalf of the clients on the internal network.
- Packets from the exchange server with any destination using the SMTP protocol are accepted. This rule allows the Exchange server to send email to the internet using SMTP.
- The next rule allows the Domain Controller, which functions as the DNS server for the internal network to send DNS requests out to the internet. This allows the server to resolve names for external servers.
- Rule 5 allows the internal management station to contact the external router via the telnet protocol.

The next section holds rules that allow traffic to the DMZ. This includes access from people on the Internet as well as people located within our internal network.

- Rule 6 allows anyone to access the server named WWW using the HTTP or HTTPS protocol. This allows access to the web site and web based applications located on these servers.
- The next rule allows anyone to connect to the SMTP proxy server using the SMTP protocol. This allows us to receive email from the general public.
- Rule #8 specifies that both the internal and external routers are allowed to send log data to the log server via the syslog protocol. The routers send log data to this server where it is cataloged, and stored for later review.
- The next rule allows the management station to connect to the log server using the HTTP protocol. This allows an administrator to view reports and other data using his web browser. Custom written applications serve up the data using an apache web server.

The next section in our rulebase is for communications from the DMZ to the internal network, and is made up of the following rules;

- Rule #10 allows the SMTP proxy server to send the mail it has received from the Internet on to the exchange server located in the internal network. It does this after it has scanned the messages for viruses and other unauthorized content.
- The next rule allows the WWW server to contact the database server using port number 7890. Even though the Oracle server is listening on an unusual port, the protocol in use is still SQLNet.

The next section in the ruleset is designed to allow access to the network from administrators using VPN. Administrators use VPN not only for routine things like checking their email, but also to work on the various systems within the network.

- The first rule in this section is designed to allow the VPN-Admins group access to the exchange server using the HTTPS protocol. This allows them access to their email via Outlook Web Access, an application on the exchange server that allows someone complete access to their outlook resources using only a web browser.
- The next rule allows the VPN-Admins group to access the routers via the Telnet protocol. Administrators often have to make changes to routers after hours. This rule allows them the convenience to make these changes from their home offices, while on vacation, or anywhere else they have access to the Internet and their VPN client.
- Rule #14 Allows the VPN-Admins group access to the terminal services protocols to contact any machine on the internal network. The administrators use this ability to remotely control any of these machines almost exactly as if they were sitting in front of it.
- Rule #15 the VPN-Admins group to contact the proxy server on port 8080. This allows them to send requests for web pages to the proxy server.










































































































































The next section is designed to allow the mobile sales team access to the network resources they need while on the road. These rules include;

- Rule #16 allows the Sales Team access to the exchange server via HTTP while using their VPN connection. This allows them to send and receive email using Outlook Web Access.
- The next rule allows the Sales team access to the proxy server. This allows them to retrieve web pages from the internet without disconnection from VPN.
- The last rule in this section allows the Sales team to connect to the database server directly using port 7890. The Sales team has custom applications that talk directly with the database over this port.

The final rule in our ruleset is a clean-up rule. Since CheckPoint processes these rules in a top-down manner, this rule drops any traffic that is not explicitly accepted by an earlier rule. Not only does this rule drop the packets that are not accepted by earlier rules, it also logs them. A review of these packets is important because it can tell you what traffic has attempted to cross your firewall intended for your internal network.

© SANS Institute 2004, Author retains full rights.

Security Policy: Standard

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Firewall Management (Rule 1)									
1	 Mgt_Station  INTERNAL	 Cerberus	 Any Traffic	TCP CPMI TCP FW1 TCP https	 accept	 Log	 Policy Targets	 Any	This allows the Management Station to connect to the Firewall to manage it with SmartDashboard and HTTP.
Access to the Internet (Rules 2-5)									
2	 Proxy_Server	 Any	 Any Traffic	TCP http TCP https	 accept	 None	 Policy Targets	 Any	The Proxy Server is allowed to retrieve web pages from the Internet on behalf of internal workstations.
3	 Exchange_Server	 Any	 Any Traffic	TCP smtp	 accept	 None	 Policy Targets	 Any	The Exchange Server is allowed to send mail to the Internet.
4	 Domain_Controller	 Any	 Any Traffic	TCP dns	 accept	 None	 Policy Targets	 Any	The internal DNS Server is allowed to access the Internet for DNS.
5	 Mgt_Station	 EXTERNAL	 Any Traffic	TCP telnet	 accept	 None	 Policy Targets	 Any	Management Station is allowed to access the External router to make changes via telnet.
Traffic to the DMZ (Rules 6-9)									
6	 Any	 WWW	 Any Traffic	TCP http TCP https	 accept	 None	 Policy Targets	 Any	Anyone is allowed to connect to the WWW Server via HTTP and HTTPS.
7	 Any	 SMTP_Proxy	 Any Traffic	TCP smtp	 accept	 None	 Policy Targets	 Any	Anyone is allowed to send email to the SMTP Gateway.
8	 EXTERNAL  INTERNAL	 Log_Server	 Any Traffic	UDP syslog	 accept	 None	 Policy Targets	 Any	This rule allows the routers to send log messages to the log server.
9	 Mgt_Station	 Log_Server	 Any Traffic	TCP http	 accept	 None	 Policy Targets	 Any	The Management Station needs to access the Log Server via HTTP to view the custom designed log viewer web pages
Traffic from the DMZ to the internal network (Rules 10-11)									
10	 SMTP_Proxy	 Exchange_Server	 Any Traffic	TCP smtp	 accept	 None	 Policy Targets	 Any	The SMTP Proxy Server sends email to the internal Exchange after the emails have been scanned to eliminate SPAM and viruses.
11	 WWW	 DB_Server	 Any Traffic	TCP TCP-7890	 accept	 None	 Policy Targets	 Any	The WWW Server retrieves information from the Database Server via port 7890.
VPN Access - Admins (Rules 12-15)									
12	 VPN-Admins	 Exchange_Server	 Any Traffic	TCP https	 accept	 None	 Policy Targets	 Any	Admins access their email via Outlook Web Access on the Exchange Server on port 443.
13	 VPN-Admins	 EXTERNAL  INTERNAL	 Any Traffic	TCP telnet	 accept	 None	 Policy Targets	 Any	Administrators need to telnet to the routers for configuration changes.
14	 VPN-Admins	 Internal_Network	 Any Traffic	TCP Terminal-Service	 accept	 None	 Policy Targets	 Any	Admins use Terminal Services to administer the Windows Servers
15	 VPN-Admins	 Proxy_Server	 Any Traffic	TCP Proxy_Port	 accept	 None	 Policy Targets	 Any	Admins can access the proxy server via port 8080 to retrieve web pages from the Internet.
VPN Access - Sales (Rules 16-18)									
16	 VPN-Sales	 Exchange_Server	 Any Traffic	TCP https	 accept	 None	 Policy Targets	 Any	Sales Staff can access their email through https using the Microsoft Outlook Web Access on the Exchange Server
17	 VPN-Sales	 Proxy_Server	 Any Traffic	TCP Proxy_Port	 accept	 None	 Policy Targets	 Any	The mobile Sales Force can use the Proxy Server to access web pages on the Internet.
18	 VPN-Sales	 DB_Server	 Any Traffic	TCP TCP-7890	 accept	 None	 Policy Targets	 Any	Sales can use port 7890 to access the Oracle Database.
Clean-up Rule (Rule 19)									
19	 Any	 Any	 Any Traffic	 Any	 drop	 Log	 Policy Targets	 Any	Default deny rule. This drops any traffic that has not been specifically approved by another rule.

References

- ¹ Intrusion Detection on Wireless Network; David Dobrotka; [www.sans.org; http://www.sans.org/resources/idfaq/wireless_ids.php](http://www.sans.org/resources/idfaq/wireless_ids.php)
- ² 802.11 WEP: Concepts and Vulnerability; Jim Greier; WI-Fi Planer [Internet]; <http://www.wi-fiplanet.com/tutorials/article.php/1368661>
- ³ Wireless Security Blackpaper; Trey "Azariah" Dismukes; Ars Technica [Internet]; <http://arstechnica.com/paedia/w/wireless/security-3.html>
- ⁴ WPA wireless security offers multiple advantages over WEP; Brien M. Posey MCSE; TechRepublic [Internet]; <http://techrepublic.com.com/5100-6265-5060773.html>
- ⁵ Overview of the WPA Wireless Security Update in Windows XP; Microsoft [Internet]; <http://support.microsoft.com/default.aspx?scid=kb;en-us;815485#7>
- ⁶ Mike Chapple, Security Policy Tips, Egress Filtering, TechTarget.com [online], URL: http://whatis.techtarget.com/tip/0,289483,sid14_gci883409,00.html. (June 2004).
- ⁷ Checkpoint Firewall-1, Mistral Internet [Online]. URL: <http://www.mistral.co.uk/products/security/firewalls-firewall1.asp>. (June 2004).
- ⁸ Secure Platform, CheckpointSoftware [Online]. URL: <http://www.checkpoint.com/products/secureplatform/index.html>. (June 2004).
- ⁹ Symantec Web Security, Symantec [Online], URL: <http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=60>

© SANS Institute 2004, Author retains full rights.