Global Information Assurance Certification Paper

Kevin Murphy
March 21, 2004
GCFW Practical Assignment v4.1

Table of Contents

Assignment 1

Wireless Network Integration for GIAC Enterprises

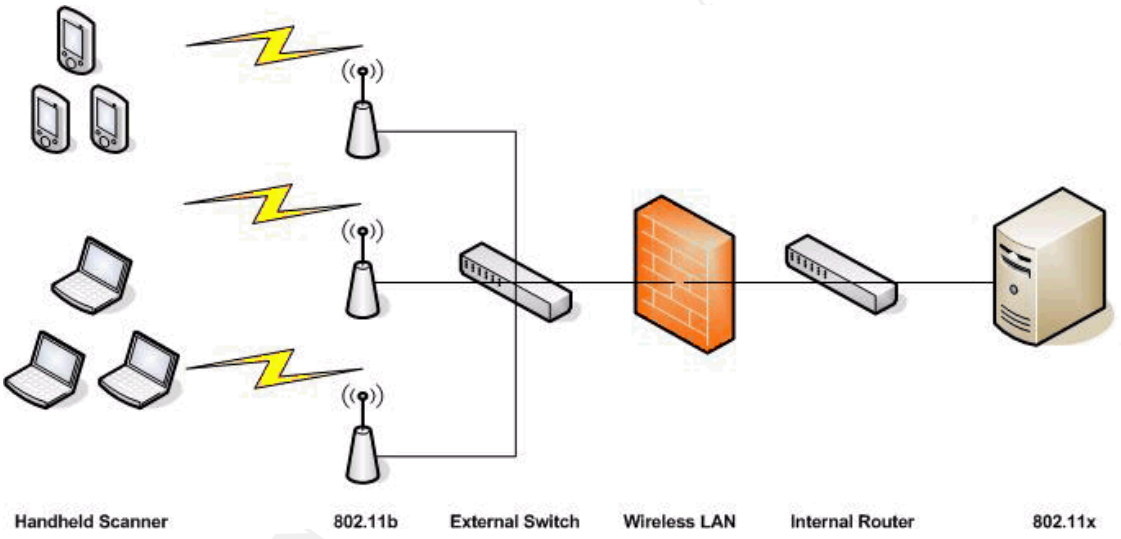
Abstract

GIAC Enterprises has decided to implement a wireless network in their new warehouse for shipping and manufacturing of fortune cookies. Handheld scanners and laptop computers will connect to the network in order to access the company's inventory web application. The network will need to be secured from unauthorized users and encrypt data for security. GIAC will also need to deploy a firewall between this network and the main corporate LAN for security and monitoring.

This document will review and make recommendations for this new wireless network - network design, wireless technology, encryption standards and security recommendations will all be addressed.

Network Design

Below is a simplified diagram of the proposed GIAC Wireless Network. Specific IP addressing will be included as part of Assignments 2, 3, and the entire GIAC Network Diagram.



Handheld Scanners

Handheld Scanners running Windows Mobile will access GIAC's inventory web application over this new wireless network. They will be accessing a special text-only HTTPS webpage. The scanners will read labels on inventory and shipments, and automatically fill the fields into the web application for submission.

Laptop Computers

Laptop Computers running Windows XP will access GIAC's HTTPS inventory web application over this new wireless network. The managers in the warehouse area will also use them to read email.

802.11b Access Points

802.11b Access Points will be installed throughout the warehouse to be accessed by scanners and laptops. GIAC will need to undergo a physical site survey of the new warehouse to determine the number and location of access points and repeaters required to provide coverage to all areas. Power and network drops this equipment will need to be considered when constructing or purchasing a warehouse. All of the access points will be connected to a network switch. For testing signal strength and client range, there are numerous tools – both software based, and integrated hardware devices available. "Netstumbler" (http://www.netstumbler.com) is easy to use and free although donations are requested for corporate use.

Checkpoint Firewall

Checkpoint Firewall running on the Nokia IPSO platform will be deployed to segregate the wireless network from GIAC's corporate LAN. The firewall will be dual-homed, connected to the switch (with the access points), and to the corporate LAN. It will be a satellite firewall – receiving its policy from the central management server, and transferring its logs to the logging server.

802.1x RADIUS Server

An 802.11x RADIUS server will be deployed behind the firewall, on the corporate LAN. The 802.11b access points will communicate through the firewall to this server to manage allowed clients and encryption keys.

Network Printers

Network Printers will be physically wired into the main Corporate LAN for ease of install and administration. Handheld Scanner and Laptop users will be able to generate shipping labels and order summaries via the web application.

Wireless Technology

There are a number of different wireless technologies currently available, and several emerging technologies as well. The first thing GIAC needs to do is choose a standard with the bandwidth, security, and potential upgradeability that meets their needs. The following is a summary of the advantages and disadvantages of each technology, based on the Wikipedia entry for "IEEE 802.11" http://en.wikipedia.org/wiki/IEEE_802.11 [1].

802.11b

Introduced in September 1999, 802.11b is the most mature of the wireless technologies. It has an 11Mbps theoretical maximum bandwidth and operates in the unlicensed 2.4Ghz radio spectrum. This makes it somewhat susceptible to interference from machinery/electronics and signal degradation through walls and floors. After being introduced, several security flaws were discovered in the default WEP encryption algorithm [2]. Other security protocols have been developed since then to properly secure 802.11b. The market for 802.11b

equipment is very competitive and prices are low.

802.11g
802.11g is the successor to the 802.11b standard, supporting the older standard and operating in the same radio spectrum. Officially approved in June 2003 [3] this standard has a 54Mbps theoretical maximum bandwidth and supports the older 802.11b standard. However, 802.11g access points supporting 802.11g and 802.11b clients will force all clients to operate at 11Mbps (802.11b speed). Because of its 802.11b compatibility, the market for 802.11g equipment is becoming competitive and prices are falling.

802.11a
802.11a was approved at the same time of 802.11b but equipment did not hit the market until 2001. Supporting a 54Mbps maximum theoretical bandwidth and operating in the less-crowded 5Ghz radio spectrum, 802.11a had several advantages over 802.11b but could not overcome its head start in the market. 802.11a equipment is still priced at a premium over both 802.11b and 802.11g equipment. 802.11a also requires "almost line of sight" [1] between clients and the base station for maximum communication speeds making deployments more difficult and expensive.

802.11n
An emerging technology that has not been officially approved yet, "Pre-N" equipment has just hit the market. With maximum theoretical speeds of 108Mbps and better signal range/coverage than the older wireless standards [4], 802.11n is designed to fix some of their shortcomings. Testing has demonstrated the 802.11n signal passes through walls and floors better. Pre-N equipment pricing is high because it is so new. There are two major caveats with 802.11n though, the standard is not expected to be finalized until 2006, and the Pre-N equipment is not guaranteed to work with the finalized standard.

It is recommended that GIAC deploy the 802.11b wireless technology in their new warehouse. At this time, this is the only standard available for the Windows Mobile Handheld Scanners. The standard will be fast enough to support their inventory applications while the cost will be reasonable enough to cover the large warehouse area. Once 802.11g wireless becomes available in the handheld scanners, GIAC can consider upgrading.

Encryption

An inherent flaw with any wireless technology it is susceptible to eavesdropping by anyone in range, an activity known as "War Driving" [5]. Therefore it is critical to encrypt the communications on the network. With the recommended 802.11b wireless standard, GIAC has three choices of encryption technologies; Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) or WPA2 which is an implementation of the 802.11i standard [6].

WEP
Wired Equivalent Privacy was developed in 1999 and introduced with the 802.11 standard. As mentioned before, in 2001 the encryption was cracked and this standard is no longer considered secure – especially in a corporate environment [7].

WPA
Wi-Fi Protected Access was developed in April 2003 to replace the broken WEP standard. It is deployed along with an 802.1x authentication server to manage clients and handle the distribution of encryption keys. The major advantage over sWEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys over time; something that WEP did not do that led to its ultimate cracking [8]. WPA can also be deployed in a home or small office environment using a pre-shared key instead of 802.1x, however this configuration is less secure.

WPA2
Developed in June 2004 using the Advanced Encryption Standard (AES) block cipher, which is stronger than the RC4 stream cipher of WPA. WPA2 is the "marketing name" for products that support the 802.11i encryption standard for wireless networks. This standard meets certain government requirements for encryption, and is likely to be used by government agencies, financial institutions, and other industries looking for the highest level of encryption available [9].

It is recommended that GIAC deploy WPA Encryption in conjunction with an 802.1x authentication server. While GIAC's Fortune Cookie Sayings can be considered their "trade secret" and need to be protected, because there is neither sensitive customer data, nor governmental security regulations on the Fortune Cookie business it is probably not necessary to deploy WPA2 at this time. Should the need arise, GIAC could upgrade to WPA2 in the future.

Additional Security Recommendations

MAC Filtering
All GIAC scanners and laptops being deployed in the warehouse will have their MAC address noted. The access points will be configured to allow only these clients to connect. This will provide an additional layer of security on top of the encryption and 802.1x authentication.

Assignment 2

Security Architecture for GIAC Enterprises

Abstract

GIAC Enterprises is a small but worldwide business that creates and markets fortune cookie sayings. They are expanding their business, having recently purchased a new warehouse for the manufacturing and shipping of fortune cookies. GIAC will also be moving its main corporate offices into office space in this new warehouse. In order to

support their new line of business and salesforce, GIAC is upgrading its entire corporate LAN and is soliciting proposals.

GIAC employs approximately 50 people, the majority at the new corporate HQ and warehouse in Albany, NY. This office houses the majority of the IT infrastructure, including the company's main internet connection. GIAC has a high-speed 100MB internet connection from Cogent Communications (http://www.cogentco.com/) which is sufficient enough to support their remote offices, remote users, and host their public website.

There are 4 worldwide satellite offices: Los Angeles (CA), London (England), Sydney (Australia), and Seoul (South Korea). None of the offices employ more than 10 people. Each office has a full T1 and connects to the HQ office via an IPSEC VPN.

GIAC IT is mostly a Microsoft shop, running Windows 2003 Server, Microsoft Exchange 2003, and Microsoft SQL 2000 servers. Management decided on the platform because of the ease of server integration and end-user familiarity with Windows XP. Management encourages the IT department to use Linux "behind-the-scenes" when appropriate. IT has standardized on Red Hat Enterprise Linux 4 for use due to its stability and support options.

Access Requirements:

To properly design the GIAC network, it is critical to understand which groups of people will be accessing it and what requirements they each have.

Customers

Customers of GIAC will access a publicly available, SSL secured web application in the DMZ. They will need to logon with a username and password that will be provided by GIAC after establishing an account with GIAC Accounts Receivable. New customers must phone or fax in their billing information to the corporate HQ to open an account. They will be then able to view inventory, place orders, check on shipping and review billing for their account via the website. For security and cost savings purposes (lower credit card fees), no credit card information will be taken or stored online.

The web application will have a back-end DB server in the DMZ as well. For security, this DB server will be completely separate from the company's main DB server on the corporate LAN. Scheduled tasks/batch jobs will be setup to export the customer DB tables to text file and transfer them to the web development FTP server (via SSL). The web development team will then import these orders into the main GIAC web application. The frequency of these export/imports is to be determined by management and the web development team.

Suppliers

Suppliers of GIAC will connect to the GIAC network via a secure IPSEC VPN

using a GIAC provided SecurID card. They will be assigned an IP address from the external firewall for the Supplier and Partner Virtual LAN (VLAN). Suppliers mainly need to upload a DB export text file with new fortune cookie sayings. They will upload this file via FTP over SSL to a server in the DMZ.

Suppliers also need access to a HTTPS server on the Corporate Server LAN running the GIAC web application. This will be a different server and different application than the main corporate web application, but running on the same back-end DB.

Partners
Partners of GIAC will connect to the Supplier and Partner VLAN in the same manner as the suppliers to access the same web application.

Occasionally, partners will need a DB export text file from GIAC. The web development team will place these files on the DMZ FTP server for downloading via FTP over SSL. As mentioned, access to this server will be password protected to keep out the majority of the partners whose only need is the web application.

Internal Employees
Internal Employees need general internet access – DNS, HTTP, HTTPS, and FTP. In order to properly monitor employee internet usage, all internet traffic will go out through the company's main internet connection. This includes the remote offices – traffic will sent to the HQ LAN over the VPN connection, and then out to the internet. Due to the threat of viruses Instant Messaging will be blocked.

Internal employees will also need access to various servers on the corporate server LAN:
- File and print sharing to the main file and print server
- HTTPS access to web application
- RPC access to Exchange server

Web Developers
Web developers responsible for the company's internal and external web applications and databases will be located at the corporate HQ on their own separate LAN. They will need the same access as the rest of the internal employees for the internet and corporate servers. In addition, they will need FTP over SSL access to the DMZ FTP server in order to transfer files between the testing and production environments.

Warehouse Users
GIAC staff in the warehouse will be accessing the network via the company's wireless network, using handheld scanners. They will need HTTPS access to the corporate web application. Also warehouse managers with laptops will need

the same HTTPS access, plus RPC access to the corporate email server.

Remote Users
Remote Users will receive a SecurID card and connect via VPN to the corporate LAN. Users will be at home on cable/DSL connections, or on the road. Once connected, they will be placed on their own VLAN separate from the Suppliers and Partners. They will need the same access as the internal users, to the corporate servers and to the internet.

IT Support Staff
Occasionally, a member of the IT Support Staff will need secure remote access to the GIAC LAN. To facilitate this, they will connect via a VPN much like the standard remote users. Using an alternate set of credentials than their normal account, they will be authenticated, assigned an IP address and placed on VLAN separate from the normal remote users.

They will then need Terminal Server access from the VLAN to servers on the corporate server LAN.

General Public
The general public will need access to the company's public HTTP server located in the DMZ. Here they will be able to learn about the company and contact us if they are interested in doing business.

This chart summarizes the access requirements:

Group	Source	Destination	Ports/Protocols	Description
Customers	Internet	HTTP server in DMZ	443 (TCP)/HTTPS	Public access to HTTPS customer web application
Suppliers	Internet	External Firewall	500 (UDP)/IKE 50 (TCP)/ESP 51 (TCP)/AH	Establish VPN tunnel with SecurID card to Partner and Supplier VLAN
	Supplier & Partner VLAN	FTP server in DMZ	989 (TCP)/FTPS-Data 990 (TCP)/FTPS	Transfer DB files via FTP over SSL
	Supplier & Partner VLAN	HTTPS server in Corp. LAN	443 (TCP)/HTTPS	Access to HTTPS Supplier and Partner web application
Partners	Internet	External Firewall	50 (TCP)/ESP 51 (TCP)/AH 500 (UDP)/IKE	Establish VPN tunnel with SecurID card to Partner and Supplier VLAN
	Supplier & Partner VLAN	FTP server in DMZ	989 (TCP)/FTPS-Data 990 (TCP)/FTPS	Transfer DB files via FTP over SSL
	Supplier & Partner VLAN	HTTPS server in Corp. LAN	443 (TCP)/HTTPS	Access to HTTPS Supplier and Partner web application

Internal Users	Office LANs	Internet	21 (TCP)/FTP 53 (UDP)/DNS 80 (TCP)/HTTP 443 (TCP)/HTTPS	Internet access for internal staff
	Office LANs	Corporate File and Print server	137 (UDP)/NetBIOS 138 (UDP)/NetBIOS 139 (TCP)/NetBIOS 445 (UDP)/MS DS 445 (TCP)MS DS	Access to File and Print servers for internals staff
	Office LANs	HTTPS server in Corp. LAN	443 (TCP)/HTTPS	Access to HTTPS corporate web application
	Office LANs	Exchange server in Corp. LAN	135 (TCP)/RPC	RPC access required for Exchange/Outlook access
Web Developers	Web Developer LAN	Internet	21 (TCP)/FTP 53 (UDP)/DNS 80 (TCP)/HTTP 443 (TCP)/HTTPS	Internet access
	Web Developer LAN	Corporate File and Print server	137 (UDP)/NetBIOS 138 (UDP)/NetBIOS 139 (TCP)/NetBIOS 445 (UDP)/MS DS 445 (TCP)MS DS	Access to File and Print servers
	Web Developer LAN	HTTPS server in Corp. LAN	443 (TCP)/HTTPS	Access to HTTPS corporate web application
	Web Developer LAN	Exchange server in Corp. LAN	135 (TCP)/RPC	RPC access required for Exchange/Outlook access
	Web Developer LAN	FTP server in DMZ	989 (TCP)/FTPS-Data 990 (TCP)/FTPS	Transfer DB files via FTP over SSL
Warehouse Users	Warehouse Wi-Fi LAN	HTTPS server on Corporate LAN	443 (TCP)/HTTPS	Access to HTTPS corporate web application
	Warehouse Wi-Fi LAN	HTTPS server on Corporate LAN	135 (TCP)/RPC	RPC access required for Exchange/Outlook access
Remote Users	Internet	External Firewall	500 (UDP)/IKE 50 (TCP)/ESP 51 (TCP)/AH	Establish VPN tunnel with SecurID card to Remote User VLAN
	Remote User VLAN	Internet	21 (TCP)/FTP 53 (UDP)/DNS 80 (TCP)/HTTP 443 (TCP)/HTTPS	Internet access
	Remote User VLAN	Corporate File and Print server	137 (UDP)/NetBIOS 138 (UDP)/NetBIOS 139 (TCP)/NetBIOS 445 (UDP)/MS DS 445 (TCP)MS DS	Access to File and Print servers

	Remote User VLAN	HTTPS server in Corp. LAN	443 (TCP)/HTTPS	Access to HTTPS corporate web application
	Remote User VLAN	Exchange server in Corp. LAN	135 (TCP)/RPC	RPC access required for Exchange/Outlook access
IT Support Staff	Internet	External Firewall	500 (UDP)/IKE 50 (TCP)/ESP 51 (TCP)/AH	Establish VPN tunnel with SecurID card to IT Support Staff VLAN
	IT Support Staff VLAN	Corporate Server LAN	3389 (TCP)/RDP	Terminal Server access to Corporate Server LAN
Public	Internet	HTTP server in Corp DMZ	80 (TCP)/HTTP	Public access to HTTP homepage

Network Infrastructure

The proposed design of the GIAC network is based on the principles of "Defense in Depth" – multiple layers of security working together to properly secure the network. The advantage of Defense in Depth is that no one server/device is responsible for the entire security of the network. Even if one device is bypassed, there are other lines of defense ready to protect against and log malicious activity.

The Defense in Depth principle is recommended and taught by the SysAdmin, Audit, Network, Security Institute known as SANS (http://www.sans.org). SANS is a highly respected security organization with members from educational, government, and corporate IT organizations worldwide.

1.0 Routers

The first line of defense at GIAC HQ and all remote offices will be a filtering router. GIAC will deploy (5) Cisco 1721 Routers running Cisco IOS 12.3. These routers come standard with (1) ethernet port and (2) expansion WIC ports.

The routers will apply static ingress and egress filtering rules. All recommended filtering rules are from SANS Institute training [10] [11].

1.1 EXT_Router

The Cogent Communications internet connection at the GIAC HQ is supplied via ethernet, so the HQ router will be configured with a Cisco WIC-4ESW 4-Port Fast Ethernet Switch WAN Interface Card.

To start we will create a new extended access list and apply ingress filtering to block private IP address ranges from entering the network.

```
interface eth0/0
ip address 200.1.1.1 255.255.255.240
ip access-group 10 in
access-list 10 deny ip 10.0.0.0 0.255.255.255 any
access-list 10 deny ip 172.16.0.0 0.15.255.255 any
access-list 10 deny ip 192.168.0.0 0.0.255.255 any
```

Next we will block and log multicast networks, the loopback adapter, and our own ISP provided address space.

```
access-list 10 deny ip 224.0.0.0 31.255.255.255 any log
access-list 10 deny ip 127.0.0.1 0.255.255.255 any log
access-list 10 deny ip 200.1.1.0 0.0.0.14 any log
```

Next, we will filter out the SANS.org Top 10 Threats.

```
access-list 10 deny tcp any any range 135 139
access-list 10 deny udp any any range 135 139
access-list 10 deny tcp any any 445
access-list 10 deny tcp any any range 6000 6255 log
access-list 10 deny udp any any 69 log
access-list 10 deny udp any any 514 log
access-list 10 deny udp any any range 161 162 log
access-list 10 deny icmp any any host-redirect echo
```

Next, since we will have a firewall (and IDS) behind the router to log and block traffic we need to add a “permit any” rule on this interface because otherwise the router defaults to a “deny any” rule.

```
access-list 10 permit any any
exit
```

Finally, since there is only 1 interface (because we are using the switching features of the router) we will create another extended access list and apply it outbound. We can apply egress filtering on it by allowing only our ISP’s assigned address space out. Anything else is spoofed or mis-configured NAT. The –input switch on our drop rule adds the layer 2 (MAC address) information to the logs.

```
interface eth0/0
ip access-group 20 out
access-list 20 deny tcp any any range 135 139
access-list 20 deny udp any any range 135 139
access-list 20 deny tcp any any 445
access-list 20 deny tcp any any range 6000 6255 log
access-list 20 deny udp any any 69 log
access-list 20 deny udp any any 514 log
access-list 20 deny udp any any range 161 162 log
access-list 20 deny icmp any any echo-reply unreachable
access-list 20 permit 200.1.1.0 0.0.0.14
access-list 20 deny any log-input
exit
```

1.2 SAT#_Router

The remote offices will have a T1 connection and a Cisco WIC-1DSU-T1-V2 1-Port T1/Fractional T1 DSU/CSU WAN Interface Card installed into each router. The routers will be very similarly configured to the HQ router. The notation w.x.y.z represents the external ethernet address provided by each office’s ISP.

It is not detailed here, but another option to lock down the SAT_Routers would

be to allow only IPSEC VPN traffic from the corporate EXT_Firewall. This is because all remote office traffic will be sent over the VPN connection. The downside to this configuration is that the router logs would need to be reviewed for suspicious activity instead of the firewall logs, which is why we did not implement this.

```
interface ser0/0
ip access-group 10 in
access-list 10 deny ip 10.0.0.0 0.255.255.255 any
access-list 10 deny ip 172.16.0.0 0.15.255.255 any
access-list 10 deny ip 192.168.0.0 0.0.255.255 any
access-list 10 deny ip 224.0.0.0 31.255.255.255 any log
access-list 10 deny ip 127.0.0.1 0.255.255.255 any log
access-list 10 deny ip w.x.y.z 0.0.0.2 any log
access-list 10 deny tcp any any range 135 139
access-list 10 deny udp any any range 135 139
access-list 10 deny tcp any any 445
access-list 10 deny tcp any any range 6000 6255 log
access-list 10 deny udp any any 69 log
access-list 10 deny udp any any 514 log
access-list 10 deny udp any any range 161 162 log
access-list 10 deny icmp any any host-redirect echo
Access-list 10 permit any
Exit
```

```
Interface eth1/0
ip address w.x.y.z 255.255.255.252
ip access-group 20 in
access-list 10 deny tcp any any range 135 139
access-list 10 deny udp any any range 135 139
access-list 10 deny tcp any any 445
access-list 10 deny tcp any any range 6000 6255 log
access-list 10 deny udp any any 69 log
access-list 10 deny udp any any 514 log
access-list 10 deny udp any any range 161 162 log
access-list 10 deny icmp any any host-redirect echo
access-list 20 permit w.x.y.z 0.0.0.2
access-list 20 deny any log -input
exit
```

2.0 Firewalls

The next line of defense will be stateful inspection firewalls. GIAC will deploy (2) Nokia IPSO 380 firewalls at their HQ location, one internally, one externally. (4) Nokia IPSO 265 firewalls will be deployed across the remote offices. Finally, (1) Nokia IPSO 265 firewall will deployed between the warehouse wireless network and the corporate LAN. Each firewall will be running Checkpoint Firewall NG R55. A Checkpoint management station will be installed in the IT Administration LAN to establish the rulebase and push the firewall policies out.

This section is a summary of the network and hardware configuration of each firewall. Specific firewall policies will be provided in Assignment 3.

2.1 EXT_Firewall

The GIAC external firewall will be placed behind the external router at the corporate HQ. This firewall will be connected to three physical networks: the

external ISP, the internal DMZ, and the internal corporate. Taking advantages of Checkpoint's VPN1 features, this firewall will also act as a VPN end-point for remote offices, end users, suppliers, and business partners.

End users, suppliers, and business partners will connect via Checkpoint's SecureClient application and authenticate using SecurID cards. The external firewall will then provide DHCP IP addressing for these clients and connect them to 1 of 3 Virtual LAN's (VLAN). Each VLAN will have different access rights depending on the group using it. There will be a VLAN for remote users, one for Suppliers and Partners, and one for the IT Support Staff (for remote administration).

2.2 INT_Firewall

The GIAC internal firewall will be hooked up to a switch behind the external firewall. This firewall will not have any direct external connections, but will be connected to 5 internal GIAC subnets. With (4) ethernet ports standard on the Nokia IPSO 380 we will need to purchase a (2) NIC expansion card for the INT_Firewall. Then it will be hooked up to the corporate server LAN, the web development LAN, the Albany HQ office LAN, the warehouse wireless LAN, and the IT Administration LAN.

2.3 SAT#_Firewall

Each remote office will have it's own firewall behind the external router. This firewall will protect the remote office and also establish a site-to-site VPN connection to the corporate HQ. All traffic (including internet) will travel across this VPN link where it will then be properly routed – out to the internet or into the corporate network.

3.0 VPN/Encryption

For security, GIAC will employ encryption technology wherever possible to secure the company's data. Taking advantage of the IPSEC VPN features of Checkpoint Firewall, all traffic from the remote offices will be encrypted and sent to the corporate HQ for proper routing via a site-to-site VPN connection. Additionally, remote users connecting from home or the road will first establish a VPN tunnel using Checkpoint SecureClient. The same arrangements will be made for the IT Support Staff (remote administration) and GIAC partners and suppliers.

Where a VPN is not appropriate, GIAC will make extensive use of SSL encryption to secure its web applications. The two internal corporate webservers (one for internal users, one for partners and suppliers) will both use SSL encryption to protect data. As will two of the external corporate webservers (one for customers, one for employee email access). The only webserver not using SSL encryption will the company's informational-only public website.

GIAC will also use SSL encryption to secure FTP data transfers. This is

extremely important, as these will be text-only database files with potentially confidential information.

4.0 Web Filtering

GIAC will deploy Surf Control Superscout 4.1 (http://www.surfcontrol.com), a commercial application that integrates with Checkpoint Firewall to block inappropriate websites as determined by management. User accessing inappropriate websites will be redirected to an internal webpage reminding them of GIAC's Internet Acceptable Usage policies.

A separate Surf Control server will be installed on the switch between the external and internal firewalls. It is important to locate this server as close to the firewall as possible for categorization look-ups (although the firewall does cache categorization details for a user-configurable amount of time).

5.0 Intrusion Detection System

The final piece of our Defense in Depth design for GIAC is an Intrusion Detection System (IDS). Routers and firewalls are excellent at applying and enforcing a static set of rules, but what if malicious traffic matches one of the rules? Case in point – we are allowing HTTPS access from the public internet to the customer web application in the DMZ. If a hacker was to attempt an IIS exploit against this webserver, the router and firewall would both allow the traffic through.

Another vulnerable situation is a worm or Trojan program trying to spread itself within one of GIAC's office subnets. As long as this attack stayed within it's own subnet, there would be no router or firewall in place to block it.

With an IDS in the proper location, attack signatures for various exploits can be programmed in and administrators can be alerted to potentially malicious traffic. A shortcoming of IDS is that it only detects malicious traffic it does not stop them. GIAC could consider an Intrusion Prevention System if the situation warranted it. These devices add the ability to stop the traffic that matches its signature patterns.

For GIAC's IDS deployment, we will deploy (6) Linux servers running the free SNORT IDS (http://snort.sourcefire.com) application. One of these servers will be placed on each LAN at the corporate HQ – DMZ LAN, Corporate Server LAN, Web Development LAN, Albany office LAN, Wireless LAN, and one between the external and internal firewall. All of these servers will be physically connected to the IT Administration LAN, along with a MYSQL Database server to consolidate all the logging. They will all have a second network card installed, without an IP address configured, and connected to the switch of the network it is monitoring. The switch will then be configured for port-spanning on that particular port the IDS is hooked up to. This allows the IDS to be transparent – it sees all the LAN traffic, but the server is invisible to the LAN it is monitoring.

Additional Recommendations

Once the new GIAC LAN is installed and configured, there are several security-related initiatives that should be performed to confirm the network is configured properly. There are also some recommendations for additional layers of defense.

- Port Scanning – each LAN should be port scanned from every other LAN to ensure only the proper and necessary services are running.
- SNORT – SNORT is not exactly "plug and play". GIAC will need to add/remove/edit some SNORT alerts to reduce the number of false positives generated.
- Penetration Testing – the corporate DMZ should be tested from the public internet. This test can also be applied to the router and firewall at each remote office.
- Spam/Virus Filtering – to reduce the amount of spam, and add an extra layer of Anti-Virus security, GIAC should consider a Spam/Virus Filtering software application on the external SMTP server. Another option would be to contract with a Spam/Virus service provider like Frontbridge Communications (http://www.frontbridge.com) to do the same. The advantage of using a service provider is that you can then limit incoming SMTP connections to just the providers' SMTP servers (instead of the public internet).
- IPS – GIAC should consider upgrading to an Intrusion Prevention System – especially for the external facing servers.

Assignment 3

Firewall Policy for GIAC Enterprises

Firewalls

Following is a list of the Firewall Objects in the Checkpoint Firewall Dashboard.

Name	Ext. IP Address	Int. IP Address	Description
EXT_FW	200.1.1.2	10.1.1.1	External firewall
INT_FW	10.1.1.2		Internal firewall
LAX_FW	w.x.y.z	10.30.1.1	LAX office firewall
LON_FW	w.x.y.z	10.40.1.1	LON office firewall
SEO_FW	w.x.y.z	10.50.1.1	SEO office firewall
SYD_FW	w.x.y.z	10.60.1.1	SYD office firewall

Networks

Following is a list of the Network Objects that need to be created in the Checkpoint Firewall Dashboard.

Name	IP Address	Description
NET_DMZ	192.168.0.1/24	DMZ LAN
NET_INT	10.1.1.1/16	Internal network between firewalls
NET_IT	10.2.1.1/16	IT Admin LAN
NET_CORP	10.3.1.1/16	Corporate Server LAN
NET_DEV	10.4.1.1/16	Web Development LAN
NET_WIFI	10.5.1.1/16	Warehouse wireless LAN
VLAN_REMOTE	10.7.1.1/16	Remote GIAC user VLAN

VLAN_PART_SUPP	10.8.1.1/16	Partner and Supplier VLAN
VLAN_IT_REMOTE	10.9.1.1/16	Remote GIAC IT Admin VLAN
NET_ALB	10.20.1.1/16	Albany, NY – Corporate HQ LAN
NET_LAX	10.30.1.1/16	Los Angeles, CA – Remote Office LAN
NET_LON	10.40.1.1/16	London, England – Remote Office LAN
NET_SEO	10.50.1.1/16	Seoul, South Korea – Remote Office LAN
NET_SYD	10.60.1.1/16	Sydney, Australia – Remote Office LAN

Servers (Hosts)

Following is a list of the Host Objects that need to be created in the Checkpoint Firewall Dashboard.

Name	IP Address	NAT Address	Description
IIS_HTTP_PUBLIC	192.168.1.2	200.1.1.4	Public HTTP server in DMZ
IIS_HTTPS_CUST	192.168.1.3	200.1.1.5	Customer HTTPS server in DMZ (password protected)
IIS_HTTPS_EMAIL	192.168.1.4	200.1.1.6	Employee HTTPS server in DMZ (password protected)
IIS_SMTP	192.168.1.5	200.1.1.7	Public SMTP server in DMZ
FTP_DMZ	192.168.1.6		External FTP server in DMZ
SURF_CONT	10.1.1.3		Surf Control server in between firewalls
FW_MGMT	10.2.2.3		Checkpoint Firewall management station in IT Admin LAN
FTP_IT	10.2.2.4		Internal FTP server in IT Admin LAN
FILE_PRINT_CORP	10.3.2.2		Corporate File and Print server in Corp. Server LAN
BACKUP	10.3.2.3		Backup server
EXCHANGE	10.3.2.4		MS Exchange Server
IIS_HTTPS_CORP	10.3.2.5		Corporate HTTPS server in Corp. Server LAN
IIS_HTTPS_PART_SUPP	10.3.2.6		Partner and Supplier HTTPS server in Corp. Server LAN
SEC_ID_RADIUS	10.3.2.8		RSA Security SecurID Appliance
802.1X_RADIUS	10.3.2.9		802.1x Authentication and Encryption server for Wireless LAN
WIN_UPDATE	10.3.2.10		Internal Windows Update server
IIS_HTTPS_DEV	10.4.2.3		Development HTTPS server in Web Development LAN
FTP_DEV	10.4.2.5		Development FTP server in Web Development LAN

Rulebase

Following is a list of the rules that need to be created in the Checkpoint Firewall Dashboard.

Our first set of rules handles our external servers in the DMZ. We have (1) HTTP server, (2) HTTPS servers, and (1) SMTP server. We also need to permit the Web Developers access to the FTP_DMZ server. We can then deny all other DMZ traffic.

#	Source	Destination	Service	Action	Track

1	ANY	IIS_HTTP_PUBLIC	HTTP	Accept	Log
2	ANY	IIS_HTTPS_CUST	HTTPS	Accept	Log
3	ANY	IIS_HTTPS_EMAIL	HTTPS	Accept	Log
4	ANY	IIS_SMTP	SMTP	Accept	Log
5	NET_DEV	FTP_DMZ	FTPS	Accept	Log
6	ANY	NET_DMZ	ANY	Deny	Log

Next, we setup the remote office VPN. First we allow IPSEC traffic, and then we create rules to encrypt traffic between offices. We also need a deny rule here to stop all other traffic from the remote offices.

#	Source	Destination	Service	Action	Track
7	Any	EXT_FW	ESP AH IKE	Accept	Log
8	EXT_FW	Any	ESP AH IKE	Accept	Log
9	NET_LAX NET_LON NET_SEO NET_SYD	FILE_PRINT_CORP	NET_BIOS MS_DS	Encrypt	Log
10	NET_LAX NET_LON NET_SEO NET_SYD	EXCHANGE	RPC	Encrypt	Log
11	NET_LAX NET_LON NET_SEO NET_SYD	IIS_HTTPS_CORP	HTTPS	Encrypt	Log
12	NET_LAX NET_LON NET_SEO NET_SYD	WIN_UPDATE	HTTP	Encrypt	Log
13	NET_LAX NET_LON NET_SEO NET_SYD	NET_IT NET_CORP NET_DEV NET_WIFI	ANY	Deny	Log

Next, we need similar rules for the Albany Corporate HQ LAN, the Web Development LAN, the Remote User VLAN and the Warehouse Wireless LAN without any encryption. The Web Developers need a couple of extra access rules to/from the FTP_DMZ server. At this point, we can then deny all other traffic to the Web Developer LAN.

#	Source	Destination	Service	Action	Track
13	NET_ALB NET_DEV VLAN_REMOTE	FILE_PRINT_CORP	NET_BIOS MS_DS	Accept	Log
14	NET_ALB NET_DEV NET_WIFI VLAN_REMOTE	EXCHANGE	RPC	Accept	Log
15	NET_ALB NET_DEV NET_WIFI VLAN_REMOTE	IIS_HTTPS_CORP	HTTPS	Accept	Log

16	NET_ALB NET_DEV NET_WIFI VLAN_REMOTE	WIN_UPDATE	HTTP	Accept	Log
17	FTP_DEV	FTP_DMZ	FTPS	Accept	Log
18	FTP_DMZ	FTP_DEV	FTPS	Accept	Log
20	ANY	NET_DEV	ANY	Deny	Log

Next, we give everyone internet access. This is accomplished by created a "URI resource" in Checkpoint Firewall for the Surf Control server. In this URI Resource we will check off which categories we want to block (i.e. porn, gambling, etc.). We then create a deny rule for those resources, followed by an accept rule for all other internet traffic.

#	Source	Destination	Service	Action	Track
21	NET_WEB NET_ALB NET_LAX NET_LON NET_SEO NET_SYD VLAN_REMOTE	ANY	BLOCKED_SC (Chkpt. Resource)	Deny	Log
22	NET_WEB NET_ALB NET_LAX NET_LON NET_SEO NET_SYD VLAN_REMOTE	ANY	DNS HTTP HTTPS FTP	Accept	Log

Next, backup jobs. GIAC will be using Veritas Backup Exec 9.1 for backups (http://www.veritas.com). The backup server will be located on NET_CORP, per the Veritas Knowledge Base we need to open ports 10000 and 1024-1031.

#	Source	Destination	Service	Action	Track
23	BACKUP	ANY	10000 1024-1031	Accept	Log
24	ANY	BACKUP	10000 1024-1031	Accept	Log

Next, we setup access for the other VLANs and then deny all other traffic from them.

#	Source	Destination	Service	Action	Track
25	VLAN_PART_SUPP	IIS_HTTPS_PART_SUPP	HTTPS	Accept	Log
26	VLAN_PART_SUPP	FTP_DMZ	FTPS	Accept	Log
27	VLAN_IT_REMOTE	NET_CORP	RDP	Accept	Log
28	VLAN_IT_REMOTE VLAN_PART_SUPP	ANY	ANY	Deny	Log

Next we need rules for our RADIUS servers. One for authenticating remote users, partners and suppliers at the firewall, and another for authenticating wireless LAN clients. RADIUS ports are 1812 and 1813.

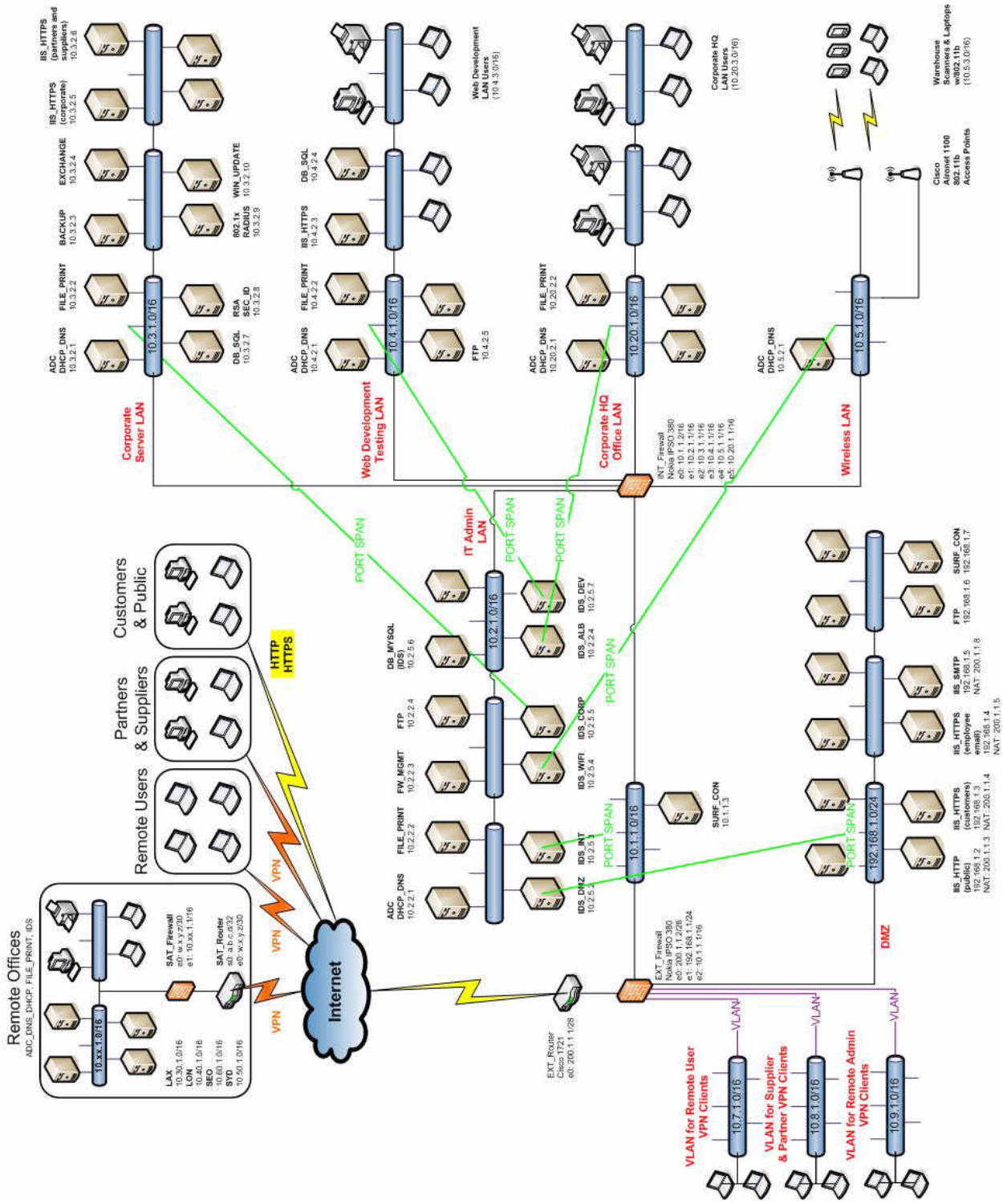
#	Source	Destination	Service	Action	Track
29	FW_EXT	SEC_ID_RADIUS	RADIUS	Accept	Log
30	LAN_WIFI	802.1X_RADIUS	RADIUS	Accept	Log

Finally, we need to allow Checkpoint Firewall Management ports (TCP 256, 257, 18191 and 18192) from our management station to our firewalls. After that, we finalize our rulebase with a drop rule for all other traffic.

#	Source	Destination	Service	Action	Track
31	FW_MGMT	FW_EXT FW_INT	CKPT MGMT	Accept	Log
32	FW_MGMT	FW_LAX FW_LON FW_SEO FW_SYD	CKPT MGMT	Encrypt	Log
33	Any	Any	ANY	Deny	Log

APPENDIX

A. Network Diagram



B. References

(1) Wikipedia.com. “IEEE 802.11.”
http://en.wikipedia.org/wiki/IEEE_802.11
(2) Mannion, Patrick. “Intern proves WLAN encryption protocol vulnerable.” EETimes.com 8 Aug 2001
http://www.eetimes.com/story/OEG20010808S0042
(3) Shim, Richard. “802.11g is approved, 802.11n is next in line.”
CNET News.com 13 Jun 2003
http://news.zdnet.co.uk/communications/networks/0,39020345,2136013,00.htm
(4) Mitchell, Dave. “Belkin Wireless Pre-N Router.”
Trusted Reviews.com 7 March 2005
http://www.trustedreviews.com/article.aspx?art=1124
(5) Wikipedia.com. “War Driving.”
http://en.wikipedia.org/wiki/War_driving
(6) Cisco.com. “Wi-Fi Protected Access, WPA2, and 802.11i.”
http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/netqa0900aecd801e3e59.html
(7) Wikipedia.com. “Wired Equivalent Privacy.”
http://en.wikipedia.org/wiki/WEP
(8) Wikipedia.com. “Wi-Fi Protected Access.”
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
(9) Wikipedia.com. “802.11i.”
http://en.wikipedia.org/wiki/WPA2
(10) SANS.org. “2.2 Packet Filters.” 2004
(11) SANS.org. “2.6 Network Design and Assessment.” 2004

Checkpoint Management Ports
http://www.secinf.net/firewalls_and_VPN/The_Firewall_Hardening_Guide/The_Firewall_Hardening_Guide_v01__Checkpoint_Firewall1_Specific_Requirements__Implicit_Rules_Rule_Zero_rules.html

Cisco 1700 4-port switch configuration info
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1700cnts/1711swm.htm

File and Print Sharing Ports
http://ecross.mvps.org/howto/icf.htm

IPSec VPN Ports
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod111.asp

Veritas Backup Exec Ports
http://seer.support.veritas.com/docs/255174.htm

C. Product information

Cisco 1721 Router
http://www.cisco.com/en/US/products/hw/routers/ps221/index.html

Cisco Aironet 1100
http://www.cisco.com/en/US/products/hw/wireless/ps4570/index.html

Cogent Communications
http://www.cogentco.com/

IBM R52 Laptop
http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?catalogId=-840&productId=8745971&storeId=1&langId=-1&dualCurrId=73&categoryId=2302836

IBM xSeries 306 Server
http://www-132.ibm.com/webapp/wcs/stores/servlet/CategoryDisplay?catalogId=-840&storeId=1&langId=-1&dualCurrId=73&categoryId=2588410

Nokia IP380 Firewall
http://www.nokia.com/BaseProject/Sites/NOKIA_MAIN_18022/CDA/Categories/Business/LargeBusiness/NetworkSecurity/IPSecurityPlatforms/Enterprises&ServiceProviders/_Content/_Static_Files/sec_nokia_ip380_datasheetna.pdf

Nokia IP265 Firewall
http://www.nokia.com/BaseProject/Sites/NOKIA_MAIN_18022/CDA/Categories/Business/NetworkSecurity/IPSecurityPlatforms/DistributedEnterprises/_Content/_Static_Files/nokiaip260-ip265_datasheet_emea.pdf

RSA Security SecurID Appliance
http://www.rsasecurity.com/products/securid/datasheets/APPL_DS_0205.pdf

Symbol MC50 Handheld Scanner
http://www.symbol.com/products/mobile_computers/mc50.html

Veritas Backup Exec 9.1
http://www.veritas.com/Products/www?c=product&refId=57

D. Budget

Item		Qty	Price	Total		
Networking						
	Cisco 1721 Router	5	$800	**$4,000**		
	Expansion Card: WAN	4	$700	**$2,800**		
	Expansion Card: 4port Eth	1	$300	**$300**		
	Cisco 2950 Switch	10	$600	**$6,000**		
					$13,100	
Firewall/VPN						
	Nokia IP380	2	$8,000	**$16,000**		
	Expansion Card: 2port Eth	1	$1,000	**$1,000**		
	Nokia IP265	4	$1,600	**$6,400**		
	RSA Security SecurID Appliance	1	$4,500	**$4,500**		
					$27,900	
Servers						
	IBM xSeries 306	10	$2,000	**$20,000**		(6) IDS servers, (1) MYSQL server for IDS, (1) Surf Control server, (1) 802.1x server
	1GB RAM	10	$700	**$7,000**		
					$27,000	
Wireless						
	Cisco Aironet 1100 Access Point	5	$600	**$3,000**		*qty estimated
	IBM R52 Laptop	5	$1,500	**$7,500**		*qty estimated
	Symbol MC50 Handheld Scanners	10	$1,000	**$10,000**		*qty estimated
					$20,500	
TOTAL					**$88,500**	