Global Information Assurance Certification Paper

GCFW Practical

Richard Park

GCFW Practical
Version 4.0

Date: November 26, 2004

Table of Contents

List of Figures

Abstract

GIAC Enterprises is a small company that makes fortune cookies worldwide. GIAC currently employees 50 people with the majority located near its head office and the remainder located near the 4 regional offices around the world.

This document discusses:

- The integration of wireless technology into GIAC Enterprises network and the associated security risks.
- The network security architecture for GIAC Enterprises.
- The rulebase for GIAC Enterprises primary firewall.

Assignment 1- Future State of Security Technology: Wireless Network Integration

Background / Introduction

GIAC Enterprises has built a warehouse to manufacture and ship fortune cookies. The warehouse will use handheld scanners in the shipping process and wireless laptops on the warehouse floor[1].

The warehouse business operations must be integrated into GIAC Enterprises exiting network architecture as defined in assignments 2 and 3.

This document discusses the integration of wireless technology into GIAC Enterprises network. Included in the discussion are the security risks of wireless technology and how these risks can be mitigated.

Problem Domain

The problem that needs to be resolved is the integration of handheld scanners and wireless laptops into GIAC Enterprises existing network architecture. This integration should be secure and security risks should be mitigated.

Addressing the Problem Domain

Access Devices
The Cisco Aironet 350 wireless card installed on a laptop and the Intermec CK30 handheld scanner will be the two types of wireless devices that will connect to the wireless access point. The wireless access point will be a Cisco Aironet 1200 Series 802.11g Access Point.

The Cisco Aironet 350 wireless card and the Intermec CK30 handheld scanner support 802.11g. 802.11g is a wireless LAN specification developed by IEEE. 802.11g provides 20 plus Mbps in the 2.4 GHz band.

The following diagram illustrates the wireless LAN for GIAC Enterprises:

[1] GIAC

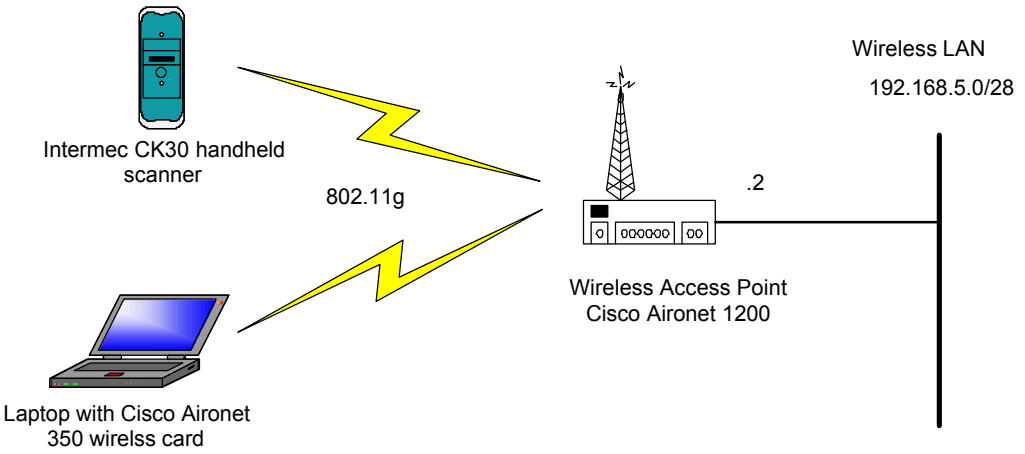

Figure 1: Wireless Access

Wireless Security Today

Wireless networks cannot be physically secured like wired networks. They can be attacked from inside and outside of the physical security of the warehouse. Deploying a wireless network would make it easy for anyone to eavesdrop on the wireless LAN and collect all packets sent over the wireless network.

Due to the ease of eavesdropping on a wireless LAN, security must be enabled. We must be able to provide authentication, integrity and privacy. Authentication is required to allow access to those devices that should have access and deny access to those devices that should not have access to the wireless LAN. Integrity is required to ensure that the packets have not been altered. Privacy is required to prevent eavesdropping.

There are several security standards that are offered on wireless devices today. They are WEP, WPA and WPA2 (802.11i).

WEP stands for Wired Equivalent Privacy and is part of the 802.11 standard. WEP is used to prevent eavesdropping. WEP creates a seed by concatenating the shared secret key with a randomly generated 24 bit IV (initialization vector)[2]. The seed is used to produce a keystream equal to the length of the frame's payload plus the 32 bit ICV (integrity check value). This keystream is used to encrypt the frame. On a busy network, transmission of packets with similar keystreams can be captured. By capturing enough packets of the same IV, one can determine the keystream. Once the keystream is determined, all 802.11 packets can be decrypted.

WPA stands for Wi-Fi Protected Access and is a subset of the IEEE 802.11i security standard. WPA is the intermediate step from WEP to WPA2 (802.11i). WPA addresses some of the vulnerabilities of WEP. WPA has two major security components:

[2] InteropNet Labs

- 802.1x authentication
- TKIP encryption

802.1x authentication is based on the EAP (Extensible Authentication Protocol, IETF RFC 2284). 802.1x includes a range of EAP authentication methods like LEAP and PEAP. PEAP stands for Protected Extensible Authentication Protocol. PEAP is an IETF Internet-draft submitted by Cisco Systems, Microsoft and RSA Security.

TKIP (Temporal Key Integrity Protocol) allows for the changing of keys on a frame by frame basis. TKIP solves some of the issues with WEP. However, TKIP still uses RC4 and is still susceptible to weak key scheduling algorithm as discussed in Fluhrer, Mantin, and Shamir's paper entitled "Weaknesses in the Key Scheduling Algorithm of RC4".

WPA2 (802.11i) is an IEEE security standard that uses AES to address the weak key issuing algorithm of RC4. WPA2 supported devices are just starting to come into the market place.

Mitigation Strategy

In order to reduce the security risks associated with wireless networks, the following Defense-In-Depth strategies were placed on the wireless network for GIAC Enterprises.

Wireless Security
Since WPA2 (802.11i) is not widely available today, WPA will be used to secure the packets on the wireless LAN at GIAC Enterprises. Specifically, PEAP authentication and TKIP encryption will be deployed on GIAC's wireless network.
Since PEAP requires a Radius server, Cisco Secure Access Control System version 2.3 for UNIX will be deployed to authenticate PEAP requests.

The following network diagram identifies the wireless and wired network for GIAC Enterprises head office:

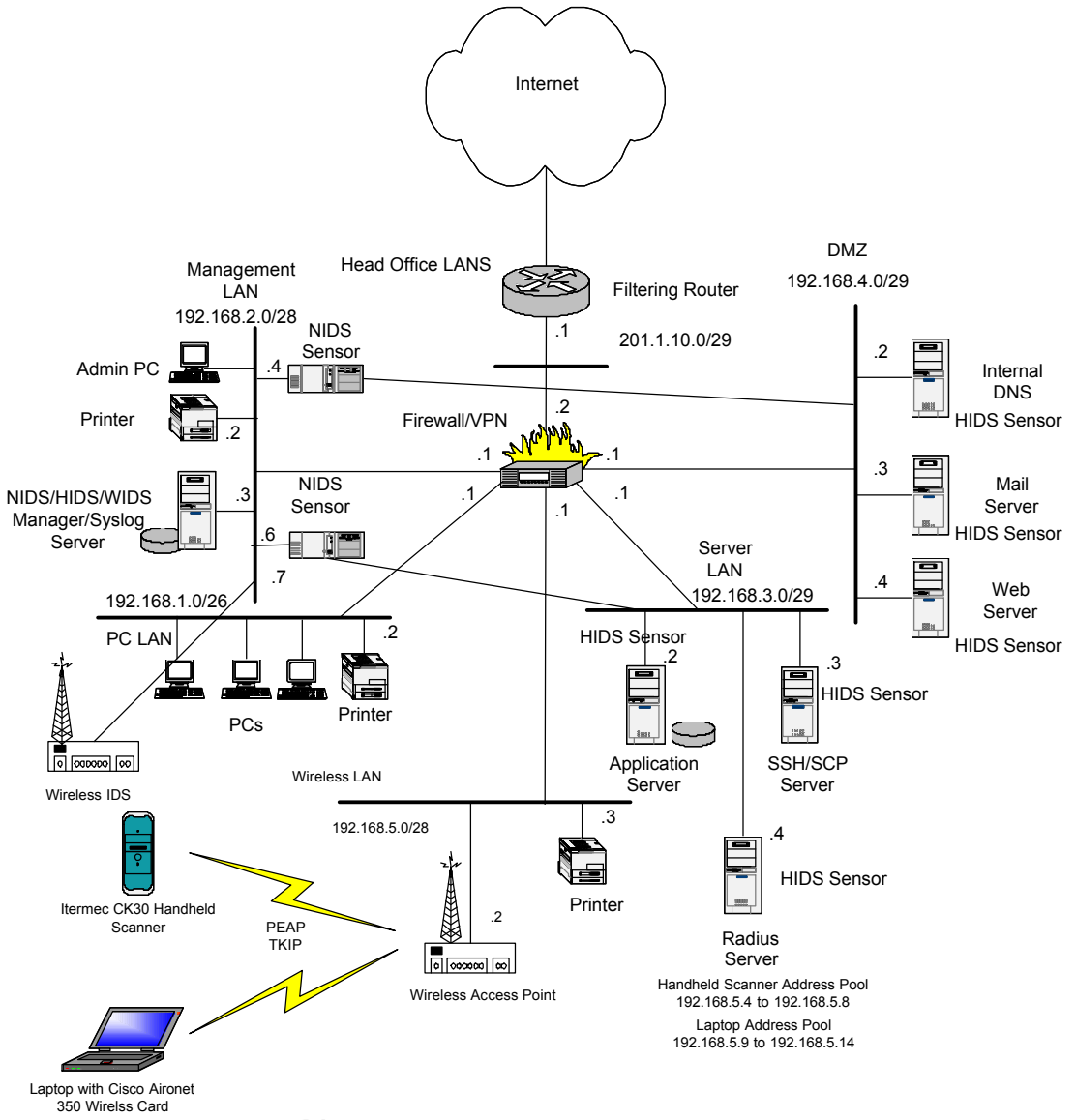

Figure 2: GIAC Enterprise Wireless and Wired Network

Authentication will be required to get onto the wireless network. The handheld scanners and laptops will use PEAP to authenticate to the wireless network. The username and password entered on the wireless device with be forwarded by the wireless access point to the Radius server. The Radius server will verify the username and password. Upon successful authentication, an IP address will be assigned from the Radius server to the wireless access point. The wireless access point will forward the assigned IP address to the wireless device. There will be separate IP address pools for handheld devices and laptops. This is required since there will be different access policies for handhelds and laptops.

Password Locking and Expiration
In order to reduce the risk of password cracking from brute force, wireless access password locking and expiration will be used on the Radius server. Passwords will be locked after 3 consecutive failed attempts and passwords will expire after 30 days.

Separate Wireless LAN Zone
The wireless LAN will be separated from the wired LANs at GIAC Enterprises head office. The wireless LAN will be connected to the existing firewall at the head office. By incorporating the firewall, we will be able to apply rules to meet our access requirements for the handheld scanners and laptops. The subnet 192.168.5.0/28 will be the WLAN zone. The handheld scanners will be assigned an IP address from 192.168.5.4 to 192.168.5.8 and the laptops will be assigned an IP address from 192.168.5.9 to 192.168.5.14.

The handheld scanners will have access to the DNS and web servers in the DMZ. The laptops will have access to all the servers in the Server LAN and DMZ. The laptops will have access to the Internet.

For the firewall at the head office, the following are the access rules that are required to allow access to the devices on the wireless LAN. These rules would be appended to the rulebase given in assignment 3.

ID	Src Zone	Src IP	Dst Zone	Dst IP	Service	Action	Options
39	WLAN	192.168.5.3/32	ServerLAN	Any	any	deny	log
40	WLAN	192.168.5.3/32	PCLAN	Any	any	deny	log
41	WLAN	192.168.5.3/32	DMZ	Any	any	deny	log
42	WLAN	192.168.5.3/32	Untrust	Any	any	deny	log
43	WLAN	192.168.5.2/32	ServerLAN	192.168.3.4/32	udp ports 1645, 1646	accept	
44	WLAN	192.168.5.9/32 192.168.5.10/32 192.168.5.11/32 192.168.5.12/32 192.168.5.13/32 192.168.5.14/32	ServerLAN	192.168.3.2/32	http, https, sql*netv2	accept	
45	WLAN	192.168.5.9/32 192.168.5.10/32 192.168.5.11/32 192.168.5.12/32 192.168.5.13/32 192.168.5.14/32	ServerLAN	192.168.3.3/32	ssh	accept	
46	WLAN	192.168.5.9/32 192.168.5.10/32 192.168.5.11/32 192.168.5.12/32 192.168.5.13/32 192.168.5.14/32	DMZ	192.168.4.2/32	dns	accept	
47	WLAN	192.168.5.9/32 192.168.5.10/32 192.168.5.11/32 192.168.5.12/32 192.168.5.13/32 192.168.5.14/32	DMZ	192.168.4.3/32 192.168.4.4/32	http, https	accept	

48	WLAN	192.168.5.9/32 192.168.5.10/32 192.168.5.11/32 192.168.5.12/32 192.168.5.13/32 192.168.5.14/32	Untrust	Any	http, https	accept	NAT src
49	WLAN	192.168.5.4/32 192.168.5.5/32 192.168.5.6/32 192.168.5.7/32 192.168.5.8/32	DMZ	192.168.4.2/32	dns	accept	
50	WLAN	192.168.5.4/32 192.168.5.5/32 192.168.5.6/32 192.168.5.7/32 192.168.5.8/32	DMZ	192.168.4.4/32	http, https	accept	

Rules 39 to 42 are required to deny any packets from the printer on the wireless LAN to pass through the firewall.

Rule 43 is required to allow the wireless access point to send Radius requests to the Radius server.

Rules 44 to 48 are required to allow the laptops to have access to the Internet, the ServerLAN and the DMZ.

Rules 49 and 50 are required to allow the handhelds to have access to the DNS and web server.

NIDS
We can mitigate some of the security risks associated with the wireless network by using the NIDS (described in assignment 2) to detect and alert us of attacks taking place on the Server and DMZ LANs. We can configure the NIDS to identify if these attacks are originating from the wireless LAN.

HIDS
We can use the HIDS (described in assignment 2) to identify and alert us of unknown attacks. By using the HIDS as an IPS, we can prevent attacks on our servers.

Wireless IDS (WIDS)
We can use Wireless IDS to detect attacks on the wireless network. Wireless intrusion detections systems like AirDefense and the planned Snort-Wireless are intrusion detection systems designed to detect attacks specific to 802.11 networks. Wireless intrusion detection systems will be able to detect attacks like bogus access points, detect NetStumbler and adhoc networks.

Impact on Perimeter Security

By deploying wireless networks, the existing perimeter security of your network can be degraded. In fact, the existing perimeter security may be non-existent due to the deployment of the wireless network. Your wired network may now be susceptible to attacks originating from the wireless networks.

Perimeter security must include the securing of wireless networks. A Defense-In-Depth approach to securing wireless networks must be used. Securing wireless networks can be achieved by enabling authentication and encryption protocols specific to 802.11 networks like WPA and WPA2 (802.11i).

Your existing network can be secured by deploying a firewall between the wireless and wired networks. Firewall rules can be used to enforce the access policy to and from the wireless network.

The security weaknesses of wireless networks can be also be mitigated by deploying different intrusion detection systems like NIDS and HIDs on the wired networks. In addition, wireless IDS should be deployed on the wireless network.

To secure you network, perimeter security must include the securing of both wireless and wired networks.

Assignment 2 - Security Architecture

GIAC Enterprises markets fortune cookie sayings worldwide. GIAC Enterprises currently employees 50 people with the majority located near its head office and the remainder located near the 4 regional offices[3].

The following document defines the network security architecture for GIAC Enterprises.

Access Requirements

The following section identifies the access requirements for each type of user who requires network access into or out of GIAC Enterprises. The assumption is made that customers, suppliers, partners and the general public have email and phone access.

Customers

Companies or individuals that purchase bulk online fortunes will require http (tcp port 80) and https (tcp port 443) access into the web server. These customers will not be allowed to enter GIAC Enterprises network with a protocol other than http and https. Also, access is restricted to the web server only. No restriction will be placed on the source IP address since we expect to have many customers from all over the world.

Suppliers

GIAC Enterprises will require http (tcp port 80) and https (tcp port 443) access into the Companies that supply fortune cookie sayings. Suppliers will require http (tcp port 80) and https (tcp port 443) access into the web server. These suppliers will not be allowed to enter GIAC Enterprises network with a protocol other than http and https. Also, access is restricted to the web server only. No restriction will be placed on the supplier's source IP address since we expect to have many suppliers from all over the world.

Partners

International companies that translate and resell fortunes will have http (tcp port 80) and https (tcp port 443) access into the web server. Partners will not be allowed to enter GIAC Enterprises network with a protocol other than http and https. Also, access is restricted to the web server only. No restriction will be placed on the source IP address since we expect to have many partners.

GIAC Enterprises Employees

GIAC Enterprises employees on the internal network will be connected to either the head office PC LAN or one of the 4 regional office PC LANs. Each regional

[3] GIAC

office PC LAN will be connected to the head office using a branch to branch VPN connection. PCs and printers will be connected to the PC LANs. All servers will reside at the head office. File transfer between regional office LANs can be established by using either email or the ssh/scp server at the head office.

All PC LANs will have http (tcp port 80), https (tcp port 443) and sql*net v2 (tcp port 1521) access to the application server in the Server LAN. All PC LANs will have ssh/scp (tcp port 22) access to the ssh/scp server in the Server LAN. All PC LANs will have http (tcp port 80) and https (tcp port 443) access to the internal mail and web servers in the DMZ as well as dns (tcp/udp port 53) access to the internal dns server in the DMZ. All PCs will be allowed http (tcp port 80) and https (tcp port 443) access to the Internet. Printers will not have access to anywhere.

GIAC Enterprises Remote Users

The sales force will be limited to dns (tcp/udp port 53) access to the internal DNS server, http (tcp port 80) and https (tcp port 443) access to the mail and web server. No restriction will be placed on the source IP address since we expect to have our sales force to travel all over the world.

General Public

The general public will have http (tcp port 80) to the web server. Since https was enabled for our customers, the general public will also have https (tcp port 443) access into the web server by default.

Architecture Components

The following section identifies the security architecture components of GIAC Enterprises network.

Network Diagram

The following network diagram identifies the location and IP addresses of all security devices belonging to GIAC Enterprises:

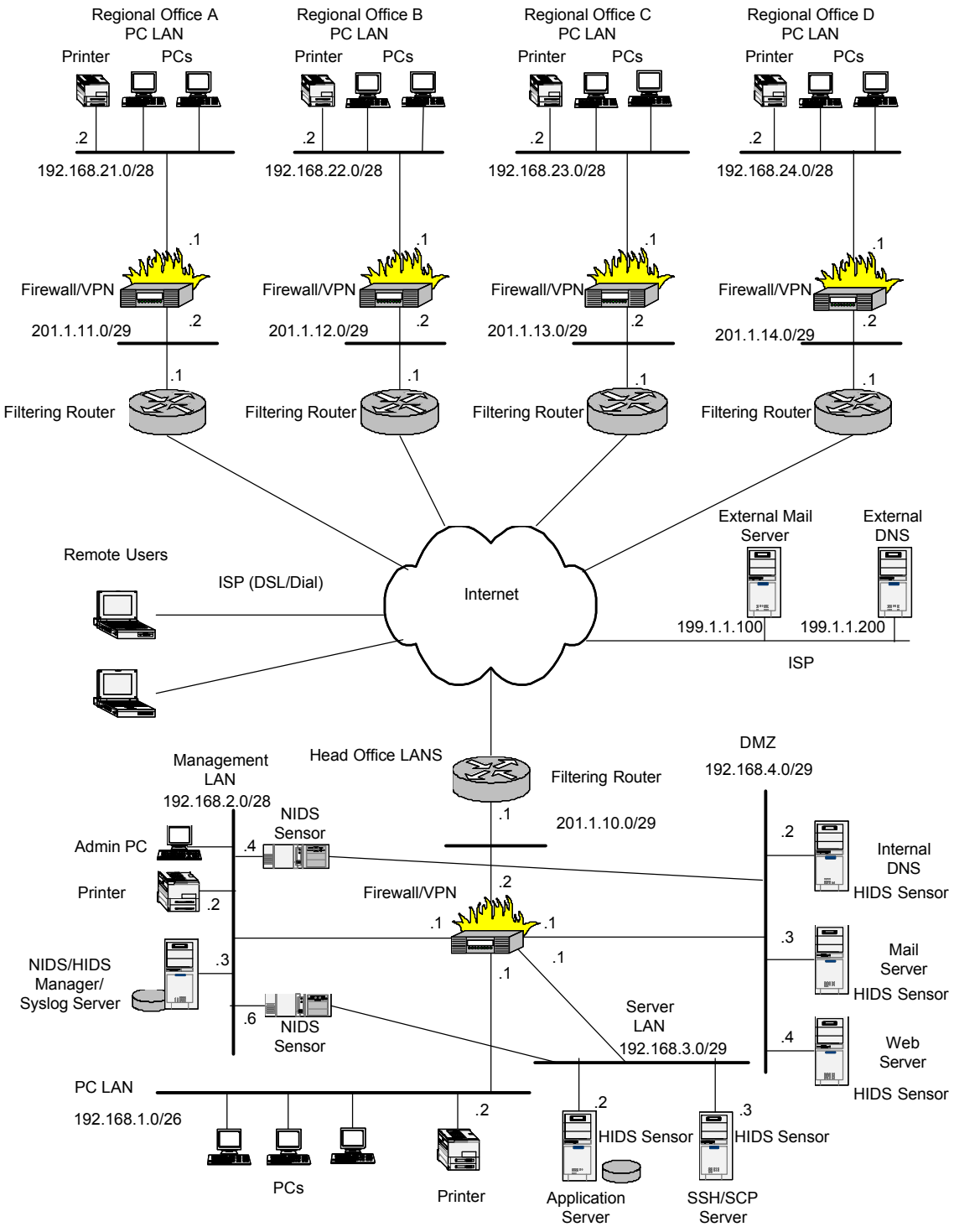

Figure 3: GIAC Enterprises Security Network

All equipment is owned by GIAC Enterprises with the exception of the external Mail and DNS servers. The external Mail and DNS servers are provided to us by our ISP for a monthly fee.

Filtering Routers

The filtering routers will be Cisco 2691 and 1760s.

Location	Brand	Model	OS Version
Head Office	Cisco Router	2691	12.3
Regional Offices	Cisco Router	1760	12.3

Firewalls and VPNs

The firewalls and VPNs will be Juniper NetScreen-208 and NetScreen-25s.

Location	Brand	Model	OS Version
Head Office	Juniper Networks	NetScreen-208	NetScreen OS 5.1.0
Regional Offices	Juniper Networks	NetScreen-25	NetScreen OS 5.1.0

Network Based IDS

Snort will be used as the network based IDS and ACID will be used as the network based IDS manager.

Location	Brand	Model	OS Version
Head Office	Snort	Snort	2.2 on Redhat Linux 9.0
Head Office	Snort Manager	ACID	ACID 0.9.6b23, MySQL 4.1 and Apache 2.0 on Redhat 9.0.

IP Addressing Scheme

All internal IP addresses are non-routable. All external IP addresses are routable.
The following table identifies the subnets used in GIAC Enterprises:

LAN Name	Public/Private	Subnet	Usable IPs
Regional Office A PC LAN	Private	192.168.21.0/28	14
Regional Office B PC LAN	Private	192.168.22.0/28	14

Regional Office C PC LAN	Private	192.168.23.0/28	14
Regional Office D PC LAN	Private	192.168.24.0/28	14
Head Office PC LAN	Private	192.168.1.0/26	62
Head Office Management LAN	Private	192.168.2.0/28	14
Head Office Server LAN	Private	192.168.3.0/29	6
Head Office DMZ	Private	192.168.4.0/29	6
Regional Office A Public LAN	Public	201.1.11.0/29	6
Regional Office B Public LAN	Public	201.1.12.0/29	6
Regional Office C Public LAN	Public	201.1.13.0/29	6
Regional Office D Public LAN	Public	201.1.14.0/29	6
Head Office Public LAN	Public	201.1.10.0/29	6

Additional Components

HIDS

A HIDS will be used to identify attacks on the servers. McAfee Entercept version 5.0 Manager and standard agents will be used as our HIDS.

Location	Brand	Model	OS Version
Head Office	Network Associates	McAfee Entercept Sensor	5.0
Head Office	Network Associates	McAfee Entercept Manager	5.0

Implementing Defense in Depth

Filtering Routers

The filtering routers main purpose it to route traffic between the internal and external networks. The filtering routers are the first line of defense. The security function of the filtering routers is to block packets with specific source and/or destination IP addresses.

The filtering routers will block incoming packets from the external network whose source IP address is one of the public IP addresses belonging to the subnet associated with the router. For example, the head office router will deny packets with source IP belonging to 201.1.10.0/29 to enter the internal network.

The filtering routers will allow outgoing packets from the internal network whose source IP address is one of the public IP addresses belonging to the subnet associated with the router. For example, the head office router will allow packets

with source IP belonging to 201.1.10.0/29 to the external network. All other packets will be denied.

All filtering routers will deny incoming packets from the external network with a private source IP address. According to RFC 1918[4], the private IP addresses are:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

Directed broadcasts are controlled by applying the "no IP directed-broadcast" command on each router's interface. All ICMP redirects will be filtered out. Services like finger, ntp and cdp will be disabled. IP source routing will be disabled using the "no IP source-route" command.

All access required will be specified in the router. All access not specifically permitted will be denied.

The filtering routers must be placed on the customer edge facing the external network. This placement is required so that the filtered packets are dropped before reaching the firewall. This will alleviated the amount of packets the firewall will have to process.

The strength of this component is its capability to filter packets very quickly based on packet header information (source and destination IP address/ports). The weakness of this component is that it does not check the actual packet contents beyond the packet header. Using Defense-In-Depth, the weakness of the filtering router is mitigated by the stateful inspection firewall and the network intrusion detection system.

The decision to use Cisco 1760 and 2691 are based on price performance costs and Cisco's reputation and longevity as a router vendor.

Firewalls

The firewalls become the second line of defense. The purpose of the firewalls is to block unwanted packets from entering or leaving the various internal LANs and the external network. The firewalls will perform both packet filtering and stateful inspection. The firewalls also perform source NATing on internal private IP addresses accessing the external network as well as destination NATing for the internal DNS, mail and web servers.

The firewalls are placed between the filtering routers and the LANs in the internal network. The placement of the firewalls in this network location allows the firewall to process all packets that are entering or leaving the internal

[4] Rekhter, Y., et al, page 4

network. It also allows the filtering router to filter out unwanted packets coming in from the external network before they reach the firewall.

The strength of the NetScreen firewalls is its ability to do both packet filtering and stateful inspection. NetScreen keeps track of the state of each TCP session and UDP pseudo-session to ensure that each packet matches the state of that associated session. NetScreen also provides protection against some common DOS attacks like SYN and UDP flood attacks. The weakness of the NetScreen firewalls is that it does look into patterns of traffic that may signal an attack is taking place. By using Defense-In-Depth, this weakness can be mitigated by using a NIDS to look for traffic patterns identifying an attack and sending an alert.

A technical reason for using the NetScreen firewall is that we wanted a high performance firewall capable of performing stateful inspection. The NetScreen-25 can process up to 100Mbps[5] and the NetScreen-208 can process up to 550Mbps[6]. Since NetScreen is an ASIC-based firewall appliance, we do not have to worry about OS hardening. Also, the NetScreen firewalls can support multiple zones. This will allow us the flexibility of having one physical firewall that can protect the 4 zones located at the head office (Untrust, DMZ, PC LAN and Server LAN).

VPNs

The purpose of the VPNs is to join the branch office LANs to the head off LANs. The VPNs will also allow remote workers to access the head office LANs. A branch to branch VPN will be used between the regional office PC LAN and the head office. Client to branch VPN will be used from the remote user PCs to the head office.

The VPNs security function is to allow traffic to securely traverse the Internet by using authentication and encryption.

Due to the dual functioning NetScreen devices that do both firewall and VPN functionality, the VPN placement is dictated by the placement of the firewall.

The strength of the NetScreen devices is that it offers a flexible suite of VPNs to meet any VPN type configuration. The weakness of the NetScreen devices is that we are performing both firewall and VPN functionality on one physical device. By gaining illegal access to a firewall, the intruder has also gained access to the VPN device. By using Defense-In-Depth, this weakness can be mitigated using a NIDS to look for traffic patterns identifying an attack.

A technical reason for using the NetScreen device is that we want high 3DES

[5] Juniper Networks, “Juniper Networks NetScreen-25/50 Spec Sheet”

[6] Juniper Networks, “Juniper Networks NetScreen-204/208 Spec Sheet”

performance. The NetScreen-25 can perform up to 20Mbps 3DES[7] encryption/decryption and the NetScreen-208 can perform up to 200Mbps 3DES[8] encryption/decryption. Since NetScreen devices are firewall and VPN devices, we eliminate an additional 5 VPN devices that would have to be purchased and managed.

NIDS
The NIDS purpose is to detect known attacks that have bypassed the firewall. The NIDS sensor will be Snort and the NIDS manager will be ACID.

A Snort sensor is placed on the Server and DMZ LANs attached to the head office's Firewall/VPN device so that it can analyze unencrypted traffic arriving or leaving each LAN. If the NIDS sensor was placed between the Firewall/VPN and the filtering router then it would not be able to analyze the VPN traffic since it would be encrypted at this point.

The NIDS is good at detecting know attacks by using a signature file. The disadvantage of the NIDS is that it cannot detect unknown attacks or analyze encrypted traffic like https. By using Defense-In-Depth, detection of unknown attacks and analysis of https traffic can be accomplished by using a HIDS at the server.

Additional Components

HIDS
The HIDS purpose is to detect attacks on the servers owned by GIAC Enterprises. The HIDS sensors will be placed on all our servers. The HIDS will be McAfee Entercept.

McAfee Entercept works at the kernel level and uses a "combination of behavioral rules and signatures"[9] to detect attacks. The HIDS is great at protecting against unknown attacks. The HIDS will also allow us to analyze unencrypted https traffic at the server that cannot be analyzed by the NIDS.

A technical reason for selecting McAfee Entercept is that it is both a HIDS and an IPS. McAfee Entercept will be deployed as a HIDS first to detect attacks. After a comfort level has been achieved in production, it will be configured to act as an IPS and prevent attacks.

Budget

A budget of $100K US plus or minus 10% was used in selecting all security

[7] Juniper Networks, "Juniper Networks NetScreen-25/50 Spec Sheet"
[8] Juniper Networks, "Juniper Networks NetScreen-204/2088 Spec Sheet"
[9] Network Associates

hardware and software. The following table lists the prices for the security devices for GIAC Enterprises:

Item	Quantity	Unit Price $US	Total Price $US
Filtering Router: Cisco 2691	1	4.5k	4.5K
Filtering Router Cisco 1760	4	1.2K	4.8K
Firewall/VPN: NetScreen-208	1	14.0K	14.0K
Firewall/VPN: NetScreen-25	4	12.0K	48.0K
IDS Sensor: Dell Power Edge SC1420, 2G RAM, 2X80GB Disk running Snort	2	6.0K	12.0K
NIDS/HIDS Manager/Syslog Server: Dell Power Edge SC1420, 2G RAM, 2X80GB Disk	1	6.0K	6.0K
HIDS: McAfee Entercept Standard Agent 5.0	5	1.0K	5.0K
HIDS: McAfee Entercept Manager 5.0	1	5.2K	5.2K
		Total	**99.5K**

Due to budget constraints, specific products like the NetScreen-208 and NetScreen-25 Firewall/VPN products that support multiple zones were selected to meet our overall budget.

Assignment 3 - Firewall Policy

The following section identifies the rulebase for the primary firewall in assignment 2.

Primary Firewall Rulebase

The primary firewall is the NetScreen-208 at the head office. There are 5 zones configured on the firewall at the head office. The 5 zones are:

- MgtLAN: the Management LAN (192.168.2.0/29)
- PCLAN: the PC LAN at the head office (192.168.1.0/26)
- ServerLAN: the Server LAN at the head office (192.168.3.0/29)
- DMZ: the Demilitarized Zone (192.168.4.0/29)
- Untrust: the Internet

Using the access requirements identified in Assignment 1, the following table identifies the rulebase for this firewall:

ID	Src Zone	Src IP	Dst Zone	Dst IP	Service	Action	Options
1	PCLAN	192.168.1.2/32	ServerLAN	Any	any	deny	log
2	PCLAN	192.168.1.2/32	DMZ	Any	any	deny	log
3	PCLAN	192.168.1.2/32	Untrust	Any	any	deny	log
4	PCLAN	192.168.1.0/26	Untrust	Any	http, https	accept	NAT src
5	PCLAN	192.168.1.0/26	ServerLAN	192.168.3.2/32	http, https, sql*netv2	accept	
6	PCLAN	192.168.1.0/26	ServerLAN	192.168.3.3/32	ssh	accept	
7	PCLAN	192.168.1.0/26	DMZ	192.168.4.2/32	dns	accept	
8	PCLAN	192.168.1.0/26	DMZ	192.168.4.3/32 192.168.4.4/32	http, https	accept	
9	DMZ	192.168.4.2/32	Untrust	199.1.1.200/32	dns	accept	
10	DMZ	192.168.4.3/32	Untrust	199.1.1.100/32	mail	accept	
11	DMZ	192.168.4.4/32	ServerLAN	192.168.3.2/32	sql*netv2	accept	
12	Untrust	192.168.21.0/28	ServerLAN	192.168.3.2/32	http, https, sql*netv2	tunnel	
13	Untrust	192.168.21.0/28	ServerLAN	192.168.3.3/32	ssh	tunnel	
14	Untrust	192.168.21.0/28	DMZ	192.168.4.2/32	dns	tunnel	
15	Untrust	192.168.21.0/28	DMZ	192.168.4.3/32 192.168.4.4/32	http, https	tunnel	
16	Untrust	192.168.22.0/28	ServerLAN	192.168.3.2/32	http, https, sql*netv2	tunnel	
17	Untrust	192.168.22.0/28	ServerLAN	192.168.3.3/32	ssh	tunnel	
18	Untrust	192.168.22.0/28	DMZ	192.168.4.2/32	dns	tunnel	
19	Untrust	192.168.22.0/28	DMZ	192.168.4.3/32 192.168.4.4/32	http, https	tunnel	
20	Untrust	192.168.23.0/28	ServerLAN	192.168.3.2/32	http, https, sql*netv2	tunnel	
21	Untrust	192.168.23.0/28	ServerLAN	192.168.3.3/32	ssh	tunnel	
22	Untrust	192.168.23.0/28	DMZ	192.168.4.2/32	dns	tunnel	
23	Untrust	192.168.23.0/28	DMZ	192.168.4.3/32 192.168.4.4/32	http, https	tunnel	
24	Untrust	192.168.24.0/28	ServerLAN	192.168.3.2/32	http, https, sql*netv2	tunnel	
25	Untrust	192.168.24.0/28	ServerLAN	192.168.3.3/32	ssh	tunnel	

26	Untrust	192.168.24.0/28	DMZ	192.168.4.2/32	dns	tunnel	
27	Untrust	192.168.24.0/28	DMZ	192.168.4.3/32 192.168.4.4/32	http, https	tunnel	
28	Untrust	10.0.0.0/8	DMZ	any	any	deny	log
29	Untrust	172.16.0.0/12	DMZ	any	any	deny	log
30	Untrust	192.168.0.0/16	DMZ	any	any	deny	log
31	Untrust	Any	DMZ	201.1.10.5/32	http, https	accept	NAT dst 192.168.4.4
32	Untrust	Any	DMZ	192.168.4.2/32	dns	tunnel	
33	Untrust	Any	DMZ	192.168.4.3/32 192.168.4.4/32	http, https	tunnel	
34	ServerLAN	192.168.3.2/32	MgtLAN	192.168.2.3/32	syslog	accept	
35	ServerLAN	192.168.3.3/32	MgtLAN	192.168.2.3/32	syslog	accept	
36	DMZ	192.168.4.2/32	MgtLAN	192.168.2.3/32	syslog	accept	
37	DMZ	192.168.4.3/32	MgtLAN	192.168.2.3/32	syslog	accept	
38	DMZ	192.168.4.4/32	MgtLAN	192.168.2.3/32	syslog	accept	

*Note: By default, NetScreen denies anything unspecified.

The following table identifies the definition for each service used in the rules above:

Service	Protocol/Port	Definition[10]
DNS	UDP src port 1-65535, dst port:53 TCP src port 1-65535, dst port:53	Domain Name Service translates domain names into IP addresses
HTTP	TCP src port 1-65535, dst port:80	Hypertext Transfer Protocol is the underlying protocol used by the World Wide Web (WWW)
HTTPS	TCP src port 1-65535, dst port:443	Hypertext Transfer Protocol with SSL (Secure Socket Layer) is a protocol for transmitting private documents via the Internet
MAIL	TCP src port 1-65535, dst port:25	Simple Mail Transfer Protocol is a protocol for sending email messages between servers
SQL*Net V2	TCP src port 1-65535, dst port:1521	SQL*Net Version 2
SSH	TCP src port 1-65535, dst port:22	Secure Shell is a program to log into another computer over a network through strong authentication and secure communications on an unsecured channel
SYSLOG	UDP src port 1-65535, dst port:514 UDP src port 1-65535, dst port:514	Syslog is a UNIX program which sends messages to the system logger

[10] Juniper Networks, "Service Definitions"

Printers
Rules 1 to 3 are required to deny packets originating from the printer on the PC LAN to any host on the Untrust, Server LAN and DMZ.

GIAC Enterprises Employees at Head Office
Rule 4 is required to allow the PCs on the PC LAN to get http and https access to the Internet with source NATing. This rule will also let GIAC Enterprises employees access our supplier's websites.

Rules 5 and 6 are required to allow the PCs on the PC LAN to get access to the application and ssh/scp servers on the Server LAN.

Rules 7 and 8 are required to allow the PCs on the PC LAN to get access to the dns, mail and web servers on the DMZ.

DNS and Mail Relays
Rule 9 and 10 are required to allow the internal DNS and mail servers on the DMZ to communicate with the external DNS and mail servers owned by the ISP.

Web Server's Access to Application Server
Rule 11 is required to allow the web server on the DMZ to communicate with the application server on the Server LAN.

GIAC Employees in Regional Offices
Rules 12 and 13 are required to allow the PCs on the Regional Office A's PC LAN to get access to the application and ssh/scp servers on the Server LAN using a VPN tunnel.

Rules 14 and 15 are required to allow the PCs on the Regional Office A's PC LAN to get access to the dns, mail and web servers on the DMZ using a VPN tunnel.

Rules 16 and 17 are required to allow the PCs on the Regional Office B's PC LAN to get access to the application and ssh/scp servers on the Server LAN using a VPN tunnel.

Rules 18 and 19 are required to allow the PCs on the Regional Office B's PC LAN to get access to the dns, mail and web servers on the DMZ using a VPN tunnel.

Rules 20 and 21 are required to allow the PCs on the Regional Office C's PC LAN to get access to the application and ssh/scp servers on the Server LAN using a VPN tunnel.

Rules 22 and 23 are required to allow the PCs on the Regional Office C's PC

LAN to get access to the dns, mail and web servers on the DMZ using a VPN tunnel.

Rules 24 and 25 are required to allow the PCs on the Regional Office D's PC LAN to get access to the application and ssh/scp servers on the Server LAN using a VPN tunnel.

Rules 26 and 27 are required to allow the PCs on the Regional Office D's PC LAN to get access to the dns, mail and web servers on the DMZ using a VPN tunnel.

Customers, Suppliers, Partners and the General Public
Rules 28 to 30 are required to deny packets where the source IP address from the Untrust zone are private IP addresses.

Rule 31 is required to allow customers, suppliers, partners and the general public to access GIAC Enterprises web server on the DMZ using destination NATing.

GIAC Enterprises Remote Users
Rules 32 and 33 are required to allow GIAC Enterprises remote users coming in on client to branch VPN to access the internal DNS, mail and web servers.

Syslog
Rules 34 to 38 are required to allow the servers on the DMZ and Server LAN to send syslog messages to the syslog server on the Management LAN.

Order of Rulebase

The order of the rules in the rulebase is important. For the same source and destination zones, a deny rule should be place before the accept rule if the accept rule accepts a packet that we really wanted to be denied by the deny rule.

Acronyms

AES:	Advanced Encryption Standard
ASIC:	Application-Specific Integrated Circuit
CDP:	Cisco Discovery Protocol
DES:	Data Encryption Standard
DMZ:	De-Militarized Zone
3DES:	Triple DES
EAP:	Extensible Authentication Protocol
HIDS:	Host Intrusion Detection System
HTTP:	HyperText Transfer Protocol
HTTPS:	HyperText Transfer Protocol Secure
IPS:	Intrusion Prevention System
LAN:	Local Area Network
LEAP:	Lightweight Extensible Authentication Protocol
Mbps:	Mega bits per second
NAT:	Network Address Translation
NIDS:	Network Intrusion Detection System
NTP:	Network Time Protocol
PEAP:	Protected Extensible Authentication Protocol
RC4:	A cipher designed by RSA Data Security, Inc.
SCP:	Secure Copy
SQL:	Structured Query Language
SSH:	Secure Shell
TCP:	Transmission Control Protocol
TKIP:	Temporal Key Integrity Protocol
UDP:	User Datagram Protocol
WEP:	Wired Equivalent Privacy
WPA:	Wi-Fi Protected Access
WPA2:	Wi-Fi Protected Access 2 (802.11i)

References

Assignment 1

1. Cisco Systems, “Cisco Aironet Wireless LAN Security Overview”, http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html

2. Cisco Systems, “Cisco Aironet 350 Client Adapters”, http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a0080088828.html

3. Cisco Systems, “Cisco Secure ACS 2.3 for Unix User Guide: Advanced Group and User Management”, http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_chapter09186a00800eb6dc.html

4. AirDefense, Inc., “AirDefense Guard”, http://www.airdefense.net/products/airdefense_ids.shtm

5. Lockhard, A., “Snort-Wireless”, November 2004, http://snort-wireless.org/

6. Fluhrer, S., et al., “Weaknesses in the Key Scheduling Algorithm of RC4”, http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

7. Blunk, L., Vollbrecht, J., “RFC 2284, “PPP Extensible Authentication Protocol (EAP)”, March 1998, http://rfc.net/rfc2284.html

8. Intermec, “CK30 Handheld Computer Specifications”, http://www.intermec.com/eprise/main/Intermec/Content/Products/Products_ShowDetail?section=Products&Product=CMPTRCK30&Category=CMPTR&Family=CMPTR1%20target=#

9. Palekar et al., “Protected EAP Protocol (PEAP) Version 2”, October 2004, http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-10.txt

10. InteropNet Labs, “What’s Wrong with WEP?”, http://www.opus1.com/www/whitepapers/whatswrongwithwep.pdf

Assignment 2

1. GIAC, “Certified Firewall Analyst (GCFW) Practical Assignment Version 4.0”, July 2004, http://www.giac.org/GCFW_assign_40.php

2. Rekhter, Y., et al, “RFC 1918: Address Allocation For Private Internets”, February 1996, http://rfc.net/rfc1918.html

3. Juniper Networks, “Juniper Networks NetScreen-25/50 Spec Sheet”, September 2004, http://www.juniper.net/products/integrated/dsheet/110003.pdf

4. Juniper Networks, Juniper Networks NetScreen-204/208 Spec Sheet”, November 2004, http://www.juniper.net/products/integrated/dsheet/110004.pdf

5. Network Associates, “McAfee Entercept Management System”, July 2004, http://www.networkassociates.com/us/_tier2/products/_media/mcafee/ds_entercept.pdf

6. Cisco, Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services, Release 12.3”, http://www.cisco.com/application/pdf/en/us/guest/products/ps5317/c2001/ccmigration_09186a008018e5e0.pdf

7. Cisco, “Cisco 1760 Modular Access Routesr Data Sheet”, http://www.cisco.com/en/US/products/hw/routers/ps221/products_data_sheet09186a00800920f2.html

8. Cisco, “Cisco 2600 Modular Access Routers Data Sheet”, http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet0900aecd800fa5be.html

9. Juniper Networks, “Denial of Service and Attack Protection”, http://www.juniper.net/products/integrated/dos.html

10. Sourcefire, “Snort User Manual 2.2.0”, http://www.snort.org/docs/snort_manual/

Assignment 3

1. Juniper Networks, “Service Definitions”, NetScreen WebUI Software Version 5.1.0

2. Juniper Networks, “NetScreen Concepts & Examples ScreenOS Reference Guide: All volumes combined”, http://www.juniper.net/techpubs/software/screenos/screenos5.1.0/CE_all.pdf