GCFW Practical

Gregory Lalla

GCFW Practical
Version 4.0

Date: December 7, 2004

Table of Contents

List of Figures

Summary

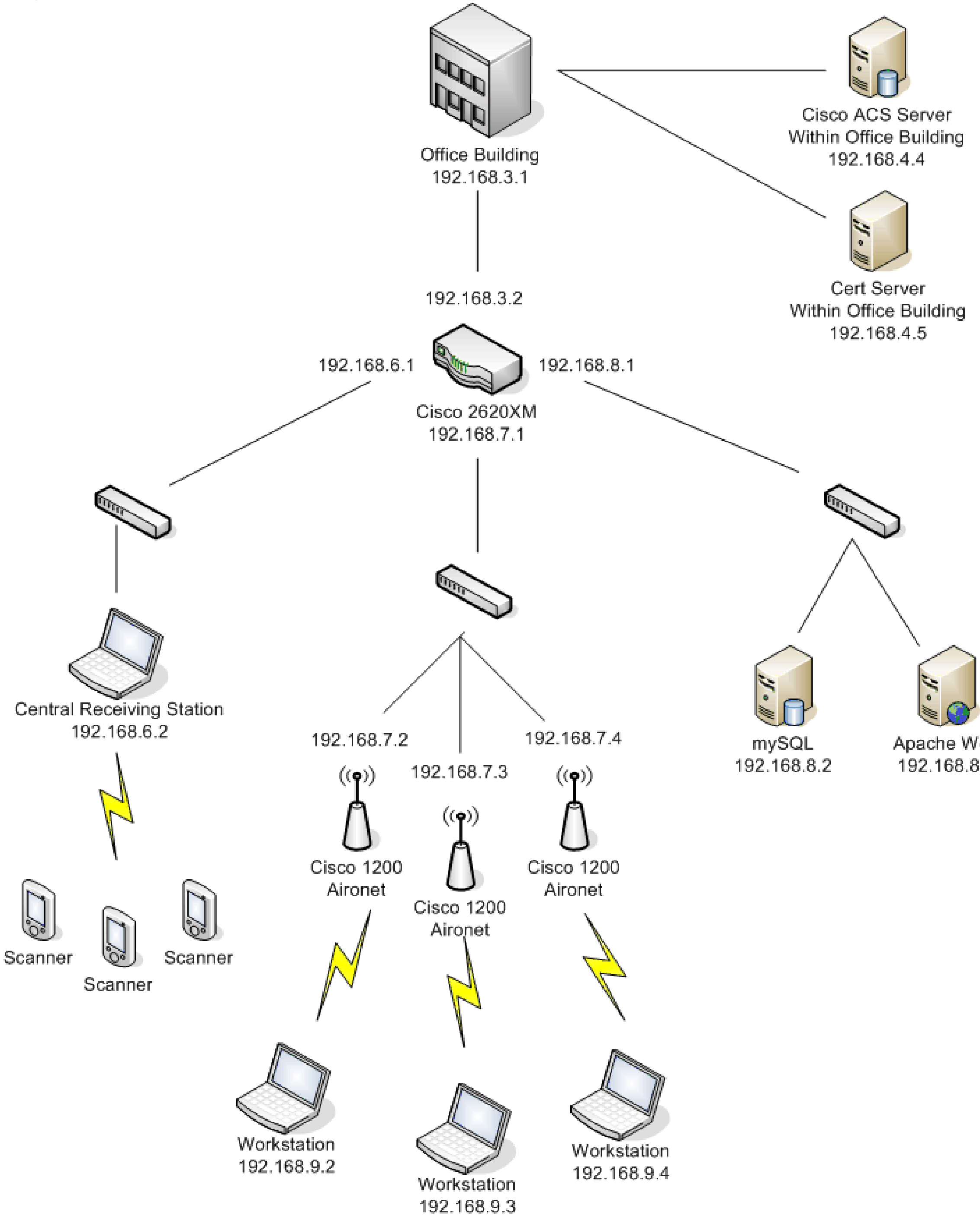
> GIAC Enterprises is a small business which markets fortune cookie sayings to customers worldwide. GIAC employs fifty people with the majority located in or near its head office and the remainder located in or near the four regional satellite offices geographically distributed around the world. All of the GIAC Enterprises sales are done via the internet.[1] (Sans.org, p.1)

The security team for the company will present the security measures put in place to protect the company's assets along with the security measures for the resent wireless networking integration. The home office's firewall policy will also be shown to explain how the device protects the network. GIAC Enterprises does not have an unlimited budget to spend on its IT infrastructure, so cost is a major issue. For this reason, the company will look to use open-source software wherever possible unless an overriding reason exists to purchase software from a vendor. Also, the company will only purchase equipment and software that meets its current needs and the needs of the company during what is forecasted to be small growth in the next 5 years.

Assignment 1: Wireless Network Integration

A newly built edition has been added to the head office building. This new edition will be used as a warehouse for the production and shipping of fortune cookie sayings. The GIAC Enterprises security staff has been asked to securely integrate wireless technology in the warehouse with the existing network architecture, described in Assignment 2. The warehouse will be using handheld scanners in the shipping process and wireless laptops on the warehouse floor for day to day operations. The diagram of the warehouse network is below.

Figure 1



Wireless Architecture

During the construction of the warehouse, a network closet was built to house a Cisco 2620XM Multiservice router and three Cisco 2950 Catalyst switches. These devices are running the latest version of Cisco's IOS 12.3 software. The router has four Ethernet interfaces. Three of the interfaces lead to the three switches in the closet. The remaining interface connects the warehouse network to the head office network. There are three Cisco 1200 Series Aironet Access Points (AP) that are connected to one of the three switches. These AP's provide wireless connectivity for the wireless laptops in the warehouse. There is also a central receiving station that connects to one of the two remaining switches. This central receiving station allows the handheld scanners to transmit the information they have scanned to a mySQL 4.0 database server. That database server, along with an Apache 1.3.31 web server, resides on the last switch. These two servers are used in the day to day operation in the warehouse. CAT5 cabling is used throughout the wired network. Traffic bottlenecks are not a concern for normal network activity.

In the shipping area there are five handheld devices that are used to scan every package that is shipped to the company's customers. The handhelds scan a bar code that is affixed to the package. This information is sent to a central receiving station where custom software collects the information and forwards it through an ODBC connection to a database on the mySQL server. There is also a front-end intranet Apache web server that houses a custom web application where authorized users can query the database to track shipments. The web application requires a user name and password to login and both are stored on the database server. The company chose to use the no cost mySQL and Apache open-source software because they do not require a capital investment and they are easy to use and fulfill all of the company's requirements and needs.

Bluetooth Wireless Scanners

The handhelds are Flic Cordless Laser Bar Code Scanners. These scanners use Bluetooth to communicate with a Bluetooth USB Base Station (BS). The BS is connected to the USB port of a fully patched Windows XP SP2 laptop. The laptop would not connect to the wired network using an 802.11x wireless network card because there could be interference between the two wireless protocols. Therefore, the laptop is wired to a switch using CAT 5 Ethernet cabling. The laptop is running software called Flicware, which receives the scanned bar codes from the BS. A contractor was hired to write software that would take this input and immediately send it through an ODBC connection to a mySQL database. The scanners have a range of 30 to 50 ft from the BS. If the scanner is out of the range of the BS it has an auto-connect feature which will capture the data and hold it until the scanner comes back into range. The BS is centrally located to allow maximum maneuverability and coverage for the shipping department.

The warehouse and office building are surrounded by a security fence and only authorized personnel are allowed onto the grounds of GIAC Enterprises. There is a security guard booth at the entrance of the grounds that is manned 24 hours a day. The security guards patrol the grounds periodically throughout the day. At its closest, the perimeter fence is 30 yards from the buildings. This protects the wireless network from the casual war driving attacker where the perpetrator attempts to discover insecure wireless devices either by actively scanning or passively listening to wireless communications.

A more determined attacker or a disgruntled employee could attempt to get within range of the Bluetooth devices. To protect against attacks, each scanner is paired with the BS using a strong pairing. The pairing is used for authentication purposes and normally employs a PIN code. The PIN has been changed from the default of 0000 to a 16 digit PIN that is more resistant to a brute force attack. "The length of time it takes to crack the code depends on the number of digits a person uses in his or her code. A 6-digit PIN can be broken in just more than 10 seconds, while a 16-digit PIN would take more than a million days to crack."[2] (Lemos, p.1) Flic allows for a stronger pairing, which uses the scanners Bluetooth device address and a PIN code to create the pairing. Each Bluetooth device has a distinctive device address. "This ensure[s] a unique pairing, and it prevents a second Bluetooth host from connecting to the scanner, even when the second host knows the scanner's PIN code."[3] (MicroVision, p.14) This helps to prevent man in the middle attacks and unauthorized access to the BS. In the company's security policy the security team states that the pairings or bondings will be checked bi-weekly to ensure there are no new unauthorized bondings. The registry on the Windows XP laptop will also be checked for any intruder who "might have placed a temporary bond or pairing upon"[4] (Whitehouse, p.18) the host. The registry "lists all devices ever paired with the host."[5] (Whitehouse, p.18) This will help to detect an intrusion that has gone un-noticed.

The devices are running Bluetooth version 1.1 and "access code and packet header are never encrypted."[6] (Whitehouse, p.3) This means that the devices are easily identified by sniffing the network. The latest version of Bluetooth allows "a stealth mode in which a device ignores broadcast queries, rendering it invisible to any other devices that don't know its specific eight-byte address."[7] (Poulsen, p.1) However, this can be defeated with a tool from @stake called Redfang that "decloaks such hidden devices using brute-force-- it sends queries over a large range of addresses, and listens for replies."[8] (Poulsen, p.1) You can also use Bluesniff (http://bluesniff.shmoo.com/) or use the tools installed with Bluez (http://www.bluez.org/) to sniff the traffic and gather information such as the version of Bluetooth, its class, the device name, the device address and the manufacture of the device.

> To launch an attack using the flaw…is not simple and can be expensive. @Stake found that an attacker has to be able to eavesdrop on the initial negotiation between two Bluetooth devices, called 'bonding.' The would-be eavesdropper has to collect some key data during that process to have enough information to crack secret PIN codes.[9] (Lemos, p.1)

There are also other limitations. "You can't just use an ordinary Bluetooth card…The attack requires some pretty hefty equipment… The specialized gear for hacking Bluetooth signals could cost more than $15,000."[10] (Lemos, p.1) Considering the lengths an attacker would have to go to exploit this flaw and the non-critical information an attacker could gain, GIAC Enterprises accepts the risk.

The security team, however, will use the above tools as much as they can to scan for unauthorized Bluetooth devices in the area. The GIAC Enterprises security policy also states that employees must disable all unauthorized Bluetooth device like cell phones and PDAs. There are also firewall technologies available for Bluetooth enabled devices such as http://www.bluefiresecurity.com/, but the scanners will not work with this technology. If a firewall product becomes available that offers protection for the handheld devices, they'll look into implementing it as soon as possible.

802.11g Wireless Laptops

On the warehouse floor, wireless laptops are used to track how many fortune sayings are being produced, what supplies need to be ordered, how much of each particular saying is being produced, who the product is being shipped to and the bar code labeling for the boxes.

The laptops are running Windows XP Service Pack 2 and are fully patched. They also have the latest virus protection and the Windows XP firewall is enabled. The laptops each have a Cisco Aironet 802.11a/b/g Cardbus wireless LAN client adapter running the latest firmware. There are three APs equally distributed across the warehouse floor for complete coverage. These APs are configured as an Extend Service Set (ESS) and communicate over a Distributed System (DS) to allow the laptops to be moved from one location in the warehouse to another without losing connectivity. The protocol used between the AP and wireless network cards is 802.11g exclusively. This provides a maximum throughput of 54mbps at the 2.4 GHz range.

To secure the 802.11g communications the GIAC security team employed several different techniques to harden the wireless network against intrusion. First, an Extended Service Set Identifier (ESSID) of WAREHOUSE was set, which "is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network."[11] (Netgear, p.1) In order for a client to connect to the Wireless LAN (WLAN), the client must know the ESSID. This value is normally broadcast from the AP. The broadcast feature has been turned off and the value is manually entered on each of the warehouse laptops. The GIAC security team has ensured that the AP does not respond to ESSID probes of "ANY". If this setting is not disabled, an AP will answer the probe. This is rather rudimentary security because the ESSID can be easily sniffed by passively listening to the initial communications between the AP and legitimate clients. Netstumber is one tool that can accomplish the sniffing. That being said, the disabling of the ESSID broadcast defends against casual attackers trying to access the network. The ESSID can also be attacked with a brute force tool called Wellenreiter, but this tool can be detected on your network as it uses pseudo random MAC addresses to hide its presence. By capturing the wireless traffic and comparing the MAC addresses with known good addresses from your legitimate wireless network cards, you can see if there are any unknown addresses sending out Probe Request. A detailed explanation of this can be found at http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf.

The second security measure is Wireless Card Access Lists. Each wireless network card has a unique identifier known as a MAC address. By identifying MAC addresses that are authorized to be on the network, an access list can be created that only allows authorized addresses to connect to the AP. This will prevent any rogue device that is not specified in the access list from connecting to the APs. This security measure will also keep out the casual attacker and will normally keep out the slightly more determined intruder. However, this security measure can also be circumvented by spoofing the MAC address to one that is on the Access List. This can be done using a tool called SMAC. There is also a suite of tools called AirJack that uses a spoofed MAC address to inflict a Man-in-the-Middle attack. One of the tools in the suite is called wlan-jack. It's a "tool to perform a denial-of-service attack against users on a target wireless network; it works by sending spoofed deauthenticate frames to a broadcast address, purportedly from the network access point's MAC address."[12] (Wright, p.7) The de-authentication frames disconnect the client from the AP. Again, by capturing wireless packets the security team can detect this type of attack by "anomalies in sequence numbers."[13] (Wright, p.8) A detailed explanation of this can be found at http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf. Using a packet sniffer called Ethereal, the packets can be captured for analysis. Kizmet can also be used to sniff the network and it can be used as an IDS which can set off an alert when it sees unusual traffic.

The third security measure is to use Cisco Wireless Security Suite to provide Confidentiality, Integrity, Authentication, Authorization and Auditing. All of the wireless devices are made by Cisco and support the Cisco Wireless Security Suit. The security team will use this method instead of Wired Equivalent Privacy (WEP) which has several security flaws that enable attackers to discover the encryption keys used to encrypt the network traffic. There are several tools that exploit the vulnerabilities in WEP. Airsnort and WEPCrack are the most notable. A further discussion of the WEP flaws can be found at http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf. WEP is also discussed below when it is compared to Wi-Fi Protected Access (WPA).

This implementation does cost money. The company chose to invest in this area of the network because of the weaknesses in wireless communications and because this is a potential backdoor into the company's network that bypasses the security put in place at the firewall. The company felt that obtaining the best product possible to secure this potential threat was worth the cost.

The Wireless Security Suite will be using Cisco Protected Extensible Authentication Protocol (PEAP) for authentication and WPA and Temporal Key Integrity Protocol (TKIP) for Encryption. PEAP clients will authenticate against a Cisco Secure Access Control Server (ACS) that houses the user credentials for all legitimate laptop users. The server-side certificate will be issued by a Microsoft Server running Certificate Services. Each of the Windows XP laptops will have the Cisco wireless client software installed which supports PEAP.

PEAP uses Transport Layer Security (TLS) "to encrypt all user-sensitive authentication information…does not expose the logon user name in the EAP identity response [and] is not vulnerable to dictionary attacks."[14] (Cisco Systems, p.5) This provides secure authentication. Authorization and Auditing happen on the Cisco ACS server where logging is enabled and user and group profiles determine access.

Because of the insecurities of WEP, the GIAC team will use WPA to encrypt network traffic once the client has been authenticated. WPA uses TKIP and Message Integrity Check (MIC) as its encryption method. TKIP solves two of the major weaknesses in WEP. First, WEP uses a 24 bit Initialization Vector (IV) to

> concatenat[e] a shared secret key. WEP eventually uses the same IV for different data packets. This results in the transmission of frames having encrypted frames that are similar enough for a hacker to collect frames based on the same IV and determine their shared values leading to the decryption of 802.11 frames. WPA with TKIP, however, uses 48-bit IVs that significantly reduce the IV reuse and the possibility that a hacker will collect a sufficient number of 802.11 frames to crack the encryption.[15] (Geier, p.1)

The second enhancement is that "WPA automatically generates a new unique encryption key periodically for each client. This avoids the same key staying in use for weeks or months as they do with WEP."[16] (Geier, p.1)

A stronger MIC or Michael is used for checking integrity.

> With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver. With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte *message integrity code* (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV. Michael also helps provide replay protection.[17] (Microsoft, p.1)

These improvements make WPA much more difficult to hack. However, that does not mean that WPA cannot be hacked. WPA2 has just been standardized and it introduces AES encryption. This is a much stronger encryption scheme which solves the inherent problems with WEP and WPA. Once Cisco offers products that support WPA2, the company will immediately upgrade.

This implementation of the Cisco Wireless Security Suite solution was chosen because it provides the best possible security for the wireless network. It offers Authentication through PEAP, Authorization and Auditing through Cisco ACS, Confidentiality through TKIP and Integrity through MIC. This protects against "Man-in-the-Middle Attacks, Authentication Forging, Weak IV Attacks (AirSnort), Packet Forgery (Replay Attacks), Brute-Force Attacks and Dictionary Attacks."[18] (Cisco Systems, p.12)

Physical security is very important for all of the wireless devices. The laptops and the scanners are not allowed to leave the warehouse and the handheld scanners are locked in a secure cabinet each night. The laptops are required to be locked in a drawer each night before the employees leave for the day. Periodic audits are conducted to make sure each device is accounted for and properly stored.

With these security measures in place the company can be reasonably assured that the wireless network is secure. Of course, ongoing auditing and log reviews will continue to insure the network is secure. In particular, Netstumbler will be used to find unauthorized APs, Kismet will be used to sniff the wireless network and act as an Intrusion Detection System and audits will be performed on the wireless devices to make sure they are properly configured.

Assignment 2: Security Architecture

Access Requirements

When defining the network for GIAC Enterprises the GIAC security team took into consideration all aspects of the company's business. This included the customers who purchase bulk online fortunes, the suppliers who supply the company with fortune cookie sayings, the international partners who translate and resell fortunes, the remote sales force who need to connect back to the network, the general public who access the company web site and the internal workforce who are responsible for day to day operations.

Customers

The customers who purchase bulk online fortunes require access to the company's main web site. The customers use a link from the home page to open a web application where they can submit purchase orders. This link is secured using Secure Socket Layer (SSL) and brings the user to a login screen where they must enter a valid user name and password to get into the purchase order system. Once the customer has successfully logged in they can purchase bulk fortunes. These purchase requests are stored in a backend database where they can be processed. The backend database contains the user name and password information for each of the customers. For new customers, there is a link from the home page informing them to contact, via email or phone, the company's sales representatives to set up a new account. In order for the customers to get to the web server's home page and purchase order application they must connect to TCP ports 80 (HTTP) and 443 (HTTPS). If a customer or potential customer wishes to send the company an email they connect to TCP port 25 (SMTP).

For name resolution, UDP port 53 (DNS) is available. These services are offered on the DMZ (also referred to as Services Network) in the network architecture.

Suppliers

The suppliers write unique fortune sayings for GIAC Enterprises. Each month these sayings are uploaded to the GIAC network and then retrieved by GIAC employees who take the sayings and import them into a database for processing. The sayings are compiled in a Microsoft Word document which is never larger than 2 MB. These files are SFTP to an SSH server sitting on the company's DMZ. Each supplier has their own user name and password that is stored locally on the SSH server. Each supplier also has their own restricted location on the SSH server to drop their fortunes. This prevents suppliers from seeing another suppliers work and possibly tampering with the files. The suppliers connect through TCP port 22 (SSH) to transfers their files. They will also connect to TCP port 25 (SMTP) for mail and UDP port 53 (DNS) for name resolution.

Partners

The international partners translate and resell the company's fortunes. The partners, through a secure SSL link off of the company's main web site, can query the fortunes database and download what they require. To access the front-end web application the partners must login using a unique user name and password which is stored on the database server. In order for the Partners to get to the web server they connect to TCP ports 80 (HTTP) and 443 (HTTPS). They also connect to TCP port 25 (SMTP) for mail and UDP port 53 (DNS) for name resolution.

Employees

GIAC Enterprise employees on the internal network do most of the day to day activities. Most of the employee's resources are located on the internal network. There are a few individuals who have access to the SSH server and employees do access the company's home page for any company related news. There are also resources on the internet that the employees might need. For this reason, the company allows outbound connections to the internet on TCP ports 80 (HTTP), 443 (HTTPS) and 21 (FTP). Certain employees are given access to the DMZ for TCP port 22 (SSH) and all employees are allowed access to the DMZ on TCP port 80 (HTTP). If employees need other ports opened at the firewall to do their job, a waiver request can submitted with proper justification for approval. There are currently no waivers.

Sales Force/Teleworkers

The GIAC Enterprise sales force is located in four regional satellite offices geographically distributed around the world. These sites each have a static IP address from a local ISP to use with their firewall. The users at each office connect to the head office through a VPN tunnel between the local gateway and the company's main firewall. The VPN connection permits the office to access the internal network so that they can complete their day to day business. The VPN tunnel uses AES for encryption and MD5 for data integrity. There are also users out on sales calls or working from home that need to be able to connect to the home office. These users, through a local client on their mobile pc, can establish a VPN connection with the main firewall and get access to the company's internal resources. The ports opened at the firewall to allow this communication are UDP port 500 (IKE) and protocol 50 (ESP).

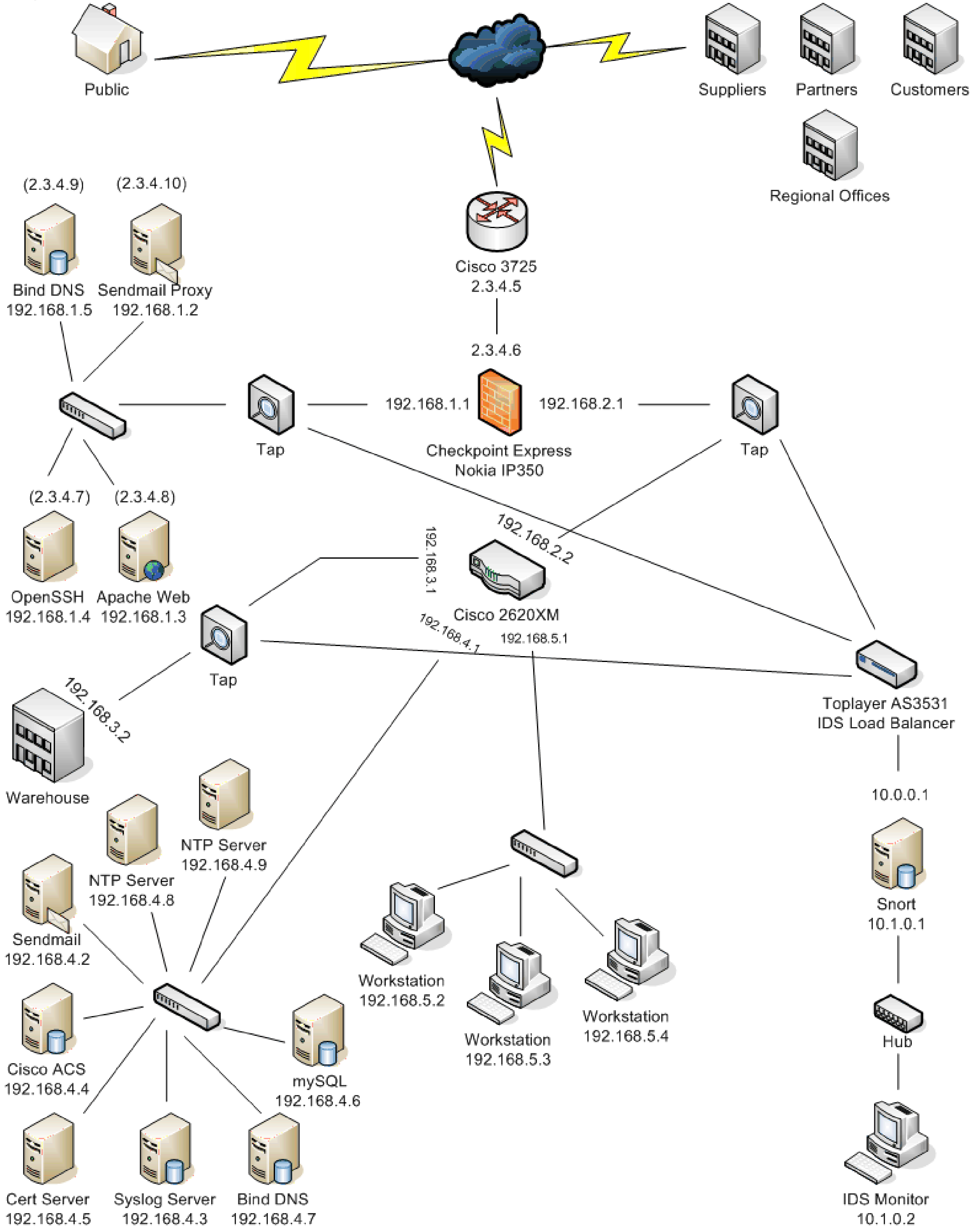
General Public

The general public is allowed to access the company's web site for general information and is permitted to send emails to the company. The ports open for this access are TCP ports 80 (HTTP) and 25 (SMTP). UDP port 53 (DNS) is also open for name resolution.

Access Requirements

Below is the diagram of the GIAC Enterprises network including all IT security components. Each device will be explained in detail and a discussion of the measures taken to add Defense in Depth to the environment will follow:

Figure 2



Filtering Router

The company's first line of defense is its boarder router. This router is a Cisco 3725 Multiservice Access Router running the latest version of Internet Operating System

(IOS) 12.3. This mid-priced router is a nice sized router which will be able to handle the company's network capacity. The main purpose of the boarder router is to route internet traffic destined for the GIAC network to the main firewall. There is a static route configured on the router to point directly to the firewall interface for each valid IP address used on the DMZ. This allows traffic destined for the publicly offered services to reach their destination. The router also has the ability to provide some protection against unwanted traffic from entering or leaving the network. Since it is the first device that network traffic encounters before entering the network address space, filters can be applied to filter out obviously bad or malicious traffic. This action takes some of the load off of the main firewall.

The GIAC security team has set up static packet filters to block the following types of traffic:

Ingress Traffic – This traffic is blocked from entering the network using standard Access Control Lists (ACL) which are fast to process and have less overhead on the router. The following rules are applied to the external interface of the router:

access-list 20	deny	10.0.0.0	0.255.255.255	log
access-list 20	deny	172.16.0.0.	0.15.255.255	log
access-list 20	deny	192.168.0.0	0.0.255.255	log

The above rules block all private IP addresses as defined in RFC 1918. These addresses are private and should be non-routable and therefore should not be seen on the internet facing interface.

access-list 20	deny	169.254.0.0	0.0.255.255	log

The above rule blocks Dynamic Configuration of IPv4 link local addresses used by some DHCP clients when they cannot allocate an IP address from the DHCP server. These addresses should not appear on the internet.

access-list 20	deny	224.0.0.0	31.255.255.255	log

The above rule blocks Multicast traffic which is not allowed on the network.

access-list 20	deny	127.0.0.0	0.255.255.255	log

The above rule blocks the Loopback address. IP addresses that fall within this range should not be routed to the GIAC network.

access-list 20	deny	0.0.0.0	0.255.255.255	log
access-list 20	deny	1.0.0.0	0.255.255.255	log
access-list 20	deny	3.0.0.0	0.255.255.255	log

The above rules block legal IP addresses that have not been issued.

access-list 20	deny	2.3.4.0	0.0.0.255	log

The above rule blocks the GIAC's IP address space from entering the network if it is the source address. Since it is impossible for traffic that is from the company's network to originate outside the network, there is obviously something wrong with the packets and they should be dropped.

access-list 20	permit	any

This last rule above allows all traffic not matching the above rules through to the GIAC network.

Egress Traffic - This traffic is blocked from leaving the network. Again, standard Access Control Lists (ACL) are used. These rules below are applied to the internal interface of the router.

access-list 21	permit	2.3.4.0	0.0.0.255
access-list 21	deny	any	Log

The first rule above allows any traffic from the GIAC network to pass through the router. The second rule denies all other traffic. This helps to prevent spoofed traffic from leaving the network and attacking others.

The GIAC security team chose not to use extended or reflexive ACLs to block specific ports or other types of protocols, because of the increased burden those filters might place on the boarder router. Instead, those functions will be performed by the firewall.

The GIAC security team has also taken steps to harden the router since there is nothing protecting it from being attacked. Telnet has been disabled so that the only way to login to the router is through a direct console connection. All services and protocols are confirmed to be turned off with the following commands:

no snmp
no ip http
no ip bootp
no services tcp-small-servers
no services upd-small-servers
no service finger

All network related activities are also confirmed to be tuned off with the following commands:

no ip source-route
no ip direct-broadcast
no ip unreachables

Banners are also enabled to warn intruders that only authorized users are allowed to access the router. The logs are reviewed daily by the GIAC security team.

Firewall

Where the boarder router is the first line of defense, the firewall is the main line of defense. A firewall is defined as:

> A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. [19] (Webopedia.com, p.1)

Because of the importance of a firewall, the company believed that it should spend the most capital in this area to ensure that the network environment is as secure as possible. The firewall hardware chosen was a Nokia IP350. This device is specifically designed for the purposes of being a firewall and unlike using a Dell or Sparc server which has USB ports, keyboard and mouse ports, video cards, audio cards, etc, this device only has the necessary hardware components to run the firewall. This means there are fewer components that can bring the system down if they fail. It also has its own secure proprietary operating system which is stripped down to only offer the services needed on a firewall. The Nokia IP350 comes with a built-in hardware based encryption accelerator for increased VPN performance. This makes the system extremely reliable. The Nokia IP350 offers excellent throughput at 507 Megabits per second, which is more than adequate for the traffic that traverses the GIAC network. Another advantage to using a Nokia is that the hardware is specifically designed to run Checkpoint's Express software. This software combines Checkpoint's Firewall-1 and VPN-1 NG with Application Intelligence (R55) software together on the same machine. The Nokia also integrates Real Secures IDS software. Because of the cost of the Real Secure IDS, GIAC has chosen not to activate it. However, it may do so in the near future to augment its Snort IDS implementation.

The Nokia operating system is called IPSO and it is currently running the latest build of version 3.8. This system, like the boarder router, is exposed to the internet. To lock this device down, the company only permits connections to the IPSO through a SSH connection. The web based Voyager service and telnet are disabled for remote administration. The small services, ftp, tftp, snmp and http are also disabled. Any TCP traffic that has both the SYN and FIN bits set are configured to be dropped. Logging is enabled and the logs are sent to the central Syslog server.

Checkpoint Express software was chosen because it includes a large amount of standard features and capabilities. Two of the most important features are the firewall and VPN software included in the product. The firewall software is extremely user friendly with a GUI management client used to configure and maintain the firewall ruleset. The product is very intuitive, which makes it less likely that mistakes will be made during configuration. This has allowed the small IT staff to become familiar and comfortable with the product. The GUI is also flexible enough where specific permissions can be given to individual IT staff members. The more experienced members have full permissions on the firewall and staff with less experience have only read permissions, which allow them to view the firewall configurations to help troubleshoot network issues. Logging has been enabled in the Global Properties window under Logs and Alerts. All track options are set to log. Logging has also been enabled on a per rule bases. These logs are checked daily.

GIAC Enterprises uses the firewall software mostly for Stateful packet filtering and address translation, but it has the capability to perform application level proxying, stateful inspection, and content filtering. The software also helps to protect the network by blocking malformed packets, SYN floods, fragmentation and other Denial of Service attacks. It has the ability to defend against well know attacks like worms and cross-site scripting. Each interface is set to perform anti-spoofing based on the interface topology. The anti-spoofing prevents spoofed ingress and egress traffic from passing through the firewall and may locate mis-configured hosts.

The placement of the firewall behind the boarder router allows it to protect the internal network and the DMZ network. The DMZ network hangs off of one internal interface and the rest of the corporate network hangs off another internal interface. GIAC uses Network Address Translation (NAT) to allow its publicly offered services to communicate with the internet and to allow the users on the internal private network to connect to the internet while not exposing their system. When users on the internal network connect to the internet their private IP address is translated to the IP address of the firewall's external interface. The firewall keeps track of each connection by the source port it assigns to the traffic. When a system on the internet receives the connection, all it sees is the IP address of the firewall. This protects the internal IP address space from the internet. This type of NAT also protects the internal network because devices on the internet cannot initiate a connection to these hosts. That traffic would be dropped. The firewall uses a second type of NAT for the servers on the DMZ. These hosts need to be able to accept connections from the internet. The firewall provides a one-to-one translation. Each server has its own public IP address associated with it. When the firewall receives a connection to one of these IP addresses, it will translate the destination to the private address of the server. Likewise, when the server makes a connection to the internet, the firewall will translate its private IP address to the public IP address. The details of this implementation are discussed in the IP Address Scheme section below.

The firewall ruleset is maintained from a management console running SmartConsole software. This management console also manages all of the regional office firewalls. All communications between the console and the firewall are sent over SSL to encrypt the traffic. The ruleset is configured to allow authorized traffic between network segments.

To help provide defense in depth, the company has taken the approach of the Principle of Least Privileges. If a port or service is not being used it should be closed. This includes traffic in both directions on each of the firewalls interfaces. The firewall ruleset is discussed in detail in Assignment 3.

VPN

For compatibility and familiarity the regional offices are also running Checkpoint Express on Nokia hardware. The Nokia model is an IP130 which is more appropriate for the GIAC office size. The regional offices are running the latest build of IPSO 3.8 and this setup allows for a single management station to manage all the firewalls. The firewalls each have a set of ACL's to protect their sites. They offer no publicly available services so only outbound connections are allowed to the internet. The internal IP addressing scheme is also the same at each site as the one at the home office. The security team has established a VPN connection from each remote office firewall (or gateway) to the corporate office firewall.

The VPN has been set up in Simplified mode using certificates for authentication from the firewalls certificate authority. All traffic is protected using IPSec to tunnel communications. Internet Key Exchange (IKE) security protocol is used with 256 bit Advanced Encryption Standard (AES) key exchange encryption with Message Digest (MD5) data integrity during phase 1 of the Security Association (SA). This IKE SA is renegotiated every 720 minutes. During phase 2, IPSec data encryption is done with 256 bit AES and MD5 data integrity. The IPsec SA is renegotiated every 1440 minutes.

The VPN is configured in a star like configuration with VPN routing enabled that allows each site to communicate with the home office but it also allows each site to communicate with each other. This is done by the main firewall which will decrypt the traffic sent by the remote site and then re-encrypt the traffic and send it to another remote site. This adds some overhead, but the feature is rarely used so the main firewall does not see any ill effects of it being enabled. Also, all services are encrypted between the regional offices and the home office since the traffic is light and the bandwidth can handle the load. NAT is also disabled within the VPN community.

GIAC Enterprises allows some employees to telework from home and there are sales people who are on the road that need to connect back to the network from time to time. These individuals are allowed to establish a VPN connection through their ISP back to the home office network. Each user has Checkpoint's SecureClient installed on their GIAC laptop and the VPN connection is setup similar to the firewall connections using 256 bit AES for encryption and MD5 for data integrity. Certificates are used on each client and are generated by the firewall. Each certificate is installed on the client's laptop by a member of the IT staff. Each laptop also has a personal firewall installed with anti-virus protection to protect the machines when they are outside the protection of the GIAC firewalls.

There are some potential issues with using both the firewall and the VPN on one system. The combined effort could overload the device, slowing traffic down and possibly dropping connection or packets. To compensate for this threat the company has purchased hardware and software that is capable enough to handle all the traffic that would normally be seen even on the busiest day. This solution will also handle any growth the company may experience in the next 5 years.

Network based Intrusion Detection System

GIAC Enterprises will deploy a network based intrusion detection system (nIDS) to monitor the network. A nIDS collects network traffic and analyzes it to see if any of the traffic is malicious. Taps will be used to capture the traffic that the company is interested in analyzing. The taps are NetOptics Ethernet Taps that passively monitor the network traffic and forwards a copy of it to a Toplayer AS3531 IDS load balancer. The load balancer takes that traffic and distributes it to a server for analysis. Taps are inexpensive devices and do not require power and if they happen to fail they do not interrupt the flow of network traffic. The taps will be located at critical locations throughout the network to help detect malicious activities.

The first tap is located on the DMZ network segment between the firewall and the switch. This location is critical because it houses the servers that are accessible by the internet. These systems are the ones most likely to be attacked and it is therefore important that the security team detect any type of malicious activity directed towards these servers so that they can take appropriate action. This tap will also allow the security team to detect any mis-configuration of the firewall, which may allow in unwanted traffic. The second tap is located between the firewall and the internal network router and this tap will help to detect any malicious activities attempting to reach the inside of the network. This includes users who download malicious content or visit malicious web sites. It can also help to detect tunneled attack if the DMZ is to be compromised and is being used as a launching point for systems inside the network. Another benefit would be the detection of systems on the internal network trying to infect other parts of the network with a worm or virus. The nIDS could detect scans and denial of service attacks by the infected systems. The last tap is located between the internal network router and the warehouse router. This tap is needed because of the wireless network located in the warehouse. If any rogue system were to attach to the wireless network or compromise a wireless workstation, the security team would want to detect any attacks against the internal network or the DMZ.

A tap was not installed outside the firewall for two reasons. First, since this is a small company with limited man power, the number of alerts generated by the constant scanning and attacks of automated tool would take up valuable time and resources. These types of attacks are easily blocked by the firewall and normally the attacks are old enough that the systems are already patched against the exploit. Second the firewall logs can be checked to see what is hitting the outside interface. Also, the security team is really only concerned with the traffic that makes it inside the network. The attacks blocked at the firewall are just that, blocked.

These three taps connect back to an IDS load balancer which is on a separate private network. The purpose of the IDS load balancer is to take the network traffic fed into it from such devices as taps, mirrored ports or spanned ports on switches or routers and direct that traffic to multiple outputs for analysis. These outputs can be a Snort IDS sensor, an ISS Real Secure sensor, a Bro sensor, etc. The load balancer is intelligent enough to be able to send the same traffic to multiple sensors or send specific types of traffic to each individual sensor. For example, the load balancer can send all port 80 traffic to the Snort senor, all internal communications to the Real Secure sensor and all traffic to the Bro sensor. The load balancer, the sensors and the monitoring stations are placed on a separate private network to ensure that the information being provided is kept secure from prying eyes that might use the information against a vulnerable machine. An attacker could also tamper with the sensors to cover their tracks while hacking the network. By keeping the nIDS components on a private network it also keeps the attacker unaware that their activities are being monitored.

Using a load balancer instead of individual sensors for each tap saves the company money. Not only does the company have to purchase less hardware since only one sensor is needed instead of three, the company saves time managing fewer sensors freeing the security team to focus on other areas of the network. It also allows the company to expand without having to change the network infrastructure if the sensors become overloaded.

Currently the load placed on the sensors is low enough that only one sensor is needed. In the future, if the load increases the company will add additional sensors to the load balancer. The purpose of a sensor is to take the network traffic passed to it and analyze it according to the application that sits on top of the senor. Some sensors use anomaly detection, which looks for traffic that is outside normal activity parameters. These types of sensors try to detect known and unknown attacks. Anomaly detection requires a known baseline so that it can detect the unusual traffic and this can be done easily on host based systems where the setup is fairly static. However, in a network environment that is changing frequently it is very difficult to get that baseline and it creates a high volume of false positives. The other common sensor is rule based. This type of sensor has rules or signatures of known attacks. It compares these signatures against the traffic that is sent to the sensor. If the network traffic matches that of a signature an alert can be generated. The issue with rules based detection systems is that they have to have the signature to detect the malicious activity. This means that the rule base must be kept current on all the signatures and if there is a zero day exploit that does not have a signature yet, the IDS will not pick it up.

Snort is the sensor GIAC Enterprises will use on a robust Fedora Core 2 Linux server. Snort was selected because it is a free open source application and with the company's limited budget it cannot afford to pay for the more expensive IDS software. Snort is also an extremely powerful and flexible nIDS and is used by many organizations. As mentioned above, the Snort sensor resides on an isolated network segment to prevent tampering. Snort is a rules based sensor. The rules are updated quite often and with the company's limited man power, a free product called Oinkmaster is used to help with rule management. This product automatically downloads the latest rules and manages the rules that are already enabled. The rules are configured in such a way as to limit the amount of false positives while still alerting one to malicious traffic. When alerts are generated they are logged on the server and sent to a console on the isolated network that is constantly monitored.

For purposes of defense in depth, the company needed to find a way around the limitation of rules based software. There is a plug-in that is available for Snort which is called Spade. The Spade plug-in gives snort anomaly based detection capability.

> Spade will review the packets received by Snort, find those of interest…and report those packets that it believes are anomalous along with an anomaly score. The anomaly score that is assigned is based on the observed history of the network. The fewer times that a particular kind of packet has occurred in the past, the higher its anomaly score will be…At any given time, a reporting threshold is defined for the sensor. For each event that exceeds this threshold, an alert is sent.[20] (Hoagland & Staniford, p.1)

As mentioned above, anomaly detection does not work well in a changing environment. However, the GIAC network is small enough and relatively static that SPADE can be used effectively while not burdening the administrators with excessive false positives. This sensor configuration gives a fairly complete picture of what malicious activity is happening on the GIAC network.

IP Addressing Scheme

GIAC Enterprises and its regional offices use a private addressing scheme behind the firewalls. The range of addresses being used falls within the 192.168.0.0 address space. Each network segment has its own class C subnet with a netmask of 255.255.255.0. The isolated network where the nIDS resides has a private address range of 10.0.0.0. This network has been broken down into two subnets with a netmask of 255.255.255.0. The network segment attached to the external interface of the firewall has a public address range assigned by the company's ISP. The IP range is 2.3.4.0 with a netmask of 255.255.255.0.

GIAC Enterprises uses NAT to allow for communications with the internet. In order for internet traffic to reach the publicly offered services on the servers in the DMZ, changes must be made on the firewall and boarder router for the traffic to make it to its final destination. As discussed in the Boarder Router section, static routes have been mapped from the public IP address of each service to the MAC address of external firewall interface. This is needed because the router sees the public IP addresses as being on its subnet and will attempt to send an ARP request to forward it on to that IP address. Since those IP's are not actually listening on the subnet, no response is sent and the packet is discarded. This fix will forward the traffic to the firewall to be routed. In order for the routing to take place on the firewall, routes are configured to forward the traffic from the public IP address to the corresponding private IP address. NAT rules and Security rules are created in the firewall policy to allow this traffic to happen. The company's implementation of Split DNS resolves issues of the internal users attempting to connect to services on the DMZ.

When GIAC users on the internal network connect to the internet, NAT is applied in Hide Mode. The firewall takes this traffic and changes the source IP address to that of the firewalls external interface. This hides the users IP address from the device at the final destination and to anyone who may be sniffing the traffic. Replies are sent back to the firewall which forwards the packets on to the user. The firewall keeps track of all the connections using the source port for UDP and TCP traffic and the data field for ICMP traffic. Hide mode also prevents anyone on the internet from making an initial connection to a listening device on the internal network.

One issue with NAT might be the added overhead on the firewall. "NAT requires extra memory and CPU on the gateway. In most cases, this is negligible, but it starts becoming noticeable when over 20,000 connections through a single gateway are subject to NAT."[21] (Welch-Abernathy, p.338) The GIAC firewall will never handle this much traffic at once so this potential problem is not an issue.

Defense in Depth

The DMZ is located off one of the firewall interfaces and each device on the DMZ has a private IP address but is mapped to a specific public IP address that is accessible through the firewall. The DMZ allows the company to have a public presence on the internet without exposing the entire network. The company offers four services: Web, DNS, E-mail and SSH.

The Web server serves multiple functions. First, it offers a static web site for the general public who can browse its pages and see information about the company including what products are offered and who to contact for questions. The Second function is to allow the company's customers to purchase their orders in bulk. This is done through a web application front end that communicates with a backend database on the internal network. The web application is protected by SSL purchased through Verisign and a login screen so that each customer must logon in order to place an order. The last function of the web server is to allow the company's partners to choose and download fortunes. They do this through another web application front-end that communicates with the backend database on the internal network. They access this application through a link off the front page. This application is also protected by a login which must be completed before the partners can download the fortunes. This application also uses the same SSL certificate to encrypt the traffic. The web server is running Apache 1.3.31 on a fully patched Sun Solaris 9 server. Apache was chosen because it is free open-source software which is reliable, robust, secure and easy to maintain and configure. The Apache configuration file is locked down and MOD_SECURITY is used to protect the system from passing any dangerous arguments to the applications. Web logging is enabled and the log files are sent to the internal Syslog server for analysis.

The backend database that the web server communicates with is a mySQL 4.0 database on a fully patched Sun Solaris 9 server. Database software can be extremely expensive and mySQL was chosen because it is free open-source software. It was also chosen because it can easily handle the small databases on the server and because it is very reliable and easy to use and maintain. The purpose of this server is two fold. First, it stores all the purchasing information the company's customers enter through the web server interface. This information is used by several authorized employees in the purchasing department. A third party application gathers the purchase requests and then prints out purchase orders for processing. The second function of the database server is to store the fortunes provided by the company's suppliers. This information is downloaded by the company's partners via the front-end web server. Since this server provides no services to the public, it is located on the internal network to protect it from the internet. The firewall only allows the web servers IP address to connect to this server and only on the mySQL ports. This server sends its log files to the internal Syslog server.

A Domain Name System (DNS) server also resides on the DMZ network. The DNS server translates domain names to IP addresses and this allows the company's publicly offered services to be accessible by the internet community. It is also necessary for the company's employees to connect to services outside the organization. Unfortunately, people with malicious intentions could attempt to use the information in the DNS to attack the network or use the DNS server as a tool to help them attack others. To protect against these weaknesses, the DNS is setup as a Split DNS. To implement this an external DNS server is located in the DMZ and allows DNS queries about the company's public name space to be answered so the publicly offered services can be found. The external DNS does not contain any information on the internal name space which helps to protect the systems behind the firewall. The external DNS server is also setup to be non-recursive except for those machines offering services on the DMZ and to the internal DNS server. This helps to protect the DNS server from cache poisoning attacks or the DNS server being used to assist in the attack of others. The external DNS server also does not allow zone transfers of its database. The Internal DNS server is used by internal clients for name resolution. It contains all the private address space mappings for the internal hosts and those on the DMZ. This DNS server is recursive so that it can be used to query the internet for outside resources. Zone transfers are also turned off. Both DNS servers are running the Bind 9.3 on fully patched Sun Solaris 9 servers. This software was selected because it is robust, reliable, and easy to use. It is also free open-source software. DNS logging is enabled on both DNS servers and the logs are sent to a central Syslog server for analysis.

GIAC Enterprises rely heavily on E-mail to communicate with customers, partners, suppliers and others on the internet. It is also important because on the internal network, employees are able to communicate with each other in a fast reliable manner. The company designed the network with an E-mail proxy server on the DMZ network and an E-mail server on the internal network. Both E-mail servers run Sendmail 8.13.1 on fully patched Sun Solaris 9 servers. The company would have liked the internal mail server to be a Microsoft Exchange server as the different types of E-mail servers makes it more difficult for a hacker to compromise each platform. Cost is an issue and the company decided to accept the risk and use the free Sendmail server software for both E-mail servers. Sendmail was also chosen above other open-source solutions because of its reliability and ease of use. Plus, many years of scrutiny have made this a very secure product.

The Sendmail Proxy server on the DMZ acts as a relay server. It takes E-mail messages it receives and forwards them on to their destination. The internal Sendmail server is used by all of the employees to send E-mail. These messages are then forwarded on to the Proxy Sendmail server which strips the headers from the messages. This conceals the internal IP address space and the type of internal E-mail server being used. This setup overcomes the weakness of having the primary E-mail server exposed to the world. The Proxy Sendmail server is also set up to only relay mail from the IP address of the internal E-mail server.

The last server on DMZ is a Sun Solaris 9 server running OpenSSH 3.9. OpenSSH is a free open-source product which allows the suppliers to securely transfer files to the company's network. These files contain the unique fortunes that are used in the company's product. By placing the server in the DMZ, the company prevents a compromised system from having direct access to the internal network. Once the fortunes have been transferred to the SSH server, authorized employees connect to the server using an SSH client and copy the files locally to their workstations. The sayings are then imported into the backend mySQL database where they'll be used to create the fortunes and where they can be downloaded by the company's partners. A user name and password is required to authenticate to the SSH server. Since there are a limited number of suppliers, account credentials are stored and managed locally on the server. The encryption is SSHv2. SSHv1 has been disabled. Each supplier is restricted to a specific location when they login to the server. This protects supplier's files from being examined and potentially altered by other suppliers. It also limits the exposure of the server if it were to be hacked through one of the SSH accounts.

On the internal network there are two Cisco 2620XM Multiservice Routers running IOS 12.3 (one has already been described in the wireless section). These devices are used to route network traffic to the appropriate locations within the internal network. The devices also break up broadcast domains and can isolate traffic that is local to the network segment. These devices can easily handle the day to day network traffic. In order to protect the routers, these devices have all remote administration features turned off. The company is small enough that an administrator with a laptop can directly connect to each of the devices for configuration. The routers have all the small services disabled along with finger, http, bootp, and snmp. Source routing and direct broadcast are also turned off.

Connected to the routers are Cisco 2950 IOS 12.3 Catalyst switches. The switches keep network traffic local and prevent it from being sniffed. These devices can also be used to shut off the LAN ports of compromised systems which may help prevent the contamination of other systems on the network. These devices are also configured so that they cannot be administered remotely. The routers and the switches are kept in a locked closet to physically protect them tampering.

The Network Time Protocol (NTP) servers run version 4.2.0 on fully patched Sun Solaris 9 servers. These servers are critical because they keep all the servers synchronized on the same time and this helps correlate log files when analyzing events from several different sources. It is also very important when doing forensics and presenting any evidence to law enforcement. If one server is 20 hours off from another server, it might be difficult to prove that a compromise happened at a specific time and date. Because NTP is so important, this is the one service the company has invested money into for redundancy. The servers are configured to connect through the firewall to two different Stratum 2 time servers. The servers on the DMZ and the servers on the internal network are all configured to get their time from the internal NTP server.

The last component on the network is a central Syslog server. This server is used to house a copy of all the logs generated by the servers on the DMZ, the servers on the internal network, the firewall itself and the routers on the network. This is a robust server with plenty of hard drive space. This server sits on the internal network so that it is protected from the outside. The servers that are on the DMZ must go through the firewall to get to the internal network. At the firewall, those specific servers are allowed through on the Syslog port to only the Syslog server. The server is also protected with IP filtering to restrict access to only those IP addresses that need access to it. The reason for the central log server is to protect the log files that are generated on the individual servers that send the logs. If a hacker compromises a system, one of the areas they usually modify or destroy is the logs to help cover their tracks. Even if the logs are tampered with, the central log server will still have an intact copy of logs on the log server. This is critical when doing forensics on a compromised system. The company's policy is to keep the logs for 60 days. These logs are reviewed daily. Filters and scripts are setup to make the task more manageable.

Additional security measures have been put in place to protect the GIAC Enterprises network. Every server is kept fully patched and runs the latest software version. All unnecessary services are disabled on all systems. For the Sun Solaris 9 servers and the Fedora Core 2 Linux server, the security team has enabled IPSec packet filtering, TCP Wrappers and Tripwire. The Microsoft Windows servers, workstations and laptops all have the latest service packs installed and are fully patched. Employee computers also have Mcafee virus protection enabled, Adaware spyware scanners installed and the Microsoft Windows firewall activated. The Microsoft servers have Mcafee virus protection enabled and are configured with IPSec packet filtering which allows only specific IP addresses to connect to the server. The Event Viewer logs on the Microsoft servers are checked daily.

The security team performs a monthly vulnerability scan against all the devices on the network using Nessus and SARA scanning software. There is also a quarterly security audit performed by the security team which verifies compliance with the company's security policy. The security policy is based on the SANS Step-by-Step guide and the Center for Internet Security's security recommendations. The security team uses the CIS scoring tools to help check compliance. The Microsoft Baseline Security Analyzer is used to make sure the Windows systems are properly patched and configured. The tool is also used to ensure that passwords follow the company's security policy. For the Unix systems, the security team uses John the Ripper and Crack to check password complexity.

Privileges are also kept to a minimum on all systems. Users who require access to the servers are given the least amount of permissions needed to complete their job. Employees are also not given administrative privileges on their own systems. This helps to prevent employees from installing unauthorized software, modifying critical files and helping to prevent the system from root level compromise.

Remote administration of the servers on the DMZ is not permitted. Each server must be logged into at the console. Backups are done to tape on each system and tapes are rotated by a member of the System Administrators group. Honeypots and Honeynets are not used in this environment. GIAC Enterprises does not have the staff or resources to dedicate and maintain a Honeypot.

Assignment 3: Firewall Policy

The rule base for the Checkpoint Express firewall in Assignment 2 is detailed in this section.

Firewall Ruleset

Implied Rules

The first rules in the firewalls rule set are the implied rules. These rules are configured in the Global Properties page and the first implied rules used are the "Accept VPN-1 & Firewall-1 control connections" rules. The rules allow communications between the GUI clients, management station and the firewalls. It also permits the gateways to set up the VPN connections needed to communicate with each other. The second implied rule is the "Accept outgoing packets originating from Gateway" rule. This rule allows communication from the firewall and can be useful for updates need by the Nokia IPSO operating system. This rule is placed before the last rule in the firewall policy. The "Accept RIP", "Accept Domain Name over UDP (Queries)" and "Accept Domain Name over TCP (Zone Transfer)" rules have been disabled. These rules are not needed in the company's environment and may lead to a less than secure network. The "Accept ICMP requests" rule is also disabled. This rule would allow all ICMP type request traffic through the firewall. ICMP can be a dangerous tool. Attackers use it to map networks, launch denial of service attacks and even as a communication channel. The next rule that the company has enabled is "Accept CPRID connections (SmartUpdate)." This rule allows the firewall modules to be upgraded remotely. The last rule, "Accept dynamic address Modules' DHCP traffic," is disabled since the company does not use DHCP on its network.

Firewall Access Rule

No	Source	Destination	VPN	Service	Action
1	NOT Internal-Net	Firewall-Group	Any Traffic	Any	Drop

Rule number is called the Stealth rule and it protects the firewall from being attacked. This does not prevent traffic from getting through to the DMZ since only the IP address of the external interface on the firewall is affected, not the public IP's of the services. The rule also "separates the traffic so you can more easily see what traffic is being direct at your firewall."[22] (Welch-Abernathy, p.99) The source address refers to any host that is not on the internal network and the destination is the firewalls themselves. This rule drops the traffic that matches the rule.

VPN Rules

No	Source	Destination	VPN	Service	Action
2	Any	Any	VPN-Gateway-Community	Any	Accept

Rule number two allows VPN traffic for any service between the regional firewalls and the home office firewall. The VPN object "VPN-Gateway-Community" is a group object that contains each of the company's VPN gateways. This community is set up in Star Mode which allows each regional VPN to only communicate directly with the home office VPN and not to each other.

No	Source	Destination	VPN	Service	Action
3	VPN-Users	Any	VPN-Users-Community	Any	Accept

Rule number three allows the users who are in the "VPN-Users" group to communicate on any service through a VPN connection to the home office firewall. The user groups and VPN gateways are identified in the "VPN-Users-Community" group.

General Rules

No	Source	Destination	VPN	Service	Action
4	DMZ-Net	Internal-Log	Any Traffic	udp Syslog	Accept

Rule number four allows all of the servers on the DMZ to communicate through the firewall on UDP port 514 to the internal Syslog server. These communications are the logs that each server produces and are centralized on one server for analysis and data retention. The object "DMZ-NET" includes each of the privately addressed server objects that are on the DMZ network. The "Internal-Log" represents the Syslog server on the internal network. The private addresses are used for the servers on the DMZ because the traffic does not leave the external interface of the firewall.

No	Source	Destination	VPN	Service	Action
5	Any	DMZ-Web-Ext	Any Traffic	tcp HTTP	Accept

Rule number five allows any source IP address to access TCP port 80 on the Apache web server sitting on the DMZ network. This rule allows the public to see the home web site and it allows the partners and customers to navigate to the private areas of the web server to conduct business. The "DMZ-Web-Ext" object represents the public IP address of the web servers so traffic from the internet can be properly routed by the firewall.

No	Source	Destination	VPN	Service	Action
6	NOT GIAC-Enterprise-Group	DMZ-DNS-Ext	Any Traffic	tcp DNS	Accept
	DMZ-DNS-Ext	NOT GIAC-Enterprise-Group		udp DNS	

Rule number six allows the DNS server on the DMZ to answer internet requests for its name space and allows the server to recursively query internet DNS servers for requests received from the internal DNS server. The policy allows for both UDP and TCP protocols on port 53 to ensure delivery of the recursive queries. If the initial UDP response is larger than 512 bytes, the information is truncated. When this happens the DNS server will send another query, but this time using TCP so that the entire response can be received. The "DMZ-DNS-Ext" object represents the public IP address of the DNS server on the DMZ. This allows the firewall to properly route the traffic to the server. The policy also restricts the GIAC-Enterprise-Group because the company does not want employees to attempt to resolve names with this server. In the case of compromise, the policy also acts to restrict the DNS server from communicating with the internal network.

No	Source	Destination	VPN	Service	Action
7	Internal-DNS	DMZ-DNS	Any Traffic	tcp DNS	Accept
				udp DNS	

Rule number seven is setup to permit the internal DNS server to initial recursive queries with the DMZ DNS server on UDP and TCP port 53. Once again, TCP and UDP are used in case the responses are too large. The "DMZ-DNS" object represents the private address of the DNS server on the DMZ since the initial query does not leave the external interface of the firewall.

No	Source	Destination	VPN	Service	Action
8	Internal-Net	NOT DMZ-Net	Any Traffic	tcp HTTP	Accept
				tcp HTTPS	
				tcp FTP	

Rule number eight allows the users on the internal network to access the internet on TCP ports 80, 443 and 21. GIAC Enterprises only opens ports that are necessary for it to do business. It is felt that the average employee only requires web access and ftp access to complete their day to day activities and it also denies access to the DMZ network which is represented by the "DMZ-Net" object. This restriction prevents internal users from getting to resources they do not normally have access to. For example, if a restricted FTP server was placed in the DMZ and this rule had ANY in the Destination column, then all internal users would have the ability to reach the server.

No	Source	Destination	VPN	Service	Action
9	Internal-NTP-Group	NTP-Stratum-2-Group	Any Traffic	udp NTP	Accept

Rule number nine is set to allow the internal NTP servers to connect to the two Stratum 2 time servers on the internet over UDP port 123. This allows the internal NTP servers to synchronize time with the Stratum 2 servers. The "Internal-NTP-Group" object represents the two IP addresses of the internal NTP servers. The "NTP-Stratum-2-Group" object represents the two IP addresses of the Stratum 2 servers that provide accurate time.

No	Source	Destination	VPN	Service	Action
10	DMZ-Net	Internal-NTP-Group	Any Traffic	udp NTP	Accept

Rule number 10 is set to allow the servers on the DMZ network to synchronize their time with the internal NTP server over UDP port 123. This allows the DMZ server and the servers on the internal network to have time synchronization.

No	Source	Destination	VPN	Service	Action
11	NOT GIAC-Enterprise-Group	DMZ-Mail-Proxy-Ext	Any Traffic	tcp SMTP	Accept
	DMZ-Mail-Proxy-Ext	NOT GIAC-Enterprise-Group			

Rule number 11 is set up to allow the Sendmail server on the DMZ to deliver E-mail or receive E-mail from the internet on TCP port 25. The "DMZ-Mail-Proxy-Ext" object represents the public IP address of the E-mail server. This allows the firewall to properly route the traffic to its destination. The "GIAC-Enterprise-Group" object represents each internal network segment of the home office and the network segments of the regional offices. The NOT indicates that all traffic to and from the E-mail server is acceptable except for those networks in the GIAC-Enterprise-Group. This prevents the E-mail server from sending or receiving email directly to company employees. Sending or receiving directly to company employees may happen either from a mis-configuration of the Sendmail server, a rogue computer on the network or if the server itself has been compromised.

No	Source	Destination	VPN	Service	Action
12	Internal-Mail	DMZ-Mail-Proxy	Any Traffic	tcp SMTP	Accept
	DMZ-Mail-Proxy	Internal-Mail			

Rule number 12 allows traffic between the company's E-mail servers to communicate on TCP port 25. Messages from the internet that are received at the DMZ Sendmail server are then allowed through the firewall to the internal Sendmail server for distribution. Likewise, E-mail received on the internal Sendmail server will be forwarded through the firewall to the DMZ Sendmail server for distribution to the internet. The "DMZ-Mail-Proxy" object represents the private address of the E-mail server since the communication does not leave the external interface of the firewall. The internal DNS server handles the translation to the correct IP address.

No	Source	Destination	VPN	Service	Action
13	Customers-Group	DMZ-Web-Ext	Any Traffic	tcp HTTPS	Accept
	Partners-Group				

Rule number 13 allows the company's customers and partners to connect to its secure web site on TCP port 443. This allows them to access the restricted applications to purchase and download fortunes. The "Customers-Group" object and the "Partners-Group" object represent the IP addresses for each company that is allowed access. No other IP addresses are permitted to access this portion of the web server. The DMZ-Web-Ext object is used again because the connection is coming in through the internet and must be properly routed to the correct destination.

No	Source	Destination	VPN	Service	Action
14	Suppliers-Group	DMZ-SSH-Ext	Any Traffic	tcp SSH	Accept

Rule number 14 allows the suppliers to upload their fortune sayings to the SSH server on the DMZ using TCP port 22.The "Suppliers-Group" object represents the IP addresses of all the suppliers. No other internet IP addresses are allowed to connect to this server. The "DMZ-SSH-Ext" object represents the public IP address of the SSH server and is used to properly routed the traffic through the firewall to the correct destination.

No	Source	Destination	VPN	Service	Action
15	Internal-SSH-Group	DMZ-SSH	Any Traffic	tcp SSH	Accept

Rule number 15 allows authorized employees to connect through the firewall over TCP port 22 to the SSH server on the DMZ. The "Internal-SSH-Group" represents authorized employees who take the files uploaded by the suppliers and import them into the backend database. The "DMZ-SSH" object represents the private address of the DNS server on the DMZ since the SSH traffic does not leave the external interface of the firewall.

No	Source	Destination	VPN	Service	Action
16	DMZ-Web	Internal-Backend	Any Traffic	tcp mySQL	Accept

Rule number 16 allows the front-end web server on the DMZ to communicate with the backend mySQL database server on the internal network for mySQL traffic on TCP port 3306. This communication consists of the purchase orders entered by the customers and the fortune sayings provided to the partners. All traffic is passed within the company's private IP address space.

No	Source	Destination	VPN	Service	Action
17	Internal-Net	DMZ-Web	Any Traffic	tcp HTTP	Accept

Rule number 17 allows the internal users to connect to the company's home web site on TCP port 80. The object "Internal-Net" represents the internal network space of the company. Since these users are accessing a resource on the DMZ the DMZ-Web object is used to represent the private address of the Web server.

No	Source	Destination	VPN	Service	Action
18	Internal-Net	Any	Any Traffic	icmp Echo	Accept
				Traceroute	

Rule number 18 allows user on the internal network, represented by the Internal-Net object, to send out ICMP Echo Request and Traceroute packets to any destination. This allows users to do such things as troubleshoot network problems and see if internet web sites are up and running. To allow ICMP replies and error messages back into the network, the "Accept Stateful ICMP Replies and Errors" settings are enabling in the Global Properties page.

No	Source	Destination	VPN	Service	Action
19	Any	Any	Any Traffic	Any	Drop

Rule number 19 is the last rule in the firewall policy and sometimes referred to as the Cleanup Rule. This rule will drop all traffic that has not been matched by a rule above. Traffic that has not been specifically allowed should not make it through the firewall.

Logging is enabled on all rules and the logs are sent to the internal Syslog server for analysis.

Rule Ordering

The rule ordering is important in the company's ruleset. Because rules are processed in the order they appear, rules that get used the most generally appear at the top of the list. This saves the firewall from using processing power analyzing rules that aren't frequently utilized.. For rulesets that use drop rules, the ordering becomes even more critical. There is the potential to drop traffic after hitting a rule that is too general if place before a rule that specifically allows restricted access to the same service. However, the security team does not use drop rules except for traffic directed to the firewall's external interface and the Cleanup rule. These two rules will not result in the above mentioned drop rule issue.

Most of the implied rules are first in the ruleset. These rules mostly focus on the firewall communication traffic and these rules are automatically placed first by the Checkpoint software. The first rule the security team has created is the Stealth rule. This rule is placed at the beginning of the rule set to separate the traffic destined for the external interface of the firewall so that it can be logged properly and easily identified when the logs are reviewed. This also protects against a rule that might be mis-configured and allows traffic to hit the firewall's IP address. Since this rule is first, all traffic destined to the firewall's IP address is dropped and any mis-configured rule would not be reached.

The VPN rules are next and GIAC Enterprises expects a fair amount of VPN traffic between the regional offices and the home office. Since there is already overhead placed on the system by encrypting and decrypting all the VPN traffic, the security team attempted to lessen the load by having these rules near the top so that they can be executed in a rapid manner.

The General Rules are ordered by the services that see the most traffic. The first rule is the Syslog traffic. The company collects a vast amount of logs throughout the day and these logs are forwarded constantly through the firewall to the central Syslog server on the internal network. The firewall will be doing a majority of work on this one rule and that's why it is first in the General category. The next rule is the Web traffic. The web site is used by the company's customers, partners and the public. This web site sees a lot of hits throughout the day so it is placed second. The next busiest rule is the DNS service and this not only resolves address for the internal network, it answers requests from the internet on its domain space. This generates a lot of traffic so this service is also at the top of the list along with its corresponding internal rule. The company also expects a lot of outbound traffic from the internal users. Rule number eight allows browsing of the internet and using FTP. The NTP traffic is another protocol that sees a lot of traffic, both out to the internet and from the DMZ to the local network. The last service that expects a lot of traffic is the SMTP rule. The company relies heavily on its E-mail communications and as a result, produces a lot of E-mail traffic. Besides the last rule, the remaining rules are not expected to produce much traffic so they are near the bottom of the list.

The last rule is critical. This rule must be placed last in order to deny all traffic that has not explicitly been allowed. Without this rule all traffic except traffic to the firewall's external interface, would be allowed through. If this rule was placed higher on the list, those rules below it would never be processed and the traffic which would normally be accepted, would instead get dropped.

References

[1] SANS.org. “GIAC Certified Firewall Analyst (GCFW) Practical Assignment.” V4.0. 22 July 2004. URL: http://www.giac.org/GCFW_assignment_print.php.

[2,9,10] Lemos, Robert. “Expert: Gaps still pain BlueTooth security.” 22 April 2004. URL: http://zdnet.com.com/2100-1105_2-5197200.html.

[3] Microvision. “Flicware^{tm} Cordless Software User’s Guide for PC.” Rev A. 31 October 2003. URL: http://www.flicscanner.com/pdfs/flicware_cordless_users_guide.pdf.

[4,5,6] Whitehouse, Ollie. “War Nibbling: Bluetooth Insecurity.” October 2003. URL: http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf.

[7,8] Poulsen, Kevin. “Security Researchers Nibble at Bluetooth.” 18 June 2003. URL: http://www.securityfocus.com/news/5896.

[11] Netgear. “Wireless Networking Basics.” URL: http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm.

[12,13] Wright, Joshua. “Detecting Wireless LAN MAC Address Spoofing.” 21 January 2003. URL: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf.

[14] Cisco Systems, Inc. “Protected EAP (PEAP) Application Note.” V4.0. June 2004. URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps430/c1227/ccmigration_09186a008025d6ba.pdf.

[15,16] Geier, Jim. “WPA Security Enhancements.” 20 March 2003. URL: http://www.wi-fiplanet.com/tutorials/print.php/2148721.

[17] Microsoft. “Overview of the WPA Wireless Security Update in Windows XP.” V4.0 23 September 2004. URL: http://support.microsoft.com/?kbid=815485.

[18] Cisco Systems, Inc. “The Cisco Aironet Series – Wireless Freedom with Enterprise-class Security.” URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.pdf.

[19] Webopedia.com. “Firewall.” URL: http://www.webopedia.com/TERM/f/firewall.html.

[20] Hoagland, Jim and Staniford, Stuart. “README file for the Spade v010818.1.” V010818.1. URL: http://cvs.snort.org/viewcvs.cgi/*checkout*/snort/doc/Attic/README.Spade?rev=1.2.

[21,22] Welch-Abernathy, Dameon D. Essential Check Point^{tm} Firewall-1 NG. Boston: Addison-Wesley, January 2004. 338,99.