

# SANS Institute
# InfoSec Reading Room



## Secure Perimeter Network Design for GIAC Enterprises

This paper puts forth a secure perimeter network design for the fictional company GIAC Enterprises, which is in the business of brokering fortune cookie sayings. The paper consists of three assignments and is completed in fulfillment of the requirements of a practical exam for the GIAC Certified Firewall Analysis Certification.

# Secure Perimeter Network Design for GIAC Enterprises

Ted Franger

GCFW Practical
Version 4.1

Date: Mar. 21, 05

# Table of Contents



# List of Figures

# List of Tables

## Summary

This paper puts forth a secure perimeter network design for the fictional company GIAC Enterprises, which is in the business of brokering fortune cookie sayings. The paper consists of three assignments and is completed in fulfillment of the requirements of a practical exam for the GIAC Certified Firewall Analysis Certification.

The first assignment discusses the security of wireless network implementations, specifically in the case of a hypothetical adding of a warehouse to GIAC Enterprises, and the wireless barcode scanners and laptops that will be used. Integration with the proposed overall network design, security risks of the wireless technology chosen, techniques to mitigate said risks, and the design's overall impact on the perimeter security of the enterprise are explored.

The second assignment is a technical design for a secure perimeter network that will meet the connection needs of GIAC Enterprise's various groups of users. The overall architecture, types and functions of security and other elements, the addressing scheme and data flows are all presented.

The final assignment is a detailed discussion of the overall security stance of the enterprise, and the specific security policies of the border router and firewall.

This paper will show a practical implementation of the concept of defense-in-depth and solid network design that can be used as a model for any small to medium sized business.

# Assignment 1: Future State of Security Technology

This portion will discuss wireless technology implementation in GIAC Enterprise's hypothetical warehouse operation, what risks this entails, and how these risks can be mitigated through a sound design and defense-in-depth.

## *Abstract*

Wireless networking has expanded greatly in the last year. It was a simple technology that allows users to freely move around while doing their work. But simplicity also meant insecurity as more and more business data was flowing through these wireless connections. Since wireless networks transmit data over the airwaves, it is important to secure access and information through a combination of access control and data encryption.

This paper will explore a wireless implementation centered on a hypothetical warehouse operation for GIAC Enterprises. It will cover an implementation of Cisco's Aironet systems, using LEAP authentication, various aspects of wireless networks, their impact on network security, and the techniques that are used by leveraging Aironet products, sound design, and defense-in-depth to mitigate these risks.

## *Introduction*

GIAC Enterprises (GEnt) has hypothetically expanded its operations to include the manufacturing and distribution of fortune cookies to house the sayings that it sells. To this end, GEnt will deploy wireless scanners in their warehouse, and will use wireless-enabled laptops on the warehouse floor. We will explore the implementation of wireless technology, particularly Cisco Aironet with LEAP (Extensible Authentication Protocol, also known as LEAP – Lightweight EAP) authentication, and how we can maintain a strong perimeter defense.

## *Wireless Networking for GIAC Enterprises*

Although wireless networking takes many forms such as infrared, short-range radio (Bluetooth), and building range radio (Wi-Fi), microwave, and satellite communications, we will only concern ourselves with the local area network (LAN) equivalents used in our hypothetical design.

Wireless handheld scanners and laptops will be used on the warehouse floor as part of the overall operation. These devices will need to connect to the corporate network in order to upload and download product information to the supply chain applications, and the users will need to connect to conduct their usual business functions (e-mail, Intranet, access to application servers).

### Wireless Network Design

Adding a warehouse operation to the existing GEnt network is as simple as

adding another remote office. Connectivity to the main corporate network at the HQ will be achieved through a point-to-point VPN connection between the warehouse site's firewall and the HQ network's firewall, as given in Assignment 2 of this paper.

The difference with this deployment, however, revolves around technologies used at the site rather than how the site will connect to the rest of the network. Unlike the other remote offices, the warehouse will have a wireless network (overriding the assumption in this case only), which can introduce significant exposure of the company network if not implemented correctly. Therefore, we must ensure that the wireless portion of the warehouse network is segregated from the rest of the site, and that connections to the rest of the site are appropriately controlled. Once a connection is authorized into the site, it will be treated like any other connection originating at a remote office.

To implement the wireless network, GEnt will deploy one or more wireless access points (depending on the size of the warehouse and any interference present). Our wireless system of choice will be the Cisco Aironet system, comprised of access points and wireless cards for the laptops. The barcode scanners will be the Dolphin 7400 RF wireless handheld computer from Handheld Products (HHP). This scanner is 802.11b-compliant and is designed to work specifically with the Cisco Aironet system[1]. The laptops will also be outfitted with Cisco Aironet PC Card wireless adapters. All wireless devices will be configured to use Cisco's LEAP protocol for authentication and WEP key management. To support LEAP and the laptop's VPNs, a Cisco ACS server will be deployed on the warehouse site's internal network for RADIUS and TACACS+ authentication as appropriate. This ACS server will only be used for the wireless environment and will be separate from the corporate ACS server used at the HQ for remote access.

The access point(s) will be deployed around the warehouse floor to give acceptable coverage of working areas. The ethernet connections from the access points (AP) will connect to a switch (is more than one AP is used), which will be logically located in a 'wireless DMZ'. The original specification for firewalls at the remote site does not have any extra interfaces, so a Cisco PIX 515E will need to be used. The firewall will allow the TN3270 (telnet) traffic from the scanners to a collection server inside the remote office's network, which will in turn connect with the application servers at the HQ through the normal remote office VPN connection. The laptops will use the standard VPN client to connect into the firewall VPN on the wireless interface and will be given the same access as any other remote user (e-mail, applications, web surfing, but not open access to the entire network).

## *Wireless Networking Security Issues*

[1] The Dolphin 7400 RF barcode scanners use a Cisco Aironet PC card as their wireless antenna, which has LEAP functionality built into it. (Handheld Products 5-2)

**Wireless Overview**

Wireless networking depends on energy transmitted through the air as a means to connect devices together. This energy takes the form of infrared or radio waves. Each has its benefits and risks that need to be explored if their use is to be used securely in a business environment.

Wireless networking removes the physical media of the traditional LAN and replaces it with infrared/radio waves. This freedom from physical media also allows anyone within range to pick up the signal, however. Wireless allows connections anywhere in the radius where signal strength is strong enough for a consistent connection. This is significant when compared to traditional wired LANs for a few reasons; 1) You no longer need to physically plug in a wire to connect to the network; 2) The places you can connect to the LAN from are no longer bounded by physical walls and locked doors; and 3) The connection area is now three dimensional – extending up and down in addition to side to side. These characteristics have a profound effect on securing wireless networks because you remove the ability to physically secure the connection media. As such, you must rely on other means to restrict access. 802.11 wireless has a nominal range of around 300 feet[2], with walls and metal structures interfering with the maximum range by attenuating the signal strength. It would be nice to have a restricted area out to the maximum range around your facility, but this is not always possible so we must look to other techniques for securing the wireless network.

**Wireless Security Issues**

Foremost among the wireless security issues is the inability to physically keep people from accessing the medium, since the medium is being broadcast in three dimensions. Unless you are a government/military facility that can implement TEMPEST[3] measures, or can control complete access to your facilities, you must use other security controls to prevent compromise of your network.

Default configurations of wireless networks typically have several 'features' that make them easy to set up. The SSID (service set identifier), or node name is broadcast so that others can easily find the network. In addition, the network is unencrypted, to allow the maximum usage by all. As you can see, these features also make it quite easy to find and connect to a wireless network, even if you are not meant to.

To return some modicum of 'physical' protection to the network, the WEP (wired equivalent privacy) protocol sought to encrypt the wireless traffic so that others

[2] Range according to product data from D-Link (D-Link 1), Zoom Technologies (Zoom 1), and Dealtime.com (Viewsonic WAPBR-100 802.11g/b Wireless Access Point)

[3] According to John Pike of the Federation of American Scientists "TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations." Facilities can be shielded from emissions by various techniques, all of which are expensive.

may not see it. WEP uses a set of pre-shared keys to set up this encryption. Due to problems with the algorithm with initialization vector (IV) collisions (Borisov), WEP is not as secure as initially thought. Encrypted traffic can be captured and analyzed, and the more IV collisions that are detected, the higher the probability is of statistically analyzing the collision traffic and deducing the key. Hence, the longer a given key is in use, the higher the probability that it can be cracked. If the WEP key is cracked, an attacker can then use it to connect to a WEP-enabled network.

To add an additional layer of physical access control to wireless networks, Media Access Control (MAC) address authentication was used. MAC addresses are the OSI Layer 2 addresses of network cards, and are preset by manufacturers with each one unique to that card. The wireless access point would be set with a list of authorized MAC addresses and accept connections from only those addresses. The problem lies in the fact that wireless connection utilities, such as Kismet or NetStumbler, along with packet sniffers such as Ethereal or Ettercap, allow an attacker to sniff wireless traffic, capture a valid MAC address and use it to connect to the network.

In the following section we will discuss ways to mitigate these vulnerabilities in wireless networks, and specifically in GEnt's design.

## *Mitigating Threats to GEnt's Wireless Network*

The first method we will use to mitigate threats to the wireless portion of the network is to disable the broadcast of the SSID on all access points. Authorized users will be given the SSID to set up their network cards with, so there is no need to broadcast it. Disabling the broadcasts will not keep the SSID hidden, however, as it is still used when connecting to the network and can be readily sniffed if passed in the clear. But disabling the SSID will prevent easy identification of the network by attackers, making their job that much more difficult.

Enabling WEP will protect the network and its traffic for a while, depending on the amount of traffic flowing through the network (and the corresponding chance of an IV collision). WEP keys can be generated and manually rotated after a given time, which will cut down on the chance of an individual key being compromised, but this is a labor-intensive effort.

Another option to protecting the network is to leave the wireless portion open but require a VPN with access control to connect to the firewall and the rest of the network. This poses problems in two areas. First, it requires devices sharing the wireless portion of the network to protect themselves from each other with a personal firewall. This is fine for the laptops, but as GEnt is using wireless barcode scanners that may not have this option (while the barcode scanners use Windows CE on a proprietary or Pocket PC handheld computer, firewall software may not be compatible with the particular implementation[4]), only some

of the devices would be protected. Second, it requires a full-featured VPN client to be running on the devices, which again may not be available for the barcode scanners.

As discussed before, straight MAC address authentication only slightly complicates an attacker's efforts to breach a network, and can easily be compromised. Cisco Aironet products utilize a Cisco proprietary authentication method known as EAP[5]. This method uses a RADIUS username and password to authenticate a device to the network. The password is used in a challenge-response hash according to the EAP protocol, so the password is not passed in the clear. The EAP authentication process then issues a unicast session WEP key, used only for that device and that session, which encrypts the traffic and allows access to the network. This allows the key to be changes with each session, and greatly reduces (but not totally mitigates) the chances of compromising the key. Given some luck and capturing the correct frames, an attacker could still crack the WEP key, but the probability is relatively slim.

The barcode scanner users will be given a username and password to use in authenticating to RADIUS for connections to the network. This username and password is entered into the Wireless Login Module of the Dolphin to allow LEAP to function. As stated before, the laptops will use LEAP and the company VPN to authenticate to the network and protect their traffic.

LEAP does have one vulnerability in that a weak password used in the authentication routine can be captured and brute forced offline if enough processing power and time are available to the attacker (this is a vulnerability with any reused password authentication scheme). There currently is no way around this as the scanners are not able to use any form of PKI authentication at this time. To mitigate this, we will pick strong, long (10+ character) passwords and change them regularly.

## *Impact on Perimeter Security*

Wireless can be a great boon to business productivity, but can also be a significant risk to perimeter security. Left in its user-friendly state, wireless networks can compromise any perimeter security measures as easily as a modem that accepts inbound calls without authentication can. By deploying wireless in as secure a manner as possible, we can ensure the network perimeter maintains a strong defensive posture.

As previously mentioned, there is no physical control over the wireless medium. Baring physical control, we must implement measures of authentication and encryption to protect access to the network and protect the data flowing through it. Through a combination of segregating the wireless network 'outside' the site

[4] An example of a Windows CE firewall is the AirScanner Mobile Firewall
[5] Cisco Aironet 1200 Series Access Point Installation and Configuration Guide, 12.2(8)JA, 10-4

network, controlling access to the network through robust authentication methods, encrypting network traffic to maintain its confidentiality, and allowing access from the wireless systems to only the necessary services on the site network, we can achieve a sufficient amount of security that will ensure the wireless network is not the weak point in the network perimeter.

# Assignment 2: Security Architecture

GIAC Enterprises (GEnt) markets fortune cookie sayings to customers world-wide, with a headquarters and four satellite offices. There are approximately 50 employees, and the company offices, as well as its partners, connect via the Internet. This section will discuss a possible architecture to secure their perimeter and information.

## *Assumptions*

In a normal business environment, the architecture for the company's network and security will be formed through many meetings and discussions, as well as the evolving business needs. Since this cannot be done actively (the company exists only on paper), the following assumptions were made while designing this architecture:

- Business needs are assumed to only be centered on the conduct of commerce around the buying, selling, and distribution of fortune cookie sayings. Any other aspects of the business (no matter what they may be) are out of scope and not covered by this design.
- The fortune cookie sayings are the company's lifeblood and must be protected from exposure to unauthorized persons
- The company is a small to medium business and thus will not need every security product known to man. Where possible, the design will use components appropriate to a small to medium sized business, and will use free components where possible.
- No EDI (electronic data interchange) e-commerce was to be conducted over the Internet. Payment would be made through invoices and out-of-band payment methods, or through web page submissions (i.e., credit cards). Database to database or other types of EDI transmissions are not used.
- All remote offices will not allow direct employee connectivity to the Internet. All company use of the Internet will pass through the HQ site. The firewall will be connected to the Internet (through a border router) but will only allow VPN connections to the HQ site and all employee traffic will be routed through these connections.
- Remote offices are assumed to not have any infrastructure servers. All company services (mail, intranet, etc.) will be hosted at the HQ site. Remote offices will not have wireless networks, nor will they have other means of connection to the Internet (modems, etc.).
- All remote access from the field via VPN would only be to the HQ VPN
- Application-level security will not be discussed past the function that such security will provide (such as segregating user access into only specific directories, or application-level authentication). It is assumed that all internal applications will require separate logon credentials from other logon sources for access.

- All servers, unless otherwise noted, are running Windows 2000 server

## *Access Requirements*

GIAC Enterprises has several diverse groups that require access to portions of the network to conduct their business. Each of these groups and their access requirements are detailed below. All groups are assumed to need access to public information on the public web server and external DNS server, as well as send e-mail to GEnt.

### Customers

Customers are companies or individuals that purchase bulk fortunes online. These entities interact with GEnt through order placement and fulfillment. Customers will have access to the web portion of the extranet server (used as a secure server ordering, payments, and for downloading purchased files of sayings).

### Suppliers

Suppliers are companies that produce the bulk fortune cookie sayings. GEnt will get their sayings from these companies to then send on to their customers. GEnt may retrieve them from the company, or the company may deposit them on GEnt systems. Since the sayings are GEnt's products, and thus represent revenue, these transfers must be done securely. Rather than setting up VPN clients at all the suppliers, our design will rely on the freely available SSH/SFTP client PuTTY to make transfers to the extranet server, or through file downloads via HTTPS. Suppliers will also have access to the web portion of the extranet server.

### Partners

Partners are companies that translate the fortune cookie sayings into other languages, as well as those that sell fortunes to other markets. Partners will need access to the files on the extranet server so that they can download sayings and upload translated files through SSH/SFTP or HTTPS. Partners will also have access to the web portion of the extranet server.

### Employees

Employees connect to the GEnt network both in the offices and from the field (covered below). In addition, the various remote offices connect to the HQ office through a point-to-point VPN over the Internet. Employees have much more access than other groups to resources and information, as they are more trusted than other groups. Employees in the offices will have complete access to all internal network systems (although not systems on the DMZs except for administrators).

### Sales/Teleworkers

Employees do not only connect to company resources while in the various offices. Sales people in the field, as well as teleworkers working from home require access to GEnt information and resources to do their jobs. Employees who VPN in from the field will have access to the infrastructure servers (mail, intranet, application, etc.) but not to the entire internal network as a security precaution. Administrators will have access to the entire network.

### General Public

The general public requires limited access to GEnt resources to get information on the company, its products and services, and to correspond with the company for various reasons. This group has the least requirements for access, and the information they access is completely non-sensitive. The General Public will only have access to the public web server.

## *Data Flows*

Below are detailed the data flows necessary to allow the access that the various servers and groups require to GEnt information resources.

Table 1 depicts all data flows into the network from the Internet, within each zone, and from zone to zone in an inbound direction.

**Table 1: Data Flow - Inbound Internet Connections**

| Source | Destination (Inbound) | Port(s)/Protocol | Description |
|---|---|---|---|
| **Internet to Public DMZ** | | | |
| Internet (any) | Inbound Proxy | 80/TCP (HTTP)<br>80/UDP (HTTP) | Access to general company information and basic product information |
| Internet (any) | Mail Relay | 25/TCP (SMTP) | E-mail to mail relay |
| Internet (any) | DMZ DNS Server | 53/UDP (domain) | Name resolution for DMZ hosts |
| Remote Office Firewall | Firewall (VPN Termination) | 500/UDP (IKE) | Key negotiation for site to site VPN |
| Remote Office Firewall | Firewall (VPN Termination) | IP 50 (ESP) | Site to site VPN encrypted traffic |
| Teleworkers (Internet) | Firewall (VPN Termination) | 500/UDP (IKE) | Key negotiation for client to site VPN |
| Teleworkers (Internet) | Firewall (VPN Termination) | IP 50 (ESP) | Client to site VPN encrypted traffic |
| **Within Public DMZ** | | | |
| Inbound Proxy | Public Web Server | 8080/TCP (HTTP)<br>8080/UDP (HTTP) | Backend connection from proxy to web server, preventing direct connections to the web server from the Internet. |
| **Internet to Extranet DMZ** | | | |
| Customers | SSL Proxy | 443/TCP (HTTPS) | Customer access for purchasing and downloading product files. Forwards connection on through separate SSL connection to the Secure Server, preventing direct access to the server from the Internet. |
| Suppliers | Extranet Server | 443/TCP (HTTPS) | Supplier access for product information (such as requests for more sayings by GEnt) |
| Suppliers | Extranet Server | 22/TCP (SSH) | Supplier access for uploading product files |
| Partners | Extranet Server | 443/TCP (HTTPS) | Partner access to web server to view online catalog and place orders |
| Partners | Extranet Server | 22/TCP (SSH) | Supplier access for uploading product files |

| Source | Destination (Inbound) | Port(s)/Protocol | Description |
|---|---|---|---|
| **Within Extranet DMZ** | | | |
| SSL Proxy | Secure Server | 8443/TCP (HTTPS) | Backend connection from proxy to web server, preventing direct connections to the web server from the Internet. Done over another SSL link to prevent sniffing of payment data on the Extranet DMZ network. |
| **Public DMZ to Internal Network** | | | |
| Mail Relay | Internal mail server | 25/TCP (SMTP) | Inbound e-mail from relay to internal mail server |
| DMZ DNS | Internal DNS | 53/UDP (domain) | DNS query responses from internal DNS |
| Public DMZ | CSAMC | 5401/TCP<br>5401/UDP | Cisco Security Agent communications with CSA Management Console (CSAMC) |
| Public DMZ | Central Syslog Server | 514/UDP (Syslog) | HIDS syslog feed to central server for log consolidation |
| **Extranet DMZ to Database DMZ** | | | |
| Extranet server | Database Server | 1433/TCP (SQL) | Backend connection with database for partners and suppliers |
| Secure server | Database Server | 1433/TCP (SQL) | Backend connection with database for customers purchasing files |
| **Extranet DMZ to Internal Network** | | | |
| Extranet DMZ | Central Syslog Server | 514/UDP (Syslog) | HIDS syslog feed to central server for log consolidation |
| Public DMZ | CSAMC | 5401/TCP<br>5401/UDP | Cisco Security Agent communications with CSA Management Console (CSAMC) |
| **Database DMZ to Internal Network** | | | |
| Database DMZ | Central Syslog Server | 514/UDP (Syslog) | HIDS syslog feed to central server for log consolidation |
| Database DMZ | CSAMC | 5401/TCP<br>5401/UDP | Cisco Security Agent communications with CSA Management Console (CSAMC) |
| **Firewall to Internal Network** | | | |
| Firewall | Cisco Secure ACS Server | ICMP (all) | Required by ACS |
| Firewall | Cisco Secure ACS Server | 49/TCP (TACACS+) | AAA functions |
| Firewall | Cisco Secure ACS Server | 1645/UCP (RADUIS) | AAA functions |
| Firewall | Cisco Secure ACS Server | 1812/UCP (RADUIS) | AAA functions |
| Firewall | Cisco Secure ACS Server | 1813/UCP (RADUIS) | AAA functions |
| Firewall | Central Syslog Server (internal network) | 514/UDP (Syslog) | Firewall syslog feed to central server for log consolidation |
| **Remote Office VPN to Internal Network** | | | |
| Remote Office IPs | Internal Network | Any | Open access for remote offices through VPN connections |
| **Teleworker VPN to Internal Network[6]** | | | |
| Teleworkers (general) | Intranet Server | 80/TCP (HTTP)<br>80/UDP (HTTP) | Web access to Intranet Server |
| Teleworkers (general) | Intranet Server | 443/TCP (HTTPS)<br>443/UDP (HTTPS) | Web access to Intranet Server |
| Teleworkers (general) | Application Server(s)[7] | 80/TCP (HTTP)<br>80/UDP (HTTP) | Web access to designated application servers (based on access group) |
| Teleworkers (general) | Application Server(s) | 443/TCP (HTTPS)<br>443/UDP (HTTPS) | Web access to designated application servers (based on access group) |
| Teleworkers (general) | Internal DNS | 53/UDP (domain) | Access to internal DNS for name resolution |

[6] This access will be controlled by AAA functionality based on the teleworker's login ID and not directly through firewall rules.

[7] Access groups will be set up based on the role of the teleworker who logs in (based on their login ID). The group will give them access to only what they need in the way of application servers.

| | | | |
|---|---|---|---|
| Teleworkers (general) | Mail Server | 110/TCP (POP3) | Access for mail clients to company e-mail server |
| Teleworkers (administrators) | Internal Network | Any | Open access for administrators through VPN connections |
| **Teleworker VPN to Public DMZ[8]** | | | |
| Teleworkers (general) | Outbound Proxy | 8080/TCP (HTTP)<br>8080/UDP (HTTP) | Teleworker access to Internet |
| Teleworkers (general) | Outbound Proxy | 8443/TCP (HTTPS)<br>8443/UDP (HTTPS) | Teleworker access to Internet |
| **Remote Office VPN to Public DMZ** | | | |
| Remote Office IPs | Outbound Proxy | 8080/TCP (HTTP)<br>8080/UDP (HTTP) | Remote Office access to Internet |
| Remote Office IPs | Outbound Proxy | 8443/TCP (HTTPS)<br>8443/UDP (HTTPS) | Remote Office access to Internet |

Table 2 depicts all data flows out of the internal network to the other zones, as well as out to the Internet.

**Table 2: Data Flow – Outbound Internal Network Connections**

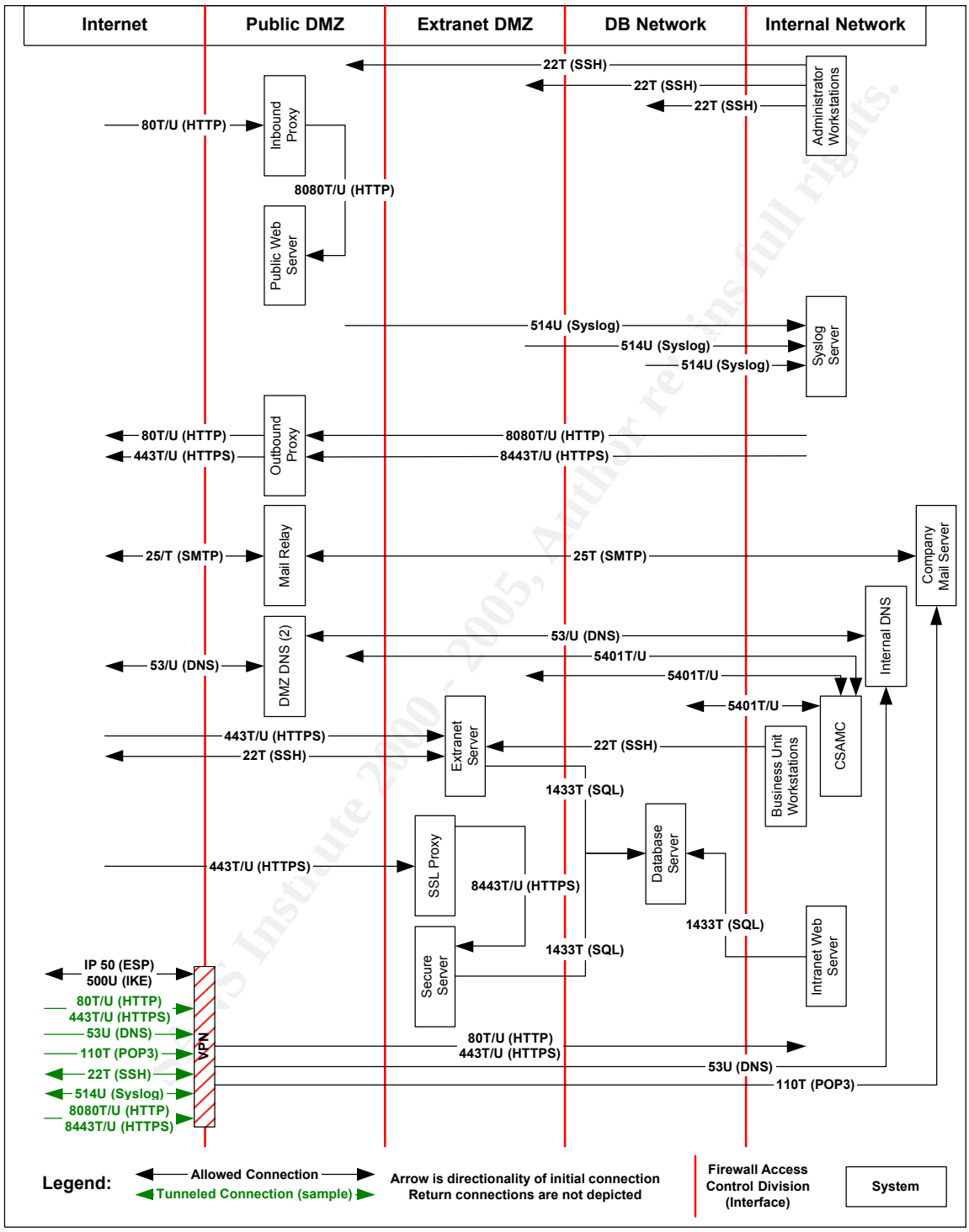
| Source | Destination (Outbound) | Port(s)/Protocol | Description |
|---|---|---|---|
| **Internal Network to Database DMZ** | | | |
| Intranet Web Server | Database Server | 1433/TCP (SQL) | Backend connection with database for internal users |
| Administrator workstation(s) | Database DMZ | 22/TCP (SSH) | Management connection for Database DMZ systems |
| **Database DMZ to Extranet DMZ** | | | |
| None[9] | | | |
| **Internal Network to Extranet DMZ** | | | |
| Business unit workstations | Extranet Server | 22/TCP (SSH) | SSH to extranet server as relay for SSH/SFTP connections to suppliers/partners for file transfer |
| Administrator workstation(s) | Extranet DMZ | 22/TCP (SSH) | Management connection for Extranet DMZ systems |
| CSAMC | Extranet DMZ | 5401/TCP<br>5401/UDP | Cisco Security Agent communications with CSA Management Console (CSAMC) |
| **Internal Network to Public DMZ** | | | |
| Internal Network (any) | Outbound Proxy | 8080/TCP (HTTP)<br>8080/UDP (HTTP) | HTTP requests from internal network browsers |
| Internal Network (any) | Outbound Proxy | 8443/TCP (HTTPS)<br>8443/UDP (HTTPS) | HTTPS requests from internal network browsers |
| Internal mail server | Mail Relay | 25/TCP (SMTP) | Outbound e-mail to relay from internal mail server |
| Internal DNS | DMZ DNS | 53/UDP (domain) | Forwarded DNS queries from internal clients |
| Administrator workstation(s) | Public DMZ | 22/TCP (SSH) | Management connection for Public DMZ systems |
| **Public DMZ to Internet** | | | |
| Outbound Proxy | Internet (any) | 80/TCP (HTTP)<br>80/UDP (HTTP) | HTTP requests from internal users through proxy |
| Outbound Proxy | Internet (any) | 443/TCP (HTTPS) | HTTPS requests from internal users through proxy |
| Mail Relay | Internet (any) | 25/TCP (SMTP) | Outbound e-mail from mail relay |
| DMZ DNS Server | Internet (any) | 53/UDP (domain) | DNS query responses to Internet hosts |
| Firewall (VPN Termination) | Remote Office Firewall | 500/UDP (IKE) | Key negotiation for site to site VPN |
| Firewall (VPN Termination) | Remote Office Firewall | IP 50 (ESP) | Site to site VPN encrypted traffic |

[8] This access will be controlled by AAA functionality based on the teleworker's login ID and not directly through firewall rules.
[9] No connections will be originated from the Database DMZ to any other zones. All connections will be to the database, not from it.

| | | | |
|---|---|---|---|
| Firewall (VPN Termination) | Teleworkers (Internet) | 500/UDP (IKE) | Key negotiation for client to site VPN |
| Firewall (VPN Termination) | Teleworkers (Internet) | IP 50 (ESP) | Client to site VPN encrypted traffic |
| **Extranet DMZ to Internet** | | | |
| Extranet Server | Suppliers | 22/TCP (SSH) | GEnt access for transferring product files |
| Extranet Server | Partners | 22/TCP (SSH) | GEnt access for transferring product files |
| **Internal Network to Firewall** | | | |
| Administrator workstation(s) | Firewall | 22/TCP (SSH) | Management connection for firewall |
| Cisco Secure ACS Server | Firewall | ICMP (all) | Required by ACS |
| Cisco Secure ACS Server | Firewall | 49/TCP (TACACS+) | AAA functions |
| Cisco Secure ACS Server | Firewall | 1645/UDP (RADUIS) | AAA functions |
| Cisco Secure ACS Server | Firewall | 1812/UDP (RADUIS) | AAA functions |
| Cisco Secure ACS Server | Firewall | 1813/UDP (RADUIS) | AAA functions |
| **Internal Network to Remote Office VPN** | | | |
| Internal Network | Remote Office IPs | Any | Open access for remote offices through VPN connections |

Figure 1, on the next page, depicts the connections from each network zone or server to other zones or servers in support of these data flow requirements. Flows are depicted by arrowed connections (with the arrow signifying the directionality of the initial connection) between systems and zones. Systems are depicted as boxes, while zones are depicted with the arrow terminating in that zone (signifying access to the entire zone). The firewall interfaces are depicted with red boundary lines dividing the zones. Note, a connection must start or end in a zone to be from/to that zone. Merely passing through does not imply access to that zone.

**Figure 1: Data Flow Depiction**



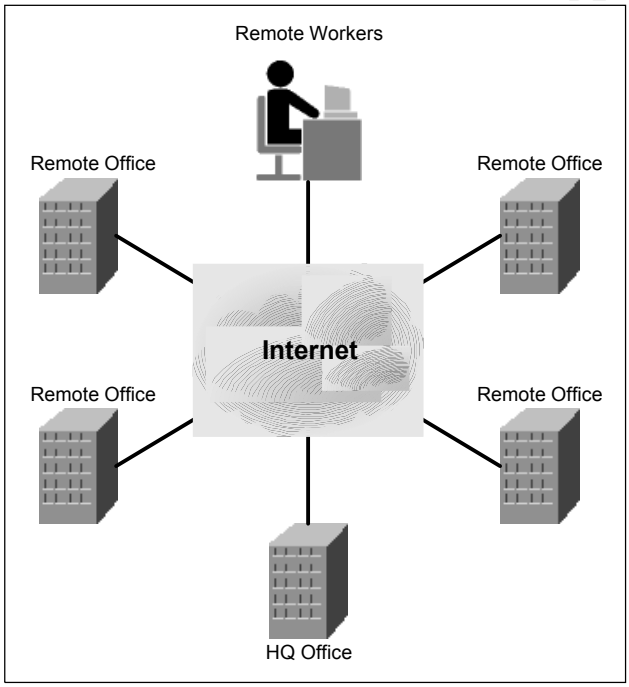
## *Overall Network Topology*

The overall network topology for the company is a hub-and-spoke design using the Internet as the company's Wide Area Network (WAN). This is accomplished by using VPNs from each remote office 'spoke' to the central 'hub' of the HQ office. With a company this size, there is no need to implement a fully meshed design between the offices since all network services are housed at the HQ. Thus, the various offices do not need to communicate directly with each other.

Remote users in the field or at home (teleworkers) will also communicate with the central HQ for all their work needs. Teleworkers will only have access to infrastructure servers (e-mail, intranet, and application servers), however, as a security precaution.

The HQ network topology segregates the public, extranet, and database resources in separate DMZs. The firewall is used to control access to each segment and protects the other segments if a system on one segment is compromised.

**Figure 2: High-level Company Network Overview**



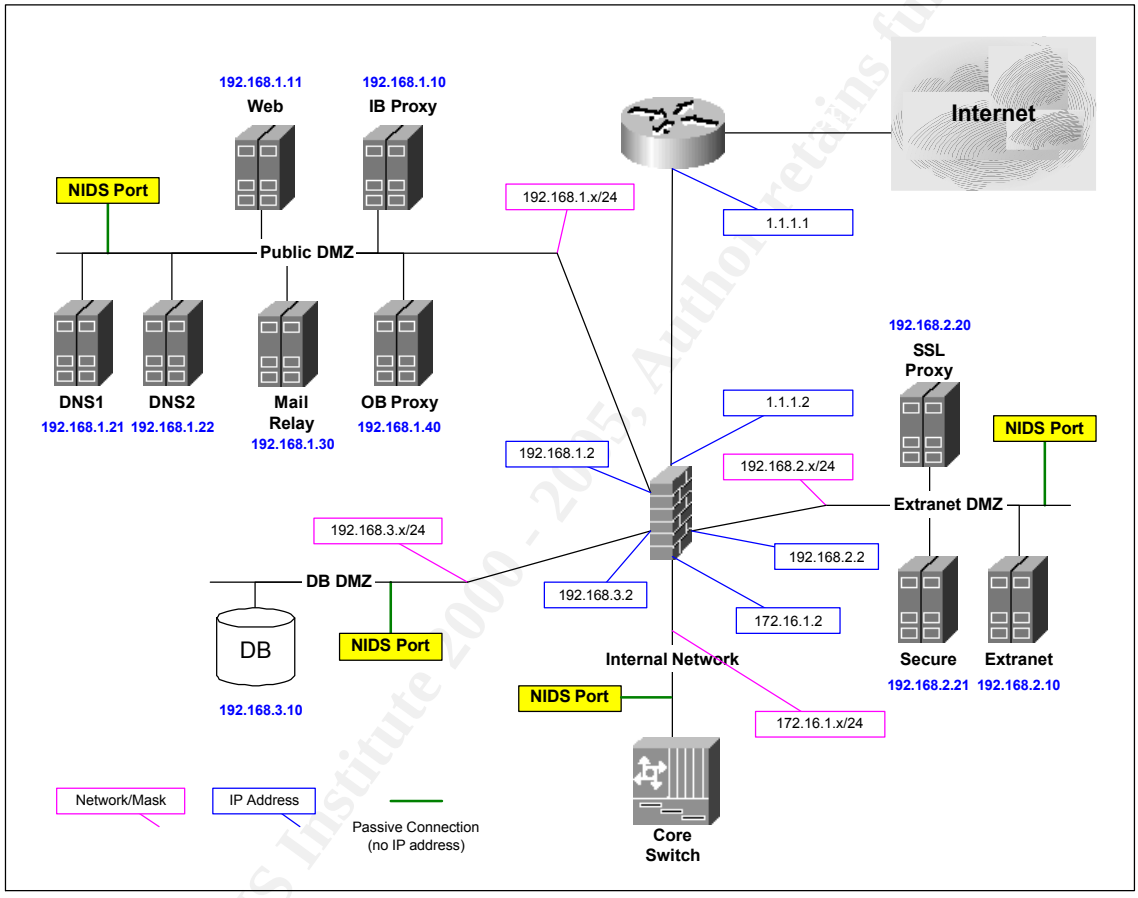

Since the database houses the company's sensitive information (the fortunes), our design puts it on its own DMZ. This placement accomplishes three objectives: 1) Not allowing the database to be directly accessed by anyone outside of GEnt's corporate network; 2) Protecting the database server by controlling access from internal users using the intranet web interface; and 3)

Allowing controlled access to the database server from the partners and customers using the extranet web interface.

## *Network Diagram*

The following diagram depicts the design for a secure perimeter at the GEnt HQ site.

**Figure 3: Detailed Network Architecture of HQ Perimeter Network**



## *IP Addressing Scheme*

To protect the internal resources, GEnt will use a public-private addressing scheme for all internal and DMZ systems. All publicly-accessible systems will have Internet-routable public addresses.

Inside the firewall, only RFC 1918 private addresses will be used (Rekhter, et al.). Systems in the DMZ will have their addresses translated to public Internet addresses through Network Address Translation (NAT) at the firewall. This will allow GEnt to purchase only a limited number of public Internet addresses, while having a large number of internal addresses at their disposal. In addition, there are certain techniques that can be used with NAT and its sister PAT (Port Address Translation) to effectively mask the real number of internal systems in the DMZ.

The addressing scheme is given in Table 3 below.

**Table 3: Network Addressing Scheme**

| Device/Network | Network/Mask | Interface | Address |
|---|---|---|---|
| **Public IPs[10] and Firewall** | | | |
| Border router | NA | ISP interface | Serial[11] |
| Border router | 1.1.1.0/24 | Internal interface | 1.1.1.1 |
| Firewall | 1.1.1.0/24 | External interface | 1.1.1.2 |
| Firewall | 192.168.1.0/24 | Public DMZ Interface | 192.168.1.2 |
| Firewall | 192.168.2.0/24 | Extranet DMZ Interface | 192.168.2.2 |
| Firewall | 192.168.3.0/24 | Database DMZ Interface | 192.168.3.2 |
| Firewall | 172.16.1.0/24 | Internal Interface | 172.16.1.2 |
| Reserved for servers (NAT-see below) | 1.1.1.0/24 | | 1.1.11.3-254 |
| **Public DMZ** | | | |
| Inbound proxy server | 192.168.1.0/24 | NIC | 192.168.1.10<br>1.1.1.10 (NAT) |
| Public web server | | NIC | 192.168.1.11 |
| DMZ DNS server 1 | | NIC | 192.168.1.21<br>1.1.1.21 (NAT) |
| DMZ DNS server 2 | | NIC | 192.168.1.22<br>1.1.1.22 (NAT) |
| Mail relay | | NIC | 192.168.1.30<br>1.1.1.30 (NAT) |
| Outbound proxy server | | NIC | 192.168.1.40<br>1.1.1.40 (NAT) |

[10] 1.1.1.x is used as a placeholder representing sanitized Internet-routable public addresses
[11] The serial interface on the border router is assigned according to the type of connection to the upstream ISP at that point-of-presence (ATM, Frame Relay, etc.)

| Device/Network | Network/Mask | Interface | Address |
|---|---|---|---|
| **Extranet DMZ** | | | |
| Extranet server | 192.168.2.0/24 | NIC | 192.168.2.10<br>1.1.1.130 (NAT) |
| SSL Proxy | | NIC | 192.168.2.20<br>1.1.1.140 (NAT) |
| Secure server | | NIC | 192.168.2.21 |
| **Database DMZ** | | | |
| Database server | 192.168.3.0/24 | NIC | 192.168.3.10 |
| **Internal Networks** | | | |
| Internal Network – HQ | 172.16.1.0/24 | | |
| Internal Network – Remote Office 1 | 172.16.2.0/24 | | |
| Internal Network – Remote Office 2 | 172.16.3.0/24 | | |
| Internal Network – Remote Office 3 | 172.16.4.0/24 | | |
| Internal Network – Remote Office 4 | 172.16.5.0/24 | | |
| VPN Users (teleworkers) | 10.1.1.0/24 | | |

## *Architecture Components*

This section details the roles of various architecture components in the overall perimeter defense scheme. Each device will have its primary function listed, and how it integrates into the overall defense-in-depth strategy.

The table below covers the architecture components, their functions, and their security roles for all elements used in this design. Following the table are more in-depth descriptions of each component, and discussions of their individual strengths, weaknesses, and mitigating factors that can be used to lessen the risk brought on by their weaknesses.

**Table 4: Architecture Components and Roles**

| Component | Primary Role | Security Function(s) | Threats Mitigated |
|---|---|---|---|
| **Border routers** | • Provide connectivity to upstream ISP | • Basic ingress filtering for known malicious traffic<br>• Egress filtering for internal addresses and non-standard traffic | • SYN Flood Defense to/from Internet<br>• Leak of internal addresses to Internet<br>• Prevention of propagation of spoofed RFC 1918 source addresses |

| | | | |
|---|---|---|---|
| **Firewall** | • Access control to company network<br>• VPN connectivity for remote offices and teleworkers (see below) | • Block all inbound traffic not specifically authorized<br>• Block all outbound traffic not specifically authorized<br>• Segregates extranet web server and database server from other zones (DMZ, Internet, and internal) | • Unauthorized access to company systems from the Internet<br>• Prevent spread of successful attack against accessible systems to database<br>• Prevent direct access to database from internal network (insider threat) |
| **Firewall VPN Function** | • Functions as WAN for company's remote offices<br>• Allows remote access to network from teleworkers in the field | • Segregate access through user groups to allow unrestricted access to remote offices, and only infrastructure access to teleworkers<br>• Encrypt traffic between offices/teleworkers and network to protect from sniffing | • Allows remote access to network by only authorized entities<br>• Eavesdropping of corporate network traffic from outlying entities |
| **Inbound Proxy** | • Caching of web pages for quicker access<br>• Proxies all connections from the Internet to the public DMZ systems | • Reduction of load for public web server<br>• Reconstructs and forwards connections from the Internet to the public DMZ systems<br>• Provides extra level of logging for incoming web connections | • Mitigates fragmentation, protocol-, and OS-based attacks on the web server |
| **Public Web Server** | • Presents public information about the company to viewers on the Internet | • None – public access is available to all data on this web server | • Hardening of web server mitigates web and web server vulnerabilities |
| **DMZ DNS Server** | • Resolves DNS queries for accessible systems in the Public and Extranet DMZs | • Provides information only on accessible systems, preventing connections by hostname to protected systems | • Hardening server mitigates reconnaissance of DMZ systems, Cache poisoning, and DNS spoofing |
| **Mail Relay** | • Proxies mail inbound and outbound from the company | • Prevent direct access to company mail system<br>• Checks incoming and outgoing mail for viruses or dangerous attachments<br>• Content filtering of e-mails | • Attacks on the mail server<br>• E-mail virus propagation (inbound and outbound)<br>• Legal or regulatory compliance for e-mail content (sexual harassment, etc.) |
| **Outbound Proxy** | • Proxies all connections from internal network to the Internet | • Provides access control for connections originating on the internal network<br>• Reconstructs and forwards connections from the internal systems to the Internet | • Prevents unauthorized connections over authorized ports from reaching the Internet<br>• Mitigate fragmentation and other protocol or OS-level attacks originating within the company |
| **SSL Proxy** | • Proxies customer connections to the secure server<br>• Caching of web pages for quicker access | • Reconstructs and forwards connections from the Internet to the secure server<br>• Provides extra level of logging for incoming web connections | • Mitigates fragmentation, protocol-, and OS-based attacks on the secure web server |

| | | | |
|---|---|---|---|
| **Extranet Web Server** | • Presents web front-end for partner and customer applications | • Prevents direct access to the database server by partners | • Attacks on the database or database server<br>• Unauthorized queries to the database |
| **Secure Web Server** | • Presents web front-end for customer application | • Prevents direct access to the database server by customers | • Attacks on the database or database server<br>• Unauthorized queries to the database |
| **Database Server** | • Holds product information (fortunes) and order/fulfillment information | • Prevents access to company sensitive information through database controls (permissions and stored procedures) | • Access to company sensitive information |

## Filtering Router(s)

Filtering routers serve as the initial screen for the Internet connection. Since a router's job is to efficiently route traffic, it should not be overburdened with packet inspection, although there are some kinds of known malicious traffic that can efficiently be blocked by the router. The routers will prevent known spoofed traffic (filtering RFC 1918 private addresses and RFC 2827 filtering (Ferguson and Senie)) from entering the network, and will be the first filter for Denial-of-Service attacks. By blocking this traffic early, it relieves the burden of filtering from the firewall.

GEnt will use Cisco 1800 series routers for their border routers at each location. One interface will connect to the ISP through the point-of-presence, and the other will connect to the perimeter architecture. The Cisco 1800 series router allows for modular WAN connections so that it can be adapted for whatever connectivity may be needed at the locality. The routers also provide appropriate bandwidth and processing for a small to medium business without undo cost.

A terminal server connected to the console port of the router will be used to manage the border router. The terminal server will be deployed on the internal network and will use TACACS+ to authenticate connections via SSH for administrator access. Once the administrators are connected to the terminal server, they can manage the router just as if they were physically connected to the console port. This will prevent the need for a listening service on the router (on either interface) for administrative services.

**Table 5: Strengths, Weaknesses, and Mitigation – Filtering Routers**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Cannot perform stateful inspection on packets, but are very efficient at filtering based on source or destination IP addresses. Thus they can be used to filter out known bad traffic (such as RFC 1918 source addresses arriving on the Internet interface). | • Outer routers are, by necessity, accessible to the public. This makes them prime targets for attack.<br>• Routers can give be vulnerable to poisoning of various functions (routing tables, arp caches, etc.) | • Harden the router against known threats (i.e. disable unneeded services, allow SSH access instead of telnet, etc.)<br>• Configure the router so that all interactions with foreign systems (such as BGP to the ISP routers) are secure and authenticated if possible<br>• Configure router to block common DoS attacks (i.e., Floodguard)<br>• Test router security using tools such as RAT (Router Assessment Tool) to determine residual vulnerability |

## Firewall(s)

Firewalls are the gatekeeper for the network. They permit or deny traffic into and out of the GEnt network based on a series of rules. The firewall will be the main choke point for all traffic through the Internet connection. The firewall will prohibit all traffic not specifically allowed to DMZ systems, and will also prohibit outbound connections that do not originate from the proxy server or other specifically designated systems. Outbound control will prevent some worms and Trojans from contacting their masters out on the Internet.

GEnt will use a Cisco PIX 515E firewall (with the 515-UR license) at the headquarters site and PIX 506E firewalls at each remote site. The 515 has the required number of interfaces to enable the DMZ design given, while the 506Es are for small/remote offices and do not need any extra interfaces. Both models are capable of creating the VPN tunnels needed to form the company WAN.

**Table 6: Strengths, Weaknesses, and Mitigation – Firewalls**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Deep packet inspection for more than just source and destination addresses. Can track connections to prevent spoofing of connection establishment.<br>• Can dynamically allocate return ports for connections, so that you don't have to have a large range of ports open to accommodate dynamic protocols (FTP, HTTP, etc.)<br>• Can automatically add dynamic rules in response to detected threats as part of an integrated threat defense system | • May be overwhelmed by DoS traffic, thus preventing access to/from the Internet<br>• Complicated protocols can lead to improper rules if specialized tools are not used (i.e. fixup commands in Cisco products) | • Use upstream routers to filter DoS traffic before it gets to the firewall. Also turn on any available DoS mitigation on the firewall.<br>• Use available tools to accommodate complicated connections without compromising overall security<br>• Test firewall with packet crafting software to make sure ruleset functions as intended |

## VPN(s)

Virtual Private Networks (VPNs) will be used to leverage the world-wide Internet in connecting GEnt offices and workers with the company's resources in a secure manner. Given the small size of the enterprise, this will lessen the overall cost by not requiring private leased lines. Both site-to-site and client-to-site VPNs will be used. The VPN will prevent others on the Internet from intercepting company traffic.

The models of routers and firewalls selected are all capable of being endpoints for VPN tunnels. For security reasons, we will use the PIX firewalls we selected to terminate the tunnels so that at no time will traffic be exposed to untrusted networks. In addition, all activities by partners and suppliers that are centered on the sayings (ordering, payment, upload, and download) will utilize SSL (HTTPS) and FTP tunneled through SSH (SFTP) as individual secure connections in place of a client-server VPN.

Remote office connections will allow access for all protocols between the remote office networks and the HQ internal network. Client connections for employees will be placed in an access control group that will allow only HTTP, HTTPS, SSH, DNS queries, and POP3. Client connections for administrators will allow access to the entire network. A Cisco Secure ACS for Windows server, running on the internal network, will provide access control decisions based on the client connection. The PIX will contact the ACS server through the Authentication, Authorization, and Accounting (AAA) functionality when a client is logging on and assign the appropriate access control list (Cisco *User Guide for Cisco Secure ACS for Windows Server*).

**Table 7: Strengths, Weaknesses, and Mitigation – VPNs**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Encrypts traffic to prevent eavesdropping<br>• Can use the Internet in place of more expensive private lines to connect remote offices<br>• Can allow remote workers connectivity with offices for working in the field<br>• May be implemented as an integrated function within a network device (router, firewall, or switch) or as a separate device (concentrator)<br>• Allows tunneling of virtually any traffic from point to point | • Early integrated devices had processing issues when performing more than one function (routing and VPN) under heavy loads<br>• Can be hard to install and troubleshoot<br>• Encrypted traffic cannot be monitored by normal devices | • Use appropriately scaled devices that can handle required traffic and still perform needed functions<br>• Keep connection details as simple as possible to ease installation<br>• Terminate VPNs at appropriate points so that traffic is still secure, but can be appropriately monitored |

## Network-based Intrusion Detection (IDS) Sensor(s)

Network-based IDS sensors (NIDS) serve to monitor overall traffic for suspicious events on a network-wide basis. While the firewall may also accomplish this function, we do not want the firewall to become bogged down in analyzing traffic more than it needs to in determining access for that traffic. In addition, NIDS can be used to monitor several different areas of the network to see what is, in fact, getting through, and as a correlation tracker for traffic moving through the network.

To give maximum coverage, we will deploy Cisco NIDS at various points in the network. To cut down on overall cost and maintenance, a Cisco 4255 Intrusion Prevention Sensor (IPS) will be used. Three of the four monitoring interfaces will be connected, one each, to the DMZs. The fourth interface may be connected to a span port on the core switch, or to an inline hub on the connection from the firewall to the core switch. This will monitor traffic that makes it through the firewall as well as insider attacks. The management interface will be connected to the internal network and the device will be configured to only respond to select management workstations. Cisco product literature claims 4255 devices have 600 MB/s monitoring capability, which leaves ample extra capacity on all links so that packets are not dropped during high bandwidth usage (network links within GEnt are all 100 MB/S).

Individual NIDS appliances could be deployed in each segment, with their management ports connected to an internal management network as an alternative, but in a company this size the extra cost is unwarranted.

**Table 8: Strengths, Weaknesses, and Mitigation – Network-based Intrusion Detection**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Can monitor traffic destined for entire networks and detect attacks through correlation of traffic to several hosts<br>• Most often dedicated devices and may be scaled for appropriate bandwidth<br>• | • May or may not identify host-specific attacks that use protocol manipulation<br>• If not appropriately scaled, the device may drop packets under heavy load and miss important traffic<br>• Must be tuned over a significant amount of time to eliminate false positives. Improper tuning may lead to introduction of false-negatives<br>• Can only detect attacks which it knows how to recognize (signatures – although this is evolving)<br>• If detected (through the use of a combined port for monitoring and control), may be specifically targeted during an attack | • Complement with Host-based IDS/IPS sensors to detect protocol manipulation or host-specific attacks on a particular target<br>• Monitor processing capability of device and network interface to ensure it can handle the necessary traffic level<br>• Use appropriate tuning period and traffic analysis to ensure appropriate stabilization time for device<br>• Keep up to date on new signatures. Have a process to evaluate new signatures when released to ensure only necessary signatures are added to the rulebase (cuts down on subsequent chance for false positives or follow-on tuning)<br>• Separate the management port from the monitoring port. Use an unbound monitoring port (no IP address). Consider use of a passive tap device to connect to the network (such as a Shomiti Tap).<br>• Test IDS systems with packet crafting or network scanning tools (SATAN, Nessus, etc.) |

## Host-Based IDS/IPS sensors

Supplementing the NIDS system is its counterpart, the Host-based IDS sensor (HIDS). While NIDS looks at traffic as a whole for the network segment, the HIDS looks at traffic specifically for its host, and is more apt to catch anomalies that use proper protocols and interactions, but may have malicious payloads. In addition, certain Intrusion Protection System (IPS) agents monitor system processes for anomalies and react to behaviors and not signatures.

In our design, we will deploy the Cisco Security Agent (CSA) on all DMZ servers. According to Cisco product literature[12], this software monitors the following:

- Host intrusion prevention
- Spyware/adware protection
- Protection against buffer overflow attacks
- Distributed firewall capabilities
- Malicious mobile code protection
- Operating-system integrity assurance
- Application inventory

[12] Cisco, "Cisco Security Agent" Web Page

- Audit log-consolidation

The agent will report back to the CSA Management Console (CSAMC) if an alert is sounded. This is done over ports 5401 or 443 (as a fallback if 5401 is not available) (Azlan para 3.2). The Management Console will also be able to poll individual agents for status as well as push policy changes to the agents.

**Table 9: Strengths, Weaknesses, and Mitigation – Host-based IDS/IPS**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Host-specific protection of an individual system. Avoids false positives from other OS attacks (UNIX attacks destined for a Windows host)<br>• ISP-capable agents can monitor processes on the system and prevent rogue processes from executing<br>• Some agents can monitor files for unauthorized modification (detects installation of rootkits etc.) | • Does not detect attacks against several hosts (such as network-wide scans)<br>• File monitoring can be difficult to configure for other than standard files. File monitoring cannot watch dynamic files. | • Complement with Network IDS to cover all types of attacks<br>• File monitoring requires tuning, similar to signature-based sensors. Once tuning is complete, false-positives should be minimized.<br>• Test IDS systems with packet crafting or network scanning tools (SATAN, Nessus, etc.) |

## Proxy Servers

Proxies serve as an intermediary in the network traffic path that can serve as both an access control and a malicious traffic detection/prevention function. Proxies can be used inbound to protect web servers, and can be used outbound to mitigate backdoors or viruses that 'call home' over port 80 or other common ports that are typically allowed through the firewall.

Inbound proxies protect the web servers from these types of attacks. Outbound proxies also enforce authentication for outbound traffic as well as protect return traffic from Internet web sites in the same way inbound traffic is protected.

Web servers can be vulnerable to protocol- or OS-based attacks separate from payload attacks. Fragmentation of packets, and overlapping of these fragments, as well as segmentation attacks, can cause various problems with the underlying operating system or the server software.

When dealing with malicious traffic, the proxy captures the traffic, reconstructing any fragmented packets or streams, and then recreates the traffic and sends it to the intended host through a separate connection. This reconstruction as a separate connection effectively corrects the errors that form the attack, filtering them out of the traffic. Also, since the proxy is not a true server, it will not process the commands in the traffic, just pass them on (after review). For example, some protocol- or payload-based attacks on a web server will not be processed as web commands and will not compromise the proxy, but can be detected and filtered out instead.

Outbound proxies can provide access control by routing all outbound traffic through the proxy server (or another relay, such as the mail relay). The firewall blocks all traffic from the internal network, except for that which originates from the proxy server. The proxy must be set for authentication so that it will forward only allow traffic through that comes from authenticated sources. This setup will require all outbound traffic to be authenticated through a username and password.

Proxy servers can also serve as a traffic logging and accounting function. By tracking traffic that passes through the proxy server, it can relieve the firewall or other devices from having to keep these records. Proxies also keep records of the authentication used for the connection in addition to the usual IP address that the firewall tracks. This gives investigators the ability to match a person (or at least their logon) with a source address when looking at suspicious traffic.

Note that GEnt will only proxy inbound traffic to the Public Web Server and Secure Server, and not the Extranet Server. The Secure Server will require an SSL capable proxy to properly terminate the SSL tunnel. The firewall restricts connections to the Extranet Server to only certain semi-trusted source IP ranges; another proxy is probably an unwarranted expense at this point. For all proxies, we will use Squid Proxies (version 2.5 is current) running on Fedora Core 3 Linux servers. Both are open source and free, to cut costs down.

Also note that this design separates the Secure Server and Extranet Server for the purposes of segregating credit card data (used by customers in purchasing sayings) from file transfer and other partner/supplier activities in compliance with Payment Card Industry (PCI) standards.

**Table 10: Strengths, Weaknesses, and Mitigation – Proxy Servers**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Collects and retransmits traffic streams destined for protected servers to defeat protocol manipulation attacks<br>• Can be used for access control (require authentication for connections to pass). Can be used to defeat unauthorized transmissions over authorized ports.<br>• In caching mode, can be used to lighten load on web server by caching frequently requested pages in memory<br>• Can record logs of connections, including any authentication information, in addition to firewall and other security devices | • Can only proxy certain connections. Some complicated connections are very difficult to proxy and require custom made proxy servers.<br>• Authentication can burden users with having to provide username and password when they go to surf the Internet. Users may react negatively. | • May need to create custom proxy software, or may need to utilize a separate device, such as an SSL accelerator, for particular connections. Not all connections need to be proxied however, so assess the business need before proceeding.<br>• Educate users as to the need for proxies. Create solid policies reinforcing the use of proxies in the overall security posture. |

## Mail Relays

To avoid exposing the company mail server to the Internet, GEnt will use a mail relay device to pass e-mail traffic from the Internet to the mail server. This mail relay will not only proxy the connection from foreign mail servers (with the benefits detailed above for the proxy servers) but will also inspect the mail traffic for viruses and dangerous traffic, both inbound and outbound.

GEnt will use Tumbleweed's MailGate E-mail Firewall[13], and will be used to provide anti-virus, anti-spam, and anti-Denial of Service against the mail system, in addition to proxying e-mail traffic.

**Table 11: Strengths, Weaknesses, and Mitigation – Mail Relays**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Used to proxy mail transfer so that Internet connections do not have access to company mail servers<br>• Prevents some protocol-based attacks against mail servers<br>• Can perform virus and content scanning on inbound and outbound e-mail | • Can be overloaded by DoS attacks against the server<br>• Requires maintenance of content-filtering software | • Mitigate DoS attacks with hardening of the server as well as upstream DoS mitigation (eg. Floodguard on the routers)<br>• Institute a regular maintenance program for all anti-virus and other security software |

## DNS Servers

DNS servers translate human-friendly server names and URLs into machine-friendly IP addresses. However DNS servers can be a security risk since they contain listings for all systems they translate for, which may allow attackers to easily gain a listing of systems that they should not know about. Furthermore, if not correctly configured, they can be used against the enterprise.

GEnt will use a split-DNS methodology, separating the tables of addresses and hostnames of the publicly addressable systems from the internal systems. DNS servers must be accessible to the public to do their job, so they are subject to attack. By splitting the DNS records up between servers, an attacker cannot harvest information on the internal systems by attacking the external DNS server.
Split-DNS (or Split-Brain DNS) is discussed in the paper titled *Split-Brain DNS Server Configuration for ISPs* from Microsoft. Even though the title concerns ISPs, the concept is still valid for security-minded businesses.

The DMZ DNS systems (called DMZ DNS for ease of reference since they are clones of each other) will be authoritative for all publicly accessible GEnt systems and will not share this information with other DNS systems (internal or external). Note also that only UDP DNS traffic for query resolution will be

[13] see Tumbleweed.com "MailGate Email Firewall"

allowed through the firewall so that zone transfers (which only use TCP traffic) cannot occur even if the internal or DMZ DNS is set to perform them.

The internal DNS servers will be set as forwarders for queries from the internal users, passing the queries to the DMZ DNS for resolution. This will prevent a hole being opened in the firewall from the internal network to the Internet. The DMZ DNS will effectively proxy DNS queries from internal clients. Also, to prevent DNS cache poisoning attacks the DMZ DNS will not allow recursive queries from outside GEnt. GEnt will use Windows 2000 Server's DNS implementation for all DNS servers.

**Table 12: Strengths, Weaknesses, and Mitigation – DNS Servers**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Split-DNS (limited records and no zone transfer) can hide non-public servers from Internet notice | • Allowing recursive queries can lead to poisoning of the DNS cache and potential DNS spoofing<br>• If DNS contains records from internal or non-public hosts, these addresses can be compromised through queries<br>• If zone transfers are allowed, and not restricted to authorized hosts, the entire record file can be compromised | • Prohibit recursive queries to requests from the Internet<br>• Use a split-DNS where the public DNS contains only the records for systems that are publicly accessible<br>• Do not allow zone transfers. If zone transfers are necessary (such as those to upstream ISPs), allow transfers to only authorized systems, and require authentication if available. |

## Syslog Server

An important part of an overall security posture is monitoring the various security devices. This involves capturing and analyzing log data to note trends or to determine what is happening or has happened after an incident. Most of the security devices are capable of capturing their own log data, but this data could be lost if the device crashes or is compromised. To mitigate this risk, GEnt will export log data from the firewall and IDS Sensors (NIDS and HIDS) to a central syslog server on the internal network. This serves two functions: 1) aggregating log data so that it may be correlated and immediately available; and 2) compromise of a single device in a DMZ will not compromise the log data since an attacker will need to penetrate the internal network and the syslog data to erase their tracks or otherwise alter the log data.

GEnt will use the syslogd daemon on a hardened Fedora Core 3 system located on the internal network. Access control will be set to only accept syslog feeds from the designated devices (the HIDS on each server in the various DMZs, the firewall itself, remote firewalls (through the remote office VPNs), and the IDS unit (through the internal network). Administration will be done through SSH from designated administrator workstations.

**Table 13: Strengths, Weaknesses, and Mitigation – Syslog Servers**

| Strengths | Weaknesses | Mitigation |
|---|---|---|
| • Central accumulation of log data from a variety of security devices and systems for ease of administration<br>• Provides protected, off-platform storage of log data (on-platform log data could be altered or deleted if an attacker compromises a system) | • Volume of log data maybe impossible for normal people to review on a timely basis<br>• System may not have enough space or processing power available to record all log data in high traffic times and will lose data | • Utilize log correlation and reduction tools to filter out routine or non-critical events. Notify administrators of critical alerts.<br>• Ensure enough storage space and processing power is available for peak volume events<br>• Protect log data on the central server through strong access controls or writing the log data to unalterable media (CD/DVD-ROM, etc.) |

## *Implementing Defense in Depth*

Defense in depth prevents each device from having to provide all of its own security needs and allows you to leverage various technologies to complement the overall security of the enterprise. There are several good white papers and references discussing the topic and architectures that go along with it, foremost being the Cisco SAFE Blueprint. To quote the Blueprint, a defense in depth design creates an architecture "resulting in a layered approach to security where the failure of one security system is not likely to lead to the compromise of the rest of the network." Defense in depth not only leverages placement of devices and connections, but leverages preventative and detective controls. In the following section, we will talk about the layers of defense used in GEnt's architecture. This design of GEnt's network is based on the SAFE blueprint and serves as a demonstration of how to implement the theory (and more) in a practical way.

### Defense Layers – Outside In

This section will cover traffic from the Internet entering GEnt's network.

*External Router*

The external router initially screens traffic coming into the network perimeter. Traffic with source addresses from the RFC 1918 ranges, as well as the loopback address, are known to always be bad, so we can safely filter then at the router. Bad source addresses that are from reserved address ranges (as noted by IANA and other assignment organizations) can also be put in the filtering rules, since these are sometimes used as spoofed sources, but doing this will incur a significant management burden. Addresses will have to be continually reviewed and the access control lists updated because the authorities may assign these reserved addresses at any time. You may lose important traffic if you continue to block previously reserved addresses that are now in use. Finally, you can block addresses from known hostile sources if they are subsequently identified. The external router will also filter Denial of Service

attacks (using Cisco Express Forwarding Mode or other throttling techniques[14]) to keep the load off other network devices.

*Primary Firewall*
Traffic that passes the router will then enter the firewall. Here, only connections to specific systems and ports for business purposes will be allowed through – all other traffic will be dropped. This way, the attacker will get no feedback on what happened. The traffic simply disappeared.

The firewall only allows connections to the Inbound Proxy (80/TCP), DMZ DNS (53/UDP), and Mail Relay (25/TCP) on the Public DMZ. It also allows connections to the SSL Proxy (443/TCP), and Extranet Server (22/TCP, 443/TCP) on the Extranet DMZ. All of these hosts are given virtual Internet-addressable IP addresses through NAT.

*Name Resolution*
Name resolution is provided by the DMZ DNS, which contains records only for the DNS servers, Inbound Proxy, the mail server, and the SSL proxy. The VPN will use IP address only, as will the outbound proxy (for return traffic). Zone transfers will be disabled, as will recursion for externally sourced queries. This will protect the DNS servers from most DNS attacks, while the firewall and router protect the server itself from other attacks. Internal queries will also be forwarded to the DMZ DNS for resolution, so that a connection from the internal network directly to the Internet does not have to be made.

*Inbound and SSL Proxies*
Public web traffic will be allowed to the Inbound Proxy, which will capture and retransmit the connection to the Public Web Server. This way, attacks cannot be mounted directly against the web server, and protocol-based attacks (such as fragmentation attacks) cannot be used as the proxy will simply detect the traffic is not correctly formed and will drop it. As a secondary benefit, the proxy can perform web page caching to improve the efficiency of page retrieval for clients. Information on this web server is mostly static, which is a prime candidate for caching. The Inbound Proxy will protect the Public Web Server from direct access, and attack.

If a customer wants to purchase a file of fortune cookie sayings, they are redirected to the Secure Server through the SSL Proxy for purchasing sayings files. The SSL Proxy serves the same functions as the Inbound Proxy, with the addition of being able to handle the SSL connection. The SSL proxy will then make another SSL connection to the Secure Server so that the payment information is protected even inside the Extranet DMZ. The Secure Server cannot be contacted directly from the Internet.

The Inbound and SSL proxies will also log all connections and export these logs

[14] Cisco "Improving Security on Cisco Routers"

to the central syslog server for aggregation, analysis, and safekeeping.

*VPN Connections*
The firewall is also the termination point for the company's VPN traffic. Remote offices connect to the HQ office by point-to-point VPNs between the firewalls at each location. This connection group is passed on to the internal network and given complete access to all addresses on the HQ internal network. Teleworkers connect to the HQ firewall with the Cisco Secure Desktop Client, and only have access to the Intranet Server, company mail server, the outbound proxy, and any application servers they may specifically need. At this time, due to the small size of the company, authentication is done through username and password. The restrictions on destination IPs for teleworkers are an effort to mitigate physical security concerns about their laptops being stolen and hacked to gain access to the company network. Note we are assuming that internal applications will also require different logon credentials, so stolen VPN access alone will not breach any information directly.

*Extranet Server*
Partners and Suppliers will connect directly to the extranet server to conduct their business with GEnt. While this does place the Extranet Server at some risk since there is no proxy front-ending it, the risk is minimal since the firewall only allows connections from known partner and supplier addresses and not the general Internet. Also, the data is stored on the Database server, not the Extranet Server, so there are additional steps that must be taken for an attacker to get the 'crown jewels'. Finally, only encrypted traffic (HTTPS and SSH/STFP) is allowed past the firewall, so information is protected as it transits the Internet.

*Mail Relay*
The Tumbleweed mail relay system accepts incoming mail from the Internet and scans it for known viruses and other security threats, and then relays it on to the internal company mail server. Clients then connect to the internal mail server to retrieve their mail and send new mail (covered in the outbound section). In this way, any attack mounted against the mail relay will only disable the external link and not the entire mail system. In addition, being a proxy, the mail relay is not a full mail system and will not be vulnerable to attacks that exploit flaws in mail handling software. The mail relay simply accepts the mail, scans it, and then passes it on.

*Network IDS*
A Cisco IDS will be configured to monitor all DMZ segments and the link immediately inside the internal firewall interface to supplement the firewall's detection capabilities. The IDS will be configured to listen passively, and the management port will be connected to the internal network. This ensures the IDS sensor is not detectable and cannot be compromised and used to bridge the DMZ to the internal network. Logs will be aggregated on the IDS and on the management console (also on the inside network).

**Internal DMZ Security**

Security measures are taken within DMZ zones, not just between zones. These measures complement the traffic controls in the firewall and routers and serve to secure the endpoints. In this way, even if hostile traffic makes it through the network controls, it will have a difficult time compromising the destination system.

*Proxy to Backend Traffic and Host Security*

As discussed earlier, we are using proxies for most Internet-accessible services. The actual servers are not exposed to the Internet (the firewall blocks traffic to them) and are relatively safe from direct attack. Once traffic from the Internet has reached the proxy device for that service, it is relayed by a backend connection to the server actually providing the service. All systems in the DMZ will have unnecessary services turned off, all applications and operating systems patched to current levels, and vulnerability scans conducted on them periodically. All servers will have local anti-virus programs installed and updated regularly, as appropriate for the operating system. Finally, all servers will have the Cisco CSA Agent installed and configured as a host-based IPS.

*Database Segregation*

Protecting the fortune cookie saying information there are an additional three factors of security, even from the internal network: 1) There is separation in that the sayings are kept on the database server, which is in a different access controlled network zone from the Public, Extranet, and Internal Network zones; 2) The firewall only allows SQL connections between the Extranet, Secure, and Intranet servers, and the Database Server – all other connections are denied; and 3) Access control is set on the Database Server to only allow stored procedures to be run and not direct SQL queries (out of scope, but a protection nonetheless). Not having direct SQL queries is also a requirement of the Payment Card Industry (PCI) standards when processing credit cards, as is separating web and database servers (Visa USA 8.5.16).

*Network Port Security*

Other security measures will be taken in the DMZs to protect the overall security of the network through defense-in-depth. Unused ports on all DMZ network devices will be disabled and port security[15] will be enabled on all in-use ports so that you cannot simply plug in a new device on the DMZ or replace an existing device. Finally, Cisco devices will have the Cisco Discovery Protocol[16] (CDP)

[15] Cisco devices can be set to record the MAC address of the system connected to a specific port and allow traffic only from that address in the future to be accepted by the device. If a new device (with a different MAC address) is connected to that port without authorization, the port will shut down, effectively shutting out the connection. While the MAC address of any network connection can be faked, this feature prevents casual connections to the DMZ devices by unauthorized individuals and devices. (Software Configuration Guide (5.4) Configuring Port Security)

turned off.

**Defense Layers – Inside Out**

Defense-in-depth does not apply only to traffic coming in from the network. To have comprehensive security, you must also secure your outbound traffic so that unauthorized connections cannot be made from inside the network to hosts on the Internet. Some Trojan Horse programs, and some viruses, use uncontrolled outbound access to 'call home' and download more malicious software onto the infected computer. Hackers can then connect to the internal system through this outbound connection. To complement our inbound defenses we will also have the following outbound defenses in place.

Only authorized connections will be allowed to the Internet. This will be achieved by a series of access control lists inbound to the inner and DMZ interfaces so that unauthorized traffic cannot leave that network segment. The DMZ segments will only allow traffic out destined for the recipients as given in the firewall policy. The internal firewall interface will also only accept connections to destination DMZ systems that are authorized by the firewall policy. Note that we have engineered the firewall policy so that all connections must stop at a DMZ device before they can continue to their ultimate destination.

*Primary Firewall*

For business uses, the firewall will only allow access from the internal network to the Outbound Proxy, DMZ DNS servers (from the internal DNS only), mail relay (from the internal mail server only), and the Database Server (from the Intranet server only). In addition to these services, the firewall will also allow SSH connections to the various DMZs (from administrator workstations only) for administration, and SSH to the Extranet Server (from administrator and business unit workstations only) for use in file transfer with partners and suppliers. Syslog connections will be allowed from the central syslog server, and traffic will be allowed to the VPNs in accordance with their destination (all traffic to remote offices, and only appropriate traffic to the teleworkers, based on their access group.

The firewall will also only allow employee web traffic out of the Public DMZ from the Outbound Proxy. It will block attempts to connect to the Internet that do not originate from the proxy. Likewise, it will only allow SMTP traffic outbound from the mail relay. This will prevent adding unauthorized mail servers or using terminal emulators to manually send SMTP mail by connecting to foreign mail servers. Thus the Tumbleweed appliance will scan all outbound mail and will ensure viruses are not being spread from GEnt to the rest of the Internet.

[16] CDP allows Cisco devices to discover and monitor their neighbor devices, and you can use CDP to go from device to device to see what each device's neighbors are. An attacker can use this to map out your network. (Cisco "Cisco Discovery Protocol (CDP)")

The DMZ DNS servers will be the link from clients on the internal network to Internet DMZ servers. Clients will connect to the internal DNS server, which in turn will forward the query to the DMZ DNS to be sent to the Internet. Once a response has been returned to the DMZ DNS, it will be passed on to the internal DNS for transmission to the client.

Finally, the firewall will not allow internal addresses (RFC 1918) to go out onto the Internet (except when tunneled through the VPN to remote offices or teleworkers). The router will also block these addresses in case changes are made in the firewall that do not cover these addresses in the future. This will prevent traffic with spoofed private/internal IP addresses from getting to the Internet and affecting others.

*Outbound Proxy*

The outbound proxy will request authentication for all web connections to the Internet. Users will only be able to use the proxy to access Internet Web sites, and only over ports 80 and 443. The proxy will log all connections and authentication information and will export these logs via syslog to the central log server for analysis and safekeeping. GEnt can also install content detection and filtering software (such as Websense) on this proxy if desired or required by regulation in the future.

*Remote Office Use of the Internet*

In keeping with our goal of allowing only authorized traffic out to the Internet, users in the remote offices or in the field will have to connect to the Outbound Proxy for connections to the Internet. This will require all Internet connections to be authenticated and logged. The use of a proxy is also required since the firewall cannot send a packet immediately out the same interface it just received it on[17]. Thus, remote offices/teleworkers could not connect to the Internet even if they wanted to since the firewall is also the VPN termination point.

[17] Cisco "Configuring PIX-to-PIX-to-PIX IPSec (Hub and Spoke)"

# Assignment 3: Router and Firewall Policies

This assignment details the overall security stance that was used as a guideline for determining access control and device placement. Also included are the security policies of both the border router and the primary firewall (HQ site).

## *General Security Stance*

A company's security stance should be guided by its policy. A strong policy gives guidance to all employees on how to implement security, as well as sets standards on how architecture and devices must be configured.

The following policies will be used as a guide for the general security stance:

- All traffic to/from the Internet is to be denied unless explicitly allowed
- All connections into/out of the company must have a justified business need
- All transactions involving the product (the sayings) must be done securely
- All management of DMZ systems and security devices will be done through secure means
- Traffic from the remote offices will have open access to the internal network
- All Internet connectivity for internal employees will go through the corporate HQ connection and servers. Remote offices will have no access to the Internet outside of the VPN to the HQ office.
- Critical systems must be monitored for security events
- Access to the database will only be allowed through front-ends. No users, internal or external, will be allowed directly to the database with the exception of the DBA.

## *Border Router(s) Security Policy*

The border router at the HQ site will be the first line of defense for common network threats. Primary access control of connections will be done by the firewall.

Cisco processes rules from top down, and stops after reaching an applicable rule. As there are so few rules, and all with the same purpose, the order is not relevant and will not be shown.

To protect the network from external spoofing attacks, the router will filter the following traffic inbound on the external interface:

- Block and log traffic with RFC 1918 source addresses
    - 10.0.0.0/8
    - 172.16.0.0-172.31.255.255
    - 192.168.0.0/16
- Block and log spoofed traffic with the loopback address as a source
    - 127.0.0.1

To prevent internal traffic with spoofed source addresses from 'escaping', the router will also filter the same traffic inbound to the internal interface of the router from the firewall (in effect, an egress filter). The firewall will not be able to filter these inbound to itself from the internal network, since it will be processing traffic from valid addresses in these ranges, but only VPN traffic and legitimate traffic originating from the public addresses (after NAT) of the DMZ hosts, should be exiting the firewall and getting to the router. It will also prevent the internal network addresses (172.16.x.x) from being exposed.

The router will also have Cisco Floodguard enabled to assist in preventing Denial-of-Service attacks.

## *Primary Firewall(s) Security Policy*

The firewall controls all access from the Internet, and also functions as the VPN termination point for the tunnels from the remote offices and the teleworkers in the field.

By default, Cisco devices implicitly deny all connections from lower security zones (outside) to higher security zones (inside), requiring explicit permit statements. Outbound connections are the opposite, implicitly allowing all connections from higher security zones (inside) to lower security zones (outside), requiring explicit deny statements. To ensure we allow only authorized traffic and block all other traffic, we will use explicit permit and deny statements (including deny all at the end of each list) for each traffic rule.

Cisco processes rules from top down, and stops after reaching an applicable rule, so rules should be ordered with the following guidelines in mind:

- Go from specific to general in rule scope
    - This allows a specific condition (i.e. traffic from one designated host to the other) to be evaluated before net to net traffic is evaluated, giving you more finite control
- Deny first, permit later[18]
    - If you explicitly deny a particular connection early on, it will not then be allowed by a later general rule. Remember to stay with the 'specific then general' guideline given below or the deny rule may lock out an entire network if used before denying a specific host.
- Most used rules should go first
    - This uses less firewall CPU time to evaluate the connection, since it reaches a matching rule early on
- There is an implicit deny all statement at the end of the list for inbound access (low to high security)[19]
- There is an implicit permit all statement at the end of the list for outbound

[18] Cisco Systems, *Cisco PIX Firewall and VPN Configuration Guide, V6.3* 3-2
[19] Cisco Systems, *Cisco PIX Firewall and VPN Configuration Guide, V6.3* 3-2

access (high to low security)[20]

Using these guidelines, we will create the proper access control lists to match our data flows given in Assignment 2. The access lists in Tables 14-18 cover the various access lists that will be used and are given in general terms for ease of understanding instead of using the Cisco syntax in the actual rule configuration. Where the access list is applied, and why, will be noted at the top of the table. Note the ACS server will provide dynamic access lists for VPN users (not remote offices) based on the user's login. These are discussed in the VPN Connection heading of the Implementing Defense In Depth section above, and are not repeated here due to their variability.

**Table 14: Firewall Security Policy (Inbound from Internet)**

| **Applied inbound to the External Interface**<br>Governs traffic coming into the firewall from the Internet | | | | | | |
|---|---|---|---|---|---|---|
| **Rule #** | **Source** | **Destination** | **Port/Protocol** | **Action** | **Rule Reason** | **Notes** |
| 1 | Any | Any | ICMP | Deny | Blocks all ICMP traffic to the firewall and internal network | Does not allow an attacker to use ICMP (echo/replies or other) from outside the firewall to the firewall itself or any internal system |
| 2 | Any[21] | Firewall | IP 50 (ESP) | Permit | Encrypted traffic from remote office VPN | Interoffice traffic will likely be the highest amount of traffic so this rule is first. Grouped with teleworker rules for simplicity of rule set even though teleworker traffic is much less than remote office. |
| 3 | Any | Firewall | 500/UDP (IKE) | Permit | Key negotiation for remote office VPN | Tunnel maintenance for interoffice and teleworker VPNs is important as the Internet is the company WAN, so this rule has higher priority than other traffic |
| 4 | Any | Inbound Proxy | 80/TCP (HTTP) | Permit | Public access to Public Web Server | Allows access to the proxy, but not access to the web server itself |
| 5 | Any | Mail Relay | 25/TCP (SMTP) | Permit | Incoming e-mail | Allows access to the mail relay, but not the e-mail system itself |

[20] Cisco Systems, *Cisco PIX Firewall and VPN Configuration Guide, V6.3* 3-4

[21] Note that traffic with spoofed internal source addresses coming from the Internet will be filtered at the router, so these Any commands will not allow spoofed traffic in from the Internet, only internal traffic from the VPN.

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | Any | DMZ DNS | 53/UDP (domain) | Permit | Incoming name resolution for DMZ hosts | Allows access to DNS for public reachable systems only |
| 7 | Any | SSL Proxy | 443/TCP (HTTPS) | Permit | Access for customers for purchasing sayings | Since customers may be anywhere on the Internet, this server must be open to all. SSL Proxy protects the Secure Server from direct connections. |
| 8 | Supplier IP addresses | Extranet Server | 443/TCP (HTTPS) | Permit | Access to extranet server for suppliers to upload files | Services on this port will require username/password authentication in addition to specific source addresses provided by suppliers |
| 9 | Partner IP addresses | Extranet Server | 443/TCP (HTTPS) | Permit | Access to extranet server for partners to upload and download files | Services on this port will require username/password authentication in addition to specific source addresses provided by partners |
| 10 | Supplier IP addresses | Extranet Server | 22/TCP (SSH) | Permit | SSH/SFTP access for uploading files | Services on this port will require username/password authentication in addition to specific source addresses provided by suppliers |
| 11 | Partner IP addresses | Extranet Server | 22/TCP (SSH) | Permit | SSH/SFTP access for uploading files | Services on this port will require username/password authentication in addition to specific source addresses provided by partners |
| 12 | Any | Any | Any | Deny | Blocks all other traffic from Internet (just in case…) | |

**Table 15: Firewall Security Policy (Public DMZ)**

| **Applied inbound to the Public DMZ Interface**<br>Governs traffic coming out of the Public DMZ for other zones | | | | | | |
|---|---|---|---|---|---|---|
| **Rule #** | **Source** | **Destination** | **Port/Protocol** | **Action** | **Rule Reason** | **Notes** |
| 1 | Outbound Proxy | Internal networks | 80/TCP (HTTP) | Deny | Blocks web traffic from hitting proxy and then returning to internal networks or DMZ (bouncing traffic) due to implicit allow from higher to lower security zones (and any address of permit rules below) | Specific deny for internal addresses is more stringent than any address so traffic will be blocked only to internal network/DMZ addresses (and allowed out to the Internet) since this rule comes before the any permit rule for this traffic. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | Outbound Proxy | Internal networks | 80/UDP (HTTP) | Deny | Blocks web traffic from hitting proxy and then returning to internal networks or DMZ (bouncing traffic) due to implicit allow from higher to lower security zones (and any address of permit rules below) | Specific deny for internal addresses is more stringent than any address so traffic will be blocked only to internal network/DMZ addresses (and allowed out to the Internet) since this rule comes before the any permit rule for this traffic. |
| 3 | Outbound Proxy | Internal networks | 443/TCP (HTTPS) | Deny | Blocks web traffic from hitting proxy and then returning to internal networks or DMZ (bouncing traffic) due to implicit allow from higher to lower security zones (and any address of permit rules below) | Specific deny for internal addresses is more stringent than any address so traffic will be blocked only to internal network/DMZ addresses (and allowed out to the Internet) since this rule comes before the any permit rule for this traffic. |
| 4 | Outbound Proxy | Internal networks | 443/UDP (HTTPS) | Deny | Blocks web traffic from hitting proxy and then returning to internal networks or DMZ (bouncing traffic) due to implicit allow from higher to lower security zones (and any address of permit rules below) | Specific deny for internal addresses is more stringent than any address so traffic will be blocked only to internal network/DMZ addresses (and allowed out to the Internet) since this rule comes before the any permit rule for this traffic. |
| 5 | Outbound Proxy | Any | 80/TCP (HTTP) | Permit | Employee web access from proxy to Internet | Only proxy is allowed to go out to the Internet |
| 6 | Outbound Proxy | Any | 80/UDP (HTTP) | Permit | Employee web access from proxy to Internet | Only proxy is allowed to go out to the Internet |
| 7 | Outbound Proxy | Any | 443/TCP (HTTPS) | Permit | Employee web access from proxy to Internet | Only proxy is allowed to go out to the Internet |
| 8 | Outbound Proxy | Any | 443/UDP (HTTPS) | Permit | Employee web access from proxy to Internet | Only proxy is allowed to go out to the Internet |
| 9 | Mail Relay | Internal Mail Server | 25/TCP (SMTP) | Permit | Inbound mail traffic from relay to internal mail server | Access to mail server from mail relay only |
| 10 | DMZ DNS | Internal DNS | 53/UDP (domain) | Permit | Responses to queries that were forwarded from the internal DNS server | Maintains open connection for returning query responses |

| | | | | | | |
|---|---|---|---|---|---|---|
| 11 | Public DMZ net | CSAMC | 5401/TCP | Permit | Cisco Security Agent traffic to Management Console | Alert traffic from agent to console |
| 12 | Public DMZ net | CSAMC | 5401/UDP | Permit | Cisco Security Agent traffic to Management Console | Alert traffic from agent to console |
| 13 | Public DMZ net | Syslog Server | 541/UCP (syslog) | Permit | Log export from devices to central log server | |
| 14 | Any | Any | Any | Deny | Blocks all other traffic out of Public DMZ to any other zone | Needed to prevent implicit allow to lower security zones from Public DMZ |

**Table 16: Firewall Security Policy (Extranet DMZ)**

| **Applied inbound to the Extranet DMZ Interface**<br>Governs traffic coming out of the Extranet DMZ for other zones | | | | | | |
|---|---|---|---|---|---|---|
| **Rule #** | **Source** | **Destination** | **Port/Protocol** | **Action** | **Rule Reason** | **Notes** |
| 1 | Secure Server | Database Server | 1433/TCP (SQL) | Permit | DB calls from applications on Secure web server | Web applications will only make calls to the DB server, not the reverse |
| 2 | Extranet Server | Database Server | 1433/TCP (SQL) | Permit | DB calls from applications on Extranet web server | Web applications will only make calls to the DB server, not the reverse |
| 3 | Extranet DMZ net | Syslog Server | 541/UCP (syslog) | Permit | Log export from devices to central log server | |
| 4 | Extranet Server | Partner IP addresses | 22/TCP (SSH) | Permit | SSH/SFTP connections to partner/supplier servers to transfer files. | Business unit personnel will use the Extranet server as an SSH proxy to make connections to outside servers at partners and suppliers. |
| 5 | Extranet Server | Supplier IP addresses | 22/TCP (SSH) | Permit | SSH/SFTP connections to partner/supplier servers to transfer files. | Business unit personnel will use the Extranet server as an SSH proxy to make connections to outside servers at partners and suppliers. |
| 6 | Any | Any | Any | Deny | Blocks all other traffic out of Public DMZ to any other zone | Needed to prevent implicit allow to higher security zones from Extranet DMZ |

**Table 17: Firewall Security Policy (Database DMZ)**

| Applied inbound to the Database DMZ Interface<br>Governs traffic coming out of the Database DMZ for other zones | | | | | | |
|---|---|---|---|---|---|---|
| **Rule #** | **Source** | **Destination** | **Port/Protocol** | **Action** | **Rule Reason** | **Notes** |
| 1 | Database DMZ net | Syslog Server | 541/UCP (syslog) | Permit | Log export from devices to central log server | |
| 2 | Any | Any | Any | Deny | Blocks all other traffic out of Database DMZ to any other zone | Needed to prevent implicit allow to lower security zones from Database DMZ |

**Table 18: Firewall Security Policy (Internal Network to DMZ/Internet)**

| Applied inbound to Internal Interface<br>Governs traffic coming out of the internal network for other zones | | | | | | |
|---|---|---|---|---|---|---|
| **Rule #** | **Source** | **Destination** | **Port/Protocol** | **Action** | **Reason** | **Notes** |
| 1 | Any | Outbound Proxy | 8080/TCP (HTTP) | Permit | Web access for employees | Prevents web access directly to Internet by requiring authentication to the proxy. Most expected traffic. |
| 2 | Any | Outbound Proxy | 8080/UDP (HTTP) | Permit | Web access for employees | Prevents web access directly to Internet by requiring authentication to the proxy. Most expected traffic. |
| 3 | Any | Outbound Proxy | 8443/TCP (HTTPS) | Permit | Web access for employees | Prevents web access directly to Internet by requiring authentication to the proxy. Most expected traffic. |
| 4 | Any | Outbound Proxy | 8443/UDP (HTTPS) | Permit | Web access for employees | Prevents web access directly to Internet by requiring authentication to the proxy. Most expected traffic. |
| 5 | Internal DNS | DMZ DNS | 53/UDP (domain) | Permit | DNS queries for Internet hosts forwarded by internal DNS | The DMZ DNS will be used as a query relay for internal users (internal DNS is a forwarder) |
| 6 | Internal mail server | Mail relay | 25/TCP (SMTP) | Permit | Outbound e-mail to Internet (through relay) | Mail relay scans outbound mail for viruses and, optionally, content |
| 7 | Intranet server | Database server | 1433/TCP (SQL) | Permit | SQL connections for database operations and applications | Access to database server is limited to only from the Intranet server. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8 | Business Unit workstations | Extranet Server | 22/TCP (SSH) | Permit | SSH/SFTP access for sending/ retrieving files from extranet server. | Not all persons in the company require access to the extranet server, so access is limited to only those business unit personnel who have a business need. Business unit personnel will also use the Extranet server as an SSH proxy to make connections to outside servers at partners and suppliers (see Extranet table above). |
| 9 | Administrator workstation(s) | Firewall | 22/TCP | Permit | Administrator access to firewall | Protects firewall management interface in that no other SSH connections can access the firewall directly. |
| 10 | Administrator workstation(s) | Public DMZ net | 22/TCP (SSH) | Permit | Administrator access for public DMZ hosts. | Limited to only IP addresses for administrators. Secondary security provided by SSH logon on individual systems. |
| 11 | Administrator workstation(s) | Extranet DMZ net | 22/TCP (SSH) | Permit | Administrator access for extranet DMZ hosts. | Limited to only IP addresses for administrators. Secondary security provided by SSH logon on individual systems. |
| 12 | Administrator workstation(s) | Database DMZ net | 22/TCP (SSH) | Permit | Administrator access for database DMZ hosts. | Limited to only IP addresses for administrators. Secondary security provided by SSH logon on individual systems. |
| 13 | Cisco Secure ACS Server | Firewall | ICMP | Permit | Must be able to ping firewall | Required by ACS. Can restrict to only echo request/replies but source is only the ACS server so one rule can cover it |
| 14 | Cisco Secure ACS Server | Firewall | 49/TCP (TACACS+) | Permit | AAA functions | Required by ACS for authenticating VPN clients |
| 15 | Cisco Secure ACS Server | Firewall | 1645/UDP (RADIUS) | Permit | AAA functions | Required by ACS for authenticating VPN clients |
| 16 | Cisco Secure ACS Server | Firewall | 1812/UDP (RADIUS) | Permit | AAA functions | Required by ACS for authenticating VPN clients |
| 17 | Cisco Secure ACS Server | Firewall | 1813/UDP (RADIUS) | Permit | AAA functions | Required by ACS for authenticating VPN clients |

| | | | | | | |
|---|---|---|---|---|---|---|
| 18 | Any | Any | Any | Deny | Blocks all other traffic out of Public DMZ to any other zone | Needed to prevent implicit allow to lower security zones from Database DMZ |

## References


Airscanner. "AirScanner Module Firewall User's Manual". Mar 20, 2005. <http://www.airscanner.com/downloads/firewall/fwmanual.htm>

Azlan "Cisco Security Agent (Okena) Quick Reference Deployment Guide". Azlan.at. Mar 20, 2005. <www.azlan.at/Resources/Cisco/Cisco_csa_deployment_interview.pdf>

Borisov, Nikita, Ian Goldberg, and David Wagner. "Security of the WEP Algorithm". ISAAC (Internet Security, Applications, Authentication and Cryptography), University of California, Berkeley, Department of Computer Sciences. Mar 20, 2005. <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

Cisco Systems Inc. "Cisco Discovery Protocol (CDP)". Cisco.com. 2005. Mar 20, 2005. <http://www.cisco.com/en/US/tech/tk648/tk362/tk100/tsd_technology_support_sub-protocol_home.html>

---, "Configuring PIX-to-PIX-to-PIX IPSec (Hub and Spoke)". Cisco.com. 2005. Mar 20, 2005. <http://www.cisco.com/warp/public/110/pixhubspoke.pdf>

---, Cisco PIX Firewall and VPN Configuration Guide, Version 6.3. 2005. Mar 20, 2005. <http://www.cisco.com/application/pdf/en/us/guest/products/ps3918/c2001/ccmigration_09186a0080312c02.pdf>

---, Cisco PIX Firewall Command Reference, Version 6.3. Cisco.com. 2005. Mar 20, 2005. <http://www.cisco.com/application/pdf/en/us/guest/products/ps3918/c2001/ccmigration_09186a00801cd79b.pdf>

---, Cisco PIX Firewall Hardware Installation Guide, Version 6.3. Cisco.com. 2005, Mar 20, 2005, <http://www.cisco.com/application/pdf/en/us/guest/products/ps2030/c2001/ccmigration_09186a008017293a.pdf>

---, "Cisco Security Agent". Cisco.com. 2005. Mar 20, 2005. <http://www.cisco.com/en/US/ products/sw/secursw/ps5057/>

---, "Improving Security on Cisco Routers". Cisco.com. Feb 2. 2005. Mar 20, 2005 <http://www.cisco.com/warp/public/707/21.html>

---, "Product Bulletin No. 2683 Cisco 4255 Intrusion Prevention Sensor". Cisco.com. 2004. Mar 20, 2005. <http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_bulletin0900aecd801e64c6.html>

---, "Software Configuration Guide (5.4)". Cisco.com. 2005. Mar 20, 2005. <http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_book09186a008007eee4.html>

---, User Guide for Cisco Secure ACS for Windows Server, Version 3.3. Cisco.com. 2005. Mar 20, 2005. <http://www.cisco.com/application/pdf/en/us/guest/products/ps2086/c2001/ccmigration_09186a0080314477.pdf>

Convery, Sean and Roland Saville. SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks. Cisco.com, 2003. Mar 20, 2005. <http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.pdf>

Convery, Sean, Bernie Trudel, Greg Abelar, and Jason Halpern. SAFE: A Security Blueprint for Enterprise Networks. Cisco.com. 2004. Mar 20, 2005. <http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.pdf>

Dealtime.com. "ViewSonic (WAPBR-100) 802.11g/b (wapbr100) Wireless Access Point". Dealtime.com. Mar 20, 2005. <http://www.dealtime.com/xPF-WRLS_ACCES_POINT_REAPTER_BRIDGE_WITH_125_HIGH_SPEED_MODE >

D-Link Systems Inc. "DWL-1000AP Wireless Access Point User's Manual". dlink.com. Mar 20, 2005. <ftp://ftp.dlink.com/Wireless/DWL1000AP/Manual/dwl1000AP_manual_100604.zip>

Ferguson, P. and D. Senie. "RFC 2827 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing". Internet FAQ Archives. May 2000. Mar 20, 2005. <http://www.faqs.org/rfcs/rfc2827.html>

Handheld Products, Inc. "Dolphin® 7400/7450 Hand Held Computer User's Guide". hhp.com. Nov 29 2004. 20 Mar 2005 <http://www.handheld.com/ download.aspx? download=/data/3006c78c-0fdb-4426-a82a-7b2c721b7d62.pdf&filename= Dolphin+7400+Mobile+Computer+User>

Microsoft Corporation, Split-Brain DNS Server Configuration for ISPs, Microsoft.com. 2003. Mar 20, 2005. <www.microsoft.com/serviceproviders/whitepapers/ split_dns.asp>

Pike, John. "FAS Intelligence Resource Program, TEMPEST". Federation of American Scientists. Feb 11, 2000. Mar 20, 2005. <http://www.fas.org/irp/program/security/tempest.htm>

Rekhter, Y., B. Moskowitz, D. Karrenberg, G. J. de Groot , and E. Lear. "RFC 1918 Address Allocation for Private Internets". Internet FAQ Archives. Feb 1996. Mar 20, 2005. <http://www.faqs.org/rfcs/rfc1918.html>

Rosenberg, Burt. "Split DNS". University of Miami, Department of Computer Science. Burt Rosenberg. Aug 2, 2002. Mar 20, 2005. <http://www.cs.miami.edu/~burt/local/cs-arch-2002/split-dns.html>

squid@visolve.com. "Configuration Manual for Squid 2.4 Stable x". Squid Web Proxy Cache. ViSolve. May 26, 2002. Mar 20, 2005. <http://squid.visolve.com/ squid/squid24s1/squid24s1.pdf>

Tumbleweed Communications Corp. "MailGate Email Firewall". Tumbleweed. 2005. Mar 20 2005 <http://www.tumbleweed.com/products/emailfirewall.html>

Visa USA. "Payment Card Industries Security Audit Procedures". Visa.com. 2005. Mar 20, 2005. <http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Security_Audit_Procedures_and_Reporting.doc?it=il|/business/accepting_visa/ops_risk_management/cisp_training_tools.html|PCI%20Security%20Audit%20Procedures%20and%20Reporting>

Zoom Technologies. "Zoom Air AP11, 11 Mbps IEEE 802.11b Wireless

Hardware Access Point, Model 4120". Zoom.com. 2001. Mar 20, 2005. <http://www.zoom.com/graphics/datasheets/networking/41200401.pdf>

Last Updated: December 19th, 2018

# Upcoming SANS Training

**Click here to view a list of all SANS Courses**

| | | | |
|---|---|---|---|
| SANS Sonoma 2019 | Santa Rosa, CAUS | Jan 14, 2019 - Jan 19, 2019 | Live Event |
| SANS Threat Hunting London 2019 | London, GB | Jan 14, 2019 - Jan 19, 2019 | Live Event |
| SANS Amsterdam January 2019 | Amsterdam, NL | Jan 14, 2019 - Jan 19, 2019 | Live Event |
| SANS Miami 2019 | Miami, FLUS | Jan 21, 2019 - Jan 26, 2019 | Live Event |
| Cyber Threat Intelligence Summit & Training 2019 | Arlington, VAUS | Jan 21, 2019 - Jan 28, 2019 | Live Event |
| SANS Dubai January 2019 | Dubai, AE | Jan 26, 2019 - Jan 31, 2019 | Live Event |
| SANS Las Vegas 2019 | Las Vegas, NVUS | Jan 28, 2019 - Feb 02, 2019 | Live Event |
| SANS Security East 2019 | New Orleans, LAUS | Feb 02, 2019 - Feb 09, 2019 | Live Event |
| SANS SEC504 Stuttgart 2019 (In English) | Stuttgart, DE | Feb 04, 2019 - Feb 09, 2019 | Live Event |
| SANS Anaheim 2019 | Anaheim, CAUS | Feb 11, 2019 - Feb 16, 2019 | Live Event |
| SANS Northern VA Spring- Tysons 2019 | Vienna, VAUS | Feb 11, 2019 - Feb 16, 2019 | Live Event |
| SANS London February 2019 | London, GB | Feb 11, 2019 - Feb 16, 2019 | Live Event |
| SANS Zurich February 2019 | Zurich, CH | Feb 18, 2019 - Feb 23, 2019 | Live Event |
| SANS Secure Japan 2019 | Tokyo, JP | Feb 18, 2019 - Mar 02, 2019 | Live Event |
| SANS Scottsdale 2019 | Scottsdale, AZUS | Feb 18, 2019 - Feb 23, 2019 | Live Event |
| SANS New York Metro Winter 2019 | Jersey City, NJUS | Feb 18, 2019 - Feb 23, 2019 | Live Event |
| SANS Dallas 2019 | Dallas, TXUS | Feb 18, 2019 - Feb 23, 2019 | Live Event |
| SANS Riyadh February 2019 | Riyadh, SA | Feb 23, 2019 - Feb 28, 2019 | Live Event |
| SANS Reno Tahoe 2019 | Reno, NVUS | Feb 25, 2019 - Mar 02, 2019 | Live Event |
| Open-Source Intelligence Summit & Training 2019 | Alexandria, VAUS | Feb 25, 2019 - Mar 03, 2019 | Live Event |
| SANS Brussels February 2019 | Brussels, BE | Feb 25, 2019 - Mar 02, 2019 | Live Event |
| SANS Baltimore Spring 2019 | Baltimore, MDUS | Mar 02, 2019 - Mar 09, 2019 | Live Event |
| SANS Training at RSA Conference 2019 | San Francisco, CAUS | Mar 03, 2019 - Mar 04, 2019 | Live Event |
| SANS Secure India 2019 | Bangalore, IN | Mar 04, 2019 - Mar 09, 2019 | Live Event |
| SANS London March 2019 | London, GB | Mar 11, 2019 - Mar 16, 2019 | Live Event |
| SANS St. Louis 2019 | St. Louis, MOUS | Mar 11, 2019 - Mar 16, 2019 | Live Event |
| SANS Secure Singapore 2019 | Singapore, SG | Mar 11, 2019 - Mar 23, 2019 | Live Event |
| SANS San Francisco Spring 2019 | San Francisco, CAUS | Mar 11, 2019 - Mar 16, 2019 | Live Event |
| ICS Security Summit & Training 2019 | Orlando, FLUS | Mar 18, 2019 - Mar 25, 2019 | Live Event |
| SANS Secure Canberra 2019 | Canberra, AU | Mar 18, 2019 - Mar 23, 2019 | Live Event |
| SANS Norfolk 2019 | Norfolk, VAUS | Mar 18, 2019 - Mar 23, 2019 | Live Event |
| SANS Munich March 2019 | Munich, DE | Mar 18, 2019 - Mar 23, 2019 | Live Event |
| SANS Bangalore January 2019 | OnlineIN | Jan 07, 2019 - Jan 19, 2019 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |