GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Securing GIAC Enterprises' Operations

Kenneth Ciangura

GIAC GCFW Practical
Version 4.0

Date: October 31, 2004

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Abstract

This document explores security issues related to GIAC Enterprises, an online company selling fortune cookies. The first part is a research based paper outlining solutions to securely integrate a wireless extension of the network in a new manufacturing plant. The second part describes the defence-in-depth security architecture in place on the network with the different components used to achieve this. Finally, the main firewall security policy is described in detail.

© SANS Institute 2000 - 2005, Author retains full rights.

Table of Contents

1 Assignment 1: Future state of security technology: Wireless Network Integration 3
1.1 Business Motivation 3
1.2 Wireless Network Security 3
1.2.1 Inherent security problems with WLAN 3
1.2.2 The WLAN security evolution 5
1.2.2.1 WEP 5
1.2.2.2 802.11i and WPA 6
1.2.2.3 802.1x and EAP methods 7
1.2.3 IPsec VPN over WLAN transport 8
1.2.4 Hybrid network architecture 8
1.3 Selecting a Solution for GIAC Enterprises 9
1.3.1 Possible solutions 9
1.3.2 Network and Security Configurations 10
1.3.3 Required Hardware 11
1.3.4 Operations and Maintenance 12
2 Assignment 2 – Security Architecture 13
2.1 Introduction 13
2.2 GIAC Enterprises' Business Operations 13
2.3 Network and Security Architecture 15
2.3.1 Network architecture 15
2.3.2 Network Devices 18
2.3.2.1 Filtering Router 18
2.3.2.2 Firewall 18
2.3.2.3 VPNs 19
2.3.2.3.1 Site-to-site VPN 19
2.3.2.3.2 Dial-in VPN 19
2.3.2.4 Internal Router 21
2.3.2.5 Network Based IDS 22
2.3.3 Remote Offices 23
2.3.4 Servers 23
2.3.5 GIACE Users 23
2.3.5.1 User workstations 23
2.3.5.2 User training 24
2.3.6 IP Addressing Scheme 24
2.3.7 Defence-in-Depth Strategy 24
3 Assignment 3 – Firewall Policy 26
3.1 Inbound Rules 26
3.2 Outbound Rules 26
3.3 Forwarding Rules 26
4 Appendix A - IP Addressing Scheme 30
5 Appendix B – Server Details 32
5.1 Service Network (DMZ) servers 32
5.2 Internal Servers 33

© SANS Institute 2000 - 2005 Author retains full rights.

6 Appendix C – Firewall Rules 36
7 List of References 40

List of Figures

Figure 1 - GIAC Enterprises Network 16
Figure 2 – Network Security Equipment connectivity 17

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

1 Assignment 1: Future state of security technology: Wireless Network Integration

1.1 Business Motivation

European based GIAC Enterprises (GIACE), the world leader in the online fortune cookie business, has recently started manufacturing edible fortune cookies. Until now, GIAC was selling fortune cookie sayings over the Internet through its myfortune.giac.com™ branded portal. This portal gives myfortune customers worldwide different service options: purchasing bulk fortune cookie saying or subscribing to daily fortune cookies. The customers can select whether to receive cookies in their e-mail or on their mobile phone through Short Message Service (SMS).

Recently, GIAC has acquired a small cookie manufacturing plant in an industrial area close to its main offices and has invested into turning the plant into a state-of-the-art fortune cookie manufacturing business. Fortune cookie sayings are securely retrieved from the GIAC network, printed onto small slips of paper and are then embedded into the cookies themselves before being baked. The fully automated process then places the cookies into containers, which are wrapped, sealed and packed into boxes ready for distribution. Currently GIAC ships only to European Union (EU) countries, but it plans to expand its operations in order to cater for other markets. A physical extension to the current plant is already underway, but GIAC wants to make the manufacturing process as efficient as possible to reduce overheads and to control costs. GIAC has decided to use only wireless devices on the shop floor, namely wireless handheld barcode scanners used to track stock movements and wireless laptops for plant managers to control the various manufacturing stages while being free to roam about the plant.

1.2 Wireless Network Security

1.2.1 Inherent security problems with WLAN

The introduction of Wireless Local Area Network (WLAN) has proven to be a challenge for people in charge of protecting organisations' perimeters. Whereas before one could define the perimeter of the network fairly easily, with only a handful of potential entry points to the network, such as the Internet access router and a couple of dial-up modems, WLANs are now potentially exposing any

© SANS Institute 2000 - 2005 Author retains full rights.

part of the network to anyone just outside the physical boundary of the organisation or even of a remote worker's home.

Carrying network traffic over the radio waves is inherently insecure; moreover this is multiplied by orders of magnitude if certain basic precautions are not taken. Even the most experienced security professionals are overwhelmed by the number of steps that must be taken in order to ensure a safe deployment of WLAN in an enterprise, and also to ensure that other employees are not breaching the security policy. In fact, one of the most serious problems is that WLAN equipment has become very cheap, and it is tempting for employees both in the office and at home to install access points, most probably with their default factory settings without any authorisation whatsoever from their network administrators. This immediately leads to serious problems, due to any of the following issues. While none of the proposed solutions is enough on its own, a defence in depth strategy requires that all possible precautions are taken in order to achieve the most secure system possible.

Broadcast (Service Set Identifier) SSID: This is comparable to hanging an Ethernet hub out of the window onto the roadside together with an advert banner and starting shouting "Hi everyone! Here's my network; anyone interested?" This "open network" is the default configuration of most access points off the shelf. While running a "closed network" will not keep away determined attackers, it surely helps not to attract unnecessary attention.

No user or device authentication: Wireless networks with no authentication will allow anyone into the network. This should not be the case for any organisation, where some type of user authentication is a must before granting the users access to any part of the network. In cases where handheld devices are shared between more users, such as WLAN scanners and Voice over IP (VoIP) phones, device specific authentication should be used if user authentication is not possible. From the WEP experience, one can safely state that shared keys don't work due to the large administrative overheads, especially in environments with more than a couple of devices.

No or very poor encryption: Once users are authorised to use the wireless network, it is essential to ensure that the packets visible over the air are not readable or modifiable by anyone. While WEP provides some type of encryption, one should not allow a false sense of security to prevail: in fact it was found that the encryption used in WEP as easily broken and is also subject to man in the middle attacks. A strong encryption and data integrity solution is needed to overcome this. WPA and later WPA2 (802.11i) were designed to provide a suitable solution for the years to come.

No filtering (MAC and IP): In line with a system wide defence in depth strategy, MAC address filters and IP filters should be employed where possible to make it more difficult for unauthorised people to gain access to the network. It should be noted however, that a determined attacker could still spoof both the IP address and the MAC address of their machine.

© SANS Institute 2000 - 2005 Author retains full rights.

No Intrusion detection: An intrusion detection system should be aware of the wireless network configuration in order to detect anomalies. A useful addition is a module to detect rogue access points that are not authorised by the system administrators. Rogue access points can be either unauthorised access points installed by employees, or else access points set up by attackers to modify traffic passing through them, leading to man in the middle attacks and potentially stealing other credentials and confidential information such as passwords and credit card details.

Denial of service attacks: Over the radio part, denial of service is possible either by frequency jamming or interference with devices on the same frequency (these can even be other access points or Bluetooth devices). Also, management requests such as association and disassociation are not authenticated if the network is open (i.e. if no authentication is necessary), so the radio network can be flooded with these messages and resulting in a degradation or loss of service.

1.2.2 The WLAN security evolution

1.2.2.1 WEP

WLAN (Wi-Fi) 802.11 standards originally provided security through Wired Equivalent Privacy (WEP). As its name implies, WEP was intended to provide over the air confidentiality equivalent to that available on wired networks. However, WEP immediately had its security weaknesses exposed since it was not thoroughly tested before it found its way into the 802.11 standards.

Although WEP gives some basic protection from the casual eavesdropper, it is generally considered broken. The encryption provided by WEP using the RC4 algorithm is very weak and one of the main problems with WEP is the fact that it does not cater for key management and distribution and does not provide user authentication. There is no way to disable individual users, neither by disabling the user account nor by mechanisms such as certificate revocation as is the case with Public Key Infrastructure (PKI) systems. Since the same shared key is used over and over again, this provides an opportunity for hackers to deduce the key fairly easily. Along with the shared key, which is fixed at 40 bits (later versions support 128 bit keys), an Initialisation Vector (IV) of 24 bits is used. However this does not add much security since due to its small size the IV is repeated often. In a busy network, keys can be cracked in as little as 15 minutes [1] using an FMS type attack [2] which exploits weaknesses in the RC4 key scheduling algorithm and requiring only one million packets using the same key. In [3] RSA Security discusses the fact that the cause of the problem is key generation and not the RC4 algorithm itself. In fact, RC4 is used in SSL without being vulnerable to any known attacks since the key changes with each session.

© SANS Institute 2000 - 2005 Author retains full rights.

Another crucial point is that since the key has to be added manually to all devices and access points, administrators tend not to change the keys often enough due to the large manual overheads and it is very difficult to determine if the key has been broken until it's too late.

To overcome these problems, various vendor specific WEP variations followed, including the use of longer (128 bit) WEP keys and dynamically changing WEP keys over the air, but still these suffered from major inter-operability problems with other vendors' equipment and the key management issue for user authentication was still not solved. Another option was to disable WEP altogether and instead use a VPN on top of the unsecured network layer. Still the solution had to be found how to provide a standards- based strong encryption and data integrity solution with authentication and access control.

1.2.2.2 802.11i and WPA

The IEEE 802.11i specification was designed to provide a framework for security mechanisms on 802.11 compliant WLAN devices. Based on IEEE 802.1x port based access control already used on wired networks, and Extensible Authentication Protocol (EAP) [4], 802.11i is intended to provide robust security to address all the weaknesses of WEP while being flexible enough to be adapted to the security needs during the foreseeable future. However, since the 802.11i specification process was lengthy and the security needs of the industry were pressing, the Wi-Fi Alliance and IEEE introduced Wi-Fi Protected Access (WPA) as a temporary solution, which implemented a subset of features from 802.11i until the full 802.11i (also known as WPA2) was fully standardised. WPA was intended to be used on existing 802.11 equipment requiring only firmware and software updates, but the full WPA2 requires a major investment since new hardware devices would need to be introduced due to the new AES-CCMP encryption used in WPA2. 802.11i was finally ratified on the 24th June 2004.

WPA security uses 802.1x and EAP for mutual authentication between client and network devices. A new protocol, the Temporal Key Integrity Protocol (TKIP) was introduced to provide dynamically changing keys on top of the existing WEP (40 or 128 bit) RC4 encryption. Thus keys are changed every 10000 packets in order to minimise the useful time window for attackers intending to break the keys. Also, a Message Integrity Check (MIC) known as Michael was added to ensure data integrity.

WPA2 security architecture is similar to WPA except that it uses the new industry standard AES-CCMP encryption instead of WEP RC4 with TKIP and MIC, and it provides a few other features such as "secure IBSS, secure fast handoff, secure de-authentication and disassociation" [5]. WPA2 requires new hardware in most devices so most current WPA deployments will not be changed immediately. However, as new products are certified as WPA2 compliant, organisations with security policies requiring very strong encryption can now consider deploying

© SANS Institute 2000 - 2005 Author retains full rights.

wireless solutions. It is worth pointing out however, that WPA2 is not addressing any weaknesses found in WPA, it only provides stronger encryption.

1.2.2.3 802.1x and EAP methods

The 802.1x protocol is used to control how devices are authenticated before they are allowed access to the LAN. To achieve this, 802.1x compliant Ethernet switches and Wireless Access Points set their ports in unauthorised mode, allowing only the transport of EAP authentication traffic. The client device, known as the supplicant, will provide its authentication credentials to the authenticator, being the network switch or in case of 802.11 the Wireless Access Point (otherwise the Access Point can be transparent to 802.1x since this can be handled by a Wireless Service Gateway (WSG) behind the Access Point). The authenticator will relay these credentials to the authentication server, typically a Remote Authentication Dial In User Service (RADIUS) server. If successful, the reply will include authorisation parameters, such as the Virtual LAN (VLAN) to be assigned to that port. Thus the port is configured for client access depending on the authenticated user (or device) profile that is defined on the network, for example in a RADIUS user account or a Windows 2000/2003 Domain Active Directory with Internet Authentication Service (IAS) providing the RADIUS interface. The authentication to be used is defined through EAP methods that must be supported by each one of the supplicant, authenticator and authentication server. Negotiation of encryption parameters and keys is dependent on the particular EAP method used.

WPA supports two modes: WPA Personal is intended mainly for home use and a username and password defined on the access point are needed for authentication; WPA Enterprise requires an external authentication server supporting EAP.

Different authentication mechanisms, usually promoted by different vendors who contributed in some way to their specification, are known as EAP methods. Some are based on username and password; others require one or two way certificate authentication while others support smart cards or one time passwords (OTP). A good description of different EAP methods can be found in [6].

Of particular interest for the GIAC warehouse scenario are EAP methods using Public Key Infrastructure (PKI) certificates, namely EAP-TLS, EAP-TTLS and EAP-PEAP. PKI provides manageable access control through certificate expiry and revocation. Furthermore certificates can be used both for user and machine authentication.

© SANS Institute 2000 - 2005 Author retains full rights.

1.2.3 IPsec VPN over WLAN transport

An alternative to WLAN security mechanisms is to disable WEP and WPA/WPA2 altogether and instead use IPsec Virtual Private Network (VPN) security (authentication, encryption and integrity) between the client and a VPN gateway. Some organisations may prefer this approach since they would be using the same tried and tested VPN technology that they have already been using over the Internet. Standard precautions such as: MAC and IP filters on the access points and not broadcasting the SSID, should still be taken.

VPN clients should use personal firewalls with split tunnelling disabled so that once connected to the VPN, all traffic would pass through the VPN gateway, thus minimising the risks of session hijacking.

In order to connect to the VPN gateway, VPN clients would need to first get an IP on the local access network. Thus a DHCP server is needed to assign an IP address and related network settings to the device once it's associated with the WLAN SSID. Most probably a DNS server will also be used so that the name of the VPN gateway would be resolvable. Alternatively, the VPN gateway would be reached via its IP address so the DNS server is eliminated. The access point, Ethernet switch (using VLAN ACLs) or router capable of packet filtering would need to restrict access to the DHCP and DNS servers and IPsec traffic (IKE, ESP and perhaps ICMP for troubleshooting) to the VPN gateway. No other services should be accessible for devices on this unauthenticated network. It is also a good idea to place an Intrusion Detection System (IDS) probe on this access network to detect any attacks. Only legitimate users should be able to authenticate to the VPN gateway and get the authorisation to access the internal network. Finally, decrypted user traffic coming out of the VPN gateway should still be treated with caution, by applying the required packet filters and possibly monitoring with another IDS probe. This would ensure a layered defence in depth architecture.

1.2.4 Hybrid network architecture

WPA and WPA2 technologies, whilst providing a flexible architecture that can be extended with new authentication mechanisms in the future, may be considered to be still immature to deploy in the field by some organisations with stringent security policies. On the other hand, the IPsec solution described above lacks protection of the service network (DHCP, DNS and VPN servers) before the VPN tunnel itself is established.

A solution can be designed that takes advantage of both technologies and increases the layers of defence protecting the internal networks. It is possible to overlay the WPA 802.1x/EAP and IPsec solutions. In this way WPA would be used to allow access to a DMZ or service network comprising of the DHCP, DNS

© SANS Institute 2000 - 2005 Author retains full rights.

and VPN servers. Then a VPN tunnel would be established with the VPN gateway. In this way, two authentication stages are necessary and all traffic to the internal network would be encrypted twice. Various options of deploying this method are discussed in [1].

However the following points should be considered: (a) network administrators need to manage the two infrastructures, (b) traffic throughput will be reduced due to the extra protocol headers, and due to the processing power needed to encrypt traffic twice, and (c) increased complexity for the network users.

1.3 Selecting a Solution for GIAC Enterprises

In the previous section we have seen how the new specifications for WLAN security coupled with best practices and technologies already proven on wired networks can be used to mitigate known security risks. Although no panacea can be found since new vulnerabilities and attacks are discovered day by day, one can take all the precautions necessary in order to allow the business to take advantage of benefits provided by new technologies in the safest way possible.

GIAC Enterprises' warehouse will use WLAN to increase efficiency of the shipping employees who will be free to move about the warehouse floor and the loading bays while updating stock movements in real time. Also, warehouse managers will be able to move out of their offices and roam about the shop floor with their laptops while still being able to access their email and the GIAC Intranet. They will be able to monitor the business processes for quality control and to process new orders as they are generated.

1.3.1 Possible solutions

The chosen solution needs to take into consideration the two types of devices that will need to connect to the wireless network for different purposes.

The barcode scanners will need to update stock quantities on the stock management front end server located on site at the warehouse. The scanners are not owned by any particular employee, so user authentication is not strictly needed. However, machine authentication will be necessary.

The laptops, on the other hand, are assigned to the individual warehouse managers by GIAC's IT Department. Thus user authentication should be used on the laptops.

Since the warehouse is a new investment for GIAC, the organisation has decided to use the latest technologies available wherever possible. New access points will be purchased, so 802.11i certified (WPA2) access points will be used. In this way AES-CCMP encryption will be available.

© SANS Institute 2000 - 2005 Author retains full rights.

Authentication methods will be chosen to reflect the user/device considerations above. So the barcode scanners will authenticate with EAP-TLS using machine certificates, while the laptops will use EAP-TLS with user certificates. The certificates will be generated by a local Certificate Authority (CA) which will be part of GIAC's Windows 2003 Active Directory Domain infrastructure.

1.3.2 Network and Security Configurations

The access points will be connected to the Ethernet Switch using CAT5 UTP cables. A separate management VLAN will be used to manage the access points using SSH. All other management interfaces (Telnet, HTTP, SNMP) will be disabled, but read-only SNMP with a modified community string will be used to monitor the access points. The access points will be configured to send SNMP traps to a Network Management Server (NMS) located at the central GIAC site. The SSID named "giac" on the access points will not be broadcast in order not to attract potential attackers.

The access points will be configured to use the Windows 2003 IAS server cluster (for redundancy) at the central GIAC site as RADIUS servers for authentication, authorisation and accounting. Only 802.1x traffic will be allowed before EAP-TLS authentication takes place. Then, if the authentication is successful, the RADIUS server will determine what VLAN the device will be placed in.

The Certificate Authority will be used to generate both machine and user certificates for the barcode scanners and laptop users respectively. These certificates will be installed on the devices, along with the CA root certificate. The time on the devices needs to be synchronised with a Network Time Protocol (NTP) server to reduce time differences which may cause the devices to show a warning if they erroneously think that the certificate is expired. If this happens often, and the user get accustomed to accept the certificate just the same, then a man in the middle attack that uses a rogue access point with fake certificates may go undetected by users [7].

When a barcode scanner authenticates successfully to the network (using the machine certificate), it is assigned to a VLAN that can only see the stock management front end server and a DHCP server. The latter will assign the network settings to the scanner so that it can communicate with the stock management server. The scanner can then safely transmit updates to this server.

When a laptop user authenticates successfully to the network (using the user certificate and Windows 2003 Domain username and password), it is assigned to a VLAN that can see a local DHCP proxy and the ADSL router. The IP address and related network settings are assigned by the local DHCP proxy. Traffic from the laptop can then reach the central GIAC site over an IPsec tunnel over a private connection between the ADSL router and the central GIAC ATM router. Encapsulating Security Payload (ESP) is the chosen IPsec method, with AES (256 bit) encryption and SHA1 integrity checking. Since the warehouse is in the

© SANS Institute 2000 - 2005 Author retains full rights.

vicinity of the central GIAC site, a local data provider will be used to provide a Classical IP (CIP) point-to-point private connection between the two sites instead of going over the Internet. A Permanent Virtual Circuit (PVC) from the ADSL line at the warehouse will be cross connected with a PVC on the Asynchronous Transmission Mode (ATM) layer over optical fibre entering the GIAC router. This private connection will have a dedicated 1024/512 kbps towards the ADSL router. Thus confidentiality is ensured between the two sites.

The stock management front end server will communicate over the IPsec connection to the main stock management server operated by the logistics section on the GIAC network. In this way, logistics will have a real time view of the stock status at the warehouse.

Multiple filter layers can be configured: the Ethernet switch can use its VLAN ACLs to restrict traffic in the warehouse LAN. The ADSL router can perform additional stateful packet filtering for traffic leaving the warehouse, while the GIAC ATM router at the border and the main firewall can perform additional filtering as required. The combination of different layers of packet filters and firewalls from different vendors is useful to implement a defence in depth strategy since if one implementation is flawed or if a filter configuration is incorrect, then another filter behind it might provide the intended functionality.

Also, IDS probes both on the warehouse LAN and between the GIAC perimeter devices helps to detect malicious activity and to provide substantial logging and traces for better incident handling.

All access point, switch and router logs will be sent to a central Syslog server located at the main GIAC site. The IDS and all network and server equipment will be managed centrally from the GIAC network.

1.3.3 Required Hardware

The following hardware is required at the warehouse:

Item	Specification	Quantity
Access Point	Supports 802.11b, 802.11i, 802.1x and EAP-TLS	6 (Quantity determined after a radio site survey: needed to cover warehouse and loading bays)
Ethernet Switch	802.1q VLAN, VLAN ACL support, external logging facility, 24 x 10/100 Mbps ports	1
ADSL Router	IPsec support, ADSL interface, stateful packet filtering, external logging facility	1

© SANS Institute 2000 - 2005 Author retains full rights.

IDS	Latest Snort IDS on Linux (i386 hardware) with 2 x 100 Mbps Ethernet interfaces	1
Laptop	Windows XP SP2 with built-in 802.11b interface and 802.11i support and EAP-TLS	1 per warehouse manager
Barcode Scanner	Embedded operating system with built-in 802.11b interface, 802.11i support and EAP-TLS (for example, Intermec 700 Series Mobile Computer[8])	Depends on simultaneous number of employees in shipping shift plus a couple of spares

It is assumed that an ATM router with IPsec support, RADIUS interfaces on the Windows 2003 IAS server and Certificate Authority are in place at the GIAC corporate site.

1.3.4 Operations and Maintenance

The proposed solution introduces a number of new technologies that would require retraining of support staff. Configuration and management of access points, generation of machine and user certificates, installation of certificates on barcode scanners and user laptops as well as the maintenance and log reviewing of the new switches, routers and IDSs will have to be tackled by the IT staff at GIAC. Also, support issues such as radio coverage problems, failure to authenticate to the wireless network and the detection and solution of WLAN specific problems (rogue access points, denial of service attacks, etc) will be encountered at some point.

Extra care has to be taken by IT support staff to ensure that all wireless enabled devices are updated with the latest operating system patches, virus scanner update files and that a personal firewall is installed and duly configured. Otherwise these devices will become unmanageable, especially if the number of such devices increases. It is also important that only IT support staff has access rights to modify system settings on such devices, since users might disable or uninstall any of these software updates without knowing the consequences.

Adequate training should be given to support staff, primarily to raise awareness of the implications of having a wireless network connected to the corporate secure LAN, and the importance of segregating and filtering such traffic as far as possible.

© SANS Institute 2000 - 2005 Author retains full rights.

2 Assignment 2 – Security Architecture

2.1 Introduction

GIAC Enterprises (GIACE) is an online business which markets fortune cookie sayings and sells them over the Internet. With its 50 employees situated at the headquarters, four regional offices distributed worldwide and a warehouse where fortune cookies are manufactured, the GIACE network is essential for the ongoing business operations.

2.2 GIAC Enterprises' Business Operations

In order to understand better what network setup is required to support GIAC Enterprises, we will first go through the various business operations that dictate what interactions the various parties will have with the organisation's infrastructure.

Customers

All of GIAC Enterprises' customers purchase fortune cookie sayings over the Internet through its myfortune.giac.com™ branded portal using SSL. GIAC offers two main product lines:

a) Bulk fortune cookie sayings that are mainly targeted for companies who use them within their own products, such as printed T-shirts and mugs. The fortune cookie sayings are downloadable from the secure portal

b) Daily fortune sayings delivered to individual customers' mobile phones through Short Message Service (SMS) or e-mail.

Suppliers

GIAC purchases its fortune cookie sayings from various suppliers around the world. Every supplier has secure access to an SSL web based portal on GIAC's Content Management System (CMS). Small suppliers use forms to submit new content, while larger suppliers communicate with the CMS using XML web services. A site to site VPN is used between GIAC and suppliers.

Business Partners

GIAC has recently started offering content in different languages, including English, French, Spanish, German, Italian, Portuguese, Chinese and Japanese. Business partners that provide translation services have secure access to an SSL web based portal where according to the user's translation capabilities, a fortune saying is displayed in a language and the translator has to write it in a second

© SANS Institute 2000 - 2005 Author retains full rights.

language. Business partners get paid by GIAC according to the number of phrases translated by their employees.

Some business partners are authorised resellers that purchase bulk fortune cookie sayings and then sell them to regional customers in specialised niche markets through their web sites.

A site to site VPN is used between GIAC and business partners.

GIAC Enterprises employees on the internal network	Employees at the GIAC headquarters and at the four regional offices perform duties such as: Finance and Administration including Human Resources Management; Sales, Marketing and Customer Care including personalised Account Management for larger customers; Information Technology who is responsible for operations and maintenance of all the servers, networking and security and includes a software development section.
GIAC Enterprises remote users	The majority of the sales force is always on the road visiting current and potential customers of bulk fortune cookie sayings. They mostly access the web based e-mail on the corporate intranet servers and other web based applications that include functionality to create and manage customer's accounts. Due to their mobility requirements all of the sales force connects to the GIAC network using General Packet Radio Service (GPRS) with two factor authentication using GSM Subscriber Identity Module (SIM) card and Windows 2003 Domain username and password. A dedicated L2TP/IPsec VPN connection between the GSM/GPRS operator and GIAC Enterprises network is used to transport packets. This allows remote users to securely access the network from virtually everywhere, even when abroad, including on the road or on trains. The in house developed intranet portal is lightweight and well suited for GPRS speeds. Remote users also have the possibility of connecting directly to the VPN server using an L2TP/IPsec connection over the Internet to achieve higher speeds. Authentication is done via through a user certificate and the Windows domain username and password credentials.
Fortune Cookie Manufacturing	GIAC Enterprises has also started manufacturing edible fortune cookies in a warehouse close to its headquarters. Employees in the warehouse are using the latest wireless technologies to securely access the network in the production and shipping stages. A research oriented discussion on the approach to integrate the wireless

© SANS Institute 2000 - 2005 Author retains full rights.

network with the other parts of GIAC Enterprises' network is given in Assignment 1 of this paper. Note: The firewall policy in the next section is not intended to cover the requirements of the warehouse, but only the requirements specified in the GIAC GCFW Practical v4.0.

The general public	The general public can access GIAC Enterprises' web site anytime to learn about its latest offerings and can send queries through e-mail. GIAC Enterprises also offers an e-mail subscription service whereby individuals can choose to receive promotional material in relation to special offers being promoted.

The next section will provide a detailed look at the network components and the security approach that was taken in order to support the above business operations in the safest way possible.

2.3 Network and Security Architecture

As an online business, GIAC Enterprises needs to be connected to the Internet and at all times. The business is centred on its most valuable assets, namely the fortune cookie sayings that it sells. If these are stolen or lost then the whole business is at stake. The servers storing and backing up the fortune cookie sayings and the network that transports them must be treated as the most protected layer in GIAC Enterprises' infrastructure.

The business has also created value chains by enhancing its service offering: different types of customers are catered for both over the Internet and through its regional sales forces, strategic business partners are contributing to extend the customer base by offering translation services and by promoting the product to niche markets all over the globe. Finally, GIAC Enterprises has recently entered the manufacturing business to diversify its product range. Thus the value of the business as a whole depends on the availability and confidentiality of all these interconnections.

2.3.1 Network architecture

The GIAC Enterprises network is depicted in Figure 1. The core network at the GIAC Enterprises headquarters is segmented into four physical networks with their associated IP network. These are: Information Technology; HR, Finances and Administration; Sales and Marketing; and the Operations and Maintenance management network. An internal router connects these networks, providing

© SANS Institute 2000 - 2005 Author retains full rights.

connectivity to the outside world and at the same time filtering packets that are routed between the networks.

The internal router connects to the main Internet firewall. This firewall has an interface on the services network (the Demilitarized Zone, or DMZ), another interface towards the external router and connectivity towards the Windows 2003 VPN server used for remote user VPN connections. The main firewall itself is also an IPsec VPN gateway for site-to-site VPN connections with business partners, suppliers, the warehouse and the regional offices.

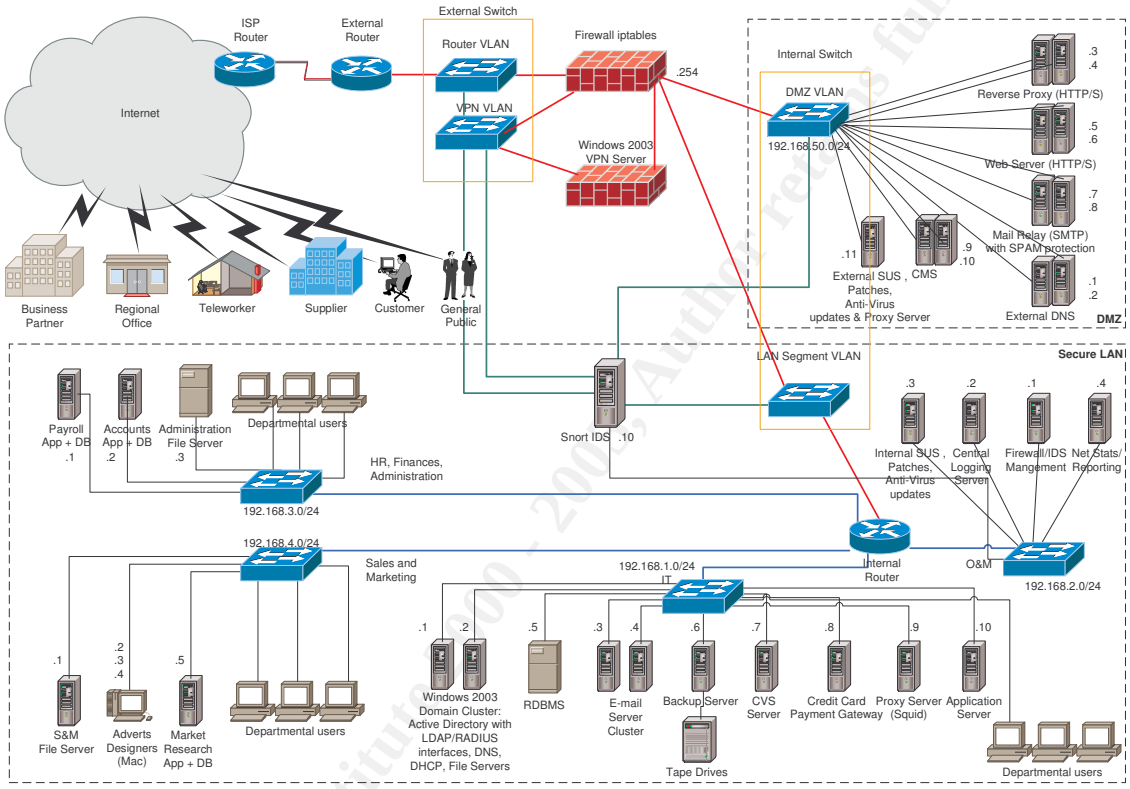

Figure 1 - GIAC Enterprises Network

The external router has an OC-3 interface for ATM over optical fibre connectivity a network services provider. This gives GIACE the advantage of using ATM's flexibility with regards to connection setup. One ATM PVC connects the external router to the Internet Service Provider (ISP) router using a classical IP connection. The ISP routes all traffic with destination IP on the a.b.c.0/24 public IP network, which was purchased by GIACE, towards the external router.

Private connections can be set up over the same ATM link. One such connection is used for the warehouse described in Assignment 1. The network services provider cross connects an ATM PVC on the same ATM link to a PVC on the ADSL router at the warehouse, and a classical IP connection is used between the two routers.

An IDS was set up to monitor traffic in key locations of the network. It has four probes that analyse traffic between the external router and the firewall, traffic

© SANS Institute 2000 - 2005 Author retains full rights.

coming out of the Windows 2003 VPN server back to the firewall, traffic coming out on the DMZ network and traffic entering the core LAN. All IDS probe interfaces are not assigned IP addresses and are connected to mirrored ports which are not members of any VLAN so that the IDS passively sees all the traffic without introducing any packets in the network and without the IDS being reachable from any of the networks. Another interface on the IDS connects it to the O&M network for management and logging.

Two Ethernet switches configured with VLANs and port mirroring are used as part of the perimeter infrastructure to provide connectivity between these devices and at the same time mirroring port traffic to be used by the IDS's probes. The internal switch is also used to connect the servers in the DMZ to the network. The VLAN configuration can be seen in detail in Figure 2.

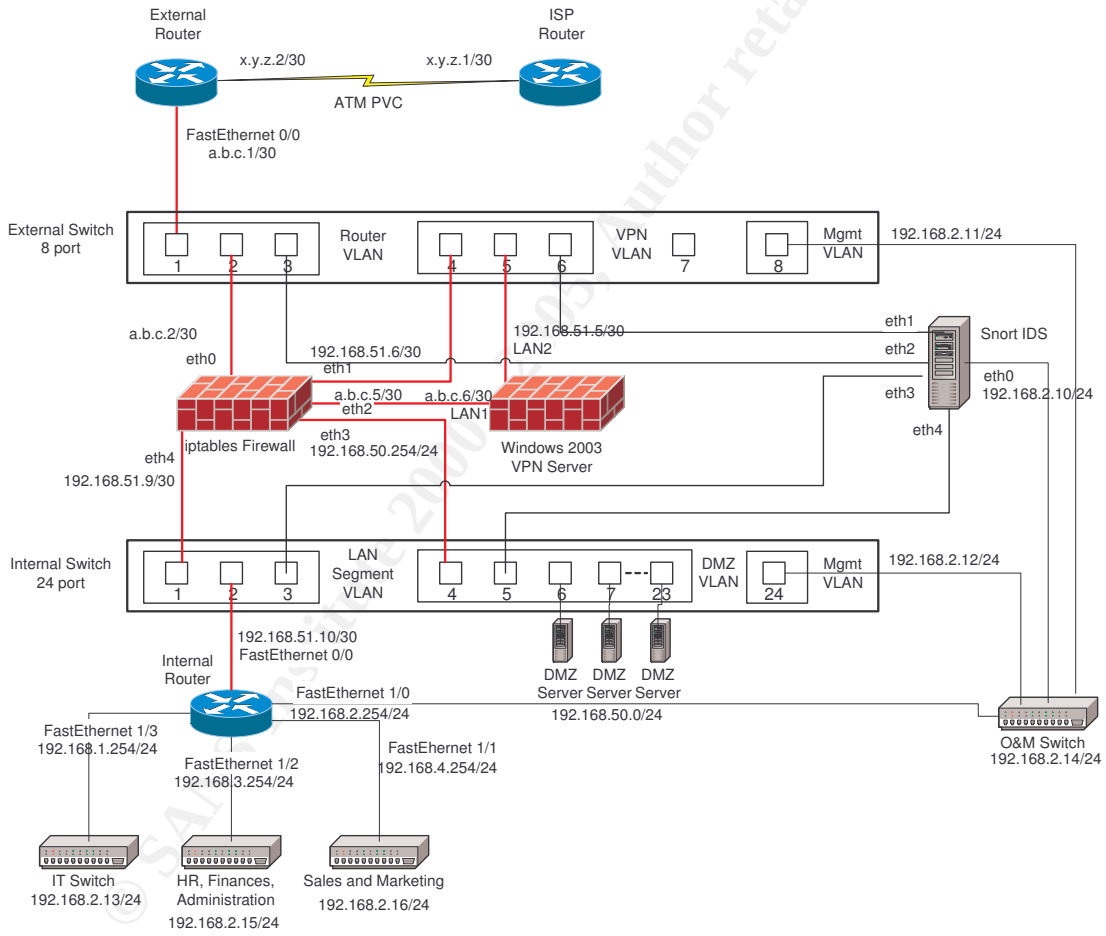

Figure 2 – Network Security Equipment connectivity

In the following sections, we will have a detailed look at each of these security components.

© SANS Institute 2000 - 2005 Author retains full rights.

2.3.2 Network Devices

This section will list all the key security devices, together with their security functionality and their role in the overall network security architecture.

2.3.2.1 Filtering Router

The external router is a Cisco 2691 Access Router with an OC-3 ATM Interface and IOS version 12.2(13)T Plus IPsec / Firewall / IDS. Apart from routing traffic to and from the ISP and the other private connections, this router uses stateful packet filtering (extended access lists) for inbound traffic from the ISP interface as a first line of defence against spoofed IP packets (having source IP addresses from GIACE's public IP address range a.b.c.0/24) and also filters out any unwanted traffic such as RFC 1918 private addresses and multicast addresses.

The router denies any traffic directed towards its interfaces. In this way, the router is not accessible from outside the network.

Only the required services are allowed through the router from the ISP interface, such as HTTP and HTTPS for website access, SMTP for email, DNS, ICMP and the IPsec protocols UDP port 500 for IKE and IP protocol 50 for ESP. Return traffic for outgoing packets is also allowed. All other traffic is dropped. In this way any vulnerability related to other services will never get past this router. The warehouse interface only allows the IPsec protocols through since all traffic from the warehouse is encrypted in the VPN tunnel.

The router is configured to send all logging to a Syslog server, and also sends SNMP traps to the NMS. It also allows read only SNMP access from the internal interface only. Telnet and HTTP management are disabled on the router, and all management takes place through Secure Shell (SSH). Ntop [9] is used to process Cisco Netflow [10] data for traffic analysis.

The Router Auditing Tool (RAT) [11] available from the Centre for Internet Security (CIS) is used periodically to assess the router setup. RAT points out any settings which were overlooked and suggests improvements based on best practices. When these suggestions are implemented there is less chance that the router will be vulnerable to any known attack patterns.

2.3.2.2 Firewall

The main Internet firewall is an iptables (netfilter) [12] based firewall on a Red Hat 9 Linux OS [13] on a Dell PowerEdge 2650 server [14]. The iptables firewall is a stateful packet filter which is very flexible both in the policy configuration, network address translation (NAT) options and extensive logging capabilities. The throughput on a mid range server such as the Dell is very well suited to handle the type of traffic expected by GIACE on its perimeter.

The Dell server provides a hardware RAID controller with up to 5 hot swappable SCSI hard disk drives, two Intel Xeon processors, two hot swappable power supply unit (PSU), two on board Gigabit Ethernet ports and multiple PCI cards for

© SANS Institute 2000 - 2005 Author retains full rights.

additional Ethernet ports (5 in total). This ensures high availability and provides the required performance (this firewall is also used to terminate site-to-site VPN tunnels).

The firewall defines rules for traffic directed towards the firewall, traffic originating from the firewall, traffic forwarded by the firewall as well as source and destination NAT. Each rule can specify the source and destination interface of traffic for additional control. The firewall policy is described in detail in section 3.

All iptables logs are redirected to the local and an external Syslog server. The firewall is only managed using SSH with RSA key authentication and read only SNMP from the internal interface. SNMP traps are sent by the firewall to the NMS. SFTP through SSH is used instead of FTP.

Scripts on the firewall are used to filter the logs from out any known dropped packets to leave those whose patterns are not known. These log entries, coupled with output from the IDS, helps the incident response team to detect anomalies quickly and to take the necessary actions in the shortest time possible.

2.3.2.3 VPNs

As already outlined above, two types of VPN servers are used by GIACE:

2.3.2.3.1 Site-to-site VPN

The site-to-site VPN gateway is used for IPsec tunnels from the business partners, suppliers, the GIACE warehouse and the regional offices located worldwide. Openswan [15] is the selected VPN solution for site-to-site tunnels. X.509 certificate mutual authentication is used with the remote VPN gateways. The certificates are generated by a local Certificate Authority.

256 bit AES encapsulating security payload (ESP) encryption is used together with SHA1 integrity checking for all VPN tunnels.

Both the external router and the main Internet firewall policies allow IKE and ESP traffic towards the VPN gateway. Since the VPN gateway is the firewall itself, traffic coming out of the IPsec tunnels will be filtered again as it comes out of the tunnel.

Thus the Internet firewall has rules to allow IKE and ESP packets from the known remote VPN gateways and other rules to allow only the required traffic coming out of the VPN tunnels towards any services on the DMZ. These rules are described in detail in Section 3.

The Dell hardware described above scales well to cope with the encryption and decryption of packets required for IPsec VPN functionality.

2.3.2.3.2 Dial-in VPN

GIACE employees who are equipped with laptops required remote access to the network in order to use e-mail and other intranet applications. Shared folders on

© SANS Institute 2000 - 2005 Author retains full rights.

the Windows 2003 network are also used to store documents that need to be viewed and edited by different parties.

GIACE offers two methods for remote users to connect to the network, both based on an IPsec VPN. The Windows 2003 VPN server is used in both cases to terminate the VPN endpoint and to perform user authentication and authorisation.

2.3.2.3.2.1 VPN access over the Internet

The laptops are configured by the IT department with an IPsec certificate generated by a local Certification Authority which forms part of the Windows domain. An L2TP/IPsec VPN connection is set up on the laptop and configured to access the Windows 2003 VPN gateway, authenticating with the certificate and also requiring a valid domain user name and password. The Active Directory user must have dial-in access enabled and the VPN server's Routing and Remote Access policy must be defined to allow users to be authenticated against the Internet Authentication Service (providing RADIUS services) and to be granted access to the network.

The VPN server is configured to assign the network settings to an authenticated user based on the user's department: each department has an associated IP address pool. In this way every department's users are given restricted access as defined by the security policy.

Windows 2003's IPsec VPN supports Network Address Translation Traversal (NAT-T). This is a useful feature since some Internet service providers, particularly Wireless ISPs (providing public Wi-Fi hotspot access to the Internet) use NAT for user traffic going over the Internet.

2.3.2.3.2.2 Wireless GPRS access

Since most of the remote users spend most of their time travelling or visiting customers, the need was felt to provide a more mobile form of remote access. For this reason, GIACE has recently set up a dedicated GPRS connection in conjunction with its mobile network operator.

GPRS [16] provides a packet data network over a mobile operator's GSM infrastructure. GPRS speeds are typically in the order of 40kbps downstream and 10-20kbps upstream (depending on the capabilities of the GPRS data card and the network operator being used). The GSM mobile network operator uses its SIM cards in order to authenticate its users. The SIM card is a type of specialised smart card that contains the subscriber's identity and keys that are used for authentication and encryption over the air, and is protected by a 4 digit Personal Identification Number (PIN) for added security in case the SIM card is lost.

In this case the GPRS operator has set up a dedicated Access Point Name (APN) connection for GIACE, which allows only registered GIACE employees with their SIM cards to initiate a connection to this APN. This connection is initiated through the GPRS PCMCIA data card's connection utility, and having the

© SANS Institute 2000 - 2005 Author retains full rights.

SIM card inserted inside the data card. The connection profile should include GIACE's own APN identifier and the user name and password on the Windows 2003 domain. No SIM cards other than those with GIACE's own APN can be used to initiate this connection, and this setting can only be configured by the GPRS operator.

Furthermore, the APN connection setup requires GIACE to authenticate its users. This is achieved by the GSM operator having an L2TP/IPsec connection over a private ATM PVC to GIACE (on the same Windows 2003 VPN server used for Internet VPN access). Each APN connection request initiates an L2TP connection setup request against the VPN server. At this point, the user's username and password credentials are passed on to the GIACE VPN server for authentication. If this is successful, the same network settings as described in the previous section are passed over to the GPRS operator who transparently forwards the same settings to the GIACE remote user's laptop. If the user is not authenticated, then no L2TP connection is established. Thus the user is seamlessly connected to the VPN server with just one connection setup, and this can be done from virtually anywhere even when abroad (depending on the GPRS operator's roaming facilities) on the road or in a hotel. Moreover, GIACE has full control over who connects from the GPRS network since every authentication depends on its policy: individual users can be blocked and the user account can be disabled if the wrong password is entered three times.

From GIACE's perspective, these GPRS connections are seen terminated on the VPN server just like the other VPN connections coming over the Internet and are filtered on the firewall using the same rules. The only difference is that a specific rule allows IPsec traffic from the mobile operator's network to reach the Windows 2003 VPN server. This IPsec tunnel is authenticated using an X.509 certificate.

2.3.2.4 Internal Router

The internal router is a Cisco 2621XM router with 2 on board Ethernet ports and a 4 Ethernet port Network Module (NM-4E). This router is running IOS version 12.2(13)T Plus IPsec / Firewall / IDS. Extended access lists provide stateful packet filtering of traffic between the network segments that are connected by this router. For example, only traffic from the IT network is allowed to reach the O&M network, and only traffic from the IT and O&M is allowed to manage the perimeter network equipment. This filtering router adds an extra layer of protection to the most important services running on the internal network, such as e-mail and intranet services, internal DNS, file servers and the financial and database servers.

GIACE's policy of filtering internal traffic has increased overheads since new rules have to be configured for each new internal connectivity requirement, but on the other hand such filtering makes it harder for potential attackers or even malicious software (malware) such as viruses and worms to propagate freely within the internal network.

Like the other devices, this router is only accessible using SSH with RSA key authentication and is monitored with read only SNMP, while it sends SNMP traps

© SANS Institute 2000 - 2005 Author retains full rights.

to the NMS and logs to the Syslog server. Ntop is used to process Cisco Netflow data for traffic analysis. 802.1q VLAN trunk interfaces are used between the router and the internal switches to provide segregated departmental networks and at the same time allowing the switches to be part of the O&M IP network.

2.3.2.5 Network Based IDS

All traffic entering and leaving GIACE's network is monitored by a network based IDS. The solution chosen is based on the Snort IDS [17]. As seen in the network diagrams, the IDS has four probes onto different segments of the network, covering every interface of the Internet firewall. In this way, any inbound packets that should have been dropped by the firewall but are somehow finding their way through can be detected after careful analysis.

Four instances of Snort are launched, each listening on a different interface and writing to a different log file.

Snort is deployed on a Red Hat 9 operating system running on another Dell PowerEdge 2650 server. There are two motivations for this:

- This server provides the robustness, scalability and performance needed for this solution, and
- Since another similar server is being used for the firewall, GIACE can store spares (hard disks, RAM and PSUs) to cover both servers thus minimising potential downtime while keeping costs down.

The Snort IDS is configured to analyse network traffic without sending any packets onto the monitored network segments. This is achieved by using port mirroring on the Ethernet switches to replicate all the traffic on the interfaces we're interested in and plugging in a probe in that port. A 4 port Ethernet card is being used on the Snort IDS to cover all the network segments.

Since the IDS is transparent to the traffic flowing to and from the firewall, the IDS is not directly reachable via the probe interfaces. A fifth interface, one of the server's on board Ethernet ports, is connected to the O&M switch for management purposes. SSH access to the IDS requires RSA key authentication. SNMP traps are sent to the NMS and SNMP read only access is allowed for monitoring. Snort alerts are sent to the NMS Syslog server so that they are immediately visible on a central server. These alerts are also logged in a MySQL database on the logging server. SFTP through SSH is used instead of FTP.

The IT security team updates the snort rules regularly with signatures of new attacks and the logs are reviewed regularly. Special attention is given to the alerts shown on the filtered probes (VPN, DMZ and LAN segments). Anything unexpected on these probes is checked against the firewall logs to make sure the firewall is configured correctly and that the firewall is not marking logs as dropped when in fact packets are still being forwarded.

© SANS Institute 2000 - 2005 Author retains full rights.

2.3.3 Remote Offices

All remote offices with the exception of the warehouse connect to the GIACE network with a site-to-site VPN over the Internet. The warehouse connects via a site-to-site VPN over a private PVC as described earlier.

The Internet router model depends on the connectivity available in the country where the office is located. Mostly these are ADSL connections but one office has a leased line connection to the ISP. A Cisco 831 Ethernet Broadband Router [18] is connected to the Internet router supplied by the ISP.

This router provides stateful packet filtering and supports IPsec. A site-to-site VPN connection is established to the Openswan VPN gateway at the GIACE headquarters as described in section 2.3.2.3.1. An extended ACL is used to block all traffic except IPsec (IKE and ESP) from the GIACE network. PKI authentication is used to authenticate the IPsec connection. All traffic to and from the remote offices passes through the GIACE network and no direct Internet access is allowed.

To facilitate management of the remote offices, GIACE has decided to have a minimal installation at each site, thus no servers are located at the remote offices but all employees use the same servers located at the headquarters. This removes the need of having to send specialised support personnel at the remote offices to solve server related problems.

2.3.4 Servers

Servers located in the service network (DMZ) and the internal networks are shown with their IP addresses in the network diagram (Figure 1).

A detailed list of the most important servers, including their IP addresses, operating system and services (including the software type and version providing this service) is given in Appendix B – Server Details.

2.3.5 GIACE Users

2.3.5.1 User workstations

The majority of GIACE employees use Windows XP SP1 based PCs and laptops. The IT Department is in the process of upgrading to SP2 after testing compatibility issues. Laptops are mainly used by the sales people and at the warehouse. These laptops are equipped with built in 802.11b/g Wi-Fi and have a GPRS data card with a GPRS SIM card for remote access as described above.

Three graphic designers (for web site and adverts) use Apple Macintosh based workstations. A dedicated file server located on the Sales and Marketing network is used for multimedia file sharing (these are usually very large files) between the three designers.

Normal users do not have administrator rights on their workstations to reduce the chances of installing unlicensed and potentially harmful software.

© SANS Institute 2000 - 2005 Author retains full rights.

Personal Firewalls (the Sygate Personal Firewall Pro [19]) have been installed on the laptops since these may be connected directly to the Internet at various times. Virus scanning software (McAfee VirusScan [20]) is installed on all workstations. The virus scanning network management software is used to make sure that all devices connected to the network are upgraded with the latest virus signature updates.

An internal Windows Updates Server (SUS) [21] is used to facilitate downloading of the latest security patches and other Windows updates. The Microsoft Baseline Security Analyser (MBSA) is periodically used to check which machines need particular attention. In that case someone from the IT help desk will personally take the necessary actions.

2.3.5.2 User training

Since the weakest link in the security chain is usually the human aspect, GIACE has taken a pro-active role to solve this problem. It users periodically undergo a security awareness session where basic training is given on issues such as: opening attachments from unknown users; replying to and forwarding SPAM e-mails; and the importance of having a workstation with up to date Windows updates, virus scanning software and personal firewall. Most important, these users become aware that security is all about the business being able to move along without any unwanted hurdles (by accidental or deliberate damage or loss of competitive advantage), and everyone has a part to play in this process.

2.3.6 IP Addressing Scheme

A table outlining the IP addressing scheme on the GIACE networks can be found in Appendix A - IP Addressing Scheme.

2.3.7 Defence-in-Depth Strategy

Each component in GIACE's network security infrastructure attempts to introduce another layer in the defence-in-depth strategy. The main idea is to try not to leave any single point of failure in the security infrastructure[1]. In this way any security breach, be it accidental (viruses through e-mail) or deliberate (an attacker trying to break into the network) against the first line of defence will find another obstacle blocking its way to the internal network.

For this reason, packet filtering is done on the external router, the Internet firewall and the internal router. Inbound traffic from the internet is kept to the bare minimum: only the well known services are allowed through, and then again proxies (HTTP/S, SMTP) are used so that no Internet traffic directly reaches the internal network. Virus scanning and other measures such as e-mail spam filtering can be done on such proxies so that only legitimate traffic is then forwarded towards the internal network. All third party connections are using

[1] One can argue that several points of failure exist in the proposed network architecture; however this paper is intended to show how to secure a network and not how to make it more robust. Several options exist that allow routers and firewalls to operate in failover mode but these are outside the scope of this assignment.

© SANS Institute 2000 - 2005 Author retains full rights.

IPsec VPNs with strong certificate based authentication and the latest AES encryption. Where possible, these VPNs are not passing over the Internet but over a private connection. Traffic coming out of all VPNs is then filtered by the Internet firewall to reduce chances of session hijacking going any further.

An IDS has probes in all strategically important interfaces and the most important security devices and servers have a host based IDS installed. This together with extensive logging on all packet filtering devices, helps to detect incorrect configurations of the firewalls or bugs in the filtering software so that the necessary counteractions taken.

Disaster recovery procedures are in place; together with tried and tested backup and restore procedures for all services. In this way potential downtime in case systems have been compromised will be reduced and the business can safely continue with its operations.

The human element is also being tackled since it is difficult to have a sound technical solution if the people who use the technology every day do not appreciate its function and are not willing to cooperate.

Additionally, it is worth pointing out that the security field is changing every day: as new technologies are developed, new threats arise to any secure network design. This implies that improvements to the network security architecture can always be done by better understating the new threats and their implications, and by finding the most appropriate ways to mitigate them.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

3 Assignment 3 – Firewall Policy

This section will describe the rulebase of the Internet firewall. The rulebase has three distinct sections, the inbound and outbound traffic from the firewall and the traffic forwarded by the firewall including Network Address Translation (NAT) done as packets enter or leave the firewall. All traffic is logged and IP and TCP options are included in the IP headers for additional details. Iptables is stateful, so any reverse traffic associated with a rule shown below will be allowed and there is no need to specify such rules explicitly.

Basic ingress filtering is being done by the external router so there is no need to replicate these rules again on the main firewall.

3.1 Inbound Rules

The only traffic that is allowed to reach the firewall interfaces is:

- SSH (TCP port 22) from the IT and O&M networks on the internal interface
- SNMP (UDP port 161) from the IT and O&M networks on the internal interface
- ICMP echo-request from all interfaces.
- IPsec (IKE on UDP port 500 and ESP on IP protocol 50) from the external interface for site-to-site VPNs. This rule only serves to terminate the IPsec endpoint and not to forward traffic coming out of this tunnel. A separate rule under the forwarding rules section is used for this purpose.

All other incoming traffic is silently dropped.

3.2 Outbound Rules

The following traffic originating on the firewall is allowed out of its interfaces:

- ICMP echo-request
- IPsec (IKE on UDP port 500 and ESP on IP protocol 50) to the external interface
- UDP port 162 (SNMP traps) and Syslog (UDP port 514) to the NMS and the central log server through the internal interface.

All other outgoing traffic is dropped.

3.3 Forwarding Rules

The firewall is configured to forward the following packets. For clarity we will classify the rules according to their type and direction.

Before any packets are forwarded, packets that are known not to be needed are immediately dropped to optimise performance. These include NetBIOS and other UDP broadcasts and multicast addresses.

© SANS Institute 2000 - 2005 Author retains full rights.

Inbound IP traffic from external interface:

- UDP port 53 towards the external DNS servers. Inbound TCP port 53 is not allowed since this is only used to return large DNS responses and for DNS zone transfers. Since no zone transfers will be done with external servers and the GIACE replies are contained within a UDP reply, TCP port 53 is not needed. A related DNAT rule translates the public IP to the private IP of the DNS server before routing (and before this rule is evaluated).
- TCP ports 80 and 443 traffic towards the reverse proxy servers. The reverse proxy servers will then issue requests towards the Web servers or the CMS as required. Only traffic originating from the site-to-site VPNs is allowed to be redirected to the CMS (using filtering on the reverse proxy rules). A related DNAT rule translates the public IP to the private IP of the reverse proxy server before routing (and before this rule is evaluated).
- TCP port 25 traffic towards the external SMTP relays to receive inbound e-mails. A related DNAT rule translates the public IP to the private IP of the mail relay before routing (and before this rule is evaluated).
- UDP port 162 (SNMP traps) and Syslog (UDP port 514) from the external router towards the NMS and the central log server.

Inbound IPsec traffic from external interface:

- IPsec (IKE on UDP port 500 and ESP on IP protocol 50) towards the Windows 2003 VPN server.

Inbound IP traffic from IPsec interface:

- TCP ports 80 and 443 traffic from the internal networks (the remote encryption domain) of the business partners and suppliers is forwarded. A related DNAT rule translates the public IP to the private IP of the mail relay before routing (and before this rule is evaluated).
- All traffic from the internal networks (the remote encryption domain) of the remote offices and the warehouse is forwarded as is without any NAT since the remote IP addressing scheme is under GIACE control.

Outbound IP traffic towards external interface:

- UDP port 53 and TCP port 53 for outgoing DNS requests from the external DNS servers. A related SNAT rule translates the private IP of the DNS server to the public IP after routing (and after this rule is evaluated).
- TCP port 25 from the external SMTP relays for outgoing e-mails. A related SNAT rule translates the private IP of the SMTP relay to the public IP after routing (and after this rule is evaluated).
- TCP ports 80 and 443 (HTTP/S) and 21 (FTP) from the external and internal proxy server. A related SNAT rule translates the private IP of the proxy server to the public IP after routing (and after this rule is evaluated).

© SANS Institute 2000 - 2005 Author retains full rights.

- SSH and SNMP from the IT and O&M networks towards the external router.
- UDP port 123 for Network Time Protocol (NTP) from the DMZ NTP servers to external NTP servers on the Internet.

Outbound IPsec traffic towards external interface:

- IPsec traffic from the Windows 2003 VPN server towards the Internet is not needed – reverse traffic for inbound connections will be implicitly allowed.

Outbound IP traffic towards the IPsec interface:

- Traffic originating on the GIACE network towards the remote offices and the warehouse is allowed to be forwarded through the IPsec interface. As for inbound traffic on the same interface from these destinations, no NAT is required.
- Traffic originating from the credit card payment gateway used for online purchases is forwarded towards a bank payment gateway through a dedicated IPsec VPN. A related SNAT rule translates the private IP of the credit card payment gateway to the public IP after routing (and after this rule is evaluated).

Traffic from Windows 2003 VPN server towards domain servers:

- The Windows 2003 VPN server is allowed to use RADIUS authentication, authorisation (UDP port 1812) and accounting (UDP port 1813) on the internal Windows Internet Authentication Service (IAS) running on the domain servers.

Traffic from Windows 2003 VPN users towards the internal network:

- Traffic coming from the IP networks allocated to dial-in VPN users (from the Windows 2003 VPN server address pools) towards the internal network. All traffic is allowed by this firewall, the internal firewall will the do the per department filtering.

Traffic from DMZ towards internal network:

- SMTP (TCP port 25) from the external mail relays towards the Internal e-mail servers
- TCP traffic on ports 80 and 443 is allowed from the web servers and the CMS towards the internal application server (backend). XML web services are being used between the external servers and the internal application server. GIACE plans to deploy an XML firewall [22] between the two servers to provide application layer filtering of XML content while not allowing a direct connection from the DMZ towards the internal network.

Traffic from internal network towards DMZ:

© SANS Institute 2000 - 2005 Author retains full rights.

- DNS requests (UDP port 53) from the internal DNS servers towards the external DNS servers.
- DNS zone transfers (TCP port 53) from the internal DNS servers towards the external DNS servers.
- SMTP (TCP port 25) from the internal e-mail servers towards the external SMTP relays.
- Terminal services (TCP port 3389), VNC (UDP port 5900 to 5910) and SSH (TCP port 22) for management from the IT and O&M networks towards servers on the DMZ
- Passive FTP from the IT and O&M networks towards servers on the DMZ outbound TCP port 21 (FTP commands). The ip_conntrack_ftp module takes care to open access to a high port on the FTP server during the FTP session.
- UDP port 123 for Network Time Protocol (NTP) from the internal NTP servers to DMZ NTP servers.
- HTTP/S (TCP ports 80 and 443) from internal proxy server towards DMZ machines to allow users on the internal network to access the Web servers and the CMS.

All other traffic is dropped.

A more detailed description of the filtering rules can be found in Appendix C – Firewall Rules.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

4 Appendix A - IP Addressing Scheme

The following tables show the complete list of IP addresses assigned to different parts of the GIACE network.

ISP subnet		
IP network	*Subnet Mask*	*Description*
x.y.z.0	255.255.255.252	x.y.z.1 on ISP router, x.y.z.2 on External Router
This subnet was assigned by the ISP according to its addressing scheme.		

Public IP addresses		
IP network	*Subnet Mask*	*Description*
a.b.c.0	255.255.255.252	a.b.c.1 on external router, a.b.c.2 on firewall
a.b.c.4	255.255.255.252	a.b.c.5 on firewall, a.b.c.6 on Windows 2003 VPN server
a.b.c.8 to a.b.c.63		Reserved for future use
a.b.c.64	255.255.255.192	Subnet used for NAT
a.b.c.128	255.255.255.192	Subnet used for NAT
a.b.c.192	255.255.255.192	Subnet used for NAT
The a.b.c.0/24 public IP network was purchased from the ISP. Both the firewall and the Windows 2003 VPN server have public IP addresses on the external interfaces to terminate IPsec VPNs without NAT.		

DMZ		
IP network	*Subnet Mask*	*Description*
192.168.50.0	255.255.255.0	Service Network
Static Destination NAT is used for inbound traffic, and static Source NAT for outbound traffic		

VPN Subnet		
IP network	*Subnet Mask*	*Description*
192.168.51.4	255.255.255.252	192.168.51.5 on VPN server, 192.168.51.6 on firewall
This network is used to forward decrypted VPN packets back to the firewall for filtering		

© SANS Institute 2000 - 2005 Author retains full rights.

Internal Router Subnet		
IP network	*Subnet Mask*	*Description*
192.168.51.8	255.255.255.252	192.168.51.9 on firewall, 192.168.51.10 on internal router

Internal Networks		
IP network	*Subnet Mask*	*Description*
192.168.1.0	255.255.255.0	IT
192.168.2.0	255.255.255.0	O&M
192.168.3.0	255.255.255.0	HR, Finances and Administration
192.168.4.0	255.255.255.0	Sales and Marketing

Dial-in VPN IP adress pools		
IP network	*Subnet Mask*	*Description*
192.168.21.0	255.255.255.0	IT
192.168.22.0	255.255.255.0	O&M
192.168.23.0	255.255.255.0	HR, Finances and Administration
192.168.24.0	255.255.255.0	Sales and Marketing
These address pools are defined on the Windows 2003 VPN server. Users are assigned IP addresses according to their department		

Remote offices		
IP network	*Subnet Mask*	*Description*
192.168.11.0	255.255.255.0	Office1
192.168.12.0	255.255.255.0	Office2
192.168.13.0	255.255.255.0	Office3
192.168.14.0	255.255.255.0	Office4
192.168.15.0	255.255.255.0	Warehouse

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

5 Appendix B – Server Details

The following is a list of servers on the DMZ and on the internal network.

5.1 Service Network (DMZ) servers

Server	External DNS and NTP	IP Address	192.168.50.1, 192.168.50.2
Operating System	Red Hat Linux 9		
Services	DNS: ISC BIND v9.3.0 (http://www.isc.org/index.pl?/sw/bind/) , NTP server: NTP from RH9 distribution v 4.1.2. Tripwire v2.3.1 is installed as a host based IDS.		

Server	Reverse Proxy	IP Address	192.168.50.3, 192.168.50.4
Operating System	Red Hat Linux 9		
Services	Reverse Proxy: Squid v2.5-STABLE7 (http://www.squid-cache.org/Versions/v2/2.5/) configured with reverse proxy access control lists towards web servers for Internet visitors and customers and towards CMS for business partners and suppliers. Listening on TCP 80 and TCP 443. Jeanne scripts were used to tighten the reverse proxy rules. (http://www.ists.dartmouth.edu/library/classroom/jeanne.php) Tripwire v2.3.1 is installed as a host based IDS.		

Server	Web Server	IP Address	192.168.50.5, 192.168.50.6
Operating System	Red Hat Linux 9		
Services	Apache HTTP Server v2.0.52 (http://httpd.apache.org/) with Jakarta Tomcat v4.1.31 (http://jakarta.apache.org/tomcat/tomcat-4.1-doc/index.html). Configured with access lists to allow only reverse proxies to connect directly to ports TCP 80 and TCP 443. Tripwire v2.3.1 is installed as a host based IDS.		

Server	External SMTP Relay	IP Address	192.168.50.7, 192.168.50.8
Operating System	Microsoft Windows 2003 Server		
Services	Lotus Domino v6 (with latest patches) SMTP relay		

© SANS Institute 2000 - 2005 Author retains full rights.

Server	Content Management System	IP Address	192.168.50.9, 192.168.50.10
Operating System	Red Hat Linux 9		
Services	Apache HTTP Server v2.0.52 (http://httpd.apache.org/) with Jakarta Tomcat v4.1.31 (http://jakarta.apache.org/tomcat/tomcat-4.1-doc/index.html). Configured with access lists to allow only reverse proxies to connect directly to ports TCP 80 and TCP 443. Tripwire v2.3.1 is installed as a host based IDS.		

Server	External Updates Server	IP Address	192.168.50.11
Operating System	Microsoft Windows 2003 Server		
Services	Windows Update Services (http://www.microsoft.com/windowsserversystem/sus/default.mspx) McAfee ePolicy Orchestrator (http://www.networkassociates.com/us/products/mcafee/mgmt_solutions/epo.htm) to deliver anti-virus updates on DMZ. Squid proxy running in a Cygwin shell (http://www.cygwin.com/) (used by DMZ servers).		

5.2 Internal Servers

Server	NMS	IP Address	192.168.2.1
Operating System	Red Hat Linux 9		
Services	OpenNMS 1.0.2 (http://wiki.opennms.org/tiki-index.php)		

Server	Log Server	IP Address	192.168.2.2
Operating System	Red Hat Linux 9		
Services	Syslog server MySQL database v4.1.7 (http://dev.mysql.com/) used for Snort logging		

Server	Internal updates server	IP Address	192.168.2.3
Operating System	Microsoft Windows 2003 Server		
Services	Windows Update Services (http://www.microsoft.com/windowsserversystem/sus/		

© SANS Institute 2000 - 2005 Author retains full rights.

	default.mspx) McAfee ePolicy Orchestrator (http://www.networkassociates.com/ us/products/mcafee/mgmt_solutions/epo.htm) to deliver anti-virus updates on DMZ.

Server	Network stats, reporting	IP Address	192.168.2.4
Operating System	Red Hat Linux 9		
Services	Ntop v3.0 (http://www.ntop.org) to collect traffic statistics from Cisco routers. In house developed Perl scripts and Java applications to generate reports from firewall, IDS and proxy logs.		

Server	Windows 2003 Domain Servers	IP Address	192.168.1.1, 192.168.1.2
Operating System	Windows 2003 Server		
Services	Active Directory LDAP, RADIUS (IAS), Windows file shares, internal DNS (separate domain from external public domain – as a DNS caching server zone updates are done with the external DNS servers), DHCP by MAC address of users on LAN, Certificate Authority, internal NTP servers.		

Server	Internal Email	IP Address	192.168.1.3, 192.168.1.4
Operating System	Windows 2003 Server		
Services	Lotus Domino v6 (with latest patches). Does not accept SMTP except from external relays. Users access e-mail using Louts Notes client and web mail client. Domino user names and passwords are synchronised with Active Directory for single sign on capabilities.		

Server	Internal proxy server	IP Address	192.168.1.9
Operating System	Red Hat Linux 9		
Services	Squid v2.5-STABLE7 (http://www.squid-cache.org/Versions/v2/2.5/) configured in proxy server mode. Squid is configured with NTLM protocol awareness so that it knows the identity of the users doing requests. Thus user based access control can be done and all proxy logs include the user identifier apart from the client machine's IP address. (http://squid.sourceforge.net/ntlm/).		

Server	Internal	IP Address	192.168.1.10

© SANS Institute 2000 - 2005 Author retains full rights.

	application server		
Operating System	Red Hat Linux 9		
Services	Apache HTTP Server v2.0.52 (http://httpd.apache.org/) with Jakarta Tomcat v4.1.31 (http://jakarta.apache.org/tomcat/tomcat-4.1-doc/index.html). Configured with access lists to allow only the web servers and the CMS to connect directly to ports TCP 80 and TCP 443. GIACE is evaluating XML firewalls to restrict further the valid transactions that the application server will process. Such firewalls can check for the validity of XML signatures inside the web service requests. Tripwire v2.3.1 is installed as a host based IDS.		

Server	RDBMS	IP Address	192.168.1.5
Operating System	Sun Solaris 8		
Services	SQL database: Oracle 9i Database level access control is implemented to restrict access to the live database only to the back end application server. Tripwire v2.3.1 is installed as a host based IDS.		

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

6 Appendix C – Firewall Rules

Iptables treats traffic entering, leaving and forwarded by the firewall in three separate "chains". Each chain can be considered as a distinct rule list, evaluated from top to bottom. For readability, the rules have been displayed in a table format. In practice each rule shown in the table might require multiple iptables rules since non-contiguous blocks of IP addresses or ports must be configured in separate rules. The traffic flows that define these rules were introduced in section 3. The order of the rules is intended to first eliminate unwanted traffic, then allowing traffic starting with the most used rules and then explicitly dropping all other traffic.

Basic actions are "ACCEPT" or "DROP". The security policy states that filtered packets must be silently dropped not rejected, in order to minimise chances of network mapping through analysis of firewall replies or TCP/IP fingerprinting.

An "NAT, ACCEPT" action implies that the rule must also include a related Destination NAT rule for inbound packets to the firewall interface. The destination address should be translated before the filtering rule is evaluated, so the filtering rule should be specified with the private IP address.

On the other hand, an "ACCEPT, NAT" action implies that the rule must include a related Source NAT rule for outbound packets from the firewall. The source address should be translated after the filtering rule is evaluated, so the filtering rule should be specified with the private IP address.

All packets are logged unless stated otherwise. Logs include a log prefix indicating the chain and the action, such as "LOG FORWARD DROP" or "LOG INPUT ACCEPT", and also include IP and TCP options for additional packet details inside the log string.

Input Chain

This list filters packets with the destination being one of the firewall interfaces.

Description	Source IP	Destination IP	Dest Port or Service	In I/F	Out I/F	Action
Allow established and related traffic					N/A	ACCEPT
Allow SSH and SNMP management	192.168.1.0/24, 192.168.2.0/24	192.168.51.9	TCP 22, UDP 161	eth4	N/A	ACCEPT
Allow ICMP from all interfaces	any	192.168.51.9	ICMP-echo request	all	N/A	ACCEPT
Allow IPsec from outside	Remote VPN server IP address	a.b.c.2	UDP 500, IP protocol 51	eth0	N/A	ACCEPT
Drop all other traffic					N/A	DROP

© SANS Institute 2000 - 2005 Author retains full rights.

Output Chain

This list filters packets originating from one of the firewall interfaces

Description	Source IP	Destination IP	Dest Port or Service	In I/F	Out I/F	Action
Allow established and related traffic				N/A		ACCEPT
Allow ICMP from all interfaces	any	any	ICMP-echo request	N/A	All	ACCEPT
Allow IPsec to outside	a.b.c.2	Remote VPN server IP address	UDP 500, IP protocol 51	N/A	eth0	ACCEPT
Allow SNMP traps to NMS	192.168.51.9	NMS	UDP 162	N/A	eth4	ACCEPT
Allow Syslog to log server	192.168.51.9	Log Server	UDP 514	N/A	eth4	ACCEPT
Drop all other traffic				N/A		DROP

Forward Chain

This list filters packets which have to be forwarded by the firewall.

Description	Source IP	Destination IP	Dest Port or Service	In I/F	Out I/F	Action
Allow established and related traffic						ACCEPT
Drop ICMP traffic (not needed for internal hosts)	any	any	ICMP	any	any	DROP (no logging)
Drop protocols that are not needed	any	any	UDP 135 to 129, TCP 135 to 139, TCP 445	any	any	DROP (no logging)
Inbound DNS	any	External DNS	UDP 53	eth0	eth3	NAT, ACCEPT
Outbound DNS	External DNS	any	UDP 53, TCP 53	eth3	eth0	ACCEPT, NAT
Inbound HTTP/S	any	Reverse Proxies	TCP 80, TCP 443	eth0	eth3	NAT, ACCEPT
Outbound HTTP/S from external proxy	External Proxy	any	TCP 21, TCP 80, TCP 443	eth3	eth0	ACCEPT, NAT
Outbound HTTP/S from internal proxy to the Internet	Internal Proxy	any	TCP 21, TCP 80, TCP 443	eth4	eth0	ACCEPT, NAT
Outbound HTTP/S from internal proxy to DMZ servers	Internal Proxy	any	TCP 80, TCP 443	eth4	eth3	ACCEPT
Inbound SMTP	any	SMTP relays	TCP 25	eth0	eth3	NAT, ACCEPT
Outbound SMTP	SMTP relays	any	TCP 25	eth3	eth0	ACCEPT, NAT

© SANS Institute 2000 - 2005 Author retains full rights.

External Router Management	192.168.1.0/24, 192.168.2.0/24	a.b.c.1	TCP 22, UDP 161	eth4	eth0	ACCEPT
SNMP from external router to NMS	a.b.c.1	NMS	162	eth0	eth4	ACCEPT
Syslog from external router to log server	a.b.c.1	Log server	514	eth0	eth4	ACCEPT
Inbound IPsec towards Windows 2003 VPN	any	a.b.c.4	UDP 500, IP protocol 51	eth0	eth2	ACCEPT
Inbound HTTP/S from VPN sites	suppliers and partners remote encryption domains	Reverse Proxies	TCP 80, TCP 443	ipsec0	eth3	ACCEPT
Inbound traffic from remote offices and warehouse	offices and warehouse remote encryption domains	any	any	ipsec0	eth4	ACCEPT
Outbound traffic to remote offices and warehouse	any	offices and warehouse remote encryption domains	any	eth4	ipsec0	ACCEPT
Credit card gateway to bank	Credit card gateway	Bank encryption domain	TCP 443	eth4	ipsec0	ACCEPT, NAT
NTP synchronization	External NTP Servers	any	UDP 123	eth3	eth0	ACCEPT, NAT
Windows 2003 VPN user RADIUS authentication with domain	192.168.51.5 on Windows 2003VPN	Windows 2003 Domain Servers	UDP 1812, UDP 1813	eth1	eth4	ACCEPT
Windows 2003 VPN user traffic towards internal network	VPN IP address pools	any	any	eth1	eth4	ACCEPT
SMTP from external to internal mail relays	External SMTP relays	Internal SMTP relays	25	eth3	eth4	ACCEPT
SMTP from internal to external mail relays	Internal SMTP relays	External SMTP relays	25	eth4	eth3	ACCEPT
XML web services towards application server backend	CMS and Web servers	Application Server	TCP 80, TCP 443	eth3	eth4	ACCEPT
DNS forwarding requests	Internal DNS	External DNS	UDP 53	eth4	eth3	ACCEPT
DNS Zone transfers to update internal DNS with public domain	Internal DNS	External DNS	TCP 53	eth4	eth3	ACCEPT

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

DMZ server management	192.168.1.0/24, 192.168.2.0/24	DMZ network 192.168.50.0/24	TCP 3398, UDP 5900-5910, TCP 22, TCP 21	eth4	eth3	ACCEPT
Internal NTP synchronization	Internal NTP servers	DMZ NTP Servers	UDP 123	eth4	eth3	ACCEPT
Drop all other traffic						DROP

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

7 List of References

1. Convery, S., et al, *Cisco SAFE: Wireless LAN Security in Depth*. 2003, Cisco Systems, Inc.
2. Shamir, A., et al., *Weaknesses in the Key Scheduling Algorithm of RC4*. 2001.
3. *RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4*.http://www.rsasecurity.com/rsalabs/node.asp?id=2009
4. *RFC 3748 - Extensible Authentication Protocol (EAP).* 2004.http://www.faqs.org/rfcs/rfc3748.html
5. *Wi-Fi Protected Access Overview*. 2002, Wi-Fi Alliance.
6. *Selecting an EAP Method for your Wireless LAN*. 2004, Meetinghouse Data Communications.
7. Terry Simons, J.S., *802.1X: Deployment Experiences and Obstacles to widespread Adoption*.http://www.merit.edu/~nanog/mtg-0410/pdf/snyder.pdf
8. Intermec, *Intermec 700 Series Mobile Computer.* 2003.http://www.scansource.com/intermec/2003_webinars/700SeriesUpdateSeptember20.ppt
9. Deri, L., *Ntop.* 2004.http://www.ntop.org/ntop.html
10. *Cisco IOS Netflow Data Sheet*.http://www.cisco.com/en/US/tech/tk648/tk362/tech_brief0900aecd80173f71.html
11. *Center for Internet Security - Cisco Benchmarks.* 2004.http://www.cisecurity.org/bench_cisco.html
12. *netfilter/iptables Project Homepage*.http://www.iptables.org/
13. *Red Hat website*.http://www.redhat.com
14. *Dell PowerEdge 2650 Server specifications*.http://www.dell.com/downloads/global/products/pedge/en/2650_specs.pdf
15. *Openswan website*.http://www.openswan.org/
16. *General Packet Radio Service overview*.http://en.wikipedia.org/wiki/GPRS
17. *Snort IDS website*.http://www.snort.org/
18. *Cisco 830 Series Secure Broadband Routers*.http://www.cisco.com/warp/public/cc/pd/rt/800/prodlit/ssbro_ds.pdf
19. *Sygate Personal Firewall Pro*.http://smb.sygate.com/products/spf_pro.htm
20. *McAfee Virus Scanning*.http://www.mcafee.com
21. *Software Update Services website*.http://www.microsoft.com/windowsserversystem/sus/default.mspx
22. *Protecting Web Services with the XML/SOAP Security Gateway.* 2004.http://www.xtradyne.com/documents/whitepapers/Xtradyne-WS-DBC-WhitePaper.pdf

© SANS Institute 2000 - 2005 Author retains full rights.