# Global Information Assurance Certification Paper

# “Securing a virtual fortune cookie saying business in the wired and wireless world”

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment
Version 4.1



Klaus Wagner

22. February 2005

**Table of Content**

**Table of Figures**

# 1 Abstract

GIAC Enterprises is a small business which markets fortune cookie sayings to customers worldwide. All of GIAC Enterprises sales are done via the Internet.

The Company employs fifty people worldwide with the majority located in its head office in Munich, Germany. About a dozen employees are located in one bigger regional office in Zurich, Switzerland, and the remainder is located in three small regional satellite offices geographically distributed around the world (America, Asia Pacific and Eastern Europe).

GIAC Enterprises has also diversified into the fortune cookie manufacturing business and built a warehouse to use for manufacturing and shipping of its products.

The first part of this paper shows the risks arising from deployment of IEEE 802.11g technology, how to mitigate these risks and eventually describes the wireless integration of GIAC Enterprises warehouse.

In the second part of this paper the security architecture of GIAC Enterprises is developed based on the access requirements and access restrictions of different groups interacting with GIAC Enterprises.

The last part briefly describes the security policies of the main components of the developed security architecture.

# 2 Assignment 1 – Wireless Integration of GIAC Enterprises Warehouse

## 2.1 Summary

GIAC Enterprises is a small business which markets fortune cookie sayings to customers worldwide. All of GIAC Enterprises sales are done via the Internet.

GIAC Enterprises has diversified into the fortune cookie manufacturing business and has built a warehouse for manufacturing and shipping of its product. Due to technical and practical restrictions it is not possible to deploy wired technology therefore the warehouse will use handheld scanners in the shipping process and wireless laptops inside the warehouse. GIAC Enterprises decided to use IEEE 802.11g technology.

This assignment shows the risks arising from deployment of wireless technology for GIAC Enterprises, how to mitigate these risks by enforcing policies and defense in depth and eventually shows the integration of warehouse business operations into GIAC Enterprises existing network architecture.

## 2.2 Enforced Policies

GIAC Enterprises has defined the following policies to ensure proper business operations. GIAC Enterprises strictly enforces these policies

### 2.2.1 Network Usage Policy

Network usage is allowed only for business purpose and must not be used for private activities. Employees are not allowed to install additional hardware without prior written permission.

### 2.2.2 Need-to-Know Principle

GIAC Enterprises resources are access restricted. Every employee has only those permissions that are needed for him/her to fulfill his/her tasks.

### 2.2.3 Defense in Depth

Whenever possible and economically justifiable, defense in depth is applied to protect the assets of the company.

## 2.3 Risks Deploying Wireless Technology

Wireless technology can easily be deployed in locations with technical and practical restrictions of a wired installation. Contrary to wired installations the

physical access to the network layers can not be controlled due to the nature of the propagation of radio waves.

### 2.3.1 Privacy

The coverage of a typical IEEE 802.11g installation is about 250 ft in range outside buildings. Everybody within that range can easily monitor the complete network traffic using suitable hardware. In case of IEEE 802.11g this is possible with a standard laptop and a standard wireless network card. Using suitable software like Kismet, "sniffing" of the network can be done completely unnoticed, thus being classified as a passive attack. Using special antenna equipment with amplifier an eavesdropper can be located even further away.

### 2.3.2 Integrity and Authenticity

Using standard hardware and a standard wireless network card an attacker can easily disrupt network transmission or replay captured packets. An attacker can also try to connect to the network using captured or no credentials. He also can set up his own access point and provoke wireless clients to connect to this rogue access point. These attacks are classified as active attacks.

### 2.3.3 Denial of Service

IEEE 802.11g operates in the 2.4 GHz band within different channels. Other access points or devices also operating in the 2.4 GHz band can interfere with the wireless network. An attacker can leverage this to completely disrupt legitimate network traffic.

### 2.3.4 Theft of Devices

Wireless devices like laptops are handy in size and are easily stolen. Stored credentials on stolen devices could be used to connect to a wireless network or to compromise the complete network.

## 2.4 Mitigating the Risks

The previous section has shown risks involved in deploying wireless technology. Some of these risks can be lowered to zero by using proper encryption and authentication measures, while others like Denial of Service can only be circumvented with administrative measures.

### 2.4.1 Standard Measures

Wireless LANs should be deployed with some standard measures to prevent the ordinary "war-driver" from connecting to the network. Some of these also help being a good "wireless neighbor".

The standard measures include:

- Enabling MAC-Access-Control on access points
- Allowing only IEEE 802.11g traffic to connect

- Disabling SSID Broadcast and using non standard SSID's
- Enabling the wireless network only during working hours (if possible)
- Optimizing coverage and range of wireless network through smart placement of access points
- Checking for "wireless neighbors" and using channels with least expected interference

These measures can not prevent a sophisticated attacker from attacking the network (as for example MAC-addresses can be spoofed, the SSID can be sniffed easily with tools like Kismet), but an attack would take more time and effort and would possibly generate more suspicious network traffic. Optimizing the coverage and the channels of the wireless network lowers the output of false positives from the IDS in those cases where "wireless neighbor" clients are trying to connect to the wrong network.

### 2.4.2 Physical Access Control

Wireless devices like laptops or access points normally contain some sort of credentials. In case a device is stolen these stored credentials could be used to compromise the network.

Laptops and other wireless clients should be stored and locked in a safe place after business hours and, if possible, locked while in use with some sort of theft prevention (for example security cable locks).

Access points must be placed in secured and locked places.

### 2.4.3 Authentication and Data Encryption

IEEE 802.11 supports different encryption and authentication methods to ensure privacy, integrity and authenticity, like WEP, WPA-PSK, WPA and WPA2.

WEP (Wired Equivalent Privacy) is considered to be seriously flawed due to the usage of short cryptographic initialization vectors (IV).[1] There are numerous tools available to crack the WEP-Key, one of the first being AirSnort.

WPA-PSK (WiFi Protected Access - PreShared Keys) seems to be a better protection than WEP, up to now there is no known vulnerability to the used encryption and authentication scheme, but the key exchange protocol is susceptible to a passive dictionary attack.[2] Using long keys would mitigate this risk. Disclosure of the key (for example by theft of one device) can compromise the entire wireless network, when all network traffic is protected with one single key.

[1] Fluhrer
[2] Takahashi

WPA authentication is based on IEEE 802.1X Port Based Network Access Control and encryption is based on IEEE 802.11i Temporal Key Integrity Protocol (TKIP). WPA is also called a Transition Security Network (TSN).
WPA2, also called a Robust Secure Network (RSN), is based on IEEE 802.1X for authentication as well, but encryption is done with IEEE 802.11i Counter Mode with CBC-MAC Protocol (CCMP).

Both methods, TKIP and CCMP, provide integrity and privacy of the transmitted data. CCMP uses AES as its cryptographic algorithm and is therefore more CPU intensive compared to RC4 used in TKIP.

Extensible Authentication Protocol (EAP) is the authentication framework used with IEEE 802.1X and there are numerous EAP authentication methods defined like Lightweight EAP (LEAP), EAP-TLS or Protected EAP (PEAP) and many more. EAP-TLS and PEAP provide mutual authentication.

Within 802.1X the wireless client that requests authentication contains a Supplicant and the access point contains an Authenticator. When the wireless client requests access to the network its Supplicant uses EAP to send its identity to the Authenticator. The Authenticator forwards these EAP packets (encapsulated via EAPOL) to an Authentication Server (RADIUS) for Authentication, Authorization and Accounting. The Authentication Server advises the Authenticator whether to accept the connection of the wireless client or not. In case of a successful authentication unique cryptographic session keys are established between Supplicant and Authenticator.[3]

### 2.4.4 Intrusion Detection and Auditing

Intrusion detection can be done with Kismet and Snort on the wireless LAN. All captured unencrypted traffic will be forwarded to Snort. This way some attacks and even some sorts of denial of service can be detected and the position of the attacker can be calculated (by means of triangulation) to a certain degree.

Kismet can be used to detect rogue access-points connected to the wired LAN by employees.

Modern laptops are equipped with wireless LAN network cards by default and are often configured to connect to any access point or ad-hoc network in range. These potential vulnerabilities can be identified using Kismet and NetStumbler.

[3] Strand

## 2.5 Wireless Integration of the Warehouse

### 2.5.1 Business Needs

The warehouse staff needs to access their email, the web-based e-commerce platform and files on the fileserver. As soon as they get a work order by email, they look up this order (and all for the production necessary data) in the e-commerce platform, download the fortune sayings and feed them into the "fortune cookie production machines" and mark the order as being in production. While producing the cookies staff prints out labels. The printers and the "fortune cookie production machines" are connected to the laptops via USB on their docking stations. Once the cookies are produced they will be packed, the boxes get the labels attached and the labels will be scanned with the handheld scanners. The scanners transmit this data to the e-commerce platform and mark the order as being produced and ready for shipment. Shipment will be scheduled, the boxes are scanned one last time when they leave the warehouse and the order on the e-commerce platform will be updated.

### 2.5.2 The Solution

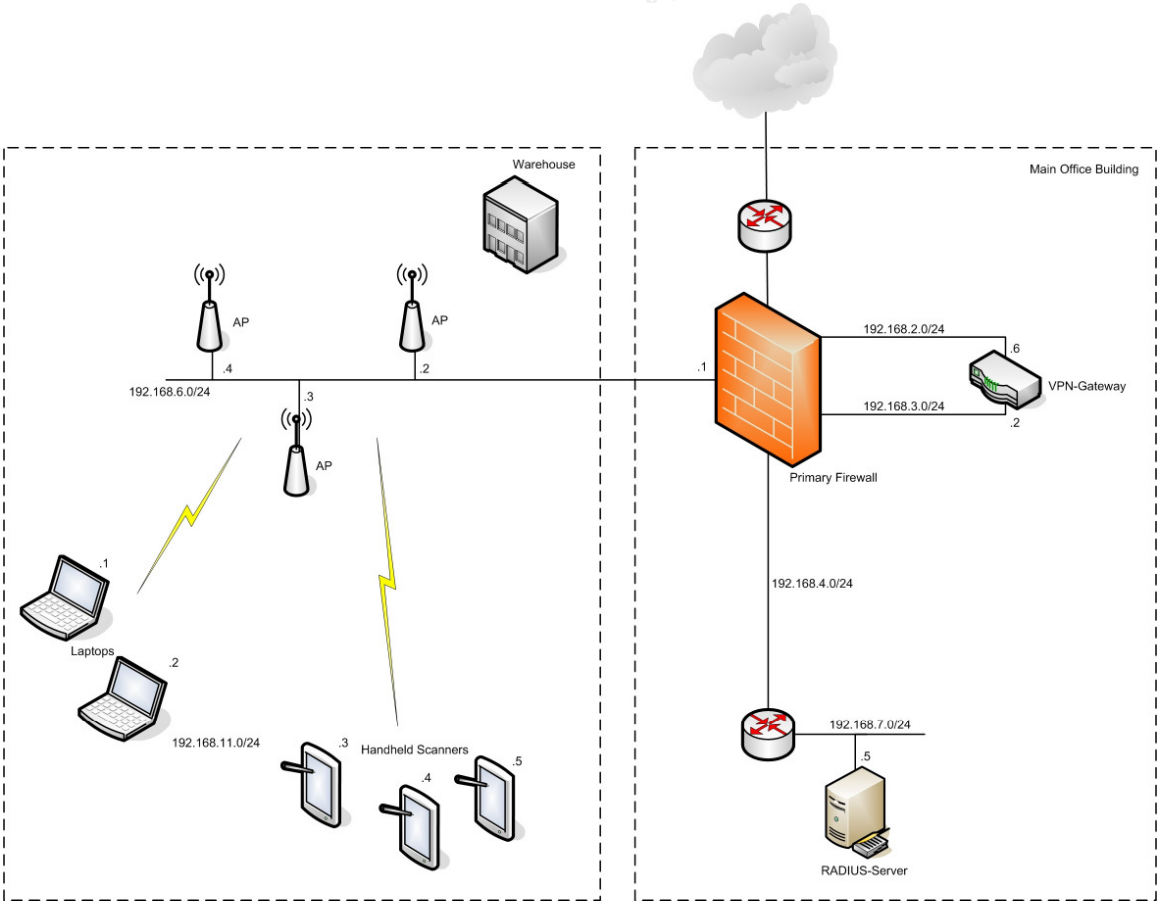


**Figure 1: Wireless LAN**

GIAC Enterprises chooses to deploy Cisco Aironet 1200 Series access points in its warehouse. They are specially designed for indoor RF environments like warehouses, support roaming and WPA and WPA2 with IEEE 802.1X authentication including EAP-TLS and PEAP. Cisco Aironet Series support WPA2 Mixed Mode operations, which permits the coexistence of WPA and WPA2 clients on the same wireless network[4].

The laptops GIAC Enterprises deploys inside the warehouse are standard laptops equipped with Windows XP (SP2). Administrative procedures ensure that they are always updated with the latest patches. The users of the laptops do not have administrative rights. The integrated software-firewall is turned on and the laptops are equipped with anti-virus software. The laptops connect to the access-point with WPA2 and EAP-TLS using X.509 certificates for client and server authentication.

The wireless scanners are Pocket PC 2003 based devices and they will connect to the access-point with WPA and EAP-TLS using X.509 certificates for client and server authentication. The X.509 certificates will be deployed on the PPC-devices with the tool “crtimport”. Once available WPA2 will also be used for the wireless scanners.

FreeRADIUS will be used as the RADIUS-Server.

The previously discussed standard measures (like MAC-Access-Control) will be applied to the access-points and physical access control (as described) will be enforced for the wireless devices and laptops.

Intrusion detection will be done on the wireless network with Kismet and Snort. An additional IDS-sensor will be deployed in the subnet of the access points.

The warehouse network of GIAC Enterprises is connected to the main firewall to control all traffic between the wired and the wireless network, as the wireless network is considered to be less secure than the wired network. To leverage security the existing VPN solution will be used and all traffic (except the authentication traffic between the access points and the RADIUS server) must be encrypted using IPSec. This will be enforced with firewall rules. Access restrictions will also be applied for the traffic through the firewall behind the VPN-gateway according to the business needs in the warehouse.

The wireless network will be audited at regular intervals with Kismet and NetStumbler to ensure that all traffic is encrypted and to learn about possible new “wireless neighbors”. The audit will also detect potentially deployed rogue access points and mis-configured wireless clients.

[4] Cisco Systems 2005, p.10

### 2.5.3 Assessment of the Solution

The deployed solution enforces strong encryption and authentication to ensure privacy, integrity and authenticity on the wireless network. Using the existing VPN solutions for layered security is a good example for defense in depth. Even un-known flaws in the WPA/WPA2 implementation will not compromise the network.

Using WPA instead of WPA2 on the wireless scanners does not affect the overall security of the solution, due to the second layer of encryption supplied by the VPN solution.

GIAC Enterprises decided to use EAP-TLS with X.509 certificate based authorization, since they have an existing PKI infrastructure. Other EAP authentication methods providing mutual authentication like PEAP require a X.509 server certificate for the authentication server as well but also additional user/password management.

Another option would have been to deploy WPA-PSK using long and unique keys for every wireless client to connect to the network. This would mitigate the risk of the mentioned dictionary attack. The disclosure of one key would allow an attacker to connect to the network and he would be able to exploit vulnerabilities on all other wireless clients. Clients are protected through their software firewalls and the wireless PPC-devices do not provide services to the network. The wireless LAN is also separated from the wired LAN through the firewall and the VPN solution. Network based intrusion detection would be able to detect this kind of attack. These considerations also apply in case of the existence of flaws in the access-points or in the authentication scheme, which could also allow an attacker to connect to the network unauthenticated.

Special attention needs to be drawn to the RADIUS-Server. Existing vulnerabilities could be exploited through the wireless LAN. An attacker could passively sniff the network for the MAC-addresses of the wireless devices and wait for one of the wireless clients to disconnect. After that the attacker could spoof his MAC-address, request authorization from the access-point and would then be able to send specially crafted EAP authorization requests to the RADIUS-server through the firewall to attack the network. Network based intrusion detection might not be able to detect this kind of attack as the authentication mechanism is protected with TLS.

A denial of service attack (for example through placement of a jamming transmitter in the 2.4 GHz band) would interfere with the process flow of the warehouse. If this attack can not be stopped in a reasonable period of time the process flow in the warehouse needs to be changed according a defined emergency plan. This could mean for example connecting the laptops to the wired LAN and downloading of the fortune sayings this way and then moving back with the laptops to the docking stations with the production machines attached.

# 3 Assignment 2 – Security Architecture

## 3.1 Summary

GIAC Enterprises is a small business which markets fortune cookie sayings to customers worldwide. All of GIAC Enterprises sales are done via the Internet.

The Company employs fifty people worldwide with the majority located in its head office in Munich, Germany. About a dozen employees are located in one bigger regional office in Zurich, Switzerland, and the remainder located in three small regional satellite offices geographically distributed around the world (America, Asia Pacific and Eastern Europe).

This assignment shows the network security architecture for GIAC Enterprises based on the access requirements and restrictions of different groups interacting with the company.

## 3.2 Access Requirements and Access Restrictions

### 3.2.1 The General Public

GIAC Enterprises operates a public Internet Web-Server to provide different information to the general public, like business reports, job offers or contact information. The general public can contact GIAC Enterprises via email.

| Source | Destination | Port(s)/Protocol | Description |
|---|---|---|---|
| General public | DNS-Server | 53/UDP (DNS)<br>53/TCP (DNS) | Public access to name server to resolve IP-addresses. (N.B. the primary DNS server is outsourced at ISP) |
| General public | Public Web Server | 80/TCP (HTTP) | Public access to web server to get information about GIAC Enterprises. (N.B. the public web server is outsourced at ISP) |
| General public | SMTP-Relay | 25/TCP (SMTP) | General public sending emails to GIAC Enterprises. |

### 3.2.2 Customers

Customers, including companies and individuals, can purchase bulk online fortune sayings over the internet. The customers place their orders on the SSL-secured e-commerce platform. They also provide payment details this way. After the payments are processed the customers can download their purchased fortune sayings on the e-commerce platform. Customer access is restricted to the shop area and the download area of the e-commerce platform.

In addition to the access requirements of the general public the following applies to the customers:

| Source | Destination | Port(s)/Protocol | Description |
|---|---|---|---|
| Customer | SSL-Proxy | 443/TCP (HTTPS) | Public access to the secured e-commerce platform via the SSL-Proxy. This proxy protects the dedicated web server running the business application. Access is restricted to shop and download area within the business application. |

### 3.2.3 Suppliers

The fortune cookie sayings are produced by different suppliers on request of GIAC Enterprises. The company orders the sayings via (encrypted and signed) email. There are different ways for the suppliers to deliver the sayings in different formats including upload of the sayings on the GIAC Enterprises e-commerce platform or on dedicated areas on GIAC Enterprises secure file transfer server. The supplier can also provide the sayings via (encrypted and signed) email or provide a download area for the sayings on one of his servers. In either case the sayings get imported into GIAC Enterprises e-commerce platform.
Access is restricted to the supplier area on the e-commerce platform and to the secured file transfer area. GIAC Enterprises provides X.509 client certificates to its suppliers for this purpose.

In addition to the access requirements of the general public the following applies to the suppliers:

| Source | Destination | Port(s)/Protocol | Description |
|---|---|---|---|
| Supplier | SSL-Proxy | 443/TCP (HTTPS) | Protected access to the secured e-commerce platform via the SSL-Proxy. Access is restricted to supplier area within the business application. This is enforced with mutual authentication based on X.509 client and server certificates and additional passwords. |
| Supplier | Secure File Transfer Server | 22/TCP (SSH/SFTP) | Protected access to the secured file transfer server. Access is restricted to dedicated upload areas on the server. |

### 3.2.4 Partners

International partner companies translate and resell fortune cookie sayings. They first need to access the fortune cookie sayings via the secured e-commerce

platform or by means of a secured file transfer. In some cases they deliver the translated sayings back to GIAC Enterprises the same way as the suppliers do. Access is restricted to dedicated areas on the e-commerce platform and on the secured file transfer area. GIAC Enterprises provides X.509 client certificates to its partners for this purpose.

In addition to the access requirements of the general public the following applies to the partners:

| Source | Destination | Port(s)/Protocol | Description |
|---|---|---|---|
| Partner | SSL-Proxy | 443/TCP (HTTPS) | Protected access to the secured e-commerce platform via the SSL-Proxy. Access is restricted to partner area within the business application. This is enforced by mutual authentication based on X.509 client and server certificates and additional passwords. |
| Partner | Secure File Transfer Server | 22/TCP (SSH/SFTP) | Protected access to the secured file transfer server. Access is restricted to dedicated upload/download areas on the server. |

### 3.2.5 Head Office Munich

All GIAC Enterprises servers are located at the head office in Munich. The employees need to access the internal mail server, the file server, the internal e-commerce platform and the secured areas on GIAC Enterprises file transfer server. The warehouse staff needs the same access to the local resources using the deployed VPN-gateway. Internet access is restricted to http, https and secure file transfer.

| Source | Destination | Port(s)/Protocol | Description |
|---|---|---|---|
| Internal User Network | Internal DNS Server | 53/UDP (DNS) | Access to the internal DNS server to resolve IP-addresses. |
| Internal User Network | Internal Mail Server | 110/TCP (POP3)<br>25/TCP (SMTP) | Access to the internal mail server for sending and receiving emails. |
| Internal User Network | Internal File Server | 137-139/TCP netbios<br>137-139/UDP netbios<br>445/TCP ms-ds | Access to the internal file server. |
| Internal User Network | SSL-Proxy | 443/TCP (HTTPS) | Protected access to the secured e-commerce platform via the SSL-Proxy. Access is restricted within the business application according to the needs of the user. This is enforced by mutual authentication based on X.509 client and server certificates and additional passwords. |

| | | | |
|---|---|---|---|
| Internal User Network | Secure File Transfer Server | 22/TCP (SSH/SFTP) | Protected access to the secured file transfer server. Access is restricted to dedicated upload/download areas on the server. |
| Internal User Network | Public Web Server via proxy | 80/TCP (HTTP)<br>443/TCP (HTTPS) | (Encrypted) Access to public web servers (including customer, supplier, etc.). |
| Internal User Network | Partner Secure File Transfer Server | 22/TCP (SSH/SFTP) | Protected access to the partner's secured file transfer server. |

Additional requirements for the warehouse are:

| Source | Destination | Port(s)/Protocol | Description |
|---|---|---|---|
| Warehouse network | VPN-Gateway | 500/UPD (IKE) | Key negotiation for establishment of VPN. |
| Warehouse network | VPN-Gateway | IP 50 (ESP) | VPN-Access from the warehouse. |
| Warehouse network | RADIUS-Server | 1812/UPD (RADIUS) | Authentication of wireless clients in the warehouse. |
| Warehouse network | Internal DNS Server via VPN | 53/UDP (DNS) | Access to the internal DNS server to resolve IP-addresses. |
| Warehouse network | Internal Mail Server via VPN | 110/TCP (POP3)<br>25/TCP (SMTP) | Access to the internal mail server for sending and receiving emails. |
| Warehouse network | Internal File Server via VPN | 137-139/TCP netbios<br>137-139/UDP netbios<br>445/TCP ms-ds | Access to the internal file server. |
| Warehouse network | SSL-Proxy via VPN | 443/TCP (HTTPS) | Protected access to the secured e-commerce platform via the SSL-Proxy. Access is restricted within the business application according to the needs of the user. This is enforced by mutual authentication based on X.509 client and server certificates and additional passwords. |
| Warehouse network | Secure File Transfer Server via VPN | 22/TCP (SSH/SFTP) | Protected access to the secured file transfer server. Access is restricted to dedicated upload/download areas on the server. |
| Warehouse network | Public Web Server via VPN | 80/TCP (HTTP)<br>443/TCP (HTTPS) | (Encrypted) Access to public web servers (including customer, supplier, etc.). |
| Warehouse network | Partner Secure File Transfer Server via VPN | 22/TCP (SSH/SFTP) | Protected access to the partner's secured file transfer server. |

### 3.2.6 Employees in Small Regional Offices

The employees in the three small regional offices access the e-commerce platform the same way as the partners do. They can exchange a bigger amount

of data with the head office through secured areas on GIAC Enterprises secure file transfer server. Email between the head office and the regional offices will be encrypted. Due to limited administrative resources these small offices do not get full VPN-access to the head office. Access is restricted to dedicated areas on the e-commerce platform and on the secured file transfer area. GIAC Enterprises provides X.509 client certificates to its employees for this purpose.

The same requirements and restrictions as for the partners apply to this group.

### 3.2.7 Regional Office Switzerland

The regional office in Switzerland gets full VPN-access to the head office. They have access to the internal mail server, to the file servers and to the e-commerce platform. They also have access to the secured areas on GIAC Enterprises secure file transfer server. Additional internet access is restricted to DNS, http, https and secure file transfer.

| Source | Destination | Port(s)/Protocol | Description |
|---|---|---|---|
| Regional office | VPN-Gateway | 500/UPD (IKE) | Key negotiation for establishment of VPN. |
| Regional office | VPN-Gateway | IP 50 (ESP) | VPN-Access from the regional office. |
| Regional office | DNS Server | 53/UDP (DNS) | Access to the public DNS server to resolve IP-addresses. |
| Regional office | Internal Mail Server via VPN | 110/TCP (POP3)<br>25/TCP (SMTP) | Access to the internal mail server for sending and receiving emails. |
| Regional office | Internal File Server via VPN | 137-139/TCP netbios<br>137-139/UDP netbios<br>445/TCP ms-ds | Access to the internal file server. |
| Regional office | SSL-Proxy via Internet | 443/TCP (HTTPS) | Protected access to the secured e-commerce platform via the SSL-Proxy. Access is restricted within the business application according to the needs of the user. This is enforced with mutual authentication based on X.509 client and server certificates and additional passwords. |
| Regional office | Secure File Transfer Server via Internet | 22/TCP (SSH/SFTP) | Protected access to the secured file transfer server. Access is restricted to dedicated upload/download areas on the server. |
| Regional office | Public Web Server via Internet | 80/TCP (HTTP)<br>443/TCP (HTTPS) | (Encrypted) Access to public web servers (including customer, supplier, etc.). |
| Regional office | Partner Secure File Transfer Server via Internet | 22/TCP (SSH/SFTP) | Protected access to the partner's secured file transfer server. |

### 3.2.8 Sales Force

GIAC Enterprises has employed field staff. They are based at the head office in Germany. The sales force (5 employees) is equipped with laptops. Docking stations are supplied for them at the head office. They are present in the head office once a week. They also need access to the mail server, the file servers, the e-commerce platform and to the secured areas on the file server. Additional internet access is restricted to http, https and secure file transfer. All access will be available through the VPN-solution when they work in the field.

| Source | Destination | Port(s)/Protocol | Description |
|---|---|---|---|
| Field staff | VPN-Gateway | 500/UPD (IKE) | Key negotiation for establishment of VPN |
| Field staff | VPN-Gateway | IP 50 (ESP) | VPN-Access from the regional office |
| Field staff | Internal DNS Server via VPN | 53/UDP (DNS) | Access to the internal DNS server resolve IP-addresses |
| Field staff | Internal Mail Server via VPN | 110/TCP (POP3)<br>25/TCP (SMTP) | Access to the internal mail server for sending and receiving emails |
| Field staff | Internal File Server via VPN | 137-139/TCP netbios<br>137-139/UDP netbios<br>445/TCP ms-ds | Access to the internal file server. |
| Field staff | SSL-Proxy via VPN | 443/TCP (HTTPS) | Protected access to the secured e-commerce platform via the SSL-Proxy. Access is restricted within the business application according to the needs of the user. This is enforced with mutual authentication based on X.509 client and server certificates and additional passwords. |
| Field staff | Secure File Transfer Server via VPN | 22/TCP (SSH/SFTP) | Protected access to the secured file transfer server. Access is restricted to dedicated upload/download areas on the server. |
| Field staff | Public Web Server via VPN | 80/TCP (HTTP)<br>443/TCP (HTTPS) | (Encrypted) Access to public web servers (including customer, supplier, etc.) |
| Field staff | Partner Secure File Transfer Server via VPN | 22/TCP (SSH/SFTP) | Protected access to the partners secured file transfer server. |

## 3.3 Security Architecture

### 3.3.1 Architecture Diagram

Based on the access requirement of the different groups interacting with GIAC Enterprises the following security architecture is being developed.

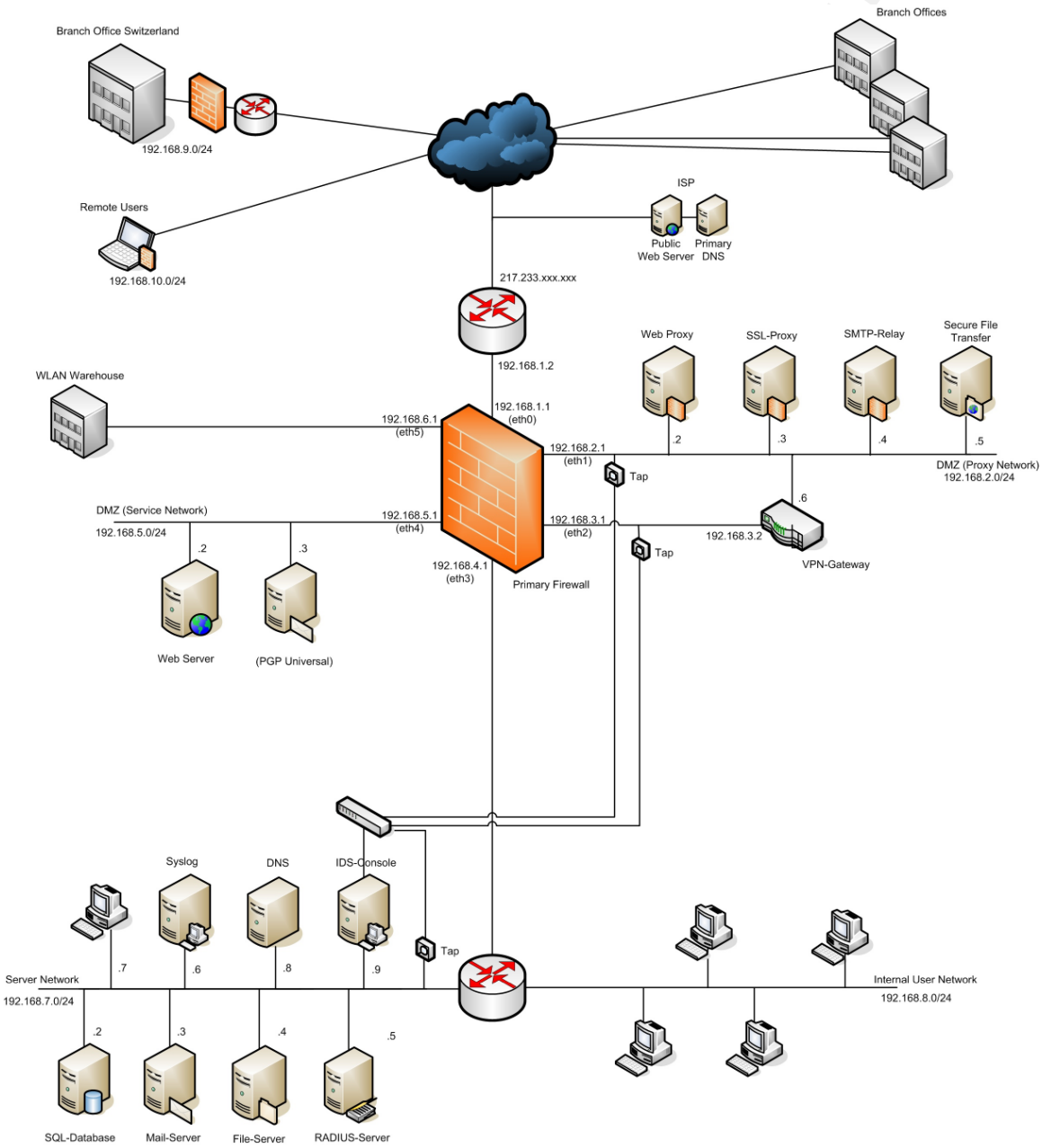


**Figure 2: Architecture Diagram**

#### 3.3.1.1 IP Address Scheme

The following address scheme is used to segment the network:

| | |
|---|---|
| 192.168.1.0/24 | Outside Firewall |
| 192.168.2.0/24 | DMZ Proxy Network |
| 192.168.3.0/24 | VPN Gateway Inside |
| 192.168.4.0/24 | Inside Firewall |
| 192.168.5.0/24 | DMZ Service Network |
| 192.168.6.0/24 | Warehouse Network |
| 192.168.7.0/24 | Server Network (and Management Network) |
| 192.168.8.0/24 | Internal User Network |
| 192.168.9.0/24 | Branch Office Switzerland |
| 192.168.10.0/24 | Remote Users (Sales Force) |

### 3.3.2 Architecture

#### 3.3.2.1 Primary Firewall and Border Router

The first line of defense is the border gateway router. Based on the access requirements, the relatively low amount of data being transmitted in the fortune cookie saying business and the relatively low interest of the general public into this business GIAC Enterprises decided to install a Cisco 26020XM (with the latest 12.3 software release installed). The router drops all obviously spoofed incoming/outgoing traffic and stops all internal traffic leaking to the internet.

All other filtering is done on the firewall, the second line of defense. GIAC Enterprises installed a Cisco Pix 515E firewall (with the latest software release 6.3(4) installed) with six interfaces. The firewalls performance fits the access requirements. This design allows a good separation of the different networks:

- Internet
- Local network
- Wireless local network of the warehouse
- Service network
- VPN-Gateway
- Proxy Network

Traffic to the service network must first pass the proxy network. Server software running in the proxy network is different from the software running on the service network. Both measures act as an additional layer of defense to protect the servers in the service network.

The server network, containing the database server, the internal mail server and the file server, is separated from the local network through an additional router. This router uses reflexive filters as an additional layer of defense. This security measure mitigates the risks of an internal attack performed by internal users or by malicious software.

#### 3.3.2.2 Business Data Flow

Nearly all of the business data flows through the e-commerce platform or is transmitted via email. According to GIAC Enterprises encryption policy all business data transmitted on public networks must be encrypted.

The business data itself is stored in a Microsoft SQL-Server database, located in the server network. The business application (e-commerce platform) is running on the web-server in the service network. Special care has been taken to protect the business application and the SQL-Server against SQL-Injection attacks.

The access to this web-server is encrypted with Secure Socket Layer (SSL) and requires mutual authentication based on X.509 client and server certificates. All traffic to the web-server must pass the reverse proxy based on Pound in the proxy network, which supports an additional layer of protection. The reverse proxy Pound handles the SSL-traffic, forwards the client credentials to the actual web server and also allows "sanitizing" the incoming http requests.

#### 3.3.2.3 Email

Email to and from smaller branch offices, partner and suppliers must be encrypted. Incoming email is first handled on the SMTP-relay in the proxy network based on Sendmail. The mail is filtered for spam and known viruses on the relay and then forwarded to the internal mail server in the server network. Email is one of the major gateways for viruses and Trojans. GIAC Enterprises wants to ensure that only expected attachments can pass the gateway. Only attachments with certain extensions (like ".giaczip" instead of ".zip") are allowed to pass the gateway, all others attachments will be discarded and the recipient will be notified. In this case the employees request the sender to send the attachment again with the arranged extension.

GIAC Enterprises plans to install a second mail-relay like "PGP-Universal" in the service network in the near future to automatically enforce the email encryption policy. Additional Decryption Keys will then be used to scan encrypted mails for viruses and Trojans.

Outgoing email will be "sanitized" at the SMTP-relay.

#### 3.3.2.4 Secure File Transfer

The secure file transfer GIAC Enterprises uses to exchange bulk data with partner, supplier and the remote offices is based on SSHv2. This guarantees that business data is securely encrypted while being transferred on public networks. The file transfer area is intended for temporary storage only.

#### 3.3.2.5 Public Web Server and Primary DNS

GIAC Enterprises public web server and its primary DNS server is outsourced to its ISP. The relatively low interest of the general public in the fortune cookie business generates only low traffic on the web server. This would not justify

setting up an additional web server in the service network and an additional reverse web proxy in the proxy network.

#### 3.3.2.6 Outbound Traffic

Outbound http- and https-traffic goes through the web proxy “squid” located in the proxy network. The proxy is configured in transparent mode and allows additional filtering of outbound and inbound traffic.

Secure file transfer is allowed outbound according to the access requirements.

#### 3.3.2.7 Virtual Private Network

The VPN device needs to handle the traffic originating from the branch office in Switzerland, from the WLAN located in the warehouse and from the remote users. The traffic will be encrypted with 256-bit AES IPSec and authentication is based on X.509 certificates. The VPN appliance needs to handle about 20 simultaneous IPSec-connections. GIAC Enterprises decided not to use the VPN capabilities of the primary firewall, as this would put additional load on the firewall and running services on the firewall might compromise its security. Instead a Cisco VPN 3005 Concentrator will be used.

The branch office in Switzerland has only limited IT resources on location. It is protected through its own firewall (Cisco PIX 506E, latest software release installed) and a border gateway router. All inbound traffic is blocked and only outbound DNS, http, https, secure file transfer and outbound IPSec is allowed. All other traffic (expect “local” traffic) is tunneled through the VPN to the head office. The firewall is used as VPN-endpoint.

The remote users are equipped with laptops running Windows XP (SP2). Personal firewalls installed on the laptops block all inbound traffic and allow only outbound IPSec. The complete traffic is consequently tunneled through the VPN. Users only have limited permissions on the laptops and can not change any security settings. Patches are automatically deployed to the laptops.

The external interface of the VPN Gateway is attached to the proxy network. All traffic passing the VPN gateway is routed back through the main firewall. This protects the internal network from malicious traffic tunneling from the branch office, from the warehouse WLAN or from the remote users to the head office. Alerts will be generated in case of suspicious traffic patterns.

#### 3.3.2.8 Network based Intrusion Detection System

Network based Intrusion Detection (NIDS) is done with Snort. Therefore network taps are placed in different places of the network, to passively monitor all network traffic. These sensors are all connected to a dedicated switch in a separated management network. This way the NIDS is protected from connection based attacks and additional taps can easily be deployed if needed. The sensors are placed in the proxy network, the server network and on the inside interface of the

VPN-gateway. The traffic received from the “wireless” sensor placed in the warehouse is also forwarded to the NIDS. The IDS-rules are optimized to validate the firewall rule-set. The placement of the sensors is sufficient for GIAC Enterprises security needs due to the following reasons:

- All “directly” exposed hosts are located in the proxy network. This is the place with the highest likelihood of an attack. In the worst case the attack is successful and the attacker will try to get further on. In both cases the IDS-sensor will monitor this traffic.
- All traffic from the remote office, the VPN-users and from the warehouse LAN can be monitored behind the VPN-gateway. In case one of these networks is compromised the IDS-sensors will also monitor this traffic.
- GIAC Enterprises most valuable business data is stored on the servers in the server network, therefore a IDS-sensor is placed in this segment. This placement also allows monitoring “internal” attacks.
- No sensor is placed outside the firewall due to the expected high amount of false alarms produced by the IDS and the limited IT resources to go behind them.

#### 3.3.2.9 Logging

Logging is done with a Syslog server placed in the server network. Logs will be audited every day.

#### 3.3.2.10 X.509-Certificates

GIAC Enterprises operates its own Public Key Infrastructure (PKI) based on OpenSSL. The PKI and GIAC Enterprises root certificate is installed on a laptop. Access is restricted to that laptop and it will be locked in a vault when not in use. The PKI allows the company to issue X.509 client certificates for their employees, suppliers and partners as well as certificates for the VPN-solution and the WLAN authentication.

#### 3.3.2.11 Additional Restrictions

Running peer-to-peer networking, file-sharing or instant messaging software is not allowed for employees by network usage policy due to security and legal considerations. Firewall and routing filters will be applied to prevent this traffic if possible and traffic will be monitored to detect this kind of network traffic.

## 3.4 Defense in Depth

A high level of security is achieved by the layered design and the partition of the different security measures. This design prevents the existence of a “single point of failure”. No accessible services are running on the firewall or on the border gateway router, as both are configured through the console interface and all services are disabled to prevent connection based attacks on these devices.

The most vulnerable and public available services are grouped together in the proxy network. This network is monitored with IDS. The firewall triggers alerts in case of suspicious traffic patterns in the proxy network (for example if the SMTP-Proxy tries to open a connection to an FTP-server on the internet).

The web server, also one of the vulnerable services, is protected through the reverse proxy Pound and is located in a separated network. Pound is configured to clean the incoming https-request and additionally filters attack patterns. Attack patterns missed by the reverse proxy can be detected with the IDS.

VPN-traffic from the warehouse network, the remote users and the remote office needs to pass the firewall, as these networks are considered to be less secure than the internal network in the head office. All VPN-traffic is monitored with the IDS and the firewall triggers alerts in case of suspicious traffic patterns.
This way problems in these networks are detected easily and strict filtering of the traffic can prevent escalation of these problems.

One of the big drawbacks of this firewall design is the higher complexity of the rulebase due to the firewall’s six interfaces. This complexity makes the audit even more important.

The protocols used to exchange business data (like SSL, SSH and also IPSec) provide mutual authentication and ensure that authentication credentials passing the public network are always encrypted.

Vital business data is stored on servers in the additionally protected server network, which is also monitored by the Network base Intrusion Detection System.

# 4 Assignment 3 – Router and Firewall Policies

## 4.1 Router Policy

GIAC Enterprises security architecture is designed with defense in depth in mind. This shows the layered design with a Stateful Inspection based firewall and proxy hosts. To create a balanced design that supports functionality as well as security the router is simply used for blocking “absolute” traffic patterns with static packet filtering. As an additional inevitable measure the router will be hardened, as it is the first line of the defense. Some of the filter rules also help to augment the firewall policy.

### 4.1.1 Ingress ACL

Ingress filtering is done with extended access lists applied on the external interface of the router.

All traffic having “invalid” source IP addresses is blocked:

- Private Networks:

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
```

- “Autoconfiguration” address (unassigned DHCP clients):

```
access-list 101 deny ip 169.254.0.0 0.0.255.255 any
```

- Multicast or engineer Networks:

```
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
```

- Loopback address:

```
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
```

- Internal address:

```
access-list 101 deny ip <internal adresses> 0.0.0.255 any log
```

- Unallocated legal addresses (according to iana.org):

```
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
…
```

All denied traffic is logged as it might be an indication of an upcoming attack, except for the private network addresses and the “autoconfiguration” addresses. Due to the high amount of mis-configured systems on the internet logging of this traffic would provide no additional benefit.

Incoming traffic to specific destination ports is blocked:

```
access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 139
access-list 101 deny tcp any any 445
access-list 101 deny udp any any 1434
access-list 101 deny tcp any any 1433
access-list 101 deny udp any any 69 log
access-list 101 deny udp any any 514 log
access-list 101 deny udp any any range 161 162 log
access-list 101 deny icmp any any host-redirect echo
```

These rules have been added to augment the firewall policy. It additionally blocks services that are critical to GIAC Enterprises internal infrastructure, giving a second layer of protection. Logging is only done when it provides additional benefit.

As a last rule all traffic not matching the above rules is allowed.

```
access-list 101 permit any any
```

The order of the rules is not significant, except for the last rule. Any "successful" packet must pass all other rules before it is permitted by the last rule. For performance reasons the most commonly used rules are placed at the beginning.

### 4.1.2 Egress ACL

Egress filtering is also done with extended access list.

Outgoing traffic to specific destination ports is blocked:

```
access-list 102 deny tcp any any range 135 139
access-list 102 deny udp any any range 135 139
access-list 102 deny tcp any any 445
access-list 102 deny udp any any 1434 log
access-list 102 deny tcp any any 1433 log
access-list 102 deny udp any any 69 log
access-list 102 deny udp any any 514 log
access-list 102 deny udp any any range 161 162 log
access-list 102 deny icmp any any echo-replay unreachable
```

These rules have been added to block information leakage out to the internet from services that are critical to GIAC Enterprises internal infrastructure. The blocking of outbound ICMP echo-replays and unreachable packets constrict attackers abilities to map the network.

Second, outgoing traffic is only allowed from legitimate source IP addresses:

```
access-list 102 permit <internal addresses> 0.0.0.255
access-list 102 deny any log-input
```

These last both rules prevent spoofing of source IP addresses and logs MAC address information of the host spoofing its address.

Once again the order of the rules is not significant, except for the last two rules. Any “successful” packet must pass all other rules before it is permitted to leave the network. Every packet not explicitly permitted contains a spoofed source IP address and is therefore stopped and logged.

### 4.1.3 Hardening the Router

Access to the router is only permitted through the console interface. Other “unprotected” administrative access (like SNMP, telnet, SSHv1, etc.) is disabled. The password on the router will be encrypted.

Loose Source Routing is disabled, as it can be used to route malicious traffic to destinations than can not be reached due to access lists restrictions.

All running services like echo, discard, chargen and daytime, as well as the finger service and the http and bootp servers will be disabled. These services are not needed for proper operation and therefore should not be enabled, as this could give attackers valuable information or, in case of undiscovered vulnerabilities, access to the router.

ICMP traffic will be limited at the router. “IP direct-broadcast” will be disabled to prevent malicious directed broadcast causing Denial of Service problems like “Smurf Amplification”. ICMP unreachable messages will be disabled to prevent leakage of network information based on ICMP error messages.

Warning banners will be provided. The banner only shows “WARNING: authorized access only!” indicating that it would be unlawful to enter or attempt to enter without authorization. No further information is included to prevent unwanted “leakage” of information.

Significant events (see ingress and egress ACL’s) will be logged to Syslog.

The router will be checked for unwanted services and proper configuration with a portscan before it is deployed.

## 4.2 Firewall Policy

The firewall is the second line of defense after the border gateway router. The router is configured to filter only "absolute" traffic patterns, whereas the firewall uses stateful packet filtering. Strict filter rules are applied to the firewall allowing only traffic according to the defined access requirements. Alerts will be generated in case of suspicious traffic dropped on the DMZ interfaces.

Dropped traffic due to the egress filtering for specific destination ports on the router indicates that the firewall is compromised (or not properly configured). Such packets should not leave the firewall due to its rulebase.

The firewall could be used as VPN-gateway, but in this case a service needs to run on the firewall. In case of vulnerabilities an attacker could use this service to gain access to the firewall. Therefore an additional VPN-gateway is installed.

All traffic is logged to Syslog except when explicitly noted.

### 4.2.1 General Rules

According to the access requirements there are only few services GIAC Enterprises need to access on the internet. The firewalls rulebase will reflect this and only the required ports will be "opened" on the firewall. All other outbound traffic will be restricted. The routers configuration is less restrictive, but it additionally blocks services that are critical to GIAC Enterprises internal infrastructure. Internal hosts are allowed to send Echo-Request packets to the firewall for diagnostic reasons. All other traffic to the firewall interfaces and broadcast traffic is blocked. Broadcast traffic will not be logged.

```
permit –i eth3 –p icmp –s 192.168.7.0/24 – d 192.168.6.1 echo-request
permit –i eth3 –p icmp –s 192.168.8.0/24 – d 192.168.6.1 echo-request

drop –i eth3 –p ip –s 192.168.7.0/24 –d 192.168.1.1
drop –i eth3 –p ip –s 192.168.7.0/24 –d 192.168.2.1
….
```

### 4.2.2 Inbound Traffic

Inbound traffic to the interface eth0 is allowed only for SMTP, SSL, SSH and VPN to the servers on the proxy network.

```
permit –i eth0 –p tcp –s 0/0 –d 192.168.2.4 - -dport 25
permit –i eth0 –p tcp –s 0/0 –d 192.168.2.3 - -dport 443
permit –i eth0 –p tcp –s 0/0 –d 192.168.2.5 - -dport 22
permit –i eth0 –p udp –s 0/0 –d 192.168.2.6 - -dport 500
permit –i eth0 –p ip –s 0/0 –d 192.168.2.6 - -dip-proto 50
```

### 4.2.3 Outbound Traffic from Internal User Network

According to the access restrictions employees are only allowed to use http, https, secure file transfer, email and file services. The mail server, the file server and the DNS server are located in the server network. Therefore no rules need to be applied for that on the primary firewall.

Access to the SSL-Proxy and to secure file transfer server as well as to all other secure file transfer servers in the internet is permitted.

```
permit –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.2.3 - -dport 443
permit –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.2.5 - -dport 22
drop –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.0.0/16 - -dport 22
permit –i eth3 –p tcp –s 192.168.8.0/24 –d 0/0 - -dport 22
```

Http and https traffic is routed (by means of policy based routing) to the web proxy Squid in the proxy network. Http and https traffic to all other destinations within the local networks is explicitly dropped.

```
drop –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.0.0/16 - -dport 80
permit –i eth3 –p tcp –s 192.168.8.0/24 –d 0/0 - -dport 80 fwd 192.168.2.2

drop –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.0.0/16 - -dport 443
permit –i eth3 –p tcp –s 192.168.8.0/24 –d 0/0 - -dport 443 fwd 192.168.2.2
```

### 4.2.4 Outbound Traffic from Internal Server Network

From the internal server network outbound DNS-traffic and outbound SMTP-traffic to the SMTP-relay needs to be allowed:

```
permit –i eth3 –p udp –s 192.168.7.8 –d <primary dns> - -dport 53
permit –i eth3 –p tcp –s 192.168.7.8 –d <primary dns> - -dport 53
permit –i eth3 –p tcp –s 192.168.7.3 –d 192.168.2.4 - -dport 25
```

### 4.2.5 Traffic from Proxy Network and Service Network

The web proxy Squid needs to access web servers (http and https) on the internet:

```
drop –i eth1 –p tcp –s 192.168.2.2 –d 192.168.0.0/16 - -dport 80
permit –i eth1 –p tcp –s 192.168.2.2 –d 0/0 - -dport 80

drop –i eth1 –p tcp –s 192.168.2.2 –d 192.168.0.0/16 - -dport 443
permit –i eth1 –p tcp –s 192.168.2.2 –d 0/0 - -dport 443
```

The SMTP-Relay delivers mail to mail servers on the internet and to the internal mail server:

```
permit –i eth1 –p tcp –s 192.168.2.4 –d 192.168.7.3 - -dport 25
drop –i eth1 –p tcp –s 192.168.2.4 –d 192.168.0.0/16 - -dport 25
permit –i eth1 –p tcp –s 192.168.2.4 –d 0/0 - -dport 25
```

The SSL-Proxy forwards to the web server in the service network:

```
permit –i eth1 –p tcp –s 192.168.2.3 –d 192.168.5.2 - -dport 80
```

The web server in the service network needs to access the SQL-Server in the server network:

```
permit –i eth4 –p tcp –s 192.168.5.2 –d 192.168.7.2 - -dport 1433
```

### 4.2.6 VPN-Traffic

VPN-traffic from the branch office, the remote users and the WLAN of the warehouse needs to be processed. The rules for the remote users will be shown exemplarily for this group; similar rules apply for the branch office and for the warehouse WLAN (which additionally needs access to the RADIUS-server).

Remote users need access to email, file services and DNS in the server network:

```
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.7.3 - -dport 25
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.7.3 - -dport 110

permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.7.4 - -dport 137
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.7.4 - -dport 138
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.7.4 - -dport 139
permit –i eth2 –p udp –s 192.168.10.0/24 –d 192.168.7.4 - -dport 137
permit –i eth2 –p udp –s 192.168.10.0/24 –d 192.168.7.4 - -dport 138
permit –i eth2 –p udp –s 192.168.10.0/24 –d 192.168.7.4 - -dport 139
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.7.4 - -dport 445

permit –i eth2 –p udp –s 192.168.10.0/24 –d 192.168.7.8 - -dport 53
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.7.8 - -dport 53
```

Remote users need access to the secured file transfer server and the SSL-Proxy in the proxy network:

```
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.2.3 - -dport 443
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.2.5 - -dport 22
```

Remote users are allowed to access http and https-servers on the internet via the http-Proxy:

```
drop –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.0.0/16 - -dport 80
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 0/0 - -dport 80 fwd 192.168.2.2

drop –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.0.0/16 - -dport 443
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 0/0 - -dport 443 fwd 192.168.2.2
```

Remote users are allowed to access secured file transfer server on the internet:

```
drop –i eth2 –p tcp –s 192.168.10.0/24 –d 192.168.0.0/16 - -dport 22
permit –i eth2 –p tcp –s 192.168.10.0/24 –d 0/0 - -dport 22
```

### 4.2.7 Additional Rules

Logging is done on the Syslog-Server in the service network. Therefore access to this server must be allowed for all logging devices:

```
permit –i eth0 –p udp –s 192.168.1.2 –d 192.168.7.6 - -dport 514
permit –i eth1 –p udp –s 192.168.2.2 –d 192.168.7.6 - -dport 514
….
```

To prevent delays on outbound mail delivery Ident will be rejected:

```
reject –i eth0 –p tcp –s 0/0 –d 192.168.2.4 - -dport 113
```

All other traffic is not allowed and will be dropped explicitly:

```
drop –i eth0 –s 0/0 –d 0/0
drop –i eth1 –s 0/0 –d 0/0
drop –i eth2 –s 0/0 –d 0/0
drop –i eth3 –s 0/0 –d 0/0
drop –i eth4 –s 0/0 –d 0/0
drop –i eth5 –s 0/0 –d 0/0
```

### 4.2.8 Optimization

Some of the drop-rules can be generalized, for example the three drop-rules for the outbound traffic from the internal user network.

To increase performance the first one of the following three “special” rules

```
drop –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.0.0/16 - -dport 22
…
drop –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.0.0/16 - -dport 80
…
drop –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.0.0/16 - -dport 443
```

can be replaced with this more general rule

```
drop –i eth3 –p tcp –s 192.168.8.0/24 –d 192.168.0.0/16
```

and the last two rules can then be omitted.

### 4.2.9 Rule Order

The analysis of log files helps identifying the most common used permit-rules. These rules should be moved to the top of the rulebase to increase performance. This has to be done carefully as the rule order is often significant. To retain the context, blocks of rules, as shown in the following example, must be moved.

```
permit –i eth1 –p tcp –s 192.168.2.4 –d 192.168.7.3 - -dport 25
drop –i eth1 –p tcp –s 192.168.2.4 –d 192.168.0.0/16 - -dport 25
permit –i eth1 –p tcp –s 192.168.2.4 –d 0/0 - -dport 25
```

### 4.2.10 Hardening the Firewall

Access to the firewall is only permitted through the console interface. “Unprotected” administrative access and all other services are disabled on the firewall. The rulebase also prevents direct connection to the firewall interfaces.

The firewall is checked for unwanted services and proper configuration with a portscan before it is deployed.

# 5 List of References


Microsoft Corporation. Solutions for Security. Choosing a Strategy for Wireless LAN Security. 2004.

Microsoft Corporation. Securing Wireless LANs with Certificate Services v1.6. November 10, 2004.
<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/swlan.mspx>

Microsoft Corporation. Securing Wireless LANs with PEAP and Passwords. April 3, 2004.
<http://www.microsoft.com/technet/security/topics/cryptographyetc/peap_0.mspx>

Aboba, et al. RFC3748. Extensible Authentication Protocol (EAP), June, 2004.
<http://www.ietf.org/rfc/rfc3748.txt>

FreeRADIUS
<http://www.freeradius.org/>

Takahashi, Takehiro. WPA Passive Dictionary Attack Overview.
<http://www.tinypeap.com/docs/WPA_Passive_Dictionary_Attack_Overview.pdf>

Strand, Lars. 802.1X Port-Based Authentication HOWTO. August 18, 2004.
<http://tldp.org/HOWTO/html_single/8021X-HOWTO/>

Kismet
<http://www.kismetwireless.net/documentation.shtml>

AirSnort
<http://airsnort.shmoo.com/>

Fluhrer, Scott, Mantin, Itsik and Shamir, Adi. Weaknesses in the Key Scheduling Algorithm of RC4.
<http://www.drizzle.com/~Eaboba/IEEE/rc4_ksaproc.pdf>

Cisco Systems. Cisco Aironet Wireless Access Points. 2004

Cisco Systems. Cisco Aironet 1200 Series Access Points. 2004

Cisco Systems. Give your Network Users Freedom and Mobility without Giving up Network Security. 2005

Snort
<http://www.snort.org/>

Laing, Brian. How To Guide-Implementing a Network Based Intrusion Detection System. 2000.
<http://www.snort.org/docs/iss-placement.pdf>

McCarty, Alan. Distributed NIDS: A HOW-TO Guide. September 4, 2003.
<http://www.sans.org/rr/whitepapers/detection/1249.php>

SANS Institute. Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks. Volume 2.1. SANS Press, 2004.

SANS Institute. Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks. Volume 2.2. SANS Press, 2004.

SANS Institute. Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks. Volume 2.3. SANS Press, 2004.

SANS Institute. Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks. Volume 2.4. SANS Press, 2004.

SANS Institute. Track 2 – Firewalls, Perimeter Protection and Virtual Private Networks. Volume 2.5. SANS Press, 2004.

Tikart, Andreas. Cisco Router. Bonn: mitp-Verlag, 2003

Tikart, Andreas. Cisco Firewall. Bonn: mitp-Verlag, 2003

Pound
<http://www.apsis.ch/pound>