Global Information Assurance Certification Paper

Designing the Network: How to own the Enterprise

Niels Bach

GCFW Practical
Version 3.0

Date: August 21, 2004

Introduction

This assignment is made in the context of the GIAC GCFW certification[1]. There are several sub assignments answered in the paper. The overall purpose of the assignment is to demonstrate how a secure network design could be implemented for the fabricated GIAC Enterprise, as well as to demonstrate the security aspects of network design in general.

The paper consists of four separate assignments:
Assignment 1 – Security Architecture
GIAC Enterprise is described and business operation is defined. In this part the network is presented with all the, in a security perspective, relevant components.

Assignment 2 – Security Policy and Component Configuration
The central components of the network are configured and hardened, and the practical implementation is described in detail.

Assignment 3 – Design under fire
A previous assignment is analysed for possible weaknesses and an imaginary attack is conducted and described. Furthermore suggestions are presented on how to mitigate the weaknesses of the design.

Assignment 4 – Future State of a Security Technology
In this assignment a security technology is presented with regard to the current state of the technology as well as possible future development and impact. I have chosen to look at the possibilities for automating policy enforcement.

[1] The title “Designing the Network: How to own the Enterprise” is inspired by the book “Stealing the Network: How to own a Continent” published by Syngress (ISBN: 1931836051) and written by some of the greatest all time hackers in the world.

Typographic Conventions

There are different typographic conventions in this document to ease the reading.

Code and screen text

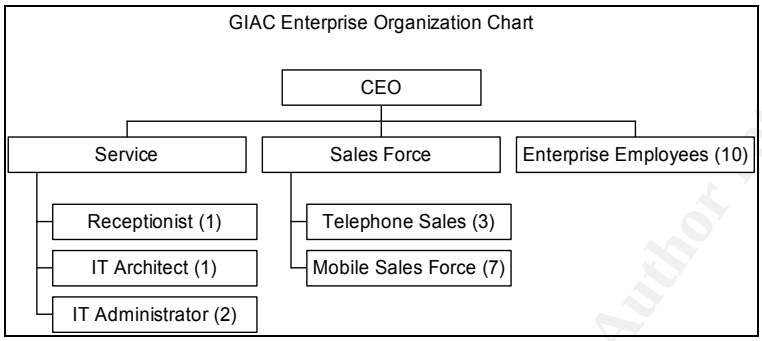
Examples of code or text that is taken directly from screen shots are presented in boxes.

```
$apt-get install debhelper kernel-package modutils \
libncurses5-dev gcc fakeroot libnet0-dev
```

Figures

Figures are presented in boxes with a caption above. The caption contains the figure number as well as a heading describing the figure.

Figure 1 - Organization Chart



Quotes

Quotes that are taken from web pages or books are indented and surrounded by (“).

> *“this a citation from a book or web site. It might be several lines, but if it is only one a short quotation is might be placed in the text.”*

Protocols and commands

Protocols like SMTP are written with in capitalized to stand out from a normal word. The same is the case for commands like SSH for example.

Use of colours

If the document is read online or printed in colour I have used the colour blue for comments in code and similar to ease the reading.

Assignment 1 – Security Architecture

The size of the GIAC Enterprise is small and so is the budget therefore is has been chosen to focus on Linux to build the infrastructure, since you will get a lot of functionality for free and here by cut down on expenses related to licenses.

There is an ongoing discussion on whether the running expense is higher or lower than if a system is based on proprietary software. This is mainly due to the lack of a structured support centre or hotline, and the need for the real competent administrators to get the best out of open source. I will put it this way, open source is freedom under responsibility and it might be hard to find people that have enough knowledge to take that responsibility.

The GIAC Enterprise have concluded that the newly hired IT architect is well educated regarding Linux and open source, so they have decided to chose that path.

Access requirements and restrictions

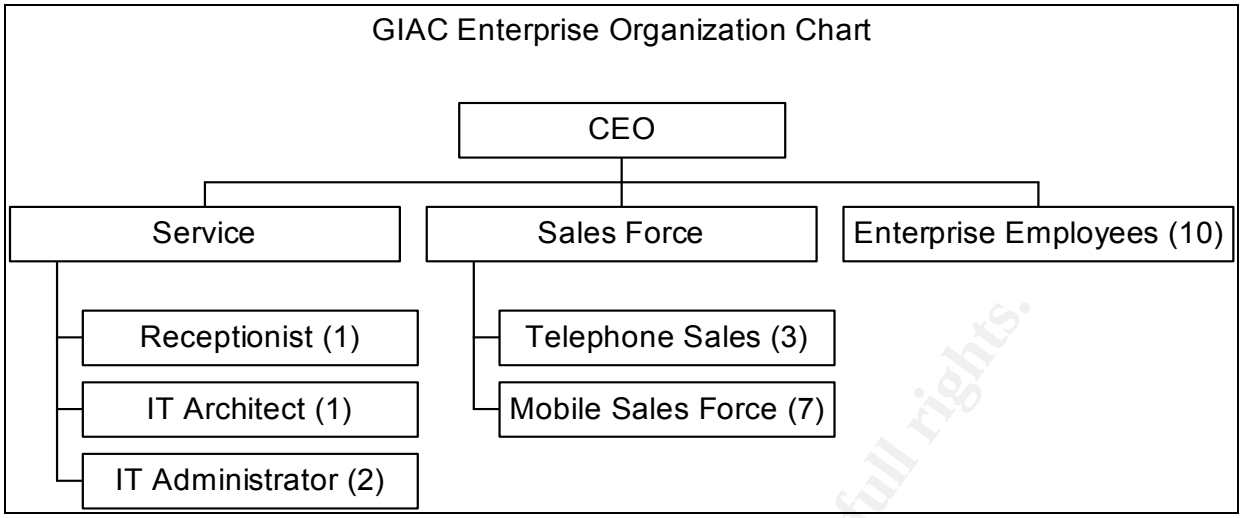
Success in the fortune business relies on two factors. 1) Sell a lot of fortunes, because the earning per volume is small – which means you need a good and dynamic sales force. 2) Minimize costs – fortunes does not involve sophisticated technologies and patents so it is important to be competitive on the price and quality as well as having a stable and fast Internet web site, to keep market shares.

Company Structure

GIAC Enterprise has 25 employees including the CEO. The enterprise organization can be studied in Figure 2 - Organization Chart. The company consist of:

- CEO
- 10 Enterprise Employees doing support and development
- Sales force consists of 3 people located in the office doing telephone sales and 7 mobile sales people.
- The receptionist.
- 1 system IT architect – design and update the network infrastructure.
- 2 system administrators – takes care of backup, patching and updates, as well as user support.

Figure 2 - Organization Chart



Business operation

GIAC Enterprise buys fortunes from the suppliers. The fortunes are placed in a central database. From this database bundles of fortunes are generated each night. The bundles are sold to customers. Customers are typically factories that print the fortunes and place them inside cookies or other merchandise. Partners are typically foreign companies that translate fortunes and resell them in their own country.

The GIAC Enterprise workforce consists of the employees located at the GIAC Enterprise internal network and the mobile sales force. To assist the mobile sales force when they are out of the house a VPN is deployed to grant access to necessary resources.

Customers – Companies or individual customers

Customers need access to the fortunes, so they can download bundles of fortunes. There are two functions that the customers need access to: 1) Browse the products available and the corresponding pricelists. 2) Download the bundles of fortunes.

Because the customers have different agreements with GIAC Enterprise and because the GIAC Enterprise handles details about the customers, it is necessary to use a secure connection for login and web pages that contains customer details and individual pricelists for larger customers. The fortunes have to be handled with care since they are what make the wheels spin at the GIAC Enterprise, so they are transferred using SFTP.

Customers inbound access protocols:

- HTTP (tcp port 80) – Standard for web browsing.
- HTTPS (tcp port 443) – Secure HTTP and supported by 99% of all browsers.
- SFTP (using SSH2 tcp port 22) – Encrypted FTP that is widely supported.

The customers need easy access to the services that GIAC Enterprise provides and they need the security that their information is treated respectfully and securely. This is accomplished through the use of standard protocols and strong encryption. Only standard protocols are used, so bundles of fortunes are not transferred with the HTTP because FTP is better to handle connection breakdown and resume download and so forth.

Suppliers – Suppliers of fortunes

The suppliers consist of a few companies that write the fortunes and sell them to the GIAC Enterprise. Suppliers upload bundles of fortunes to the GIAC Enterprise server, each supplier have a separate folder on the GIAC Enterprise file server.

Suppliers inbound access protocols:

- SFTP (using SSH2 TCP port 22) – Encrypted FTP that is widely supported

The suppliers need secure access to the SFTP server so the new fortunes delivered securely to the GIAC Enterprise. Certificates are used both on the server and client so both the GIAC Enterprise and the supplier is certain that the source and destination of the delivery is valid.

Every morning a script from the database server downloads the fortunes from the SFTP server, run a bunch of sanity checks and insert the fortunes in a central database. The database is connected to the web servers where the fortunes are presented. The database server is not directly accessible.

Partners – Translators and resellers

Partners consists of translators and resellers, their access are similar to customers they access the partner web site and download fortunes.

Partner's inbound protocols:

- HTTP (TCP port 80) – Standard for web browsing.
- HTTPS (TCP port 443) – Secure HTTP and supported by 99% of all browsers.
- SFTP (using SSH2 TCP port 22) – Encrypted FTP that is widely supported.

The partners download fortunes from one SFTP server and the suppliers upload to another one. This setup is established to ensure that there is a physical separation of the fortunes that are bought and the fortunes that are sold.

GIAC Enterprises employees located on GIAC Enterprises internal network

The employees located at the GIAC Enterprise need access to the Internet, email, file servers and servers in the DMZ. During the working hours they access the Internet to do general tasks like sending and receiving email and browsing web sites. The employees also need access to the web servers in the DMZ.

GIAC Enterprise employee's outbound protocols:

- HTTP (TCP port 80) – Standard for web browsing.
- HTTPS (tcp port 443) – Secure HTTP and supported by 99% of all browsers.
- FTP (TCP port 20/21) – Standard for file transfer.

The GIAC Enterprise employees use a mail gateway to send and receive email.

GIAC Enterprises mobile sales force

The sales force keeps GIAC Enterprise running and makes sure that market shares are expanded. They need access to customer data and file servers that are located on the LAN over the Internet, so they can work from outside the GIAC Enterprise. From inside the LAN they have the same access as the rest of the employees located at the GIAC Enterprise.

GIAC Enterprise mobile sales force outbound protocols (when located inside GIAC Enterprise):

- HTTP (TCP port 80) – Standard for web browsing.
- HTTPS (TCP port 443) – Secure HTTP and supported by 99% of all browsers.
- FTP (TCP port 20/21) – Standard for file transfer.

GIAC Enterprise mobile sales force inbound protocols (when located outside GIAC Enterprise):

- PPTP (TCP port 1723 + GRE protocol 47) – Standard for PPTP connection

The general public

The general public is also the mass of potentially new customers and they need access to the primary information channel of the GIAC Enterprise – the web site. They need to see the news and be able to gather information about how to buy fortunes and so on.

General public inbound access:

- HTTP (TCP port 80) – Standard for web browsing.

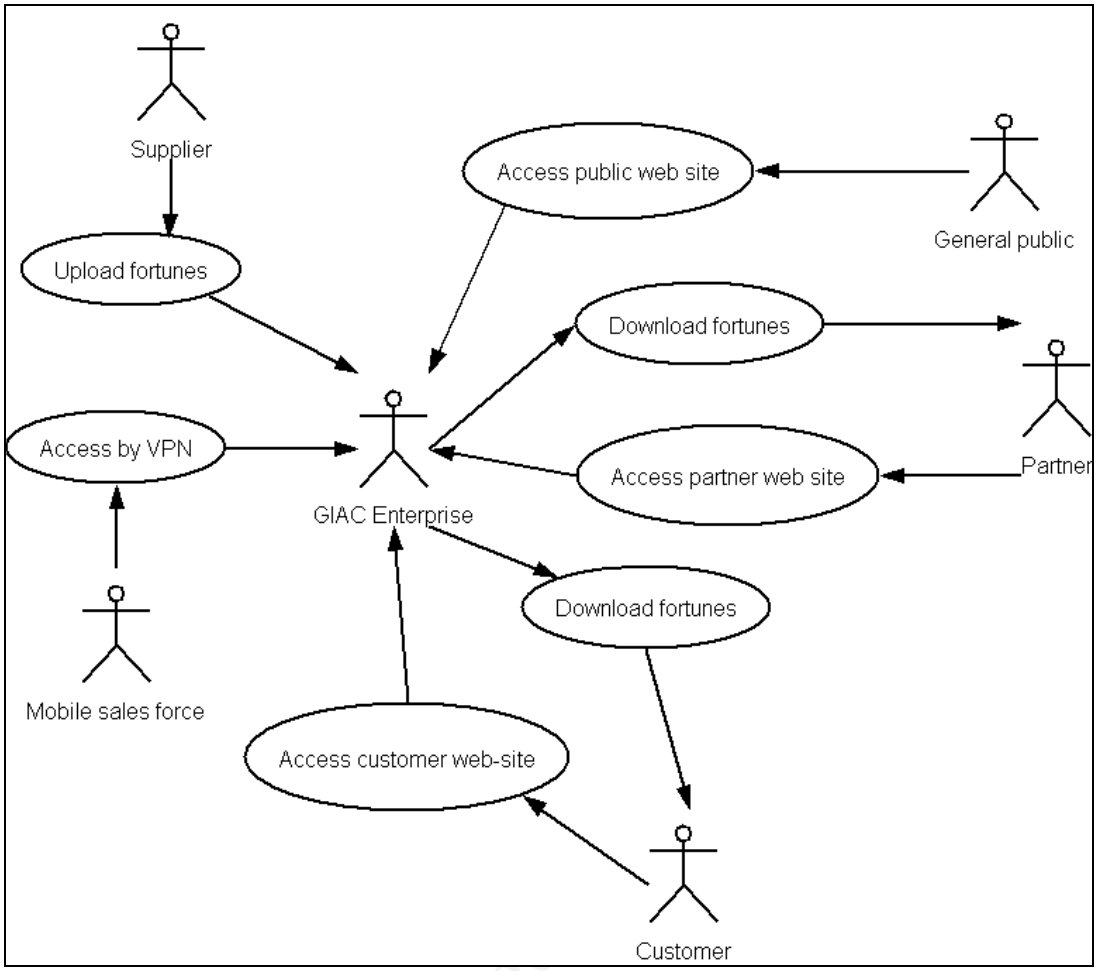
The general public need access to the web site of the GIAC Enterprise and using a standard web browser. The web site has to be stable and fast so customers get what they come for and this is the face of GIAC Enterprise on the Internet.

Interaction with the GIAC Enterprise

Figure 3 - Use Case Diagram shows the interaction of the GIAC enterprise with the outside world. The GIAC Enterprise covers the GIAC Enterprise employees and the sales force. The figure should reflect the overall business operation of the GIAC. The GIAC Enterprise, buy fortunes from the supplier and sell them to customers and partners/resellers. Some of the budget is spend on information and advertising to the public.

The handling of financial transactions will be outsourced to a trusted payment service. This eliminates a lot of security problems, laws and regulations with the storing of credit card information and other sensitive information. There are a lot of services offered on the Internet, that can be used to handle money transactions and therefore this issue is not considered so interesting in this context.

Figure 3 - Use Case Diagram



Network structure

In this section an overview of the entire network is presented followed by a detailed description of each component and its functionality.

Overview

In correspondence with the description of the GIAC Enterprise access requirements and restrictions, a network is designed which fulfil the needs of the enterprise.

Figure 4 - Network Diagram

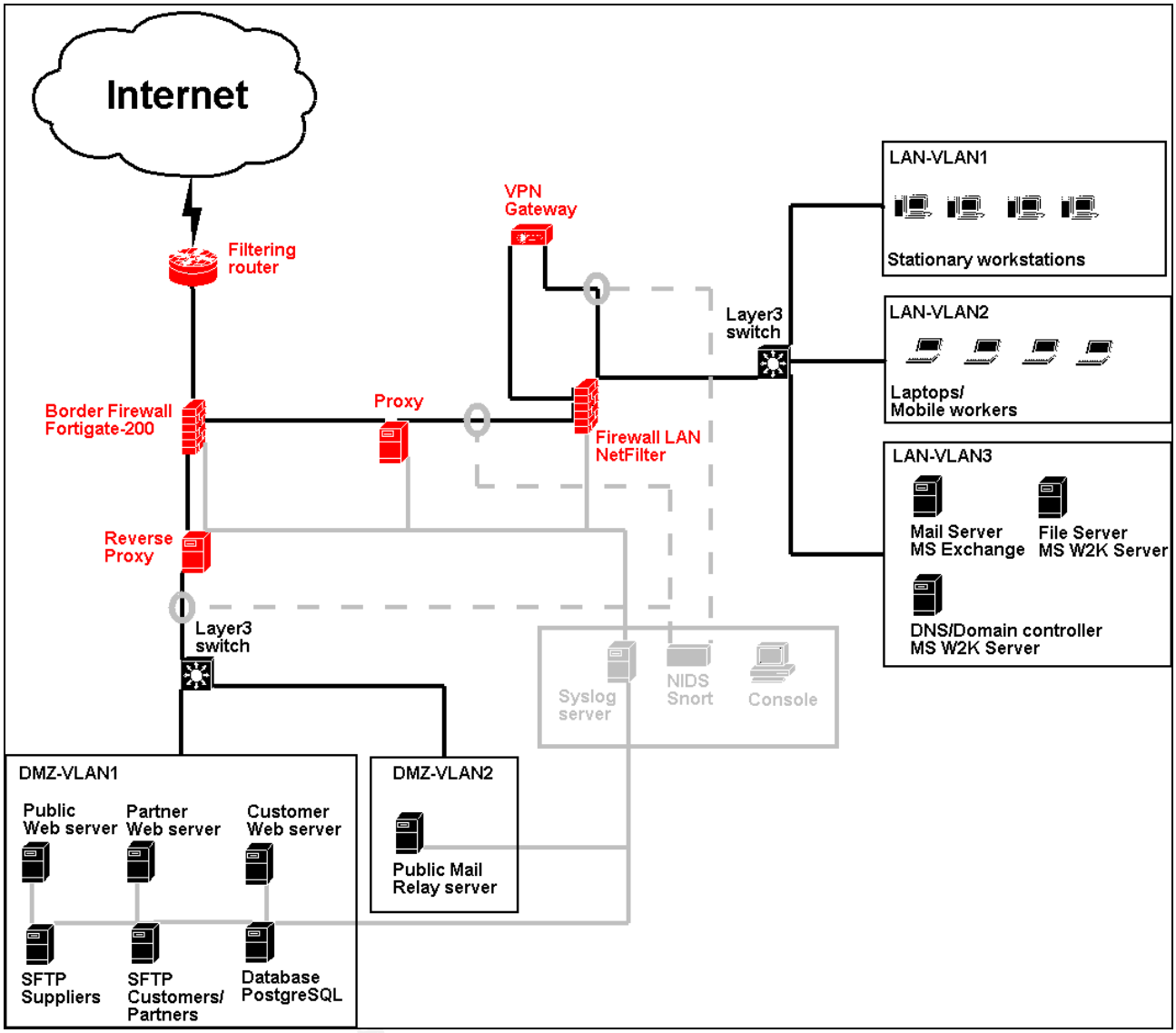


Figure 4 - Network Diagram shows the network topology and all the major components involved.

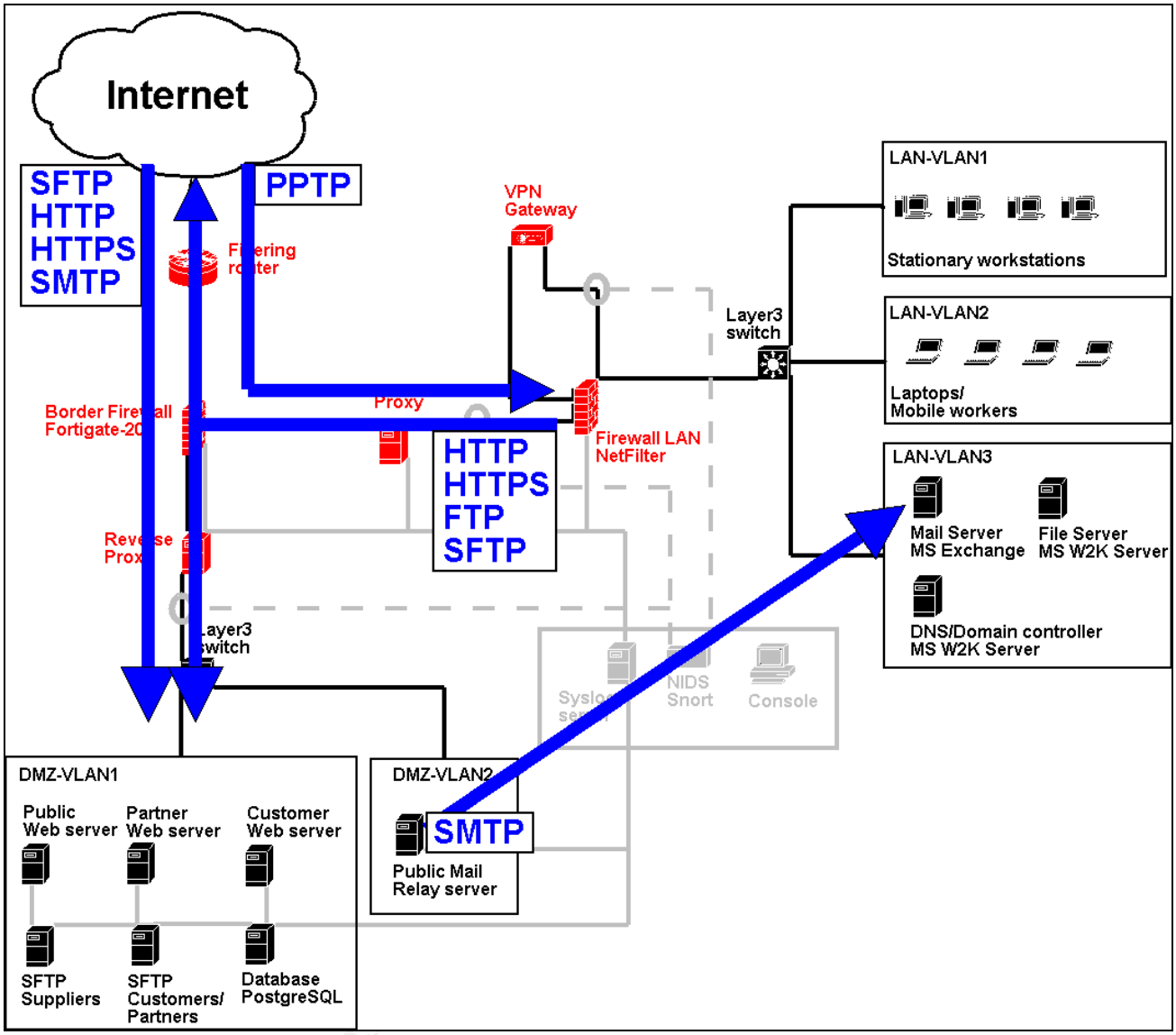
The general points to notice are:

- The Fortigate-200 (F200) firewall makes a single point of entry. This makes general access control easy with the use of the web interface. The powerful real time scanning provided by the F200 is utilized both for the DMZ and LAN.

- A NetFilter firewall is used to further protect the LAN and terminate VPN connections.
- A Squid proxy server in front of LAN accelerates the Internet connectivity, provides further protection of the LAN clients and makes it possible to utilize ACL's to avoid GoToMyPC and other sites that are considered harmful.
- VPN traffic from the Internet is terminated in conjunction with the LAN firewall. This offers maximum access control and possibilities for NIDS and virus scanning of tunnelled traffic.
- Network intrusion detection is focused on the LAN segment. The NIDS is used to detect suspicious traffic from the DMZ directed at LAN, like TCP SYN requests, which should never happen except from the mail server. There is also a probe analyzing traffic that has slipped behind the reverse proxy protecting the DMZ. The other part of the NIDS is used to check the traffic that has been decrypted by the VPN gateway. This is to detect if a hacker tries to use the VPN gateway as a backdoor to the LAN.

Figure 5 - Major Protocols show a combination of the network layout and the major access protocol needed for the GIAC Enterprise. Besides the protocols shown here, there is a need for ICMP, NTP and DNS traffic, as well as SMTP traffic from the mail server, to make the setup useable in practice.

Figure 5 - Major Protocols



In the following text the main components of the network architecture is presented in detail. There is an estimated price on each component. The important thing to notice is the difference characteristics of the servers in the network, some need to be fast and have a lot of disk space and some need neither. Another important aspect of the servers is standardization, all the servers are IBM x series and that makes it possible to have spares ready for replacement in case of breakdowns. Also the disks are standardized as much as possible.

Filtering Router

Purpose	• Provide Internet access. • Filter IANA private destination addresses. • Filter specific types of packages like ICMP source routing.
Details	The router is good at routing packets and filtering at IP level. Some routers can also do stateful inspection and act as VPN gateway but in this case we are adhering to the principle of using specific components for the assignment they where designed to do. The Cisco router is the first line of defence. It is possible to buy and extend the router with firewall functionality and stateful inspection, but that is expensive and with budgetary concerns it has been decided to use it as a filtering router to take the worst heat of malicious packages and traffic from faulty configured devices. The Cisco router is not very handy to configure and therefore the rules in it are made so general that it should very seldom be necessary to fiddle with it. Important characteristics of the border gateway router include: • Filter packets that should never appear. • Spare the firewall and IDS of processing the obvious malformed packets • Hardware box with few moving parts. • No general purpose OS
Placement	The border gateway is the very first line of defence. All data packets send or received from the Internet has to pass through it.
Hardware	Cisco 2611
Software	
Price	$800

Border Firewall – Fortigate 200 (F200)

Purpose	• Separate WAN, LAN and DMZ physically. • Manage public IP addresses. • Real time scan of Internet traffic. • First layer of stateful traffic inspection.
Details	The choice fell on Fortigate because of the following characteristics: • Low maintenance – it is automatically updated when you pay a yearly fee to Fortinet.

	• Easy access to block ports and IP addresses with a graphical user interface so even a non-technical person can do it. • Real time scanning of traffic. Fortigate contains powerful scan capabilities that allows it to scan traffic real time. The product includes virus scanner, NIDS, email and HTTP pattern scanning. • It can be used to terminate VPN connections using PPTP or IPSEC. The GIAC Enterprise will utilize IPSEC in the future to interconnect the remote offices with the head quarter. • ICSA certified with the firewall, intrusion detection, virus scanner and IPSEC technology. The F200 is the second line of defence; it separates the WAN (Internet), LAN and DMZ physically on three different interfaces. The F200 has a nice graphical interface that makes it handy to make quick changes for example blocking specific IP addresses and ports used by worms. The real time scanning capabilities makes the F200 nice to have since it might be able to stop most malicious traffic from entering the network. The graphical interfaces tend to be easy and good for smaller configurations but with large sets of rules and interfaces I prefer text-based configuration where it is not necessary to know about an enormous amount of windows to be sure how the thing is configured. Therefore the F200 is only used for what it is good at: Quick, dynamic small rule sets and real time scanning. The F200 is the general gateway for everyone coming from the outside customers, the general public, suppliers as well as the road warriors. All traffic goes through this box, except malformed packets that where filtered by the router. This is the place to shut down access on specific ports to block worms or modify patterns to block new viruses to the entire network. The F200 is supposed to take the load from the internal firewall by doing stateful inspection with a few basic rules. For example we don't want connections from the Internet to the LAN so this might as well be stopped as early as possible. Reasons why the F200 firewall has not been used as a one box solution: • If it is compromised the whole GIAC Enterprise would be exposed, there is too much at stake to trust one box and one technology. • It is not flexible enough to do more complicated setups as it only

	contains 3 interfaces. • Not suited for large and complex rule sets (in my opinion).
Placement	The F200 is placed directly behind the Cisco router.
Hardware	Fortigate-200 ASIC with specialized OS running of PROM
Software	
Price	$5000

Reverse Proxy

Purpose	• Accelerate web servers in the DMZ. • Second layer of defence for servers in the DMZ. • Traffic analysis.
Details	Controls ACL's to the DMZ and peaks performance of the services offered by GIAC Enterprise. The Reverse proxy is used to accelerate all the web traffic in the DMZ zone. Therefore it is necessary with a fast processor and larger disks to have plenty of cache space as well as disk space for logs used in traffic analysis. On all these business critical servers, hot swap disks are used, so minimize downtime in case of a disk crash.
Placement	Located in front of the DMZ servers to proxy traffic exchanged between the Internet and DMZ servers.
Hardware	IBM X-335 dual 3.06 GHz with 5 x 18 GB disk space RAID-5
Software	OS: Debian 3.0 GNU/Linux kernel 2.4.26 Squid version 2.5
Price	$8000

Proxy Server

Purpose	• Accelerate Internet access for LAN clients. • Protect LAN from certain web sites on the Internet that are regarded harmful. • Traffic analysis
Details	ACL on the proxy server are used to block access to web sites that are considered a threat to the security of GIAC Enterprise this includes GoToMyPC. It also has access logs so the utilization of the Internet connections can be studied. Surveillance of users is not the primary goal, but it can be relevant in case of a security breach. The traffic load is not so heavy on this segment; so a lot less have been

	spend on the hardware compared to the reverse proxy.
Placement	Located between the F200 and the firewall-LAN.
Hardware	IBM X-330 dual 1.1 GHz with 2 x 73 GB disk space RAID-1 (mirror)
Software	OS: Debian 3.0 GNU/Linux kernel 2.4.26 Squid version 2.5
Price	$3000

Firewall – LAN

Purpose	• Protect LAN from inbound access. • Control VPN (PPTP) connections from the Internet.
Details	The LAN is protected by a NetFilter firewall running on Debian. The firewall needs 5 interfaces, since it has to terminate the PPTP VPN connection (2 interfaces), as well as being connected to the support network, LAN and WAN. NetFilter was chosen to make a cheap yet complex and secure solution. The organisation of NetFilter and the principles of chains and tables make it ideal for fairly complex and specialized configurations. The security history of NetFilter is good and it is a proven technology. • Good for complex solutions because of the flexible structure. • Cheap and fast. • Can handle the 5 interfaces needed. • Proven firewall technology. The NetFilter LAN firewall is the gateway for the employees, all traffic leaving and entering the LAN have to pass the NetFilter firewall. Further more it is the critical place where PPTP connections are terminated and logged. Traffic from the PPTP tunnels are analysed and filtered for intrusion patters in conjunction with the LAN firewall. The LAN firewall controls the services and protocols that are available to the employees of the GIAC Enterprise. The firewall permits outbound packets from LAN on selected ports corresponding to the ports that are needed by the employees. The firewall also do stateful inspection to ensure that packets going into the LAN was requested from the LAN and there are no new connections established inbound from the Internet or DMZ. Firewall-LAN also protects the LAN from the proxy server. Even if the proxy server is compromised it will not be possible to directly attack the LAN. Using a software firewall makes it easy

	to customize but there are several moving parts and it is important to utilize RAID and redundant power supplies to accommodate for this.
Placement	Located in front of the LAN
Hardware	IBM X-330 dual 1.1 GHz with 2 x 18 GB disk RAID-1 (mirror)
Software	OS: Debian 3.0 GNU/Linux kernel 2.4.26
Price	$2500

VPN Gateway – LAN

Purpose	• Terminate PPTP VPN
Details	Encryption and decryption of data and termination of tunnels. The VPN software is isolated on a dedicated server. This will prevent the firewall from being touched by security issues with the PPTP software. The tunnel is terminated and lead back through the firewall which means that content analysis is possible. Firewall-LAN can both control encrypted traffic to the VPN gateway as well as unencrypted traffic from the VPN gateway to LAN. The possibilities to analyse traffic to and from the VPN gateway is especially important since GIAC Enterprise is utilizing PPTP, that lacks the authentication header found in IPSEC. The LAN firewall becomes more complex due to the handling of 2 additional interfaces but that is acceptable.
Placement	Located in conjunction with firewall-LAN, both the inbound and the outbound connection of the VPN gateway are protected by firewall-LAN.
Hardware	IBM X-330 dual 1.1 GHz with 2 x 18 GB disk RAID-1 (mirror)
Software	OS: Debian 3.0 GNU/Linux kernel 2.4.26 with MPPE/MPPC patch version 2.4.2 PoPTop version 1.1.4-b4
Price	$2500

Additional components

Beside the components needed to secure the infrastructure there are several services available on the GIAC Enterprise network. Here follows a short description of the different servers on the network and their function. They all are considered possible attack vectors and are therefore interesting to mention in this context.

First the DMZ servers are introduced:

Mail relay server - DMZ

Purpose	• Receive mail from the Internet
Details	The mail relay server is very important in a security perspective because it

	is the only server in the DMZ that is allowed to initiate connections to the LAN zone. This is necessary for the relay server to deliver mail to the exchange server. The relay server is running Exim in combination with MailScanner. The setup consists of two Exim processes one for incoming mail and one for outgoing mail. The incoming process receives mail from the Internet and passes it to the MailScanner, which utilize SpamAssassin along with Sophos and McAfee antivirus to scan mails for malicious content. At last the mail is passed to the outgoing Exim process that finally delivers the mail to the exchange server on the LAN. The mail server does not have to be fast and disk space is not needed, because mail is forwarded to the mail server on LAN.
Placement	DMZ VLAN-2
Hardware	IBM X-330 dual 1.1 GHz with 2 x 18 GB disk RAID-1 (mirror)
Software	OS: Debian 3.0 GNU/Linux kernel 2.4.26 Applications: Exim-3.35-1woody3, Spam Assassin 2.64, MailScanner 4.32.5-1
Price	$2500

Web servers – DMZ

Purpose	• Serve HTTP and HTTPS traffic for customers, partners and suppliers of GIAC Enterprise
Details	There are 3 web servers in the DMZ of the GIAC Enterprise. They all run on the same hardware and software to make them easy to maintain. The web servers are also the face to the outside world and they have to present information fast and with high stability. Therefore it has been chosen to spend some extra resources on the hardware used for these servers. This means faster processors as well as using RAID-1 to get both speed and stability. The Apache 2.0 have received some heat for the new license introduced, so the GIAC Enterprise has chosen to stick with the 1.3 series to be on the safe side, also the 1.3 branch is considered more mature. The Web servers need fast processors to deliver web pages as fast as possible. Since dynamic web pages using PHP are implemented there can be some processing to generate the pages.
Placement	DMZ VLAN-1
Hardware	IBM X-335 dual 3.06 GHz with 2 x 18 GB disk RAID-1 (mirror)

Software	OS: Debian 3.0 GNU/Linux kernel 2.4.26 Applications: Apache 1.3.31
Price	$7000

SFTP servers – DMZ

Purpose	• Offer file servers to customers, suppliers and partners
Details	There are two SFTP servers in the DMZ of the GIAC Enterprise. It has been chosen to run two servers to physically separate the fortunes that are received from the suppliers and the fortunes that are sold to customers and partners. So one for incoming fortunes and one for outgoing fortunes. The SFTP servers need to be stable, but speed is not important, since the bandwidth of the Internet connection will be the limiting factor anyway.
Placement	DMZ VLAN-1
Hardware	IBM X-330 dual 1.1 GHz with 2 x 18 GB disk RAID-1
Software	OS: Debian 3.0 GNU/Linux kernel 2.4.26 Applications: SSH 3.4ps-1.woody
Price	$2500

Mail server - LAN

Purpose	• LAN users mailbox, address book and calendar • Send mail from LAN to the world
Details	The MS Exchange server is used for keeping the users mailboxes as well as for outgoing mail that are send from LAN.
Placement	LAN VLAN-3
Hardware	IBM X-330 dual 1.1 GHz with 2 x 73 GB disk RAID-1 (mirror)
Software	OS: Windows 2000 Server Applications: MS Exchange 2000 with SP3
Price	$2500

File server - LAN

Purpose	• Network drives of the users • Provide public transport folder where people can exchange files
Details	The file server contains the documents and files that the users wish to secure with a central backup each night. The file server is equipped with a local tape station for backup.

	The file server requires a large amount of space, but processor speed is not important, since it is just used to process file transfers.
Placement	LAN VLAN-3
Hardware	IBM X-335 dual 1.1 GHz with 5 x 73 GB disk RAID-5 (mirror)
Software	OS: Windows 2000 Server
Price	$6000

DNS server/Domain controller - LAN

Purpose	• Control the windows 2000 domain • Service DNS requests from the clients of the network • Contact Internet DNS as needed
Details	This server is the key server regarding the handling of the domain; it manages IP addresses using DHCP and serves all DNS requests on the LAN. Furthermore it controls authentication and authorization of domain members connected to the LAN.
Placement	LAN VLAN-3
Hardware	IBM X-330 dual 1.1 GHz with 2 x 73 GB disk RAID-1 (mirror)
Software	OS: Windows 2000 Server
Price	$2500

Design thoughts and defence-in-depth

Generally all sections of the network are protected with several layers of packet filtering and access control. All servers are both protected by the hardware solution in form of the F200 that provide a proprietary solution with automated update. The force of the F200 is that there are no underlying OS to attack and generally should a hardware solution be more stable and less error prone. Another advantage is the specialized design and optimization that allows real time scanning of both HTTP and SMTP traffic. The drawback of using a hardware box can be in case of a security breach. If there is a breach in the F200 there is not much the GIAC Enterprise can do, other than wait until Fortinet releases a security update.

The filtering router as well as the F200 likewise protects the LAN. Furthermore there is a NetFilter firewall in front of the LAN zone that protects the LAN from: The Internet, the DMZ servers should they be compromised, as well as the proxy server.

NetFilter is a nice supplement to the F200. The NetFilter firewall is a general purpose OS and in case of a security breach there might be possibilities to reconfigure or adjust certain

configurations. The downside of the OS based firewall is the added complexity of a general purpose OS leaves additional attack vectors if not hardened correctly. Also the software based NetFilter firewall has more moving parts including hard disk and fans. The combination of F200 and NetFilter leaves a lot of possibilities to still protect the network even if one technology should fail.

The filtering router and the F200 firewall protects the DMZ servers as a first and second layer of defence. The reverse proxy adds a third layer of defence and the host based NetFilter firewalls add a fourth layer. A structured approach is used to harden and configure all the DMZ servers that are all running Linux, as described in Operating system hardening on page 43.

The network is designed with a single point of entry, namely the F200, where access can effectively be shut off or restricted in the case of a breach.

In this assignment HA considerations are only touched lightly, since it is not the main purpose of the assignment, but of course important in an Internet business.

The SYSLOG server placed in the support zone is used as a central NTP server so all logs and events on the network are synchronized.

VLAN and security

The use of VLAN's should not be considered to be a secure way to segment the network. It is only segmented at the Data Link layer and this makes it possible to spoof the ARP protocol and defy the segmentation. It can however be a convenient way to use the switches to block worms and other malicious programs that potentially propagate through the network. Even if the VLAN segmentation is not enough to stop such malicious activity it might make it harder, and an intruder might be forced to make more noise on the network and thereby expose himself.

VLAN segmentation is not considered secure way to segment the network, but rather an extra obstacle for a potential intruder or worm, which might help invoke the IDS or other alarms. Adhering to the principles of Defence-in-Depth VLAN is a cheap and simple way to add another obstacle by configuration of switches.

For detailed explanation of the security issues and hardening of VLAN I would like to quote and refer to Cisco[2]:

[2] [CISCO1]

"The security of VLAN technology has proven to be far more reliable than its detractors had hoped for and only user misconfiguration or improper use of features have been pointed out as ways to undermine its robustness. The most serious mistake that a user can make is to underestimate the importance of the Data Link layer, and of VLANs in particular, in the sophisticated architecture of switched networks. It should not be forgotten that the OSI stack is only as robust as its weakest link, and that therefore an equal amount of attention should be paid to any of its layers so as to make sure that its entire structure is sound."

NIDS strategy

The Network IDS (NIDS) is placed at the entry/exit points of the different segments; LAN, DMZ and VPN traffic entering and leaving the network zones. The NIDS are placed behind the border firewall to avoid the noise of packets that are filtered anyway. The internal traffic on the LAN would require too much bandwidth and processing power to process real time. To protect the Servers located on LAN-VLAN3 in the network diagram host based IDS (HIDS) are used instead. The DMZ servers are also protected by HIDS as well as file integrity checks and host-based firewalls.

VPN strategy

The VPN is used for access to the local servers from the Internet. Only the IP addresses of selected servers are available for the VPN clients. This is configured in the firewall protecting the LAN. The key point is to restrict the access as much as possible. VPN to the LAN introduces a backdoor to the network. There is no need for VPN clients to access other clients on the network and therefore access has been limited to the servers. If files need to be transferred from a LAN client to a VPN client a shared transport folder on the file server can be used.

Further more there is excessive analysis of the traffic that enters through the VPN. A NIDS is used to monitor the traffic and the firewall logs all connections. There is also a traffic monitor called IPAUDIT[3] placed on the VPN interface to give alerts in case the amount or duration of traffic patterns is suspicious.

The PPTP tunnel can be attacked by a man-in-the-middle attack, so screening of incoming PPTP traffic is very important and resources should be spend on surveillance of this *Achilles heel*. This is the price for a cheap VPN solution that is NAT tolerant.

[3] [IPAUDIT]

Backup strategy

Since the budget is small, the backup is done on local tape stations at the central servers. This includes the exchange server and file server on LAN as well as the database server in the DMZ.

Improvements to be considered

To further secure the LAN all Internet and mail access could be achieved through a central Citrix server. This would ensure that the LAN was isolated physically from the Internet. The reason this solution has not been chosen is due to economic considerations. It is quite expensive to get a server that can serve all the employees of the GIAC Enterprise both in regards to software, hardware and consultancy. The GIAC Enterprise does not have a huge budget and focus have been on open source and Linux since there is in-house knowledge in this area.

For a high-availability setup, a hardware box could replace the reverse proxy server. That way the DMZ would only depend on devices without moving parts. Also a failover solution for the router could be considered with two separate ISP's using for example FWA for one line and cable for the other. This way GIAC Enterprise would not be sensitive to ISP failure or cables that are dug over.

Centralized backup solution using SAN or NAS would be preferable. It would be possible to let all servers boot of a central SAN network if the budget would allow it.

IP Addressing Scheme

In this setup GIAC Enterprise have been granted the address pool **217.128.15.128/255.255.255.224** by the ISP. This means that GIAC Enterprise controls 32 public Internet addresses, namely **217.128.15.128 – 217.128.15.159**.

The public network address is **217.128.15.128** and the public broadcast address is **217.128.15.159**
The remaining 30 addresses can be used freely to servers and components that need an external IP address directly on the Internet.

On the LAN and the DMZ RFC 1918[4] private addresses are used to avoid conflicts with the public Internet addresses. Because the GIAC Enterprise uses VLAN to separate different groups of computers the addressing scheme is build up so each VLAN can have

[4] [RFC-1918]

its own range of addresses. This makes it convenient to locate where a given address belongs.

In the GIAC Enterprise it is chosen to use the address space **172.16.0.0 – 172.31.255.255** (172.16/12 prefix) for the LAN zones. Each VLAN is assigned a unique second byte so we have for example 172.16.x.x for LAN-VLAN1, 172.17.x.x for LAN-VLAN2, 172.18.x.x for LAN-VLAN3 and so forth. This gives possible 16 VLAN zones with a maximum of 65535 IP addresses in each zone. Considering the size of the GIAC Enterprise 16 possible LAN zones should be more than enough, and there are plenty of addresses to expand in each zone.

For the DMZ zones the address space chosen is **192.168.0.0 – 192.168.255.255** (192.168/16 prefix). The third byte is used to enumerate the DMZ-VLAN zone; so DMZ-VLAN1 is named 192.168.1.x and DMZ-VLAN2 is named 192.168.2.x and so forth. This gives us a maximum of 255 DMZ zones with up to 255 IP addresses in each zone. Since it is primarily servers that are placed in the DMZ zones this should be plenty.

For the VPN gateway, the support network and the DMZ zone outbound traffic is not allowed the RFC 1918 address space **10.0.0.0/8** is used.

The interface with encrypted traffic belongs to the network 10.254.254.0/30 and the interface with unencrypted traffic belongs to the network 10.253.253.0/30. This only leaves 4 addresses in each zone and that is just 1 for the firewall 1 for the VPN gateway, a network address and a broadcast address. No other devices should be connected to the VPN legs of the firewall. The NIDS does not have an IP address since it is just connected to the unencrypted leg with a network card in promiscuous mode. If there should be VPN implemented later there are plenty of address space left to make other zones.

One might wonder why it was chosen to go through the trouble of defining such a complicated address scheme, the main ideas are:

- It is easy to see where a given address belongs, and it can be isolated down to the exact VLAN without going to big trouble.
- DMZ and LAN addresses are easy to differentiate which is important in a security perspective.
- Subnets are selected, so there are plenty of room for expansion both in regards to new zones and the number of hosts.

Here follows detailed tables of the address assignment scheme for the whole GIAC Enterprise. There are also columns (**Incoming Traffic** and **Outgoing Traffic**) describing the traffic going in and out of the zones. This is not to be seen as the exact ports that have

to be open in the firewall, but just an overview of which services are offered/used by a given server/zone. Consider HTTP traffic for example; it is noted that the LAN-VLAN1 has to use outgoing HTTP traffic, but it is actually the proxy server that the hosts from LAN-VLAN1 uses that need the access, since that is the only host that exchange HTTP data with the Internet. Also it is only traffic relevant to the Internet, there are other flows internally. The following tables show what the GIAC Enterprise looks like from the outside.

WAN Addresses (217.128.15.128 – 217.128.15.159)

Address	Description	Incoming Traffic	Outgoing Traffic
217.128.15.128	External IP address of the router		
217.128.15.129	Border gateway router internal IP address. Also the default gateway used by the F200 firewall.		
217.128.15.130	Firewall border (F200) – External interface.		
217.128.15.131	Partner/customers SFTP server	SFTP	
217.128.15.132	Suppliers SFTP server	SFTP	
217.128.15.133	Primary public web site (http://www.giac-enterprise.com)	HTTP	
217.128.15.134	Customer web site (https://customer.giac-enterprise.com)	HTTPS	
217.128.15.135	Partner web site (https://partner.giac-enterprise.com)	HTTPS	
217.128.15.136	Incoming mail server	SMTP	
217.128.15.137	Firewall LAN	PPTP	
217.128.15.138 - 217.128.15.158	Free for future use		
217.128.15.159	Broadcast address		

DMZ addresses (192.168.0.0 – 192.168.255.255)

The DMZ contains the public accessible servers of the GIAC Enterprise

Address	Description	Incoming Traffic	Outgoing Traffic
192.168.1.x	DMZ-VLAN1 – Public server	HTTP SFTP	

		HTTPS	
192.168.2.x	DMZ-VLAN2 – Incoming mail server	SMTP	SMTP t

LAN addresses (172.16.0.0 – 172.31.255.255)

The LAN addresses covers that address space for the different VLAN zones. There are 3 zones namely the

Address	Description	Incoming Traffic	Outgoing Traffic
172.16.x.x	LAN-VLAN1 – Network of the GIAC Enterprise employees		HTTP HTTPS FTP SMTP
172.17.x.x	LAN-VLAN2 – Network of the GIAC Enterprise mobile users		HTTP HTTPS FTP SMTP
172.18.x.x	LAN-VLAN3 – Network of the LAN servers	SMTP Decrypted VPN traffic to the servers	SMTP DNS NTP

VPN addresses (10.254.254.0/30 and 10.253.253.0/30)

The concept of incoming and outgoing depends on the point of view. In this case it is the point of view of the firewall. This means that PPTP traffic to the encrypted leg of the firewall is send towards the PoPTop server and therefore denoted outgoing, whereas decrypted traffic are received from the PoPTop and is viewed as incoming.

Address	Description	Incoming Traffic	Outgoing Traffic
10.254.254.0/30	LAN-VPN1 – Encrypted traffic		PPTP GRE
10.253.253.0/30	LAN-VPN1 – Unencrypted traffic	Traffic to the LAN servers	

Assignment 2 – Security Policy and Component Configuration

This chapter concerns four central components of the GIAC Enterprise network

1. Cisco 2611 Border router.
2. Fortigate 200 (F200) firewall from Fortinet.
3. The NetFilter firewall protecting the LAN.
4. The PoPTop PPTP server.

The configuration is described in details. Simple one line explanation or comment is done in the scripts using comments, while longer sentences explaining details of the scripts, are put in between the sections of the scripts.

Border router

The border router is a Cisco 2611. Filtering provided by the router has to be considered. The network has to be flexible; consider if there is a need to open a TCP port to a server, then it is not convenient if it is necessary to both configure the firewall and the router. Therefore the router is only used for general purpose filtering – traffic that should never occur. This way the router will seldom need to be reconfigured and it is not necessary to buy expensive Cisco specific configuration consoles and other add-ons to ease the task.

Cisco routers are a well documented subject on the Internet, some of the resources I have been inspired by and find useful include:

- [CISCO3]
- [CISCO4]

Basic configuration of a Cisco router

The basic configuration consists of the configuration that is needed in order to make the router functional. This includes assigning IP numbers and activating the interfaces.

Everything following the "!" is a comment. This means that the code configuration blocks given in the following can be pasted directly into the router in configuration mode to make the configuration described.

To log into the router at first a serial cable is used. Once connected to the serial port the configuration can begin.

enter administration mode:

```
>enable
```
followed by user name and password. Enter terminal configuration mode:
```
$conf t
```

First of all we configure the interfaces with IP addresses:

```
! configuring the internal interface and assign an access group
!
interface Ethernet0/0
 ip address 217.128.15.128 255.255.255.224
 ip access-group 110 in
 no ip directed-broadcast
!
!configuring the serial connection
!
interface Serial0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 Shutdown
 no fair-queue
!
! configuring the external interface and assigning an access group
!
interface Ethernet0/1
 ip address 217.128.15.129 255.255.255.224
 ip access-group 150 in
 no ip directed-broadcast
```

Notice the access groups being assigned; they define the filters that the router enforces. The access lists are configured in the next section. The access lists has to be defined before they can be assigned to an interface, so it is actually done in the reverse order here, because it seems easier to explain that way.

Packet filtering with a Cisco router

Since the router is designed for packet filtering and can do it very fast, it is reasonable to do general purpose filtering at the border router. This way malicious packages that are spoofed with illegal IP addresses never enter the GIAC Enterprise network and the firewalls and VPN gateways are spared the processing of malicious and erroneous IP packages.

Here is the ingress filter used by GIAC Enterprise for their border router:

```
! deny rfc-1918 private addresses
!
access-list 110 deny     ip 192.168.0.0 0.0.255.255    any
access-list 110 deny     ip 172.16.0.0  0.15.255.255   any
access-list 110 deny     ip 10.0.0.0    0.255.255.255  any
! deny localhost and multicast as source address
access-list 110 deny     ip 127.0.0.0   0.255.255.255  any
access-list 110 deny     ip 255.0.0.0   0.255.255.255  any
! prevent spoofing of our own address space
access-list 110 deny     ip 217.128.15.128 0.0.0.31         any
! control ICMP: http://www.iana.org/assignments/icmp-parameters
! allow echo-reply
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 0
! allow dst ureachable
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 3
! allow source quench
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 4
! allow echo
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 8
! allow host-unreachable
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 3 1
! allow port-unreachable
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 3 3
! allow packet-too-big
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 3 4
! allow administratively-prohibited
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 3 13
! allow ttl-exceeded
access-list 110 permit icmp any 217.128.15.128 0.0.0.31 11 0
! deny all other explicitly
access-list 110 deny icmp any any
```

It has been chosen not to log packets on the external interface, because of the lack of resources to investigate possible offenders and malicious packets received from the Internet anyway.

The egress filter is both provided to make GIAC Enterprise a good Internet neighbour and also to provide some degree of IDS, since there are certain general packet characteristics that should not appear from the inside of the GIAC Enterprise network.

```
! only allow GIAC Enterprise addresses as source
access-list 150 permit ip 217.128.15.128 0.0.0.31 any
! deny and log all others
access-list 150 deny ip any any log
```

Hardening of a Cisco router

After the configuration of the router it is important to ensure that it is hardened so known flaws and default configurations are not going to make the router itself vulnerable to attacks. The hardening process was inspired by [CISCO2] and [MCINTOSH].

Different features are turned off; this includes IP packages that can be used to gain information about the network as well as the Cisco discovery protocol.

```
Interface Ethernet 0/0
 no ip unreachables
 no ip redirect
 no ip directed-broadcast
 no ip mask-reply
 no ip proxy-arp
 no cdp enable

Interface Ethernet 0/1
 no ip unreachables
 no ip redirect
 no ip directed-broadcast
 no ip mask-reply
 no ip proxy-arp
 no cdp enable
```

All the unnecessary services are turned off.

```
! do not allow other routers to boot from this router
no ip bootp server
! no configuration by http
no ip http server
! no configuration by https
no ip http secure-server
! SNMP service is turned off
no snmp-server
```

```
! disable services not necessary (e.g. chargen and discard)
no tcp-small-servers
! disable services not necessary (e.g. chargen and discard)
no udp-small-servers
! remove finger protocol that tells who is logged in
no ip finger
! cisco router discovery protocol is disabled
no cdp run
! disallow the router to load remote configuration on boot up
no service config
no boot network
! no DNS requests from the router
no ip domain lookup
! X.25 service that is not needed
no service pad
! we don't want source routing!
no ip source-route
```

The password should not be readable from a dump of the configuration file, and it should be encrypted. Even though the encryption used is not industrial strength, it does prevent preying eyes from spotting it.

```
service password-encryption
no enable password
enable secret 5 $!#VeRySeCrEtPaSsWoRd$!#
```

Access

All data pass through the router and the rules are generally speaking very static. The router should only be updated if for example the IP range of the GIAC Enterprise is changed. The stateful inspection and content filtering is done by other components. There is no access policies build into the border gateway router; its only purpose is to rule out and filter malformed packages that should never occur on the network.

Fortigate firewall

The border gateway firewall is a Fortigate-200 (F200) placed directly behind the router. The primary objective of the F200 is to manage the external IP addresses, schedule availability of certain services and do real time scanning of traffic. Further more it is to be used to terminate IPSEC connections from subsidiaries in the future. It has a well-written manual and I will not spend space and time on showing all possible configuration options, but just show selected screenshots of the primary windows that are used to configure it for GIAC Enterprise to illustrate the configuration process.

Configuration

The following screenshots show the overall configuration of the F200 this includes:

1. Interface overview
2. External addresses
3. Policy setup
4. Network Intrusion Detection System (NIDS) Configuration
5. Anti virus configuration
6. IPSEC Phase 1
7. IPSEC Phase 2

Figure 6 – Interface Overview

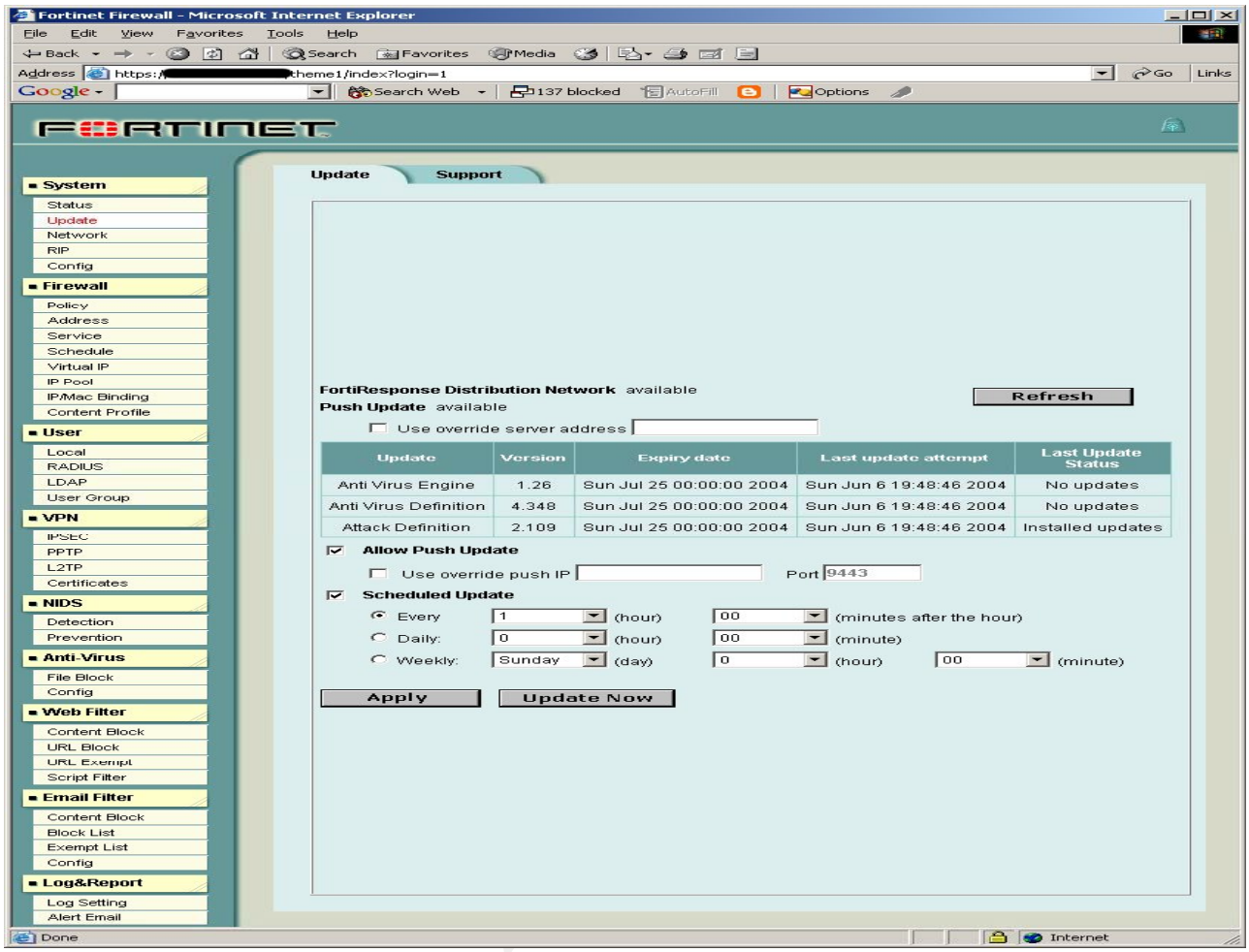


Figure 6 – Interface Overview shows a screenshot of the Fortigate user interface. The selected menu displays the status of the box and the status of the attack definitions.

The left menu bar shows all the menu items available in a Fortigate firewall. The screen shots presented here are actually taken from a Fortigate-50A but you cannot tell because the interface for all their firewall products is similar. The screenshots used in this paper are only the general ones included in all the Fortigate firewall products. This is a nice feature, if GIAC Enterprise should decide to upgrade the box it is just necessary to unplug the cables from the box and attach a larger model. There is also an export/import function included in the Fortigate firewalls that allows administrators to dump and restore the configuration.

Figure 7 – External Addresses

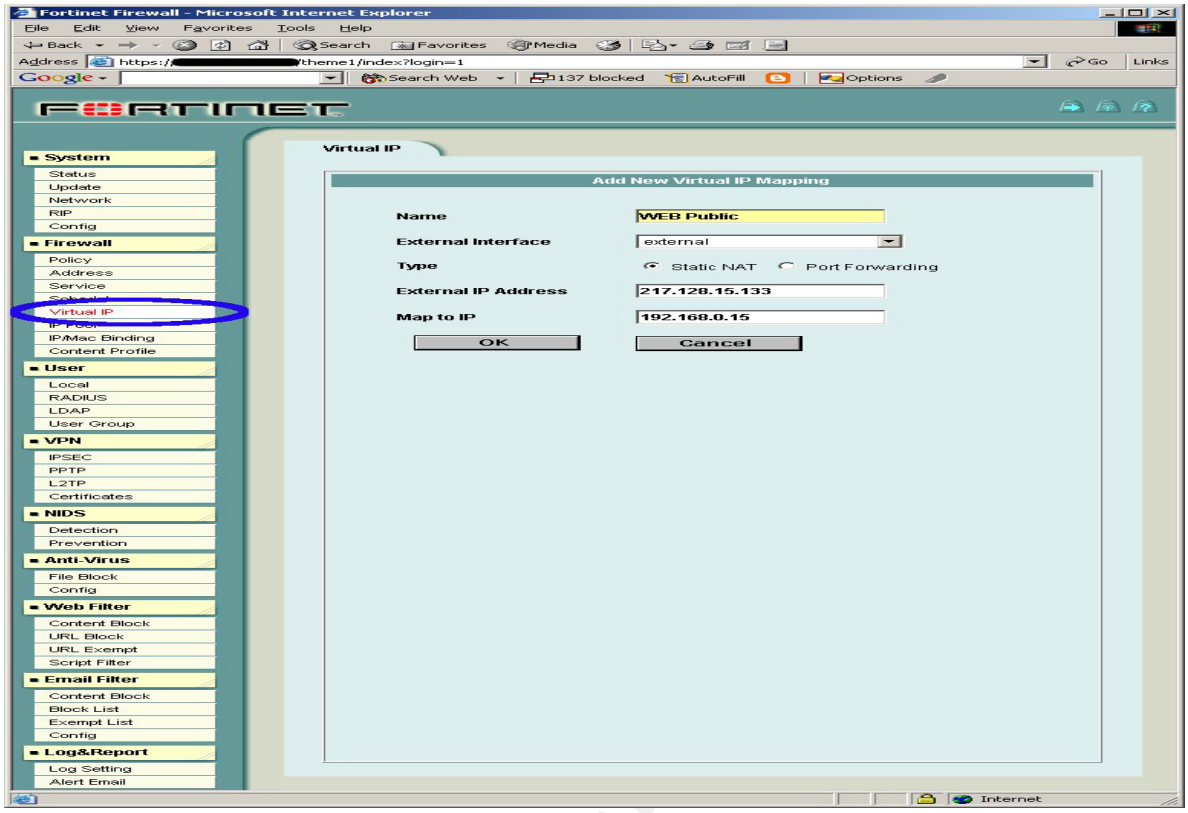


Figure 7 – External Addresses is a screenshot where an external virtual IP address is configured. Virtual IP addresses are used when the traffic for that address actually is NAT to another host.

The traffic analysis of the GIAC Enterprise shows that the web servers are the ones primarily utilizing the Internet connection. Therefore the rules for the web servers are put first in the F200 rule set. They are followed by the rules for the LAN segment and the NetFilter firewall and finally the rules for the mail server are listed.

The F200 is configured to manage all the external IP addresses of the GIAC Enterprise. This makes it easy to modify or redirect IP addresses by the use of a web interface. For less technical persons this might be a better solution than using `vi` in a remote SSH session. (Of course less technical persons should not be configuring our firewall ;-). The web interface has the advantage that it is less prone to configuration errors, since the dropdown menus only contain valid values inherited from other configuration windows.

Figure 8 – Policy Setup

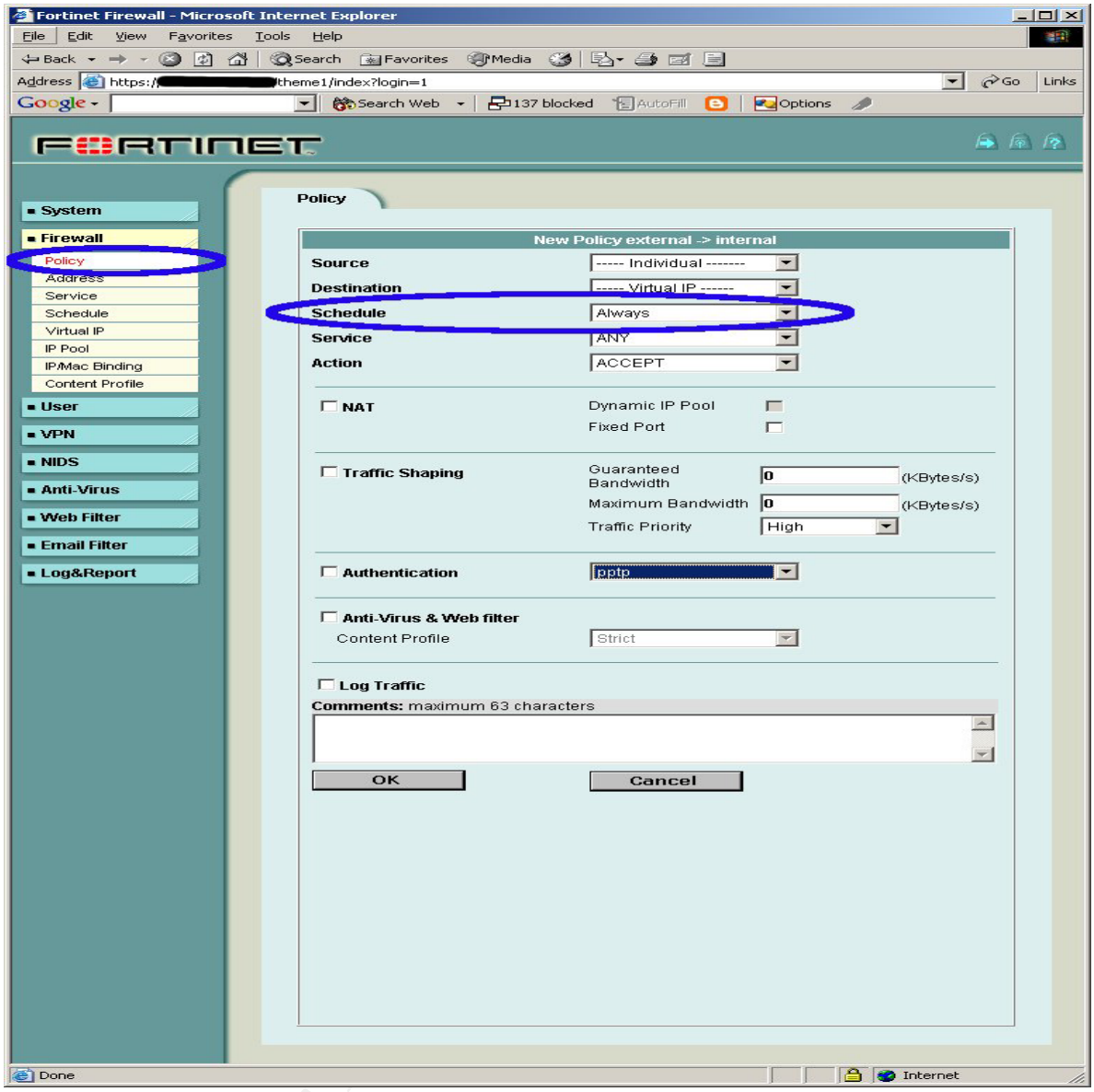


Figure 8 – Policy Setup shows a policy configuration. The policy includes NAT configuration and another very useful feature is the Schedule (circled out). This feature will be used by the GIAC Enterprise to restrict PPTP connections to the opening hours when there are capable administrators overlooking network traffic.

Figure 9 - NIDS Configuration

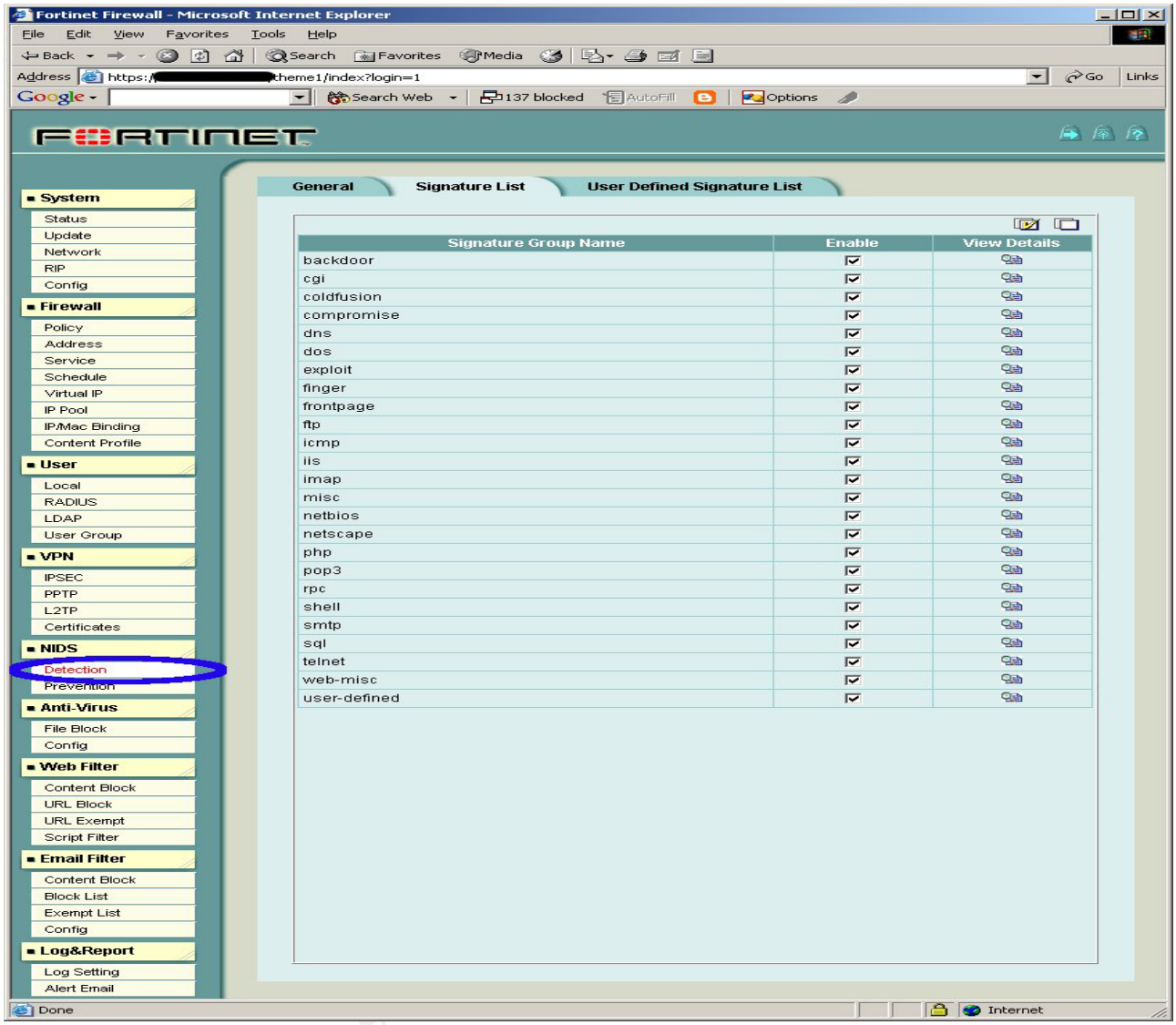


Figure 9 - NIDS Configuration shows the NIDS configuration is simple and it is not clear how updated and effective it is. It might be a mistake to blindly trust the F200. GIAC Enterprise uses the F200 NIDS as a supplement to the Snort probes on the network. Snort has a large community that produce rules and are a proven technology in the area of intrusion detection.

Figure 10 – Anti Virus Configuration

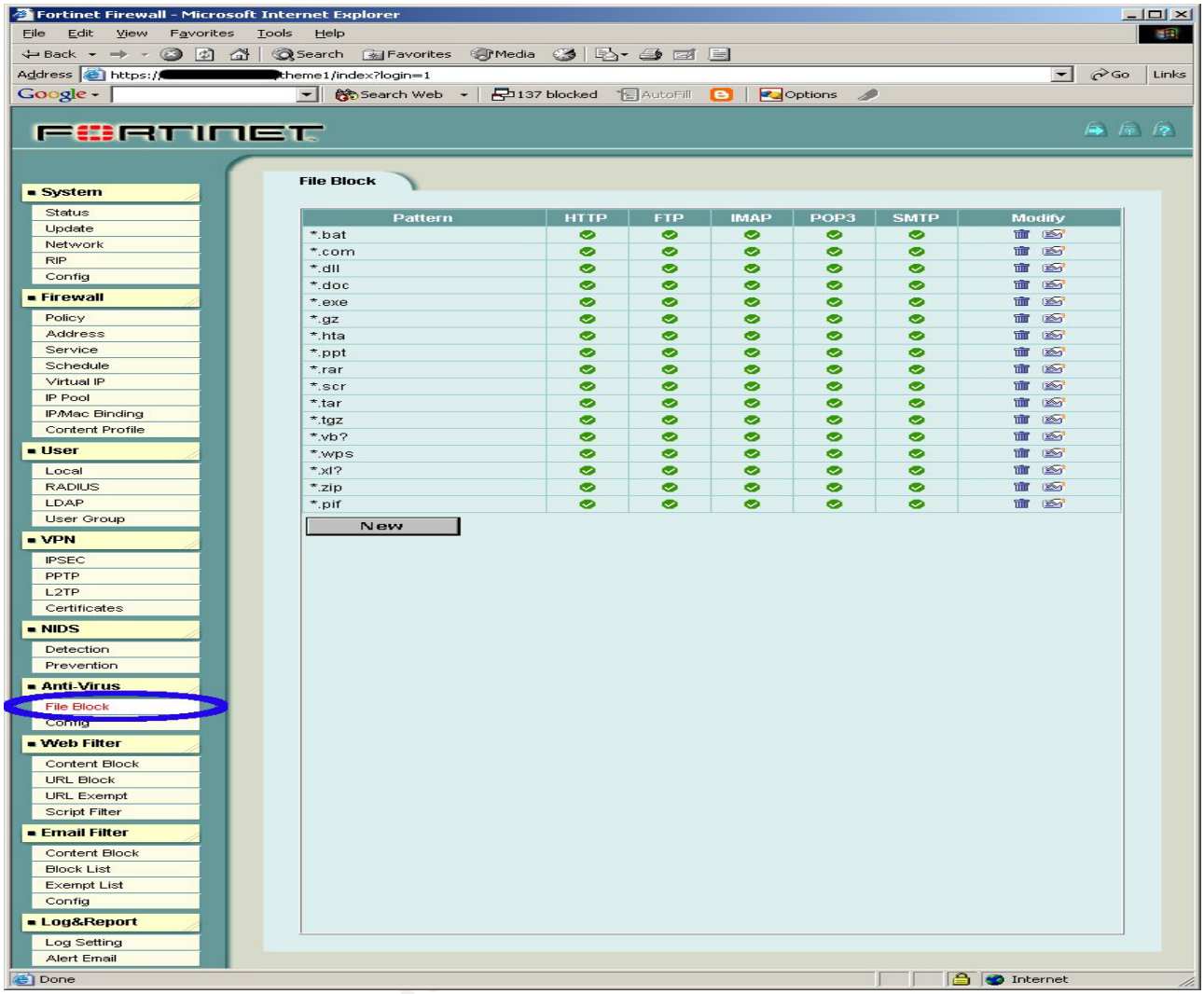


Figure 10 – Anti Virus Configuration shows the virus scanner configuration window. Like the NIDS, the AV part of the Fortigate is used as a supplement to the other virus scanners running on the clients and servers connected to the network. I have chosen not to show screen shots for the web filter and email filter but they are pretty similar. On the mail relay server MailScanner is used combined with several virus filters from several vendors as well. The real time web filter scanning is useful, and a nice supplement to the ACL's on the proxy servers.

Figure 11 - IPSEC Phase 1

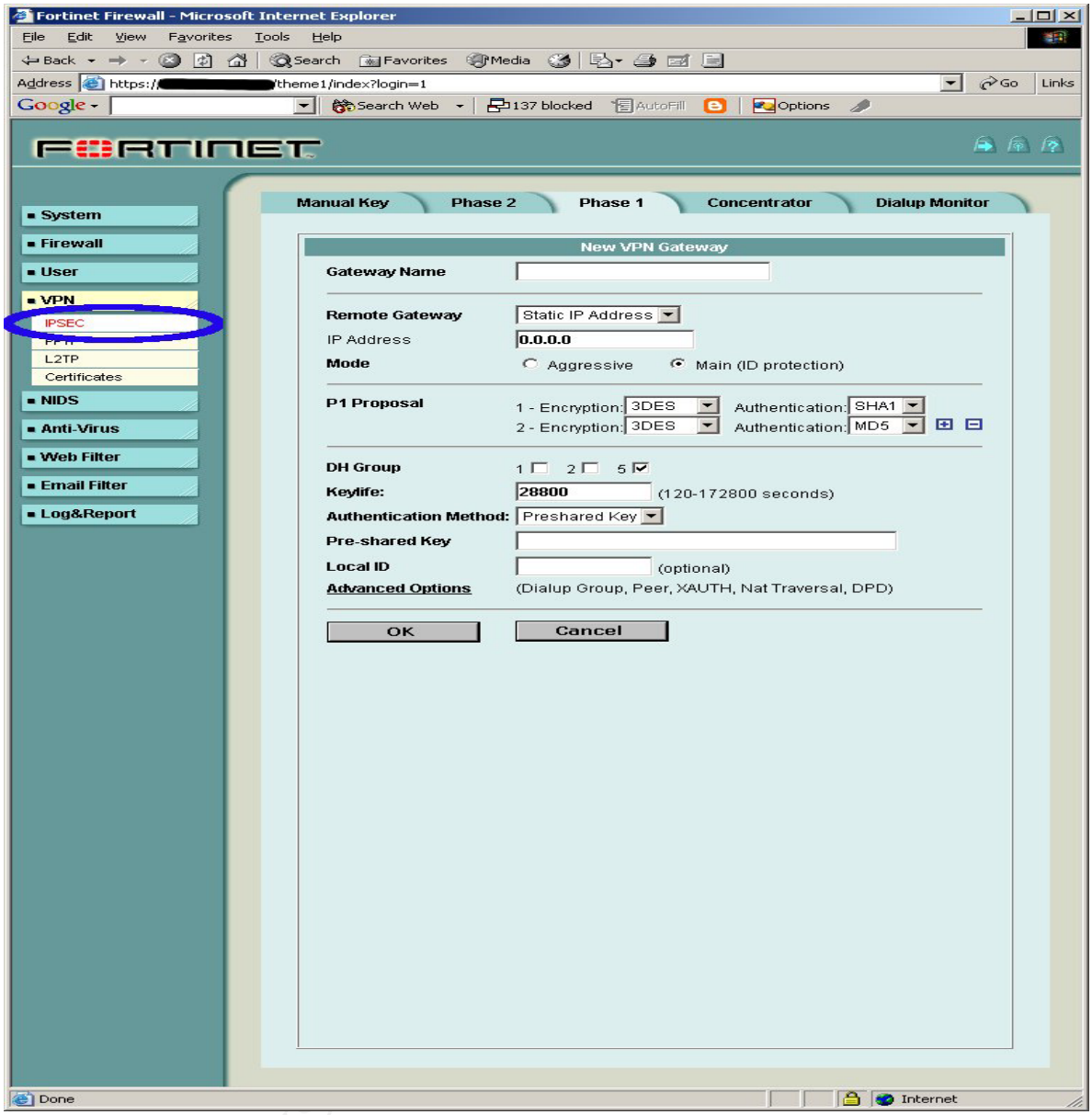


Figure 11 - IPSEC Phase 1 Shows the configuration of IPSEC phase 1 the IKE. This configuration is not used yet. But it makes it fairly easy to setup an IPSEC gateway at the perimeter of the GIAC Enterprise so subsidiaries can be interconnected with the HQ.

Figure 12 - IPSEC Phase 2

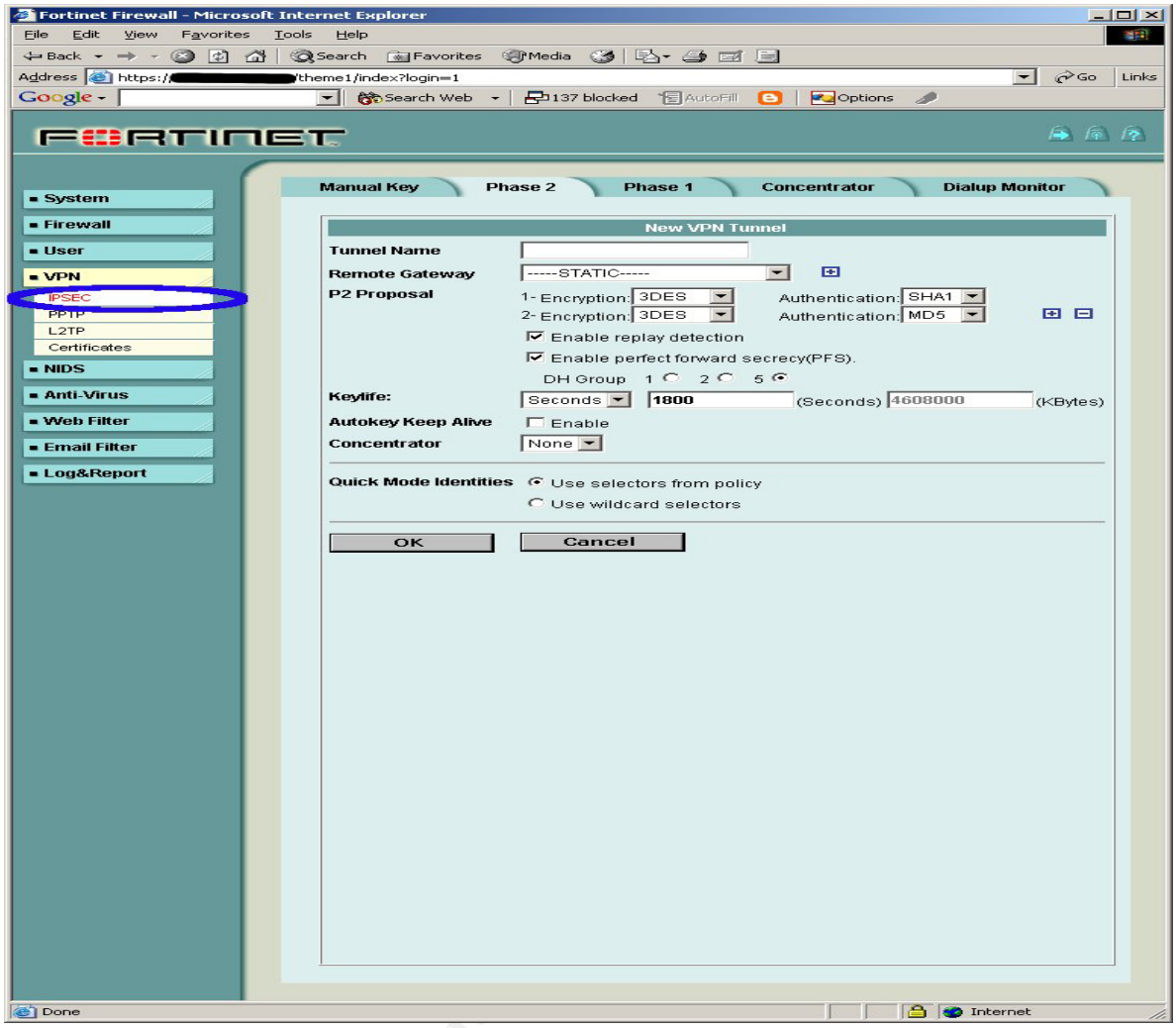


Figure 12 - IPSEC Phase 2 shows the configuration of the IPSEC tunnel that can be used for the encrypted traffic.

This concludes the configuration of the GIAC Enterprise F200 firewall.

The F200 has several other options that are not used by GIAC Enterprise yet. It is a nice and intuitive interface to setup. In the next section the configuration of NetFilter (firewall-LAN) is demonstrated.

NetFilter LAN firewall

NetFilter was chosen because it is fast, reliable, cheap (its free ;-) and secure if configured properly. It does stateful inspection for numerous protocols and it's a proven technology with a large community behind it. The structure of NetFilter makes it extremely flexible and customizable, these attributes are preferable in the LAN firewall.

Operating system hardening

Hardening of a software firewall is a project where all components of the firewall have to be analyzed. NetFilter is not a standalone hardware box running on a dedicated operating system, but it is a piece of code that can be compiled in to the Linux kernel. This means that even if NetFilter is stable and secure it also depends on the general-purpose Linux kernel to be stable and secure. NetFilter is compiled into the Linux kernel, so it can filter IP packages before they enter the application memory space and thereby are accessible for applications running on the Linux box.

The GIAC Enterprise has chosen to run the primary firewall on a Debian 3.0 (Woody) Linux distribution. Debian can be installed as a truly vendor independent Linux distribution, since one have the option to avoid applications and libraries that are non-free and/or non-open source during the installation. Also the security history of Debian is promising, the Debian project is always in front when releasing updates/patches and it has been a very stable distribution for many years. Another great feature of Debian in a security context is the possibility to make a very stripped down base installation with nothing more than the kernel and the most basic tools, like `more, vi` and a few others ;-).

The more responsive the firewall is the to packages and protocols the more possible vulnerabilities. Every interaction with the firewall is a future possible attack vector to exploit a bug or reveal information about vulnerable systems, so the art is to open up the firewall just enough to be useful. The firewall should not do anything besides packet filtering and stateful inspection.

In this chapter I will look at the overall aspects and possibilities of hardening Linux. A complete guide for Linux hardening is beyond the scope of this document, but I have supplied a number of resources that are relevant in this context.

The overall procedures of hardening the GNU/Linux firewalls include hardening the kernel, securing the configuration and securing programs and utilities.

Secure the kernel
Linux offers loadable module support and that can come in handy when you have a dynamic system, where you want to add and remove functionality. But when it comes to a firewall the loadable module functionality is discouraged. Imagine a hacker being able to load modules and thereby modify the kernel itself in run time - that is a scary scenario. Fortunately the loadable module support can be disabled, and the result is a monolithic kernel that cannot be modified without recompiling it.

Strip down the kernel and remove anything that is not needed. Consider if loadable module support is really needed, if it is not needed a monolithic kernel is preferable in regards of security. Patch the kernel appropriately and only with the stable and well tested patches. See appendixKernel compilation – the Debian way on page 97 for details on compiling the Kernel with Debian.

Patch the kernel with LIDS and make restrictions – even for root.

Two very useful things that LIDS can help with are:

- Ensure that only applications and programs with the right set of permissions can be executed. This ensures that programs that have wrong permissions and might have been exploited or modified will not be executed. This is known as Trusted Path Execution (TPE)
- Restrict applications and child processes access to the network. LIDS can restrict network access for applications. An example could be to deny the Apache server the right to create new network sockets, which can stop a worm from propagating.

Example of commands to do TPE for `/sbin` and `/lib`[5]:

```
$lidsconf –A -o /sbin –j READONLY
$lidsconf –A –o /lib –j READONLY
```

These commands will ensure that commands in `/sbin` can only be executed if their permission is set to READONLY. Also the files in the library files `/lib` need the correct permission. If an executable is using a library they both need to be READONLY for the execution to take place.

Another way to secure the kernel is to make it harder for a potential black hat to identify which operating system and kernel version that is running on the server. This can be done

[5] [LIDS]

by for example changing the TTL value of packets and other values that typically are OS/kernel specific.

The patch tcp-window-tracking from the IPTABLES patch-o-matic package adds the following functionality to the kernel – I quote[6]:

> *"This patch adds, among other things, all of the above timeouts to special sysctl variables, which means that they can be changed on the fly, while the system is still running. Hence, this makes it unnecessary to recompile the kernel every time you want to change the timeouts. These can be altered via using specific system calls available in the /proc/sys/net/ipv4/netfilter directory. You should in particular look at the /proc/sys/net/ipv4/netfilter/ip_ct_* variables"*

Some useful resources for securing the kernel of Linux in general includes:

- [TLDP1]
- [OPENWALL]
- [LIDS1]
- [IMMUNIX]
- [LINSEC]

Secure the applications and configuration
It should be considered who is allowed to do what on the system and from where. Default settings and configuration files might not be appropriate.

Hardening of Linux:

- [BASTILLE]
- [LINSEC]

Remove unnecessary programs and utilities. Patch all programs and utilities appropriately. Review important security lists regularly and make sure to obtain new patches and updates when necessary. For Debian there is a package called HARDEN, which can be used to identify and remove insecure packages and do remote auditing.

Some important resources for threats and security holes include:

- [TLDP]
- [USCERT]
- [SANS]

[6] [IPT2]

- [SECFOC]
- [BUGTRAQ]

Secure the integrity
The integrity of the server is very important in a software-based firewall running on a general purpose OS.

Root-kits typically try to replace or alter system commands in the /bin or /sbin directory. This way the attacker can maintain access to the system.

Use exclude to check everything except the files that are explicitly excluded. The primary goal of the integrity check is to insure that the commands and binaries are not modified.

The GIAC Enterprise has chosen to utilize INTEGRIT[7] as the file integrity verification program. Once the signatures for the firewall are completed they are protected with the use of LIDS. Another even more secure solution would be to burn the initial signatures on a CD-ROM so it would be physically impossible to modify them.

When the operating system is hardened and all unnecessary services are shutdown and all unnecessary applications have been uninstalled it is time to setup and harden the firewall configuration, which means its time to configure NetFilter.

NetFilter configuration

NetFilter is build up of tables and chains. There are three tables:

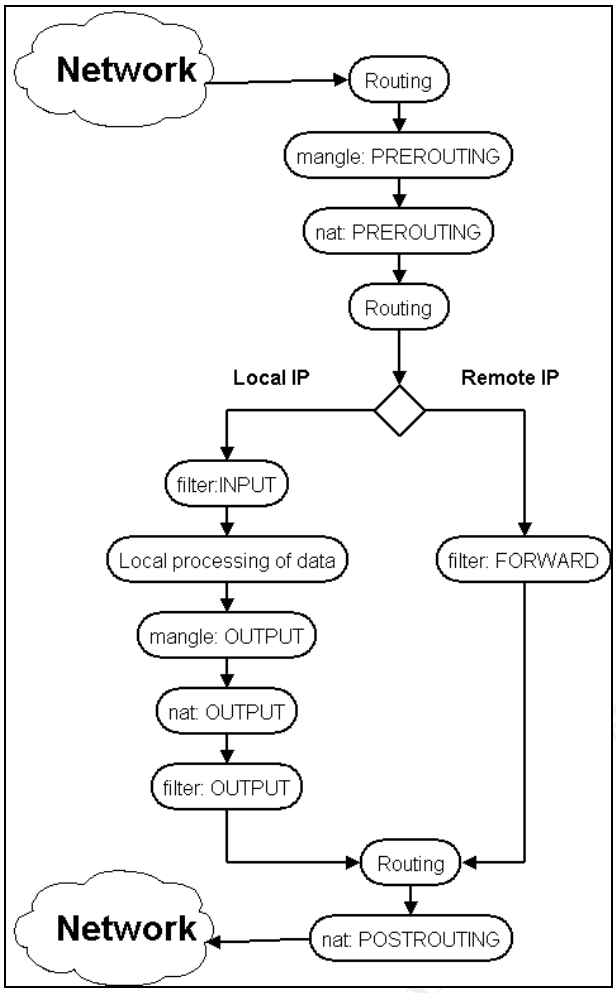
1. mangle – Is used to modify the packets that traverse the firewall. This is typically used in conjunction with traffic shaping and QoS. The mangle table has the chains PREROUTING, OUTPUT and is not used in this configuration.
2. nat – Network address translation can be done for a number of reasons, common usage is masquerading and port forwarding. The nat table has the build-in chains PREROUTING, OUTPUT and POSTROUTING.
3. filter – Is used to do the actual stateful filtering of packets. The filter table has the build-in chains INPUT, OUTPUT and FORWARD.

New packets entering the firewall can originate from two sources; either it arrives from the network by one of the interfaces in the firewall or it is generated by a local process running on the firewall.

[7] [INTEGRIT]

Figure 13 - Netfilter shows how the packets are handled by the firewall. All packets whether for the firewall or not, are send through the mangle, nat and filte tables – in that order.

Figure 13 - Netfilter[8]



It is possible to add user supplied chains in addition to the ones build in. For further information on NetFilter see the homepage (www.netfilter.org) where the inner workings of NetFilter as well as a lot of user guides and *howto*'s can be found.

To setup NetFilter a configuration file is build from scratch. The configuration file is actually just a batch script corresponding to a .bat or .cmd file known from windows. It means that it

[8] [IPT1]

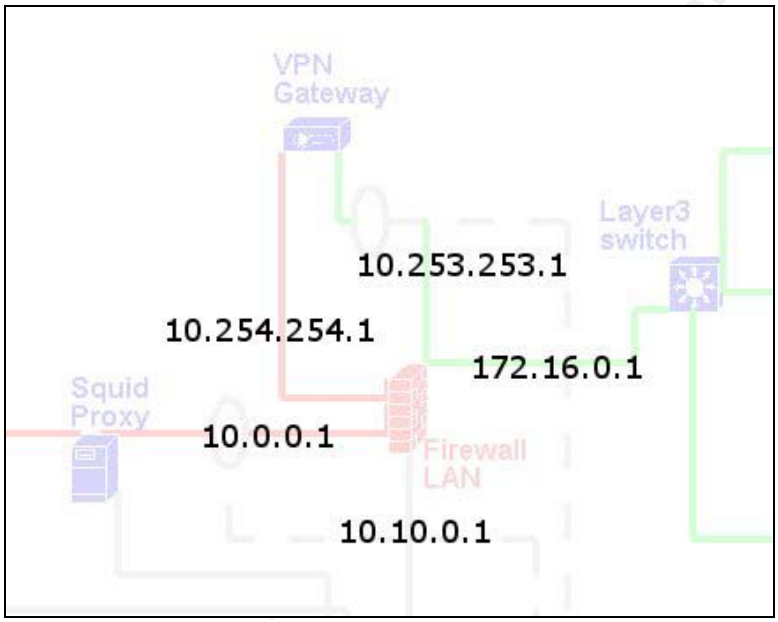
is just a list of commands that get executed and might as well have been entered on the command line, but it is easier to keep the overview in a file containing the command list. The file is also a good place to add comments so others can review the firewall rules easier.

The firewall contains 5 network interfaces and is therefore referred to as a 5 legged firewall. Figure 14 - IP addresses of the LAN firewall shows a close up of the firewall and the 5 legs. The IP addresses of the legs are written so they cross the leg they belong to.

The 5 interfaces are:

- Eth0 (10.0.0.1/24) - the network between Fortigate and NetFilter firewall.
- Eth1 (10.254.254.1/30) – the network between the VPN gateway and the firewall (encrypted)
- Eth2 (10.253.253.1/30) – the network interface between the VPN gateway and the firewall (unencrypted)
- Eth3 (172.16.0.1/12) – the network interface on the LAN leg.
- Eth4 (10.10.0.1/24) – the network interface on the support LAN.

Figure 14 - IP addresses of the LAN firewall



In the following I will run through the primary parts of the firewall-LAN script and add comments as needed. The general comments have been included in the script, so documentation can be found right were it is needed.

The initial part of the script defines the constants, networks and configures the interfaces:

```
#!/bin/bash

# GIAC Enterprise
# DMZ IPTABLES configuration script

#------------------ CONSTANTS ----------------------#
/bin/echo "CONSTANTS"

IPT="/sbin/iptables"            # location of iptables

IF_WAN="eth0"                   # WAN interface
IF_LAN="eth1"                   # LAN interface
IF_VPN_CRYPT="eth2"             # PPTP inbound interface
IF_VPN_PLAIN="eth3"             # PPTP outbound interface
IF_SUP="eth4"                   # Support zone interface

#----------------- IP ADDRESSES ----------------------------#
/bin/echo "IP ADDRESSES"

ANYWHERE="0.0.0.0/0"
BC_SRC="0.0.0.0"                # Broadcast source address
BC_DST="255.255.255.255"        # Broadcast destination address
CLASS_A="10.0.0.0/8"
CLASS_B="172.16.0.0/12"
CLASS_C="192.168.0.0/16"
CLASS_D_MULTICAST="224.0.0.0/4"
CLASS_E_RESERVED_NET="240.0.0.0/5"
```

Assign IP addresses to the interfaces based on how the interfaces are configured.

```
# determine the ip addresses assigned with the interfaces
# this is done automatically through shell script
IP_WAN=`ifconfig $IF_WAN | grep "inet addr" | \
        cut -f 2 -d ":" | cut -f 1 -d " "`

IP_LAN=`ifconfig $IF_LAN | grep "inet addr" | \
        cut -f 2 -d ":" | cut -f 1 -d " "`
```

```
IP_VPN_CRYPT=`ifconfig $IF_VPN_CRYPT | grep "inet addr" | \
        cut -f 2 -d ":" | cut –f 1 -d " "`

IP_VPN_PLAIN=`ifconfig $IF_VPN_PLAIN | grep "inet addr" | \
        cut -f 2 -d ":" | cut –f 1 -d " "`

IP_SUP=`ifconfig $IF_SUP | grep "inet addr" | \
        cut -f 2 -d ":" | cut -f 1 -d " "`

# print error if ip address assignment fail
if [ "x$IP_WAN" == "x" ]; then
        echo "Error: IP WAN missing ..."
        exit 0
Fi
if [ "x$IP_LAN" == "x" ]; then
        echo "Error: IP LAN missing ..."
        exit 0
Fi
if [ "x$IP_VPN_CRYPT" == "x" ]; then
        echo "Error: IP VPN PLAIN missing ..."
        exit 0
Fi
if [ "x$IP_VPN_PLAIN" == "x" ]; then
        echo "Error: IP VPN PLAIN missing ..."
        exit 0
Fi

if [ "x$IP_SUP" == "x" ]; then
        echo "Error: IP SUPPORT missing ..."
        exit 0
fi
```

Define the IP addresses that are hard coded into the firewall.

```
GATEWAY="172.16.0.1" # IP address of the firewalls gateway

# define the IP addresses of the VPN gateway
# this is the addresses of the linux box running PoPTop
IP_PPTP_CRYPT="10.254.254.1"
IP_PPTP_PLAIN="10.253.253.1"
# define IP ranges for the hosts on the network
LAN_SERVER_RANGE="172.30.0.0/16"
```

```
LAN_CLIENT1_RANGE="172.16.0.0/16"
LAN_CLIENT1_TCP_PORTS="21 23 53 80 443"
LAN_CLIENT1_UDP_PORTS=""
LAN_CLIENT2_RANGE="172.17.0.0/16"
LAN_CLIENT2_TCP_PORTS="21 23 53 80 443"
LAN_CLIENT2_UDP_PORTS=""
# define the servers IP addresses
LAN_DNS_SERVER="172.30.0.10"
LAN_MAIL_SERVER="172.30.0.20"

RELAY_SERVER_MAC=""
RELAY_SERVER_IP="10.0.0.10"

PROXY="10.0.0.20"
```

The next section is the configuration of the firewall including kernel parameters and modules that should be loaded upon start up of the firewall.

```
#----------------- LOG LEVEL ---------------------------------#
/bin/echo "LOG LEVEL"

LOG_LEVEL=5

#---------------- MODULES -------------------------------------#
/bin/echo "MODULES"

modprobe ip_nat_ftp
modprobe ip_conntrack_ftp

#----------------CONFIGURING KERNEL-----------------------------#
/bin/echo "CONFIGURING KERNEL"

/bin/echo "1" > /proc/sys/net/ipv4/tcp_syncookies

# Disable response to ping
/bin/echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all

# Disable response to broadcasts
/bin/echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

# Don't accept source routed packets
/bin/echo "0" > /proc/sys/net/ipv4/conf/all/accept_source_route
/bin/echo "0" > /proc/sys/net/ipv4/conf/all/send_redirects

# Disable ICMP redirect acceptance
```

```
/bin/echo "0" > /proc/sys/net/ipv4/conf/all/accept_redirects

# Enable bad error message protection
/bin/echo "1" >
/proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

# Turn on reverse path filtering
for interface in /proc/sys/net/ipv4/conf/*/rp_filter; do
/bin/echo "1" > ${interface}
Done

# Log spoofed packets, source routed packets, redirect packets
/bin/echo "1" > /proc/sys/net/ipv4/conf/all/log_martians

# Enable IP forwarding
/bin/echo "1" > /proc/sys/net/ipv4/ip_forward
```

Further more the routing table is configured so the firewall uses the correct gateway for the Internet. In this case this will be the Fortigate firewall.

```
#---------------- SETUP DEFAULT GATEWAY ------------------------#

/bin/echo "SETUP DEFAULT GATEWAY"

/sbin/route add $GATEWAY $IF_WAN
/sbin/route add default gw $GATEWAY $IF_WAN
```

This concludes the initial configuration of the firewall. Now it is time to setup the chains of the NetFilter firewall and this is actual configuration of what will be allowed and what will be denied.

First the firewall rules are reset, and the custom chains are defined.

```
#------------- FLUSH/DEFAULT IPTABLES RULE SET ------------------#

/bin/echo "FLUSH/DEFAULT IPTABLES RULE SET"
$IPT -F -t filter
$IPT -X -t filter

$IPT -F -t mangle
$IPT -X -t mangle

$IPT -F -t nat
```

```
$IPT -X -t nat

$IPT -F INPUT
$IPT -F OUTPUT
$IPT -F FORWARD

$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP

#----------- CREATE/INITIALIZE CUSTOM CHAINS --------------------#
/bin/echo "CREATE/INITIALIZE CUSTOM CHAINS"

$IPT -N FROM_WAN_FOR
$IPT -N FROM_LAN_FOR
$IPT -N FROM_VPN_CRYPT_FOR
$IPT -N FROM_VPN_PLAIN_FOR
```

The following rules defines how the firewall itself can communicate with the support network. The firewall is only accessible from the support network and all communication is run over port 22 using the SSHv2 protocol.

```
#--------------------- FIREWALL CONNECTIONS --------------------#
/bin/echo "FIREWALL CONNECTIONS"

# allow ssh (tcp port 22) connection from support zone and log new
# connections

$IPT -A INPUT -i $IF_SUP \
        -m state --state NEW \
        -p tcp --dport 22 -j LOG --log-prefix=SSH_CONNECTION:

$IPT -A INPUT -i $IF_SUP \
        -m state --state NEW,ESTABLISHED,RELATED \
        -p tcp --dport 22 -j ACCEPT

$IPT –A OUTPUT –i $IF_SUP \
        -m state --state ESTABLISHED,RELATED \
        -j ACCEPT
```

Next is the definition of the PREROUTING chain. In a security aspect these rules are really important because they define the connections that can be initialized from the outside of the LAN. This section handles PPTP connections from WAN and redirects these connections to the PoPTop server.

The actual pre routing rules are followed by several logging rules. This is an attempt to discover spoofing attempts or anomalies on the different legs of the firewall. The rules will log packets that contain a source address of a different subnet than the subnet of the interface they hit.

```
#----------------------- PREROUTING ----------------------------#
/bin/echo "PREROUTING"

# PPTP traffic is redireted to the IP address of the PPTP server
# Here it would be the place to make restrictions on traffic that
# could get through for example to restrict source IP addresses

$IPT -t nat -A PREROUTING -i $IF_WAN -p tcp --dport 1723 \
        -j DNAT --to-destination $IP_PPTP_CRYPT

$IPT -t nat -A PREROUTING -i $IF_WAN -p 47 \
        -j DNAT --to-destination $IP_PPTP_CRYPT

# LOG and DROP spoofing on the local interfaces
$IPT -t nat -A PREROUTING -i $IF_LAN \
        -s ! $CLASS_A \
        -j LOG --log-prefix=LAN_SPOOF:

$IPT -t nat -A PREROUTING -i $IF_LAN \
        -s ! $CLASS_A \
        -j DROP

# LOG and DROP spoofing on VPN_CRYPT (NOT WAN interface)
$IPT -t nat -A PREROUTING -i $IF_VPN_CRYPT \
        -s ! $CLASS_B \
        -j LOG --log-prefix=VPN_CRYPT_SPOOF:

$IPT -t nat -A PREROUTING -i $IF_VPN_CRYPT \
        -s ! $CLASS_B \
        -j DROP

# LOG and DROP spoofing on VPN_PLAIN (NOT WAN interface)
$IPT -t nat -A PREROUTING -i $IF_VPN_PLAIN \
        -s ! $CLASS_B \
        -j LOG --log-prefix=VPN_PLAIN_SPOOF:

$IPT -t nat -A PREROUTING -i $IF_VPN_PLAIN \
        -s ! $CLASS_B \
        -j DROP
```

In the next section below, the packets are directed to the 4 custom chains defined. The packets are directed based on the interface at which they arrive. This approach has two advantages; the firewall becomes more manageable since rules related to a specific interface of the firewall are located in one chain. Further more it boosts the performance of the firewall instead of possibly having to evaluate all the rules in the FORWARD chain. Only one of the custom chains has to be evaluated. This might not be significant in a small rule set like this, but when the rule set contains thousands of rules it can greatly improve performance to split up the rules in custom chains.

```
#------------- INTERFACE CONTROL ----------------------#
# packets are redirected to custom chains based on the interface
# they hit

# packet hit the WAN interface
$IPT -A FORWARD -i $IF_WAN -j FROM_WAN_FOR

# packet hit the LAN interface
$IPT -A FORWARD -i $IF_LAN -j FROM_LAN_FOR

# packet hit the CRYPT VPN leg
$IPT -A FORWARD -i $IF_VPN_CRYPT -j FROM_VPN_CRYPT_FOR

# packet hit the PLAIN VPN leg
$IPT -A FORWARD -i $IF_VPN_PLAIN -j FROM_VPN_PLAIN_FOR
```

The following parts of the firewall rule set define the rules for the four custom chains. From the WAN interface packet for the PPTP connection is accepted – but only if they are directed at the PoPTop server on the IF_VPN_CRYPT interface. Further more there are a pinhole through the firewall to allow the relay server only to deliver mail to the exchange server on LAN.

Logging of all VPN connections are also done in this section.

Finally all established and related connections are allowed. This is to ensure that responses to requests initiated from the LAN can get through.

```
#---------------------------- IF_WAN ----------------------------#
# log all new VPN connections
$IPT -A FROM_WAN_FOR –o $IF_VPN_CRYPT –p tcp --dport 1723 \
        -m state --state NEW -j LOG

# allow the VPN connections to the PoPTop box
```

```
$IPT -A FROM_WAN_FOR –o $IF_VPN_CRYPT -p \
        tcp --dport 1723 -j ACCEPT
$IPT -A FROM_WAN_FOR –o $IF_VPN_CRYPT –p 47 -j ACCEPT

# pinhole to allow the mail server to receive mail from the relay
# server
$IPT -A FROM_WAN_FOR –o $IF_LAN \
        -p tcp –dport 25 \
        -s $RELAY_SERVER_IP \
        -d $LAN_MAIL_SERVER \
        -m state --state NEW,ESTABLISHED,RELATED \
        -j ACCEPT

# allow connections to LAN if connection where established
# from LAN
$IPT -A FROM_WAN_FOR -o $IF_LAN \
        -m state --state ESTABLISHED,RELATED \
        -j ACCEPT
```

Finally the needed TCP ports and UPD ports are opened from LAN to WAN. The rules handling connections from LAN clients are suspected to have the highest utilization and are therefore placed in the top of the FROM_LAN_FOR chain.

There need to be a section for each VLAN, since the IP addresses are grouped by VLAN.

```
#------------------------------ IF_LAN --------------------------#
# LAN-VLAN1 Configuration
# Open up ports from LAN to the Internet
for PORT in $LAN_CLIENT1_TCP_PORTS; do
$IPT -A FROM_LAN_FOR -o $IF_WAN \
        -p tcp –s $LAN_CLIENT1_RANGE –d $PROXY --dport $PORT \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
Done

for PORT in $LAN_CLIENT1_UDP_PORTS; do
$IPT -A FROM_LAN_FOR -o $IF_WAN  \
        -p udp –s $LAN_CLIENT1_RANGE –d $PROXY --dport $PORT \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
Done

# Allow ICMP traffic from LAN
$IPT –A FORM_LAN_FOR –o $IF_WAN \
        -p icmp –s $LAN_CLIENT1_RANGE –d $PROXY \
        -m state –-state NEW,ESTABLISHED,RELATED –j ACCEPT
```

For LAN-VLAN2 a similar configuration is made.

```
# LAN-VLAN2 Configuration
# Open up ports from LAN to the Internet
for PORT in $LAN_CLIENT2_TCP_PORTS; do
$IPT -A FROM_LAN_FOR -o $IF_WAN \
        -p tcp –s $LAN_CLIENT2_RANGE –d $PROXY --dport $PORT \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
Done

for PORT in $LAN_CLIENT2_UDP_PORTS; do
$IPT -A FROM_LAN_FOR -o $IF_WAN  \
        -p udp –s $LAN_CLIENT2_RANGE –d $PROXY --dport $PORT \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
Done

# Allow ICMP traffic from LAN
$IPT –A FORM_LAN_FOR –o $IF_WAN \
        -p icmp –s $LAN_CLIENT2_RANGE –d $PROXY \
        -m state –-state NEW,ESTABLISHED,RELATED –j ACCEPT
```

From LAN the Server that is accessible by PPTP is allowed to respond back to connections that are established already.

```
# LAN-VLAN3 Configuration
# Allow the LAN servers to respond to VPN connections
$IPT -A FROM_LAN_FOR -o $IF_VPN_PLAIN \
        -p tcp –s $LAN_SERVER_RANGE \
        -m state --state ESTABLISHED,RELATED –j ACCEPT

$IPT -A FROM_LAN_FOR -o $IF_VPN_PLAIN \
        -p udp –s $LAN_SERVER_RANGE \
        -m state --state ESTABLISHED,RELATED –j ACCEPT
```

The DNS server is allowed to retrieve DNS records from the Internet.

```
# Allow LAN DNS server to do global DNS requests
$IPT -A FROM_LAN_FOR -o $IF_WAN \
        -p udp –dport 53 \
        -s $LAN_DNS_SERVER \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# Allow LAN DNS server to perform zone transfers
```

```
$IPT -A FROM_LAN_FOR -o $IF_WAN \
        -p tcp –dport 53 \
        -s $LAN_DNS_SERVER \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# Allow LAN DNS to do time synchronization from support zone
$IPT -A FROM_LAN_FOR -o $IF_SUP \
        -p udp –dport 123 \
        -s $LAN_DNS_SERVER \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

No connections should be initialized from the PoPTop box and out so only connections that are established are accepted in this direction.

```
#------------------------- IF_VPN_CRYPT ----------------------#
# Allow responses for a VPN connection

$IPT -A FROM_VPN_CRYPT_FOR -o $IF_WAN -p tcp --dport 1723 \
        -m state --state ESTABLISHED,RELATED -j ACCEPT

$IPT -A FROM_VPN_CRYPT_FOR -o $IF_WAN -p 47 \
        -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Connections from the PoPTop box to LAN are logged, they are connection directly from the Internet to servers on LAN and are the Achilles heel of the network, and so severe logging is necessary. Especially connections that are attempted to hosts not in the server range are alarming.

```
#------------------------- IF_VPN_PLAIN ----------------------#
# Allow connections from the PoPTop box to LAN
# Only connections to the server IP addresses is allowed
# Only the TCP and UDP protocol is allowed

# We log all connections even the ones that are not
# directed to servers
$IPT -A FROM_VPN_PLAIN_FOR -o $IF_LAN -p tcp \
        -m state --state NEW -j LOG

# Only packets with destination for the LAN servers are allowed
# Only TCP and UDP traffic are allowed
$IPT -A FROM_VPN_PLAIN_FOR -o $IF_LAN -p tcp \
        -d $LAN_SERVER_RANGE \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
$IPT -A FROM_VPN_PLAIN_FOR -o $IF_LAN -p udp \
        -d $LAN_SERVER_RANGE \
        -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

Finally all packages that leave the firewall are masqueraded so answers are send to the correct IP address – the IP address of the firewall on the given interface.

```
$IPT -A POSTROUTING -t nat -o $IF_WAN -d 0/0 \
        -j MASQUERADE

$IPT -A POSTROUTING -t nat -o $IF_LAN -d 0/0 \
        -j MASQUERADE

$IPT -A POSTROUTING -t nat -o $IF_VPN_CRYPT -d 0/0 \
        -j MASQUERADE

$IPT -A POSTROUTING -t nat -o $IF_VPN_PLAIN -d 0/0 \
        -j MASQUERADE
```

VPN

Configuration of PPTP VPN gateway

The VPN gateway chosen is PoPTop – a Linux PPTP server. This configuration is demanding in a security aspect. Since a software server is used the operating system has to be patched and hardened probably. Further more the PPTP protocol has some security measures that have to be handled. Especially there is no authentication header like with IPSEC. This is the price for being able to NAT the VPN connection.

The goal for this section is to describe how to make an overall secure VPN gateway using PPTP, MPPE and MPPC on a Debian Linux server. Further more it is necessary to force the use of 128-bit encryption to make this VPN gateway useable for the GIAC Enterprise. The PPTP authentication protocol has a bad security history and therefore it is necessary to enforce MS-CHAP version 2.

First the abbreviations are sorted out:

MPPE is the Microsoft Point-to-Point Encryption standard (RFC-3078, RFC-3079)
MPPC is the Microsoft Point-to-Point Compression standard (RFC-2118)
MS-CHAPv2 is the Microsoft Challenge Handshake Authentication Protocol version 2

Version 1 of the MS-CHAP had several security issues that have been solved by now. The table below shows the problems and solutions[9]

MS-CHAP version 1 issue	MS-CHAP version 2 solution
LAN Manager encoding of the response used for backward compatibility with older Microsoft remote access clients is cryptographically weak.	MS-CHAP v2 no longer allows LAN Manager encoded responses.
LAN Manager encoding of password changes is cryptographically weak.	MS-CHAP v2 no longer allows LAN Manager encoded password changes.
Only one-way authentication is possible. The remote access client cannot verify that it is dialing in to its organization's remote access server or a masquerading remote access server.	MS-CHAP v2 provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server that it is dialing in to has access to the user's password.
With 40-bit encryption, the cryptographic key is based on the user's password. Each time the user connects with the same password, the same cryptographic key is generated.	With MS-CHAP v2, the cryptographic key is always based on the user's password and an arbitrary challenge string. Each time the user connects with the same password, a different cryptographic key is used.
A single cryptographic key is used for data sent in both directions on the connection.	With MS-CHAP v2, separate cryptographic keys are generated for transmitted and received data.

To summarize the content of this chapter:

1. Patch and install a new kernel that supports MPPE/MPPC.
2. Patch and install a PPP daemon (PPPD) that support MPPE/MPPC
3. Configure PPPD to enforce MS-CHAPv2 and MPPE with 128-bit encryption.
4. Install and configure the PoPTop PPTP server for Linux

[9] [MS1]

Kernel configuration and installation
These instructions are specific for Debian 3.0 with a kernel version 2.4.26. Serge Stepanov[10] inspired the configuration.

```
$apt-get install debhelper kernel-package modutils \
libncurses5-dev gcc fakeroot libnet0-dev
```

Download the kernel source and the corresponding kernel patches to /usr/src

```
$cd /usr/src
$tar xvzf linux-2.4.26.tar.gz
$ln –s linux-2.4.26 linux
$patch –p0 –I linux-2.4.26-mppe-mppc-1.0.patch
$cd linux
$cp /boot/config-2.4.26 .
$make oldconfig
```

Edit the Makefile:

```
$vi Makefile
EXTRAVERSION = <kernel identifier e.g. mppe-mppc>
```

Configure the kernel

```
$make menuconfig
```

Device Drivers -> Networking Options -> select "PPP support" and then select "Microsoft PPP compression/encryption (MPPC/MPPE). Also loadable module support is disabled since this box is used as a server and it should not be necessary nor is it recommended to load modules dynamically. I will not get into the details of the exact kernel configuration, but it should be stripped down as much as possible.

```
$make-kpkg clean
$fakeroot make-kpkg --append_to_version -486 --revision=rev.01 --
bzimage kernel_image modules_image
$cd ..
$dpkg -i kernel-image*.deb
```

PPPD installation

[10] [STEPANOV]

This package includes the pppd used by PoPTop. This package also has to be patched to support MPPE/MPPC

Download the packages `ppp-2.4.2.tar.gz` and `ppp-2.4.2-mppe-mppc-1.0.patch.gz` to `/usr/src`.

```
$cd /usr/src
$tar zxvf ppp-2.4.2.tar.gz
$gunzip ppp-2.4.2-mppe-mppc-1.0.patch.gz
$patch -p0 -i ppp-2.4.2-mppe-mppc-1.0.patch
$cd ppp-2.4.2
$./configure
$make
$make install
```

PPPD configuration - /etc/ppp/options-pptpd

```
name *

#lock file for ensuring exclusive access to the device
lock

#Maximum Transmit Unit
mtu 1450

#Maximum Receive Unit
mru 1450

#proxy the arp address of the peer which has the effect
#of making the peer being connected to the local network
proxyarp

#Require the peer to authenticate itself before allowing
#networks packets to sent or received
auth

#how many echo request lost before the peer is assumed
disconnected
lcp-echo-failure 3

#echo request interval
lcp-echo-interval 5

#the deflate compression scheme should not be used
```

```
deflate 0

# Authentication method – mschap version 2 is enforced
require-mschap-v2

# Data encryption method – 128 bit encryption is enforced
mppe required,no40,no56
```

PoPTop installation

```
$tar zxvf pptpd-1.1.4-b4.tar.gz
$cd poptop-1.1.4
$./configure
$make
$make install
```

```
$modprobe ppp_mppe_mppc
```

PoPTop configuration - /etc/pptpd.conf

```
#Location of the pppd configuration
option /etc/ppp/options-pptpd

#The local address of the PoPTop servers unencrypted interface
localip 172.31.0.1

#The IP range assigned to hosts connecting
remoteip 172.31.5.10-20
```

To start the PPTPD process enter the command:

```
$/usr/local/sbin/pptpd
```

Testing the connection

To test the connection a standard window 2000 PPTP client is configured. Figure 15 shows the configuration of the *Advanced Security Settings* and here the connection to GIAC Enterprise is configured to use maximum strength encryption and only MS-CHAPv2 and disconnect if this is not possible.

Figure 15

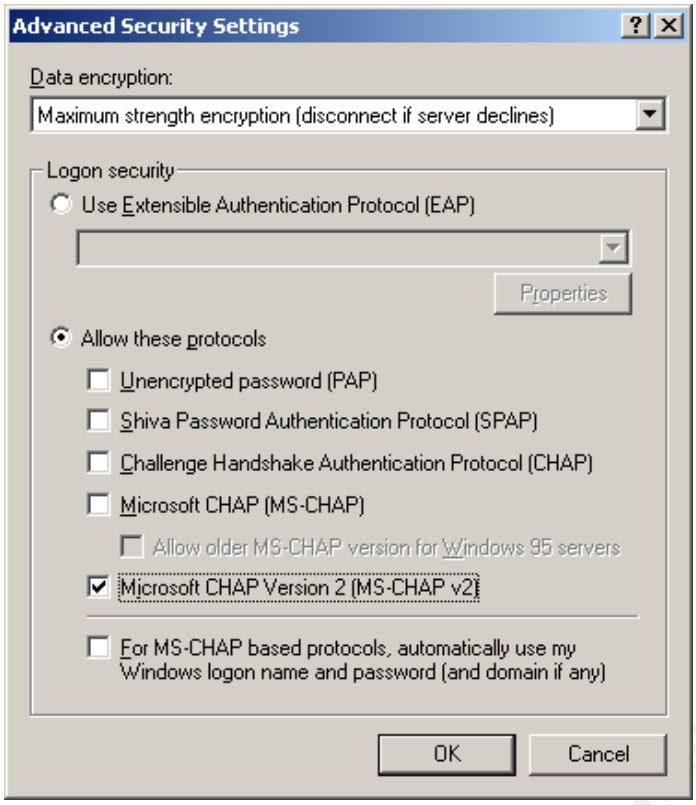


Table 1 shows the SYSLOG file after the PPTP connection. The IP addresses have been sanitized.

Table 1

```
Aug 12 16:36:29 debian pptpd[7914]: MGR: Manager process started
Aug 12 16:36:29 debian pptpd[7914]: MGR: Maximum of 3 connections
available
Aug 12 16:36:36 debian pptpd[7916]: CTRL: Client <ipaddress>
control connection started
Aug 12 16:36:36 debian pptpd[7916]: CTRL: Starting call (launching
pppd, opening GRE)
Aug 12 16:36:36 debian pppd[7917]: pppd 2.4.2 started by root, uid
0
Aug 12 16:36:36 debian pppd[7917]: Using interface ppp0
Aug 12 16:36:36 debian pppd[7917]: Connect: ppp0 <--> /dev/pts/2
Aug 12 16:36:38 debian pppd[7917]: MPPC/MPPE 128-bit stateful
compression enabled
```

```
Aug 12 16:36:41 debian pppd[7917]: found interface eth0 for proxy
arp
Aug 12 16:36:41 debian pppd[7917]: local  IP address
172.16.100.111
Aug 12 16:36:41 debian pppd[7917]: remote IP address <ipaddress>
```

The connection works and from the configuration of the client and the entries in SYSLOG I conclude that the PPTP connection is working as expected and with the required encryption strength of 128-bit and MS-CHAPv2

PPTP Security

There are no authentication headers for the PPTP traffic. Therefore it is very important to screen traffic heavily for any malicious activity. The lack of proper IP authentication headers make PPTP vulnerable to man-in-the-middle attacks.

Access from the PPTP VPN gateway is limited to the servers on the LAN network. Even if there should be a compromise the attacker will only be granted access to the servers with the privileges of the compromised user. All the servers on the LAN are hardened with the GIAC Enterprise guidelines for servers directly accessible from the Internet.

The PPTP access is only available during the working hours, which is configured in the F200. This ensures active surveillance of the VPN connections and that proper actions can be taken in the event of a compromise.

The VPN clients are forced to run a local firewall that has to be active. A script is made to start up the PPTP connection that will also check if the host-based firewall is running. This is to ensure that the client is not connected to two different networks at the same time, and thereby connecting the GIAC Enterprise with a foreign network via the PPTP connection.

The firewall-LAN has two legs dedicated to support the PPTP VPN gateway. This is to ensure that the unencrypted traffic is screened and passed back through the firewall, so no traffic enters the LAN without being scanned. Furthermore this makes it possible to have the firewall protect the servers and only allowing access on necessary ports.

On the unencrypted VPN leg Snort is scanning for intrusion patterns. NetSquid[11] is used in conjunction with snort to block PPTP connections real time if an intrusion pattern is detected.

[11] [NETSQUID]

It could have been considered to offer a Fortigate-50A running in transparent mode to scan the PPTP traffic for virus and add an extra layer of intrusion detection and content filtering, but this have not been chosen due to economic considerations.

The VPN gateway is only one way; connections cannot be initiated from LAN.

With the above restrictions and precautions the PPTP gateway is considered safe enough for the GIAC Enterprise to use for the road warriors to access the LAN from remote locations. PPTP is very convenient to use, it is supported on every Windows machine as default and there are no problems with NAT.

Testing and debugging the firewalls

It is important to verify that the firewall is acting as expected and that restrictions are in fact active.

To test the firewalls at the GIAC Enterprise TCPDUMP is used to dump traffic and show what actually hits the interfaces and what get through. Several TCPDUMP sessions can monitor multiple Ethernet cards real time. SENDIP is used to generate packages that are send toward the firewall on different interfaces.

To test the NetFilter firewall the LOG parameter is very useful. With the LOG parameter it is possible to determine if packets are recognized by certain NetFilter rules by studying the SYSLOG file.

Using SYSLOG in conjunction with NetFilter

The firewall protecting the LAN includes the following configuration line to make sure that all SSH connections to the firewall are logged:

```
$IPT -A INPUT -i $IF_SUP \
        -m state --state NEW \
        -p tcp –dport 22 -j LOG –log-prefix=SSH_CONNECTION:
```

After a SSH login the above configuration give rise to the following log entry in SYSLOG:

```
Aug 15 13:50:25 debian kernel:
SSH_CONNECTION:
IN=eth0
OUT= MAC=00:a0:24:a8:0f:f6:00:09:6b:07:a3:1f:08:00
SRC=<ip-address>
```

```
DST=<ip-address>
LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=24697 DF PROTO=TCP SPT=4225
DPT=22 WINDO
W=65535 RES=0x00 SYN URGP=0
```

This is a very effective way to determine what rule a packet match. Notice that the LOG rule is exactly matching the ACCEPT rule. Only the parameters after the –j parameter is changed.

Using SENDIP

SENDIP is a packet generator that supports ipv4 ipv6 icmp tcp udp bgp rip and ntp. The structure of SENDIP is modularized, so packets are build up using modules for each of the protocols supported.

An example to test the pinhole used to transfer mail from the relay server in the DMZ to the mail server located on LAN:

```
sendip –p ipv4 –is 10.0.0.1 –p tcp –tfs 0 –tfa 1 –ts 4400 –td 25 \
172.30.0.20
```

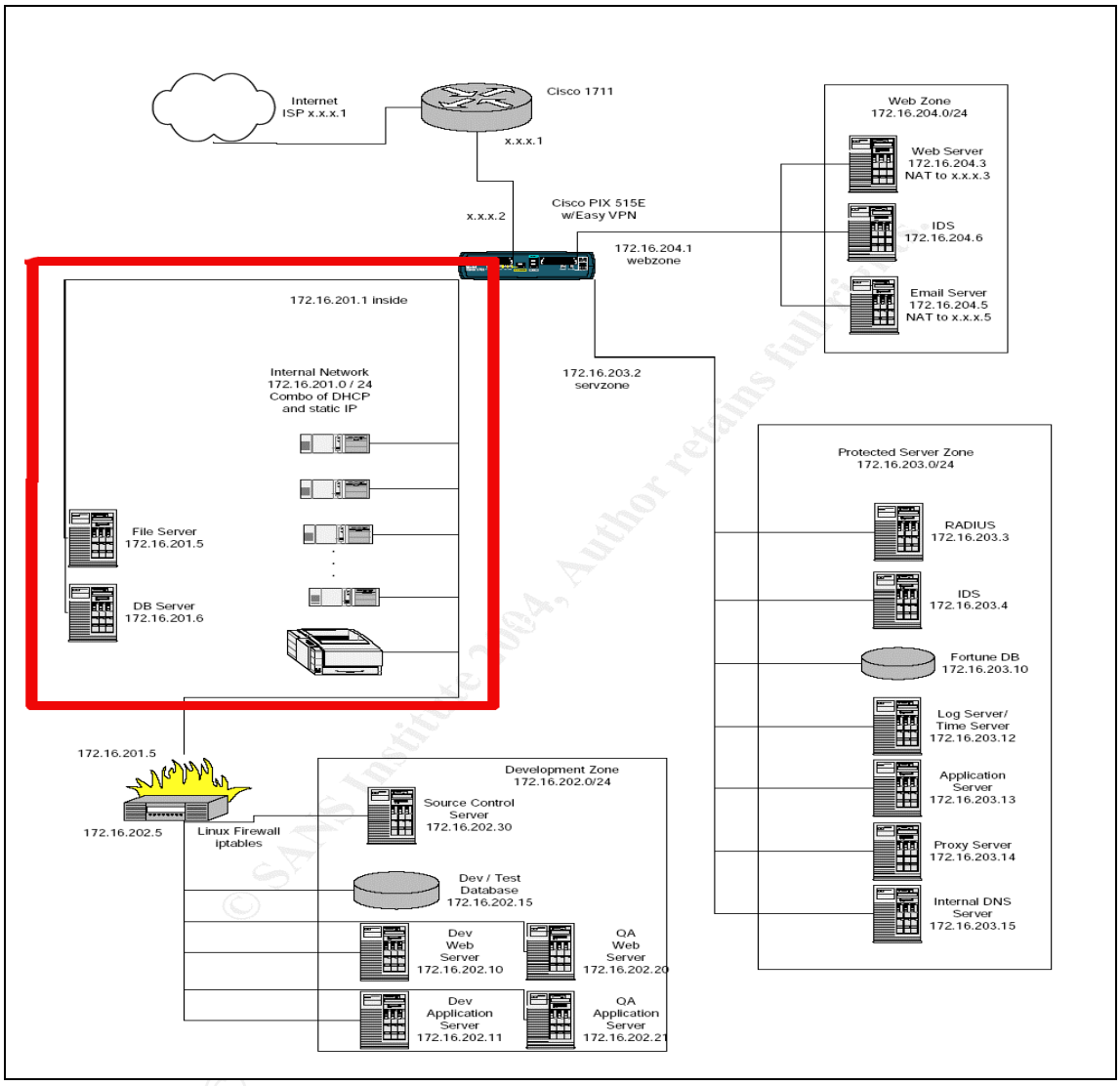
The SENDIP command above is constructing an IP version 4 packet (-p ipv4). The IP source address is 10.0.0.1 (-is 10.0.0.1). The IP packet is encapsulating a tcp package (-p tcp). The TCP SYN flag is 0 (-tfs 0) and the TCP ACK flag is 1 (-tfa 1). The TCP source port is 4400 (-ts 4400). The TCP destination port is 25 (-td 25). Finally the destination IP address is 172.30.0.20.

The SYSLOG and SENDIP in combination with TCPDUMP gives a nice test suite for testing the firewalls thoroughly.

Assignment 3 – Design Under Fire

I have chosen to attack the network designed by Mike Armstrong[12].
His network design is reprinted in Figure 16. The box indicates the LAN, which is the primary attack vector as demonstrated in the following.

Figure 16



[12] [ARMSTRONG]

Attack on the network

The GIAC Enterprise has been on the target list for some times, since their fortunes do not always tell the truth! So now we are going to teach them a lesson for not fulfilling our wishes and fortunes. Also the market for fortunes are growing and corporate information from the GIAC Enterprise might be worth something for the competitors – this can eventually mean that we can punish GIAC Enterprise as well as making a fortune.

The reconnaissance

Searching with Google through news groups reveal a few entries from an employee at GIAC Enterprise seeking help for configuring Linux servers. I mark myself the questions about CVS. This is the server of the source code and this is the ultimate target. If the CVS server can be compromised a *bomb* can be placed in the source code and that is probably a worst-case scenario for any corporation. Further more, if we posses the source code it can be analysed for bugs and exploits for future use – and possibly sold!

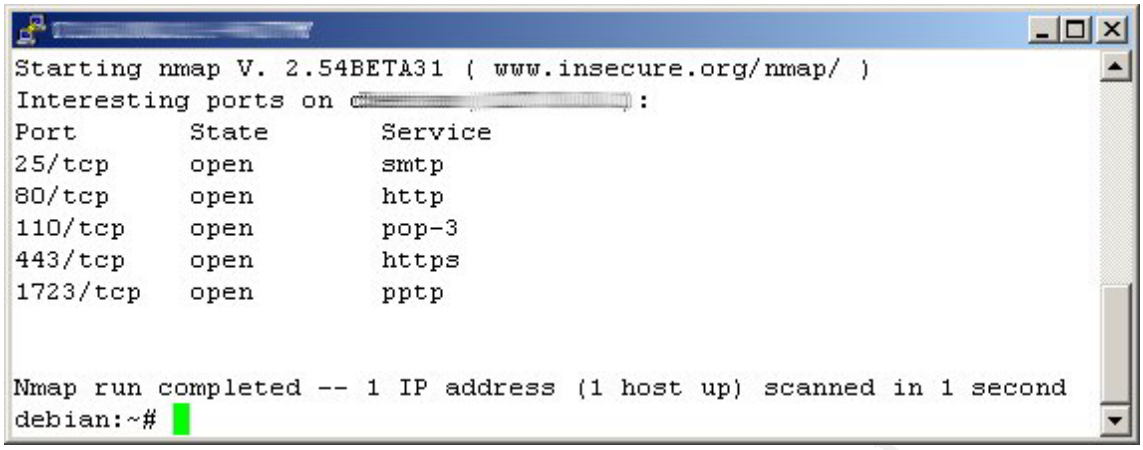
I notice that, to avoid spam probably, the GIAC Enterprise employee consulting the news groups have been using a hotmail account.

The problem is how do I compromise the CVS server. This could be a wild shot and totally impossible. The reconnaissance starts by *war driving* in the neighbourhood scanning for wireless Internet hot spots. After 10 minutes[13] I have a total anonymous address of some innocent Internet user that still haven't figured out how to shut down his/hers hot spot. This makes up an excellent cover for port scanning and other exploits. Sitting in the car, a port scanning is performed from the laptop.

Figure 17 - Nmap port scanning shows the result of running Nmap against the GIAC Enterprise.

[13] The situation in Copenhagen, Denmark is actually so bad, that it is possible to identify an open hot spot within 10 minutes – 30 minutes at worst.

Figure 17 - Nmap port scanning



Port 110 is open for checking mail, so passwords are send in plain text over the network.

The PPTP port is open and could provide a nice vector, but this seems to be an error, since there is no response to any probing on that port (In Mike's report on page 10 it is stated that port 1723 is open – on page 40 it is stated that only IPSEC is used for VPN?!).

The attack vectors

This small reconnaissance has granted us some useful information.

- I have obtained some hotmail addresses, which can be used to send malicious mails that will eventually be viewed in the browser. The attack vector is most likely to be MSIE or social engineering.
- I have identified certain news groups that the GIAC Enterprise employees are using. This can be used to learn more about their network through social engineering, by helping them with problems and responding to questions they ask.
- It is very likely that GIAC Enterprise has a CVS server running, so research on this application is initiated.
- There are services on the network that are utilizing plain text passwords.

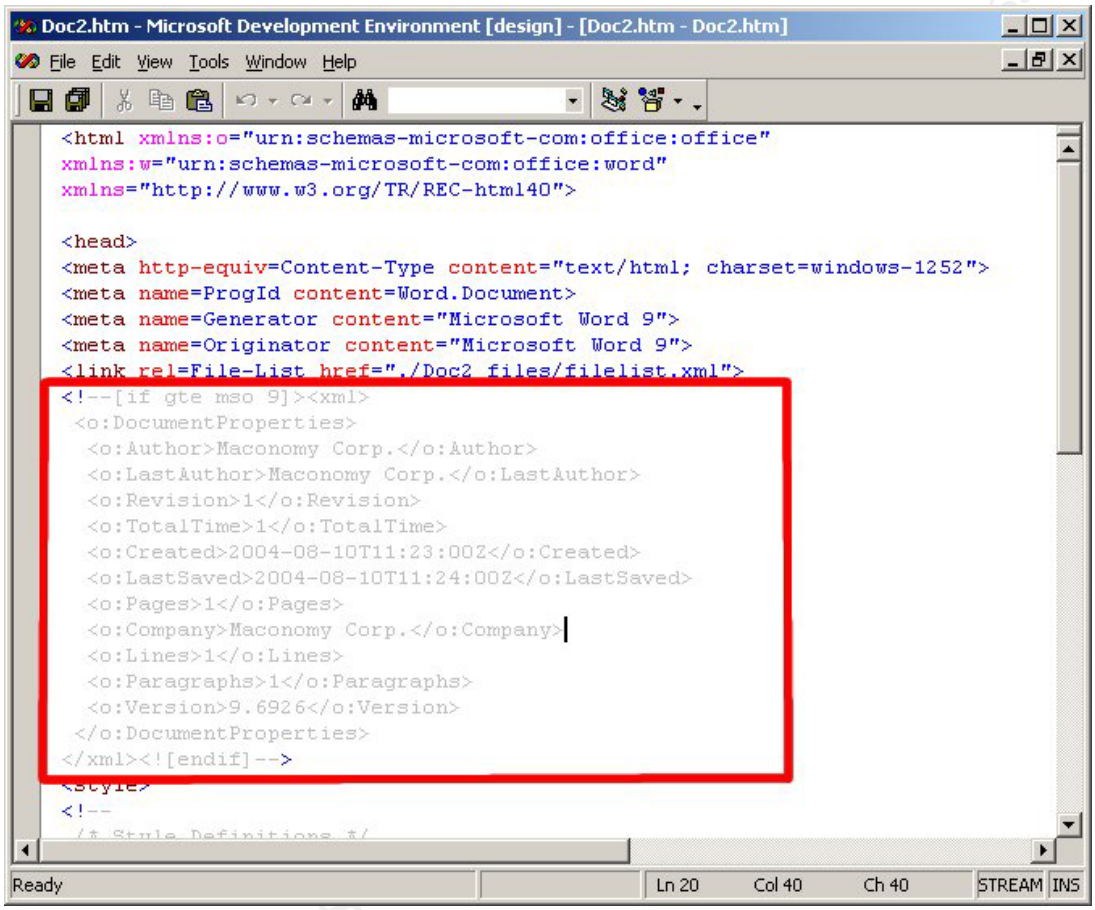
Cross scripting

July 13th, the opportunity arises, a security flaw in Hotmail is released by the GreyHats Security Group (http://freehost07.websamba.com/greyhats/). This is a Hotmail cross-scripting vulnerability that allows execution of arbitrary JavaScript code. And it has not been patched up – I quote GreyHats Security:

"Btw, It was a little mean of me to post this vulnerability on the web before I told Hotmail about it, so please be nice and use this only for educational purposes. Don't write a virus or anything because whatever happens, I will not be held accountable."

The attack is utilizing some tags that are generated when a MS Word document is saved as a HTML file. If the source code is reviewed the interesting part is the **`<!--[if gte mso 9]>`** tag. Figure 18 - Unmodified Code shows the code generated by MS Word.

Figure 18 - Unmodified Code



Unfortunately MS forgot to do some sanity checks on the code within these tags and that allows a malicious user to inject JavaScript.

Figure 19 - Modified Code

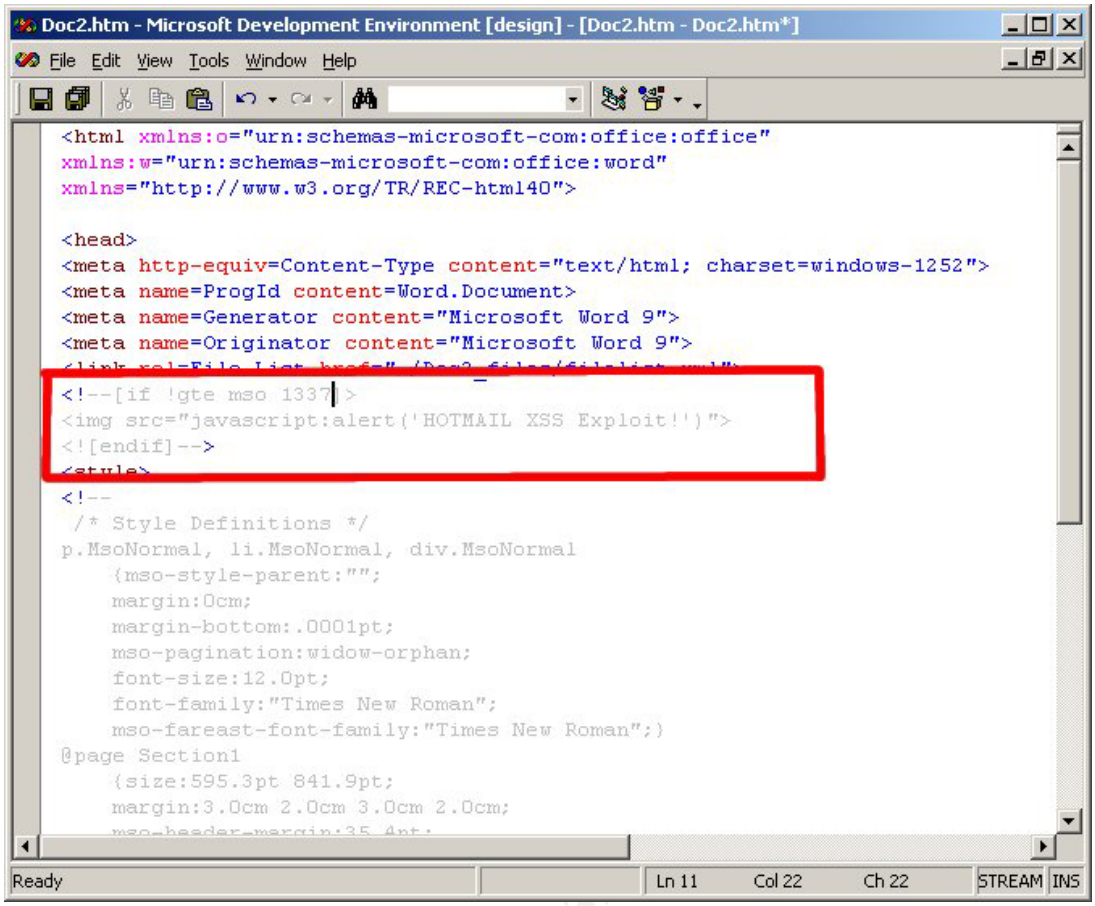


Figure 19 - Modified Code shows that the tags are being misused. The **if** statement now check if the version of MS office is **not** greater than or equal to 1337 (**`[if !gte mso 1337]`**). This is accepted by hotmail, and executed as soon as the user opens the mail, the user only need to click on mail in the browser to execute the vulnerability.

The Hotmail exploit is dangerous, because people tend to blindly trust MS and other big companies. Hotmail both do spam filtering and virus detection but nothing will detect this little injection. It also shows the power of cross scripting and demonstrates how important sanity checks are when developing web applications.

But the network of the GIAC Enterprise is not compromised yet. The next step is to use the JavaScript injection to gain access to the LAN of the GIAC Enterprise**.** The injection is

used to redirect the user to a webpage that contains a bitmap picture that is used to actual exploit the browser. After the injection the user is redirected back to the hotmail account in a hope that nothing will be noticed.

Resources:

- Description and PoC: [HOTMAIL]

Conditions for success:

- Hotmail vulnerability exists

Access to LAN

Once the user logs in to Hotmail and is redirected to our web server a MSIE bug is used to exploit the browser. The exploit of MSIE is based on the bug: *Microsoft Internet Explorer Bitmap Processing Integer Overflow Vulnerability*. The vulnerability has the bugtraq ID 9663. The bug will allow execution of arbitrary code as the user logged in. Since the user is accessing news groups and asking questions about CVS we might be lucky that this is a power user with unrestricted right to install programs and other good stuff.

To actually access the LAN a tunnel have to be created from the LAN to our server. Then the attack is complete and there is full access to the LAN so we can propagate further on to the network and hopefully target the real goal – the CVS server.

To create a tunnel from inside the LAN to our host a Trojan is needed. There are plenty to choose from on the Internet – a very popular one is Sub7. Some virus scanners do not scan so deep so putting the executable in directories with more that 255 characters might avoid detection.

Another approach is just to use Stunnel and modify the source code to hide it as much as possible, and thereby make an encrypted tunnel from the LAN to our server. A third option would be Loki that uses ICMP as the communication channel. Also the local log files is modified, as the first thing, to remove possible tracks.

Once the tunnel is in place we can continue to exploit the internal network and the ultimate trophy – the CVS server and the source code.

Conditions for success:

- MSIE is not patched up
- User must have administrative rights on the client so the Trojan can be installed.
- It is possible to circumvent possible anti virus software

Exploiting CVS server

After sniffing the LAN for short time it is evident that there is in fact a CVS server running on port 2401. This is the default port of the CVS pserver. The CVS server running over pserver is easy to exploit since the login names and passwords are send in clear text over the network and several exploits exist. In worst case we can only access the repository with login credentials picked up by sniffing the network. In the best case, if the box has not been patched recently we will be able to do a remote root exploit of the CVS server and take full control.

Figure 20 - dsniff against CVS

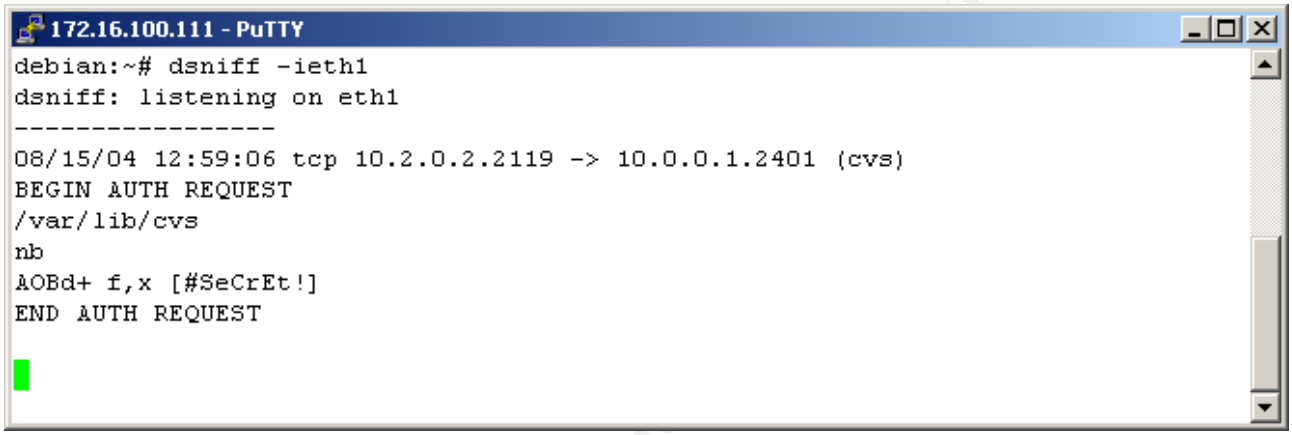


Figure 20 - dsniff against CVS shows a screen dump from sniffing with `dsniff` on the network while the user `nb` logs into the CVS server using password `#SeCrEt!` As shown, dsniff can decrypt the CVS password real time.

Lately CVS has taken a lot of heat, and warnings have been posted on the CVS website[14], because several root exploits where discovered including remote root exploits.

If it is possible to launch a root exploit against the CVS server anything is possible on that server. This includes installing other software generate tunnels out of the network, pick up passwords, and edit log files to cover traces of the intrusion. If the kernel is compiled with loadable module support, that is an excellent attack vector to retain access to the system, since custom made kernel modules can be loaded at boot time, and root privileges can be maintained.

[14] [CVS]

But that does not mean it is easy to retain access to the system. If the firewall is well configured the CVS server is not allowed to initiate any outbound connection, and it would be necessary to retain access to a client on LAN as well, so the connection to the CVS server could be initiated from LAN. Furthermore launching a root exploit against a network that is guarded by an updated NIDS is possibly going to set off all the bells and whistles. Therefore it might not be wise to utilize the possible root exploits of the CVS server initially.

Resources:

- PoC: [CVS1]
- Advisory: [CVS3]

Conditions for success:

- None – to sniff passwords that are send plain text.
- Latest patches are not installed (will avoid root exploit).
- Avoid NIDS in case remote exploit is utilized.

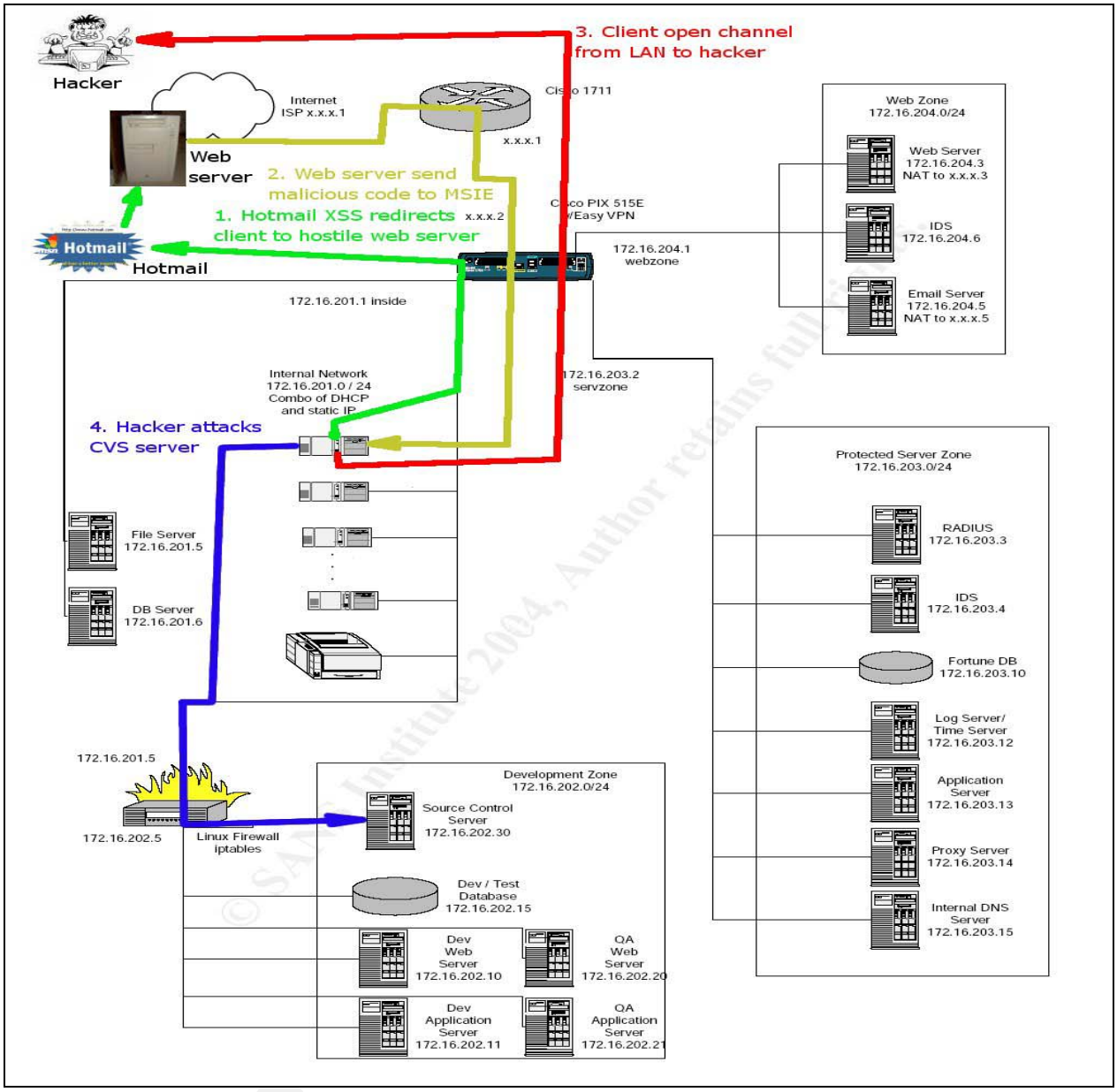
Attack summary

Figure 21 - Network Attack shows a graphical overview of the attack conducted against Mike Armstrong's version of the GIAC Enterprise.

As the figure shows the attack is pretty complicated and as pointed out in the previous sections describing the attack, there are a lot of conditions that need to be fulfilled for the attack to succeed. Given the administrator is not keeping up with patches for the servers and that clients are not updated regularly then it is not an impossible scenario at all, I believe.

Parts of the attack might have to be modified for future use, e.g. using hotmail might not be a valid attack vector for very long. But the attack on the CVS server is very likely to happen should an attacker gain LAN access.

Figure 21 - Network Attack



Another attack vector could be the MySQL database server. Secunia advisory SA8753 reveals a weakness in the way MySQL stores passwords. This could possibly be exploited if the server is not patched. Initial access to the server is required but the password of the exploited client could be grasped with at key logger.

Securing the network

There are things that could be done to Mike Armstrong's design to further strengthen the security. Generally the most important thing is not to use plain text passwords. This is a real problem in this setup. When initial access to LAN is achieved everything is open because you can sniff the passwords and usernames of other services directly with DSNIFF for example. This includes:

- POP-3 mailbox usernames and passwords.
- CVS username and passwords.

The general problem is to depend on the security build into applications that are not designed with security specifically in mind. Therefore it is wise to protect such services by other means. The network should not be considered safe even though there is a firewall, and passwords propagating over the network, should always be encrypted. Another argument is social engineering; I will bet that more than one person at the GIAC Enterprise network is using the same password for several services if it is possible, which might make sniffing plain text passwords really effective

The Hotmail vulnerability is hard to prevent. New cross script vulnerabilities show up and this one is just an example of how cross scripts can be exploited and that even MS can make mistakes that makes it possible. The only way to try and prevent cross scripting is by patching and education. If the users understand the dangers that accessing web sites mitigate they might be more aware. Even web sites controlled by MS can be dangerous ;-) Using a SUS server or alike will make sure the clients are updated frequently with patches and hot fixes.

There is a way to actually secure the LAN completely from cross scripting and other browser exploits leading to internal LAN compromise. The solution is to use Citrix or similar where the browser is isolated in a secure zone and the client computer acts as a thin client and only receives the screen shots of the browser, but it is actually only the Citrix server that is executing the code. In fact all services that involve the Internet could be executed from the Citrix server, and in that way the LAN segment could actually be totally cut off from the Internet. The only problem with this solution is that it is quite expensive and GIAC Enterprise needs a big and very stable server to serve all the clients.

Secure the CVS server

Use SSH. There, is dozens of resources on the Internet on how to configure the CVS server. An advanced setup might even include certificates. STUNNEL could be used instead of PSERVER.

The CVS server has to run as root and this is risky of course, but this is also why the exploits against the CVS server leaves root access. The solution is to run CVS in a CHROOT jail[15]. This would limit the damage caused by an exploit.

CVS in CHROOT jail: [CVS2]

Secure the mail service

The mail service is provided at port 110 for users to access mailboxes. Again the use of plain text passwords is not preferable. STUNNEL can also be used to encrypt any connections to the POP-3 server. Another possibility is to provide some kind of web access to mail from the Internet and then use HTTPS maybe even with client certificates as well as passwords.

9 quick one-line advises:

1. Don't trust other company's security not even hotmail.
2. Widely used products need patching often since they are prime targets of exploits.
3. Frequently patch programs that access the Internet.
4. Remove administrative rights to users so they cannot install programs.
5. Do not allow automatic execution of JavaScript, VBScript or other script languages
6. Total protection requires isolation of web and mail on Citrix for example
7. Use secure encryption on login credentials to avoid sniffing on the network
8. Assume the LAN is insecure if the LAN users have Internet access.
9. Protect the servers on LAN like Internet servers if the LAN clients have Internet access.

[15] [CVS2]

Assignment 4A – Future state of security technology

Introduction - Automating security policy enforcement

I will explore the possibilities for automated policy enforcement.

The approach is to look at, existing security products and evaluate their functionality and methods for policy enforcement. I will try to draw a picture of the current state of the art.

Then I will move on to look at suggest possible future scenarios of development, and the basis of development and standardization needed for these scenarios to be realistic.

The idea is to look at the security problems in a broader perspective than what is taken by the vendors of specialized products like firewalls and anti virus products.

Problem description

It can be problematic to enforce a security policy on a network, simply because the tools and components are not available or well developed – or expensive. In this assignment I will explore what a policy is and how it can be implemented. I will look at some of the technical issues with automating the process of defining and implementing a security policy.

The problem arises when I, as a network administrator want to enforce a security policy for the users of the network. The policy might concern how the anti virus software is configured or what the patch level of the OS is or how the host based firewall is configured. A security policy can also have more *soft* parts that have a more educational characteristic e.g. describe how laptops should be handled in a security perspective, and not to open mails from addresses that are not recognized etc. I have chosen to keep focus on the network security that can be automated and enforced by tools – in principle.

The tendency today in smaller companies is that every employee has a desktop or laptop and they are connected to the corporate network that is protected by firewalls and filtering routers and segmented using VLAN. The external network is the Internet and the internal network is the LAN normally there is also a DMZ zone to isolate the internal servers directly accessible from the Internet.

Another solution is to use thin clients and control everything from central servers, so the clients of the network are just dumb terminals. This greatly increases the overall security of the internal network. Since the users are not granted access to a client running a general

purpose OS, they only have access to is a client that can serve applications as needed. Often the range of applications will be limited in such an environment and for a development environment it might not be a solution. Another aspect is the price; the basic investment is very high, since you need some huge servers with all possible failover solutions – if they go down no one will be able to work. Often the software and consultancy is expensive as well.

Yet another dimension of the securing the network and the perimeter is the wireless technology. If there are any wireless access points connected to the network, the perimeter is extended to where this wireless perimeter ends. To secure the wireless access properly access should only be granted through a VPN tunnel and the access should be regarded as a VPN connection from the Internet and the same security measure should be taken as for any other VPN connection from the Internet. Therefore I will not discuss wireless access especially.

GIAC Enterprise security policy

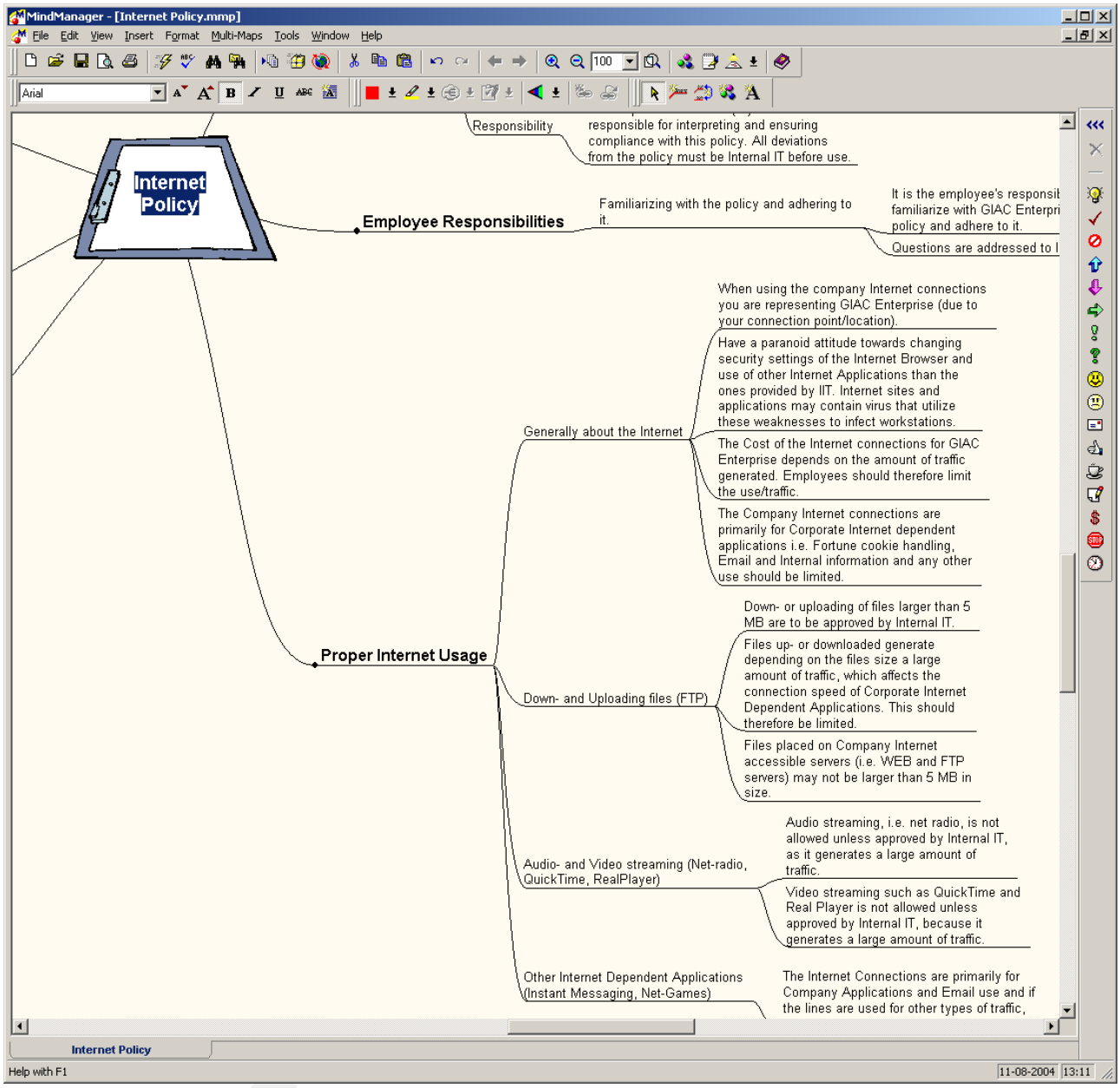
The security policy of GIAC Enterprise include many aspects ranging from physical protection of the servers and the procedures for long time storage of backup tapes to describing the password policy and the policy for introducing new software on the network. The security of the GIAC Enterprise is inspired by DS-484[16], which is the extended Danish version of BS-7799. The BS-7799 is regarded a proper subset of DS-484.

Figure 22 - Mindmap shows part of the GIAC Enterprise security Internet policy, which is organized in a mind map with the excellent MindManager program. This is only a tiny part of the entire GIAC Enterprise security policy, currently the network security policy includes:

- Anti virus policy
- Internet policy
- Remote and local access policy
- Software policy
- Access and authentication policy

[16] [DS1], [DS2]

Figure 22 - Mindmap



The policy includes both the hard facts, e.g. "*file upload and download of files larger than 5MB is to be approved by internal IT"*, as well as the general guidelines, e.g. "*When using the Internet connection you are representing GIAC Enterprise"* and so forth.

After the policies have been defined it is time to implement them and this can be hard and even impossible. Some rules like the one about representing the company requires education of employees. The restrictions on up- and downloads are to be enforced in the proxy server or the firewall. There are also rules for the size of mails and they should be implemented in the mail server. This complexity makes it hard and even impossible to fully comply with ones own security policy. E.g. the firewall might not be able to do real time tracking of the amount of traffic that have been downloaded for a given connection.

To try and ease the task of implementing a security policy the GIAC Enterprise IT department have studied the market to review the products and technologies available, that might help to automate the transition from a written security policy to the actual policy enforcement on the network.

Current state of the art

The ideas of policy enforcement are not new, and several products do implement some sort of policy enforcement. There are several commercial products on the market for securing the clients, servers and other network devices.

It is also clear from the initial research on the market that there is no silver bullet to the problem of making the written and the implemented security policy adhere automatically, but there are products that can help to some degree.

To get some ideas the GIAC Enterprise have investigated some of the popular security products on the market.

Anti Virus – F-Secure

Most corporate anti virus products include the possibility to lock down clients so the users cannot reconfigure the anti virus software. F-Secure also have the possibility to lock down the user interface on the clients. The product F-Secure further more have the possibility to do integrity checks on the applications that try to utilize the network, only approved applications are allowed access for further information see the paper F-Secure Internet Security 2004[17]. F-Secure include a simple firewall that can be used to shut down the client so only communication on selected ports is permitted.

One of the forces of F-Secure is that it can be used to control more domains from a single management console. Each domain can be another subsidiary or simple a group of clients that require other settings of the AV client.

[17] [FSEC]

Anti Virus – Trend Micro

Trend Micro is like F-Secure primarily an anti virus product but also include other programs and functions. GIAC Enterprise has investigated the brand new TM OfficeScan 6.5, which is a suite of programs that are used to secure the enterprise network. Beside the possibility to push out clients with a specific configuration it also have a tool called *Vulnerability Scanner* to scan the network for unprotected hosts. If one is found an installation can be forced automatically. If enforced installation is not possible a warning is send to the administrator. Like F-Secure the Trend Micro console can also control several domains with different configurations.

Trend Micro is working with Cisco to develop switches that can proactively prevent worms from spreading. I quote from www.infoworld.com[18] (June 08, 2004):

> *"Cisco Systems Inc. and Trend Micro Inc. on Monday announced a partnership under which Cisco will improve its routers, switches and firewalls with Trend's worm-blocking technology.*
> *Trend Micro, which uses the technology in its own VirusWall product, plans to make its signature-based worm-blocking technologies available in Cisco products by the third quarter. Cisco says the technology initially will fit into its intrusion-detection code base and be used to stop network worms that take advantage of software vulnerabilities. Trend Micro will supply updates, which will be managed via CiscoWorks and other Cisco management tools."*

Firewall – ZoneAlarm

Zone Labs is the producer of the wide spread ZoneAlarm[19] firewall. This firewall has been very popular because it is easy to use and install and it is offered free of charge for personal use. ZoneAlarm also has advanced control of applications trying to utilize the network. It is possible to set it up to do integrity check on the application as well as the libraries used by the application before access to the network is granted.

Firewall – BitGuard

A Danish produced firewall called BitGuard[20] personal firewall is actually not an application but more similar to a driver because it works at a level parallel to the operating system and not at application level. This means that it cannot only control which ports and protocols are allowed inbound and outbound and which applications can access the network, it is also able to restrict processes and even the operating system from utilizing the network.

[18] [INFOW]
[19] [ZONEA]
[20] [BITGUARD]

Sygate

The company Sygate has a product suite, which can monitor a network and react upon access of unwanted applications I quote from their web site:

> *"Sygate Secure Enterprise and Sygate On-Demand make sure that every endpoint in your enterprise — including laptops, desktops, and servers — connecting from any point – internal network, partner locations, home, hotel kiosks, or airport terminals – runs the correct patches, intrusion prevention, host firewall, and antivirus software before being permitted to connect to the corporate network."*[21]

The product that Sygate offers is very promising. It consists of three components, namely: Sygate Management Server, Sygate Security Agent and Sygate Universal Enforcement. The Management Server holds the policies for the network. When a client wants to connect to the network it has to connect to the Management Server and verify that it is complaints with the policies of the network. Sygate Universal Enforcement offers an API from which third party vendors can verify the existence and operation of a Sygate Security Agent. Furthermore the Sygate LAN enforcer, which is part of the Sygate Universal Enforcement, works with 802.1x to ensure that devices connecting to the network are authenticated and compliant with network security policies before granted access to ports on the switch for example. For further information about the Sygate suite I refer to the Sygate web site[22].

Solsoft

Solsoft is a direct competitor to Sygate they also provide a policy server application that can enforce the security policy of the network devices of the company. The Solsoft product supports a number of vendors including: Cisco, Juniper, Check Point, Nortel and Symantec. Like Sygate they have an API to ease integration with other third party products. Solsoft is only focused at the network and gateway devices like switches, firewalls and proxy servers. There does not seem to exist a security agent to enforce policies on clients in the Solsoft security suite. For further information about Solsoft I refer to their web site[23].

[21] [SYGATE]
[22] [SYGATE1]
[23] [SOLSOFT]

Symantec Enterprise Security Manager

The ESM from Symantec is used to validate the security policy of an entire enterprise. It works together with other Symantec modules to ensure that applications and databases are configured in compliance with the security policy. An operating specific agent is installed on the clients and servers on the network. The agents can make all kinds of checks including minimum and maximum password aging, file permissions and windows registry auditing. This information is gathered from the clients and servers can be used to verify and secure the configuration of the clients connected to the network. I quote from their web site[24]:

> *"Working within the framework of Symantec Enterprise Security Manager, the industry's most comprehensive solution for discovering security vulnerabilities, ESM regulatory modules ease the administrative burden of measuring the effectiveness of enterprise security policies and enforcing compliance. With the regulatory policies, ESM's centralized security scanning and integrated reporting capabilities can be utilized to automate security evaluations and policy enforcement for each server's operating system to protect them from security vulnerabilities.*
>
> *Current Symantec Enterprise Security Manager application modules include Symantec ESM for Databases (Oracle, DB2), Symantec ESM for Web Servers (Apache, IIS, and SunONE), and Symantec ESM for HIPAA."*

Summary

There are different approaches to policy enforcement on the devices connected to the network. Anti virus vendors have made specific implementations that make it possible to enforce the configuration of anti virus products on clients and servers. F-Secure have further more extended the enforcement to include which applications on a client can access the network.

The firewalls vendors are primarily concerned with which processes can utilize the network and which access is granted. This is a nice feature to protect the hosts from the network – and the network from the hosts.

Trend Micro's *Vulnerability Scanner* makes it possible to detect clients that are connected to the network but does not have anti virus installed. This is an approach that is better than nothing but not optimal, since the unprotected clients are still allowed to connect to the network initially before the vulnerability scanner might find them. A much better approach

[24] [SYMANTEC]

used by Sygate is to use agents to enforce that the switches only accept connections from devices that have an active security agent running and that the agent have approved the device by checking a wide range of different criteria's. The criteria's can include specification of how the host based firewall or anti virus software is configured.

The Cisco and Trend Micro joint venture seems promising. If the AV software detects a pattern, the switch will proactively shut down access to the network to block worms and other mal-ware.

The Symantec Enterprise Security Manager is probably the product that comes closest to the thoughts presented here on how to automate the implementation of a written security policy. They make use of modules that enforce predefined policies on different platforms. This means that one can have a module that will harden windows in accordance with HIPAA for example.

Future state

The future calls for standardization, the Sygate, Symantec and Solsoft products are definitely a step in the right direction in my opinion. The problem is that they support a limited number of vendors and they have there own standards and conventions for how things are done.

In the near future I believe that there need to be implemented standards for how to describe applications and devices configurations and settings. This will enable policy enforcement agents to ensure that the applications and devices are complying with best practice and the security policy of the enterprise.

The scenario might be similar to the way things have evolved in the AV business. All the vendors collect and develop signatures and then release them to customers so they can be used in scan engines around the world to identify viruses. Imagine if signatures for programs and network devices were released along with the programs. The signatures would contain the standard setting and configuration of the program as well as the security parameters that should be set and so on. If a setting were found to be insecure a new signature could be released and the policy enforcement agents would be able to reconfigure faulty applications and programs. The signatures could also contain patches and would thereby be some kind of hybrid of a configuration/patch/update.

For this scenario to be a success a standard format should be developed for these signature files. This would be necessary to ensure that different vendors would comply with the policy enforcement agents.

There might be a database like the OSVDB that contained signature files for applications and devices. The ideal situation would be that the format of the signature files was easy to edit and define (e.g. XML), so people could submit improved signatures to applications and devices. At least the configuration part of the signature should be editable by the public, while the patch part would probably be limited to the vendors in the case of source code any way. This would also be a uniform central channel for vendors to submit patches and updates.

An important point to make is that adhering to the security policy of the enterprise involves all the applications running on the host not only the host based anti virus program or firewall. A unified interface to how applications and programs are configured will greatly simplify the design of a general-purpose policy enforcement agent.

Initial problems

To be able to have a policy enforcement agent (PEA) check that all clients on a network are actually adhering to the security policy of the enterprise, standardization is needed. E.g. it would have to be defined what secure password policy means on Windows as well as on Linux and how to check it. The agents would have to know details about all the applications and settings on different platforms and OS that are supported.

The configuration and settings of applications as well as OS specific parameters would have to be defined and standardized to make it possible to develop agents that could check if a given client is adhering to a security policy. This is probably the biggest hurdle. One idea would have to have standards and best practices for common application in an easy parse able format on a shared open database.

Today there are best practices for how to configure the Exchange server for example that can be found on the MS website[25]. Resources for all client applications and server applications would have to be available in a format that could be interpreted and compiled into the security agents so they could check if the parameters and settings of a given application adhered to best practice and the security policy of the network.

A whole other standardization problem would arise with the part of the security policy that should be enforced by servers and gateways. First of all there had to be defined what kind of services the gateway should be able to perform e.g.:

The firewall should for example control:

- Traffic shaping

[25] [MS2]

- Protocols used
- Ports used
- Real time scanning of traffic

While the mail server should be capable of doing:

- Limits on size of mail
- Blacklists
- Spam and virus filtering
- Relay politics

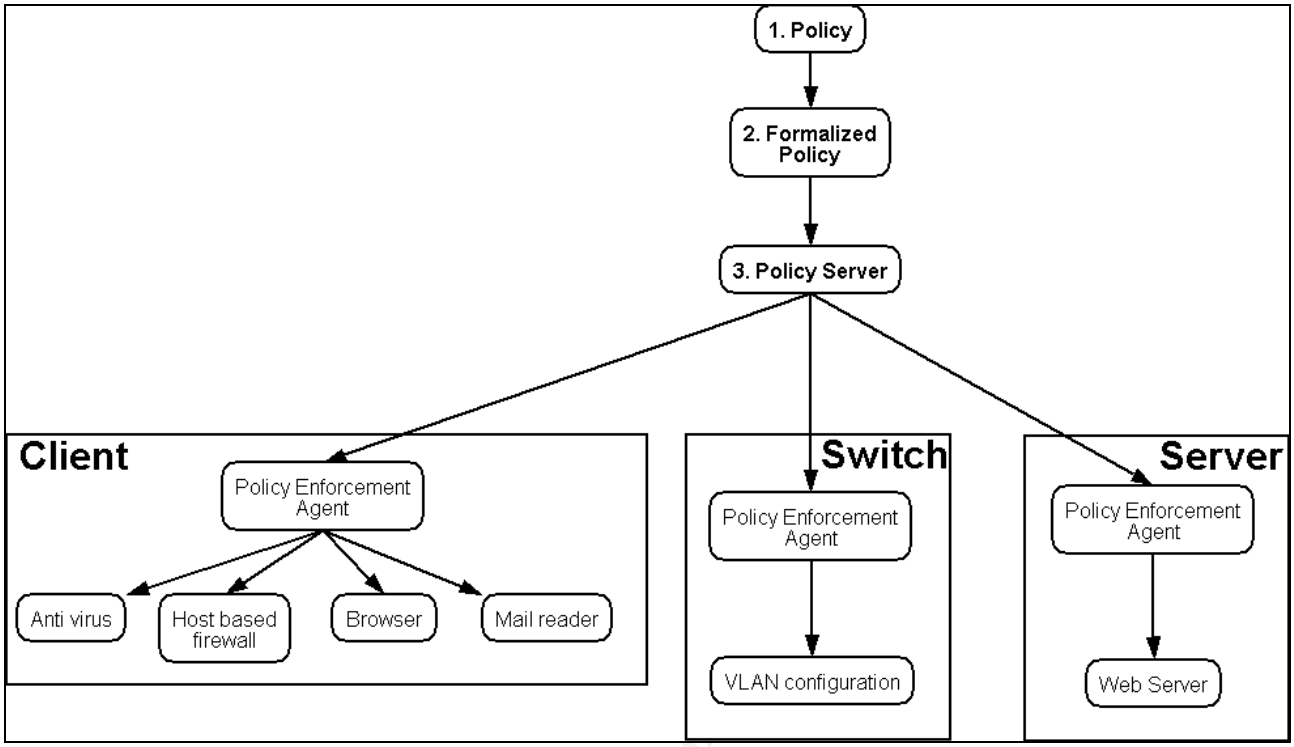
So the first step would be to standardize the border components of the network as well as the applications on clients and servers, so the agents had a uniform set of parameters and settings to work with.

Another aspect of the standardization would involve how to convert the written security policy to a format that could be parsed by the agent program.

Formalizing a security policy

Figure 23 - Deploying Security Policy shows how the security policy is deployed in the network from the initial written policy as presented in Figure 22 - Mindmap to the local PEA running on the client, server or device (here a switch). On the figure it appears that the PEA is running on the switch, this would require the producers of switches to adhere to the standard and implement some kind of generic PEA, which might not be realistic. Another approach that both Sygate and Solsoft have chosen is to make the policy server run the agent and then interface to a bunch of vendors.

Figure 23 - Deploying Security Policy



To formalize a policy standards to a standardized format that can be enforced automatically there have to be developed a method or best practice for how to extract the formalized policy from the written policy.

A recipe for formalizing a security policy, could be something like:

1. Identify the written policies that are related to the network. This includes client, servers and other network devices.
2. Identify the policies that are related to configuration or restriction of applications or services running on the network or devices connected to the network, from the subset found in 1.
3. Write them in a *standardized policy format* (SPF), this could for example be a XML format.

When the security policy of the Enterprise have been transformed to the SPF it is possible to feed it directly to the Policy Server that instructs the PEA's securing the network. An example of a pseudo SPF file could be:

```
<vendor name=superAV>
  <product id=Avscan>
    <parameter>
      <scaninterval>3600</scaninterval>
    </parameter>
    <parameter>
      <security>high</security>
    </parameter>
  </product>
</vendor>
```

Security Agents

The future state might be in the hands of agents that are spreading on the network and checking that everything is all right and everybody is adhering to the policies of the enterprise. Imagine an agent that is designed like a virus or worm, the only difference is that you **have** to be infected with it to gain access to then network. This is already a reality with Sygate for example.

Security agents might be the future authentication mechanism. A day may come when severe interrogation is needed in order to access specific network resources. Besides checking running software and processes on the connecting client, the security agent program might also be the primary authentication mechanism utilizing fingerprint, iris scanning and DNA analysis of the user.

Using security agent programs, that are similar to worms or viruses mitigate several problems. What if a security agent program is compromised and modified? Then it might turn into a terrible virus that is actually controlling the network. How should agents be stopped and limited? What should they be able to check and how much control should they be granted? Should there be meta-security agents that could control the security agents them self?

There are many questions to be asked and many answers to be found before we live in a world where the network is kept nice and clean by automatic security agents making sure that everybody is adhering to best practice and generally not making trouble – on the network that is.

Thin Clients

The use of thin clients actually eliminates many of the network security issues discussed here. In a setup with thin clients the network is only used for sending screen dumps from the server to the client and user actions from the client to the server. Applications and data are processed centrally on the server. This way nothing is or can be installed on the clients

and nothing is processed other than the graphic received from the server, which is just displayed.

With thin clients it would be much easier to enforce a security policy because you would only need to enforce the security on the central server and all applications would be installed and configured centrally.

The future might be thin clients. Imagine you have to rent MS Word for half an hour and you will just receive the screen dumps of the MS Word program you will never have it installed. This makes it flexible because you can use your television for example and you would not have to worry about the processing power or the speed of the graphic card. On the other hand you will have no control and your rights to privacy will depend on the company that you buy services from. So I believe there is a long way both regarding laws and privacy but also technological. Such a service that rented out programs would require 99.99% stable Internet connections, low latency and high speed. The global network is simply not mature for that yet.

Thin clients might be an option inside an enterprise. But there are several issues that must be considered. It is quite expensive to setup since there is a demand for powerful servers with redundancy to guarantee uptime. Customization is another issue. Software developers for example has to experiment and compile programs and often require an open customizable environment, this might not be possible. Yet another issue is the road warriors. If there is a mobile sales force like in the GIAC Enterprise it might not be possible for them to hook up with the central server when they are visiting customers or staying at a hotel. This is another possible direction, for future networks, but there are other issues as presented here, that have to be worked out.

Conclusion

It is not the technological development that stops the approach of using security PEA's; rather it is the lack of standards on how information security should actually be implemented. There are several standards and best practice documents like the BS-7799 but there is still some standardization to be done before the whole infrastructure of information technology will be uniform enough to implement the thoughts presented here.

The development of thin clients might be another direction in which the network and thereby security will evolve. Before the Internet will evolve in that direction, I believe that the whole infrastructure of the Internet generally have to be more stable and reliable.

References

[ARMSTRONG] Mike Armstrong. GCFW version 3.0. 04/04
URL: http://www.giac.org/practical/GCFW/Mike_Armstrong_GCFW.pdf

[BASTILLE] Bastille Linux. Latest stable Debian release 1.3.0-2.1.
URL: http://www.bastille-linux.org

[BITGUARD] tryus.dk, gn@tryus.dk. Bitguard Personal Firewall.
URL: http://www.tryus.dk/bitguard.asp?lang=en&

[BUGTRAQ] BugTraq mailing list.
URL: http://www.securityfocus.com/archive/1

[CISCO1] Cisco Systems. Virtual LAN Security Best Practices. 12/02.
URL: http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.pdf

[CISCO2] NSA/SNAC Router Security Configuration Guide – Executive Summary. Version 1.1. 02/03
URL: http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1

[CISCO3] Akadia Information Technology
URL: http://www.akadia.com/services/cisco_router_firewall.html

[CISCO4] Frank Keeney. 12/98
URL: http://www.pasadena.net/cisco/secure.html

[CVS] URL: http://www.cvshome.org

[CVS1] Anonymous. CVS Remote Entry Line Heap Overflow Root Exploit.
URL: http://www.securiteam.com/exploits/5WP0L0UCUO.html

[CVS2] Morgon Kanter. Secure CVS Pserver Mini-HOWTO. 2003
URL: http://www.tldp.org/HOWTO/Secure-CVS-Pserver/setuptools.html

[CVS3] US-CERT. CVS HEAP Overflow Vulnerability. Technical Cyber Security Alert TA04-147A
URL: http://www.us-cert.gov/cas/techalerts/TA04-147A.html

[DS1] Danish Standards Association. DS 484-1.
URL:
http://www.en.ds.dk/iLink?ident=misSogResultShow&misProjektDetail_projekt=38364

[DS2] Danish Standards Association. DS 484-2.
URL:http://www.en.ds.dk/iLink?ident=misSogResultShow&misProjektDetail_projekt=38409

[FSEC] F-Secure Corporation. F-Secure Internet Security 2004. 04
URL: http://www.madesafe.com/2004/UK/support/docs/madesafe_iss_manual.pdf

[HOTMAIL] GreyHats. Hotmail XSS Vulnerability.
URL: http://freehost07.websamba.com/greyhats/

[INFOW] Ellen Messmer, Network World Fusion. Trend Micro, Cisco to fight worms. 06/04.
URL: http://www.infoworld.com/article/04/06/08/HNtrendcisco_1.html

[INTEGRIT] The Integrit Project. Latest release 3.02.00-stable
URL: http://integrit.sourceforge.net/

[IPAUDIT] IPAudit latest release IPAudit beta 9 2004.02.22
URL: http://ipaudit.sourceforge.net/index.html

[IPT1] Peter Harrison, www.linuxhomenetworking.com. Iptables Packet Flow Diagram, Linux Firewalls Using iptables.
URL: http://www.siliconvalleyccie.com/linux-hn/iptables-intro.htm#_Toc80458412

[IPT2] Oskar Andreasson. Iptables Tutorial. Section 4.2 The Conntrack Entries. version 1.1.19. 2003.
URL: http://iptables-tutorial.frozentux.net/iptables-tutorial.html#STATEMACHINE

[LIDS] Yusuf Wilajati Purna. LIDS Trusted Path Execution (TPE). 09/04.
URL: http://www.lids.org/document/LIDS-TPE-feature.txt

[LIDS1] Linux Intrusion Detection System. Last Release 08/04
URL: http://www.lids.org

[LINSEC] linuxsecurity.com Resources.
URL: http://www.linuxsecurity.org/docs/

[LSH] Rob Flickenger. Linux Server Hacks – 100 Industrial-Strength Tips & Tools. O'Reilly & Associates, Inc. 2003. 87-94, 139-146.

[MCINTOSH] Brett McIntosh. Secure Configuration of a Cisco 837 ADSL Firewall Router. GSEC version 1.4. 08/02.

[MS1] Microsoft Corporation. MS-CHAP version 2. 02/00.
URL:
http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_RASS_MSCHAPv2.htm

[MS2] Microsoft Corporation. Best Practice Active Directory Design for Exchange 2000. 11/02.
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=F53662B9-4E69-40CE-AA19-7B0C48710403&displaylang=en

[NETSQUID] Ellen Mitchell, splunty, Mark Nipper, Mike Sconzo, Dave Duchscher, Daryl Hawkins, Kristen Kubenka. Current Version: 1.4.2 - Released 8.10.2004.
URL: http://netsquid.tamu.edu/main.html

[OPENWALL] Linux kernel patch from the Openwall Project. Release 08/04.
URL: http://www.openwall.com/linux

[RFC-1918] Y. Rekhter - Cisco Systems; B. Moskowitz - Chrysler Corp.; D. Karrenberg - RIPE NCC; G. J. de Groot - RIPE NCC; E. Lear - Silicon Graphics, Inc. RFC 1918. 02/96.
URL: http://www.rfc-editor.org/rfc/rfc1918.txt

[SANS] URL: http://www.sans.org

[SECCVS] Morgon Kanter. Secure CVS Pserver Mini-HOWTO. Revision 1.1. 03/03
URL: http://www.tldp.org/HOWTO/Secure-CVS-Pserver/setuptools.html

[SECFOC] URL: http://www.securityfocus.org

[SOLSOFT] URL: http://www.sygate.com/

[STEPANOV] Serge Stepanov serge@gfxcafe.com. PoPToP PPTP + MPPE 128bit Encryption + MPPC Compression VPN Server. Last revision 08/04.
URL: http://gfxcafe.com/VPN%20Howto.html

[SUB7] Mobman. SUB7 Trojan.
URL: http://www.hackemate.com.ar/sub7/

[SYGATE] Audra Eng. Sygate Secure Enterprise 4.0. 07/04.
URL: http://www.sygate.com/solutions/datasheets/wp/WP-Sygate-Secure-Enterprise.pdf

[SYGATE1] URL: http://www.sygate.com/

[SYMANTEC] Symantec Enterprise Security Manager for HIPAA.
URL:
http://enterprisesecurity.symantec.com/products/products.cfm?productid=162&EID=0

[TLDP] The Linux Documentation Project. Revision 1.4 (05/04).
URL: http://www.tldp.org/

[TLDP1] Gerhard Mourani and Open Network Architecture, Inc. Securing and Optimizing Linux: The Ultimate Solution. Revision 2.0 (06/2001). Published 06/2000.
URL: http://www.tldp.org/LDP/solrhe/Securing-Optimizing-Linux-The-Ultimate-Solution-v2.0.pdf

[USCERT] URL: http://www.us-cert.gov/current/

[ZONEA] URL: http://www.zonealarm.com

Background Literature

[ANTI] Keith J. Jones, Mike Shema, Bradley C. Johnson. Anti-Hacker Tool Kit. McGraw-Hill/Osborne. ISBN 0-07-222282-4. 2002.

[DATA] William Stallings. Data and Computer Communications. Fifth Edition. Prentice Hall. ISBN 0-13-571274-2. 1997

[HACK] Stuart McClure, Joel Scambray and George Kurtz. Hacking Exposed: Network Security Secrets & Solutions, Fourth Edition. McGraw-Hill/Osborne. ISBN 0-07-222742-7. 2003.

[IANA] Internet Assigned Numbers Authority
URL: http://www.iana.org/

[IPT] Oskar Andreasson. Iptables Tutorial. version 1.1.19. 2003.
URL: http://iptables-tutorial.frozentux.net/iptables-tutorial.html#RCDMZFIREWALLTXT

PPTP Server on Debian 3.0 (Woody)

Installation of PoPTop under Debian Woody:
http://gfxcafe.com/VPN%20Howto.html

ppp: ftp://ftp.samba.org/pub/ppp/ppp-2.4.2.tar.gz
patch: http://www.polbox.com/h/hs001/ppp-2.4.2-mppe-mppc-1.0.patch

```
$apt-get install libnet0-dev
$ tar zxvf ppp-2.4.2.tar.gz
$ patch -p0 -i ppp-2.4.2-mppe-mppc-1.0.patch
$ cd ppp-2.4.2
$ ./configure
$ make
$ make install (as root)
```

```
$modprobe ppp_mppe_mppc
```

Setting up PoPTop

```
$ tar zxvf pptpd-1.1.4-b4.tar.gz
$ cd poptop-1.1.4
$ ./configure
$ make
$ make install (as root)
```

Kernel compilation – the Debian way

One important thing when securing the kernel is to recompile it and make a stripped down kernel image. In this example I also add support for RAID.

First the needed packages are retrived from the apt repository:

```
$apt-get install \
debhelper
kernel-package
modutils
fakeroot
kernel-source-2.4.18 \
lm-sensors-source \
kernel-patch-preempt-2.4 \
```

```
kernel-patch-badram \
kernel-patch-irc \
kernel-patch-ttl \
kernel-patch-ulog \
raidtools2 \
mdadm \
gcc \
libc6-dev \
libncurses5-dev
```

Unpack the kernel sources

```
$cd /usr/src
$tar xjvf kernel-source-2.4.18.tar.bz2
$ln -s kernel-source-2.4.18 linux
$cp /boot/config-2.4.18-bf24 linux/.config
$cd linux
$make oldconfig
```

```
$vi Makefile
EXTRAVERSION = <kernel identifier e.g. raid-1>
```

Configure the kernel. This is the step where everything that is not needed is removed.

```
$make menuconfig
```

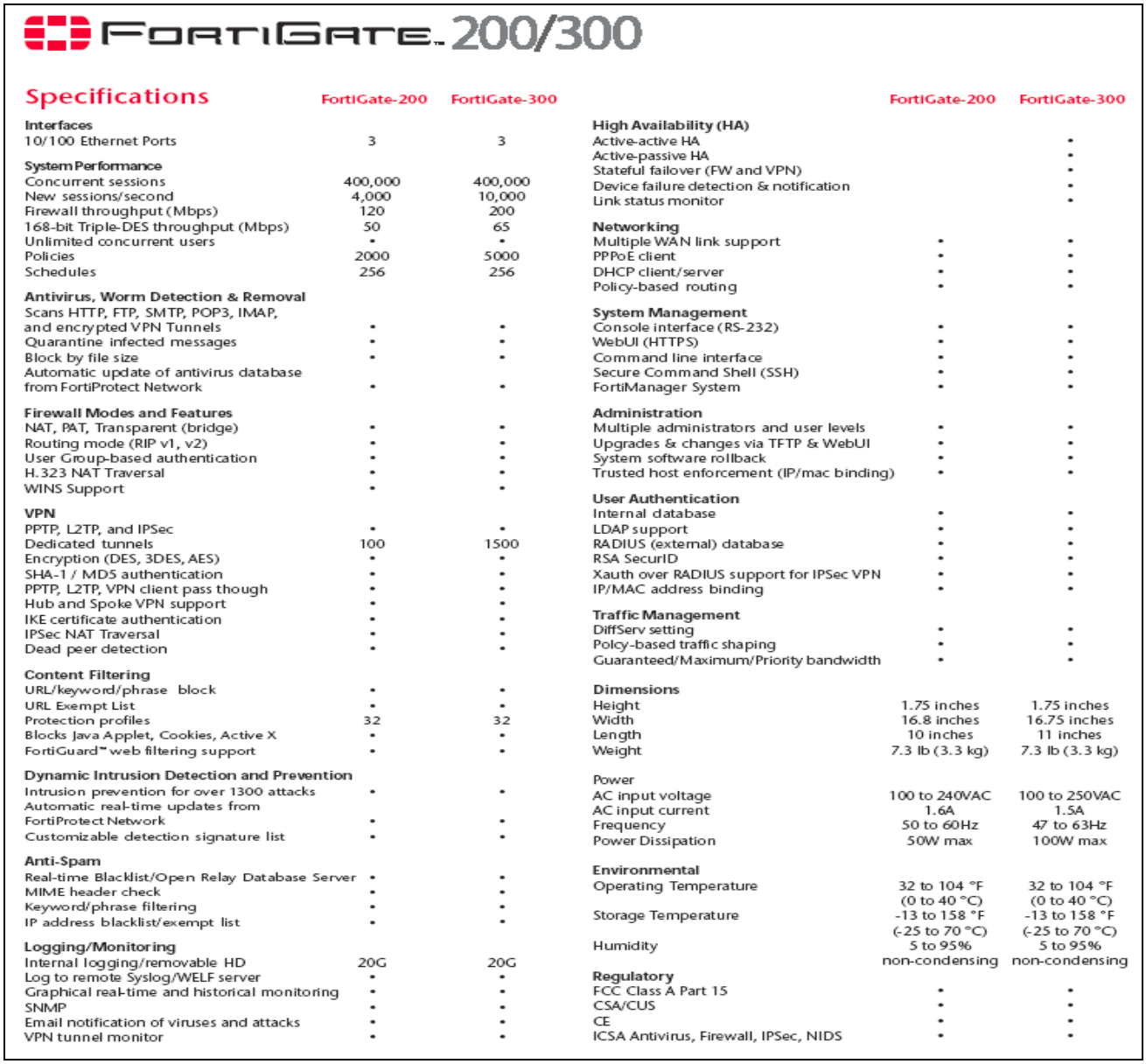
Setup the RAID support as compiled into the kernel

```
$make-kpkg clean
$fakeroot make-kpkg --append_to_version -486 --revision=rev.01 --
bzimage \ kernel_image modules_image
$cd ..
$dpkg -i kernel-image*.deb
```

Fortigate specification

The Fortigate-200 firewall has an incredible amount of functionality for one box. Figure 24 - Fortigate-200 specification Shows the specification taken from the www.fortinet.com.

Figure 24 - Fortigate-200 specification



FortiGate 200/300

Specifications	FortiGate-200	FortiGate-300
Interfaces		
10/100 Ethernet Ports	3	3
System Performance		
Concurrent sessions	400,000	400,000
New sessions/second	4,000	10,000
Firewall throughput (Mbps)	120	200
168-bit Triple-DES throughput (Mbps)	50	65
Unlimited concurrent users	•	•
Policies	2000	5000
Schedules	256	256
Antivirus, Worm Detection & Removal		
Scans HTTP, FTP, SMTP, POP3, IMAP, and encrypted VPN Tunnels	•	•
Quarantine infected messages	•	•
Block by file size	•	•
Automatic update of antivirus database from FortiProtect Network	•	•
Firewall Modes and Features		
NAT, PAT, Transparent (bridge)	•	•
Routing mode (RIP v1, v2)	•	•
User Group-based authentication	•	•
H.323 NAT Traversal	•	•
WINS Support	•	•
VPN		
PPTP, L2TP, and IPSec	•	•
Dedicated tunnels	100	1500
Encryption (DES, 3DES, AES)	•	•
SHA-1 / MD5 authentication	•	•
PPTP, L2TP, VPN client pass though	•	•
Hub and Spoke VPN support	•	•
IKE certificate authentication	•	•
IPSec NAT Traversal	•	•
Dead peer detection	•	•
Content Filtering		
URL/keyword/phrase block	•	•
URL Exempt List	•	•
Protection profiles	32	32
Blocks Java Applet, Cookies, Active X	•	•
FortiGuard™ web filtering support	•	•
Dynamic Intrusion Detection and Prevention		
Intrusion prevention for over 1300 attacks	•	•
Automatic real-time updates from FortiProtect Network	•	•
Customizable detection signature list	•	•
Anti-Spam		
Real-time Blacklist/Open Relay Database Server	•	•
MIME header check	•	•
Keyword/phrase filtering	•	•
IP address blacklist/exempt list	•	•
Logging/Monitoring		
Internal logging/removable HD	20G	20G
Log to remote Syslog/WELF server	•	•
Graphical real-time and historical monitoring	•	•
SNMP	•	•
Email notification of viruses and attacks	•	•
VPN tunnel monitor	•	•

	FortiGate-200	FortiGate-300
High Availability (HA)		
Active-active HA		•
Active-passive HA		•
Stateful failover (FW and VPN)		•
Device failure detection & notification		•
Link status monitor		•
Networking		
Multiple WAN link support	•	•
PPPoE client	•	•
DHCP client/server	•	•
Policy-based routing	•	•
System Management		
Console interface (RS-232)	•	•
WebUI (HTTPS)	•	•
Command line interface	•	•
Secure Command Shell (SSH)	•	•
FortiManager System	•	•
Administration		
Multiple administrators and user levels	•	•
Upgrades & changes via TFTP & WebUI	•	•
System software rollback	•	•
Trusted host enforcement (IP/mac binding)	•	•
User Authentication		
Internal database	•	•
LDAP support	•	•
RADIUS (external) database	•	•
RSA SecurID	•	•
Xauth over RADIUS support for IPSec VPN	•	•
IP/MAC address binding	•	•
Traffic Management		
DiffServ setting	•	•
Policy-based traffic shaping	•	•
Guaranteed/Maximum/Priority bandwidth	•	•
Dimensions		
Height	1.75 inches	1.75 inches
Width	16.8 inches	16.75 inches
Length	10 inches	11 inches
Weight	7.3 lb (3.3 kg)	7.3 lb (3.3 kg)
Power		
AC input voltage	100 to 240VAC	100 to 250VAC
AC input current	1.6A	1.5A
Frequency	50 to 60Hz	47 to 63Hz
Power Dissipation	50W max	100W max
Environmental		
Operating Temperature	32 to 104 °F (0 to 40 °C)	32 to 104 °F (0 to 40 °C)
Storage Temperature	-13 to 158 °F (-25 to 70 °C)	-13 to 158 °F (-25 to 70 °C)
Humidity	5 to 95% non-condensing	5 to 95% non-condensing
Regulatory		
FCC Class A Part 15	•	•
CSA/CUS	•	•
CE	•	•
ICSA Antivirus, Firewall, IPSec, NIDS	•	•