Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)
Practical assignment (v1.7)

Author: Paul Carr
Date: September 2002

Table of contents:

0 Summary

This paper consists of 4 assignments:

1. Provide a security architecture for GIAC Enterprises, a fictive company
2. Provide a security policy and tutorial for how to implement it for GIAC Enterprises. The policy must cover border routers, primary firewalls, and VPNs.
3. Verify the Firewall policy.
4. Design attacks on a previously posted practical.

The architecture chosen is a simple architecture using Cisco and Checkpoint solutions for the routing, firewalls, and VPN solution. The security policy tutorial goes into detail on the b order router policy, which has a fairly strict “deny anything that isn’t specifically required” ground rule.

The firewall policy is tested using various methods, mainly manual methods and the use of the nessus tool.

Finally the practical assignment produ ced by Steve Keifling (June 5, 2002) is used as a basis for designing attacks. The architecture of that practical is fairly sound, so little damage may be done (if the system is managed properly, and if the web application is tested for vulnerabilities).

1 Assignment 1 – Security architecture

1.1 Requirements

The first step in an architecture design is to establish the requirements in a way that can be used to design the solution. This chapter describes the requirements of GIAC Enterprises, relating to secur ity.

1.1.1 Security principles

The requirement for the security architecture for GIAC Enterprises has been broken down into the following principles that will be used in the design (these are assumptions that have been verified by management):

1. Investment costs are not a major concern
2. The ongoing operations costs must be kept low (this is an overall strategy for the company, and the number of staff in total is very low)
3. It must be very easy to access the systems, in particular for partners and customers
4. Access must be provided only to those services that are required
5. The architecture must be flexible to allow future growth with little or no disruption
6. The architecture must allow 24/7 uptime
7. Availability is the major security requirement, it is more important tha n confidentiality and integrity.
8. GIAC Enterprises must not be used as a vehicle for attacks on other Internet users

1.1.2 Earlier decisions

We may design the network and security architecture the way it best fits the requirements and principles above, however the following architecture components are already decided as part of an earlier architecture project:

- An application server based on Websphere, running on a Windows 2000 machine, running the main applications (component “APPL svr”).
- A WEB server based on Apache, running on a Windows 2000 machine (Component “WWW”).
- An Oracle database server (Component “DB”).
- A mail server based on MS Exchange, running on a Windows 2000 machine (Component “MAIL”).

- Clients for all internal staff, based on Compaq laptop computers, running Windows 2000.
- Office tools on each client, based on Office 2000.
- Microsoft IE v 5 used as standard for all staff
- All central applications have a browser user interface

1.1.3 Access requirements

Below is a list of access requirements, as specified by GIAC Enterprises:

- All internal staff and external staff need access to all internal applications and functionality. Note that all GIAC Enterprises applications are WEB based, so the requirement is to access an Internal WEB server with further communication to the application server and database. The only exception is the mail server, which internally will be accessed from an MS Outlook client, but externally through a WEB client via the internal WEB server. In summary, this means that the only protocol required for staff working externally is HTTP (port 80). (Note however that later when we show how to handle this securely, this will be changed to a VPN connection).
- Incoming and outgoing mail is allowed via smtp (port 25)
- All customers, partners, and suppliers need read access to data. This is achieved by replicating the data with fortune cookie sayings to the external WEB servers. These are accessed by customers via HTTP/HTTPS (ports 80/443).
- All partners and suppliers need (restricted) write access. This is achieved by writing to the external WEB servers using HTTPS (port 443). Data is collected on a daily basis by the internal application server using ftp (ports 20 and 21).
- Name server (DNS) lookup access is required between internal and external DNS servers (port 53).

This list is expected to meet what is required for the day to day business of GIAC Enterprises. Note however that outgoing access to external WEB servers is not included in the list above. It is expected that later on this (and other) requirements will be identified, so the architecture must allow for such changes, but such access will not be set up initially.

1.2 Architectural security components

To design architecture, it is necessary to describe all the components of the architecture, as well as how these components fit together. This chapter describes each component used. Note that not all components used by GIAC Enterprises have been included here – only those relevant for the periphery security architecture. There are also other components on the internal GIAC Enterprises network, e.g. clients, components for the day-to-day operation, components for development and testing of new applications, etc.

1.2.1 General comments

All components are based on Microsoft or Cisco infrastructure when possible. The main reason for this is that it is easy to get hold of staff that master one or both of these environments, so staff costs can be kept low. Other reasons are: These environments are easy to get hold of for fast replacement or expansion if necessary, they support a large number of applications, it is easier to manage a standard environment, and systems based on a standard environment are easier to integrate. Note that it is also easier for a hacker [1] to penetrate a standardised environment like this, but it is also easier to maintain a good level of security patching, and most hackers exploit old and well known vulnerabilities that are easy to fix. The Windows 2000 based servers need to be hardened in line with recommendations from Microsoft.

1.2.2 Component FIREWALL

Description:
Checkpoint Firewall-1 running on two Windows 2000 machines in a Stonebeat cluster. VPN functionality must be enabled. NAT must also be used to hide the internal network addresses. Note that the Stonebeat cluster requires a separate console for management.
See http://www.checkpoint.com and http://www.stonesoft.com/

Justification:
Checkpoint Firewall-1 is one of the leading firewalls in the market. It is also very easy to manage compared with other firewalls like PIX from Cisco. Together with Stonebeat clustering technique it provides very high uptime figures, and the possibility to add more machines without downtime, both of which are architecture principles mentioned earlier. Using VPN functionality here rather than buying a separate VPN box provides a simpler solution that is easier to manage, but has the disadvantage that it is not possible to investigate the unencrypted VPN traffic before it has been filtered or modified by the firewall. The additional load caused by the VPN encryption is not thought to be a major concern as there are not many expected users of the VPN system. The choice of running on Windows 2000 is to comply with the standard Microsoft environment to allow easy operation. Note that this is not the most efficient device for running Firewall-1, but the cost of two powerful Windows 2000 machines is not a major concern (ref. first principle stated in chapter 1.1.1). Also note that Checkpoint now have their own cluster solution – this is however fairly new, and Stonebeat was chosen due to it's good references and long history of good performance.

1.2.3 Component ROUTER

[1] Note that I have used the term "hacker" in it's negative sense throughout this document, instead of using the more correct term cracker. The reason is that the term hacker is better recognisable.

Description:
The border router selected is a Cisco 7140 router runnin g IOS v12.0. The router has one WAN connection to an ISP and one LAN connection. A second router of the same type is set up with a connection to another ISP for redundancy, to support the principle of 24/7 availability.
See http://www.cisco.com/univercd/cc/td/doc/pcat/7100.htm

Justification:
Cisco are market leaders regarding routers, and their products are well known and easy to manage. The 7140 is a fairly new router, and has 2 power supplies to ensure high uptime (power supply failure is one of the most common failures). The router is also expandable if required for up to 8 WAN connections. If required it can be set up with NAT, and/or used as an end point for VPN traffic (it has a h ardware encryption accelerator).

1.2.4 Component LB SWITCH

Description:
Cisco catalyst 4840G, with 40 possible connection points. The switch also has routing and load balancing functionality.
See http://www.cisco.com/univercd/cc/td/doc/pcat/ca4840g.htm

Justification:
The switch is a very important component, as it handles all the internal traffic routing and filtering, as well as the load balancing. The switch will allow easy growth (part of the initial requirement) up to 40 boxes per switch. It was considered to duplicate the switch to increase availability, but the switch is fairly stable, so it was decided against due to the high cost. Note that the load balancing functionality is n ot (yet) required for the internal switch (see drawing later).

1.2.5 Component HUB

Description:
A Cisco 1538 is used.
See: http://www.cisco.com/univercd/cc/td/doc/pcat/1538.htm

Justification:
This was selected for it's low price – any hub with enough interfaces would be acceptable.

1.2.6 Component MAIL RELAY

Description:

The mail relay server is not described here, as it is out of scope of the security architecture.

1.2.7 Component IDS

Description:
The Intrusion Detection system will be based on SNORT running on a Windows 2000 machine.
See: http://www.snort.org

Justification:
Several other systems where evaluated: NFR, Cisco Secure IDS, BlackICE, and ISS Realsecure. These systems all have an associated investment and maintenance cost that SNORT does not have, without providing noticeably better protection. SNORT does not provide such a user -friendly user interface, but this is not considered a major disadvantage once the IT staff have learnt to use the system.
For another evaluations, see also:
http://www.scmagazine.com/scmagazine/2001_12/pickof2001/c14/index.html

1.2.8 Component VIRUSWALL

Description:
Trend Viruswall running on a Windows 2000 machine. This will inspect any traffic: mail messages, html, or other as required, also in winzip format.
See: http://www.trendmicro.com/products/isvw/

Justification:
Trend Viruswall is one of the market leaders and one of the first to supply virus control at the perimeter, instead of the traditional checking only on the servers. Note however that server virus checking should still be performed, for many reasons (e.g. in case of virus signatures being supplied after infection, or viruses entering the network via other methods).

1.2.9 Component: AUTHENT

Description:
Authentication for customers, partners and suppliers is done within the WEB server with simple username and password, rather than using a separate authentication server. All information is encrypted using SSL, starting with access from the login screen. However, GIAC Enterprises staff will require an authentication server for access when working externally. The details of this server are not specified here.

Justification:
A separate authentications system for all users like Tivoli, Netegrity or Entrust systems was considered, but seemed too costly and complex for the simple

requirement of this system. Note that confidentiality and integrity requirements are not particularly high (ref: architecture principles). However access to GIAC Enterprises internal network (only provided to GIAC Enterprises staff) needs to be protected better and a separate (but simple) authentication server is required for them. Uptime requirements for authentication of external staff is also less than for authentication of customers.

1.2.10 Component: CRYPT

Description:
SSL encryption is done on a separate SONICWALL encryption server. Note this does not cover the encryption performed as part of the VPN connections – this is performed by the firewall.
See http://www.sonicguard.com/

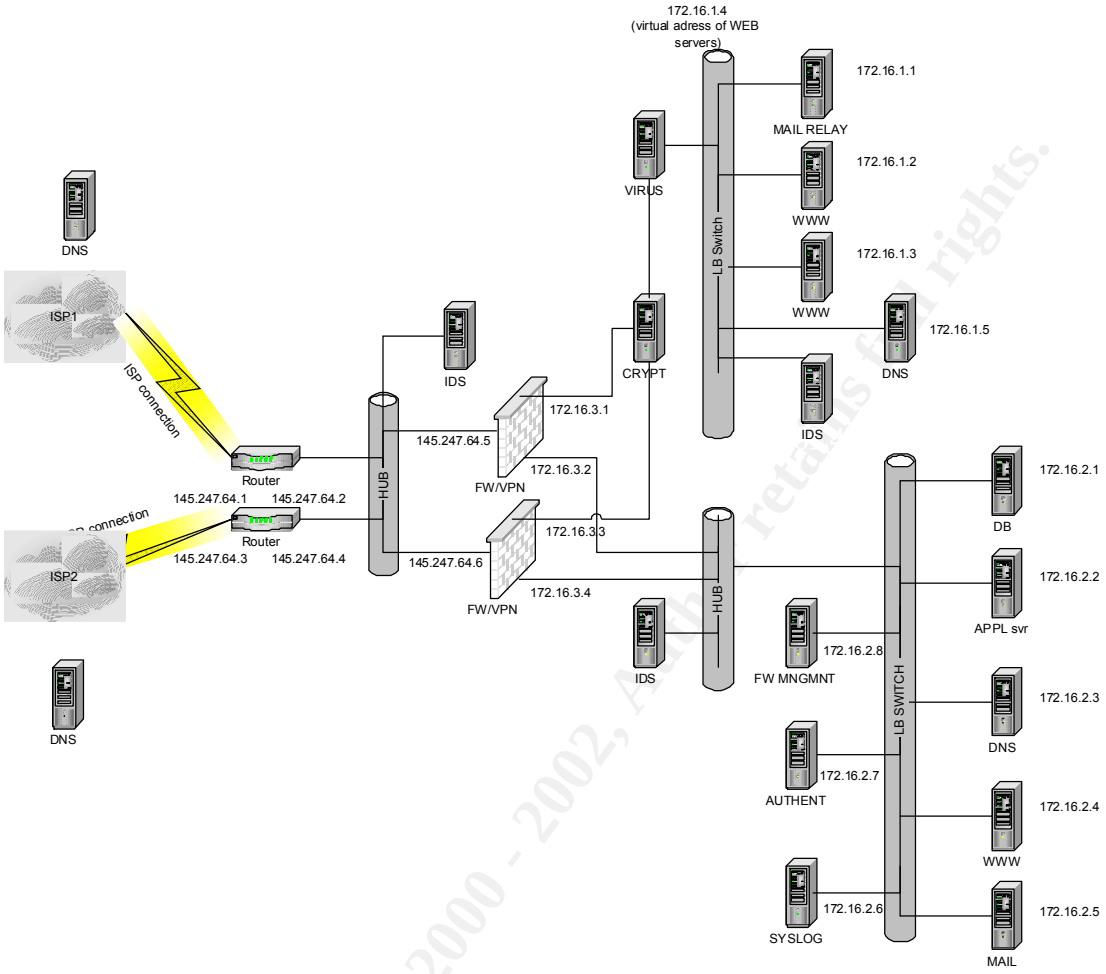
Justification:
An encryption server is required to offload the web server with the SSL encryption and decryption, and to allow easy growth. The reason for using a separate server rather than an accelerator card on the web server itself, is to allow interpretation of the decrypted traffic by the IDS system. The particular server chosen is due to its' performance and ease of setup. Note that Intel Netstructure was considered as well and would be equally acceptable.

1.3 How the components fit together

This chapter describes how the components mentioned earlier fit together.

On the next page is a drawing showing all the components, their names, and their IP addresses.

GIAC Enterprises have obtained the address space 145.247.64.0 to 145.247.64.255. This is used for all external communication. Internally they use private addresses in the range 172.16.0.0 to 172.16.255.255.



Description:
This is an explanation of the drawing, starting from the Internet connections (left side of the drawing):

The Internet connection is via two separate ISPs to two separate routers (using one AS number), to allow full redundancy and also to protect against DOS attacks. In addition agreements are set up with the ISPs on handling DOS attacks or any hacker activity to ensure the hacker is cut of before reaching the outer router, when possible.

Name resolution for external users will be handled by DNS servers at each ISP.

The external routers are set up with simple filtering.

Inside the routers is an IDS system to detect any traffic anomalies before reaching the firewalls. Note that most traffic will be encrypted at this stage, so it will not have the ability to scan everything.

Next step is a Stonebeat Firewall -1 cluster. This is the endpoint for the GIAC Enterprises employees VPN tunnel. These will be linked on to the internal WEB server. All other traffic will be linked to the DMZ (on the top of the page). First it will go through the encryption servers which will handle all port 443 traffic, decrypt it, and change to port 80. Next step is the Virus scanner, that can stop known virus signatures. All traffic is then monitored by another IDS system, which now can see all the data as it is unencrypted.

On the DMZ there are two target systems: the web servers (load balanced by the switch to ensure high availability) and a mail relay server. These are the only components that communicate from the DMZ to the internal Zone, via the Firewalls. The DMZ contains a DNS server, that communicates with the DNS servers at the ISPs. Note that the ISPs must be informed of the NAT address of the DNS server in the DMZ (145.246.64.8) to allow communication.

The internal zone (in the bottom right side of the drawing) can only be reached via the VPN connected employees, or from the DMZ. In the internal zone, only the WEB server can communicate with the Internet, and only the mail server and application server can communicate with the DMZ. The Internal zone also has a dedicated DNS server, that communicates with the DNS server in the DMZ. Zone transfers are only allowed between these two DNS servers, not with servers outside of GIAC Enterprises.

Justification:
Every critical component has been duplicated, to allow high availability [2]. High capacity load balancing switches have been used to allow flexibility and growth. Only

[2] Note that the encryption server and virus scanner are not duplicated initially – traffic will however pass through if they fail. Encryption/decryption will then be handled by the web servers, but viruses will pass through. Also

one layer of firewalls have been used to keep the solution simple and easy to operate, and also since confidentiality and integrity is not so high on the requirements list. However, a large amount of filtering and logging will be employed at the border router, allowing it to act as the first layer firewall. IDS is used on all network segments to monitor for any anomalies, and as more are learnt about these: to automate the handling of these as much as possible. Some of the components are fairly expensive (e.g. the Stonebeat cluster and the load balancing switches), but this was not a concern by GIAC Enterprises. The ongoing operations cost should however be acceptable.

the load balancing switches are not duplicated due to very high cost in doing so. The Hubs are not duplicated because they "never fail".

2 Assignment 2 – Security policy and Tutorial

2.1 IP addressing

GIAC Enterprises have obtained the address space 145.247.64.0 to 145.247.64.255.[3] This is used for all external communication. Internally they use private addresses in the range 172.16.0.0 to 172.16.255.255, which are private addresses. This allows a larger address range and more flexibility for internal use. It also allows for hiding of internal IP addresses to the general public, by use of Network Address Translation (NAT).

The NAT translation is as follows (see drawing in chapter 1.3 to see how the real IP addresses are allocated):

Server	Real IP address	NAT address
DMZ web server	172.16.1.4 (virtual address)	145.247.64.5
DMZ mail server	172.16.1.1	145.247.64.6
DMZ DNS server	172.16.1.3	145.247.64.8
FW management server	172.16.2.8	145.247.64.9
Syslog server	172.16.2.6	145.247.64.10
Internal web server	172.16.2.4	145.247.64.7

The DNS servers at the ISPs are set up to directly use these NAT addresses – they will not get any answers from lookups to the internal DNS servers. Similarly the Internal DNS servers will use these NAT addresses hardwired rather that get answers from eachother. However, the DMZ DNS server will need to communicate with external servers, and is allowed to query (and receive replys) from external DNS servers.

2.2 Border router policy

The two border routers are configured the same. They both have one interface connected to the Internet, and one interface connected to the internal network. The routers are set up to filter out as much unwanted traffic as possible, both to protect themselves and to offload the firewalls. Any services that are not required are disabled.

2.2.1 General policies

Below is a list of general policies used. The purpose of each rule is stated in *italics*.

[3] This is actually assigned to a different company today.

service password -encryption
This saves (and lists) passwords as an MD5 hash instead of in plaintext, which is the standard, to stop anybody who gets access to the configuration file or a copy of this to obtain the passwords.

no cdp run
This will stop the router from providing information about itself to any devices that are directly connected. As a general rule we do not release information that we don't have to ("need to know" principle).

no service tcp-small-servers
no service udp-small-servers
This disables services like echo and character generation. They are disabled to prevent exploitation of any undiscovered vulnerability in these services.

no service finger
This disables the finger service, to avoid providing a hacker with information about who is logged in and from where.

no ip unreachables
This prevents the router from sending out ICMP error messages about hosts that are not reachable. The messages could provide a hacker with a method to map the internal network by scanning for hosts where such a message is not generated.

no ip directed-broadcast
This prevents the router from forwarding directed broadcasts to internal hosts and thereby causing denial of service problems.

no ip bootp server
This disables DHCP services which are not needed and therefore should be disabled to prevent exploitation of any vulnerabilities.

no ip http server
This disables the browser interface to the router. We are not going to use this interface, so the service should be disabled to prevent exploitation of any vulnerabilities.

no ip source-route
This disables the routing of packets with the IP "loose source route" flag set. The flag might allow a hacker to deliver packets to destinations that cannot normally be reached (due to access lists), as they are re-routed to another host once they arrive at the remote location.

no snmp
This disables snmp, that could be used to manage/monitor the router. Snmp will not be used by GIAC Enterprises on the border routers, so it is wise to disable it so it may not be utilised by hackers.

ntp disable
This stops the network time protocol service, as this service will not be used.

logging 145.247.64.10
logging trap debugging
This directs router events to a syslog server, including events noted as part of the ACLs and other events at all severity levels, such as configuration changes and router interface status changes . It is important that such events are forwarded to another server so that the information can be better protected, but it may also be used as part of an overall monitoring system covering events from other sources in addition. Note that the address used f or the syslog server is the NAT translation

banner login $ WARNING: only authorized staff may access this interface $
Write a message to anybody attempting to access the router directly, so that they cannot legally continue trying to break in.

2.2.2 Policies on outer interface

On the named access list called "inbound" the following filter rules are used. Note that events are logged to the syslog server using the "log" switch (but not events from the "permit" rules – that would cause too much noise). Note also that as much traffic as possible is stopped inbound to the router to ensure it does not have to be processed further. The router is set up to only allow traffic that is specified, and stop all other traffic (last statement is: "deny ip any any log"). Some of the many deny statements earlier may seem unnecessary because of this last statement, but they are used to ensure that even after later changes in the form of new permit statements (that will be made when staff realise the need for access they didn't t hink of earlier), they will not open up the router more than absolutely necessary.

deny ip 0.0.0.0 any log
This stops any traffic from source 0.0.0.0 as this is an invalid address.

deny ip 10.0.0.0 0.255.255.255 any log
This stops any traffic from sourc e range 10.0.0.0-10.255.255.255 which are private addresses and therefore should not be used on the Internet

deny ip 172.16.0.0 0.15.255.255 any log
This stops any traffic from source range 172.16.0.0 -172.31.255.255 which are private addresses and therefo re should not be used on the Internet

deny ip 192.168.0.0 0.0.255.255 any log
This stops any traffic from source range 192.168.0.0 -192.168.255.255 which are private addresses and therefore should not be used on the Internet

deny ip 224.0.0.0 31.255.255.2 55 any log
This stops any traffic from source range 224.0.0.0 -224.239.255.255 because they are multicast addresses and not wanted to the internal network.

deny ip 127.0.0.0 0.255.255.255 any log
This stops any traffic from source range 127.0.0.0 -127.255.255.255 which are loopback addresses and therefore should only be used on the router itself.

deny ip 145.247.64.0 0.0.0.255 any log
This stops any traffic from source range 145.247.64.0 -145.247.64.255 which are the addresses used by GIAC Enterprises and sh ould not be used by others.

deny tcp any any range 135 139 log
deny udp any any range 135 139 log
This stops any NETBIOS/IP ports, as these are critical to our internal network and should not be allowed in. These will also be stopped at firewall, but it i s more efficient to stop them at the router (and also safer to stop both places).

deny udp any any eq 69 log
This stops any tftp traffic – we do not wish to allow tftp traffic into our network.

deny udp any any eq 514 log
This stops any syslog traffic – we do not wish to allow syslog traffic into our network, other than what is generated by the router itself.

deny udp any any range 161 162 log
This stops any snmp traffic – we do not wish to allow snmp traffic into our network as it can be used for monito ring our hosts.

deny ip any host 145.247.64.1 log
deny ip any host 145.247.64.1 log
This stops any traffic directed at the routers themselves, as this could be an attempt at attacking the routers.

deny icmp any any log
This stops any icmp traffic, which would give hackers many ways to attack our network. However it also stops our ability to use ping or tracert/traceroute to test the connection via the ISP. If we need to do that for troubleshooting, we would have to enable icmp again while we troubleshoot, or alternatively use a different protocol.

permit tcp any host 145.247.64.5 eq www
permit tcp any host 145.247.64.5 eq 443
This allows traffic to the web server via the NAT translation of the virtual address on the load balancing switch. (Web servers 172 .16.1.2 and 172.16.1.3 have a virtual address of 172.16.1.4, which is translated to 145.247.64.5 at the firewall). This is the first permit rule, as it should be the most common access and therefore will be hit most.

permit udp any host 145.247.64.7 eq 50 0
permit 50 any host 145.257.64.7
permit 51 any host 145.257.64.7

This allows traffic to the internal web server for GIAC Enterprises staff, which is expected to be the second most common access. Note that the address used is the NAT translation, and the protocol is for VPN using IPSEC.

permit tcp any host 145.247.64.9 eq 264
permit tcp any host 145.247.64.9 eq 256
This allows traffic to the firewall management server, which is required to initiate VPN sessions for GIAC Enterprises staff. Note that the ad dress used is the NAT translation.

permit tcp any host 145.247.64.6 eq smtp
This allows traffic to the mail relay server, which is expected to be the third most common access. Note that the address used is the NAT translation.

permit tcp any host 145.247 .64.8 eq domain
This allows traffic between the internal DNS server and other DNS servers. Note that the address used is the NAT translation. Note also that I have allowed DNS traffic to any external host – to make this even safer I could allow DNS traffic only via the DNS servers of the ISPs.

deny ip any any log
This stops any other traffic, as we have already allowed the traffic we want to allow.

We could also block all unallocated legal IP addresses, but this would require manual updating every time th at address list changes, so it is not included here.

2.2.3 Policies on inner interface

On the named access list called "outbound" the following filter rules are used. Note that events are logged to the syslog server using the "log -input" switch. This ensures that the MAC address of the source is also logged, and may be used for tracking an event[4]. Note also that any traffic not planned for is stopped at the router, both to stop misuse from internal users and to stop any other unauthorised outbound data. Only specified protocols from specified IP addresses are allowed, so a general deny on anything else at the end is the only deny command required.

permit tcp host 145.247.64.5 any eq www
permit tcp host 145.247.64.5 any eq 443
This allows traffic from the exte rnal web server. This is the first permit rule, as it should be the most common access and therefore will be hit most. Note that the address used is the NAT translation.

permit udp host 145.247.64.7 any eq 500

[4] Note that there is little point logging MAC addresses of incoming traffic, as it most likely will be the address of the router at the ISP.

permit 50 host 145.257.64.7 any
permit 51 host 145.257.64.7 any
This allows traffic from the internal web server for GIAC Enterprises staff, which is expected to be the second most common access. Note that the address used is the NAT translation, and the protocol is for VPN using IPSEC.

permit tcp host 145.247.64.6 any eq smtp
This allows traffic from the mail relay server for, which is expected to be the third most common access. Note that the address used is the NAT translation.

permit tcp host 145.247.64.8 any eq domain
This allows traffic betwe en the internal DNS server and other DNS servers. Note that the address used is the NAT translation.

permit tcp host 145.247.64.9 any eq 264
permit tcp host 145.247.64.9 any eq 256
This allows traffic from the firewall management server, which is required to initiate VPN sessions for GIAC Enterprises staff. Note that the address used is the NAT translation.

deny ip any any log
This stops any other traffic, as we have already allowed the traffic we want to allow.

Note that this access list could restrict traffic even more by also blocking all access to known invalid target ip addresses (similar to the blocking of source addresses in the inbound access list), but this is expected to have little other effect than to slow down the router, so it was decided ag ainst.

2.3 Firewall / VPN policy

2.3.1 General

The implied rules that come as standard must first be turned off to ensure that we have full control of which rules we are using on the firewall.

User groups used in the tables later on are described here:

No	Network object	Location	IP address	Comment
1	DMZ_WEB	DMZ zone	172.16.1.4	Web server for customers, partners, and suppliers.
2	DMZ_WEB_PROXY	Firewall	145.247.64.5	NAT translation for above
3	DMZ_Mail	DMZ zone	172.16.1.1	Mail relay server
4	DMZ_Mail_PROXY	Firewall	145.247.64.6	NAT translation for above
5	Ext _all	Internet	0.0.0.1 to 145.247.63.255 and 145.247.65.1 to 172.15.255.255	All users via Internet (we have excluded GIAC Enterprises official and private IP addresses.

No	Network object	Location	IP address	Comment
			and 172.32.0.0 to 255.255.255.255	
6	Int_WEB	Internal zone	172.16.2.4	Web server for staff
7	Int_WEB_PROXY	Firewall	145.247.64.7	NAT translation for above
8	FW_Management	Internal zone	172.16.2.8	FW management workstation
9	Firewall	Firewall	172.16.3.0 145.247.64.5 145.247.64.6	Subnets and addresses used for FW interfaces
10	DMZ_DNS	DMZ zone	172.16.1.5	DNS server in DMZ
11	Int_Mail	Internal zone	172.16.2.5	Internal mail server
12	Int_DNS	Internal zone	172.16.2.3	Internal DNS server
13	Internal	Internal zone	172.16.2.0	Internal subnet
14	Authent	Internal zone	172.16.2.7	Authentication server for staff when working externally
15	FW_Mgr_PROXY	Firewall	145.247.64.9	NAT translation of FW management workstation
16	DMZ_DNS_PROXY	Firewall	145.247.64.8	NAT translation of DNS server in DMZ
17	Syslog	Internal zone	172.16.2.6	Syslog server
18	Syslog_PROXY	Firewall	145.247.64.10	NAT translation for above
19	Router	Border	145.247.64.2 145.247.64.4	Border router internal addresses
20	Int_app	Internal	172.16.2.2	Internal application server
21				

2.3.2 Ruleset

Below is the ruleset used in the firewall. Note that as in the border router, only traffic specifically required is allowed through. Here we only allow traffic to specific ports on specific machines.

No	Source	Destination	Service	Action	Track	Install on	Time	Comment
1	FW_management	Firewall	Any	accept	Long	Gateways	Any	Accept management access
2	Any DMZ_WEB_PROXY	DMZ_WEB_PROXY Any	http https	accept	Long	Gateways	Any	Allow access to DMZ Web server for anybody
3	Any DMZ_Mail_PROXY	DMZ_Mail_PROXY Any	snmp	accept	Long	Gateways	Any	Allow access to DMZ mail relay for anybody
4	Ext_all DMZ_DNS_PROXY	DMZ_DNS_PROXY Ext_all	domain-udp	accept	Long	Gateways	Any	Allow DMZ DNS server access from externally
6	Router	Syslog_Proxy	syslog	accept	Long	Gateways	Any	Allow syslog traffic from routers
7	Int_mail DMZ_Mail_PROXY	DMZ_Mail_PROXY Int_mail	pop3	accept	Long	Gateways	Any	Allow traffic between mail relay server and mail

							server
8	Int_app DMZ_WEB_PROXY	DMZ_WEB_PROXY Int_app	ftp	accept Long	Gateways	Any	Allow internal application server to fetch data from DMZ Web server
9	Any	Any	Any	Drop Long	Gateways	Any	Stop all traffic that is not explicitly allowed
15							

2.3.3 NAT setup

Below is the setup of Network Address Translations (NAT). NAT is used f or translation of of addresses for all traffic to both the DMZ and to the internal network. This does cause some issues in DNS (ref. chapter 2.1), but makes it even safer against hackers, as they will never see the real addresses unless they obtain control of any of the machines.

No	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	Any	DMZ_WEB_PROXY	Any	Original	DMZ_WEB	Original
2	Any	DMZ_Mail_PROXY	Any	Original	DMZ_Mail	Original
3	Any	Int_WEB_PROXY	Any	Original	Int_WEB	Original
4	Any	DMZ_DNS_PROXY	Any	Original	DMZ_DNS	Original
5	Any	FW_Mgr_PROXY	Any	Original	FW_Management	Original
6	Any	Syslog_PROXY	Any	Original	Syslog	Original
7	DMZ_WEB	Any	Any	DMZ_WEB_PROXY	Original	Original
8	DMZ_Mail	Any	Any	DMZ_Mail_PROXY	Original	Original
9	Int_WEB	Any	Any	Int_WEB_PROXY	Original	Original
10	DMZ_DNS	Any	Any	DMZ_DNS_PROXY	Original	Original
11	FW_Management	Any	Any	FW_Mgr_PROXY	Original	Original
12	Syslog	Any	Any	Syslog_PROXY	Original	Original
13						
14						

Note that NAT translation takes place after other rules, just before the packet leaves the interface. That means all other rules must be written to conform with the ip addresses used before translation (which will depend on the direction of the traffic – incoming traffic will be directed at the proxy address, while outgoing traffic will come from the real address).

Note also that systems that need to communicate (e.g. mail servers) need to use the proxy address of the recipient, not the real address.

2.3.4 VPN setup

Below are the rules used for handling VPN. Note that we are still using the same firewall machines for handling VPN. VPN is only used by GIAC Enterprises staff and should not cause a major load on the firewall machines.

No	Source	Destination	Service	Action	Track	Install on	Time	Comment
1	Firewall	Authent	securid	accept	Long	Gateways	Any	Allow firewall to check authentication of user via authent server (port 5500)
2	Ext_all FW_Management	FW_Management Ext_all	Securemote - Build4157	accept	Long	Gateways	Any	Allow staff to receive information from FW console required to start sessions (ports 264 and 256)
3	Ext_all	Int_WEB_PROXY	http	Client Encrypt	Long	Gateways	Any	All staff when external should connect via VPN

2.4 Tutorial on router policy implementation

To set up the router in the way described earlier, the following steps must be performed:

1. Connect to the router by plugging a PC directly into the serial port, and using a terminal emulation program. Note that it is wise to store all commands below as a file on the PC, to simplify later changes. Type “enable” and press return.
2. Press return again at the password prompt. The router is not configured yet, so the password is blank.
3. Type “configure terminal” and press return. This will enter global configurat ion mode and allow any global configuration commands. Note: from now on pressing “return” is implied after each command typed.
4. Type “service password encryption”, to enable encrypted passwords.
5. Type “enable secret Coo123kie”, to enter an enable password fo r later use.
6. Type “no service tcp-small-servers”.
7. Type “no service udp-small-servers”.
8. Type “no service finger”.
9. Type “no ip unreachables”.
10. Type “no ip directed-broadcast”.
11. Type “no ip bootp server”.
12. Type “no ip http server”.
13. Type “no ip source-route”.

14. Type “no snmp”.
15. Type “ntp disable”.
16. Type “logging 145.247.64.10”.
17. Type “banner $ WARNING: only authorized staff may access this interface $”.
18. Type “ip access list extended filterin”. This creates the access list to be used for filtering all inbound traffic.
19. Type “deny ip 0.0.0.0 any log”
20. Type “deny ip 10.0.0.0 0.255.255.255 any log”
21. Type “deny ip 172.16.0.0 0.15.255.255 any log”
22. Type “deny ip 192.168.0.0 0.0.255.255 any log”
23. Type “deny ip 224.0.0.0 31.255.255.255 any log”
24. Type “deny ip 127.0.0.0 0.255.255.255 any log”
25. Type “deny ip 145.247.64.0 0.0.0.255 any log”
26. Type “deny tcp any any range 135 139 log”
27. Type “deny udp any any range 135 139 log”
28. Type “deny udp any any eq 69 log”
29. Type “deny udp any any eq 514 log”
30. Type “deny udp any any range 161 162 log”
31. Type “deny ip any host 145.247.64.1 log”
32. Type “deny ip any host 145.247.64.1 log”
33. Type “deny icmp any any log”
34. Type “permit tcp any host 145.247.64.5 eq www”
35. Type “permit tcp any host 145.247.64.5 eq 443”
36. Type “permit udp any host 145.247.64.7 eq 500”
37. Type “permit 50 any host 145.257.64.7”
38. Type “permit 51 any host 145.257.64.7”
39. Type “permit tcp any host 145.247.64.9 eq 264”
40. Type “permit tcp any host 145.247.64.9 eq 256”
41. Type “permit tcp any host 145.247.64.6 eq smtp”
42. Type “permit tcp any host 145.247.64.8 eq doma in”
43. Type “deny ip any any log”
44. Type “exit”, to exit the access list.
45. Type “ip access list extended filterout”. This creates the access list to be used for filtering all outbound traffic.
46. Type “permit tcp host 145.247.64.5 any eq www”
47. Type “permit tcp host 145.247.64.5 any eq 443”
48. Type “permit udp host 145.247.64.7 any eq 500”
49. Type “permit 50 host 145.257.64.7 any”
50. Type “permit 51 host 145.257.64.7 any”
51. Type “permit tcp host 145.247.64.6 any eq smtp”
52. Type “permit tcp host 145.247.64.8 any eq domain”
53. Type “permit tcp host 145.247.64.9 any eq 264”
54. Type “permit tcp host 145.247.64.9 any eq 256”
55. Type “deny ip any any log”
56. Type “exit”, to exit the access list.
57. Type “interface serial 0”. This will enter configuration mode for serial interface 0, which is the interface facing the ISP.

58. Type “ip address 145.247.64.1 255.255.255.255”. This will set the ip address for the external interface (note that this applies to the first router, the second router has a different address).
59. Type “ip access-group filterin in”. This wi ll apply the access list specified from line 18 above to this interface, for all inbound traffic.
60. Type “exit”, to exit the interface configuration mode
61. Type “interface fastethernet 0”. This will enter configuration mode for fast Ethernet interface 0, which is the fast Ethernet connection with the GIAC Enterprises network.
62. Type “ip address 145.247.64.2 255.255.255.255”. This will set the ip address for the internal interface.
63. Type “ip access-group filterout in”. This will apply the access list specified from line 45 above to this interface, for all inbound traffic (inbound from GIAC Enterprises, not from the Internet).
64. Type “exit”, to exit the interface configuration mode
65. Type “copy running-config startup-config”. This copies the live configuration to the configuration used when rebooting the router. This command may be performed after a while, when the router operation has been tested.
66. Type “exit”, to exit global configuration mode

Day to day management of the router is not explained here, but is equally imp ortant in ensuring a secure network. This concerns such items as how to handle backup of the router configuration, handling of syslog files with recordings of events from the router, how to perform changes, and how to perform troubleshooting. Such items often have an effect on the router policy, or even on the whole architecture.

3 Assignment 3 – Verify the Firewall Policy

One year after the implementation of the security infrastructure, the IT manager decides that he wants the GIAC Enterprises firewall audi ted to verify that the policies are correctly enforced.

The audit is restricted to the firewall only – the other parts of the infrastructure are handled separately. The IT manager wants to use external experts to perform the audit – both because he does n ot have the expertise in -house (he runs a slim, low cost IT operation), and also because an audit is always best performed by somebody who are not involved in the day -to-day operation. That way the chance of finding the problem areas is greater, as in -house staff are only likely to test against what they already believe is working, while external people might think of different areas to test.

3.1 Planning the audit

The IT manager talks to an external company, who comes up with a plan for the audit as described below:

The firewall consists of two W2000 computers running a Stonebeat Firewall -1 cluster. Both the machines themselves and the firewall software need to be tested to ensure that the policies are correctly enforced. We could also go all the way back to the company requirements and security principles and use those as the basis for the audit, but we will make the assumption that the basic design is correct, and only test against the policies that are part of the design.

We will use manual methods and the **nessus** tool for performing the audit. This tool is openly available (also for hackers!) and performs good and (user friendly) scanning (if required using **nmap** scan method). Tests will be performed inside the border router, as the border router is not part of the audit. The scanning (task 6 below) will be performed after normal working hours, to avoid potential disruption at peak time. It will also be planned to not be performed during other peak usage times, e.g. during nirghtly backup. All other work may be performed at daytime. Using scanning tools such as nmap may very well cause disruption in the form of bad response time (caused by load on target machine or network segment), “freezing” the target machine, or even crashing it, so care must be taken to f orewarn key staff in case of problems.

Testing will focus on the following areas:

- Tests to find general vulnerabilities
- Tests to ensure that required access and encryption is provided as planned
- Tests to ensure that access is denied where planned
- Tests to ensure appropriate logging is performed
- Tests to ensure correct NAT is performed

Below is a plan with schedule and resource estimates for the audit:

No.	Task	Time	Hours	Comments
1	Project planning	Day 1	5	Agree staffing, time schedule, scope, etc.[5]
2	Inform all	Day 2	5	Inform staff and/or users (if appropriate). Obtain a signed document from management freeing you of responsibilities in case of problems, and also as a means to explain to staff what you are doing and that you are allowed access. Note that staff involved in log review and IDS systems must be made aware of what will happen, so they don't mistake the audit with a security incident.
3	Obtain audit baseline	Day 3	2	This includes the initial design description for the firewall rulebase, the existing rulebase, or the company security policy – whatever is decided as the scope. It may also include a snapshot of the system at an earlier time, with a tool such as **tripwire**.
4	Obtain existing documentation	Day 3	5	Obtain and review documentation such as network drawings, configurations, procedures.
5	Set up tools	Day 4-5	15	Decide on tools to use. Get the latest release and update with the latest exploits. Configure the hardware and software to use, and connect to the network where required. Produce test scripts.
6	Run tests	Day 6-7	15	First produce a fresh backup, then perform the tests. Note proper time schedule and user warning.

[5] Note that it is especially important to agree on the scope, as this may be viewed differently by different staff. Are we reviewing just the system, or also staff, roles, procedures? The OS as well as the firewall? What boxes are included – are we allowed to check other systems if we find a problem? Do we check the firewall logs, system logs, or other logs for earlier problems? What about a virus scan? Effects on IDS monitoring? What policies to we audit against – the company security policies or the policies which are part of the firewall design?

7	Evaluate and document results.	Day 8-10	24	Evaluate the results. Re-do some tests if necessary. Do some further tests if necessary to check the results. Produce documentation of the results, showing what worked as expected, what didn't, what was the result, and what recommendations can be made for improvement.
8	Completion	Day 11	6	Remove audit software, data, and equipment. Produce any required baseline for next audits. Tidy up. Perform any evaluation of the project to capture learning points for next time. If required – schedule the next audit.
	Total		77	

Total estimate is 77 hours of external consultancy work. At a standard consultancy rate of 120 Euro per hour, the total cost is 9240 Euro. No costs are included for necessary travel.

Below is a list of project risks and how we expect to handle them:

Risk: Scanning tools causing excessive load and denial of service.
Management: Perform scanning after normal working hours. Monitor the network and machines during scanning to see if excessive load is caused by the test, and tune the testing tools accordingly.

Risk: During the audit, logs and other monitoring will be ignored, so a real event might happen at the same time without any action taken.
Management: Inform staff exactly what scanning will be performed, and also inform them that they should continue monitoring during scanning and that they should ask if they are uncertain about a detected event.

Risk: Hardware or software faults related to the tools used during the audit.
Management: Use up-to-date hardware and software. Ensure that the tools, their setup, and scripts are backed up, so the tools may easily be set up again on failure.

Risk: Staff unavailability (due to sickness, other priorities, etc).
Management: Availability of key staff must be a pre-requisite in the contract.

Risk: Misuse of information regarding vulnerabilities found.
Management: The contract must guarantee against misuse. Vulnerabilities found should be fixed as a high priority to avoid later misuse.

Risk: Undocumented policy changes have been implemented in the firewall.

Management: Check this as part of the project and discuss with IT management what are the correct policies, before running the tests.

3.2 Conducting the audit

After approval of the project plan, the project to conduct the audit is started. Tasks 1 and 2 of the project is performed as planned. Tasks 3 and 4 of the project is performed, and the result is the documentation provided in assigment 1 and 2 in this document.

3.2.1 Task 5: Set up tools.

Nessus is found to be the best tool for the project, as explained earlier. Nessus runs best in the Linux environment, so a Redhat Linux machine is used for these. The installation guides and user documentation is found at the Nessus web site. The description on what commands to use is taken from there. Note that there are new Nessus plugins supplied every week, so if it is already installed, the new plugins need to be added.

Nessus is downloaded from www.nessus.org, and installed as follows (based on information found at the nessus website):

```
cd nessus-libraries
./configure
make
make install
cd libnasl
./configure
make
make install
cd nessus-core
./configure
make
make install
cd nessus-plugins
./configure
make
make install
ldconfig
```

A user account to use during the test is then created as follows:

```
$ nessus-adduser

Addition of a new nessusd user
```

Login : giacaudit
Password : secret
Authentification type (cipher or plaintext) [cipher] : cipher
Now enter the rules for this user, and hit ctrl -D once you are done :
(the user can have an empty rule set)
^D

Login : giacaudit
Password : secret
Authentification : cipher
Rules :

Is that ok (y/n) ? [y] y

user added

Then start the nessus deamon (as root):

nessusd -D

Once the tools have been installed properly, and a quick test performed to see if they function properly, the scripts to be used are created (se commands used later) and the machine is connected to the hub on the outside of the firewalls.

3.2.2 Task 6 Run test

During the test all actions performed are logged, including time of action . This is both to ensure that the audit is properly documented, but also in case of any other events happening at the same time, so we can find out if the event was caused by the audit, or by something else.

Search for general vulnerabilities.

Start up nessus, and log in using the giacaudit username.

Under the “plugins” flip, click “enable all but dangerous plugins”, to ensure we don’t cause any problems to the Firewalls.

Under the “prefs” flip, select the preferred tcp scanning technique. A couple of different techniques may be tried.

Under the “scan options” flip, choose nmap, and select “optimise the test”.

Under the “target selection” flip, type in the target ip address: first 145.247.64.5, and later 145.247.64.6 (test both firewalls)

Then click “start the scan”.

The report window will then pop up with the results, showing open ports and vulnerabilities found.

Search for allowed access.

Chapter 2.3.2 in assignment 2 contains a list of firewall rules to check against. They are copied here for easy reference:

No	Source	Destination	Service	Action	Track	Install on	Time	Comment
1	FW_management	Firewall	Any	accept	Long	Gateways	Any	Accept management access
2	Any DMZ_WEB_PROXY	DMZ_WEB_PROXY Any	http https	accept	Long	Gateways	Any	Allow access to DMZ Web server for anybody
3	Any DMZ_Mail_PROXY	DMZ_Mail_PROXY Any	snmp	accept	Long	Gateways	Any	Allow access to DMZ mail relay for anybody
4	Ext_all DMZ_DNS_PROXY	DMZ_DNS_PROXY Ext_all	domain-udp	accept	Long	Gateways	Any	Allow DMZ DNS server access from externally
6	Router	Syslog_Proxy	syslog	accept	Long	Gateways	Any	Allow syslog traffic from routers
7	Int_mail DMZ_Mail_PROXY	DMZ_Mail_PROXY Int_mail	pop3	accept	Long	Gateways	Any	Allow traffic between mail relay server and mail server
8	Int_app DMZ_WEB_PROXY	DMZ_WEB_PROXY Int_app	ftp	accept	Long	Gateways	Any	Allow internal application server to fetch data from DMZ Web server
9	Any	Any	Any	Drop	Long	Gateways	Any	Stop all traffic that is not explicitly allowed
15								

Tests to be performed:

Rule 1: Check that the Firewall management console functions properly.
Expected result: Full access to the firewall

Rule 2: Try accessing the web server at www.giacent.com from an external browser.
Expected result: Full access to the welcome page.
Telnet to port 80 on 145.247.64.5
Expected result: Access allowed to the web server.
Try accessing the web server at www.giacent.com from an internal browser.
Expected result: Full access to the welcome page.

Rule 3: Try sending a mail to postmaster@giacent.com from an external mail system.
Expected result: Mail received at internal mail server.
Telnet to port 25 on 145.247.64.6
Expected result: Access allowed to mail relay server.

Rule 4: Do a nslookup for any external address, while connected to the DMZ network
Expected result: The correct ip address should be returned.

Rule 6: Try tracert to 145.247.64.7, from an external machine.
Expected result: An entry in the syslog server should show an attempt to use the icmp protocol through the router.

Rule 7: Try sending a mail from the internal system to an external user.
Expected result: Mail received at external mail server.
Telnet to port 25 on 145.247.64.6 from the internal mail server.
Expected result: Access allowed to mail relay server.

Rule 8: Try running ftp from the internal application server to 145.247.64.7
Expected result: Access allowed.

The VPN rules are shown in chapter 2.3.4. They are copied here for easier reference:

No	Source	Destination	Service	Action	Track	Install on	Time	Comment
1	Firewall	Authent	securid	accept	Long	Gateways	Any	Allow firewall to check authentication of user via authent server (port 5500)
2	Ext_all FW_Management	FW_Management Ext_all	Securemote - Build4157	accept	Long	Gateways	Any	Allow staff to receive information from FW console required to start sessions (ports 264 and 256)
3	Ext_all	Int_WEB_PROXY	http	Client Encrypt	Long	Gateways	Any	All staff when external should connect via VPN

Tests to be performed:

VPN rule 1, 2 && 3: Try accessing 145.247.64.7 as an internal staff from home.
Expected result: Access allowed, but an encrypted session is set up.
Use tpcdump on a machine connected to the internal hub, to capture the session and check that it is encrypted (port 500).

Search for access that should be denied:

We want to test the following:

1. Access to servers we should have access to, but with the wrong protocol
2. Access to servers we should not have acces s to, but with protocols that are allowed elsewhere
3. Access to internal IP addresses directly (not NAT addresses)

Actual tests performed (from the hub on the outside of the firewalls, and from the hub inside the firewalls):

1 & 2. Attempt telnet to IP add resses 145.247.64.5, 6, 7, 8, 9, and 10. Try ports 80, 21, 25, 500, but not on the machines where they should be allowed.
Expected result: Access denied.

3. Attempt telnet to 172.16.3.1 -4, 172.16.1.1-5, and 172.16.2.1 -8, using port 80.
Expected result: Ac cess failed (No such server).

Check firewall logging:

All access attempts in the previous tests should have been logged by the firewall. Check through the firewall logs to see if all events are recorded.

Check for correct NAT translation:

Redo the "all owed access" tests.

Use tpcdump on a machine connected to the internal hub, to capture the sessions and check that each address is translated as in the table in chapter 2.3.3 in assignment 2.

3.3 Evaluation of the results

Every test mentioned above is docum ented to show the results. Here is an example output from the testing:

Test	Expected result	Observed result	FW log entry
Rule 3: send mail to postmaster@giacent.com	Mail received	Mail received	Log entries both as message was sent to the mail relay server , and as message was passed on to internal mail server
Rule 3: Telnet to port 25 on 145.247.64.6	Access allowed	Access allowed	Log entry for connection to mail

			relay server

Test for general vulnerabilities.

A number of vulnerabilities was found in th e firewall. Apparently the firewall had not been changed since initial installation.

Recommendation 1: Apply patches as necessary to close the vulnerabilities found.

Recommendation 2: Set up a "security watch" routine for GIAC Enterprises staff to check for new vulnerabilities and patches for these (e.g. subscribing to the CERT mailing list[6]). Ensure they apply security patches if appropriate.

Test for allowed access:

All allowed access was provided as originally designed. No recommendation is required.

Test for access denied:

Access was denied as originally designed. However, the vulnerabilities found during the first test means that the firewall itself is vulnerable, and there is a risk that it may be compromised, and the access lists opened up.

Recommendation 3: Add a second layer of firewall between the DMZ and the internal network. This firewall should be of a different type, e.g. Cisco Pix.

Test for appropriate logging:

Logging was performed as designed. However all allowed access attempts crea te a lot of "noise" in the firewall logs. Also the time stamps are not 100% correct.

Recommendation 4: Stop logging successful access attempts at the firewall. The information provided is normally not used by anybody anyway.

Recommendation 5: Set up ntp on all servers to ensure the clocks are all the same, and that they are synchronised. Note that this also means that we need to open up the firewall and border router to allow queries to an external ntp server.

Test to ensure correct NAT:

All NAT was performed as designed. No recommendation is required.

General recommendations:

[6] To subscribe to the CERT mai ling list, send a mail to majordomo@cert.org , with the text: "subscribe cert_advisory" in the message body.

The firewalls are set up in a cluster to ensure redundancy. However there are several other components that are single points of failure. Potential for further duplication is as follows (in this order of importance):
DNS servers, network components, mail and mail relay servers, internal web server, application server, database server, virus server, encryption server.

4 Assignment 4 – Design under fire

This assignment is about des igning an attack at a different architecture. I have selected Steve Kiefling's paper, found at:
http://www.giac.org/practical/Steve_Keifling_GCFW.doc , as a basis for attacks.

The design is a fairly simple, but robust design, based on a Cisco PIX firewall and a separate Cisco VPN concentrator in parallel.

4.1 Firewall attack

4.1.1 Vulnerability

There are number of sources for identifying vulnerabilities for the Cisco PIX firewall. I have used the following sources:

CVE – Catalogue of **C**ommon **V**ulnerabilities and **E**xposures:
http://www.cve.mitre.org/cve/

NIST database of vulnerabilities:
http://icat.nist.gov/icat.cfm

Securityfocus vulnerability database:
http://www.securityfocus.com/corporate/products/vdb

Cisco's product security advisories:
http://www.cisco.com/warp/public/707/advisory.html

An archive with good information on specific vulnerabilities:
http://archives.neohapsis.com/archives/vulnwatch/

The sources need to be used in combination – a vulnerability found in one place may have more information in one of the other sources. In particular it is important to check CISCO to see what they have done to fix the vulnerability.

Most vulnerabilities found have indeed been fixed by CISCO, and I am assuming that Steve Keiflings' design has been kept up -to-date with security patches (this makes the task much harder that it would be if the router had not been updated – showing how important it is to keep up -to-date). I did however find a vulnerability that did not seem to have any fix by CISCO. Under the CVE catalogue, it is described as such:

Name: CAN-2002-0954
Description: The encryption algorithms for enable and passwd commands on CISCO PIX Firewall can be executed quickly due to a limited number of rounds, which make it easier for an attacker to decrypt the passwords using brute force techniques.

4.1.2 Discussion

This discussion is based on input by Damir Rajnovic (CISCO) and Michael Thumann (neohapsis archives).

The CISCO PIX Firewall uses 16byte passwords, and a base64 encoded MD5 hash algorithm for encryption. It uses one MD5 update round, rather than the 1000 MD5 update rounds used on the CISCO IOS based routers. This makes it much faster for brute force attacks to crack.

The firewall configuration files, including the encrypted password, should as normal practice be backed up. If somebody can get hold of these files, either during the backup process, or from their backup location, it should be possible to crack the enable password.

4.1.3 The attack

First as much information about GIAC Enterprises should be gathered. By checking the following (in this order), a lot of important information can be found:

- Check domain registry information
- Search open information about GIAC Enterprises: newsgroup postings, web pages (including their own information pages), job search databases…
- Based on names of employees found: search for personal home pages, papers written by the employees, etc..
- Contact key employees, and if possible get them to talk about their infrastructure, or even invite you to visit their site (people like to talk about what they have done)
- Perform some careful port scanning
- Try to connect to open ports to see what kind of messages are received about the end system

The following web site: http://www.ideahamster.org/ contains a methodology for this type of work, and contains a much longer list of what information may be collected.

Based on the above work, information about the use of PIX firewall and an Internal Legato backup server is gained. Offsite backups are kept in a separate building with less security.

It is usually surprisingly easy to gain physical access to a building – by following somebody else who have just unlocked a door, or by using some excuse like delivery

or repair, so it is planned to access the low security building during daytime and remove last full backup tape (they are clearly labelled, and are kept in open shelves). From this tape th e PIX configuration files are copied to disk, and the enable password cracked with a brute force attack using the freeware "Cain & Abel" password cracker from oxid.it (see www.oxid.it). Due to the vulnerability mentioned earlier (CAN-2002-0954), it is relatively easy to crack the password.

Eventually we test access to the Firewall with the cracked password. However, only internal workstations are found to have access to the Firewall for management, so if this is to succe ed, then either an employee (any employee) needs to be used for this attack, or physical access to an internal workstation is required.

The risk of being found out is fairly high, so the attempt is abandoned. The firewall itself is not the best object of attack – it is well secured.

4.2 Denial of service attack

4.2.1 The attack

The easiest way to do a Denial of service (DOS) attack, is sometimes to attack the first device at the outer perimeter. That way the attack does not have to traverse several components and possibly be stopped or detected by an internal IDS system. We will try to attack the border router, a Cisco 2610XM router.

The router only has one connection to the Internet, so the attack will have to be through this connection. Most of Steve Keifling's protection seems to be at the Firewall/VPN concentrator – the border router permits most hosts to access any internal ip address, using any ip protocol (the rule used is: *permit ip any 58.1.1.0 0.0.0.127*), so it could also be relatively simple to perform a DOS attack on other components. The external router interface does not seem to be protected against anything else than itself, so we will use this as the target address for the attack (ip address 4.4.4.5).

We will use the Tribe Flood Network 2000 (TFN2K) tool, found at: http://packetstorm.decepticons.org/ . This is a user-friendly tool, which allows a master to control a number of agents to attack any kind of target. The attack may be done with a TCP/SYN , UDP, ICMP/PING or BROADCAST PING packet flood, or a mix of these.

The TFN2K tool is installed on a master, which is used to infect the 50 compromised systems. The ip addresses of the 50 compromised systems is kept in the file *fullcontrol*. The attack is started with the border router as the target, and the following parameters set:

-f fullcontrol use file "fullcontrol" with the ip addresses of the TFN2K agents
-c 8 use a mixed packet flood, with all methods intermixed.

The attack should be run during p eak hours to have the maximum effect, and may be stopped and started again at random times, to cause even more problems (this means GIAC Enterprises will have to continue staying alert to try to solve the problem).

4.2.2 Possible countermeasures

Here is a list of possible countermeasures against the TFN2K attack:

- Ensure own systems are not easily compromised and used for such attacks. That means setting the same hard protection measures for all systems, even the non-critical ones. It also means that we should focus on other measures than just perimeter protection, including hardening of the servers themselves.
- Scan own systems regularly for TFN2K files (and other known tools).
- Avoid attacks on the router interface, by adding rules such as: *deny ip any host 4.4.4.5 log.*
- Disallow traffic that is not required, at the border router. At the moment, most traffic is allowed through, regardless of source, destination, or protocol. It is also possible to block against unallocated IP addresses, and lists of ip addresses of known attackers.
- Monitor traffic with the help of an IDS system such as SNORT.
- Build in redundancy: connect to two ISPs, with one router for each connection. Use duplicate firewalls, network components, and servers. The duplication can be implemented wit h clustering techniques, load balancing devices, or a hot standby with automatic or manual switchover, depending on how much investment money is available.
- Keep the border router (and all other components) patched with the latest security patches. Use mail ing lists (e.g. CERT) to stay up -to-date with the latest vulnerabilities and their solutions.
- Set up an agreement with the ISP(s) so that an attack may be investigated by them, and blocked at the ISP. A DDOS attack may consume all the bandwith to your bord er router even if you have taken all the measures mentioned above, but if the ISP blocks it before that stage, you are still ok. The ISPs will have larger bandwith pipes, so they can function through attacks that would effectively stop the services of most other companies.

4.3 Internal compromisation plan

4.3.1 Target selected

The only access allowed through the firewall directly from the Internet is to the web server, the partner machine (ftp), and the DNS/Mail/NTP/TFTP machine.
The target selected for the attack is the Apache web server (ip address 58.1.1.36). The reason for this choice is that this machine will be hit most by normal traffic, and the attack will therefore be easier to hide amongst that traffic.

A number of vulnerabilities exist for Apache v2.0. 36 and RedHat Linux 7.3, as well as potential vulnerabilities in the HTML code itself. We will attempt to exploit the following vulnerabilities:

1) From http://www.cve.mitre.org/cve/ :

Name: CAN-2002-0392
Description: Apache v2.0.36 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a chunk -encoded HTTP request that causes Apache to use an incorrect size.

2) Potential vulnerabilities in the HTML code based on lack of inpu t checking.

4.3.2 Attack process

First, we perform some reconnaissance as explained in chapter 4.1.3 above to find out about the systems used – copied here for ease of reading:

- Check domain registry information
- Search open information about GIAC Enterprises: newsgroup postings, web pages (including their own information pages), job search databases…
- Based on names of employees found: search for personal home pages, papers written by the employees, etc.
- Contact key employees, and if possible get them to talk ab out their infrastructure, or even invite you to visit their site (people like to talk about what they have done)
- Perform some careful port scanning
- Try to connect to open ports to see what kind of messages are received about the end system

We use the nessus tool to help us find out about the web server type and version.

Chapter 3.2.1 and 3.2.2 explains how to configure and run nessus. We start nessus, preferably using somebody else's Linux machine that we have taken control over, so that the attack can't be directly linked to us. Here we will select ip address 58.1.1.36 under the "Target selection" flip, and select first *HTTP Server type and version* , and later the *Apache chunked encoding* plugins under the "Plugins" flip. To attempt avoiding detection click "sneaky mode" under the "prefs" flip.

After clicking "start the scan", we will for the first test (if everything works the way we want) find out that the target is an Apache server running Apache 2.0.36, which we know may contain the CAN -2002-0392 vulner ability mentioned earlier. The next scan will report whether this vulnerability in fact exists on the server.

Further this vulnerability may be used to create multiple child processes on the server, causing a denial of service. It is possible to use the " apache-scalp.c" code

from http://lists.insecure.org/bugtraq/2002/Jun/0243.html to perform this denial of service attack. It might however require some coding to ensure it functions against a RedHat Linux 7.3 server, as it has only been tested against a OpenBSD server.

Our second attack is against the HTML code itself.

On http://www.owasp.org/, there is a freely available document called "A guide to building secure web applications and web services". This document provides a number of possible ways of testing (or exploiting) web application vulnerabilities. A common vulnerability in such applications is that input data is not checked for meta characters or too long input strings. The following meta characters with special use is listed in the document:

- [;] Semicolons for additional command -execution
- [|] Pipes for command -execution
- [!] Call signs for command -execution
- [&] Used for command -execution
- [x20] Spaces for faking urls and other names (especial in URLs!)
- [x00] Nullbytes for truncating strings and filenames
- [x04] EOT for faking file ends
- [x0a] New lines for additional command -execution
- [x0d] New lines for additional command -execution
- [x1b] Escape
- [x08] Backspace
- [x7f] Delete
- [~] Tildes
- [' "] Quotation marks (often in combination with database -queries)
- [-] in combination with database -queries and creation of negative numbers
- [*%] used in combination with database -queries
- [` Backticks for command execution
- [/\ ] Slashes and Backslashes for faking paths and queries
- [<>] LTs and GTs for file -operations
- [<>] for creating script-language related TAGS within documents on webservers
- [?] Programming/scripting - language related
- [$] Programming/scripting - language related
- [@] Programming/scripting - language related
- [:] Programming/scripting - language related
- [({[]})] Programming/scripting/regex and language -related

These meta characters may be used to form an attacks in various ways. First, however, information about the web pages should be gathered. Usually selecting "view" and "source" in Microsoft IE when visiting the site will provide a lot of information. An alternative method would be to use the tool "wget " (from: http://www.gnu.org/software/wget/) to download information from the site. Depending on the information found, the attack can be prepared. Example attacks are:

- Adding information to the URL to form additional SQL statement information.

- Adding a java script to an input string.
- Adding many characters in an input string to see if the web server will handle it correct.

These attacks can cause anything to happen: server crash, bad data input to the database, even full access to the web server.

4.3.3 Countermeasures

Chapter 4.2.2 lists countermeasures that also can be used against these attacks. In particular an IDS system could be used to detect and possibly even stop the attack, and using the latest patches would make sure the attack does not succeed (there is a recent patch for the CAN -2002-0392 Apache vulnerability).

In addition to those measures, the web application should be reviewed to ensure that input data is checked for meta characters as listed in chapter 2.3.2, and for too long input strings.

5 References:

All references used are web sites, as shown below:

Cisco IOS Command Reference Master Index, Release 12.0:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/rbkixol.htm

Information about the Cisco 7140 router:
http://www.cisco.com/univercd/cc/td/doc/pcat/ 7100.htm

Information about the Cisco 4840G load balancing switch:
http://www.cisco.com/univercd/cc/td/doc/pcat/ca4840g.htm

Information about the Cisco 1538 hub:
http://www.cisco.com/univercd/cc/td/doc/pcat/1538.htm

Checkpoint site – information about Firewall -1 (needs registration to access manuals)
http://www.checkpoin t.com

Stonesoft site – information about Stonebeat load balancing for Firewall -1:
http://www.stonesoft.com

Information about SNORT intrusion detection tool:
See: http://www.snort.org

Information about Trend Viruswall:
http://www.trendmicro.com/products/isvw/

Information about Sonicwall SSL accelerator:
http://www.sonicguard. com/

Several documents about firewall setup:
http://www.enteract.com/~lspitz/papers.html

FAQs and other information about Firewall -1
http://www.phonebo y.com/

Security testing methodology:
http://www.ideahamster.org/

nmap port scanning tool:
http://www.nmap.org

nessus vulnerability scanning tool:
http://www.nessus.org

Evaluation of IDS systems:
http://www.scmagazine.com/scmagazine/2001_12/pickof2001/c14/index.html

CERT – Computer Emergency Respo nse Team – may be used to find up -to-date security warnings:
http://www.cert.org

CVE – Catalogue of **C**ommon **V**ulnerabilities and **E**xposures:
http://www.cve.mitre.org/cve/

NIST database of vulnerabilities:
http://icat.nist.gov/icat.cfm

Securityfocus vulnerability database:
http://www.securityfocus.com/corporate/produ_cts/vdb

Cisco's product security advisories:
http://www.cisco.com/warp/public/707/advisory.html

An archive with good information on specific vulnerabilities:
http://archives.neohapsis.com/archives/vulnwatch/

Source of some freeware tools, e.g. password cracker:
www.oxid.it

A source of many security tools:
http://packetstorm.decepticons.org/

A catalogue with good description on vulnerabilities:
http://lists.insecure.org/bugtraq/

A freely available document called "A guide to buildi ng secure web applications and web services".
http://www.owasp.org

Steve Kiefling's paper, used as a basis for attacks in assignment 4:
http://www.giac.org/practical/Steve_Keifling_GCFW.doc

Gnu software for downloading all web site information:
http://www.gnu.org/software/wget/