Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 2.0 (revised May 26, 2003) for Alberto Partida

April 8, 2004

Humble fortune cookies

Abstract

This practical assignment aims at detailing the security architecture of a humble and recently created company named GIAC-Partida (GIAC-P). Although this company, GIAC-P, does not exist (yet), we are convinced that this imaginary and mostly theoretical exercise demonstrates the importance of the defence-in-depth security approach and the feasibility of basing core business processes on the Internet and on pieces of (some of them) open software.

This paper has four different parts. The first one introduces the technical platform initially selected to fulfil the business requirements and to implement the business processes.

The second part details the security policy of the company's border router, external firewall and VPN. This is complemented with a tutorial about the implementation of the firewall rules.

The third part describes a plan to validate the firewall policy and proposes future improvements for the network layout.

The third part presents three different proposals of attack against an already existing GCFW design (to the firewall itself, a rudimentary DDoS attempt and finally a plan to compromise an internal system).

The paper concludes with a final section numerating the Internet references consulted by the author to elaborate the assignment.

Index

1. Security Architecture

1.1 Definition of GIAC-P

GIAC-P sells fortune cookie sayings through the Internet. These sayings are predictions of the future conveyed in nicely elaborated and friendly sentences. They use to appear in little pieces of paper inside, of course, Chinese 'fortune cookies'.

The mission statement of GIAC-P is 'to provide Internet customers with fortune cookie sayings (an added value service) applying ethical, effective and efficient marketing and technical strategies always commensurate with the available resources'.

The budget and consequently the resources of GIAC-P are rather limited, but this fact will not prevent it to start up a sound and easy to further extend IT platform to leverage business processes. The mandate of the technical group in GIAC-P is enabling the company's business model with the simplest and easiest to support, maintain and evolve technical platform.

1.2 GIAC-P Business players

GIAC-P sells fortune cookie sayings to individuals and other companies using the Internet as their only communication, marketing and selling channel. The business players to consider are:

- Individual customers: Browsing the web, people around the globe can reach GIAC-P web site and order fortune cookie sayings.

- Corporate customers: Also through the web, other companies (mostly fortune cookie makers) can also order big numbers of fortune cookie sayings.

- Suppliers: Everybody can become a GIAC-P supplier. Fortune cookie saying writers can connect to GIAC-P web site and deliver their sayings.

- Partners: Fortune cookie sayings are translated to other languages so that non-English speaker markets can also take benefit of this product.

- GIAC-P employees: As the reader will notice, initially the number of GIAC-P employees is rather limited. All of them can be considered a mobile force.

- General public: The way the world has to get to know GIAC-P is through GIAC-

P web site.

1.3 Business processes for individual customers

The most important process for GIAC-P is selling fortune sayings to web users.

- A web user finds the GIAC-P web site and they decide to buy the GIAC-P standard product, i.e. a set of 5 fortune sayings (the content topic can be selected by the user e.g. love, empathy, social abilities, etc.)

- After accepting the legal terms of the selling process, the customer fills in a form with three necessary pieces of information:
    - Their full name.
    - Their email address.
    - A passphrase (chosen by the customer according to a passphrase building policy stated in GIAC-P web site) to enable afterwards the access to the set of sayings.

These steps constitute the standard information-retrieval process for all GIAC-P business-involved players: providing an email address and a passphrase chosen by them, which will authenticate them in future downloading processes.

- The user will then transfer the required amount of money to one of the GIAC-P bank accounts stating in the transfer subject the email address they used. GIAC-P has a local bank account number ready on every country where potential customers can appear so that it is always a local bank transfer for the customer.

- Once GIAC-P has checked that the money has been received, then an email is sent to the user with a customised (and secure) URL from which, after inserting the passphrase they chose, they can download the text file with the 5 fortune cookie sayings.

1.4 Business processes for corporate customers

The fortune cookie making industry can also be supplied with fortune sayings from the GIAC-P web site. The steps to be followed are just similar to the ones for individual customers:

- They insert their full name and their email address.
- They choose a passphrase.
- They transfer the required money to a GIAC-P bank account.
- GIAC-P sends the customer an email with a secure URL.
- The customer downloads the sayings from that URL.

Apart from the number of sayings that are offered in the industrial set: compressed text files with 1000, 5000 or 10000 sayings. Bank transfers are also always local to the cookie maker.

1.5 Business processes for suppliers

It is very easy to become a GIAC-P provider. If a web user decides to try out their luck and write some fortune sayings, they just have to:

- Accept the legal terms of the collaboration.
- Fill in a form with their name, email address and bank account number.
- Paste their creations in a page in the GIAC-P web site.

If GIAC-P considers their sayings worth-telling (and selling) then the corresponding amount of money will be transferred from the local GIAC-P bank account to the writer's bank account. This is the way GIAC-P opens the saying writing possibility to all web users.

1.6 Business processes for partners

Partners translate fortune sayings into other languages in order for GIAC-P to present the product to new potential markets. Partners, after agreeing on the legal framework, they also download their work packages (sets of fortune sayings to be translated into languages different to English) using the passphrase they chose and, after translating the sayings, they paste their work in a GIAC-P web page.

Currently the GIAC-P web site offers fortune sayings in French, German, Italian and Spanish.

Partners also resell fortune sayings (partners and resellers are the same players for GIAC-P). The reselling business process is identical to the process for corporate customers (they accept the legal terms and download sayings from the GIAC-P web site to resell them using the same mechanism employed by users, a customised and secure URL requiring a passphrase previously chosen by them).

Resellers transfer the saying package price to GIAC-P before the downloading process. GIAC-P will refund a percentage of the price to the resellers' bank account when GIAC-P has eventually acknowledged that the partners have resold the package. All bank transfers are also local to all resellers.

1.7 Business processes for employees

The number of GIAC-P employees is rather limited. They take care of the business processes here described and simultaneously they develop GIAC-P web site to make it every time more attractive and different.

There are three main functional staff groups: the sales force promoting the web site, the content-related employees and the IT staff. Back office tasks are performed by all of them due to the limited number of resources.

Let us remember that the GIAC-P web site is the only distribution channel for the GIAC-P fortune sayings. All GIAC-P employees can be on the road at any time, so it is essential that all their business processes can be performed remotely, among others they are:

- Maintaining and supporting the GIAC-P web site.
- Reading and evaluating new fortune sayings provided by suppliers.
- Inserting translated fortune sayings into the non-English GIAC-P web sites.
- Keeping track of user-related data and surveys.
- Operating online with all GIAC bank accounts.

1.8 Communication requirements for individual customers

Customers need to reach and interact with the GIAC-P web site using any updated web browser. This means that they require HTTP (for the public part of the web site) and HTTPS (for the private steps taken by the customer) protocols to interact with the GIAC-P web server. The address of the GIAC-P web server (www.giacp.com) needs to be known through the World Wide Web, so DNS is required.

GIAC-P sends and receives emails to their customers, so SMTP (and a corresponding mail server) is also required.

1.9 Communication requirements for corporate customers

Corporate customers require more bandwidth and the same protocols used by individual customers: HTTP, HTTPS, DNS and SMTP.

1.10 Communication requirements for suppliers and partners

Thanks to the simplicity of the initial GIAC-P business processes, suppliers and partners require the same protocols than customers: HTTP and HTTPS

(together, of course, with DNS) and SMTP for the email flow.

1.11 Communication requirements for employees

Employees not only require HTTP and HTTPS protocols to interact and check the both GIAC-P web sites (internal and external) and SMTP to reach all players but also a secure way to be able to administer, maintain and support GIAC-P systems. Keeping simplicity always in mind, technical GIAC-P employees decided to use SSH inside an IPSEC-based VPN.

After describing the business process and the access requirements, let us present the technical platform enabling GIAC-P business model. Needless to say that it follows the initial mandate of the technical group of the company: keeping a simple and easy-to-evolve (and secure) platform.

1.12 Table with communication requirements for all players

According to the description of GIAC-P business operations, every player requires some type of communication with the GIAC-P web site. Here is a table with a first summary of the different players and their communication requirements:

Players	Origin	Destination	Protocols
Individual customers/ Corporate customers/ Suppliers/ Partners	Any public IP address from Internet	External GIAC-P web server	HTTP (port 80) HTTPS (port 443)
	Any public IP address from Internet	External GIAC-P DNS server	UDP DNS queries (port 53)
	Any public IP address from Internet	External GIAC-P mail server	SMTP (tcp based, port 25)
Employees	Any public IP address from Internet/ Internal GIAC-P LAN	External GIAC-P web server	HTTP (port 80) HTTPS (port 443)
	Any public IP address from Internet/ Internal GIAC-P LAN	External GIAC-P DNS server	UDP DNS queries (port 53)

	Any public IP address from Internet/ Internal GIAC-P LAN	External GIAC-P mail server	SMTP (tcp based, port 25)
	Any public IP address from Internet/ Internal GIAC-P LAN	Internal GIAC-P mail server	SMTP (tcp based, port 25) POP 3 (tcp based, port 110)
	Any public IP address from Internet/ Internal GIAC-P LAN	Internal GIAC-P web server	HTTP (port 80) HTTPS (port 443)
	Any public IP address from Internet/ Internal GIAC-P LAN	Internal GIAC-P DNS server	UDP DNS queries (port 53)
	Any public IP address from Internet/ Internal GIAC-P LAN	Internal 'central' SSH server	SSH (tcp based port 22)
	Internal GIAC-P LAN	All internal servers	Full IP connection (in this first phase of GIAC-P, later on an internal firewall could come into play)

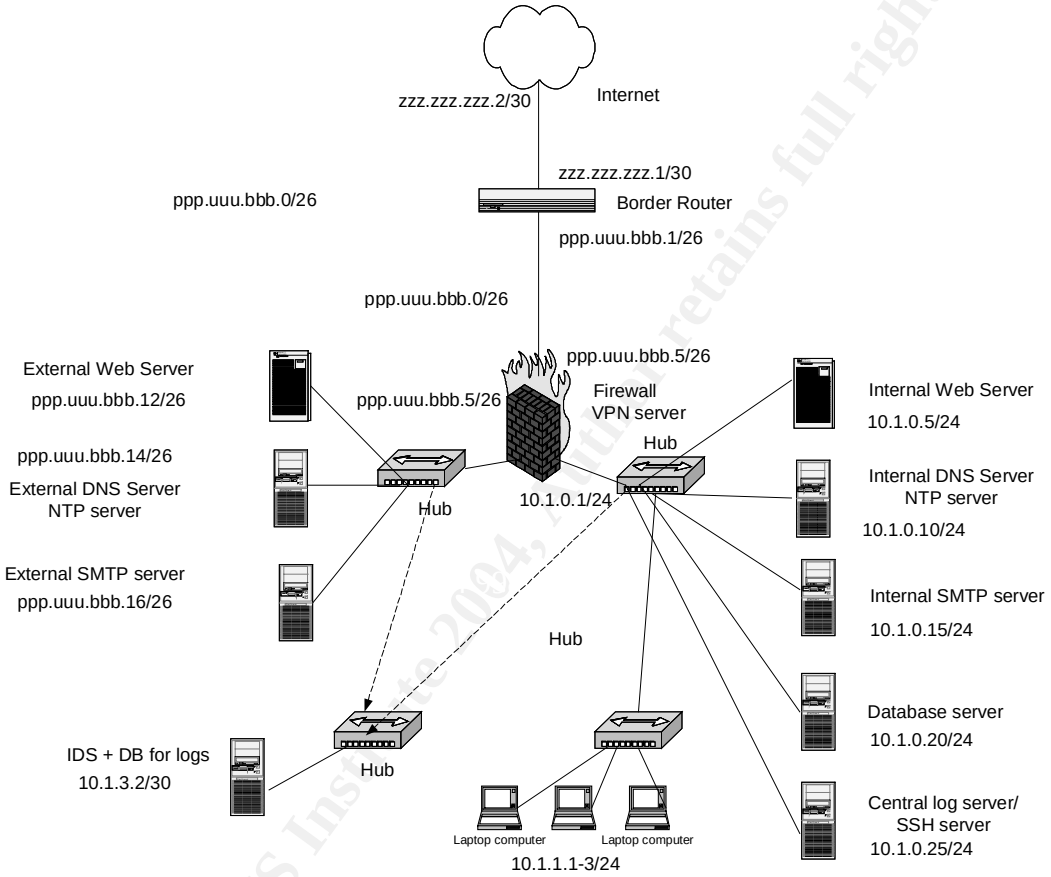
1.13 GIAC-P IP addressing schema

In order to sanitise all public addresses, we consider zzz.zzz.zzz.0 is the public network provided by the ISP to connect our external router and ppp.uuu.bbb.0 the public network we can deploy at GIAC-P.
Although currently there are no switches in the internal LAN, we already consider different sub-nets in the LAN to facilitate future migrations to a switched environment.

Network name/component	Network address	Network mask	Possible number of hosts
ISP-network	zzz.zzz.zzz.0	/30 - 255.255.255.252	2
Border router(serial)	zzz.zzz.zzz.1	/30 - 255.255.255.252	
Broadcast	zzz.zzz.zzz.3	/30 - 255.255.255.252	
DMZ	ppp.uuu.bbb.0	/26 - 255.255.255.192	62
Border router (eth0)	ppp.uuu.bbb.1	/26 - 255.255.255.192	
FW-external interface	ppp.uuu.bbb.5	/26 - 255.255.255.192	
FW-DMZ interface	ppp.uuu.bbb.10	/26 - 255.255.255.192	
External web server	ppp.uuu.bbb.12	/26 - 255.255.255.192	
External DNS server/ NTP server	ppp.uuu.bbb.14	/26 - 255.255.255.192	
External SMTP server	ppp.uuu.bbb.16	/26 - 255.255.255.192	
Broadcast	ppp.uuu.bbb.63	/26 - 255.255.255.192	
GIAC-P LAN servers network	10.1.0.0	/24 - 255.255.255.0	254
FW-internal interface	10.1.0.1	/24 - 255.255.255.0	
Internal web server	10.1.0.5	/24 - 255.255.255.0	
Internal DNS server/ NTP server	10.1.0.10	/24 - 255.255.255.0	
Internal SMTP server	10.1.0.15	/24 - 255.255.255.0	
Database server	10.1.0.20	/24 - 255.255.255.0	
Central log server/ SSH server	10.1.0.25	/24 - 255.255.255.0	
Broadcast	10.1.0.255	/24 - 255.255.255.0	
LAN workstations network	10.1.1.0	/24 - 255.255.255.0	254
Workstation 1	10.1.1.1	/24 - 255.255.255.0	
Broadcast	10.1.1.255	/24 - 255.255.255.0	
IDS server	10.1.3.2	/30 - 255.255.255.252	

1.14 GIAC-P network diagram

The following diagram shows GIAC-P network layout with the IP addressing schema. Although the diagram does not look terribly professional, GIAC-P IT staff prefer this approach because it clearly shows the real physical connections and network devices required.



1.15 GIAC-P technical platform first overview

The core element of the technical platform is certainly a web server to host the GIAC-P web site and to deliver the GIAC-P product. A second required element is an email server to contact customers (remember, the customised URL from which the customer can download the product is send to them vie email).

The key role played by the web site requires the existence of two different web servers, one external running production web pages and a second one (an internal web server) to design and test new web pages.

All sayings will be kept in a back-end system: a relational database storing all products in all languages.

As already mentioned in the required communications, it is evident that two DNS servers, one internal and the other external, are also required in GIAC-P technical platform. Two time servers (NTP), one internal and one external will provide the required time information for all logs.

For administration purposes, an ssh server in all boxes is also required.

The list of components ends up with:

- A border router as a first network device connected to the Internet.
- A firewall right after the border router to protect GIAC-P systems.
- A VPN server to enable remote administration of the platform (initially, in the same box as the firewall).
- A central log server.
- A network-based IDS to scan network traffic.
- A collection of hubs (to be substituted in the near future by layer-3 switches) to connect the servers (among others, the web servers and the database).

Let us detail each of these different components in the next sections. The order to present each component is from the most external to the most internal element.

1.16 Connection to the Internet

The way out to the world for GIAC-P is the Internet exclusively. Although initially the goals and resources of GIAC-P are rather humble and limited, GIAC-P Chief Information Officer and all the technical group decided to lease a T1 (or similar, e.g. a E1 in Europe) permanent connection to the Internet. This means a theoretical bandwidth of 1.5 Mbps for GIAC-P Internet systems provided by the local Internet Service Provider (ISP).

The estimated monthly rate for this ISP service is around 500$.

The bandwidth is considered to be initially sufficient to cater for business and administrational traffic. For instance, considering a potential number of 10000 customers (according to GIAC-P optimistic marketing people forecasts) exchanging every day on average 100 KB with the GIAC-P web site, less than 7% of the total possible traffic exchanged will be used.

Of course, it is clear that this calculation is a very rough one and it does not take occasional users browsing the web, administrational traffic and peaks of simultaneous customer HTTP requests.

1.17 Border router

The external interface of a middle-range Cisco 2600 router is connected to the T1 uplink. The estimated price of this router is 2000$. For information about this Cisco model, refer to http://www.cisco.com/warp/public/cc/pd/rt/2600/index.shtml

The purpose of this router is enabling the IP datagram routing function required to send IP datagrams from GIAC-P systems to the Internet and vice versa.

The security function the router performs is rather limited (but of importance within the defence in-depth security strategy followed in GIAC-P). Access control lists are present to allow only appropriate source and destination IP addresses. The router also performs additional tasks such as some protocol-specific blocking and filtering (as it will be seen in section 2 of this assignment).

The placement of the router as the very first network device attached to the Internet is due mainly to its routing functionality. All traffic to and from GIAC-P crosses this border and, for the time being, unique router.

The reason to choose a CISCO product is twofold. In the first place, the small technical team in GIAC-P has working experience with this vendor and, in the second place, plenty of literature and references (including SANS textbooks from this track) exist to configure and harden CISCO routers.

1.18 GIAC-P firewall

A 10 BASE T (twisted pair) Ethernet cable connects the internal interface of the CISCO 2600 directly to the external interface of a NOKIA firewall appliance running Checkpoint FW-1 NG/VPN-1.

For the feasibility analysis of GIAC-P, the price of each Ethernet cable has been considered 5$ (connectors and other accessories at 3$ each)

The model selected was the Nokia IP380, plenty of horsepower for the humble GIAC-P (see http://www.nokia.com/nokia/0,,43123,00.html). The price per unit reaches 10000$ (plus around 5000$ for the Checkpoint FW-1/VPN-1 SW)

The purpose of this stateful inspection firewall is clear: filtering all egressing and ingressing traffic from and to the two initial GIAC-P network segments, the DMZ and the LAN. It constitutes the basic pillar of the layered security strategy in GIAC-P. Source and destination IP addresses, transport-level ports and network and transport protocols are the parameters this firewall plays with.

The specific mandate behind the configuration of this firewall is 'allowing only those communications required by GIAC-P business processes'. No service, protocol, port or IP address apart from those specifically required to implement the business processes will be allowed to cross this firewall in any direction.

In addition to the FW-1 software, VPN-1 will be used in the same appliance, as we will see later on in a coming section.

The location of the firewall resembles a central point in a typical star topology. From the mere security viewpoint, de-coupling this centrally-located firewall into two different firewalls (an external and an internal firewall from different vendors, protecting the external network and the internal network) is very recommendable.

The reader at this point has to remember the humble resources available for this first life phase of GIAC-P. This should certainly be a future work direction for the GIAC-P CIO.

Two network internal interfaces are used in the firewall. The first one connects the firewall using a 10 BASE T Ethernet cable with a simple hub featuring the GIAC-P demilitarised zone (DMZ) hosting the web site. Six ports of this hub are used:

- The production external web server.
- The external DNS server and NTP server.
- The external SMTP server (email).
- Additionally, a port is used with a receive-only Ethernet cable (only traffic ingressing into the IDS) connected to a hub where a network-based Intrusion Detection System is connected.

It has to be mentioned that the author of this assignment has not tested empirically the connection of a receive-only Ethernet cable into a hub. Should this scenario not work, then a plain normal Ethernet cable could be used and a personal firewall could be used in the IDS server to avoid any egressing traffic.

The other internal interface of the firewall is connected to a second hub featuring

the GIAC-P (LAN) internal network (both hubs to be certainly substituted by a switch in the short term). At the moment, these are the four ports used:

- The development (and testing) web server.
- The (data) jewel of the crown: the relational database server.
- The NTP and DNS internal servers.
- The central log server and the central SSH server (from where connections to other internal boxes can be initiated).
- The internal email server.

As stated before, although currently there are hubs deployed in GIAC-P network, the technical team plan also to use switches instead of hubs once the team acquires enough knowledge and experience with the normal functioning of the network.

Let us also remember that a switch would require active management and configuration (and not a hub).

This firewall product was chosen for two reasons:
- The technical team had experience with Checkpoint FW-1.
- The use of an appliance combining FW and VPN capabilities was deemed to be appropriate for a start in terms of maintainability and support requirements.

1.19 The hub used in GIAC-P

The nice thing about using a hub is the lack of administrational duties. It is merely a link layer device that re-sends out through all its ports the traffic received. The selected hub is from Netgear, an easy-to-find and reliable product.

The only network function performed by a hub is to provide with a common network traffic to all elements connected to its ports.

No security function (nor insecure function) is actually performed by the hub. They are connected using 10 BASE T cables to the internal interfaces of the firewall.

The model selected by GIAC-P is the Netgear DS108 8 PORT 10/100 Mbps dual speed hub (see http://www.netgear.com/products/prod_details.php?prodID=69&view=sb for details).

The individual price for this hub is around 60$

1.20 The GIAC-P servers

Now it is the turn to introduce GIAC-P servers. It is worth mentioning that the operating system of these systems is FreeBSD production release 4.9 on Intel platforms(see http://www.freebsd.org/ for more information).

Any server used in the GIAC-P IT platform undergoes a hardening and secure configuration process (see http://www.FreeBSD.org/~jkb/howto.html) before being connected to the production network. Every server has only those required services enabled (the rest of the possible services are either not installed or disabled). Integrity checkers are also used in those file systems that are not planned to change frequently.

GIAC-P servers perform either a presentation-layer function (e.g. web servers) or a required service (e.g. email, DNS and NTP among others) or a back-end function (e.g. the database).

All servers have SSH servers installed to allow secure remote administration and maintenance. Additionally, SSH servers in internal servers can only be accessed from a specific box, the central SSH server in the internal network:

- This central SSH server will be the only one reachable from the VPN server (as we will see in the next section of this assignment).

Relaying only on a unique operating system has some advantages:

- The palette of OS knowledge required in the technical team is limited (remember GIAC-P resources are limited).
- Staying up-to-date in software updates and security patches in only one OS flavour is simpler than having various OSs.

But it also has some disadvantages (that become risks to be either accepted or mitigated by GIAC-P board):

- Should a vulnerability in the selected OS appear, the risks of being affected by e.g. a exploit (in the form of a worm or of any other type of attack) is high. This is a sample of some generic technical risks that have to be reported to the GIAC-P Board either for acceptance or mitigation.

Two different mitigation measures implemented are:

- The selection of an appliance based on a different operating system to act as the FW and the VPN server.

- A second mitigation measure defined in GIAC-P was to establish and swift and effective security vulnerability tracking and installing process, nicely inserted in

an effective change management process.

The selected hardware platform was ProLiant (HP) family:

- ML330 G3 for low-sized boxes (1 GB RAM memory, with a total estimated individual price of 1500$, see http://h18004.www1.hp.com/products/servers/proliantml330/ for more information).
- ProLiant ML530 G2 for our web servers (4 GB RAM memory and two processors with an individual price of around 7000$, see http://h18004.www1.hp.com/products/servers/proliantml530/ for information).

Again, here we main reasons to choose these servers were:
- Familiarity with the product.
- Short delivery time.
- Plans to agree on a framework contract with good economic conditions with a retailer located in the neighbourhood.

Generally, all software to be installed in these servers will be open-source based. Two main reasons for this:
- Limited economic starting capability for GIAC-P
- We would like to check whether it is actually feasible to base critical-business software on open-source bundles.

1.21 The GIAC-P web servers

The selected web server is Apache version 2.0.49 web server. Apache is a market leader and platform already known by our web developers (see http://httpd.apache.org/ for more details).

The security hardening of an Apache web server is very much linked with the hardening of the operating system it is running on (e.g. use of chroot, activate logging and configure proper access rights in the server).

The SSL module named mod_ssl comes from OpenSSL (see http://www.openssl.org/). This module provides SSL v2/v3 and TLS v1 support for the Apache HTTP Server.

The programming language chosen to implement all required functionality in the GIAC-P web site is PHP version PHP 4.3.5 (see http://www.php.net/), due to its speed and its resemblance to Java when writing lines of code.

1.22 The DNS servers

BIND version 9.2.3rc4 is the selected name server software (see http://www.bind.com/bind.html)

The main reason to choose BIND is experience with the software and its market leadership (and subsequently, finding knowledge about BIND in the IT labour market is feasible).

We have set up an internal and an external DNS server. The DNS server in the LAN (internal network) forwards, if necessary (i.e for addresses not in the internal network), DNS requests only to the DNS server in the DMZ.

The external DNS server performs DNS queries and serves DNS answers to Internet clients willing to connect with GIAC-P boxes in the DMZ.

1.23 The SMTP servers

The software used is Sendmail version 8.12.10 (see http://www.sendmail.org/). There are two email servers, the one in the DMZ receives and sends external emails. The one in the LAN is only for internal email (similar approach as the one followed with the DNS servers).

1.24 The VPN server

Here we will use an existing platform: The Nokia Firewall/VPN IP380 (again, see http://www.nokia.com/nokia/0,,43123,00.html) appliance with Check Point firewall/VPN technology and hardened Nokia platform with a security-specific operating system (IPSO). The price per unit reaches 10000$ plus around 5000$ for the Checkpoint VPN-1 SW and some additional 3000$ for the VPN Client required by the IT staff to connect remotely (see http://www.checkpoint.com/products/connect/vpn-1_clients.html.

1.25 The network IDS

Snort version-2.1.1 was the selected candidate (see http://www.snort.org/). In the same box My SQL was installed to store and study IDS data. The IDS will receive traffic from the DMZ and from the LAN, always after the FW, and using receive-only Ethernet cables.

There is a lack of experience with network-based IDS systems in GIAC-P, therefore there will be a fine-tuning phase in which alerts produced by the IDS will be customised to the GIAC-P network scenario.

1.26 The central log server and SSH server

A syslog server, together with swatch and scp (secure copy) are the key elements in our central log server. (see http://www.spitzner.net/swatch.html).

The latest version of OpenSSH will be used in all servers (see http://www.openssh.com/).

As long as these two services will be in the same hardware, we will use OS-based isolation measures (e.g. chroot or jail).

1.27 The NTP servers

The software used is NTP (version 4.2.0 released on 2003/10/15) (see http://www.ntp.org/downloads.html). The internal and the external NTP servers provide a synchronised time information pretty useful for the log information of all connected servers and networks devices.

1.28 The database server

Here the selected software is MySQL version 4.0. (see http://www.mysql.com/downloads/index.html). All fortune cookie sayings will be eventually stored in the database.

1.29 The backup policy

All servers in GIAC-P are weekly back up to a DVD (critical content-related servers such as the database and the web servers have a daily DVD-based backup process).

The CIO at GIAC-P knows that this is an interim solution till a new network (internal and completely isolated from the existing one could be used to perform backups more frequently).

1.30 GIAC-P workstations

GIAC-P staff uses two different types of laptops:
- Apple's iBook G4 (pretty elegant and full with graphic development tools).
- Intel-based laptops (running also FreeBSD).

All workstations can be either connected directly to the LAN or remotely via an ISP. All of them have been hardened and have personal firewalls.

1.31 The future layer-3 switch in the internal and the DMZ networks

The future layer-3 switch to be used in GIAC-P will be a Cisco Catalyst switch (exact model still to be chosen). The purpose of using a switch and not a simple hub is devoting the available bandwidth of all connected 10 BASE T (twisted pair) Ethernet cables (almost) entirely to the different types of traffic existing in GIAC-P. This means that database traffic should not occupy bandwidth in the cable connecting the development web server with the switch (and eventually with the firewall).

Switches offer some functionality that constitutes also a layer within the defence-in-depth security strategy followed in GIAC-P e.g. the creation of different virtual LANs (VLANs), one for the development web server and another for the database in the LAN and the same applies to the servers in the DMZ.

The location of this switch is really easy to be justified: the very first moment where traffic can be switched (i.e. sorting traffic according to its destination) is when it leaves central elements through which all traffic has to flow i.e. right after the firewall.

GIAC-P will decide to use Cisco Catalysts to look for administration and support knowledge synergies between the routers and the switches. In terms of budget, GIAC-P aimed at signing a framework contract with the vendor or a retailer to obtain a reasonable pricing.

1.32 Table with communication requirements for all servers

All GIAC-P servers require sending logs to the central log server. Additionally, NTP packets should arrive to all servers from the NTP servers. The following table describe all communication requirements for all GIAC-P servers:

Origin	Destination	Protocols/destination port	FW rule required
All DMZ servers	DMZ NTP server	NTP (UDP port 123)	No
All LAN servers	LAN NTP server	NTP (UDP port 123)	No
All DMZ servers	Central log server	Syslog (UDP based, port 514)	Yes
GIAC-P LAN central SSH server	LAN, DMZ servers and Internet	SSH (TCP port 22)	Yes
GIAC-P LAN central SSH server	LAN and DMZ servers and Internet	Sending ICMP echo request and receiving echo replies	Yes

1.33 Initial budget calculations

We paste a very rough calculation about the initial costs run by GIAC-P. The initial cost of the HW/SW platform proposed reaches 60000$.

Monthly running costs (including only ISP connection, physical office rental and typical commodities (e.g. electricity, physical security, etc.) could reach 8000$. Thus, if we consider that we could sell a 5-fortune saying set for around 10$, we would require, for example, 800 customers per month buying a 10$ set each just to cover our basic running costs.

It is also important to remember that human costs (salaries, social security, etc.) are not included in this easy calculation.

	Number	Unit price HW/SW	Total price	Running cost
Border router	1	2000	2000	
Internet connection	1		0	500
Cables	50	5	250	
Network accessories	50	3	150	
Firewall (HW+SW)	1	15000	15000	
VPN clients (25 users)	1	3000	3000	
Hubs	4	60	240	
Web servers	2	7000	14000	
Other servers	7	1500	10500	
Workstations	5	2000	10000	
			55140	
Renting space				5000

2. Security policy and tutorial

2.1 Border router configuration

GIAC-P has selected a Cisco Router model 2600. This router is the first network device owned by our company that an IP packet coming from Internet will cross through. Following our security approach based on defence in-depth (several consecutive security layers to protect our resources), we will establish some security measures in the router.

The first set of measures consists of configuring some general networking parameters in the router (e.g. enable an admin password, no servers, etc.).

The second set with some general parameters that can be configured for all interfaces in the router.

The third set deals with the packets coming from Internet and trying to traverse the serial external interface of the router. We will use an extended access control list (ACL).

The fourth set is similar to the second one but, this time, we will apply an extended ACL in the internal Ethernet interface to control generated in GIAC-P network segments.

Standard ACLs only check source IP addresses. Extended access control lists, in contrast, control source and destination IP address, protocol type, tcp/udp port and icmp type. We will perform static packet inspection applying extended ACLs in both router's interfaces.

The necessary information to elaborate this section has been extracted from the SANS Track 2 text books and from the Cisco Router 2600 configuration manual (see http://www.cisco.com/application/pdf/en/us/guest/products/ps259/c1069/ccmigration_09186a00801f6f6b.pdf), the Cisco IOS configuration fundamentals manual (see http://www.cisco.com/application/pdf/en/us/guest/products/ps1839/c1051/ccmigration_09186a00801235ba.pdf) and the Cisco IOS network management fundamentals manual (see http://www.cisco.com/application/pdf/en/us/guest/products/ps5187/c1051/ccmigration_09186a00801998c6.pdf)

2.1.1 General router configuration parameters

Now we will enumerate all the security configuration implemented in the GIAC-P border router. We will follow this approach: statement(s) introduced in the

router's command line plus explanation of the meaning of that statement(s) and a quick note on its importance.

Let us give the router a non-informative name:

hostname dwarf

Not everyone can configure the router:

The first thing to do is to establish and require a secure (MD5-based hash) password to be able to configure the router. This step is important because it will prevent anyone connecting to the router being able to modify its configuration.

service password-encryption
enable secret <password>

Disable unnecessary services:

The next step is disabling most of the services that are not required in a border router. The importance of disabling these services comes from the generic security rule to disable explicitly all functionality that is not necessarily required by our border router. This is the reason why we do not even mention the vulnerabilities linked with these services. They are disabled not only because of those vulnerabilities but rather because they are not required. Unnecessary complexity brings always more risks.

Although some of these services are not enabled by default, we just disable them explicitly to be fully certain of their non-existence in our border router.

We do not need the following services in the router running by default:

An HTTP server in the router.

no ip http server

A BOOTP server (there is nothing in the network requiring bootp to start).

no ip bootp server

A domain name server (DNS) in the router.

no ip name server

An SNMP server is not needed either.

no snmp server

Services running on ports lower than 20 (echo, discard, daytime and chargen).

no service tcp-small-servers
no service udp-small-servers

There is no need to provide via the network a list of logged-in users.

no ip finger

We are not using Cisco Discovery Protocol.

no cdp run

We do not need to send DNS queries from the border router.

no ip domain-lookup

A packet received by the router does not need the source address to specify its route.

no ip source-route

This banner will appear whenever someone will try to connect to the router. Although this measure does not have a technical impact, on legal terms it is advisable to remind potential visitors of the authorised uses only.

banner login /WARNING: Authorised uses only/

Regarding logging, we enable it. This set of logging-related commands is key to create a collection of logs that in our log server that could help us tracking an event and verifying the functioning of the router.

logging on

And send it to a box in our DMZ (from this box, the log files will be periodically retrieved by our internal log server via a NATed IP address).

logging <log server external NAT ip address: ppp.uuu.bbb.18>

Additionally, we set the trap up to notifications (Level 5: Normal but significant condition)

logging trap notifications

And we configure the syslog facility in which error messages are sent.

logging facility local5

Finally, we do not send the system logging messages to the console.

no logging console

Although already disable by default, we would also add the following line to disable autoloading of configuration files from a network server.

no service config

And we provide information about the timestamps information we would like to add in the debugging and system logging messages.

service timestamps log datetime localtime show-timezone

We also inform the router about the location of our NTP server

ntp server <NTP server ip address: ppp.uuu.bbb.14>

2.1.2 Interface configuration

The next thing to do is applying the interface configuration on both interfaces, the Serial and the Ethernet one.

For the Serial:

interface Serial 0/0
ip address zzz.zzz.zzz.1 255.255.255.252

And for the Ethernet:

interface Ethernet 0/0
ip address ppp.uuu.bbb.1 255.255.255.192

The following interface-bound commands will be enforced in all interfaces:

The router will no send out information about our internal environment.

no ip unreachable

No interface will provide information about the net mask. ICMP unreachable

messages will be stopped.

no ip mask-reply

The router will not attend redirect messages

no ip redirect

The router will prevent malicious broadcasts from causing denial of service issues.

no ip direct-broadcast

The router will be configured not to accept and respond to proxy ARP.

no ip proxy arp

Currently, our network administrator can only configure the router only from the console, so we create a very simple ACL (deny access from all IP addresses outside the router) and we apply it:

access-list 4 deny any
line vty 0 4
access-class 5 in

2.1.3 Ingress ACLs for the Serial interface

The first thing we will accomplish is not allowing packets coming from Internet with a private source address (following RFC 1466, see http://www.iana.org/assignments/ipv4-address-space).

Before continuing, let us have a look at the syntax of an extended ACL:

access-list + number (from 100 to 199) + action (deny or permit) + protocol + source address + network mask (following the opposite designation convention typical from Cisco) + destination address + log action (if required)

Blocking rules according to the non-expected source IP address:

access-list 102 deny ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log

We also block the typical DHCP failed address by default

access-list 102 deny ip 169.254.0.0 0.0.255.255 any log

The loopback address.

access-list 102 deny ip 127.0.0.0 0.255.255.255 any log

Multicast and reserved addresses.

access-list 102 deny ip 223.0.0.0 32.255.255.255 any log

From our GIAC-P DMZ including .63 and .0 addresses of GIAC-P public range to prevent multicast related attacks:

access-list 102 deny ip ppp.uuu.bbb.0 0.0.0.63 any log

We will also have to add to these rules the legal IP addresses that are reserved by IANA and therefore, not legal addresses to be used in Internet yet. This list needs to be periodically checked, since it could vary.

We do not numerate all the respective ACLs here because it does not add any additional information to this section (and there is a size limit to this assignment).

Incoming ICMP traffic with echo, redirect and mask-request packets:

access-list 102 deny icmp any any redirect log
access-list 102 deny icmp any any mask-request log
access-list 102 deny icmp any any echo log

Regarding ICMP, the only thing we have to allow is ICMP echo reply (and packet-too-big messages, but these ones will initially not be accepted by the firewall, so we expect this last rule not to be applicable) coming to our DMZ.

access-list 102 permit icmp any ppp.uuu.bbb.0 0.0.0.63 echo-reply log
access-list 102 permit icmp any ppp.uuu.bbb.0 0.0.0.63 packet-too-big

Blocking ports used by unacceptable (and unnecessary for GIAC-P) protocols:

A non-comprehensive list of the ports to be closed (for both udp and tcp protocols) is the following:

tcpmux, echo, finger, all r-command protocols such as rlogin, who, sunrpc, sundup, discard, sysstat, daytime, netstat, chargen, ftp, ftp-data, talk, whois, bootp, tftp, protocols - finger, all the various netbios flavours, rexec, xwindows, snmp, syslog, etc.

Although we could imply that these ACLs are actually not needed since the last

rule (the deny the rest rule) will catch all these protocols, following this explicit approach we will be able to discover, having a look at the logs, which ports have been the most hit ones.

All these ACLs will always have a similar aspect:

access-list 102 deny tcp any any eq <port number> log
access-list 102 deny udp any any eq <port number> log

And now probably the most important thing, the business-related rules:

The first thing we do is allowing responses to the TCP communications established from the DMZ.

access-list 102 permit tcp any ppp.uuu.bbb.0 0.0.0.63 established

The following is allowing access to ports 80m and 443 in our web server. Note that, at the router level, we are not talking about protocols but just about ports.

access-list 102 permit tcp any ppp.uuu.bbb.12 eq 80
access-list 102 permit tcp any ppp.uuu.bbb.12 eq 443

Our external DNS server also needs to receive UDP packets in port 53.

access-list 102 permit udp any ppp.uuu.bbb.14 eq 53

The next one is our SMTP server requiring TCP access to port 23.

access-list 102 permit tcp any ppp.uuu.bbb.16 eq 25

The VPN tunnel for our IT staff also needs to be established (instead of allowing any IP connection attempt to any port to our firewall. we plan to limit this to the apparently required IPSEC port 500 and the esp protocol):

access-list 102 permit udp any ppp.uuu.bbb.5 eq 500
access-list 102 permit esp any ppp.uuu.bbb.5

And finally, let us deny all the rest coming in:

access-list 102 deny ip any any log

We just only need to enable the access-list 102 on the serial interface:

interface Serial 0/0
ip access-group 102 in

2.1.4 Egress ACLs for the Ethernet interface

This section is similar to the previous section, especially the first general rules, but now applied to the Ethernet interface facing GIAC-P network. Let us have a closer look:

Again, the first thing we will accomplish is not allowing packets coming from Internet with a private source address (following RFC 1466, see http://www.iana.org/assignments/ipv4-address-space).

Blocking rules according to the non-expected source IP address. In this segment packet with private IP addresses are not expected:

access-list 108 deny ip 192.168.0.0 0.0.255.255 any log
access-list 108 deny ip 10.0.0.0 0.255.255.255 any log
access-list 108 deny ip 172.16.0.0 0.15.255.255 any log

We also block the typical DHCP failed address by default

access-list 108 deny ip 169.254.0.0 0.0.255.255 any log

Similarly for the loopback address.

access-list 108 deny ip 127.0.0.0 0.255.255.255 any log

Identically for multicast and reserved addresses.

access-list 108 deny ip 223.0.0.0 32.255.255.255 any log

We will also have to add to these rules the legal IP addresses that are reserved by IANA and therefore, not legal addresses to be used in Internet yet. This list needs to be periodically checked, since it could vary.

We do not numerate all the respective ACLs here because it does not add any additional information to this section (and there is a size limit to this assignment).

For (improbable) troubleshooting, we will allow some outgoing ICMP traffic, although we expect the last two rules not to be applicable since we will not allow packet-too-big and mask-request ICMP messages in the firewall.

access-list 108 permit icmp ppp.uuu.bbb.0 0.0.0.63 any echo
access-list 108 permit icmp ppp.uuu.bbb.0 0.0.0.63 any packet-too-big
access-list 108 permit icmp ppp.uuu.bbb.0 0.0.0.63 any mask-request

Regarding echo replies from our DMZ, they will be denied.

access-list 108 deny icmp any any echo-reply log

The same applies for ICMP host-unreachable messages and time exceeded:

access-list 108 deny icmp any any host-unreachable log
access-list 108 deny icmp any any time-exceeded log

Blocking ports used by unacceptable (and unnecessary for GIAC-P) protocols:

A non-comprehensive list of the ports to be closed (for both udp and tcp protocols) is the following:

tcpmux, echo, finger, all r-command protocols such as rlogin, who, sunrpc, sundup, discard, sysstat, daytime, netstat, chargen, ftp, ftp-data, talk, whois, bootp, tftp, protocols - finger, all the various netbios flavours, rexec, xwindows, snmp, syslog, etc.

Although we could imply that these ACLs are actually not needed since the last rule (the deny the rest rule) will catch all these protocols, following this explicit approach we will be able to discover, having a look at the logs, which ports have been the most hit ones.

All these ACLs will always have a similar aspect:

access-list 108 deny tcp any any eq <port number> log
access-list 108 deny udp any any eq <port number> log

And now probably the most important thing, the business-related rules:

The first thing we do is allowing tcp communications established from the DMZ.

access-list 108 permit ip ppp.uuu.bbb.0 0.0.0.63 any

And finally, let us deny all the rest coming out:

access-list 108 deny ip any any log

We just only need to enable the access-list 108 on the serial interface:

interface Ethernet 0/0
ip access-group 108 out

To finalise this section, a word about the order of the rules. As we will see with the firewall rules, two different parameters are to be considered:

- The ’most hit’ rule should be at the top
- The ’protecting rules’ (related to possible attacks) should prevail above the functional (business related) rules.

More about this can be read in the section about the firewall rules.

2.2 *Firewall policy*

Our GIAC-P firewall implements stateful inspection. In contrast to the packet-filtering approach of the border router, the stateful inspection firewall monitors the state of the connection and compiles the information in a state table.

Let us start showing the whole rule base to be installed in the firewall:

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	* Any	GP-ExtFWaVPN	* Any	drop	Log	* Policy Targets	* Any
2	* Any	GP-ExtWeb	TCP http TCP https	accept	Log	* Policy Targets	* Any
3	* Any	GP-ExtDNSaNTP	UDP domain-udp	accept	Log	* Policy Targets	* Any
4	* Any	GP-ExtSMTP	TCP smtp	accept	Log	* Policy Targets	* Any
5	GP-ExtDNSaNTP	* Any	UDP domain-udp UDP ntp-udp	accept	Log	* Policy Targets	* Any
6	GP-ExtSMTP	* Any	TCP smtp	accept	Log	* Policy Targets	* Any
7	GP-IntDNSaNTP	GP-ExtDNSaNTP	UDP ntp-udp UDP domain-udp	accept	Log	* Policy Targets	* Any
8	GP-MobileITgroup@Any	GP-IntLOGaSSH	TCP SSH	Client Encrypt	Log	* Policy Targets	* Any
9	GP-MobileITgroup@Any	GP-IntSMTP	TCP pop-3 TCP smtp	Client Encrypt	Log	* Policy Targets	* Any
10	GP-MobileITgroup@Any	GP-IntWeb	TCP http TCP https	Client Encrypt	Log	* Policy Targets	* Any
11	GP-MobileITgroup@Any	GP-IntDNSaNTP	UDP domain-udp	Client Encrypt	Log	* Policy Targets	* Any
12	GP-DMZservers	GP-IntLOGaSSH	UDP syslog	accept	Log	* Policy Targets	* Any
13	GP-IntLOGaSSH	* Any	TCP SSH ICMP echo-request	accept	Log	* Policy Targets	* Any
14	GP-LANWS	* Any	TCP http TCP https	accept	Log	* Policy Targets	* Any
15	* Any	GP-IntLOGaSSH	ICMP echo-reply	accept	Log	* Policy Targets	* Any
16	* Any	* Any	* Any	drop	- None	* Policy Targets	* Any

As we can see, the number of rules has been kept quite reduced. The order of the rules will be explained in the firewall policy tutorial. We also try not to merge protocols and servers in the same rule. All required protocols appear only linked to the objects that really need them.

Initially, we have enable logging for all of them, so that we can keep track of all hit rules.

2.2.1 Creation of the first rule: protecting the firewall

For every rule, we will describe the general purpose of the rule and its importance within the comprehensive security approach of defence-in-depth. Some of the rules deal with the same scenario treated by some border router

ACLs.
This is the result of applying the defence-in-depth approach. The definite goal is: should one of the defensive layers become vulnerable, we will still have at least an additional security layer taking care of the same scenario.

The very first need (rule 1) is avoiding any connection from any IP source address directly to the firewall. It is not required and it constitutes a risk to our security infrastructure. Should our firewall be compromised, then we could be exposing our entire network to the Internet.

2.2.2 Allowing HTTP(S) + DNS queries + SMTP

Rules from 2 to 4 allow connections required for the GIAC-P business (always according to part 1 of this assignment):

- Any IP address can connect to the external GIAC-P web server using http and https. Internet users should be able to browse GIAC-P external web site.

- Any IP address can connect to the external DNS server using UDP-based DNS queries. This is required for all players to be able to know public GIAC-P server's IP addresses (basically the external and the external mail server).

- Finally, GIAC-P should also be able to receive emails into their external mail server. Therefore, we allow any IP address in the Internet to connect to the SMTP port using SMTP protocol to leave emails.

2.2.3 Outgoing DNS and NTP queries

Rule 5 allows the external DNS server in GIAC-P to send UDP-based DNS queries to any IP address in the Internet. This permits GIAC-P users to get public IP addresses of external boxes located in the Internet.

Rule 5 also allows UDP-based NTP-queries to any IP address in the Internet (this rule could be further limited to only those IP addresses of the time servers we really want them to be our external time reference).

2.2.4 Outgoing SMTP emails

Rule 6 allows the external GIAC-P mail server to contact via SMTP (TCP-based) any server to emails. This rule fulfils, as the previous ones, a basic communication requirement for the business of GIAC-P.

2.2.5 DNS and NTP from internal to the DMZ

In rule 7 we allow communications between the internal DNS and NTP server to the external one. Obviously, only using UDP-based DNS and NTP queries. We require this rule so that:

- The internal employees can resolve public names (e.g. to be able to find the IP address of web servers they would like to browse).
- The internal time server can be synchronised with the external one (and eventually all our logs will be also using the same time reference).

2.2.6 VPN-1 Traffic for IT Staff

Rules 8 to 11, related to the VPN gateway, will be treated in the next section (dealing with the VPN policy).

2.2.7 Syslog from GIAC-P DMZ to the log server

All servers in the DMZ should be able to use UDP-based syslog protocol to send their log to the internal log server. This is a key step to have in a centralised (and internal) location all logging information.

2.2.8 Echo requests and SSH to everywhere from the central SSH server

IT admins in GIAC-P enjoy the possibility to send ICMP-based echo requests and talk SSH to any IP address (DMZ and the external world) from the central admin point, the internal SSH server. This is the reason of rule 13.

2.2.9 Web access for our LAN

Internal GIAC-P employees require to total web access to the Internet. Thus, in rule 14 we have allowed them to use HTTP and HTTPS to any IP address in the Internet.

2.2.10 Echo replies can reach our central admin point

Rule 15 is the complements rule 13. If IT admins can send ICMP-based echo requests to all Internet, they should also be able to receive the answers (the echo replies).

2.2.11 The final any to any rule

Rule 16 ends up denying all the possible communications that have not been specifically mentioned before. This rule is of the utmost importance since is the closing point of our firewall: everything that has not been previously treated will

be dropped.

2.2.12 Banning and additional rules

As a closure for this section dealing with firewall ruling, we would like to add two future work directions:

- After a thorough look at the first firewall logs, we could maybe discover specific ranges of IP addresses that are trying everything to break into our systems. In order to mitigate that, we would add right after rule number 1 a rule dropping all services from that IP range.

- In the SANS track 2 classes, it was mentioned that the IDENT protocol directed to an SMTP server, if not used, should be rejected (and not only dropped) to avoid an unnecessary waiting time in the SMTP server.

2.3 VPN policy

Configuring the VPN-1 policy is identical to configuring the firewall rule base. Firewall rules related with the VPN will also be listed in the normal rule list but they can be recognised by the action chosen ('client encrypt') and the source object (our 'mobile IT force').

2.3.1 VPN configuration

The VPN will be based on IPSEC encapsulation. We have chosen to use IKE as the client authentication method (logging successful authentication). Users will be authenticated using a login name and an individualised password.

Users (GIAC-P IT mobile force) can connect from any IP address and they must have the VPN-1 secure client. When they connect, the desktop security inbound and outbound rules (to be discussed later on) will be enforced.

2.3.2 VPN-related firewall rules

Rules from 8 to 11 deal with the VPN traffic between the VPN clients (used by GIAC-P mobile IT staff) and GIAC-P network. Attending to the business requirements, they require:

- Encrypted access to the internal SSH server via SSH protocol (rule 8).
- Encrypted access to the internal email server via POPv3 and SMTP (rule 9).
- Encrypted access to the internal web server using HTTP and HTTPS (rule 10).
- Encrypted access to the internal DNS server using UDP-based DNS queries (rule 11).

2.3.3 Inbound desktop security rules

Rules 1 to 4 complement rules 8 to 11 present in the firewall.

- Access from the internal SSH server via SSH protocol to their box is allowed and encrypted (rule 1).
- Access from the internal email server via POPv3 and SMTP to their box is allowed and encrypted (rule 2).
- Access from the internal web server using HTTP and HTTPS to their box is allowed and encrypted (rule 3).
- Access from the internal DNS server using UDP-based DNS requests to their box is allowed and encrypted (rule 4).

Rule 5 is the closing one: No other possible communication is allowed.

2.3.4 Outbound desktop security rules

Rules from 6 to 9 deal with the VPN traffic between the VPN clients (used by GIAC-P mobile IT staff) and GIAC-P network. Attending to the business requirements, they require:

- Encrypted access to the internal SSH server via SSH protocol (rule 6).
- Encrypted access to the internal email server via POPv3 and SMTP (rule 7).
- Encrypted access to the internal web server using HTTP and HTTPS (rule 8).
- Encrypted access to the internal DNS server using UDP-based DNS queries (rule 9).

Rule 10 is the closing one: No other possible outbound communication is allowed.

Inbound Rules

NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK
1	GP-IntLOGaSS	All Users@Any	TCP SSH	Encrypt	Log
2	GP-IntSMTP	All Users@Any	TCP smtp TCP pop-3	Encrypt	Log
3	GP-IntWeb	All Users@Any	TCP http TCP https	Encrypt	Log
4	GP-IntDNSaNTF	All Users@Any	UDP domain-udp	Encrypt	Log
5	* Any	All Users@Any	* Any	Block	- None

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK
6	All Users@Any	GP-IntLOGaSS	TCP SSH	Encrypt	Log
7	All Users@Any	GP-IntSMTP	TCP smtp TCP pop-3	Encrypt	Log
8	All Users@Any	GP-IntWeb	TCP http TCP https	Encrypt	Log
9	All Users@Any	GP-IntDNSaNTF	UDP domain-udp	Encrypt	Log
10	All Users@Any	* Any	* Any	Block	Log

2.4 Firewall policy tutorial

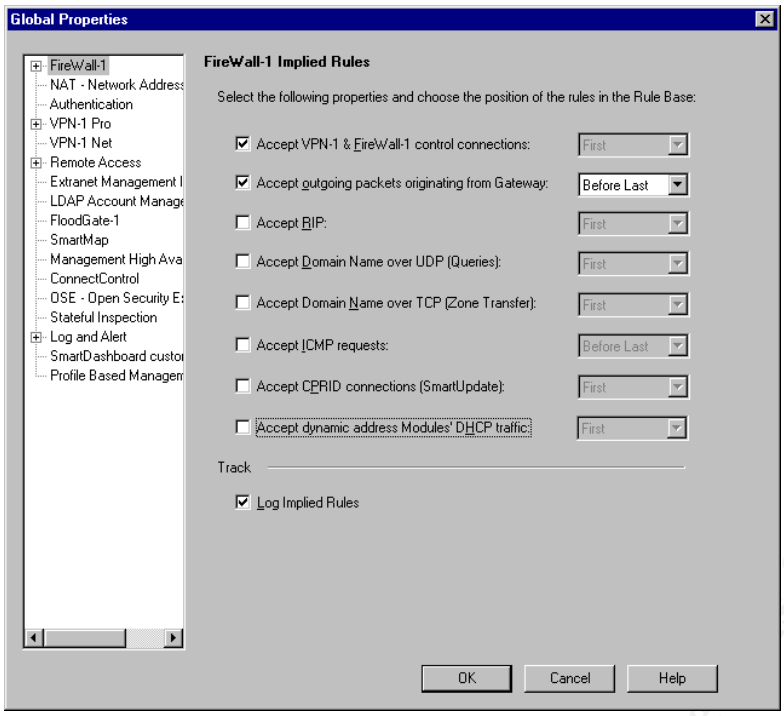
The software we use to configure the firewall policy is SmartDashboard NG Feature Pack 3 - Build 53933 from Checkpoint Next Generation. We have followed the user manual titled 'Getting Started' provided with the software package. Additionally, it is also necessary to remember a classical and didactic URL for these cases: http://www.spitzner.net/rules.html

The initial steps to be able to configure the firewall are:
- Creation of an administrator user to access the management module (called SMART client) of the firewall with read and write privileges.
- Installation of the SmartDashboard in the GIAC-P FW administrators' laptop.
- The administrator's LAN-based IP address will be registered as a valid address to administer the firewall from.
- The administrator will be authenticated by the firewall with a username and a password.
- Now they administrator is able to enforce policies.

As stated in the online help: 'The SmartCenter Server verifies that the Client's IP address belongs to an authorised GUI Client, and sends back a certificate'.

2.4.1 Preliminary settings

Before starting to define the objects and rules required, we have an initial look at the different menu options in the GUI and discover a collection of very important preliminary settings named 'Global Properties'. In the Firewall-1 section we configure:

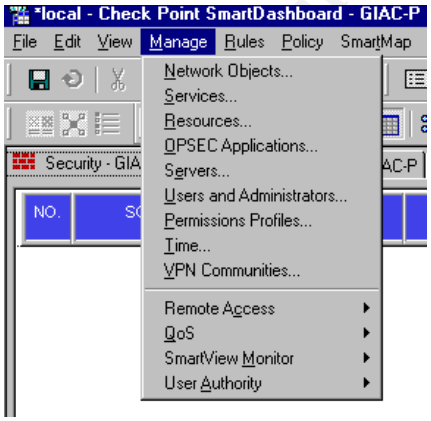


These implied rules will be applied by the firewall and, interestingly enough, they will not appear in the firewall rule base. Only the first two possibilities (accept VPN-1 and FW-1 control connections and accept outgoing packets originating from the gateway) will be required. The rest can be disabled. Finally, we also tick the logging option.

2.4.2 Creation of all host objects

In order to build the rule base, we need to build the subject elements of the rules i.e. the networks, the gateways and the existing hosts. Let us start with the external hosts:

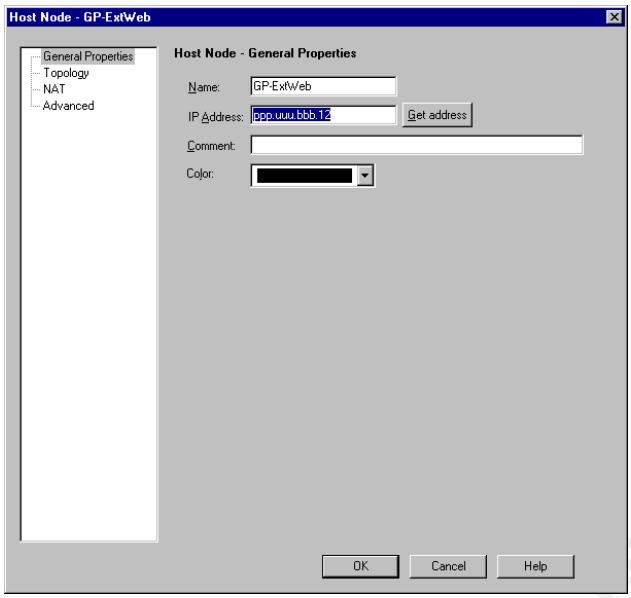
- In the Manage menu we choose the first option, Network Objects:



And we define the objects existing in the GIAC-P network:

A new little window will appear and, once there, we will press the New... button; a new menu will appear and in this one we will choose Node > Host.

This drawing is an example of the creation of an object (in this case, the external web server; GP stands for GIAC-P):



The same procedure will apply for all necessary hosts. Here is the list for all declared objects (hosts, gateways and networks):

Host	Name	IP address	NAT address
External web server	GP-ExtWeb	ppp.uuu.bbb.12	Static NAT 10.1.0.2
External DNS server/ NTP server	GP-ExtDNSaNTP	ppp.uuu.bbb.14	Static NAT 10.1.0.3
External SMTP server	GP-ExtSMTP	ppp.uuu.bbb.16	Static NAT 10.1.0.4
Internal web server	GP-IntWeb	10.1.0.5	
Internal DNS server/ NTP server	GP-IntDNSaNTP	10.1.0.10	static NAT ppp.uuu.bbb.22
Internal SMTP server	GP-IntSMTP	10.1.0.15	static NAT ppp.uuu.bbb.20
Database server	GP-IntDB	10.1.0.20 (not used so far)	

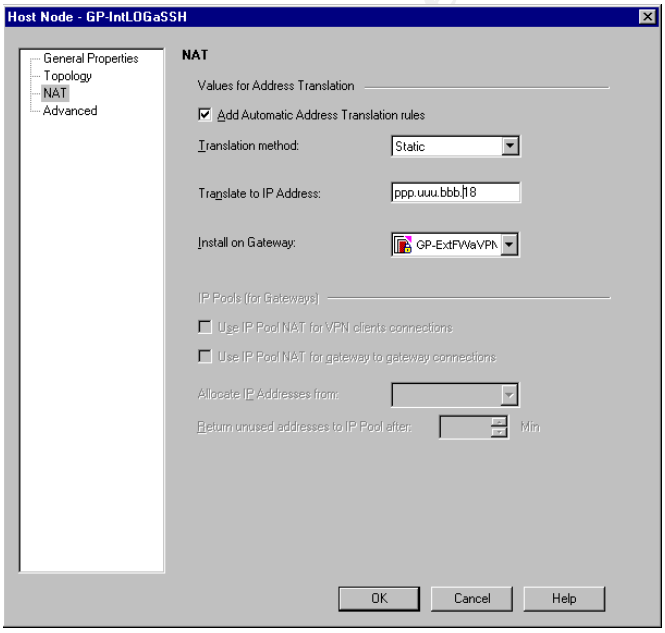
Central log server/ SSH server	GP-IntLOGaSSH	10.1.0.25	static NAT ppp.uuu.bbb.18
Networks			
GIAC-P DMZ servers	GP-DMZservers	ppp.uuu.bbb.0 mask 255.255.255.192	
GIAC-P LAN workstations	GP-LANWS	10.1.1.0 mask 255.255.255.0	hide NAT ppp.uuu.bbb.24
Gateway			
GIAC-P FW&VPN-1	GP-ExtFWaVPN	ppp.uuu.bbb.5	

2.4.3 Use of network address translation

The use of 'NATed' addresses ('static' for some specific internal servers and 'hide' for the internal LAN) is essential for:

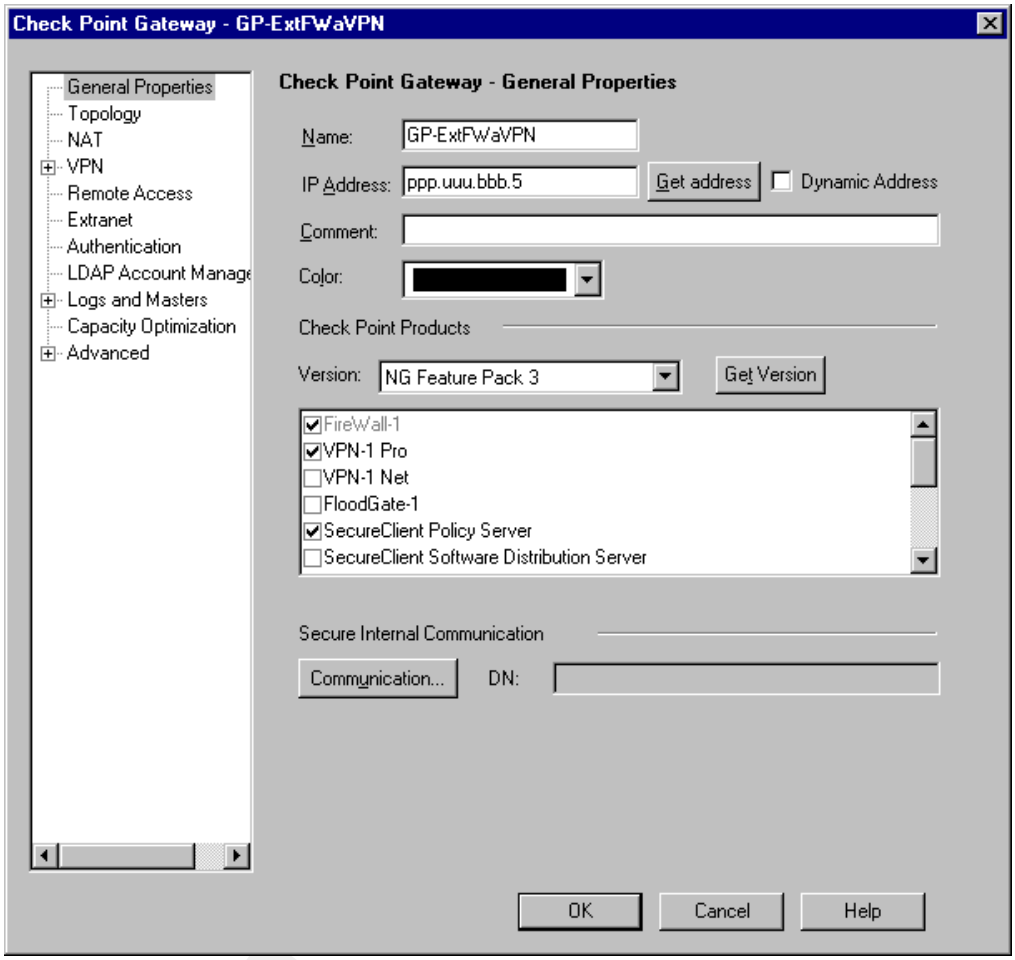
- The internal servers to be reachable from the VPN clients.
- The external servers to be reachable by the LAN servers and workstations.
- The internal LAN clients to browse the Internet.

The way to configure this address translation in the NG Dashboard is right-clicking into the respective objects and introducing the required translation method (initially, hide for entire networks and static for individual servers), the public IP address and the firewall object where this information will be installed:

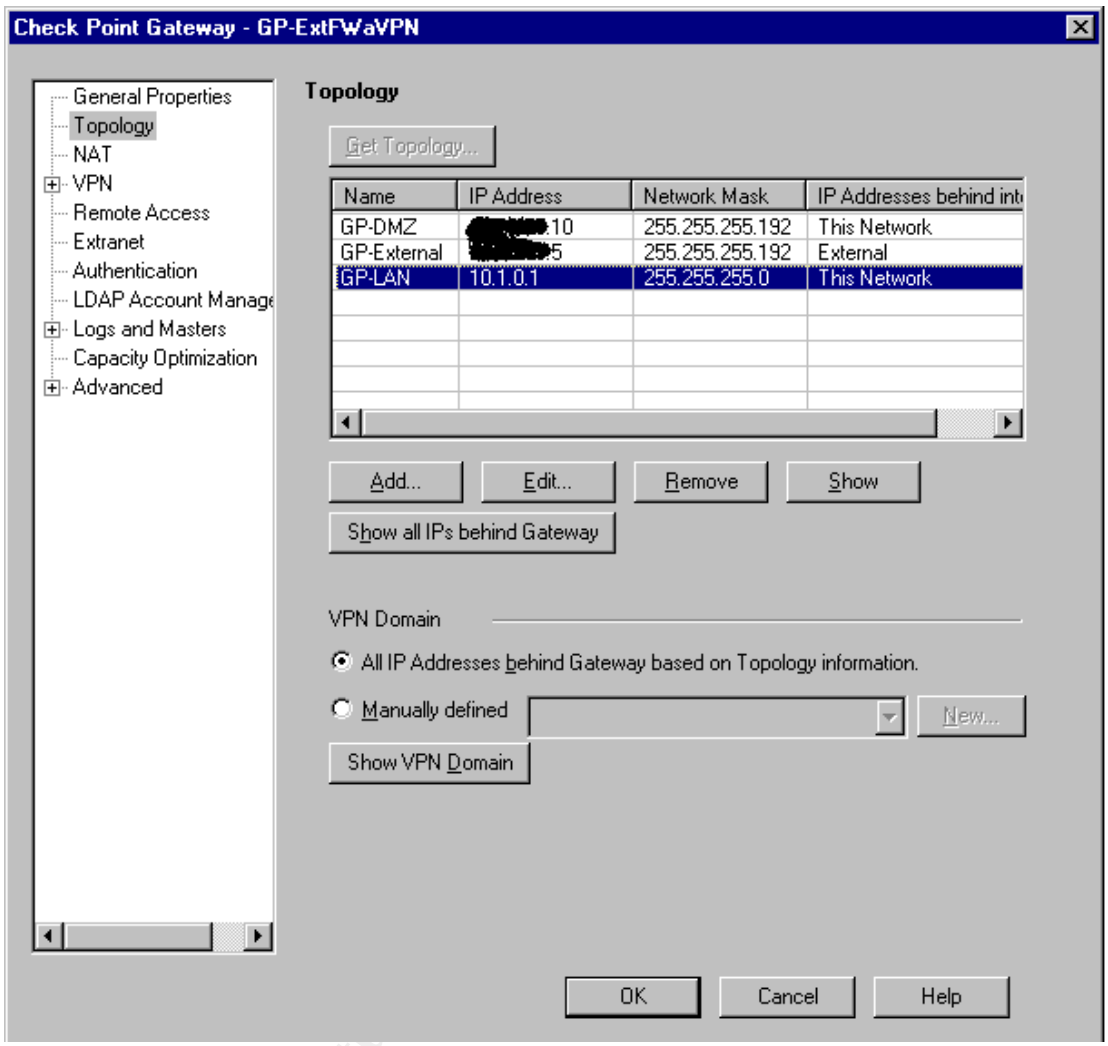


2.4.4 Creation of the gateway object

Similarly, we have to build the gateway object i.e. the external GIAC-P firewall. We would initially add its external public IP address and we also state the software products that will be running on it (FW-1, VPN-1 Pro and SecureClient Policy Server). This is how the object creation window appears:



In the subsection named Topology, we create three different networks, GP-DMZ, GP-LAN and GP-External. We add the respective IP addresses the firewall has in every of these networks and the network masks. All this can be seen in the following figure (please note that the ppp.uuu.bbb.10 and ppp.uuu.bbb.5 addresses have been hidden because the SmartDash GUI (quite rightly) does not admit letters in an IP address:



2.4.5 Creation of the first rule: protecting the firewall

The very first rule we create is to protect the firewall. No IP-address can access GP-ExtFWaVPN (this expression stands for GIAC-P External FW and VPN).

In order to create the rule, we have to go to the Rules menu and select Add Rule (this time, in the Top). Instantly, we already have a generic rule in the base. Now it is time to modify it according to our needs:

- In the source column, we click the right button of the mouse when the cursor is above the first word any in the rule. This way, we add the object we require. In this case, it is any, so nothing changes.

- We proceed similarly in the destination column, but this time we choose the object GP-ExtFWaVPN (should we select the wrong object, we just have to right click that wrong object in the rule and select 'delete' (the rule will remain, but the object will be deleted).

- IF VIA is a column important if we had defined different remote VPN communities, but this is not the case in GIAC-P (yet). By default, the value is filled in with Any (this always means any IP address).

- Service: In this column the name of the protocol serviced is inserted (obviously, we will use the value Any if the rule applies for all ports). In reality, this column only focuses on the port the protocol is going to use. Additionally, the source port of the service can also be stated in the description of a service object and, for some specific protocols (either well known or vendor-related); there is even the possibility to restrict the communication to them:

CIFS, DNS_TCP, FTP, FTP_PASV, FTP_PORT, FW1-CVP, H.323, HTTP, IIOP, INSPECT, NetShow, PNA, RSHELL and RTSP.

- The action chosen is drop: so the packet will not reach its destination. The other possible action, obviously, is accept. These are not the only possible actions: reject, user and client authentication and session authentication are also possible (but barely used in our case).

- The track column relates to the logging functionality. We have decided to log these attempts. Other possible values are none (i.e. no log), account, alert, snmptrap, mail and user defined. Initially, we will keep logs for all our rules and, most important, we will define a log-monitoring and checking process so that we can evaluate how our firewall policy is performing.

- Install on refers to the enforcement modules in which this rule will be applied (useful to centrally manage a complex network with various FWs.

- Time: we can even define the period of time (in hours and even in days in a month) during which this rule will apply.

- Finally, there is a comment column to add additional comments for the administrators.

These three last fields will not be used throughout our whole rule base (therefore, we will not refer to them anymore).

Finally, the first rule states the following:

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIM
1	* Any	GP-ExtFWaVPN	* Any	drop	Log	* Policy Targets	* Any

2.4.6 The order of the firewall rules

Let us remember that firewall rule enforcement follow a top-down approach. For every packet arriving at the firewall, the enforcement module will compare the IP datagram fields (source, destination, ports, protocols, etc.) with the rule base, starting from rule number 1 and continuing in an ascending order (rule 2 before rule 3 and so on).

Consequently, in order to save resources and improve performance, the 'most hit' rules should be placed on top of the 'least hit' rules. Obviously, this approach requires periodic log monitoring to check whether the rule order needs to be modified.

In addition to the 'number of hits' criteria, we should also consider the importance of some rules playing a 'critical' security role. A somehow limited number of these 'critical' rules should be also at the top of the rule base (like rule number 1).

2.4.7 Allowing HTTP(S) + DNS queries + SMTP

Once we have protected our firewall, we have to start providing required accesses to the key element of the company, the customers. They need to reach GIAC-P web site from any device connected to the Internet:

2	* Any	GP-ExtWeb	TCP http TCP https	accept	Log	* Policy Targets	* Any
3	* Any	GP-ExtDNSaNTP	UDP domain-udp	accept	Log	* Policy Targets	* Any
4	* Any	GP-ExtSMTP	TCP smtp	accept	Log	* Policy Targets	* Any

Firstly, following the communication requirements table appearing in part 1 of this assignment, we just have to allow HTTP (port 80), HTTPS (port 443) requests to the external web server.

Secondly, we also need to allow DNS UDP-queries (port 53) to the external DNS server for the customers (individual and corporate) and employees to be able to contact GIAC-P web site.

HTTP and HTTPS-related rules are placed before the DNS-rule following the ordering approach already mentioned in this paper. There will be more datagrams hitting the HTTP(S) rules than datagrams hitting the DNS-rule (for every web session, normally only one DNS query is required).

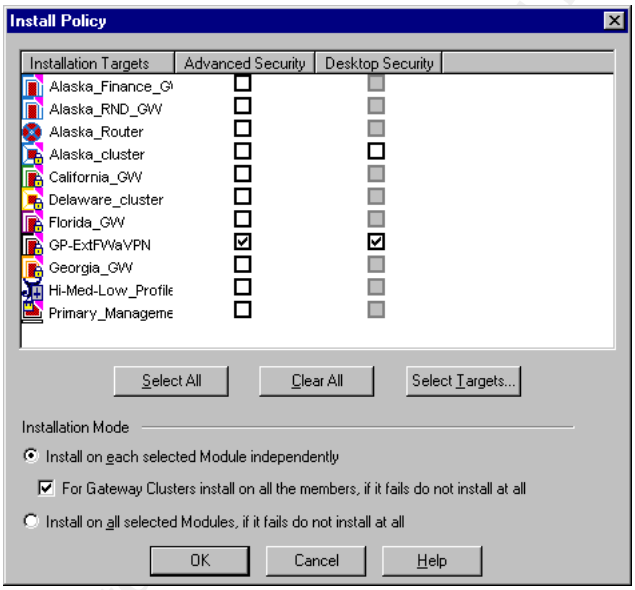
Secondly, we allow any IP address to contact GIAC-P external mail server via

SMTP (port 25).

Inserting the remaining rules require the same steps already mentioned with the first rule, placing the respective objects in the different columns. Therefore, we will not go through them again.

2.4.8 Installing the policy

Once the complete rule base has been written, including also the VPN Desktop Security Policy inbound and outbound rules, it is time to install the policy in the enforcement module. To do that, we need to go to the 'Policy' general menu and choose 'Install'. We will get the following pop-up window:



Where we will select, in this case, to install the policies (both the firewall policy and the VPN policy) in our GP-ExtFWaVPN.

3. Verify the firewall policy

3.1 Planning the validation

3.1.1 Overarching goal

Our task is now technically validating the firewall policy. We will review the firewall rules implemented in the GIAC-P firewall to check:

- Whether they really fulfil a business requirement in a secure way.
- Whether the firewall security policy is correctly enforced.

The only constraint we will have is that this validation should be non-intrusive (i.e. GIAC-P business processes should not be affected).

It is important to note that security is explicitly mentioned neither in the mandate of the technical group nor in the mission statement of GIAC-P.

3.1.2 Technical approach

We will be using a laptop with Nmap 3.00 (located in the SANS Perimeter Security CD provided in the Track 2 classes) to perform port scans and the typical network commands (ping, etc.). We will connect the laptop three different network locations:

- In front of the external interface of the firewall (using IP address ppp.uuu.bbb.3)
- In GIAC-P DMZ (using IP address ppp.uuu.bbb.9).
- In GIAC-P LAN (using IP address 10.1.1.4).

In order to place the laptop in those locations, we will be using a spare port in the already existing hubs (this is the case for the location in the DMZ and the LAN). Additionally, we will configure the laptop with a non-repeated IP address in that segment and with the corresponding default gateway address.

Regarding the first location, in front of the external interface of the firewall, we will use a simple hub to get network connectivity. This will imply a network glitch when connecting (and disconnecting) the hub. We will announce the network glitch beforehand internally and also externally (users of GIAC-P at that precise moment will only have to reconnect again).

We will trigger port scans from the laptop to check which ports are open and which ports are closed. The results obtained will have to reflect what are actually enforcing the implemented firewall rules.

Additionally we will also check VPN connections by going to the firewall logs and doing some testing in the VPN laptops with a network sniffer like tcpdump (see http://www.tcpdump.org/) to verify that the traffic is actually encrypted.

Admitting the humble and limited nature of this technical validation, at least the results obtained could be a very first check of the firewall policy apparently enforced in the GIAC-P firewall.

This first technical validation made in-house does not replace a more thorough security assessment (probably made by an external security provider) that this platform should undergo on a yearly basis.

3.1.3 Time schedule for the validation

The assessment will be done at a time when the least customer traffic takes place to cause the least possible disruption to the business. This would initially mean that the validation will be perform on a Monday early morning (there are very few people accessing GIAC-P systems around 5:00 AM). We will consider that most of the customers are located then in the same time zone (or, at least, in the same continent).

Should this not be the case, then the time slot to perform this validation will be selected so that the 'least number of players' are potentially affected.

3.1.4 Cost and level of effort

The advantage of this limited validation is the minimal cost and effort required. One IT expert in GIAC-P will devote one working day to prepare the validation and one working day to perform the assessment. After that, a third day will be required to elaborate the report and prepare recommendations. Finally, there will be a meeting with the CIO and the relevant IT staff to evaluate the results and consider the recommendations.

Action	Player	Time	Resources
Preparing the validation Information gathering Informing users	1 IT staff	1 day	Internal
Performing the assessment First look at results	1 IT staff	1 day	Internal
Elaborating the report	1 IT staff	1 day	Internal
Communicating results	Meeting with relevant IT people (including CIO)	1/2 day	Internal

Although it is a lightweight assessment with a very limited effort, it could have a nice leverage to initially detect major flaws or, in their absence, at least it will indicate that GIAC-P firewall rules are pointing at the right direction.

3.1.5 Risks incurred in these assessment

The risk of affecting the business processes is also rather limited. Port scans, if well done, and performed by someone with experience, should not be very noisy and should not create service disruptions.

Although backups should be readily available on a weekly and daily basis (depending on the criticality of the system, as said in part 1), a sampling check of the backup contents will be done before starting the validation.

Nevertheless, formal permission from the GIAC board will be seek and the assessment will be announced in advance in the change management process to avoid running other network-intensive tasks simultaneously.

3.2 Conducting the validation

The script to conduct the validation is the following: we will take the implemented firewall rules and performed the corresponding port scan(s) to initially check that the rule is functioning.

3.2.1 Validation of rule 1: protecting the firewall

We follow a simple approach for this rule. We place our laptop using a hub in front of the external firewall interface and we first try to ping the firewall:

C:\tools\nmap\nmap-3.00> ping ppp.uuu.bbb.5

Pinging ppp.uuu.bbb.5 with 32 bytes of data

Request timed out.
Request timed out.
Request timed out.

The very first good piece of news: we cannot ping the firewall.
We will repeat this from the two other interfaces (connecting our laptop to the respective hub). Firstly from the DMZ segment:

C:\tools\nmap\nmap-3.00> ping ppp.uuu.bbb.10

Pinging ppp.uuu.bbb.10 with 32 bytes of data

Request timed out.
Request timed out.
Request timed out.

And secondly from the LAN segment:

C:\tools\nmap\nmap-3.00> ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data

Request timed out.
Request timed out.
Request timed out.

The next thing is checking which ports are opened in all the firewall interfaces. We will use nmap doing ACK scan (used to map out firewall rulesets):

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sA -p 1-65535 -v ppp.uuu.bbb.5
C:\tools\nmap\nmap-3.00>nmap -eeth0 -sA -p 1-65535 -v ppp.uuu.bbb.10
C:\tools\nmap\nmap-3.00>nmap -eeth0 -sA -p 1-65535 -v 10.1.0.1

As a result, we should get that all ports are, using nmap terminology, 'filtered' (i.e. closed).

3.2.2 An inbound example: allowing HTTP(S) + DNS queries + SMTP

Rule 2: Any IP address can connect to the external GIAC-P web server using http and https.

We check that both ports are up and running.

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sT -p 80,443 -v ppp.uuu.bbb.12

And that the rest of the ports (we scan all ports using both TCP and UDP protocols) are in the state 'filtered':

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sT -sU -v ppp.uuu.bbb.12

Although this is not the real output of this action, it should look like this piece:

Starting nmap V. 3.00 (www.insecure.org/nmap)
Host testname (ppp.uuu.bbb.12) appears to be up ... good.
Initiating Connect() Scan against testname (ppp.uuu.bbb.12)
The Connect() Scan took x seconds to scan 65535 ports.

Initiating UDP Scan against testname (ppp.uuu.bbb.12)
The UDP Scan took x seconds to scan 65535 ports.
Interesting ports on testname (ppp.uuu.bbb.12):
(The 65535 ports scanned but not shown below are in state: closed)

Port	*State*	*Service*
130/tcp	*filtered*	*cisco-fna*
131/tcp	*filtered*	*cisco-tna*
132/tcp	*filtered*	*cisco-sys*
133/tcp	*filtered*	*statsrv*
134/tcp	*filtered*	*ingres-net*

And the list will continue...

We are not taking care about doing stealth scans because we do not require hiding our actions from the logs.

Rule 3: Any IP address can connect to the external DNS server using UDP-based DNS queries.

We check that both ports are up and running.

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sU -p 53,123 -v ppp.uuu.bbb.14

And that the rest of the ports (we scan all ports using both TCP and UDP protocols) are in the state 'filtered':

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sT -sU -v ppp.uuu.bbb.14

Rule 4: We check that only the SMTP port in the external SMTP server is allowed from the Internet:

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sT -p 25 -v ppp.uuu.bbb.16

And that the rest of the ports (we scan all ports using both TCP and UDP protocols) are in the state 'filtered':

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sT -sU -v ppp.uuu.bbb.16

3.2.3 An outbound example: Outgoing SMTP emails

Let us check rule 6 as an example of outgoing traffic. We should be able to reach any external SMTP server (via TCP port 25) in the Internet if we were using the IP address of our external SMTP server.

In order to keep on being non-intrusive, we will just send an email to an external

address and check that it has been received. Being non-intrusive means that we will not use the email server's IP address in our nmap-equipped laptop, since this would mean that we would have to disconnect the email server stopping the business process.

3.2.4 DNS and NTP from internal to the DMZ

Let us check rule 7 connecting our nmap-equipped laptop in the LAN and checking that we can connect to the external DNS and NTP server.

We check that both ports are up and running (using the 'NATed' internal IP address for the external DNS server):

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sU -p 53,123 -v 10.1.0.3

And that the rest of the ports (we scan all ports using both TCP and UDP protocols) are in the state 'filtered':

C:\tools\nmap\nmap-3.00>nmap -eeth0 -sT -sU -v 10.1.0.3

Validating all these firewall rules, as the previous sections show, is always following the same approach:

- A positive check confirming that the data inserted on every individual rule can be reflected on a specific answer out from the use of nmap.
- A negative check also to confirm that unexpected ports are not open.

Therefore, we will pass on to validate VPN-related rules.

3.2.5 VPN-related firewall rules

The first thing we will check is whether the network flow going to and from the clients to the GIAC network is actually encrypted (we can do that easily using tcpdump, a network sniffer) in two different locations:

- Right in front of the external interface of the firewall.
- In the VPN-equipped laptops themselves.

If we would need to check the ports that are open and closed in the client policy, a possible way could be to install nmap in one of them and check the validity of the applying rules again i.e. that it exists:

- Encrypted access to the internal SSH server via SSH protocol (rule 8).
- Encrypted access to the internal email server via POPv3 and SMTP (rule 9).
- Encrypted access to the internal web server using HTTP and HTTPS (rule 10).
- Encrypted access to the internal DNS server using UDP-based DNS queries

(rule 11).

Regarding client inbound rules, we will just proceed to check the required connectivity with the specific ports and destinations IP addresses is there:

- An SSH session with the internal SSH server can be established.
- Emails from the internal email server via POPv3 and SMTP can be received.
- The internal web server can be accessed using HTTP and HTTPS to their box.

3.3 Evaluating results

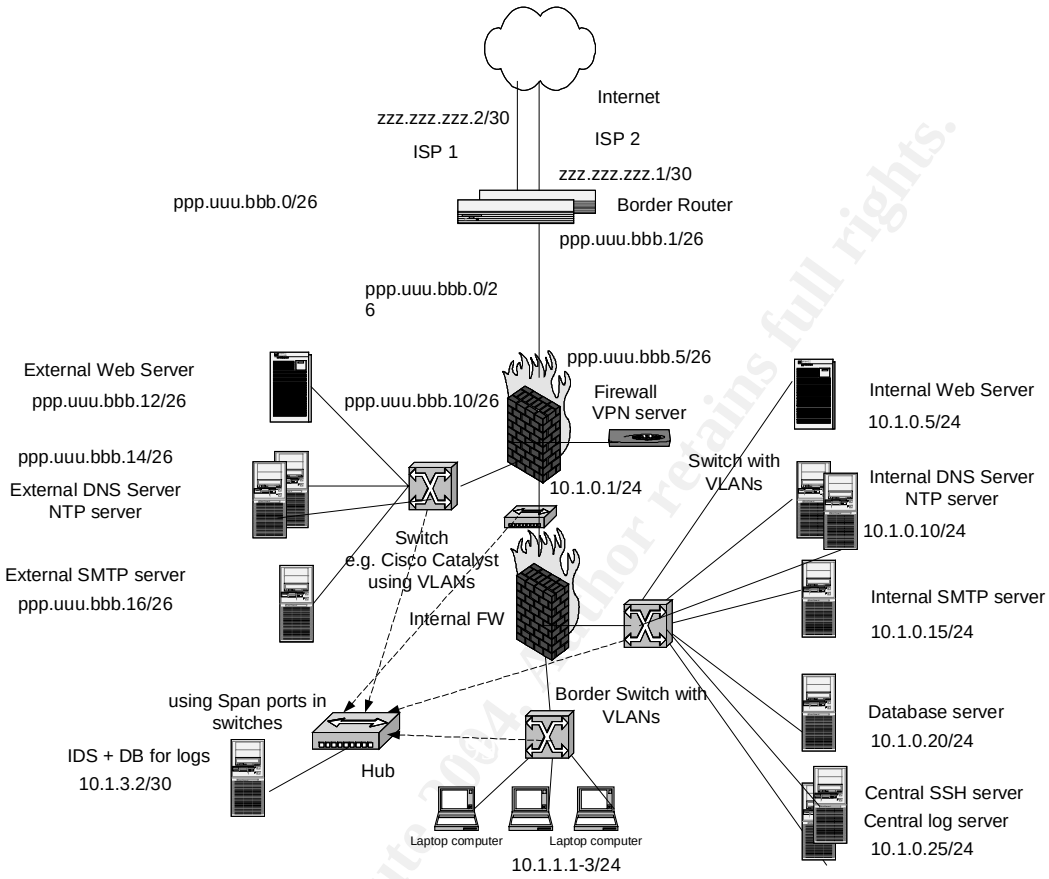
3.3.1 Analysis of the results

The direct result of this validation is the appropriateness of our firewall rule base. To be accurate, the main result is that business functionality has been basically implemented through the 16 different firewall rules.

Additional information about the global security health of our platform cannot be deduced from this basic validation. Application-level protocol attacks represent yet a threat to our infrastructure. It is important to remember that the data payload of the application protocols is not generally checked by a stateful inspection firewall. This calls for the presence of application-level filtering proxies such as an HTTP proxy. The pitfall is that at the moment there are not application-level protocol proxies for all protocols. The question is will they ever exist?

This validation is accompanied by a proposal for the future GIAC-P network layout. We will comment it in the next section.

3.3.2 Future GIAC-P network layout



3.3.3 Future design direction for GIAC-P

Let us describe the new elements present in this future network design proposal for GIAC-P (to be sent to the GIAC-P's CIO). The reader can easily follow the argumentation line of this section just comparing the elements present in the network layout previously presented in this assignment and this proposal.

Two different ISPs

The first difference is the connection to the Internet. Instead of using only one

ISP, GIAC-P will use two different ISPs to enjoy a redundant connection to the Internet and, if these ISPs are used simultaneously, they will provide much throughput, which will be very soon required due to GIAC-P expansion plans.

Additionally, this proposal constitutes a risk mitigation measure in case of a distributed denial of service performed through one of the ISPs, since the company will have an alternate routing path to the Internet.

Two redundant border routers

The fact of having two different ISPs lead us to having two border routers, so that each ISP is connected to a different border router. Both border routers will be configured identically. Should a hardware problem happen to any of the two routers, we could:

- Manually re-establishing network connectivity using the other one.
- Build a high-available solution using HSRP.

As a general comment for this improved network proposal, redundancy and high availability in core systems (e.g. border router, external firewall, web servers, etc.) will always be a plus. Therefore, we will no comment the high availability issue more extensively.

One box, one service

Initially three boxes, one at the DMZ and the other in the internal server segment, share two different functions (although they are already 'chrooted'): domain name server and NTP server in the same box, and log server and central SSH server in the same box. Without a high increase in the IT budget for GIAC-P, at least those services could be in different hardware.

Switching the network

As previously mentioned, one of the very first future improvements for GIAC-P network will be substituting the hubs for layer-3 switches to distinguish and isolate traffic from and to the different servers (and segments) present in GIAC-P.

We will have an increase in performance and we will be able to create virtual LANs that will differentiate different traffic (web traffic, log traffic, dns traffic, ntp traffic, etc.). The three proposed switches are:

- A switch in the DMZ creating VLANs for the different servers (ACLs could also be implemented in the switch).
- A switch in the internal server network segment with a different VLAN for every server.

- A switch in the internal workstation network segment to be able to start distinguishing accesses between marketing/sales and IT staff.

Splitting the firewall

GIAC-P will end up having two different firewalls (a different software installed on a different platform for security reasons), so that one firewall can be exclusively devoted to filter internal traffic between workstations and internal servers and the external firewall can deal with the DMZ servers only.

This new structure caters for new network segments (e.g. partner extranets, a second DMZ, etc.)

More network locations to scan

Consequently, as the network grows, the IDS should also be extended to scan the new places. As a first proposal (and yet avoiding scanning in front of the external firewall), we will also scan:

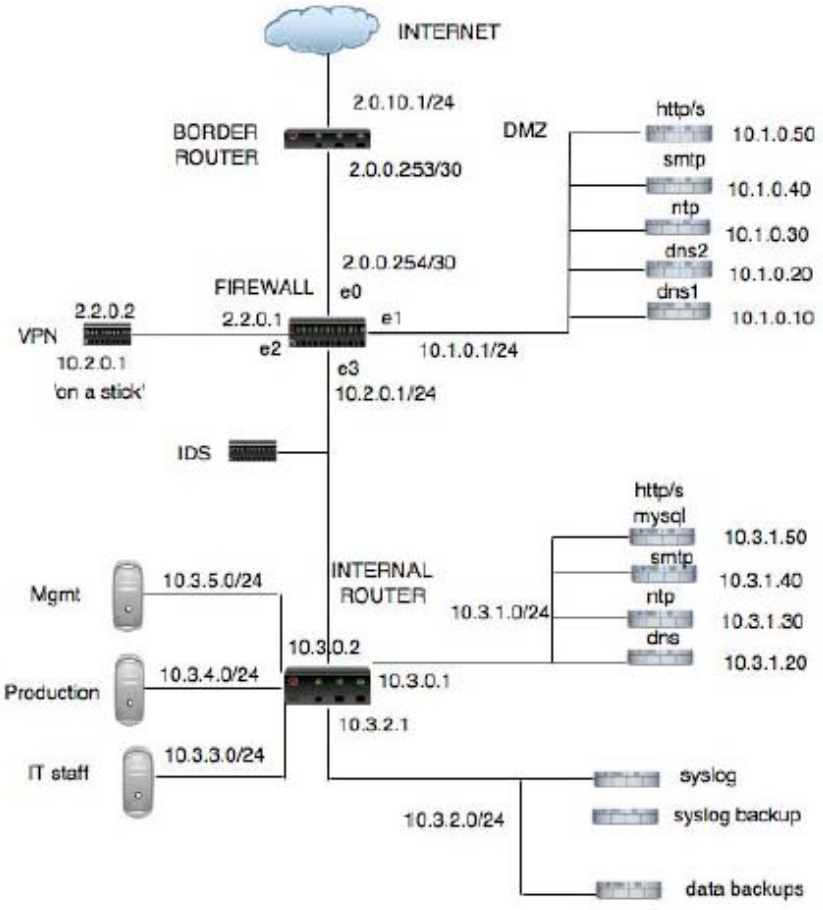
- The network segment between the firewalls.
- The internal workstation segment.

Once the switches are there, we will use the span ports in the switches to connect the IDS.

4. Design under fire

4.1 Selected network design

Eve Edelson (GCFW number 0452, December 2003, version 1.9) created the GCFW network design selected to be attacked is this paper. Its title is 'There But For Fortune' from DATE 2003. It can be found in this URL: http://www.giac.org/practical/GCFW/Eve_Edelson_GCFW.pdf. The network diagram describing her design is as it follows:



4.2 An attack against the firewall itself.

4.2.1 Preliminary assumptions

On page 3 in Eve Edelson's paper we read that 'IT staff is composed of two people who do everything. They need access to all network components and access from home in case problems come up' (among other protocols, HTTPS is mentioned). Although on page 27 she states that '...their policies specify that they are not accessed remotely unless both IT staff must be away. In that case SSH is enabled. There are other options: network components can be managed through a web browser...In this scenario neither of those options are used'.

However, the company started to make profit and soon a new sales force was hired part-time. They needed to test a CRM package requiring (oh, surprise!) strange ports and protocols. Therefore, a quick reaction time from the IT staff to allow (and after testing, disallow again) those protocols in the firewall was required. It was then decided to temporarily allow HTTPS access to the PIX for management so that it could be managed from any web browser using a secure connection (SSL-based).

According to Cisco documentation, available in Cisco URLs (see http://www.cisco.com/en/US/products/sw/netmgtsw/ps2032/), Cisco PIX Device Manager (PDM) is a browser-based configuration tool that enables the user to graphically set up, configure, and monitor their Cisco PIX Firewall. PDM is implemented as a signed Java applet which uploads to their workstation when the browser points at the firewall without requiring a plug-in or other software to be installed beforehand.

According to Cisco documentation (see http://www.cisco.com/en/US/products/sw/iosswrel/ps1833/products_feature_guide09186a00800d9eee.html), 'enable secure HTTP' is the command needed to enable this feature to have the firewall authenticate with the HTTP client, such as a web browser, using HTTP over SSL (HTTPS). If this feature is not enabled, the firewall uses HTTP and passwords will be in clear text (well, coded in Base64). This feature is disabled by default.

4.2.2 A vulnerability in the firewall used in Eve Edelson's practical assignment

The firewall present in her design is 'a Cisco 525 running Cisco Secure PIX Firewall Software version 6.2' (although there is a software version mismatch between pages 18 and 5 in her assignment, we decide to consider version 6.2 as the really used one). We browse Cisco security advisories and other public CERT vulnerabilities databases (e.g. Cert-BUND see http://www.bsi.de/certbund/) to select a vulnerability that can be used to compromise her firewall.

We decided to initially use a brand-new OpenSSL vulnerability (OpenSSL Security Advisory of the 17 March 2004) that is described in:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0079
And in these other three URLs:
http://www.cisco.com/en/US/products/products_security_advisory09186a0080207d5f.shtml
http://www.openssl.org/news/secadv_20040317.txt
http://www.securitytracker.com/alerts/2004/Mar/1009476.html

4.2.3 Vulnerability description

The description published in the last URL mentioned before states that 'using the Codenomicon TLS Test Tool (see http://www.codenomicon.com/brochures/tls.pdf) the OpenSSL group has discovered that the do_change_cipher_spec() function in OpenSSL 0.9.6c to 0.9.6k, and 0.9.7a to 0.9.7c, allows remote attackers to cause a denial of service (crash) via a crafted SSL/TLS handshake that causes a null-pointer assignment'.

The Cisco URL mentioned before states that 'a remote attacker could perform a carefully crafted SSL/TLS handshake against a server that used the OpenSSL library in such a way as to cause OpenSSL to crash. This crash on many Cisco products (including the Cisco PIX firewall) would cause the device to reload. Repeated exploitation of this vulnerability would result in a Denial of Service (DoS) attack on the device'.

The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0079 to this issue.

The do_change_cipher_spec() function sends a single message (either by the SSL client or by the SSL server) to notify the other party that subsequent records (encrypted packets) will be protected under the newly negotiated ciphering specifications and keys.

4.2.4 Designing an attack based on this vulnerability

Needless to say that a reliable (and pretty anonymous) Internet connection will be required to perform the attack (e.g. an Internet cafe).

Our first goal is to find the external IP address of the firewall. We first query the whois databases to look for administrative information and especially for IP address information. The 'nice' thing about this information-gathering step is that we do not have to send a single packet to our target (just to the different whois databases). It is an indirect attack preparation. So now at least we have a public

IP address assigned to Eve Edelson's GIAC company.

Once we have a group of possible IP addresses, we just try to see whether port 443 (the typical HTTPS port) is open hoping that the temporary nature of implementing HTTPS-based firewall management also led to using the default HTTPS port and... voilà!

We will use nmap to gather required port activity information:

nmap -sS -v -p 443 -P0 ip.address.found.of.GIAC

According to the man page of nmap (see http://www.insecure.org/nmap/data/nmap_manpage.html)

-sS: TCP SYN scan, we do not open a full TCP connection.
-v: We use verbose mode.
-p 443: Initially we only scan port 443.
-P0: not to try to ping hosts at all before scanning them.

Should have they thought about using other port, then our task would be a little bit more tedious because we would have to increase the range of scanned ports (e.g. using nmap -sS -T Sneaky -v ip.address.found.of.GIAC. We use the Sneaky timing option to send every packet every 15 seconds and make firewall log reading a little bit more fun and difficult for the log readers to discover us).

Let us then consider that we find a public IP address in the range of the GIAC company that has an HTTPS port up and running. It is important to highlight that we do not really need to know whether the found system is a Cisco PIX firewall. The only thing we know is that it is running HTTPS, and this is enough to perform our SSL-based attack.

Our second goal is to build the crafted SSL handshake packet that causes a null-pointer assignment and finally send it to the port running SSL in a public IP address (that could be the firewall).

We browse www.openssl.org (especially the pages devoted to the SSL API) and inform ourselves about the do_change_cipher_spec() function. We modify slightly a handshake sample code appearing on the OpenSSL web site (so that the mentioned function is used several consecutive times) and test the piece of code with a testing Cisco PIX firewall running the same version as the victim network to confirm that the OpenSSL library crashes.

4.2.5 How to construct the exploit

Retrieving some information from http://cvs.openssl.org/chngview?cn=12029 , we see that the exploit would have to try to change to a new ciphering

specification in a case where there is no other additional specification available. Therefore, we will just code a loop where the function do_change_cipher_spec() will be recursively called (till we are sure there no specification available and we provoke a null pointer assignment).

4.2.6 Results of running the attack against the firewall

Finally we send the packet against the public interface of the victim company and wait for results.
A possible checking exercise would be to use nmap again:

nmap -sS -v -p 443 -P0 ip.address.found.of.GIAC

Just to check whether the port is still up and running. If right after the attack the port is not open, this means we succeeded.

Seconds afterwards, as this packet would only cause the firewall to reload, a new nmap packet will tell us that the port is open again.

The only remaining step is to create a loop to constantly send the packet so that a denial of service attack is finally achieved.

4.2.7 Attack recognition through log files

As this attack is based on a simple packet directed to a specific port, while reading logs at GIAC's headquarters, the typical nmap port scanning, trying to scan a whole range of ports, will not be initially identified.

A more thorough analysis of the information provided by the IDS and the logs, specially if the border router and the firewall are logging TCP connection initiation attempts at the times where the firewall reloaded itself, could finally tell GIAC IT support the source IP address of this attack. That is the main reason why the initial Internet platform from where to initiate the attack should be as anonymous as possible.

4.2.8 Countermeasures to mitigate the attack

The countermeasure to definitively mitigate the attack (recommended by Cisco) is to upgrade to a fixed software version of code (Ms. Edelson would probably do this since she mentions in her paper the need to update software e.g. on page 6) as soon as it is available. On the mean time, Cisco proposes two temporary countermeasures:

- Restrict access to the HTTPS server on the network device. Allow access to the network device only from trusted workstations by using access lists / MAC filters that are available on the affected platforms.

- Disable the SSL server / service on the network device. Cisco also comments that this workaround must be weighed against the need for secure communications with the vulnerable device.

As always, the balance between security and functionality is always difficult.

In our selected case, we would strongly advise to restrict HTTPS access to the vulnerable PIX firewall only from trusted IP addresses by using ACLs. This would require the ISP the IT staff is using to connect remotely to always provide them with a fixed IP address (a common added value which normally means a higher monthly rate).

Consulting Cisco PDM documentation, the steps to restrict HTTPS access are the following:

1. Click on Add to open the PDM/HTTPS>Add dialog box.
2. Click on interface to add a firewall interface to the rule table.
3. Enter the IP address of the host running PDM which will be permitted HTTPS access through this Firewall interface.
4. Select or enter a netmask for the IP address to be permitted HTTPS access.
5. Select OK to accept changes and return to the previous panel.

More information about how to get the Cisco PIX Device Manager (PDM) installed and running on your PIX Firewall unit, so you can use the PDM graphical user interface to configure and monitor
PIX Firewall features and resources is here:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_11/pdmig/pdm_inst.htm
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_11/pdmig/pdm_app.htm#56843

4.3 A distributed denial of service attack

4.3.1 Method to compromise 50 Cable/DSL connected systems

As the most popular DDoS ready-to-use tools are Unix-based, as it can be read in:

http://www.cnn.com/2000/TECH/computing/09/06/fear.trinity.idg/

http://www.nwfusion.com/news/2000/0906ddos.html
http://staff.washington.edu/dittrich/misc/ddos/

We decide to do something a little bit more rudimentary but probably providing us the required number of compromised systems in less time.

To compromise 50 or more DSL-connected home systems we choose a security vulnerability appearing lately in one of the most common email clients: Microsoft Outlook 2002.

In 2003, a very well-known international bank offered the general public a nice offer together with one of the most used ISP in the country. A DSL-enabled Microsoft XP-based PC (including also Outlook 2002) at a very reduced price provided that the customer joins the DSL service for at least two years.

Getting the public IP address range of the PCs connected to the ISP mentioned is an easy task using the information provided by the whois databases and information services like ARIN. We can also go to a cybercafe nearby powered by the same ISP and find out the public IP address range they are using.

This can be achieved either executing netstat -an in a DOS window or, if this service is disabled in the public workstations in the cafe, we can always browse one of the many web sites that provide us with such an information (e.g. http://www.whatismyip.com/).

The newspapers last year announced that more than 10000 customers bought this DSL offer, so if we imagine that at a certain moment in time (e.g. one evening) around 3000 customers will have their PC up and running and connected to the Internet. We just need that around 1.5 % of these customers do not have their Outlook email client updated with the security patch issued by Microsoft on March 10, 2004.

Thus, the probability of locating vulnerable Outlook email clients is rather high.

4.3.2 Description of the Outlook vulnerability

As stated in http://www.microsoft.com/technet/security/bulletin/ms04-009.mspx, a vulnerability in Microsoft Outlook 2002 could allow code execution (828040) if an email with a crafted mailto URL is received, especially by those users with the option 'show home page by default' in the 'Outlook today' folder. An option that is enabled by default in Outlook.

We then create an HTML-based email message designed to exploit the vulnerability and persuade the user to view the HTML e-mail message. This task can be achieved using a subject that, for instance, refers to the change in the

price conditions of the DSL-connection.

4.3.3 Designing the distributed bots

In http://cert.uni-stuttgart.de/archive/ntbugtraq/2004/03/msg00008.html, we read that 'the exploit can inject command line switches and arguments to OUTLOOK.EXE because quote symbols in the URL aren't escaped or otherwise processed'.

So we go to http://www.planet-source-code.com/vb/scripts/ShowCode.asp?txtCodeId=717&lngWId=3 and slightly modify the code proposed to connect to a server and send a TCP packet so that it sends SYNs to our victim.

Afterwards, we use an Outlook switch to open the VB program attached to the email and it will be executed.

Alternatively, we could have also used a Javascript:URL so that the box receiving the email connects to a web server, downloads and execute an .EXE program.

4.3.4 Attack performed from the compromised systems

The code inserted in the mailto URL will run in the security context of the currently logged-on user. Most of the home users do not think that their boxes require a specific security hardening (especially those workstations shared with teenagers in the family). So, most of the cases we will be able to issue network commands using this vulnerability.

We plan to do a SYN flood attack from these compromised workstations. We will tell the workstations to repeatedly send the GIAC web server from Eve Edelson's assignment a TCP-based SYN packet with an unreachable IP address as a source address. Getting the public IP address (and the software version used) of the web server can be done through the netcraft.com web site (http://news.netcraft.com/).

Information on SYN flood DoS attack experiments has been found in http://www.niksula.cs.hut.fi/~dforsber/synflood/result.html#windows

To craft this SYN packet, we will use the software etherreal (see http://www.ethereal.com/), starting from a totally legal SYN packet sent to the web server and modifying the source IP address. Subsequent to building the packet, we need to link it with the Outlook vulnerability.

Most of the OSs nowadays are protected against the most obvious SYN flood

attacks. We will probably not achieve to take GIAC web server completely out of the Internet but at least the overall traffic output will be affected. Let us also remember that Eve Edelson proposed to use ipfw (a host-based firewall) in all DMZ servers, including the web server (according to http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html, ipfw does not protect against this type of attacks).

4.3.5 Attack recognition through log files

This attack is quite noisy in terms of log files. But this could also be the advantage of it. IDS, border router logs and firewall logs (if enabled, and the paper says so) will show the IP address range from which most TCP connection requests are coming. So finding out which ISP is facilitating this SYN flood will be an easy task.

However, going one step further, asking the ISP to track down and identify the 50 (or more) sending
workstations will probably not be an easy and quick task.

4.3.6 Countermeasures to mitigate the attack to Outlook

Microsoft security bulletin proposes two mitigating factors:

- Configure the Outlook email client to read messages in plain text format (and not directly in HTML). Thus, the user would really need to click on a link in an email to be affected by the attack.

- Home users should not have administrative rights when working normally with their computer (although, in our case, as the actions link to the mailto URL do not require admin rights, this factor will not be effective).

Three additional recommendations from our side are:

- Apply the advertised security update as soon as possible (also recommended by Microsoft). An not only this, it would be recommendable to set up a process to maintain home users' computers updated with the latest security patches.

- The use of a personal firewall will not avoid the content of the mail to be executed but the sending of SYN packets could be aborted if the personal firewall is properly configured (and the user is a security-literate)

- Let us also add as a mitigating factor the recommendation to use an alternative email client.

4.3.7 Countermeasures to mitigate the attack to the web server

Eve Edelson mentions already in her assignment (page 16) that TCP Intercept is already enabled in her border router policy (using the line 'ip tcp intercept list 110').

According to Cisco documentation (Cisco Pix Device Manager 3.0 Online Help: available in http://www.cisco.com/application/pdf/en/us/guest/products/ps2032/c1626/ccmigration_09186a0080189166.pdf),
with the Cisco TCP Intercept feature, 'once the optional embryonic connection limit is reached, and until the embryonic connection limit falls below this threshold, every SYN bound for the affected server is intercepted'.

This is a possible way to fight against SYN floods (it is also important to mention that the figures for the embryonic connection limit is key to only reject attempts of DDoS and not connection attempts from slow clients).

According to Cisco, the embryonic connection is the number of initiated (but not already established, i.e. SYN connections) allowed by the router/firewall to exist before it begins to deny them. The default value is 0. This means that an unlimited number of connections are allowed to be initiated (even if the TCP Intercept option is enabled). So, the recommendation will be to change this default value to something between 1 and 65,535 depending to experience and average type of connections used by the customers.

More generally, not only as a security recommendation, but also as a performance recommendation, it would be interesting to use two different ISPs (with a different routing possibility) to connect GIAC systems to the Internet, so that the consequences of this attack would be much less noticeable.

Finally, let us notice that the 'rudimentary bots build by us and attached to the emails' are not controlled in any way from the attackers apart from their sending action.

4.4 An attack plan to compromise an internal system

4.4.1 Reasons to select the target

The target will be the internal web server. According to Eve Edelson's paper (page 7), the web server runs Apache (version 1.3.29) and PHP (version 4.3.3). She also mentions that the external web server filters input and passes it to the internal web server, being this internal web server the one querying the mySQL database.

Two assumptions are required for our attempt to attack an internal system:

- Both web servers (internal and external) are running the same software versions.
- Apache Mod_survey is also running in the web servers.

Let us present now the reasoning for the second assumption:

The need to have web-based questionnaires was felt very soon after the launch of the GIAC company to check current and potential customers' views on different aspects of the product.

The IT staff of GIAC first looked for a PHP web-based survey module in PEAR, the PHP Extension and Application Repository (see http://pear.php.net/) with no success.

Although it was thought that PHP would suffice for the initial web functionality requirements, no mature survey-and-voting module was found in PHP, and there was no time to develop one from scratch.

They finally decided to use a perl-based survey module, mod_Survey, because it is an Apache module really easy to integrate with the current platform (they just had to install mod_perl and mod-survey modules) and it uses XML-based tag notation defined in the Survey v3.0.0 DTD.

This scenario might sound rather familiar to most of the readers: a sudden business requirement ends up adding a new piece of software in the IT platform without really studying all IT architecture-related issues.

Mod_Survey is a mod_perl module for Apache (see http://gathering.itm.mh.se/mod_survey/docs/Mod_Survey.pdf) that allows GIAC, according to the URL mentioned before, to 'reasonably easy write web-based questionnaires using a definition language looking quite a lot like the language you would use to write a normal home page'.

More information on Mod_Survey can be found in its mailing list http://news.gmane.org/gmane.comp.apache.mod-survey.general.

4.4.2 Process to compromise the target

The vulnerability to be used is described in http://www.securitytracker.com/alerts/2004/Mar/1009516.html. By the time this assignment is written, it is a brand-new cross-site scripting vulnerability, so the possibilities to succeed are high.

Although the security updating process in GIAC can be reasonably good and efficient, it is also probable that a reduced number of IT staff in a flourishing company would have plenty of urgent things to do before noticing that there is a new vulnerability in the surveying module of Apache.

The URL mentioned before states that 'Mod_Survey does not fully filter HTML code from user-supplied input in the survey text field answers'. So, all we have to do is connect to the public web server and fill in a survey with some crafted input.

That input would go from the external web server to the internal one to be handled by the internal staff and it will provoke an attack when the GIAC Mod_Survey administrator exports the data in HTML table format and views the table. At that moment, the code we could have inserted in the survey web page will be executed by the administrator's web browser.

So, the GIAC company could have the best configured border router and firewall in the world, that they will result completely useless to try to stop an application-level attack.

The code we would add in the survey will be a piece of Javascript to disturb the administrators (and let them know that we can access even their internal systems):

<script>alert ('Fortune cookies online will no be a successful business!')</script>

This is just a proof-of-concept attack that demonstrates how easy it would be to do more harmful things like e.g. to steal cookies from the administrator's web browser or (applying the same approach as with the previous DDoS attack) to execute a file located at a specific URL.

4.4.3 Attack recognition through log files

The only piece of information this attack would leave as a trace will be a log entry in the web server log as one of the multiple IP addresses from which the survey pages were accessed. Possibly, if the time service in GIAC is reliable in the syslog server (and we certainly expect that) and the Mod_Survey pages store also the time and date of every entry, then maybe it is possible to track down the IP address from where the survey was filled in with Javascript code.

Therefore, we would perform this attack from an anonymous cybercafe in a nearby town so that even the fact of finding out the IP address will not lead to the real authors of this attack.

4.4.4 Countermeasures to mitigate the attack

The most effective countermeasure is using a fixed version released by Mod_Survey coders (3.0.16-pre2 stable and 3.2.0-pre4development) available at http://gathering.itm.mh.se/modsurvey/download.php.

If there is no time yet to install this fixed version, a quick mitigating factor will be to recommend GIAC administrators not to export the survey data in HTML table format.

More information about cross-site scripting vulnerabilities can be found in http://www.technicalinfo.net/papers/CSS.html

5. Internet references

This assignment follows GIAC Certification Administrivia version 2.8 (revised March 2004)

5.1 Assignment 1: Security architecture

- Information about the Cisco 2600 router model:
http://www.cisco.com/warp/public/cc/pd/rt/2600/index.shtml

- Information about the Nokia IP380:
http://www.nokia.com/nokia/0,,43123,00.html

- Information about the Netgear DS108 8 PORT 10/100 Mbps dual speed hub:
http://www.netgear.com/products/prod_details.php?prodID=69&view=sb

- Information about FreeBSD production release 4.9:
http://www.freebsd.org/

- How to secure a FreeBSD box - Security HowTo:
http://www.FreeBSD.org/~jkb/howto.html.

- Info on HP Proliant ML330 G3:
http://h18004.www1.hp.com/products/servers/proliantml330/

- Info on ProLiant ML530 G2:
http://h18004.www1.hp.com/products/servers/proliantml530/ for information

- Details of Apache version 2.0.49 web server:
see http://httpd.apache.org/

- OpenSSL web site:
http://www.openssl.org/

- Info on PHP version PHP 4.3.5
http://www.php.net/

- DNS server BIND version 9.2.3rc4 information:
http://www.bind.com/bind.html

- Info on Sendmail version 8.12.10:
http://www.sendmail.org/

- Info on the VPN client SecuRemote:

http://www.checkpoint.com/products/connect/vpn-1_clients.html

- Info on swatch
http://www.spitzner.net/swatch.html
-Info on OpenSSH:
http://www.openssh.com/

- Info on the NTP servers (version 4.2.0 released on 2003/10/15):
http://www.ntp.org/downloads.html

- Info on MySQL version 4.0:
http://www.mysql.com/downloads/index.html

5.2 Assignment 2: Security policy and tutorial

- Cisco Router 2600 configuration manuals:
http://www.cisco.com/application/pdf/en/us/guest/products/ps259/c1069/ccmigration_09186a00801f6f6b.pdf

- Cisco IOS configuration fundamentals manual:
http://www.cisco.com/application/pdf/en/us/guest/products/ps1839/c1051/ccmigration_09186a00801235ba.pdf

- Cisco IOS network management fundamentals manual:
http://www.cisco.com/application/pdf/en/us/guest/products/ps5187/c1051/ccmigration_09186a00801998c6.pdf

- IANA IP v4 address space [RFC 1466]:
http://www.iana.org/assignments/ipv4-address-space

- A classical URL to learn how to build a firewall rule base:
http://www.spitzner.net/rules.html

- SmartDashboard NG Feature Pack 3 - Build 53933 from Checkpoint Next Generation. Manual titled 'Getting Started' provided with the software in pdf format.

*5.3 Assign**ment 3: Verify the firewall policy***

- tcpdump network sniffer:
http://www.tcpdump.org/

- nmap web site:
http://www.insecure.org/nmap/

5.4 Assignment 4: Design under fire

- Assignment under fire:
http://www.giac.org/practical/GCFW/Eve_Edelson_GCFW.pdf

- Info on Cisco PIX Device Manager (PDM):
http://www.cisco.com/en/US/products/sw/netmgtsw/ps2032/

- Cert-BUND vulnerabilities database:
http://www.bsi.de/certbund/

- Info on Cisco 'enable secure HTTP':
http://www.cisco.com/en/US/products/sw/iosswrel/ps1833/products_feature_guide09186a00800d9eee.html

- Description of the Cisco PIX vulnerability used, a brand-new OpenSSL vulnerability (OpenSSL Security Advisory of the 17 March 2004):
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0079
http://www.cisco.com/en/US/products/products_security_advisory09186a0080207d5f.shtml
http://www.openssl.org/news/secadv_20040317.txt
http://www.securitytracker.com/alerts/2004/Mar/1009476.html

- Man page of nmap:
http://www.insecure.org/nmap/data/nmap_manpage.html

- Info on OpenSSL change_cipher_spec() function:
http://cvs.openssl.org/chngview?cn=12029

- Info on the Codenomicon TLS Test Tool:
http://www.codenomicon.com/brochures/tls.pdf

- Additional info on the Cisco PIX Device Manger (PDM):
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_11/pdmig/pdm_inst.htm
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_11/pdmig/pdm_app.htm#56843

- Preliminary information on DDoS tools:
http://www.cnn.com/2000/TECH/computing/09/06/fear.trinity.idg/
http://www.nwfusion.com/news/2000/0906ddos.html
http://staff.washington.edu/dittrich/misc/ddos/

- A web site that provides the user's public IP address:
http://www.whatismyip.com/

- Description of the Outlook vulnerability
http://www.microsoft.com/technet/security/bulletin/ms04-009.mspx

- Web-related information gathering web site:
http://news.netcraft.com/

- Information on SYN flood DoS attacks:
http://www.niksula.cs.hut.fi/~dforsber/synflood/result.html#windows

- The world's most popular network protocol analyzer:
http://www.ethereal.com/

- FreeBSD handbook. Ipfw information:
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html

- Cisco Pix Device Manager 3.0 Online Help:
http://www.cisco.com/application/pdf/en/us/guest/products/ps2032/c1626/ccmigration_09186a0080189166.pdf

- Details about the Outlook attack:
http://cert.uni-stuttgart.de/archive/ntbugtraq/2004/03/msg00008.html
- Information about coding in VB:
http://www.planet-source-code.com/vb/scripts/ShowCode.asp?txtCodeId=717&lngWId=3

- The PHP Extension and Application Repository:
see http://pear.php.net/

- Mod_Survey is a mod_perl module for Apache:
http://gathering.itm.mh.se/mod_survey/docs/Mod_Survey.pdf

- Additional information on Mod_Survey:
http://news.gmane.org/gmane.comp.apache.mod-survey.general.

- Description of the Mod_Survey vulnerability:
http://www.securitytracker.com/alerts/2004/Mar/1009516.html

- Fixed version of Mod_Survey:
http://gathering.itm.mh.se/modsurvey/download.php.

- More information about cross-site scripting vulnerabilities:
http://www.technicalinfo.net/papers/CSS.html