



# 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.

# GIAC Certified Firewall Analyst

## Practical Assignment

Version 1.8

Brad Tauer  
March 2003

## Table of Contents

### Assignment 1 – Security Architecture

1.0 GIAC network configuration.....	4
1.1 Introduction to GIAC.....	5
1.2 Business Operation.....	5
1.2.1 Customers.....	5
1.2.2 Suppliers.....	6
1.2.3 Partners.....	6
1.2.4 GIAC sales personnel and home office employees.....	7
1.2.5 GIAC internal users.....	7
1.3 Network components.....	8
1.3.1 Border router.....	8
1.3.2 Firewall.....	8
1.3.3 Intrusion detection systems.....	9
1.3.4 Service network (DMZ).....	9
1.3.5 Internal network.....	9
1.3.6 Network time synchronization.....	10

### Assignment 2 – Security Policy and Tutorial

2.1 Border router configuration.....	10
2.2 Firewall configuration.....	15
2.2.1 Firewall logging.....	15
2.2.2 Internet Filtering.....	18
2.2.3 Firewall Rules.....	19
2.2.4 VPN Policy.....	23
2.3 VPN Tutorial.....	26
2.4 VPN Verification.....	34
2.4.1 Verify IPSec Traffic.....	34
2.4.2 Analyze sniffer capture.....	35

### Assignment 3 – Verify the Firewall Policy

3.1 Planning the audit.....	36
3.2 Conducting the Audit.....	38
3.2.1 Run Nmap scans.....	38
3.2.2 NMAP scan on border router.....	40
3.2.3 NMAP scan on the firewall.....	41
3.2.4 Nessus Scan.....	41
3.2.5 Verify VPN.....	42
3.2.6 Results.....	42

## Assignment 4 – Design Under Fire

4.0 Overview.....	44
4.1 Perimeter Attack.....	45
4.1.1 The Perimeter Router.....	45
4.1.2 The Firewall.....	46
4.1.3 The Attack.....	47
4.2 Denial of Service Attack.....	48
4.2.1 The Attack.....	48
4.2.2 The Defense.....	49
4.3 DNS Server Attack.....	50
4.4 Internal Systems Compromise.....	50
4.4.1 Attack by Social Engineering.....	50
4.4.2 Protecting Against.....	52
4.4.3 Additional Attacks.....	52
References.....	55

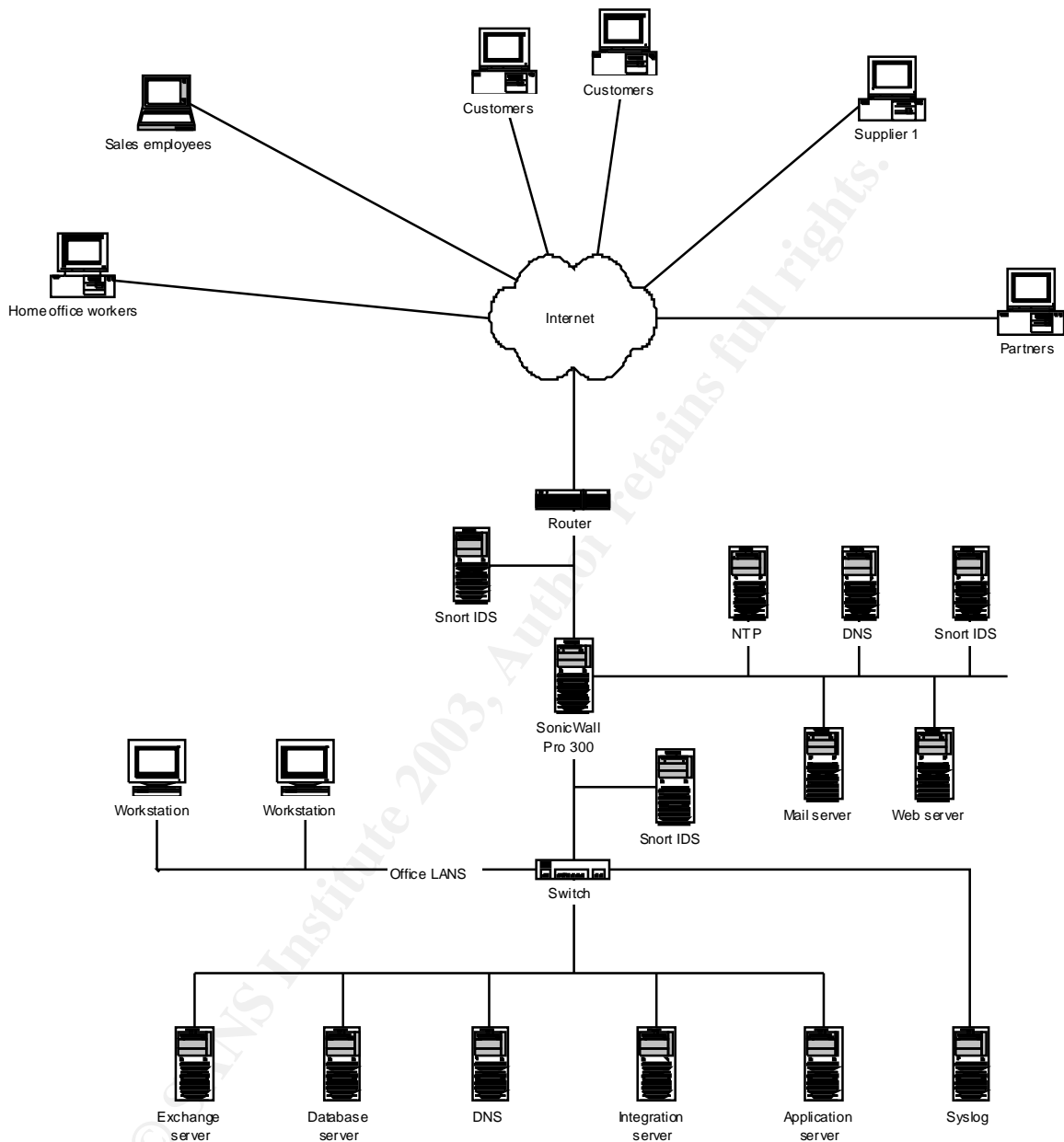
## Summary

This paper outlines the security practice of GIAC Enterprises.

Contained within this paper we will introduce the reader to GIAC Enterprises. Then we will outline their network components, their security policy, how they've configured their border router, firewall and VPN's.

Through this the reader should be able to gain an understanding of the security philosophy that guides this company.

## GIAC Enterprises, network configuration



**Figure 1: Network Diagram**

## **Assignment 1 – Security Architecture**

### **1.1 Introduction to GIAC**

GIAC Enterprises is a small privately owned business based on the sale of fortune cookie sayings.

They are an e-business born out of the internet/technology boom of the 90's offering fortune cookie sayings to their customers primarily through their web page. They also use the internet to allow their suppliers to submit the fortune cookie sayings to them.

GIAC has a secondary business which is the sale of their fortunes to partners who translate the sayings and resell them to their overseas customers.

GIAC has 15 employees working from their office, all are connected to the various servers via a typical Ethernet LAN setup. GIAC has a progressive work culture and allows some of their employees to work from home two to three days a week. They also have five sales people who are assigned to various regions of the United States who need access to the corporate network both from their homes and while they are on the road selling.

### **1.2 Business Operations**

We will define the connectivity needs of each of the business groups both internal and external to GIAC which were outlined in section 1.1 and also what accommodations were made for them.

#### **1.2.1 Customers**

GIAC has an external web server running Apache server software. The server is configured as a reverse HTTP proxy forwarding requests through the internal firewall on ports 80 and 443 to the actual HTTP servers. The HTTP servers in turn can access the internal databases which contain the fortune cookie sayings as well as account information.

GIAC is employing SSL 128 bit encryption on all connections to the web site involving personal or sensitive information. Visitors accessing the secure pages with browsers supporting only 40 bit encryption will not be allowed access to these pages. They will be instructed as to why they are being denied and directed to call or email for other options.

The web page allows visitors to view samples of the product line and open accounts. Existing customers can order product and view account information

after logging into the system using their user ID and password. In order to ensure greater security the web site requires new customers to select a password consisting of eight alpha-numeric characters and requiring at least two of each.

### 1.2.2 Suppliers

GIAC contracts with many individuals and small companies to have them provide the fortune cookie sayings.

Suppliers are provided accounts on the web site allowing them to log in with a unique user ID and a strong password. Once logged in they may view their account information, submit fortunes and view the fortune sayings database, all account activities are performed via an HTTPS session. GIAC suppliers do not need any access directly to the internal network or to any other servers on the service network other than the web server on ports 80 and 443.

When suppliers submit new fortunes to GIAC they submit them to their account on the external web server via an HTTPS session which in turn transmits them to the internal server. They may view an index of the fortune sayings database and upon selecting a category of fortune sayings to view the web server will pull them from the database for viewing if the supplier's account is authorized to view them.

Because of this arrangement the suppliers need no special access to any of GIAC's internal networks or internal servers.

They are required to use a browser which supports 128 bit SSL encryption and can only log in using such. When their accounts are set up they are given a user name and a password. The password consists of a minimum of 10 alpha-numeric characters in a combination of both with a minimum of two of each. They are required to change their password every 60 days employing the mentioned requirements.

### 1.2.3 Partners

GIAC contracts with several partners who purchase the fortune sayings from GIAC and translate them into various languages so they may sell them to their overseas customers.

GIAC supplies each partner with an individual page on the GIAC website. The web page can also be used to allow foreign speaking customers to view the translated fortunes. The partners are responsible for the content and upkeep of the web page. These pages direct customers as to how to contact the partners and order the fortunes.

GIAC partners requested access to an internal server so that they may administer their web pages and transmit to and retrieve from the server, batches

of fortunes for translation. The partners are required to connect to the GIAC network via a VPN tunnel. All of the VPN tunnels are configured as either network-to-network or host-to-network and employ the IP Sec tunneling protocol.

We have set up a separate HTTP server which also has an Oracle database server running on it. The HTTP server serves the customer web pages to our reverse HTTP proxy server on the service network. The database server interacts with the application the suppliers run on their workstations and use to submit and retrieve batches of fortunes. They are restricted by the firewall to have access only to this server on our internal network and are further restricted by login permissions on the server to access only the share containing their web page or the portion of the database they have been given access to.

For all other activities the GIAC partners must access the database through the website with their individual user ID and password via an HTTPS session. In this case they will only have access through the GIAC firewall to the service network via ports 80 and 443. As is the case with suppliers, they are required to connect using a browser which supports 128 bit encryption and have the same password requirements.

#### 1.2.4 GIAC sales personnel and home office employees

GIAC has a sales staff of five individuals residing in various areas of the US. These individuals require access to the internal GIAC network from their laptops both from customer locations and from their homes. They will connect via a VPN tunnel using an approved VPN client configured for IPSec tunneling on their laptops and terminating on the SonicWall firewall on GIAC's network. This will allow them the ability to connect by dialing into an ISP when away from their home office.

GIAC allows some of their local staff to work from home two or three days a week. Early on the decision was made to give each of these employees a personal SonicWall SOHO 3 firewall at their home. The employees are required to use a DSL connection to their ISP. The home workers connect to the GIAC internal network through a network-to-network VPN terminating on the SonicWall firewall using IPSec tunneling protocol.

#### 1.2.5 GIAC internal users

GIAC internal users are allowed connections out to the internet on an unrestricted basis, however their activity may be monitored and all have been notified of this. The company security policy states what types of internet activities are prohibited and each employee has signed a copy of the policy indicating that they have read and understand the policy.



Internal users are also granted email and FTP access to the internet and again the company security policy states which types of activities are restricted.

Internal user workstations reside on a LAN segment isolated from most of the network servers by an Ethernet switch. This practice optimizes bandwidth use on the local LAN.

Only internal users who require access to the servers on the service network have been granted access to them through the firewall.

### 1.3 Network Components

#### 1.3.1 Border router

The border router is a Cisco 2650XM Multiservice router running 12.2 IOS. This router was chosen for the following reasons: IT staff is familiar with and very comfortable with the Cisco CLI, Cisco support, this models price, performance and scalability are suitable for this implementation.

#### 1.3.2 Firewall

GIAC has chosen the SonicWall Pro 300 firewall for their firewall solution. The SonicWall is a very good, cost effective, stateful packet inspection firewall. It also performs well as a VPN gateway allowing GIAC to terminate their VPN tunnels on the firewall for added security. The Pro 300 supports IPSec tunneling from gateway-to-client and gateway-to-gateway ensuring the highest level of security for all remote connections.

The Pro 300 is a hardware based firewall eliminating the potential exploits targeted at software based systems.

The following paragraph is how the SonicWall literature describes the architecture and performance benefits:

*SonicWALL's security ASIC offloads encryption processing overhead to deliver breakthrough performance with hardware-acceleration for superior VPN and security throughput, while adhering to industry standards with ICSA-certified, stateful packet inspection technology.*

The Pro 300 is easily managed and configured through the GUI interface using a standard web browser such as Internet Explorer or Netscape. It has extensive logging capabilities with enough flexibility built in to accommodate those that want only header information to those that need detailed packet level information. The logs can be set to be sent directly to a syslog server or emailed to a local user account. It can also be configured to email specified alert events to an administrator for immediate attention.

SonicWall firewalls also offer virus protection, content filtering and authentication services. GIAC elected to purchase the virus protection as an added level of security for their network.

### 1.3.3 Intrusion detection systems

GIAC employs three intrusion detection systems (IDS) on their network. Snort was chosen for several reasons among the reasons was its ease of use, available support and cost. In each instance it is installed on a Unix platform.

There is one system installed between the border router and the firewall, one system installed on the service network and one system installed on the internal network directly behind the firewall. If any alerts are detected on any of the IDS systems an email is sent to a syslog account on the Exchange server. If any major alerts are detected an additional email is sent to an alerts mail account which is always monitored and this also causes a pager alert to be sent.

### 1.3.4 Service network (DMZ)

The service network contains the external DNS server, the NTP relay server, the SMTP mail relay and the proxy web server. There is also a Snort IDS on this network as explained in section 1.3.3 to monitor activity into and out of the network. No outbound traffic originating from the service network and destined for the internet will be allowed past the firewall. Any outbound packets originating on this network will set off a Snort major alert.

The servers can be managed from the internal network via an SSH tunnel set up for specific people who need access to them.

### 1.3.5 Internal network

The internal network is a switched network set up with all servers that require access from the internet on a separate subnet. The syslog server has also been placed on it's own subnet. Isolating it from the other LAN segments offers an extra layer of protection because it is not accessible from any device on the external or service network. If someone were to breach the internal network it would be more difficult to find it.

The office LAN is on it's own subnet, print and file servers required by users of that LAN also reside within the subnet. This cuts down on broadcast traffic and allows restricting access to the other servers by setting up additional permissions.

GIAC uses a private addressing scheme on their internal network with NAT translations handled by the firewall.

### 1.3.6 Network time synchronization

GIAC has an NTP server residing on their service network. The NTP server is set to receive its clock from various public NTP time servers. All other devices on the network are configured to synchronize their clocks to this server.

## **Assignment 2 – Security Policy and Tutorial**

### 2.1 Border router configuration

GIAC uses a Cisco 2650 XM router. This router is configured as the companies first line of defense against intrusion. We will not only use it to route packets but also to filter at a higher level than our firewall. Preventing some of the more basic unwanted types of traffic from reaching the firewall interface not only prevents unnecessary traffic on our network it also eliminates processor consuming filtering functions and provides one more layer of security.

First we'll want to give the router a name to identify it on our network. GIAC has chosen a rather generic name to give it a little bit of obscurity should someone be able to discover it. They have named it ggwr which will be the acronym for GIAC gateway router.

The next thing to do when setting up the router is to set the enable mode password. In addition to setting a password we want to encrypt it and all other passwords so they will not be displayed as plain text for prying eyes. The password-encryption command stores the passwords as an MD5 hash rather than plain text.

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

Telnet access to the router will be restricted to the outside ip address of the firewall since all addresses coming from the internal network are NATed to the firewall's outside address. Telnet from all other addresses will be rejected.

The process for this is a multi step process, the first step is to build an access list with the rules we need.

```
access-list 103 permit tcp 172.135.192.5 0.0.0.0 any eq telnet
access-list 103 deny ip any any
```

The next step is to configure the virtual terminal lines we'll use for telnet.

```
line vty 0 4
access-class 103 in
password 062603244E5C29
login
```

What we've done in this step is to enable VTY lines 0 to 4 to allow login. We also configured a password which must be entered before telnet access will be allowed. The password shown is in the encrypted form due to the service password-encryption command used above.

We then apply our access list 103 which we created above, to the VTY lines. The only users that will now be allowed to telnet to these lines are the ones listed in the access list.

While we will not be allowing telnet access to anyone outside of GIAC we have decided to employ a message of the day. Should anyone access the router via telnet they would then be greeted by our message-of-the-day.

```
ggwr (config) # banner motd
cYou have connected to a Private Computer System.
Unauthorized access beyond this point is not permitted.
Violators will be prosecuted to the full extent allowed
by Local, State, Federal and International Law.c
```

The lower case c before and after the message text is a delimiter indicating the start and end of the message.

There are services which by default are disabled on the router but it should be verified that they are in fact disabled. To verify they are disabled display the router configuration and check for the following lines, they will be displayed in the form shown below if they are disabled. Along with each command line we have included text (*italicized*) from Cisco's manual which briefly describes the service. They are as follows:

```
no service tcp-small-services
no service udp-small-services
```

*By default, the TCP servers for Echo, Discard, Chargen, and Daytime services are disabled.*

*When the minor TCP/IP servers are disabled, access to the Echo, Discard, Chargen, and Daytime ports cause the Cisco IOS software to send a TCP RESET packet to the sender and discard the original incoming packet.*

```
no ip http server
```

*This command enables a simple HTTP server on your system. The HTTP server in Cisco IOS software is used primarily for the Cisco Web browser user interface (UI) and ClickStart.*

*The Cisco Web browser UI allows configuration and monitoring of a router or access server using any web browser.*

There are several services which should be disabled on the router since we are not using them. Disabling unneeded services should be part of hardening an internet facing router. This is our first line of defense against intruders and a good step to prevent ddos attacks. These services should be disabled as follows:

```
no ip source-route
```

IP source routing allows the source of a packet to determine its path through a network rather than allow it to follow normal routing procedures. This ability is mostly no longer necessary and has no legitimate purpose on the GIAC network. The “no” form of the command will ensure that the router blocks these packets.

```
no ip bootp server
```

GIAC does not use the BootP service so we have disabled it on our router.

```
no ip finger
```

*The Finger service allows remote users to view the output equivalent to the show users command.*

*When ip finger is configured, the router will respond to a telnet a.b.c.d finger command from a remote host by immediately displaying the output of the **show users** command and then closing the connection.*

*When the ip finger rfc-compliant command is configured, the router will wait for input before displaying anything (as required by RFC 1288).*

We do not want to give anyone the ability to display the users logged into the router so we disable this option.

```
no cdp run
```

CDP is Cisco's discovery protocol. It is a service which allows a user to display devices connected to a router interface. The output of this command displays a host of information about the device which an outsider may find very useful in hacking our network. We do not want to give out this type of information therefore we will disable this service.

```
ggwr (config)#ntp source ethernet 0/0
ggwr (config)#ntp server 172.135.192.5
```

We want to point our router to the firewall as it's NTP source and tell the router which interface it will use.

```
ggwr (config)#logging 172.135.192.8
ggwr (config)#logging buffered
ggwr (config)#logging console critical
ggwr (config)#logging trap debugging
ggwr (config)#logging facility local0
```

We will configure the logging capability of the router and send our logs to the Syslog server on our internal network. The ip address of the Syslog server is being NATed to 172.135.192.8 by our firewall. That is the address we will configure our router to send its logs to.

```
no snmp-server
access-list 101 deny udp any any eq snmp
access-list 101 deny udp any any eq snmptrap
```

SNMP is used to remotely manage devices containing SNMP MIBs. SNMP is capable of returning detailed information about an enabled device on a network to allow remote monitoring and management. There are several known vulnerabilities utilizing SNMP. GIAC is not using this capability so we will use the command listed above to ensure it is disabled.

We have also set up ACL entries to block any SNMP packets from entering our network through the router.

We will now begin setting up the rest of our access lists on the router.

We will want to block traffic from any of the private IP address ranges and the loopback address and log these attempts as follows:

```
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 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
```

We will want to block multicast traffic also:

```
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
```

We will be expecting no traffic into our network from the class E network range so we will want to block that:

```
access-list 101 deny ip 240.0.0.0 15.255.255.255 any log
```

We want to block all ICMP echo request and echo reply packets as well as ICMP redirect packets from passing through our router so we will block them. The echo request/reply packets are ICMP ping packets which can be used to map the network devices inside our network. ICMP ping and redirect packets can be used to initiate a denial of service attack. The ICMP redirect packets direct changes to a hosts routing tables which could allow an attacker to corrupt our routing tables. We made sure to apply this ACL to the serial interface of our router and designate it as an inbound ACL so that interface will not respond to pings.

```
access-list 101 deny icmp any any echo
access-list 101 deny icmp any any redirect log
```

Because GIAC is primarily running on a Microsoft network we are going to harden our router to prevent known exploits aimed against Microsoft networks. To do that we will block all NetBios traffic from entering or leaving our network.

```
access-list 101 deny tcp any any eq 135-139
access-list 101 deny udp any any eq 135-139
access-list 101 deny tcp any any eq 445
```

We are going to implement the suggestions of the NSA router guide and implement filters against two common attacks, the TCP SYN attack and the Land attack.

According to the NSA guide the Land Attack involves sending a packet to the router with the same IP address in the source and destination address field and with the same port number in the source port and destination port fields.

```
access-list 101 deny ip host 172.135.192.2 host 172.135.192.2 log
```

There should never be any packets inbound from the internet with a source address range of any GIAC address. Such a packet would indicate that someone is attempting to spoof our address. We'll also want to block any packets with a broadcast source address. The packets will be blocked and the activity logged.

```
access-list 101 deny ip 172.135.192.0 0.0.0.255 any log
access-list 101 deny ip host 255.255.255.255 any log
```

Finally we want to allow all other traffic into our network so we'll specifically permit this traffic.

```
access-list 101 permit ip any 172.135.192.0 0.0.0.255
```

Access list 101 will be applied to our serial interface on the inbound direction.

```
ggwr (config-if) # ip access-group 101 in
```

We will build another access list with the rules for outbound traffic.

```
access-list 102 permit ip 172.135.192.0 0.0.0.255 any
access-list 102 deny ip any any log
```

We'll apply this access list to our ethernet interface on the inbound direction.

```
ggwr (config-if) # ip access-group 102 in
```

## 2.2 Firewall configuration

GIAC chose the SonicWall 200 firewall for several reasons, one of those reason is that the firewall runs on a proprietary, hardware based OS which eliminates the threat of hacking that software based operating systems present.

The SonicWall can be managed through any PC attached to its LAN port by using a web browser. Because of that reason a strong user name and password are important.

The SonicWall will log all successful and failed attempts to log onto and administer it. The log will give the ip address of the machine attempting to log on and whether or not it was successful, if it wasn't successful it will log the user id that attempted the logon.

### 2.2.1 Firewall logging

The first thing we are going to do is configure the logging setup of the firewall. In Figure 2.1 we specify the address of our Syslog server and the address of the mail server so the firewall can email the logs to the specified accounts. The alerts mailbox is set up to alert a pager in the event of an email from the firewall.



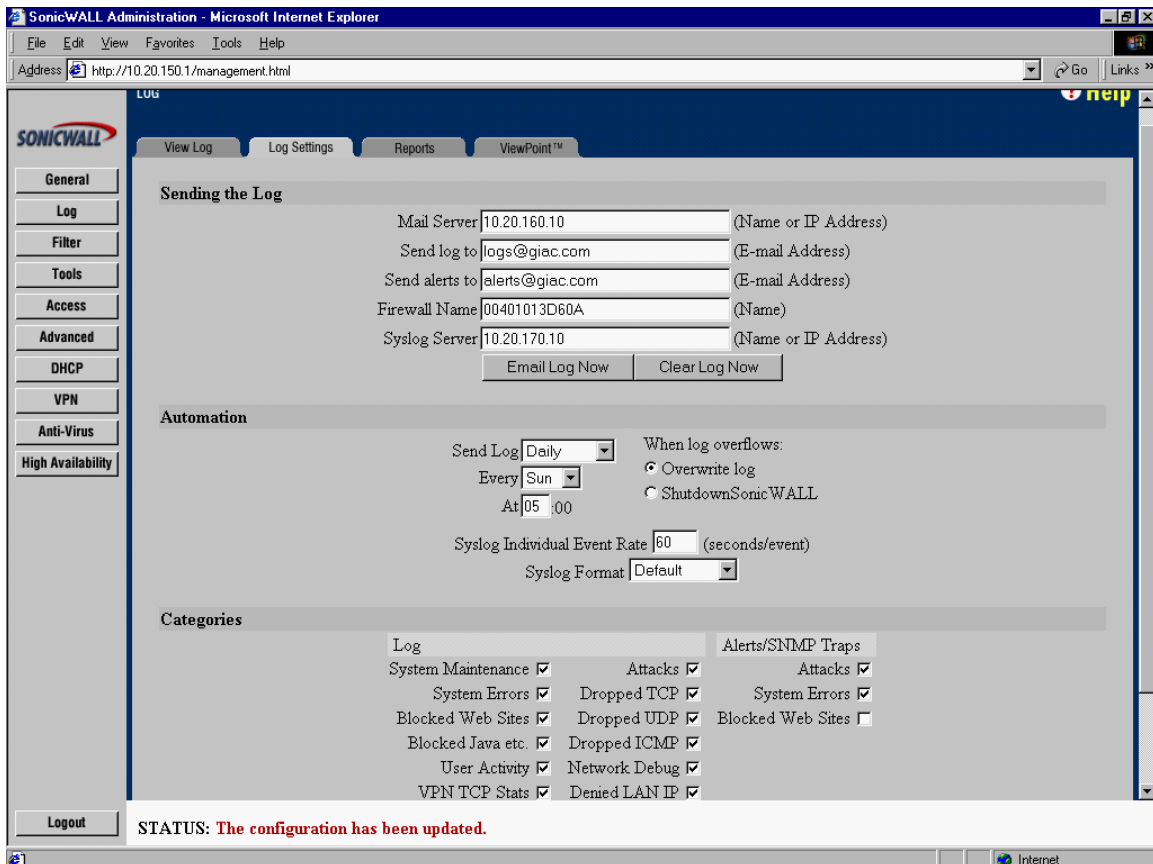


Figure 2. 1

We want to have the logs sent daily as they are checked first thing in the morning by the firewall administrator. We will also have to specify which events we want logged. GIAC has chosen to log all possible events initially and will reevaluate this policy in six months to determine the effectiveness of this policy.

Figure 2.2 We are going to enable one-to-one NAT and specify public addresses for our web server, mail server, DNS server and Syslog server. The web server must have a public address to be reached from outside the GIAC network, we've assigned the server the ip address of 172.135.192.22 which is how it will be known to the internet world, the server is actually known as 10.30.1.6 on our network. Through the NAT function of our firewall, when it sees a packet with a destination address of 172.135.192.22 it looks in its NAT table and sees that the packet's destination address must be changed to 10.30.1.6 and routed out its interface connected to the service network. For outbound packets the firewall will once again look in its NAT table and see that packets with a source address of 10.30.1.6 should have that source address changed to 172.135.192.22 before being forwarded. Our DNS and SMTP servers were configured in the same manner setting up NAT entries for each. In order to allow our router to send its logs to our Syslog server which is on our internal network we had to give it an address via NAT which is routable from our router.

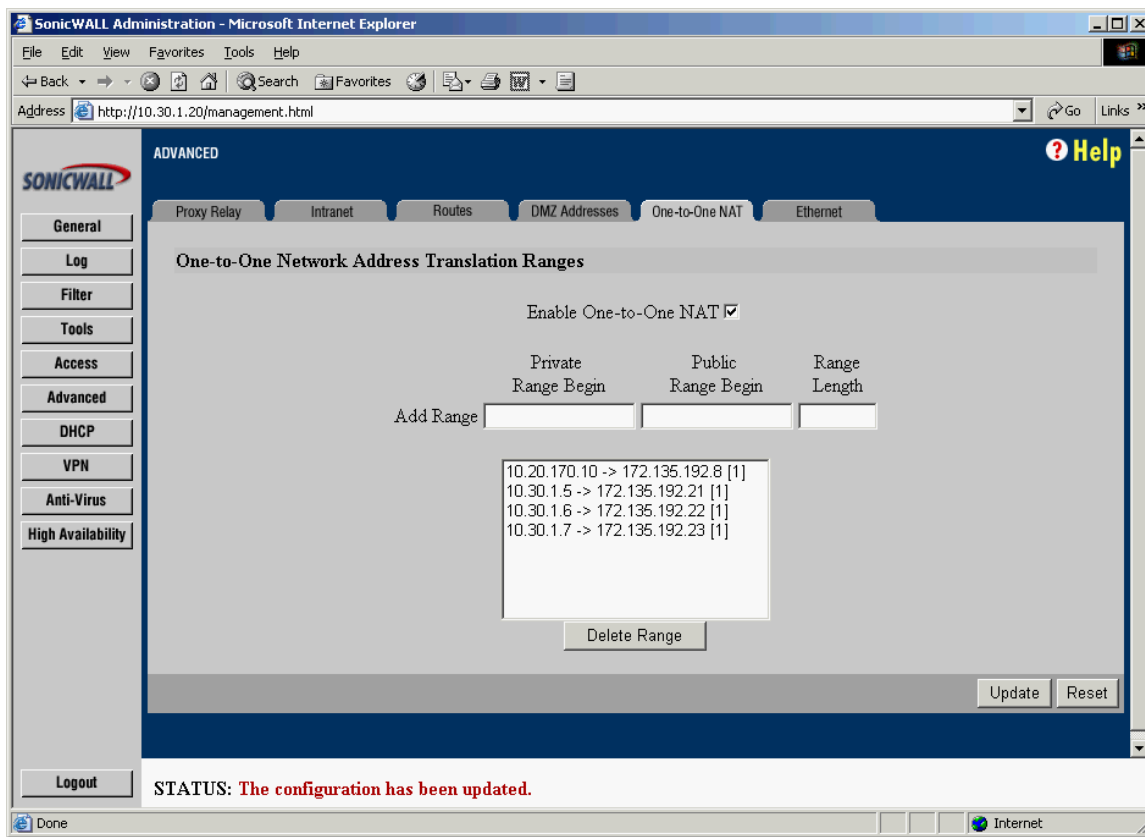


Figure 2.2

Figure 2.3 The SonicWall is capable of gathering statistics for web site hits, bandwidth usage by ip address and by service. These can be useful for monitoring activity through the firewall to determine services usage that may be allowed by rule but when expected usage is being exceeded could raise a flag.

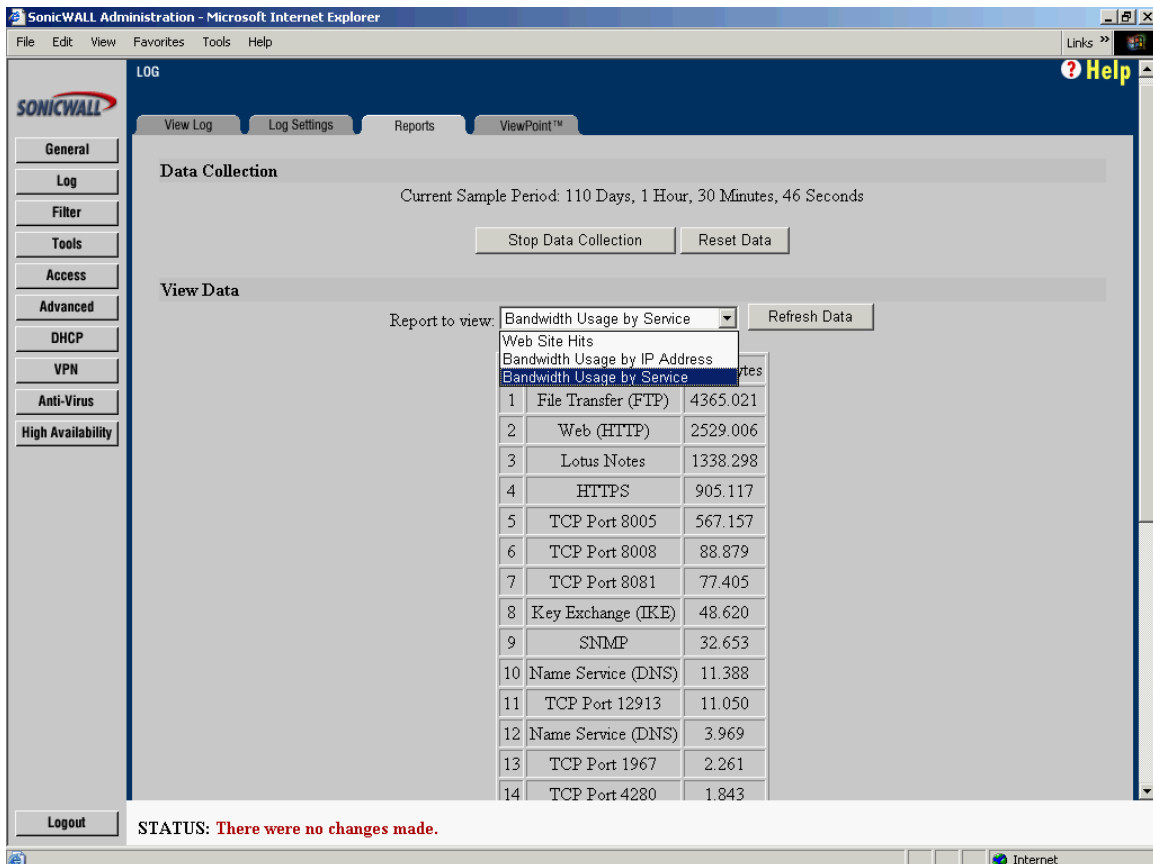


Figure 2. 3

The firewall log can also be viewed from this page on the management screen by clicking on the "View Log" tab.

### 2.2.2 Internet Filtering

The SonicWall is capable of filtering web content based on rules we set up or by a subscription service which will allow the administrator to select categories they wish to filter such as porn. GIAC has elected not to filter internet content for now so we will only need to configure one option on this page.

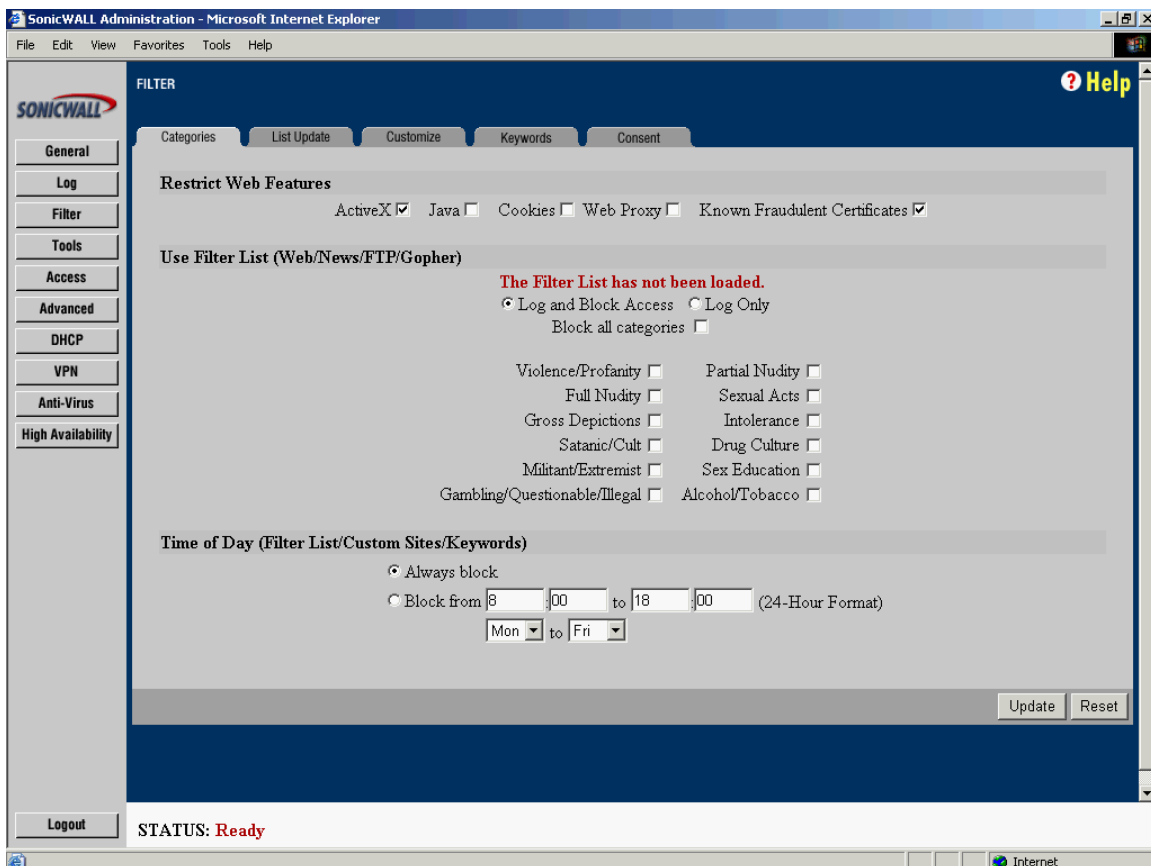


Figure 2. 4

Figure 2.4 GIAC decided to block web content using ActiveX due to the potential for spyware and other malicious content made possible by allowing ActiveX controls. We have also chosen to block known fraudulent security certificates.

### 2.2.3 Firewall Rules

The first rule set we'll configure is HTTP traffic to and from the three areas controlled by our firewall.

Figure 2.5 We are allowing all HTTP, HTTPS, FTP and ping packets from our LAN to the internet and also to our DMZ. GIAC has their proxy web, DNS and mail servers installed on their DMZ thus preventing the need for any access from the internet directly to our internal LAN. We want to enable Ping from the LAN to anywhere, ping capability out to the DMZ and the internet is vital for troubleshooting. We've restricted SMTP and DNS packets to be allowed between the associated servers on the LAN and DMZ only. All other packets from the LAN to anywhere will be blocked with the deny statement.

Priority	Action	Service	Source	Destination	Time	Day	Enable
17	Allow	Ping	LAN	*			<input checked="" type="checkbox"/>
18	Allow	Web (HTTP)	LAN	*			<input checked="" type="checkbox"/>
19	Allow	HTTPS	LAN	*			<input checked="" type="checkbox"/>
20	Allow	File Transfer (FTP)	LAN	*			<input checked="" type="checkbox"/>
22	Deny	Default	LAN	*			<input checked="" type="checkbox"/>
4	Allow	Send Email (SMTP)	10.20.160.10 (LAN)	10.30.1.5 (DMZ)			<input checked="" type="checkbox"/>
5	Allow	Name Service (DNS)	10.20.160.12 (LAN)	10.30.1.7 (DMZ)			<input checked="" type="checkbox"/>

Figure 2. 5

Figure 2.6 We'll allow HTTPS access between the DMZ and the internet. HTTPS allows secure socket layer encrypted connections to our external web proxy via TCP port 443. As stated earlier GIAC will allow only those SSL connections which support 128 bit encryption. GIAC customers will be able to order product from the web server via an HTTPS connection.

16	Allow	HTTPS	WAN	DMZ			<input checked="" type="checkbox"/>
----	-------	-------	-----	-----	--	--	-------------------------------------

Figure 2. 6

Figure 2.7 The SMTP mail server on the DMZ acts as an external mail relay. It will relay mail from our internal mail server to the internet and from the internet to our internal mail server. This gives an added layer of protection by preventing any direct access to our internal mail server from the internet community.

GIAC has employed virus scanning software on this mail server to scan all incoming mail for malicious content. Typically viruses and trojans arrive as attachments to an email, our virus software will scan for any known variants and block or quarantine any mail containing malicious content. The virus software is configured to send its logs to our Syslog server. The virus definitions are updated weekly unless the vendor has discovered a new virus which demands immediate attention, in this case they can do updates as necessary.

We have enabled SMTP from the LAN mail server to the SMTP relay on the DMZ, from the WAN (internet) to the mail relay at 10.30.1.5 on the DMZ and from the mail relay on the DMZ to our internal mail server.

DNS has been enabled from our internal DNS server to our proxy DNS server on the DMZ. Zone transfers will be allowed from the internal DNS server to the proxy on the DMZ. The DNS server on the DMZ will service all inbound DNS requests from the internet.

HTTP and HTTPS packets are allowed from the WAN to our web server proxy on the DMZ.

We have decided to allow ping packets from the IP addresses of our router and IDS into the LAN for troubleshooting efforts.

We've enabled the IKE service to allow for key exchange between us and our partners, suppliers and home office workers. The key exchange is handled by our firewall so we will allow IKE packets inbound to the firewall only, all outbound packets will be allowed.

7	Allow	Send Email (SMTP)	WAN	10.30.1.5 (DMZ)	<input checked="" type="checkbox"/>
8	Allow	Name Service (DNS)	WAN	10.30.1.7 (DMZ)	<input checked="" type="checkbox"/>
16	Allow	HTTPS	WAN	DMZ	<input checked="" type="checkbox"/>
23	Deny	Default	WAN	*	<input checked="" type="checkbox"/>
1	Allow	Syslog	172.135.192.4 (WAN)	172.135.192.8 (LAN)	<input checked="" type="checkbox"/>
15	Allow	Ping	172.135.192.4 - 172.135.192.6 (WAN)	LAN	<input checked="" type="checkbox"/>
12	Allow	Key Exchange (IKE)	*	10.30.1.20 (LAN)	<input checked="" type="checkbox"/>
13	Allow	Web (HTTP)	*	10.30.1.6 (DMZ)	<input checked="" type="checkbox"/>

Figure 2. 7

Figure 2.8 We will need to allow Syslog log reporting through from our gateway router to our Syslog server. The rule will be specific not only in the protocol allowed but the addresses allowed since this is the only exception to our policy of not allowing any packets to flow from the WAN to the LAN.



1	Allow	Syslog	172.135.192.4 (WAN)	172.135.192.8 (LAN)	<input checked="" type="checkbox"/>		
---	-------	--------	---------------------	---------------------	-------------------------------------	---	---

Figure 2.8

Figure 2.9 shows our rule allowing ESP packets originating from the firewall outbound to the WAN. This is necessary to allow our ESP encrypted packets to travel within the IPSec tunnels.



9	Allow	IPSec (ESP)	10.30.1.20 (*)	WAN	<input checked="" type="checkbox"/>		
---	-------	-------------	----------------	-----	-------------------------------------	---	---

Figure 2.9

We are putting in specific rules governing the flow of packets into and out of our DMZ for the various servers. We will restrict SMTP packets from the internet to the mail relay server on the DMZ only. The only service the mail relay serves is to relay mail to our mail server on the LAN and send and receive mail on the internet, so we are allowing packets from this server to access the mail server on the LAN and anywhere on the WAN.

HTTP packets from the web proxy on the DMZ are allowed to the actual web servers on the LAN only.

DNS packets are allowed from anywhere to our DNS server on the DMZ but are allowed to flow out to the internet from our DNS server only. We felt it best to specify exactly which types of packets would be allowed out from the DMZ and what servers they would be allowed from. This will provide protection from hackers attempting to hijack servers for malicious attacks from other networks.

2	Allow	Send Email (SMTP)	10.30.1.5 (DMZ)	10.20.160.10 (LAN)	<input checked="" type="checkbox"/>
10	Allow	Send Email (SMTP)	10.30.1.5 (DMZ)	WAN	<input checked="" type="checkbox"/>
6	Allow	Web (HTTP)	10.30.1.6 (DMZ)	10.20.160.13 - 10.20.160.14 (LAN)	<input checked="" type="checkbox"/>
11	Allow	Name Service (DNS)	10.30.1.7 (DMZ)	WAN	<input checked="" type="checkbox"/>
14	Allow	Name Service (DNS)	*	10.30.1.7 (DMZ)	<input checked="" type="checkbox"/>

Figure 2.10

Figure 2.11 There are four default rules set up initially in the SonicWall. They are set up to allow all traffic from the internet to the DMZ and DMZ to the internet, to allow traffic from the LAN to anywhere and deny traffic from anywhere to the LAN. We have modified all of the default rules to implicitly deny all packets that haven't been allowed by one of our other rules.

Because of the way the rules are accessed by the firewall these rules are the last ones in the rule set. The firewall looks for matches from the top rule which is number 1 down through the rule set until it finds a match. If no match is found by the time it gets to numbers 22 – 26 it will match one of the deny statements and drop the packet.

22	Deny	Default	*	LAN	<input checked="" type="checkbox"/>
23	Deny	Default	LAN	*	<input checked="" type="checkbox"/>
24	Deny	Default	WAN	*	<input checked="" type="checkbox"/>
25	Deny	Default	DMZ	*	<input checked="" type="checkbox"/>
26	Deny	Default	*	DMZ	<input checked="" type="checkbox"/>

Figure 2.11

Figure 2.12 By default the SonicWall firewall filters the following TCP attacks - Syn flood, Ping of death, IP Spoofing, Land attack, Smurf amplification, sequence number prediction.

The rule base is referenced linearly from the top down to see if a rule applies to the packet as it enters the interface. The rules are referenced one at a time until a rule is found that applies to the packet. If none of the specific rules apply then the last rules in Figure 2.11 will deny any packet.

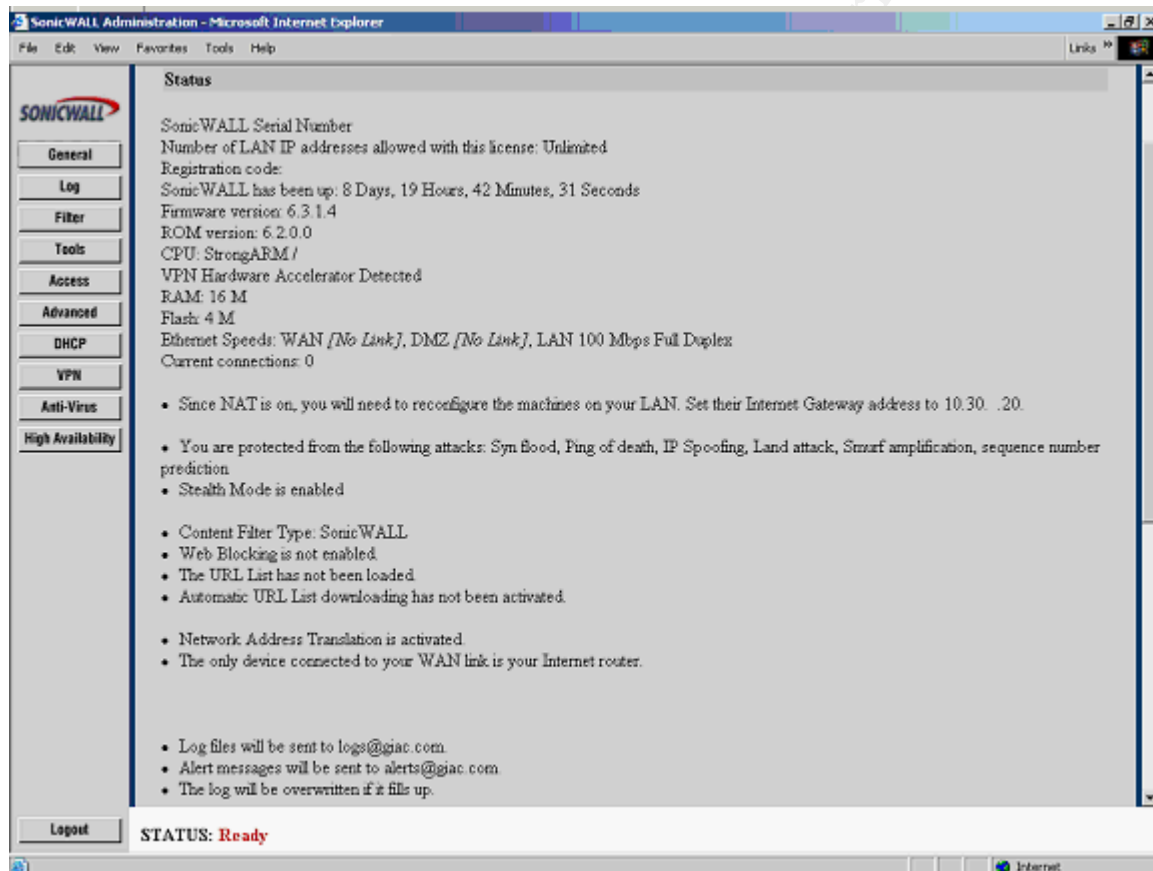


Figure 2.12

## 2.2.4 VPN Policy

As stated earlier GIAC uses the IPSec tunneling protocol for VPN's to their partners and remote employees. IPSec is a set of protocols (IKE, AH, ESP) which add security services to the network layer. IPSec supports the following types of communication – host-to-host, gateway-to-gateway and gateway-to-host.



The primary use of the VPN's at GIAC are to provide secure transport of information between the remote employees and partners and GIAC's internal network components. All GIAC VPN's will terminate on the SonicWall firewall on the local end and a specific host's ip address or a remote SonicWall firewall on the remote end. All remote hosts terminating VPN's will be loaded with approved VPN client software configured for IPSec tunneling.

IPSec will be configured using the ESP security protocol, DES3 encryption and the MD5 hashing algorithm in tunnel mode. They must also be running approved anti-virus software.

Figure 2.13 GIAC's partners will have a VPN configured to allow connections to a specific server on the internal LAN. As explained in the Partners section they will be allowed access to an internal web server which has their individual web pages and the database they need access to. VPN's will be built to have access to that server only. This is accomplished in part by enforcing all firewall rules on the VPN and setting up a specific rule to allow packets between the partner's host and the server on GIAC's LAN. Figure 2.14

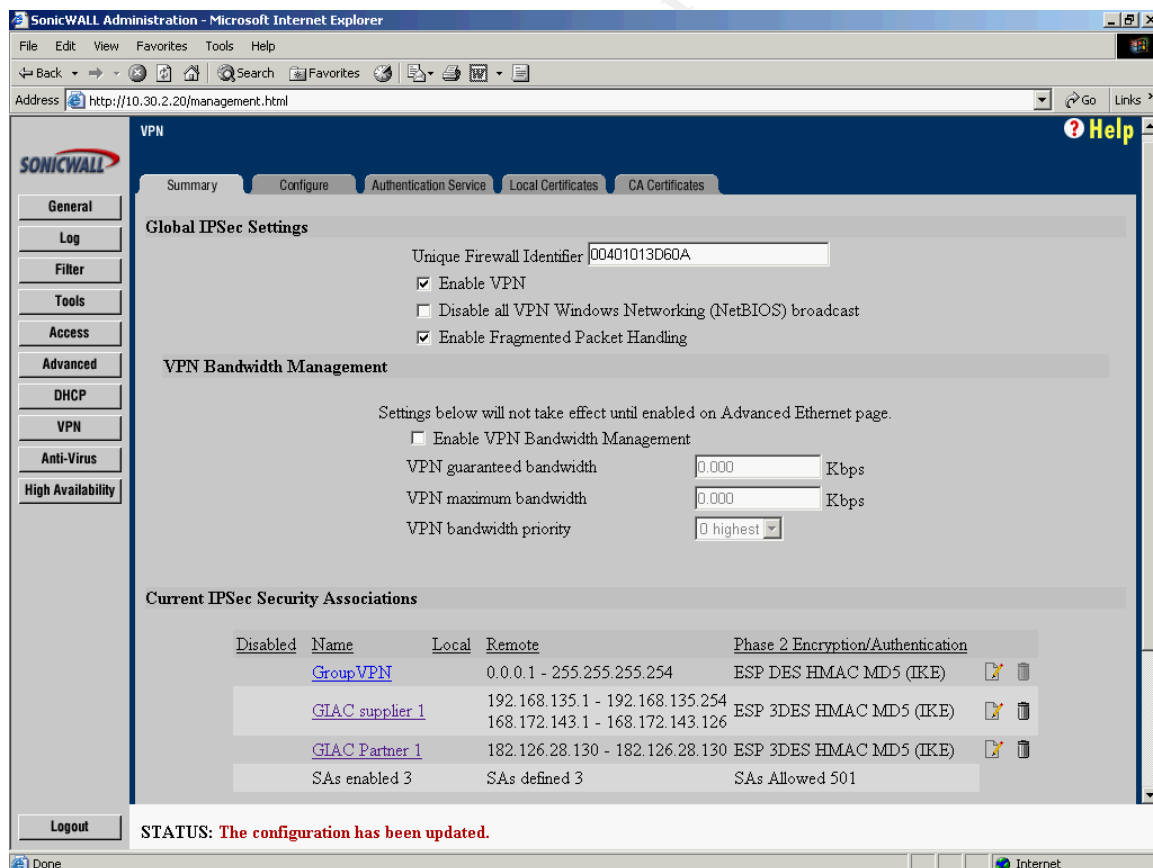


Figure 2.13

21	Allow	Default	182.126.28.130 (WAN)	10.20.160.13 (LAN)	<input checked="" type="checkbox"/>
----	-------	---------	----------------------	--------------------	-------------------------------------

Figure 2.14

Figure 2.15 GIAC's remote employees will have access to the internal LAN but all firewall rules that apply to internal users will be applied to the VPN's as well. This is accomplished by enforcing firewall rules on individual VPN's.

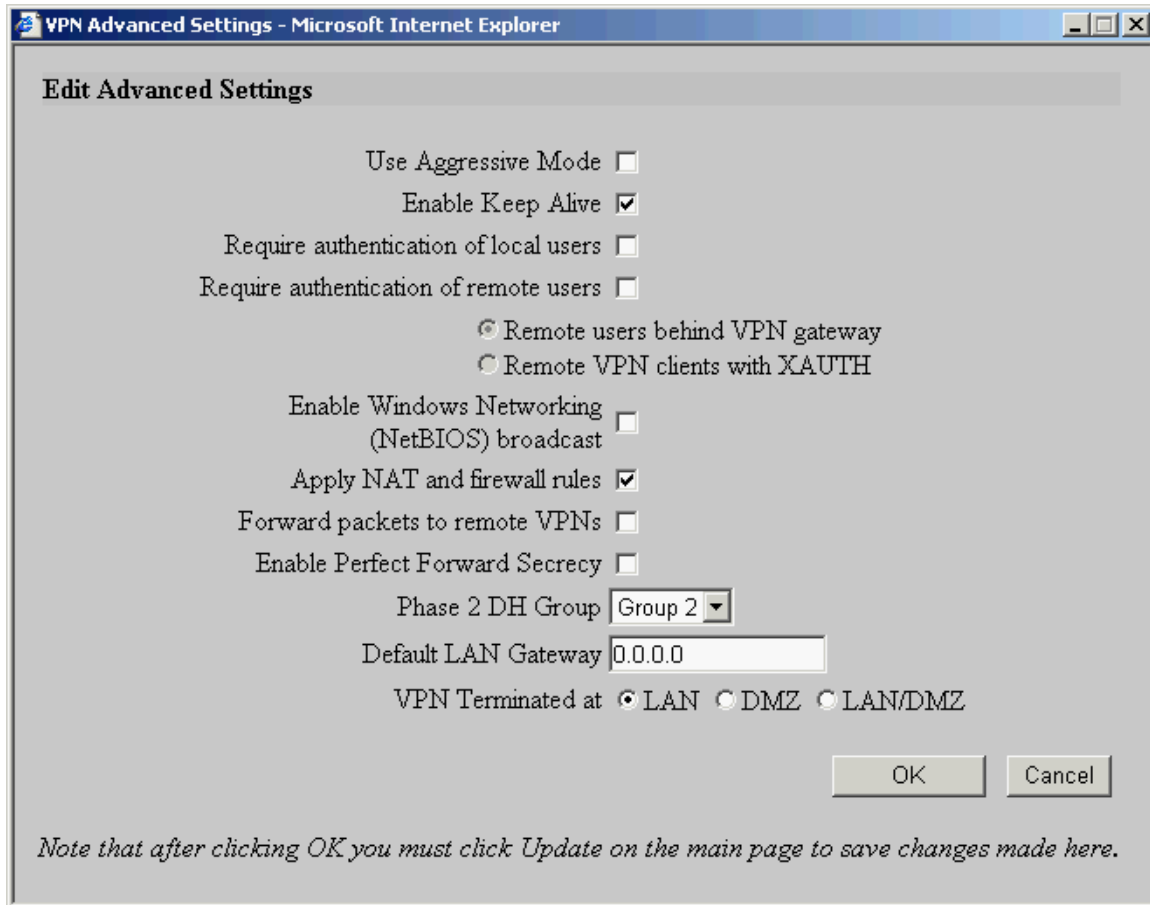


Figure 2.15

The SOHO 3 firewall's located at remote employee's homes require local authentication before allowing use of the VPN. This was done to allow their families use of the home machine for internet access through the firewall's ISP connection without the ability to access GIAC network resources.

Remote employees are provided copies of the corporate antivirus software and must have it loaded on their remote machines. This is stated in the corporate security policy the employees were required to sign.

## 2.3 VPN Tutorial

GIAC uses VPN tunnels to allow their suppliers and some home office workers access to services on the internal network. All VPN tunnels terminate on the SonicWall firewall and use the IPSec protocol.

In this VPN tutorial we will concentrate on setting a VPN to one of GIAC's remote partners.

The CA authenticates the public key we will use for IKE, GIAC has decided to use Verisign as their CA. We will use this CA to sign all VPN certificates.

PKI is the acronym for Public Key Infrastructure. PKI consists of many components which together provide authentication, confidentiality, nonrepudiation and integrity of the information exchanged.

The CISSP Exam Guide by Shon Harris gives the following example of PKI:

*The infrastructure of this technology (PKI) assumes that the receiver's identity can be positively ensured through certificates and that the Diffie-Hellman exchange protocol (or another type of key exchange protocol) will automatically negotiate the process of key exchange. So the infrastructure contains the pieces that will identify users, create and distribute certificates, maintain and revoke certificates, distribute and maintain encryption keys and enable all technologies to communicate and work together for the purpose of encrypted communication.*

The process of generating the public key certificates is one of the most important parts of PKI. The most commonly used public key certificate is the x.509 v3 certificate.

The steps in generating this certificate are briefly explained here.

If one of our users wants to initiate a session with GIAC they would first need to establish a public/private key pair for themselves. They would do this by requesting a certificate from a trusted CA, GIAC is using Verisign. The CA will generate a certificate with the users public key and their identity information. Either the CA or the user will generate a corresponding private key for the user.

*Note: The correlation between public and private keys is such that through the wonders of mathematics data encrypted with your private key, your public key and my public key can only be unencrypted with the corresponding public and private keys. Thus, if I use the your public key and my private and public keys to*

*encrypt a session key and send it to you, you can use your corresponding private and public keys and my public key to decrypt the session key. Clear as mud?*

They will then use their private key and my public key which can be obtained from the CA or I can send it separate from the encrypted data, to encrypt a session key. The only keys that can decrypt this session key are the same keys or their corresponding public/private keys.

When I receive the encrypted packet I will use my private/public keys and your public key to decrypt the session key.

At this point we both have a unique session key known only to us to use in the encryption/decryption of our data packets.

In the case of GIAC we will generate our own signed certificates for our VPN end users to use when authenticating during the IKE process of the IPSec negotiation. This eliminates the need for the end users to have to go to a CA and request one.

To do this go to the Generate Certificate Signing Request section shown in Figure 3.1, and complete the fields as follows.

First select a name you want to use to identify the certificate. We've chosen GIAC Firewall Cert.

Using the drop down menus, enter information for the certification request. As you enter information in the Request fields, the Distinguished Name (DN) is created. You may also attach an optional Subject Alternative Name to the certificate such as the Domain Name or E-mail address

Once all of the information has been filled in click the Generate button.

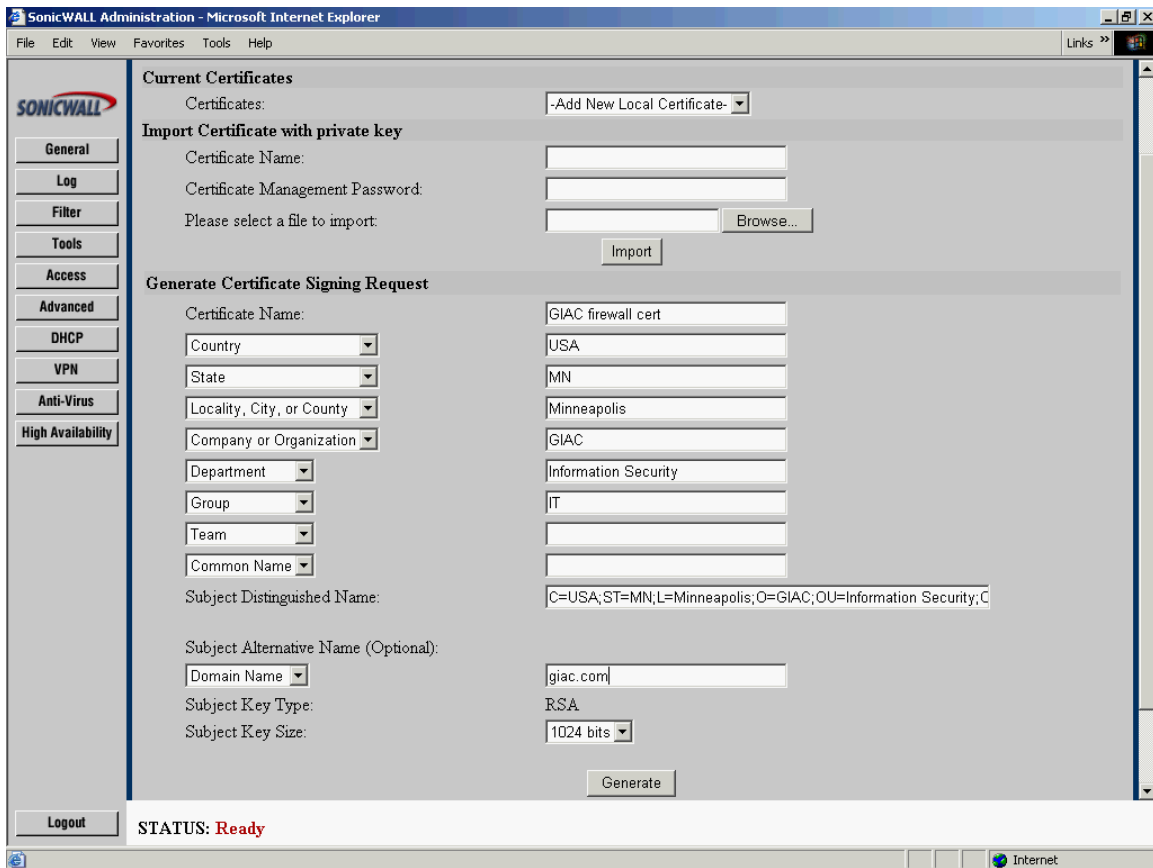


Figure 3.1

Once the key has been generated you will see the screen in Figure 3.2.

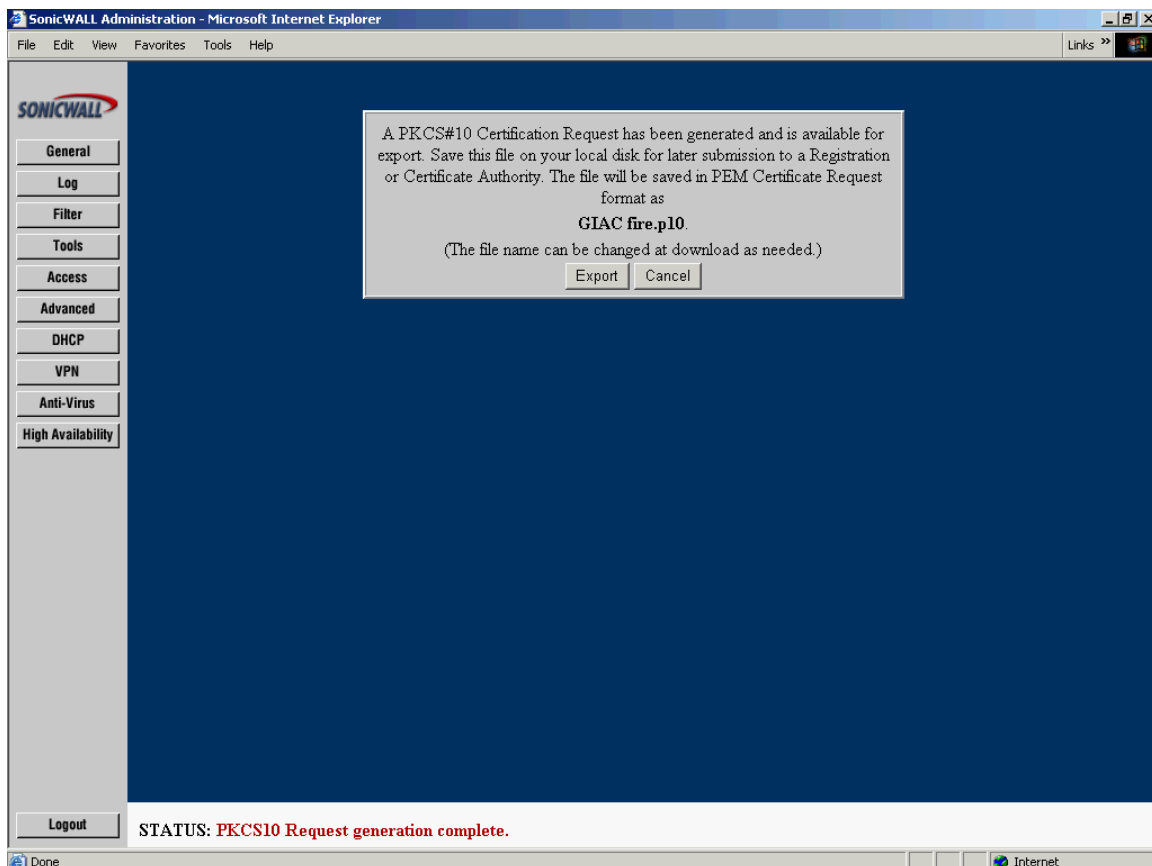


Figure 3.2

Click on the Export button and you will be asked where to save the file. This certificate will be signed by our CA.

Next go to the Local Certificates tab in the management window and you'll see the screen in Figure 3.3.

In the Import Signed Certificate box browse to the signed certificate. Click on the Import Certificate button and the signed certificate will be imported into the firewall. This certificate can now be used in our VPN configuration. We'll need to do this to create signed certificates for the remote end of the VPN tunnel as well.

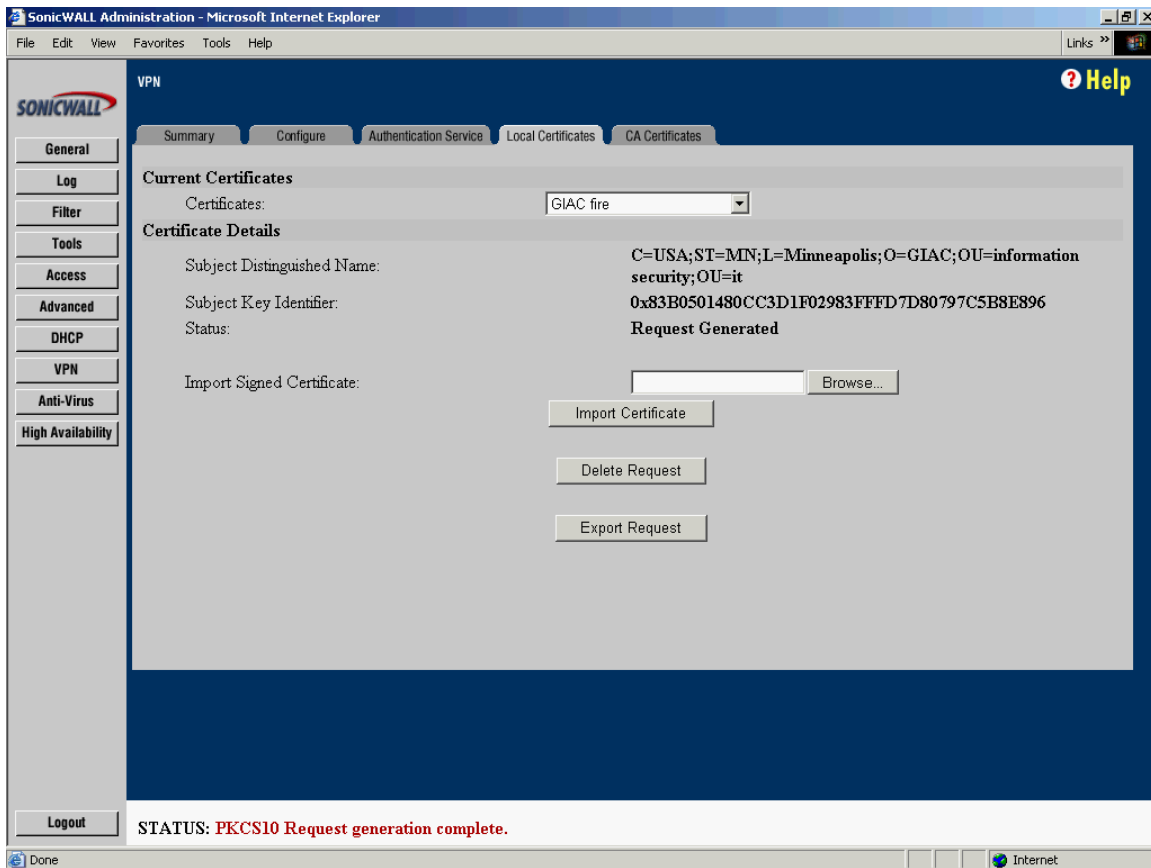


Figure 3.3

In order to get the remote user their certificate we'll have to use a method that can ensure the certificate doesn't fall into the wrong hands. In GIAC's case we have a secure web site and the supplier has their own area which they have access to for business purposes. They will access their page using an HTTPS session and retrieve their certificate via the link we've set up for them.

Our next step is configuring the actual SA. Click on the tab labeled Configure in the VPN section of the management interface. You will see the screen in Figure 3.4.

In the Security Association field select –Add new SA–

The IPSec keying mode will be IKE using 3<sup>rd</sup> Party Certificates.

We'll name the SA something that will allow us to easily identify it in the VPN summary. For our SA we've chosen to name it Service Provider 1.

In the Select Certificate field there is a drop down which will list all of the 3<sup>rd</sup> party certificates which have been imported into the firewall. Select the appropriate one.

Next we'll need to specify the ip address of the gateway which will be terminating the VPN tunnel at the remote end. We have entered the ip address of the firewall at our service provider which they'll be using to terminate the VPN.

The Phase 1 encryption/Authentication field defines the encryption and authentication methods used to secure phase 1 exchange in IKE. We've chosen to use 3DES and MD5.

The Phase 2 encryption/Authentication field we've selected ESP 3DES HMAC MD5. SonicWall's help file describes this selection as follows - Tunnel and Triple DES Encrypt with MD5 Authentication. This method uses 168 bit 3DES as the encryption method and HMAC MD5 Authentication. Security professionals consider 3DES to be an extremely secure encryption method, but it will have the most significant impact on the data throughput of SonicWALL.

In our network the increased impact on data throughput caused by using Triple DES and MD5 will not be a significant factor and is easily outweighed by the security benefit.

© SANS Institute 2003, Author retains full rights.



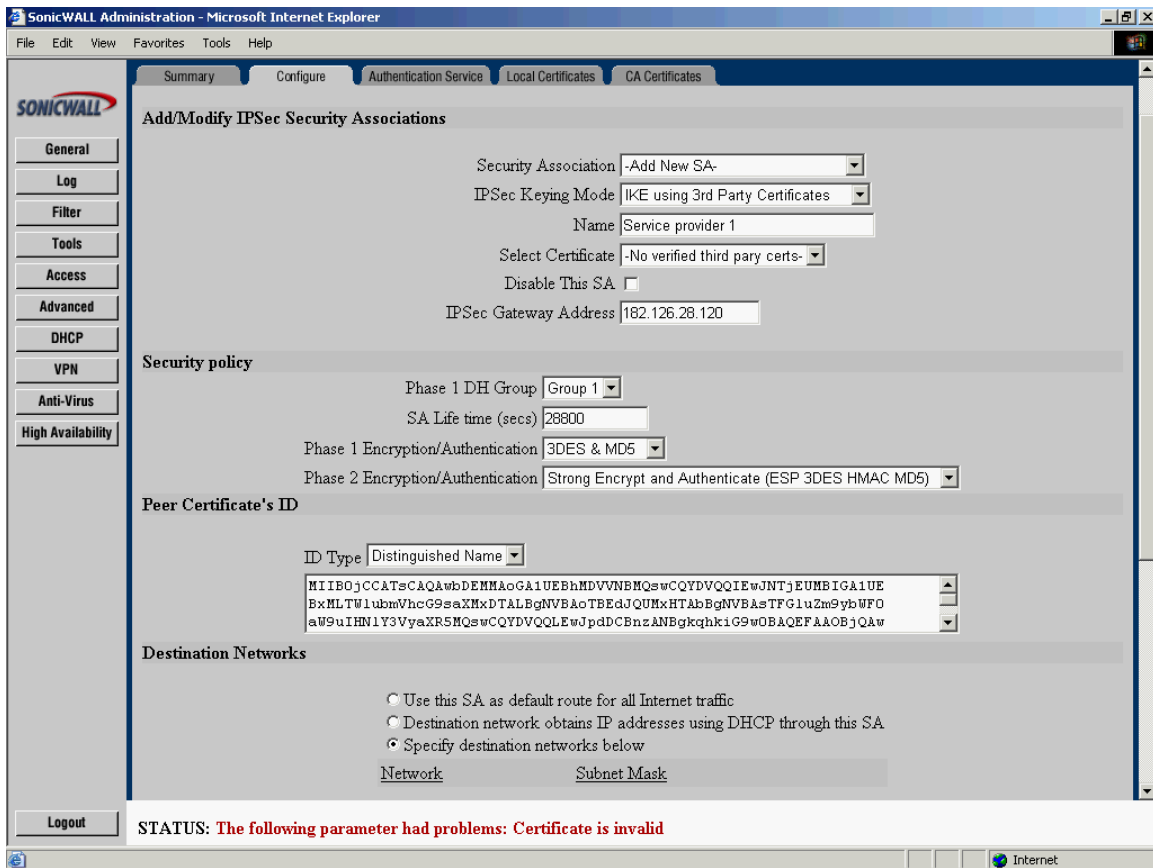


Figure 3.4

In the field labeled Peer Certificate's ID enter the ID Type and paste the information from the local certificate into the field.

Next click on the Advanced Settings button and you'll see the screen in Figure 3.5.

© SANS Institute 2003, L

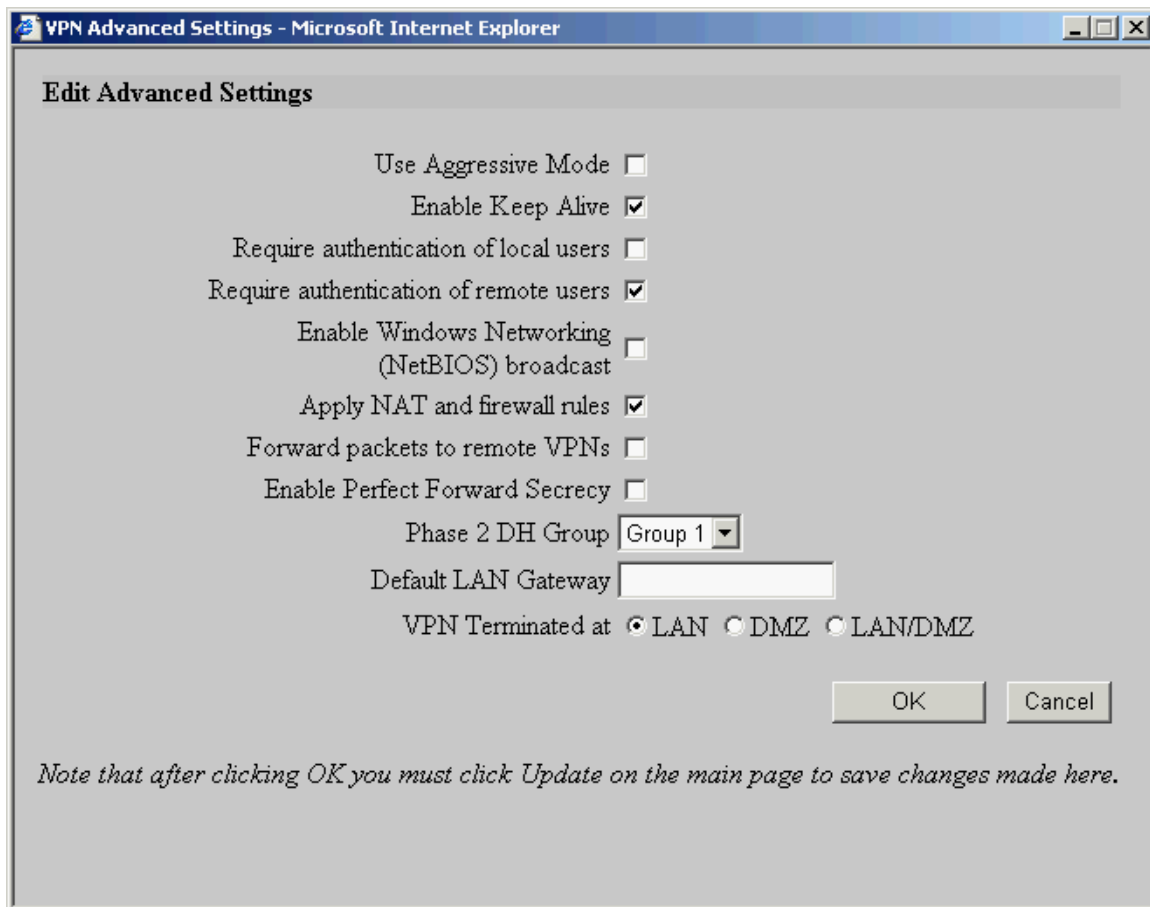


Figure 3.5

We will use main mode on all VPN tunnels terminating on a remote gateway with a static IP address. This means we'll leave the Use Aggressive Mode box unchecked.

We've elected to require authentication of the remote user. When this field is selected the remote user is required to enter the user ID and password for the user account that we've configured on the firewall. This will help to ensure that others at the remote end will not be able to access our network by simply sitting down in front of a workstation.

## 2.4 VPN Verification

Once our remote client has configured their workstation to use the VPN tunnel we will enable the VPN by checking the box labeled enable VPN shown in Figure 3.6.

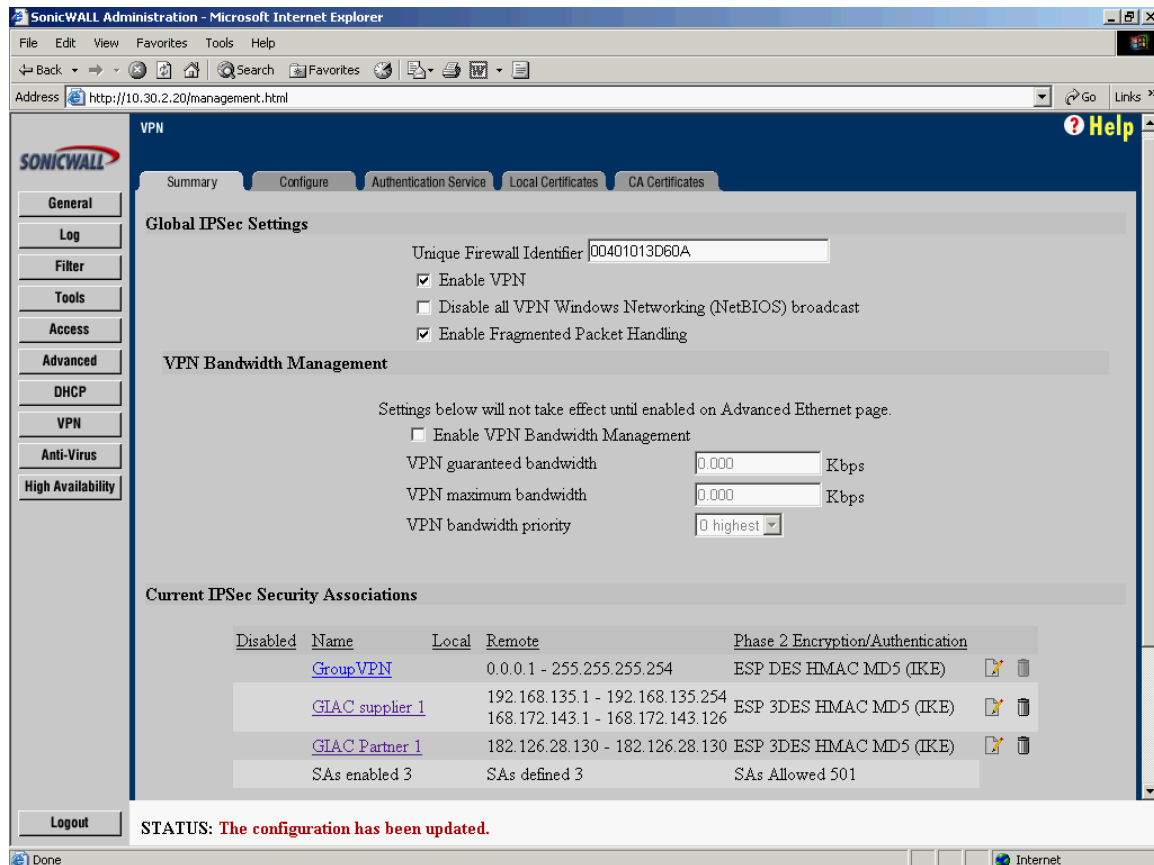


Figure 3.6

### 2.4.1 Verify IPSec Traffic

Now we will want to place a sniffer on the network and capture packets to verify our tunnel is up to the destination address. We will place the sniffer on the Ethernet segment between the router and the firewall and configure it to capture packets with a source address of 182.126.28.120.

To generate traffic we'll have someone from the users network access the application server on our network.

### 2.4.2 Analyze sniffer capture

The output from our sniffer trace should show only packets between our firewall and 182.126.28.120. With everything working properly we expect to see primarily ISAKMP and ESP packets exchanged indicating the traffic is IPSec.

As an extra step we will then have the remote user stop accessing the application server and the packet exchange will stop.

Since our remote users were able to access the server on our network we now know that the IPSec tunnel was up and working.

© SANS Institute 2003, Author retains full rights.

## **Assignment 3 – Verify the Firewall Policy**

### **3.1 Planning the audit**

For the purpose of auditing our firewall we will use three tools. The first is a port scanner, Nmap is a free software port scanner which can be run on both Unix and Windows platforms. The second is Nessus which is a security scanner. The following lines are from the Nessus home page describing the Nessus scanner.

*The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner.*

*A security scanner is a software which will audit remotely a given network and determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way.*

*Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not consider that a given service is running on a fixed port - that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number of the remote services, but will really attempt to exploit the vulnerability.*

*Nessus is very fast, reliable and has a modular architecture that allows you to fit it to your needs.*

The third tool we'll use is a sniffer running on a laptop which we'll use on the scanned network to verify the scans are actually being run against the device we intended them to be run against. The sniffer will capture any packets that make it through the firewall.

One of our first steps will be to document in simple form what the firewall rules are configured to do and on which interface. That will assist us in determining how well we've performed.

WAN interface		
Service	Inbound	Outbound
HTTP	To web proxy (DMZ)	Anywhere
HTTPS	To web proxy (DMZ)	Anywhere
FTP	Deny	From LAN
SMTP	To mail proxy (DMZ)	Anywhere
DNS	To DNS proxy (DMZ)	Anywhere
Ping	None	Anywhere
IKE	To 10.30.1.20 (LAN)	Anywhere
Syslog	172.135.192.4 (router)	172.135.192.8 (Syslog on LAN)
Deny everything else In and Out		

DMZ interface		
Service	Inbound	Outbound
HTTP	To 10.30.1.6	WAN, LAN 10.20.160.13, 14
HTTPS	To 10.30.1.6	WAN
FTP	LAN	None
SMTP	To 10.30.1.5	To 10.20.160.10
DNS	To 10.30.1.7	WAN
Ping	From LAN	None
IKE	None	None
Syslog	None	None
Deny everything else In and Out		

LAN interface		
Service	Inbound	Outbound
HTTP	From 10.30.1.6	Anywhere
HTTPS	None	Anywhere
FTP	None	Anywhere
SMTP	From 10.30.1.5	To 10.30.1.5
DNS	None	To 10.30.1.7
Ping	None	Anywhere
IKE	Anywhere to FW	Anywhere
Syslog	From router	None
Deny everything else In and Out		

The testing will be scheduled for 01:00 Saturday to ensure the least amount of impact to our customers who may be using the web site, our partners and our employees. At that time of night there should be virtually no impact to any of the groups mentioned so we will be free to test as we please, upper level management has agreed that we should be free to do all of our testing at this time.

The scanning tools we'll be using are free so there will be no cost associated with them. GIAC already has the laptop computers and the sniffer software so there will be no associated cost there either.

The only real cost will be in terms of man-hours. We are going to assume an hourly cost of \$100.00/employee and we should be able to do our testing with two people. We could probably do this with just one person but the testing will be easier and go quicker with two, offsetting the extra cost.

We'll need to schedule time as follows:

To review our policy and network architecture - 6 hours  
Plan the audit and become familiar with tools – 12 hours  
Time for two people to perform the audit (cumulative) - 16 hours  
Time to analyze audit results – 8 hours

Total; 40 hours @ \$100.00/hr = \$4000.00

Upper management has reviewed and accepted our cost estimate.

## 3.2 Conducting the Audit

### 3.2.1 Run Nmap scans

The first test we'll do is using NmapWin running on a laptop. We'll run the following scans:

- From the external network to the DMZ
- From the external network to the LAN
- From the DMZ to the WAN
- From the DMZ to the LAN
- From the LAN to the DMZ
- From the LAN to the WAN

We have a laptop running TCP Dump on the network being scanned and we'll watch for any traffic making it through the firewall that should be blocked.

NmapWin is configured as follows:

```
-sS -PT -PI -p 1-65535 -O -T 3 -oN xyz.log a.b.c.d
```

We ran the scan on TCP ports 1 through 65535

Options are as follows:

-sS is the Syn stealth scan

-PT and -PI causes TCP and ICMP pings to be sent

-O the scan attempts to detect the OS running on the scanned device (inconclusive in this case as we expected)

-T3 is normal timing

-oN xyz.log is the output name of our log file

The Nmap scans revealed about what we expected to see, Figure 3.1. One exception was a few high order ports open from the LAN out which we didn't expect. While this shouldn't cause any problems, the fact that they're open and shouldn't be still remained.

A simple tweaking of the rules might resolve this but I chose to contact SonicWall tech support to see if I can determine why they might be open when they are not implicitly opened in our rules or if it's a false report.

A quick look at our TCPDump capture shows no packets being allowed through to the inside on these ports. We sent an email to SonicWall tech support and included our firewall ACL rules. In an email response from SonicWall tech support they stated their conclusion to be that the result was a false positive, the ACL rule set should effectively block access to these high ports and the fact that TCPDump saw no packets on these ports on the inside should support that conclusion.



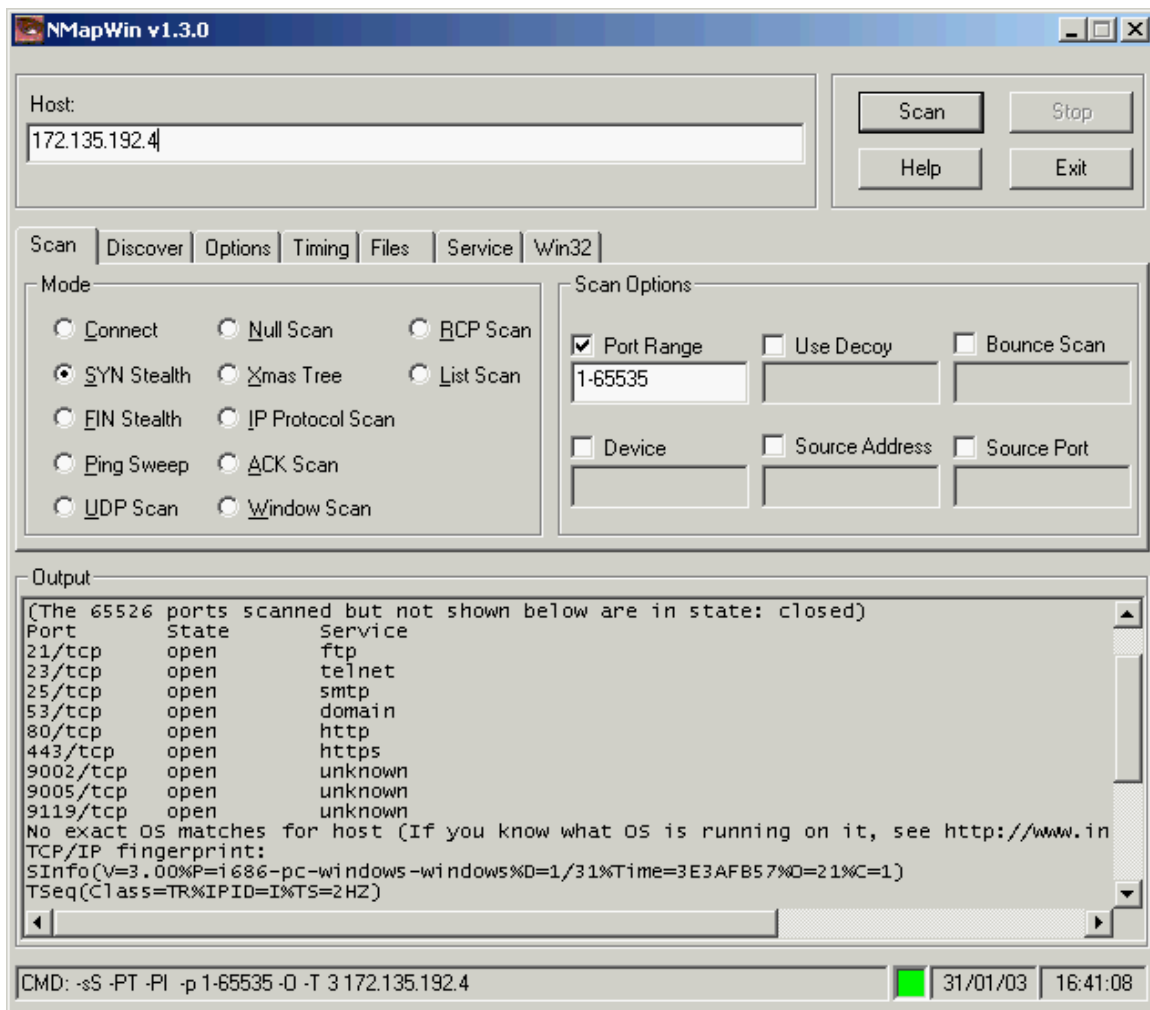


Figure 3.1

### 3.2.2 NMAP scan on border router

We want to run a port scan on our border router to test our access list. We'll run the scan targeting the Ethernet interface on the inside network of the router. Nmap will be configured to target ports 1 – 500 only. This makes the scan quicker and since we haven't configured any ports above 500 in our ACL we have no reason to scan above this.

We also want to check to ensure that ping and trace route packets are dropped. We can use Nmap to run a ping sweep to do this or simply perform ping and trace route from the workstation to the ip addresses of the serial interface and ethernet interface of the router as well as the ip addresses on the firewall. We ran ping sweep on our address range and the router blocked the pings as it was configured to do.

The port scan showed the router blocking the ports we had set up our ACL to be blocked.

### 3.2.3 NMAP scan on the firewall

Next we ran TCP port scans on all ports in the range of 1 – 65535 against the firewall from the WAN side. The firewall allowed packets through only to those ports it was configured to allow from the outside network to the LAN and to the DMZ.

We ran a scan from the DMZ to the LAN to verify the ACL and it performed as expected.

### 3.2.4 Nessus Scan

Nessus was run from a laptop with a Linux OS and the output was saved in HTML format.

The Nessus scan did not reveal anything that would cause alarm. There were two items to note.

While the amount of information given in the banner is minimal we would prefer to see no information about the server given, see Figure 3.2. This information could potentially give a hacker information they could use to exploit vulnerabilities. We'll modify the header information.

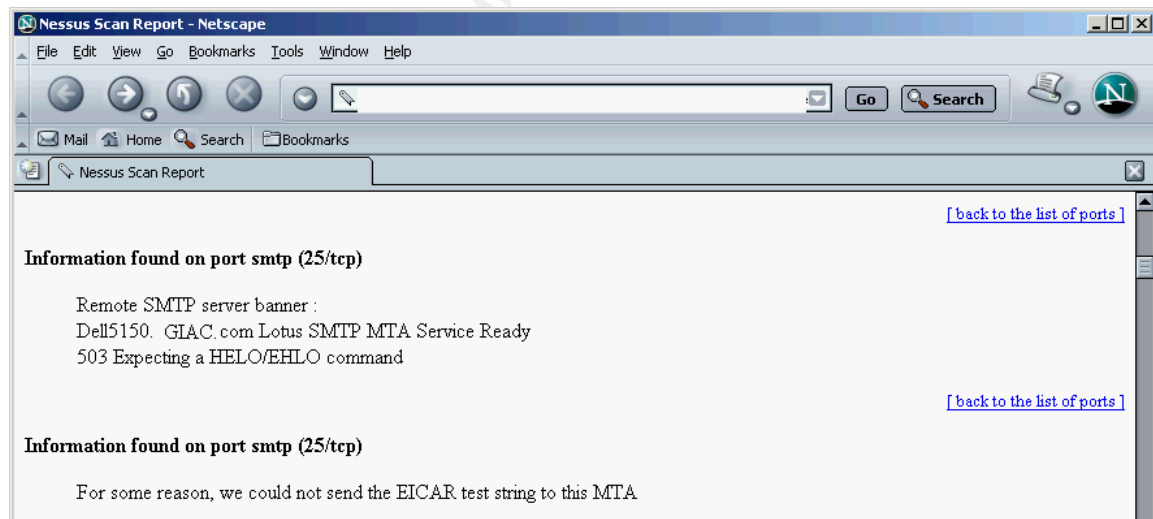


Figure 3.2

Figure 3.3 shows a warning Nessus issued about our web server. While the first item in this screen shot doesn't deal directly with port security it does raise a valid flag. We will modify the web server to send the default page suggested by Nessus when a non-existent page is requested.

The second item in Figure 3.3 is worth noting. The firewall returned notification that the web server is a SonicWall which is of course incorrect and protects the web servers identity but may reveal too much information about our firewall. We will consult with SonicWall on how to prevent the firewall from returning this information.

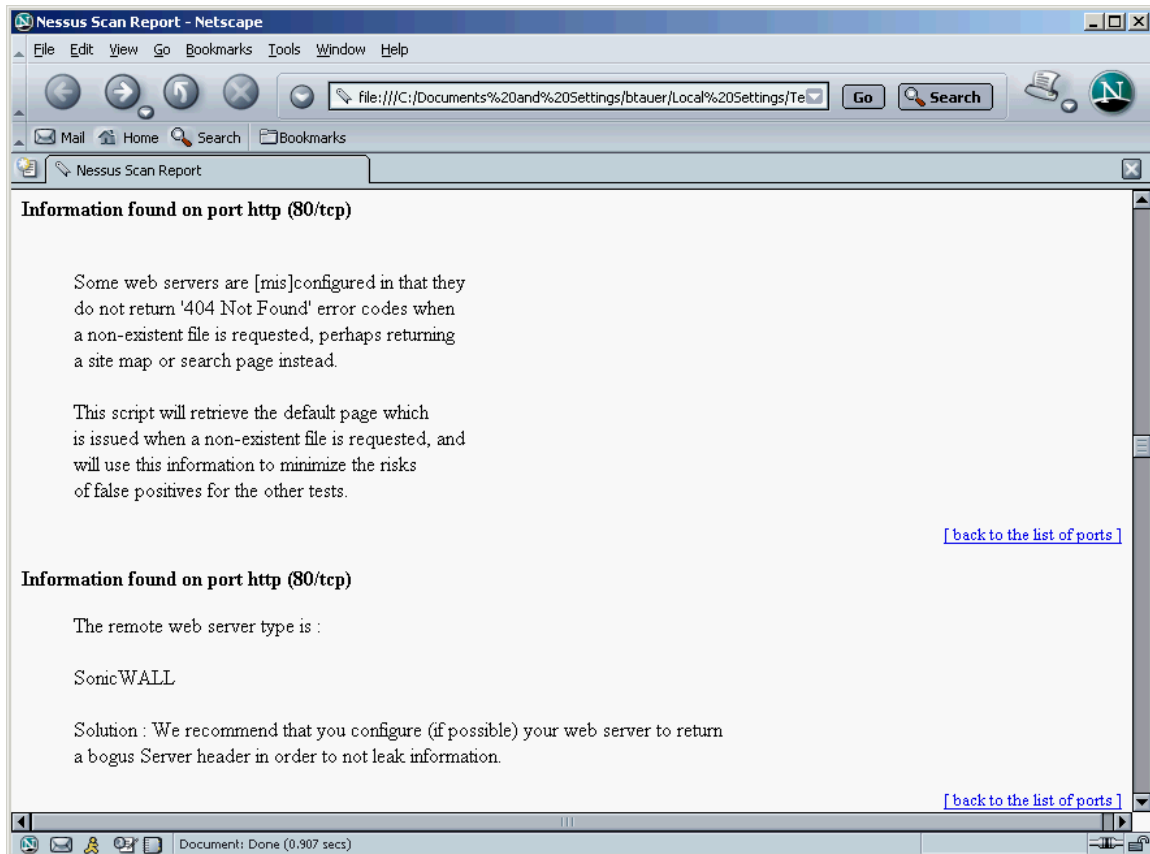


Figure 3.3

### 3.2.5 Verify VPN

Consult the VPN tutorial for information on how the VPN's were verified.

### 3.2.6 Results

Our audit revealed that our firewall and router access rules were functioning as we expected them to. There were a few minor tweaks but aside from that we were very happy with the results of our audit.

While our rule enforcement was good we found a couple of things we will want to correct, such as the web server issues. As we stated above we will work to correct these.

We would like to have an outside company come in and perform an audit of our network security in the future. Not only is it a good idea to get a second evaluation but it could prove that we know our network too well to do a totally unbiased evaluation.

© SANS Institute 2003, Author retains full rights.

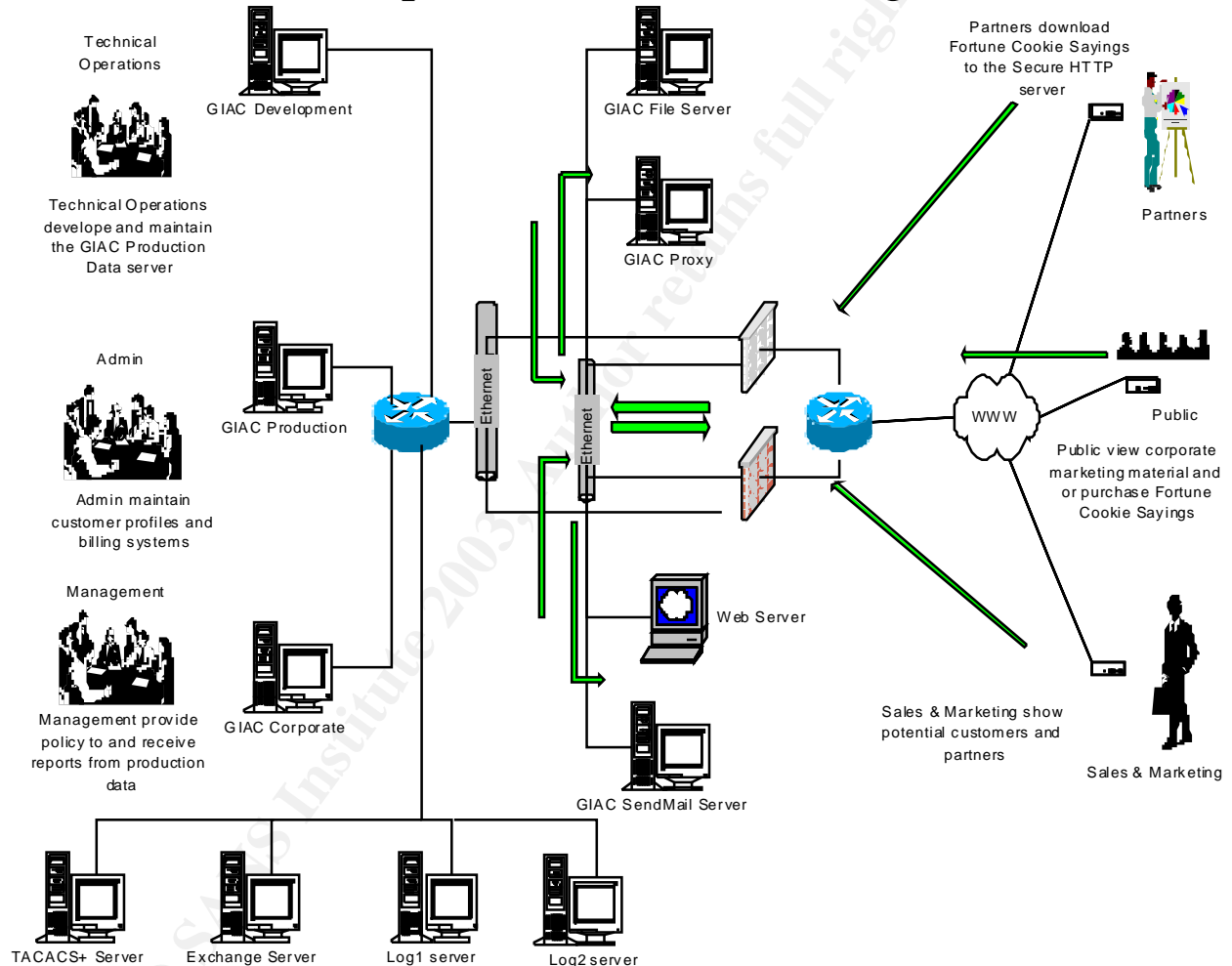
## Assignment 4 – Design Under Fire

### 4.0 Overview

For the design under fire portion of this project I will be using the network design of Stephen Monahan which can be found at:

[http://www.giac.org/practical/Stephen\\_Monahan\\_GCFW.doc](http://www.giac.org/practical/Stephen_Monahan_GCFW.doc)

### GIAC Enterprises – Data Flow Diagram



## 4.1 Perimeter Attack

### 4.1.1 The Perimeter Router

My first point of attack will be the Cisco perimeter router itself. While this may seem like a rather simple attack sometimes it's the simple attacks that cause the most trouble for a target network.

Due to a configuration error in Stephen Monahan's router configuration he is allowing his internal ip addresses to be allowed back in through his external router interface as the source address on inbound packets. The configuration is listed as follows on page 14 of his paper:

```
!  
! Define outbound access to the internet  
! Allow only GIAC registered addresses  
  access-list 101 permit ip 208.10.2.0 0.0.0.255 any  
  access-list 101 deny ip any any log  
  access-list 101 deny udp any any log  
!  
! Define inbound access from the internet  
! Deny GIAC registered addresses  
  access-list 107 deny ip 208.10.1.0 0.0.0.255 any log  
  access-list 107 deny udp 208.10.1.0 0.0.0.255 any log
```

While his routers serial interface is configured as follows on page 13:

```
! Outside link to ISP  
  interface Serial0/0  
    description Serial link to ISP  
    ip address 208.10.2.137 255.255.255.248  
    ip access-group 107 in  
!  
! Enable Access Lists  
  ip access-group 107 in  
  ip access-group 101 out  
!  
! Improve security against smurf attacks and ad-hoc routing  
  no ip redirects  
  no ip directed-broadcast  
  no ip proxy-arp  
  no cdp enable  
  no mop enabled  
!  
  interface Ethernet0/0  
    description Link to firewall hosts
```

ip address 208.10.2.132 255.255.255.248

I will have to assume that the interface addresses are correct in his configuration, in the Security Architecture Audit the addresses are tested as configured in the router. While this was obviously a configuration error when setting up the ACL rules in the router this is what makes a hackers world go 'round.

This configuration allows an attacker to spoof the source address on packets and send TCP packets with a source address of the Ethernet interface on the router.

In an attack I would simply use a tool such as Nmap and spoof the source address to be 208.10.2.132 and send TCP SYN packets with a destination of 208.10.2.129. If I send these packets continuously I should be able to cause a flood of TCP syn/ack packets to bring down the router effectively causing a DOS.

#### 4.1.2 The Firewall

Stephen Monahan's network is running the Cisco PIX 515 firewall with version 5.2 software. A quick tour of Cisco's website revealed the following SSH vulnerability for the 515 running 5.2 software.

Four different Cisco product lines are susceptible to multiple vulnerabilities discovered in the Secure Shell (SSH) protocol version 1.5. These issues have been addressed, and fixes have been integrated into the Cisco products that support this protocol. This information can be found on Cisco's web site at - <http://www.cisco.com/warp/customer/770/nifrag.shtml>

By exploiting the weakness in the SSH protocol, it is possible to insert arbitrary commands into an established SSH session, collect information that may help in brute force key recovery, or brute force a session key.

- **CRC-32 integrity check vulnerability** -- By exploiting this protocol weakness, the attacker can insert arbitrary commands in the session after the session has been established.
- **Traffic analysis** -- This vulnerability exposes the exact lengths of the passwords used for login authentication. This is only applicable to an interactive session that is being established over the tunnel protected by SSH. This can significantly help an attacker in guessing the password using the brute force attack.
- **Key recovery in SSH protocol 1.5** -- This vulnerability may lead to the compromise of the session key. Once the session key is determined, the attacker can proceed to decrypt the stored session using any

implementation of the crypto algorithm used. This will reveal all information in an unencrypted form.

#### 4.1.3 The Attack

When exposed to an overly large packet, the SSH process will consume a large portion of the processor's instruction cycles, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device. The capability to create such a packet is available in publicly available exploit code. In some cases this availability attack may result in a reboot of the device. In order to be exposed SSH must be enabled on the device. By repeatedly exploiting this vulnerability an attacker can cause a denial of service.

The full description of this vulnerability can be found at - <http://packetstormsecurity.org/advisories/cisco/cisco.ssh.advisory.txt> and <http://www.kb.cert.org/vuls/id/290140>

Cisco describes it at - <http://www.cisco.com/warp/public/707/SSH-scanning.shtml>

There is a binary that can be found at- <http://packetstormsecurity.org/0204-exploits/x2.tgz>

This can be run to a device for this vulnerability. I do not have a Cisco PIX firewall to run this against but if I were to run it against the PIX in Steven Monahan's design I would run it against the outside interface of the firewall. Once the attack was started I would attempt to make an SSH connection to the PIX. If the attack were successful it could cause the PIX to crash and reboot as described above. Also if it were successful obviously I would not be able to connect.

There are fixes available in newer versions of Cisco IOS. The person maintaining the systems should keep abreast of the latest vulnerabilities and fixes and ensure their systems are secure against these attacks.

Through a process of experimentation I could attempt to run the following exploits as well.

The CRC-32 vulnerability can be exploited as follows - In order for this attack to succeed, an attacker must possess one or two known cipher text/plaintext pairs. This should not be difficult since every session starts with a greeting screen which is fixed and which can be determined. This also implies that an attacker must be somewhere along the session path in order to be able to sniff the session and collect corresponding cipher text.



The Traffic Analysis vulnerability can be exploited as follows - an attacker must be able to capture packets. When sending a packet using the SSH protocol, it is padded to the next 8-byte boundary, but the exact length of the data (without the padding) is sent unencrypted.

The timing between packets may yield additional information, such as the relative position of a letter on the keyboard, but that depends on overall jitter in the network and the typing habits of the person.

The Key Recovery in SSH protocol 1.5 lists the following means to exploit it - In order to exploit this vulnerability, an attacker must be able to sniff the SSH session and be able to establish a connection to the SSH server. In order to recover the server key, an attacker must perform an additional  $2^{20} + 2^{19} = 1572864$  connections. Since the key has a lifespan of about an hour, this means that an attacker must perform around 400 connections per second.

All three of these exploits require the attacker to have access to the outside network in order to place a sniffer on it.

## 4.2 Denial of Service Attack

### 4.2.1 The Attack

Using a network of 50 cable modems we will launch an attack against the GIAC web server in Stephen Monahan's network design. The attack will be a DRDoS (Distributed Reflection Denial of Service) attack using a tool called Orgasm v 1.0 which can be downloaded at <http://www.netsys.com/cgi-bin/listfiles.cgi?c=3>

This is a newer type of DDoS attack which utilizes internet servers and intermediate routers which respond to TCP SYN packets.

In this attack a hacker can use the Orgasm tool to send TCP SYN packets to devices on the internet. The packets have a spoofed ip address of the web server to be attacked. When the internet servers and intermediate routers receive the TCP SYN packet on an open port they respond with a TCP SYN/ACK packet destined for the server at the spoofed source address. If this attack is launched from hundreds of different servers the result is total bandwidth consumption on the internet connection to the target web server.

In our attack we will be targeting the GIAC web server. All 50 of our systems connected to cable modems will be configured with lists of valid servers which will be sent the TCP SYN packets. The servers and intermediate routers can be located by scanning for devices with open listening ports. For our attack we will

look for devices listening on ports 22, 23, 53, 80 and 179. Once we have the targets we will send the packets with a source address of the GIAC web server. The targets will respond to our TCP SYN packets with a SYN/ACK directed to GIAC's server. This will result in thousands of packets continuously sent to the GIAC server, effectively consuming all of the bandwidth on their connection to their ISP.

An excellent description of this attack type can be found at the following site:  
<http://grc.com/dos/drdo.htm>

#### 4.2.2 The Defense

The best source of information I've found on this attack is the paper listed above. Unfortunately there do not seem to be many countermeasures available today for this type of attack. The author had the following to say about a defense:

*Preventing reflection server exploitation*

*In theory, it's simple: The trick to doing this would be to recognize a SYN source IP that never completes its connections. Since a number of failed connections occurring within a short time span would be highly unusual, the target of any reflection attack could be readily determined. Dynamic reflection attack prevention would simply "black list" any SYN packets arriving from any such IPs until none had been received for some period of time, perhaps an hour.*

*A reflection server exploitation prevention system could be easily built into a server-resident firewall application. However, expecting (or relying upon) every server on the Internet to be running such an altruistic application is probably unrealistic. Asking, or*

*requiring, ISP's to provide spoofed packet network egress filtering would seem to be far more feasible . . .*

#### *The ISP's responsibility*

*The generation of traffic for a reflection attack depends upon source IP address spoofing. If ISPs would begin adopting the practice of preventing the escape of fraudulently addressed packets from within their controlled networks, this potent attack, and its many cousins, would die overnight. In addition to being the right thing to do by helping to prevent abuses by their customers upon those outside the network, egress filtering also enhances the security for an ISP's own customers because malicious hackers would soon learn that their spoofing attack tools would not function within an egress filtered ISP network.*

This presents a pretty unsettling picture, an attack with no current defense that a security administrator can set up to defend their site. Once the attack is recognized there are countermeasures that can be taken but the ISP is the one who will have to implement them.

### 4.3 DNS Server Attack

This network design doesn't specify their design for the DNS server so I can't address specific issues but if the design isn't mindful of these types of vulnerabilities they leave themselves open to this type of DoS attack.

DNS servers running earlier versions of BIND would cache convoluted information when DNS recursion was enabled on the server. Recursion allows DNS name servers to service requests for domains and/or zones it does not serve. When a DNS name server receives a request for a zone it does not service it will forward the request to the authoritative name server. When it receives a response it will send it to the requesting name server.

If recursion is enabled on a name server running a vulnerable version of BIND an attacker can poison the cache of the name server performing the lookup.

Should an attacker successfully poison the cache of a name server the affected server would provide incorrect ip addresses to other servers using its service. The attacker could in effect redirect name lookups to a bogus ip address for the server being looked up, this would be an effective DoS. Users looking for abc.com would be told to use ip address 10.10.10.10 rather than abc.com's legitimate ip address. The web server for abc.com obviously would never be found at this bogus ip address so users could not access the site.\

There are much more current versions of BIND and if they can be run on your server they obviously should be. Newer versions are available for download at <http://www.isc.org/products/BIND/> along with a more secure version of 4.x.x should it need to be used.

Descriptions of this and other BIND vulnerabilities can be found at <http://www.isc.org/products/BIND/bind-security.html>

## 4.4 Internal Systems Compromise

### 4.4.1 Attack by Social Engineering

No matter how well a company protects the perimeter of their network if they neglect to guard against Social Engineering they are vulnerable.

We will do two things to attempt to attack GIAC. There was no mention of virus filtering software for their mail server so we attempt to exploit this vulnerability.

First using a tool such as Sam Spade we'll scan their website for email addresses. We'll also try to gather names and phone numbers from the website. Figure 4.1 shows an example of the information found using the Sam Spade tool and crawling a website looking for email addresses.

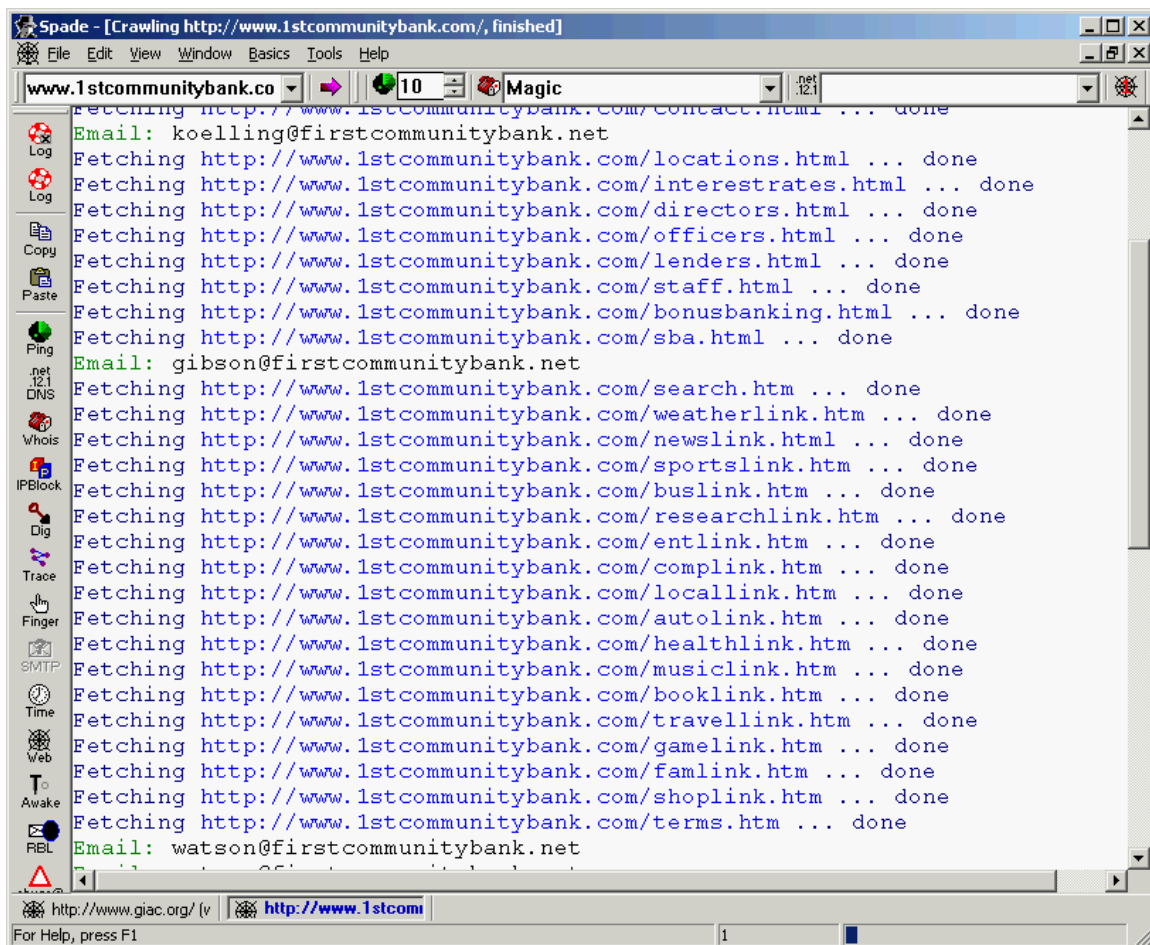


Figure 4.1

Once we have names and phone numbers we'll call some of the individuals and establish a relationship based on a business trust.

In our example we'll tell them something like we are interested in becoming a supplier of fortune cookie sayings but we don't know if our sayings are good enough for their company. We tell them we know the company president and she suggested we talk to this targeted individual and have them review some of our sayings to use their "superior judgement" (flattery will get you somewhere) to determine the quality of our sayings. If we get them to agree to review our sayings would suggest that we email them a list for their review.

Based on the format of email addresses we've discovered on their website we can probably guess their email address. This will lend an extra sense of trust to our new relationship if we tell them the president gave us this address when we discussed this with her. We'll tell the employee that we will send an email with an attachment, all they need to do is open the attachment and they will be able to view our list.

The attachment of course is not really just a list of cookie sayings, it's a Trojan for a virus. An example of a Trojan we might use is the Trojan.Idly, it is a Trojan that attempts to gather system information, including your dial-up networking user name and passwords, and send them to the hacker.

Information on the Trojan.Idly can be found on Symantec's website at <http://securityresponse.symantec.com/avcenter/venc/data/trojan.idly.html>

The dial-up networking and user name and password would allow us access to the network. At a later time we could use the information to dial into the GIAC network and have their user level access to the network. This type of attack could have devastating consequences.

#### 4.4.2 Protecting Against

The obvious defenses against this attack would be first to have a good antivirus program running on the mail system to guard against known email viruses and Trojans. Second, educate your users. Under no circumstances should they be opening attachments unless they are from known sources. This is difficult to avoid as social engineering can be a pretty effective tool against employees.

A company should avoid posting telephone numbers for individual employees on their website. It is best to post only main phone numbers and department phone numbers. Also avoid posting individual email addresses on the website, use only general email addresses when it's necessary to post email addresses. The most common email address format today is first name.last name@company name.com or first initial.last name. While it may be convenient for employees to remember this email address it is also very easy to guess. As a rule it may be advisable to devise a more secure format for email addresses.

#### 4.4.3 Additional Attacks

Using a tool such as SuperScan a person can run port scans on a specific ip address or domain name. If I run the tool on GIAC.com one of the open ports I find is the SMTP port 25. See Figure 4.1

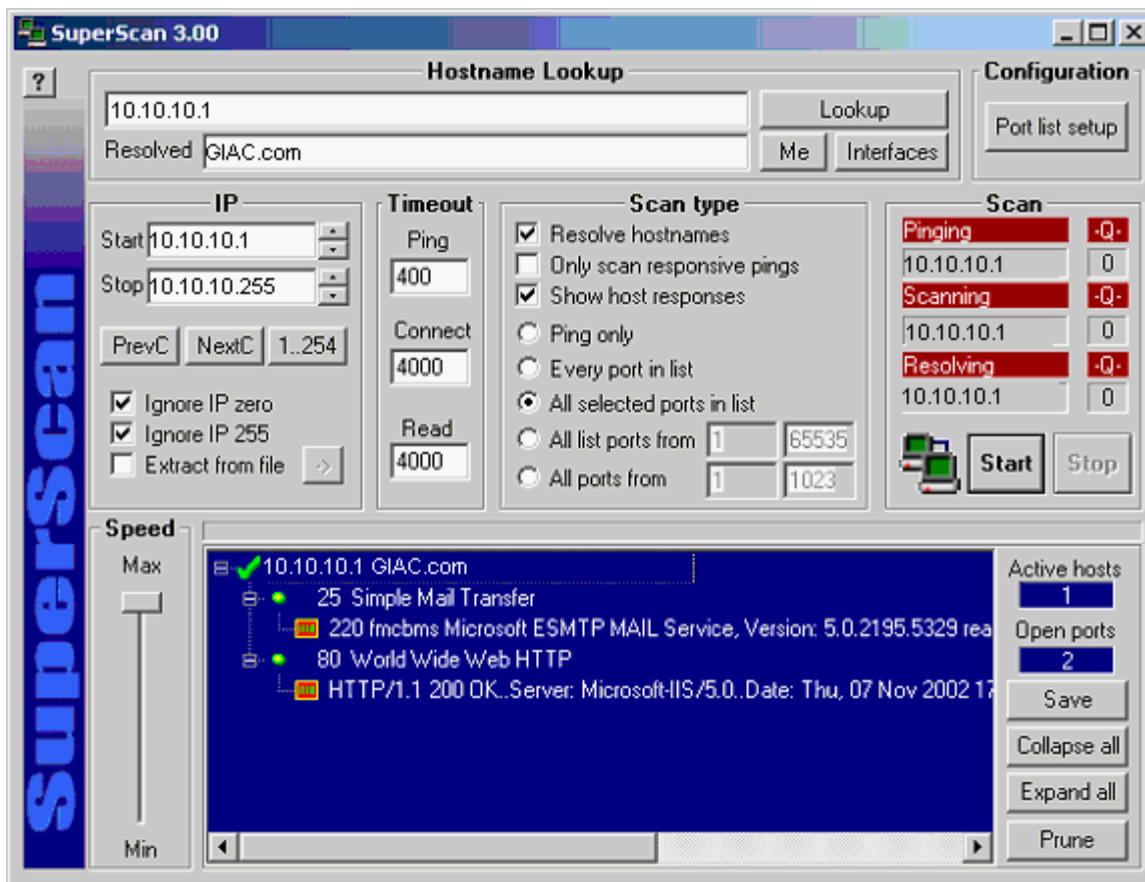


Figure 3.1

Knowing that port 25 is listening I have decided to find out if this mail server is set up for mail relay. If it is I can use it to relay “junk” mail to various mail accounts at major corporations. If I relay enough of this junk mail the recipient corporations will likely eventually block all mail sent from the offending mail server. This would cause mail from all accounts at GIAC.com to be rejected by many of the businesses I have targeted. While this wouldn’t disrupt the business of GIAC initially, over time it could have a substantial impact on their ability to do business since email is critical in today’s e-economy.

A tool that can be useful in assisting you to find legitimate email addresses at a domain is the Sam Spade tool, Figure 4.2. By using its web crawl function I can specify email addresses and find legitimate email addresses at a web site. Once I have the output I can use these addresses to send junk mail to.



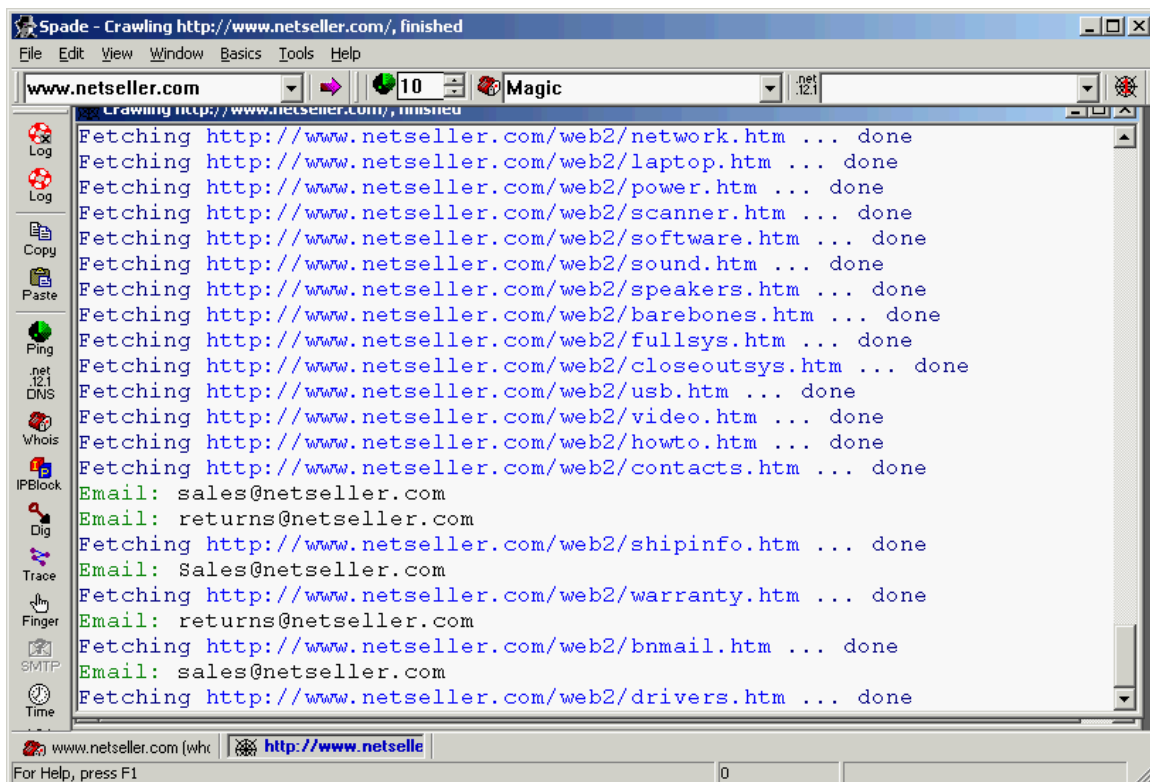


Figure 4.2

In order to find out if this mail server will allow mail relay I will perform the following steps.

#### telnet mail.giac.com 25

Trying 10.10.10.1...

Connected to giac.com.

Escape character is '^['.

220 giac.com ESMTP Mon, 6 Jan 2003

20:48:46 -0600 (MDT)

#### helo mjk.com

250 fw.mjk.com Hello Riverside.MR.Net

[137.192.2.5], pleased to meet you

#### mail from:test@hp.com

250 test@hp.com... Sender ok

#### rcpt to:joe@aol.com

550 joe@aol.com... Sender ok

#### quit

In the case above the mail server will relay mail so I can go ahead and use their mail server to relay the offending mail.



Spammers use this relay method to hide their own addresses from recipients to avoid having their mail blocked.

## References

SonicWall online documentation

<ftp://ftp.sonicwall.com/pub/info/ikeadvanced.pdf>

<ftp://ftp.sonicwall.com/pub/info/ikeadvanced.pdf>

<ftp://ftp.sonicwall.com/pub/info/ikesimple.pdf>

NSA/CSS Infosec web site documentation

Cisco router guides – Router security configuration guide

Cisco product documentation CD and online documentation

Insecure.org website for Nmap software and documentation

[http://www.insecure.org/nmap/nmap\\_documentation.html](http://www.insecure.org/nmap/nmap_documentation.html)

Bugtraq online vulnerabilities lists

<http://online.securityfocus.com/bid>

© SANS Institute 2003, Author retains full rights.