



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 (GCFW) Practical Assignment

Version 1.7 Online

Tony Enriquez

September 4, 2002

© SANS Institute 2000 - 2002, Author retains full rights.

TABLE OF CONTENTS

Assignment 1: Security Architecture	4
1.1 Introduction.....	4
1.2 Business Requirements	4
1.2.1 Customers	4
1.2.2 Suppliers.....	4
1.2.3 Partners	4
1.2.4 Local Employees	5
1.2.5 Remote Employees	5
1.3 Network Components.....	5
1.3.1 Border Router	6
1.3.2 Primary Firewall.....	6
1.3.3 Network Intrusion Detection.....	7
1.3.4 Time Synchronization	8
1.3.5 Service Network	8
1.3.6 Internal Network	8
Assignment 2: Security Policy and Tutorial	9
2.1 Border Router Configuration	9
2.2 Firewall Configuration	13
2.2.1 Definitions.....	13
2.2.2 Firewall Rule Base.....	14
2.2.3 Syslog Server	16
2.2.4 DNS Proxy Configuration.....	18
2.2.5 Mail Proxy.....	20
2.3 VPN Tutorial	21
2.3.1 Gateway Configuration	22
2.3.2 Exporting Certificate	27
2.3.3 Transferring CERT's	27
2.3.4 IPSEC Policy	28
2.3.5 IPSec Settings.....	29
2.3.6 Configuring an IPSec VPN Connection	30
2.3.7 Packet Filter Rule	32
2.3.8 Laptop Computer Setup	32
2.3.9 Verify Outbound Traffic from Laptop.....	41
2.3.10 Setup Sniffer.....	41
2.3.11 Generate Traffic from Laptop1.....	41
2.3.12 Analyze Traffic.....	41
Assignment 3: Verify Firewall.....	43
3.1 Plan the Audit	43
3.1.1 Ruleset Audit.....	43

3.1.2	Vulnerability Scan.....	45
3.1.3	Verify VPN Connection.....	46
3.1.4	Cost.....	46
3.2	Perform Audit.....	46
3.2.1	Run Nmap Scans	46
3.2.2	Rule Analysis.....	47
3.2.3	Run Nessus Scan.....	49
3.2.4	Verify VPN.....	51
3.2.5	Results.....	51
3.3	Recommendations	51
3.4	Overall	52
Assignment 4: Design Under Fire		53
4.1	Overview.....	53
4.2	Firewall Attack	54
4.3	Distributed Denial of Service Attack.....	56
4.3.1	Countermeasures	58
4.4	Internal System Attack.....	58
4.4.1	Finding a Target	58
4.4.2	Countermeasures	59
References		60
Tools		62

Assignment 1: Security Architecture

1.1 Introduction

GIAC Enterprises is a family-owned and operated start-up company selling customized fortune cookie sayings to event planners, party coordinators, caterers, and pastry chefs who concentrate on high-end weddings, parties, and special occasions. The customers customize the fortune cookie sayings to suit a particular occasion and order them via a secure, e-commerce website.

GIAC is comprised of five full-time staff members working from a small office and various remote sites when they travel. GIAC outsource their sales and marketing efforts to a mobile sales force located in another state. The primary focus of the sales force is to create online advertising and marketing campaigns to drive customers to the GIAC website to purchase products. GIAC has partnered with several international companies to translate and sell the fortunes to their designated regions.

1.2 Business Requirements

1.2.1 Customers

Customers can access the GIAC website via a web browser. The web portal uses an OpenSSL-enabled Apache web server that is connected to a web-enabled MySQL database. This configuration allows the customer to view samples, create accounts, purchase fortunes, and download fortunes.

When customers are ready to purchase products online, they can access the order form on the website via Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), 128-bit encryption to place an order with a credit card. Those prospective customers trying to connect with web browsers using 40-bit encryption will be unable to use the secure site and will be prompted to contact GIAC via email to use a different purchasing option. Upon placing an online order, customers will be notified by email to verify online purchases. Email also will provide a means to directly contact the company.

1.2.2 Suppliers

Suppliers will be allowed access into the GIAC website using a web browser to access the web-enabled MySQL database so that they can view all account information, access the fortunes database, and submit fortunes as they are completed. All supplier web browsers must support 128-bit encryption.

1.2.3 Partners

GIAC has existing partnerships with several international companies. Each company is responsible for translating and selling the fortunes for their region. GIAC will provide Virtual Private Network (VPN) connections that allow partners limited access to retrieve fortunes for translation and deposit new fortunes from the MySQL database. VPN connections are Net-to-Net and Host-to-Gateway.

Host-to-Gateway connections will utilize the Secure Shell (SSH) Sentinel Virtual Private Network (VPN) client. Authentication will be done with X.509 certificates.

1.2.4 Local Employees

GIAC employees are permitted access for web, email, and file transfer protocol (FTP) services thereby providing the employees with the resources needed to accomplish their work requirements.

Through the use of a Hypertext Transfer Protocol Overview (HTPP) proxy, GIAC has the capability to restrict certain websites and track web traffic as required. Each GIAC employee signs a disclaimer that notifies them that all network traffic is subject to monitoring.

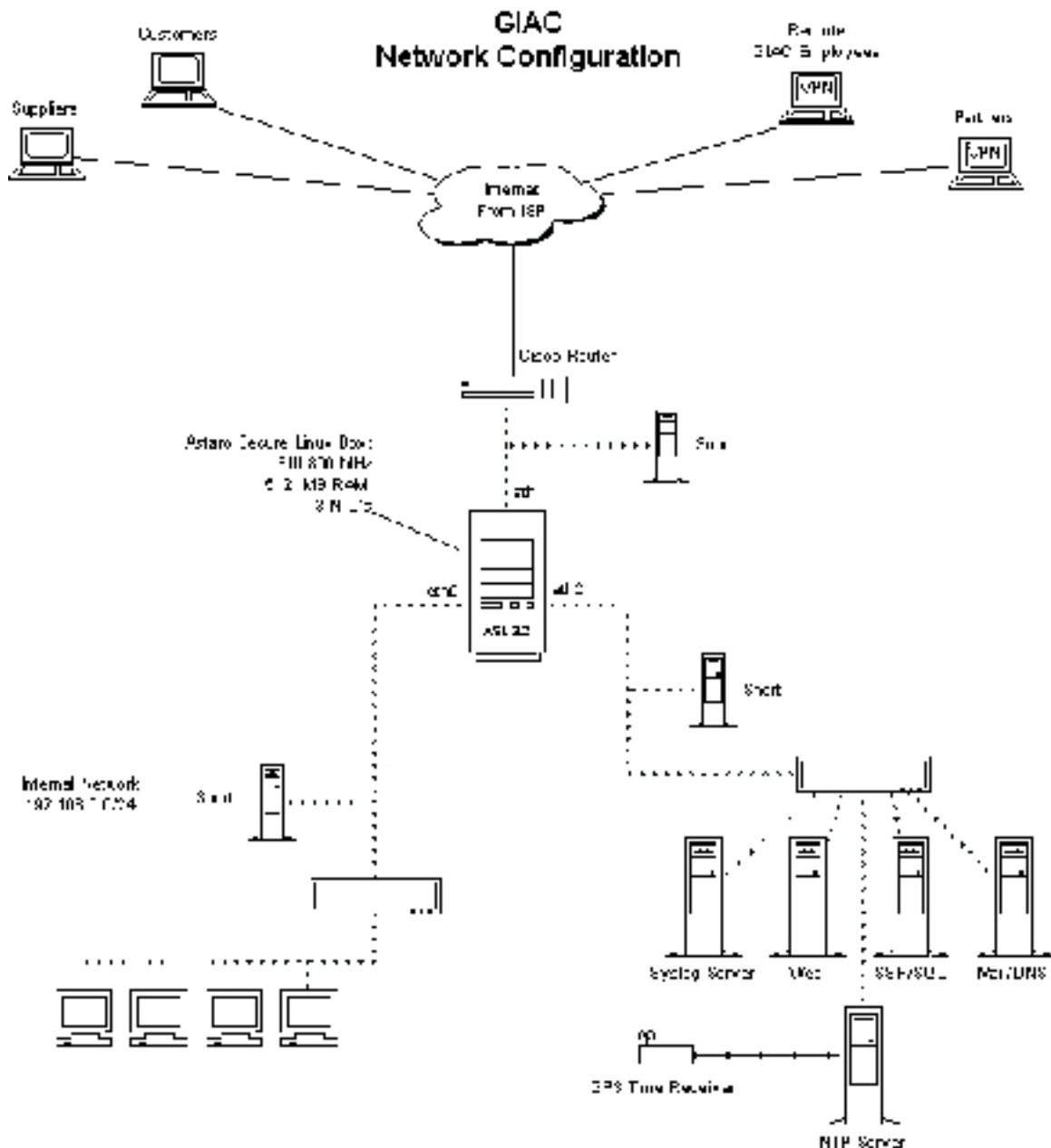
Local employees are also allowed access to the production servers located in the service network via SSH. This allows employees to service the fortune and sales databases.

1.2.5 Remote Employees

Remote GIAC employees will have network access via the VPN, which provides the remote user the same access as local employees, if granted. Each VPN user profile will grant certain network privileges. Host-to-Gateway connections will be authenticated with self-signed X.509 certificates. Employee laptops will have dial-up capabilities from a major Internet service provider (ISP). Connections will be made via the SSH Sentinel VPN Client.

1.3 Network Components

We have allocated money to the purchase the following network components. Since this is a start-up company, the majority of the budget is allocated for marketing efforts to promote product awareness and create a customer base. Additional money will be budgeted for future network upgrades as funds become available.



1.3.1 Border Router

The border router will be a Cisco 2651XM-2FE/VPN/K9 running Cisco IOS 12.2. We chose this device because of Cisco's long history of customer support as well as the network administrator's familiarity with Cisco equipment. The router also has firewall and VPN capabilities should the main firewall/VPN equipment go down.

1.3.2 Primary Firewall

The primary firewall will be the Astaro Security Linux 3.2. According to the company's website, this is ASL is "an integrated software solution that provides

superior performance in an all-in-one Firewall. Its hardened operating system, stateful packet inspection, content filtering (virus & surf protection), application proxies and IPsec based VPN provides a powerful solution to today's security issues" (Securing). Its affordable price and modest hardware requirement made this firewall product an easy choice. The latest version available at this time is ASL 3.208.

Another factor in choosing ASL is the administrator's experience with Linux. The WebAdmin interface will enable quick and easy implementation of GIAC's network policy. The ASL box will segment the traffic between the Internet, the service network, and the internal local area network (LAN). It will also serve as the gateway for VPN connections. GIAC's initial ASL will have the following capabilities:

- Firewall
- Application Gateway
- VPN Gateway
- Quality of Service
- Max. 3 NICs
- 5 Email Domains
- 10 VPN tunnels
- Max. 25 IP's (IP count includes all devices - static, dynamic, through NAT, plus number of hosted domains for ISPs)

Astaro Security Linux License Fee:	
With Up2Date Service incl. for one year	\$750.00
Virus Protection License Fee for one year	\$495.00
PIII 800MHz 512 MB RAM 3 NIC's	<u>\$400.00</u>
Total for Firewall	\$1645.00

We opted not to spend \$550.00 for the Surf Protection. At this time, banned sites can be programmed into the Linux snort boxes and alerts sent to the root account on the same boxes. Should the business expand, ASL services can be upgraded.

The ASL has two VPN options: Internet Protocol Security (IPSec) and Point-to-Point Tunneling Protocol (PPTP). GIAC will be utilizing the IPSec VPN. IPSec was chosen due to inherent security flaws associated with PPTP.

1.3.3 Network Intrusion Detection

Three Linux snort boxes will be used for intrusion detection. One will be located between the router and firewall. Another will be located with the service network, and the last snort box will be located on the internal network. All snort boxes have been configured with ACID, MySQL, and Apache with OpenSSL, using a one way cable tap. All alerts will be monitored from the web interface, with major alerts triggering email notification to the appropriate local user account.

1.3.4 Time Synchronization

Fortunately, the owner of the company owns a GPS time receiver. The output of the GPS unit is routed via RS-232 cable to the computer configured to be the Network Time Protocol (NTP) server.

1.3.5 Service Network

The service Network will contain the GIAC servers that have public access. The service network is reachable from the Internet on the required services, or from the internal LAN using SSH. All outbound connections initiated from the service network will be rejected and logged.

1.3.6 Internal Network

The internal network will be comprised of network devices using IP Masquerade (IPMASQ). This allows GIAC to network the internal machines and not use any allocated IP address space from the ISP. A proxy service will be enabled for HTTP, HTTPS, domain name system (DNS), and SMTP, simple mail transfer protocol client.

© SANS Institute 2000 - 2002, Author retains full rights.

Assignment 2: Security Policy and Tutorial

2.1 Border Router Configuration

The border router is the first line of defense for the GIAC network. The router will be configured to prevent unwanted packets entering and exiting the GIAC network. These basic ingress and egress filters are part of the defense to improve network security. If packets should get by the router, the firewall will filter out any unwanted traffic.

Since the router is the first appearance point in the Internet, it's important to take steps to "harden" the router. The first step will be to disable services not used to operate the router or provide information to hackers. According to the National Security Agency's (NSA) Router Security Configuration Guide, even though the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) protocol standards include a recommended list of simple services that hosts should provide, there is no reason to run them and they should be disabled (Antoine 62). We have no reason to run TCP or UDP small servers and will disable them:

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

HTTP service enables the web-based remote management of routers and is another service that could potentially be exploited or used by unauthorized personnel. Therefore, we will also disable the server:

```
no ip http server
```

We will not be utilizing BOOTP, so we will disable it:

```
no ip bootp server
```

According to NSA's Router Security Configuration Guide, "...the IOS finger server supports the Unix 'finger' protocol, which is used for querying a host about its logged in users. On a Cisco router, the **show users** command may be used to list the logged in users" (Antoine 63). Since we do not want unauthorized users to know who is logged in to the router, we will disable the IOS finger server:

```
no service finger
```

The Cisco Discovery Protocol is a service that allows Cisco devices to identify each other on a LAN. We are not utilizing CDP, so we will disable it:

```
no cdp run
```

The Simple Network Management Protocol allows remote network administration. Since we are not using SNMP, we should disable the server and prevent SNMP packets from coming into our network:

```
no snmp server
deny udp any any eq snmp log
deny udp any any eq snmptrap log
```

Next, we want to block private networks and traffic originating from the loopback address. Traffic originating from these ranges indicates possible spoofing.

```
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 127.0.0.0 0.255.255.255 any log
deny ip 169.254.0.0 0.0.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any log
```

GIAC will not be utilizing multicast traffic, so we'll block it at the router:

```
deny ip 224.0.0.0 15.255.255.255 any
```

Class E is experimental. We are not expecting traffic from this range, so we should block it:

```
deny ip 240.0.0.0 15.255.255.255 any
```

Source routed packets allow the packet to use a defined route instead of utilizing the path recommended by intermediary routers. These packets seldom have a legitimate purpose and will be blocked:

```
no ip source-route
```

0.0.0.0 is not a valid IP address and should be blocked:

```
deny ip 0.0.0.0 0.255.255.255 any
```

Traffic that has the source IP address range of GIAC will be blocked. This would indicate that someone has spoofed our IP address. We will want to log the error as well.

```
deny ip 65.210.19.0 0.0.0.127 any log
```

The Land Attack may cause a denial of service or degraded capability in the router by sending a packet to the router with the same IP address in the source address and destination address fields, and with the same port number in the source port and destination port fields (Antoine 79). These DOS attacks on the router interfaces can be stopped by the following:

```
deny ip host 65.210.19.1 host 65.210.19.1 log
```

We also want to prevent a Smurf Attack, which involves sending a large amount of Internet Control Message Protocol (ICMP) Echo packets to a subnet's broadcast address with a spoofed source IP address from that subnet. According to NSA guidelines, if a router is positioned to forward broadcast requests to other

routers on the protected network, then the router should be configured to prevent this forwarding from occurring (Antoine 79). This blocking can be achieved by denying any packets destined for broadcast addresses:

```
deny ip any host 65.210.19.255 log
deny ip any host 65.210.19.0 log
```

The next step will be to harden the router against possible attacks from a variety of ICMP message types, some of which are associated with programs. For example, the ping program works with message types Echo and Echo Reply. An attacker can create a map of the subnets and hosts behind the route with Echo packets or perform a denial of service attack by flooding the router or internal hosts with Echo packets. Furthermore, an attacker can cause changes to a host's routing tables using ICMP Redirect packets (Antoine 79-80). To avoid such attacks, we will block the message types Echo and Redirect for inbound ICMP traffic. Otherwise, the other ICMP message types should be allowed inbound.

```
deny icmp any any echo log
deny icmp any any redirect log
deny icmp any any mask-request log
permit icmp any 65.210.19.0 0.0.0.255
```

With the advent of high-profile distributed denial of service (DDoS) attacks in recent times, which routers cannot prevent in general, it is usually sound security practice to discourage the activities of specific DDoS agents (i.e., zombies). We will do this by adding access list rules that block their particular ports. The example below shows access list rules for blocking several popular DDoS attack tools. [Note: The NSA Configuration Guide says that some of these rules may also impose a slight impact on normal users because they block high-numbered ports that legitimate network clients may randomly select. Therefore, you may choose to apply these rules only when an attack has been detected. Otherwise, these rules would normally be applied to traffic in both directions between an internal or trusted network and an untrusted network (Antoine 82).]

```
! the TRINOO DDoS systems
deny tcp any any eq 27665 log
deny udp any any eq 31335 log
deny udp any any eq 27444 log
! the Stacheldraht DDoS system
deny tcp any any eq 16660 log
deny tcp any any eq 65000 log
! the TrinityV3 system
deny tcp any any eq 33270 log
deny tcp any any eq 39168 log
! the Subseven DDoS system and some variants
deny tcp any any range 6711 6712 log
deny tcp any any eq 6776 log
deny tcp any any eq 6669 log
deny tcp any any eq 2222 log
deny tcp any any eq 7000 log
```

When an event is "logged," it's needs to be seen by the network administrator. A common practice is to send the router logs to a central syslog server. NSA guidelines state, "There are four things that you must set for syslog logging: the destination host or hosts, the log severity level, the syslog facility, and the source interface for the messages" (Antoine 111). First, we will set the severity level for messages sent to the syslog server. Next, set the destination host (syslog server). Finally, we configure the router to identify messages from router as "local0" at the syslog server and identify which interface that the router uses to forward the syslog messages. Note: Typically, it's the closest interface to the syslog server and Eth0 is the internal GIAC interface.

```
giac-router(config)# logging trap information
giac-router(config)# logging 65.210.19.13
giac-router(config)# logging facility local0
giac-router(config)# logging source-interface eth 0/0
```

Time syncing network devices is a common practice. This becomes extremely important when tracing log entries from device to device. Should the logs become evidence for forensic analysis, the time synchronization becomes extremely important. The GIAC router is configured to use the firewall as the time server. The firewall uses the Naval Observatory Time Server in WDC, and serves NTP to the rest of the network.

```
giac-router(config)# interface eth 0/0
giac-router(config-if)# no ntp disable
giac-router(config-if)# exit
giac-router(config)# ntp server 65.210.19.3 source eth 0/0
giac-router(config)# exit
```

Next, we need to set up the ingress filtering rules. We could block all reserved Internet Assigned Numbers Authority (IANA) and unused networks. However, as IP address space shrinks, the reserved networks have the possibility of being used. For a business, we would be blocking potential customers from accessing our web site. Unless we can monitor all of the block allocations, we might inadvertently block prospective customers. To permit traffic bound only for the GIAC network, the following rule will be applied:

```
permit ip any 65.210.19.0 0.0.0.127
```

Finally, we will set the egress filtering so that only traffic with valid source addresses are allowed to leave the router. This will prevent "spoofed" packets from leaving the router to avoid participating in denial-of-service attacks.

```
ip access-list extended outbound
permit ip 65.210.19.0 0.0.0.127 any
deny ip any any log
```

2.2 Firewall Configuration

The default firewall settings for the ASL firewall should be modified to prevent unauthorized access to the WebAdmin Interface. The default setting is “ANY”, which means any interface can gain access to the WebAdmin Interface. This setting can be changed at the System Settings page. (Refer to Figure 1.) We changed it to have access from the Admin PC only, with the listed users having access to the WebAdmin Interface. Should the need arise to remotely administer the firewall, we could reconfigure that from here. We will disable the “admin” WebAdmin account once the firewall is installed.

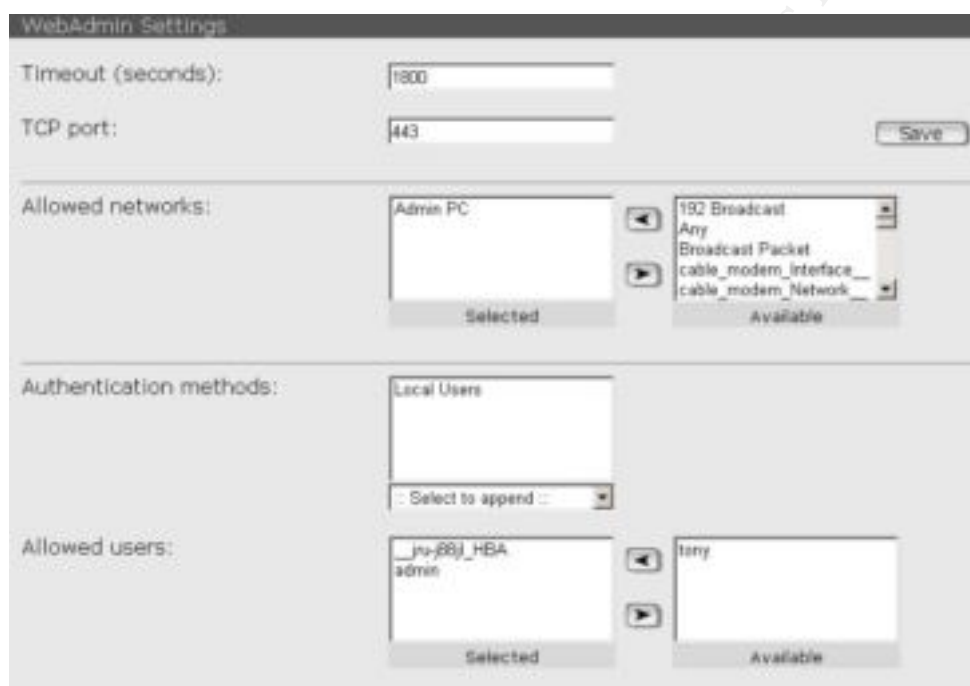


Fig. 1

Other than the WebAdmin setting, everything is dropped and sent to the Filter Live Log. From here, we must explicitly allow the required services for use at GIAC. The rules will be based on GIAC policies and network /service definitions configured in the ASL software.

2.2.1 Definitions

To use the packet Filter GUI, we must define the network devices rules. You can define networks ranges, individual devices, and network groups. Figure 2 is an example of how a network device could be defined:

Help network

Name: IP address: Subnet mask:

Hint: to create a host entry, use the subnet mask 255.255.255.255 (or /32)

Fig. 2

This process is repeated until all networks and network devices are configured.

This process also is used to define network services that are not present in the default services list. For example, ESP packets are not part of the default services list. In order for remote users and partners to “VPN” in, this service has to be defined:

Name	Protocol	SPI:	Command
VPN	esp	25614294967295	edit del

Fig. 3

Note: the ISAKAMP service is defined by default. The Astaro help screen explains:

For AHA and ESP, the SPI is a value between 256 and 4294967295 which has been mutually agreed upon by the communication partners. Values below 256 have been reserved by the Internet Assigned Numbers Authority (IANA). (Astaro Online Help: Services)

2.2.2 Firewall Rule Base

Our first set of rules will enable prospective customers, suppliers, and partners access to the web and email servers. (See Figure 4.) Note that this rule enables “from any”. This rule also enables GIAC employees to service those particular servers located in the service network from the internal LAN.

No.	From (Client)	Service	To (Server)	Action	Command
1	Any	HTTP	Web Server	Allow	edit del move
2	Any	HTTPS	Web Server	Allow	edit del move
3	Any	SMTP	Mail Server	Allow	edit del move

Fig. 4

Another requirement of the GIAC LAN is to provide internal users access to HTTP, HTTPS, and FTP. They also need SSH access to the service network. The following rules will provide those services:

6	LAN	FTP	Any	Allow	edit del move
7	LAN	FTP-CONTROL	Any	Allow	edit del move
8	LAN	SSH	Service_Network	Allow	edit del move

Fig. 5

A rule for internal LAN access for HTTP and HTTPS is not needed if the built-in proxy service is used. The ASL firewall provides HTTP proxy services to curtail certain web traffic as explained in the following text from the online help screen:

The **Mode** setting determines the basic operation mode of the HTTP proxy:

In **Standard** mode, the proxy will listen for client requests on port 8080 and will allow any client from the networks listed in **Allowed Networks** to connect. When you use this mode, clients must enter the proxy in their browser configuration.

In **Transparent** mode, the proxy will handle all traffic passing the firewall on port 80. In this mode, the clients do not need to enter the proxy in their browser configuration. Please note that the proxy cannot handle FTP and HTTPS (secure) requests in this mode. If your clients want to access such services, you must open the respective ports (21 and 443) in the packet filter. (Astaro Online Help: HTTP Proxy)

The standard mode will be enabled, and all clients will be configured to use the HTTP proxy for HTTP and HTTPS.

Next, we need to set the Log Level. The online help screen explains the options:

The **Log Level** setting lets you configure the amount of information logged by the proxy. The following settings are available:

- **Full:** Everything is logged, including proxy status data
- **Access Log only:** Only usage data, like accessed URLs, usernames and client IPs are logged
- **None:** No logging is done at all. If you select this option, the reporting function for the HTTP proxy will not produce any output. (Astaro Online Help: HTTP Proxy)

We will set the Log Level to “Full” to enables GIAC to audit web traffic, if required. The Anonymity option will be set to “None”. The Standard and Paranoid options restrict cookies. Internal GIAC users find this too restricting. If needed, GIAC can always switch to another anonymity option that is more restrictive.



Fig. 6

The Content Filter can filter the following web traffic listed in Figure 7. The online help screen details what these filters actually block:

- **Javascript:** this will block Javascript globally, by removing all tags from the HTML code.
- **Cookies:** this option will block Cookies set by websites to "remember" certain clients.
- **Embedded:** This option will remove EMBED and OBJECT tags, thus removing things like Java Applets, ActiveX controls and the like.
- **Web Bugs:** These are small, invisible GIF images used to track users across sites. (Astaro Online Help: HTTP Proxy)

After the firewall was installed, all of the filter options were selected. As users complained, the appropriate filter was disabled. No one has made a complaint since the first three were disabled.

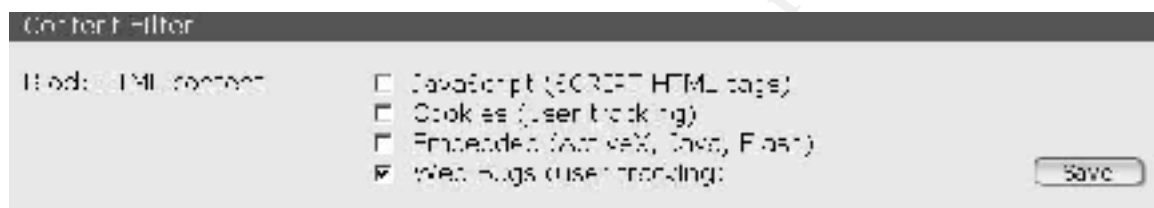


Fig. 7

Finally, we need to define the firewall rule set to allow in-bound and out-bound VPN connections as shown in Figure 8. Specific VPN configuration will be covered later in the tutorial.

4	Any	ISAKMP	Any	Allow	edit del move
5	Any	VPN	Any	Allow	edit del move

Fig. 8

2.2.3 Syslog Server

The production servers and border router send all the logs to the syslog server that is located in the service network. Should the router and firewall be compromised, the syslog server will be at risk as well. In order to protect the syslog server, a one-way cable tap was utilized. The tap enables the syslog server to receive traffic and be inaccessible at the same time. The model for this cable tap was found online (Ng). This means that the syslog server will require constant manual monitoring. The firewall will also be configured to send its logs to the same server. Figure 9 depicts the firewall and router rules configured to use the syslog server located in the service network. The configurations we made are shown in Figure 10.

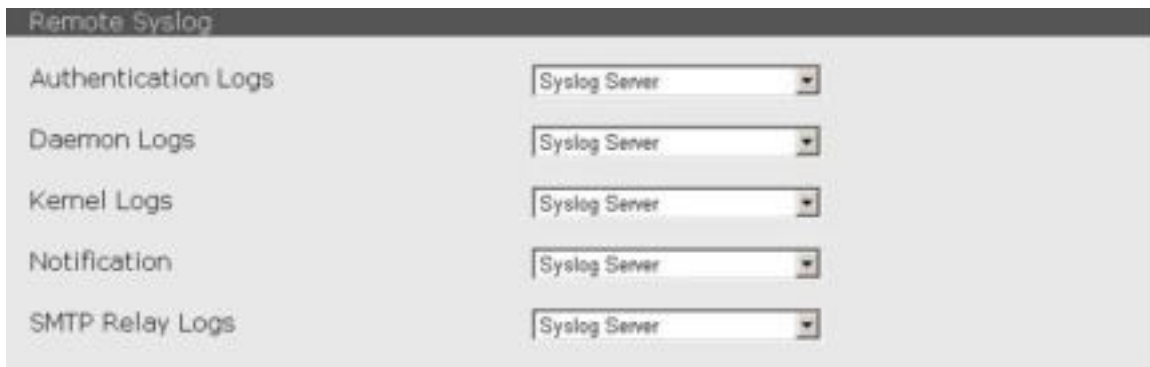


Fig. 9



Fig. 10

The next rule will reject and *not* log network basic input/output system (NetBIOS) and server message block protocol (SMB) traffic. Rejecting and not logging these packets will save CPU resources and storage space on the firewall. The default is drop and log unless explicitly allowed.

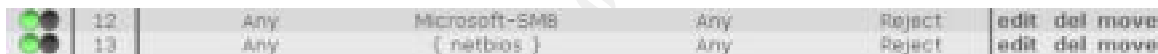


Fig. 11

The NetBIOS group is a pre-configured service group that contains:

netbios-dgm	tcp/udp	138	138	static
netbios-ns	tcp/udp	137	137	static
netbios-ssn	tcp/udp	1024:65535	139	static

Fig. 12

Microsoft-SMB service is defined as:

Microsoft-SMB	tcp/udp	1:65535	445	static
---------------	---------	---------	-----	---------------

Fig. 13

IDENT is commonly requested by the remote mail servers. We set the next rule to reject the IDENT request instead of dropping it (see Figure 14). According to SANS material, this rule "...takes care of IDENT by rejecting connections to the mail server rather than dropping them so the remote mail system can quickly figure out we don't support IDENT and accept our email message" (Building a Rule Base, 88).

	15	Any	IDENT	Any	Reject	edit del move
---	----	-----	-------	-----	--------	---------------

Fig. 14

The next two rules will drop and *not* log IP broadcast packets at all firewall interfaces:


	14	Any	Any	Broadcast32	Drop	edit del move
	15	Any	Any	Broadcast8	Drop	edit del move

Fig. 15

Next, we will define Broadcast 32 and Broadcast 8:

Broadcast32	255.255.255.255	255.255.255.255	edit del
Broadcast8	192.168.0.255	255.255.255.255	edit del

Fig. 16

The last rule will reject and log any connection attempts originating from the service network (see Figure 17). It's important to point out that the log entries will show that the packet was dropped but will reject the packet and not drop it:

	18	Service_Network	Any	Any	Log Reject	edit del move
---	----	-----------------	-----	-----	------------	---------------

Fig. 17

The final firewall configuration is shown in Figure 18. The logs are monitored to optimize the rules order and rearrange, if necessary.

No.	From (Client)	Service	To (Server)	Action	Command
1	Any	HTTP	Web Server	Allow	edit del move
2	Any	HTTPS	Web Server	Allow	edit del move
3	Any	DNS	Ext DNS	Allow	edit del move
4	Any	SMTP	Mail Server	Allow	edit del move
5	LAN	FTP	Any	Allow	edit del move
6	LAN	FTP-CONTROL	Any	Allow	edit del move
7	LAN	SSH	Service_Network	Allow	edit del move
8	Any	ISAKMP	Any	Allow	edit del move
9	Any	VPN	Any	Allow	edit del move
10	router	SYSLOG	Syslog Server	Allow	edit del move
11	Any	Microsoft-SMB	Any	Reject	edit del move
12	Any	[netbios]	Any	Reject	edit del move
13	Any	IDENT	Any	Reject	edit del move
14	Any	Any	Broadcast32	Drop	edit del move
15	Any	Any	Broadcast8	Drop	edit del move
16	Service_Network	Any	Any	Log Reject	edit del move

Fig. 18

2.2.4 DNS Proxy Configuration

GIAC will be using a DNS proxy configuration. The external DNS server located in the service network will enable Internet users to locate our web and email servers. The external DNS server also allows our mail server to verify other mail servers. The internal LAN will use the ASL DNS proxy utilizing the external DNS

server. The DNS proxy is configured so only the internal LAN can use the DNS proxy. The proxy is configured to query the GIAC domain DNS server and the ISP DNS server. Zone transfers from the Internet will not be allowed to the GIAC DNS server unless specified in the `/etc/named.conf` file.

Figure 19 illustrates the configuration on a host from the internal LAN using the ASL DNS proxy:

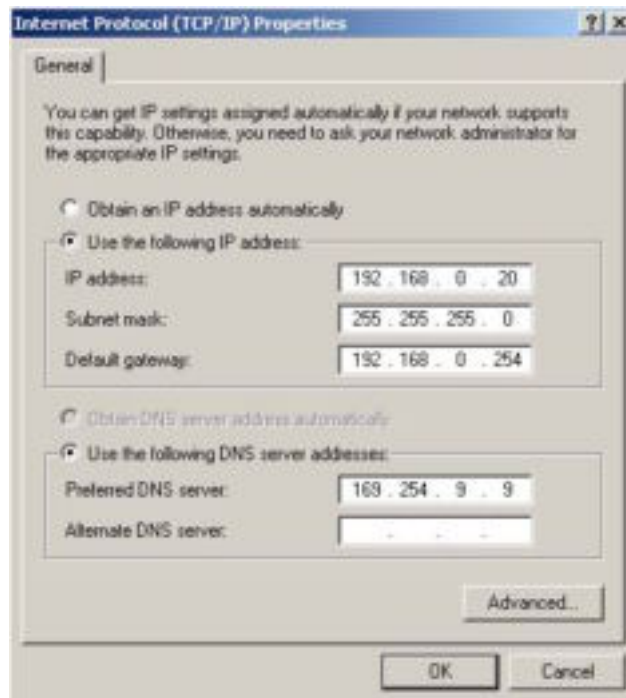


Fig. 19

Figure 20 shows the configuration window for the DNS proxy on the firewall:



Fig. 20

The internal hosts will utilize /etc/hosts files or LMHOSTS files to identify network resources on the internal network. The GIAC firewall is configured to accept DNS requests but not remote zone transfer requests.

2.2.5 Mail Proxy

The SMTP mail relay can be used to shield the internal mail server from attacks. It can act as a "relay" for both incoming and outgoing messages. In addition, email can be scanned for harmful content and anti-spam measures can be employed to block unsolicited email messages. Refer to Figure 21.

The default maximum message size is "unlimited". However, we changed it to 10 MB because customers won't be emailing files that large. Partners and suppliers can deliver large files via HTTPS or through the VPN connection. The "Max message size" will be set smaller than the largest file size accepted by the mail server. The setting will be monitored and adjusted when required.

Enabling virus protection will ensure incoming and outgoing messages are scanned for known viruses and malicious content. The exception to this rule is the mail account specified as the postmaster address. *The virus or content filters do not process the Postmaster account.* Extra care should be used when accessing email for the Postmaster account.

The following excerpt from the ASL Online Help file explains the expression filter and extension blocker functions:

The expression filter can be used to filter mails based on the presence of text strings in the body of the mail. Please see the manual for a complete reference on how to use this feature.

The file extension blocker can reject mails which contain certain types of files based on their extensions (e.g. executables). You can enter the extensions to be blocked (like "com" or "exe"), without the dot separator. (Astaro Online Help: SMTP Relay)

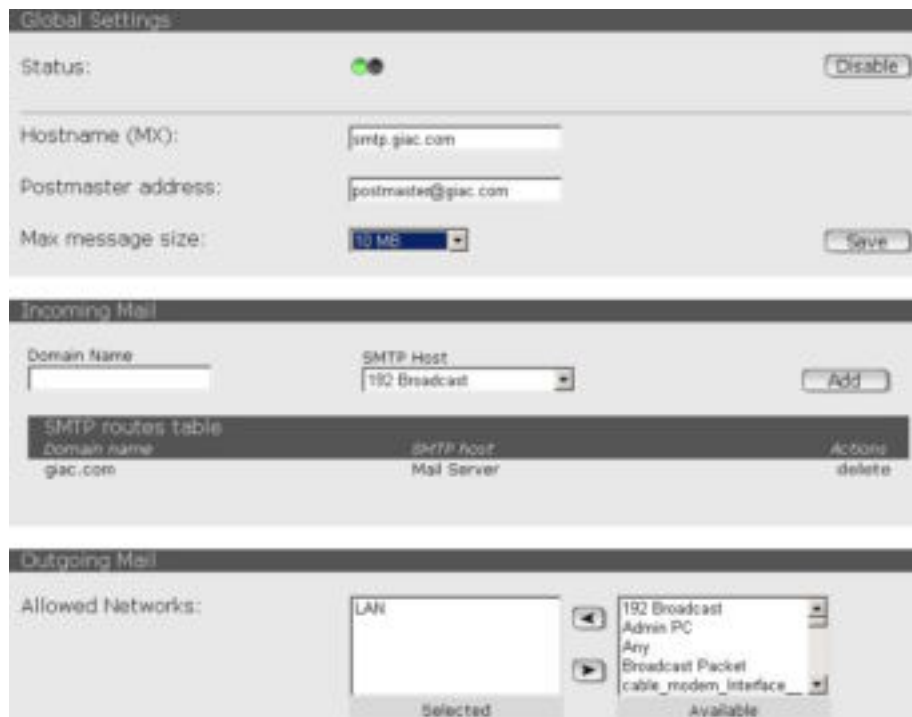


Fig. 21

Figure 22 shows the Content Control window:



Fig. 22

2.3 VPN Tutorial

The remote GIAC users and partners have access to the GIAC network via VPN connectivity, which allows users to securely access GIAC resources over un-secure links like the Internet. The current GIAC requirement calls for Host-to-Gateway VPN connections. Both partners and remote GIAC users will have specific procedures for authentication and network access. The following tutorial

will outline the configuration of a remote user accessing the GIAC internal network through a dial-up ISP connection. Authentication is accomplished through the use of X.509 Certificates.

2.3.1 Gateway Configuration

The certificate authority (CA) certifies the authenticity of the public keys. To generate the CA, go to the CA Management screen located in the IPsec VPN group. On the Certificates Authority section, select "New". The screen will appear as follows:

The screenshot shows the 'Add Certificate Authority' dialog box. On the left, under 'Predefined', a list of certificates is shown. On the right, under 'Generate', there are input fields for the following information:

- Name: giac_ca
- Passphrase: Not visually protected
- Key Size: 1024 Bits
- Country: United States
- State/Region: Your State
- City/Locality: Your City
- Organization: GIAC
- Dept./Org. Unit: (empty)
- Common Name: GIAC CA
- Email Address: admin@giac.com

Fig. 23

Type the appropriate information in the spaces provided. The "Passphrase" box allows you to type in a password to help authenticate when you work with the CA. Note: Use caution when in typing in your passphrase. If someone is shoulder surfing, they will now have your passphrase and can sign certificate-signing request (CSR) using your CA. After all the proper information is provided, press the "Start" button in the lower right hand corner. Note on passwords: Don't choose easily guessed passwords or phrases. It's your security at stake.

You should now have an entry labeled "Signing CA" in the CA list. This CA can now be used to sign requests by turning them into certificates. Now, CSR's for the firewall and remote users can be generated.

From "Certificate Management", select "New" from Host "CSRs and Certificates". The screen will look like this after clicking the "New" button:

Generate CSR

VPN ID: Hostname [huey.giac.com]

Name: tutorial_firewall

Passphrase: secret pass phrase

Key Size: 1024 Bits

Country: United States

State/Region: your state

City/Locality: your city

Organization: GIAC

Dept./Org. Unit:

Common Name: tutorial firewall cert

E-Mail Address: admin@giac.com

Start

Fig. 24

To generate a new CSR, select the "Generate CSR" option.

The VPN ID allows you to access a pull down menu to select what type of VPN ID you want to use. The selections are email address, hostname, IPv4 address, and x509 DN. In this tutorial, the "Hostname" option was selected and the hostname of the firewall inserted in the space to the right. Note: The CSR hostname may only contain letters, numbers, underscores, and dashes.

Generate CSR

VPN ID: Hostname [huey.giac.com]

Name:

Passphrase:

Key Size: 1024 Bits

Dropdown menu options: Hostname, Email Address, IPv4 Address, x509 DN

Fig. 25

Next, enter your secret pass phrase (beware of shoulder surfing). Use the pull down menu to select your "Country", and then fill in the "State" to "Email address" blocks with the appropriate information. Keep in mind that VPN connections are authorized by some of the information in the CSR. These identifiers are the email address, hostname, or IPv4 address. Be sure to enter the appropriate information.

Note: For the Common Name block, the ASL Manual recommends entering the name of the user if it's a Roadwarrior connection (connection with dynamic IP assignments like a dial up). Use the hostname if generating a CSR for a specific host. This CSR is identified using the hostname option.

When you are finished entering your information, click on the "Start" button in the bottom right hand corner. This will generate a new CSR. If you forget to fill in a space, as illustrated in Figure 24, the action will fail.

We now have a new CSR for our "tutorial firewall".

The next step is to sign the CSR. For the purpose of this tutorial, we will sign the CSR with our own CA. However, we could have used an external CA authority, such as VeriSign, to sign it for us.

In the Host CSRs and Certificates table, select the "tutorial_firewall" CSR and then select the "Issue CERT from CSR" action from the pull down menu.

Enter the "CA Passphrase" (**not** the Passphrase of the CSR you just created) and click "Start":



Fig. 26

When it's completed, the "CSR + KEY" will now be labeled "CERT + KEY" in your table as shown in Figure 27:

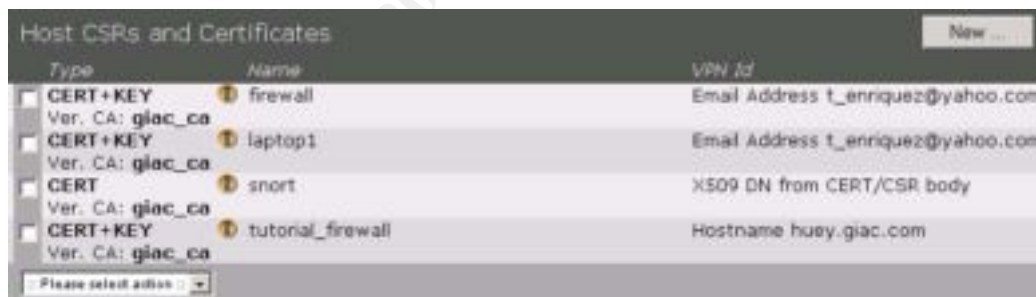


Fig. 27

Next, identify the certificate to use for the gateway:

Local IPSec X.509 Key

An excerpt from the Astaro User Manual explains the next step:

If you wish to use **X.509** authentication, use the **Local certificate** drop-down menu to select the certificate. This menu only contains those certificates for which the associated **private key** is available. In the **Passphrase** field, enter the password used to secure the **private key**. (User Manual, 133)

In this example, we selected the CERT identified as "firewall":

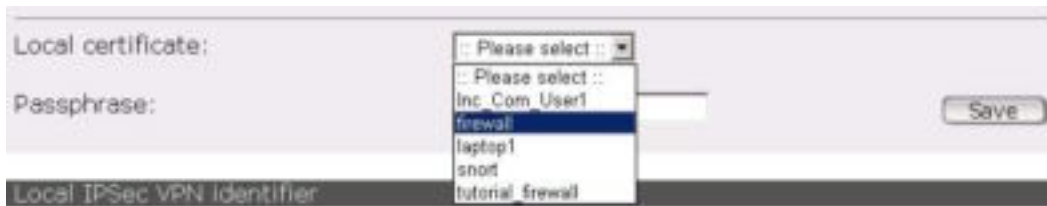


Fig. 28

After typing the correct passphrase and pressing "Save", your screen should look like Figure 29:



Fig. 29

Next, we can create CERT for a Partner using the same procedures outlined for creating the "tutorial_firewall" CSR and CERT.

Generate new CSR:

Generate CSR

VPN ID: [] Email Address: partner@inc.com

Name: Inc_Com_User1

Passphrase: another secret pass phrase

Key Size: 1024 Bits

Country: Germany

State/Region: Frankfurt

City/Locality: Frankfurt

Organization: Inc.com

Dept./Org.Unit: Sales

Common Name: Inc.Com User1

Email Address: partner@inc.com

Start

Fig. 30

Create CERT by signing CSR with the giac_ca CA (refer to Figures 31 and 32):

Certificate Authorities

Type	Name
Signing CA	giac_ca

Host CSRs and Certificates

Type	Name	VPN Id
CSR+KEY	Inc_Com_User1	Email Address partner@inc.com
CERT+KEY	firewall	Email Address t_enriquez@yahoo.com
CERT+KEY	laptop1	Email Address t_enriquez@yahoo.com
CERT	snort	X509 DN from CERT/CSR body
CERT+KEY	tutorial_firewall	Hostname huey.giac.com

take CERT from CSR

Signing CA Passphrase: fully protected

Start

Fig. 31

Host CSRs and Certificates

Type	Name	VPN Id
CERT+KEY	Inc_Com_User1	Email Address partner@inc.com
CERT+KEY	firewall	Email Address t_enriquez@yahoo.com
CERT+KEY	laptop1	Email Address t_enriquez@yahoo.com
CERT	snort	X509 DN from CERT/CSR body
CERT+KEY	tutorial_firewall	Hostname huey.giac.com

Please select action

Fig. 32

Save to file for export. Refer to Figure 33.

The above procedures should be repeated to generate CERTs for other remote users and partners. Be sure to enter the appropriate information into the certificates because the information will be identification criteria for VPN access (i.e., email address, hostname, and IPv4 address).

2.3.2 Exporting Certificate

For this tutorial, we will be installing the CERT for the GIAC computer "laptop1". This laptop is issued to a GIAC employee who frequently works away from the office.

To install the CERT, we need to transfer it from the firewall to the designated computer.

Export "laptop1" CERT+KEY in a supported format and save to disk. We selected the PKCS#12 format. From the Astaro Online Help Screen:

For downloading in PKCS#12 format, you will also need to specify an export password, which can be freely selected. You will need it when you later use the downloaded file on the IPsec client machine. (Astaro Online Help: CA Management)

Enter your Export passphrase and the laptop1 passphrase (passphrase assigned during CSR creation) in the appropriate blocks and press "Start".



Fig. 33

If you supplied the correct Passphrase for the laptop1 CSR, you will be prompted to save the p12 file. This was illustrated in Figure 27. From here, the file can be transferred to another medium so it can be installed onto the target computer.

2.3.3 Transferring CERT's

Now we can copy the file to a floppy and install it onto the GIAC laptop designated laptop1.

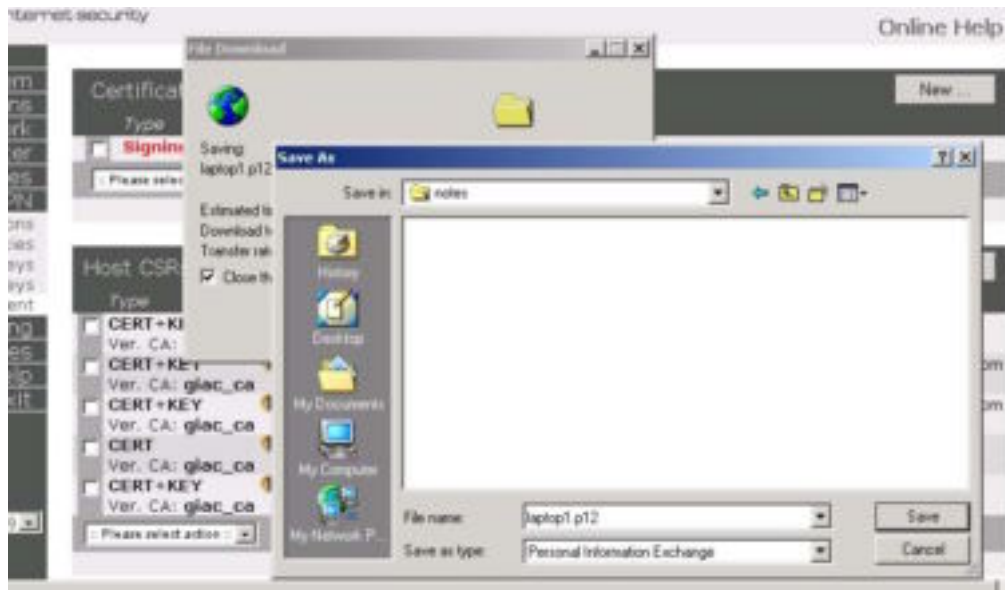


Fig. 34

It should be noted that if unauthorized people gain access to these X.509 CERT's, they would have access to your LAN. Please take the appropriate measures to transfer and safeguard the CERT's properly and safely.

2.3.4 IPSEC Policy

An IPsec policy defines IKE and IPsec proposal parameters of an IPsec connection. Each IPsec connection needs an IPsec policy. This part of the tutorial will cover the steps required to create a custom IPsec policy.

From the IPSEC VPN section, select the "Policies" menu. Enter the name of your new IPSEC policy in the name field. The default "Key Exchange" is set for IKE and is not configurable:



Fig. 35

The next window allows you to set the SA lifetime of IKE sessions in seconds. 7800 seconds is the default setting. The other two settings are not configurable:

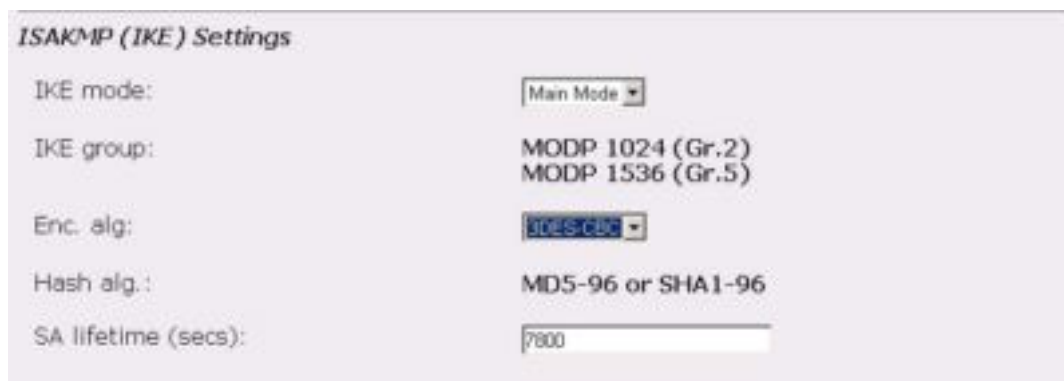


Fig. 36

2.3.5 IPSec Settings

The ASL only supports Tunnel mode for IPSec mode and ESP for the IPSec protocol.

Use the pull down menu to select the desired encryption algorithm. This is the algorithm used by the receiving end point of the VPN location. GIAC will be using AES-128 for their VPN policy.

When enabled, Perfect Forwarding Secrecy (PFS) ensures that the numbers used have not already been used by another key. Therefore, if an attacker discovers the old key, they will have no way to guess future keys. According to the ASL User Manual, PFS requires a fair amount of processing power to complete the Diffie-Hellmann key exchange. PFS is also often not 100% compatible between manufacturers. In case of problems with the firewall's performance or with building connections to remote systems, you should disable this option" (132) The VPN connection is considered to be "more secure" with PFS enabled. Therefore, we will keep the default setting and leave it on.

According to the ASL User Manual, "This algorithm compresses packets before they are encrypted, resulting in faster data speeds. At this time, this system only supports the deflate algorithm" (132). This policy will be set with the default setting of "On".

Next, save the "Laptop" policy by clicking "Add". (See Figure 25 for location of "Add" button.) Figure 37 displays the "Laptop" settings consistent with the GIAC IPSec policy:

Edit IPsec policy 'Laptop'

Name: Laptop Save

Key exchange: IKE

ISAKMP (IKE) Settings

IKE mode: Main Mode

IKE group: MODP 1024 (Gr.2)
MODP 1536 (Gr.5)

Enc. alg: 3DES-CBC

Hash alg.: MD5-96 or SHA1-96

SA lifetime (secs): 7800

IPSec Settings

IPSec mode: Tunnel

IPSec protocol: ESP

Enc. alg: AES-128 (Rijndael)

Hash alg.: MD5-96 or SHA1-96

SA lifetime (secs): 3600

PFS: On (default)

Compression: On - deflate (default)

Fig. 37

2.3.6 Configuring an IPsec VPN Connection

A VPN connection configuration must be created so remote users can connect to our firewall. Refer to Figure 38.

From the IPsec VPN section, click on "Connections" to activate that menu.

Click on "Enable" to activate the Global Settings Menu.

The new display (refer to Figure 38) will contain a selection for "New IPsec Connection." Enter the name of the IPsec connection you wish to create and select what type of connection you want to configure. From the Astaro Online Help Screen:

There are two valid Types 'Standard' and Roadwarrior. The major difference between those two is, that Roadwarrior connection always have dynamic ip addresses as remote endpoint and have no remote subnet. It is also possible to add several Remote Key Objects (different Roadwarriors) to the same Roadwarrior connection. This reduces the amount of configuration needed. Roadwarrior can

only by connected through the default gateway. All other connections are to be considered standard. (Astaro Online Help: Connections)

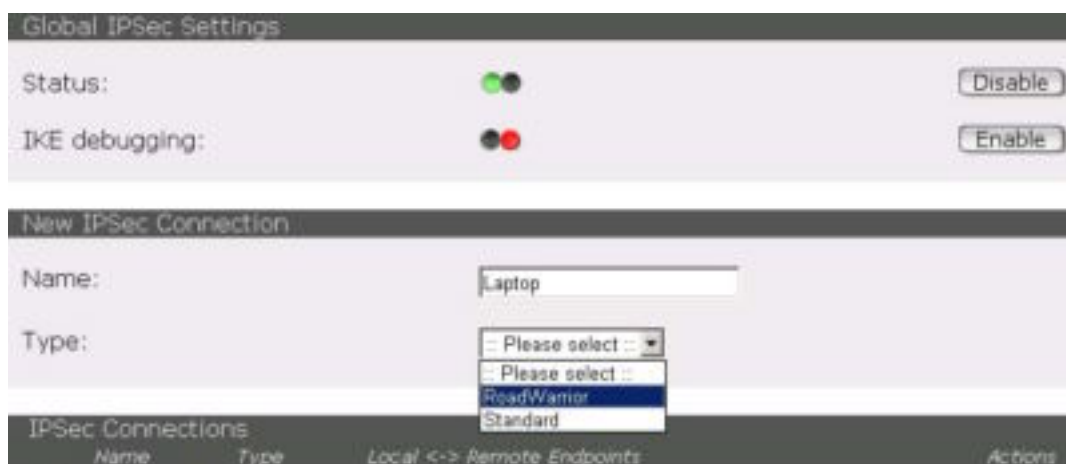


Fig. 38

The parameters for the new connection are:

- Type: Roadwarrior
- IPsec Policy: Laptop (Custom IPsec policy created earlier)
- Local Endpoint: <External Interface> (External Interface of firewall)
- Local Subnet: <LAN> (Internal Interface to the GIAC LAN)
- Add 'X509: laptop1 (Authentication for remote station)

Those parameters will enable a remote connection to access the GIAC LAN authenticating with the "laptop1" X.509 certificate. If this was a connection for our partner, we could have changed the Local Subnet to "Service Network" so they could access the database services located in the service network. This would also give them the ability to access all the systems in the service network.

Depending on the partner's computer configuration, a better configuration would be to create a "Type: Standard" and terminate the connection to the desired server. This would limit access to a specific machine only.

Once the connection parameters are entered and verified, click on "Save".

The saved connection configuration is displayed below:

Name: **laptop** Save

Type: **RoadWarrior**

IPSec Policy: **Laptop**

Tunnel Endpoints

Local Endpoint: **External Interface**

Remote Endpoint: **Any**

Subnet definition (optional)

Local Subnet: **LAN**

Remote Subnet: **None**

Authentication of remote station(s)

Keys:

x509: laptop1
Selected

←
→

x509: firewall
 x509: inc_com_user1
 x509: snort
 x509: tutorial_firewall
Available

Fig. 39

2.3.7 Packet Filter Rule

The displayed filter rule indicates that it will accept all inbound and outbound connections, which facilitates testing other VPN's. When testing is completed, destination "any" will terminate at the required interfaces:

4	Any	ISAKMP	Any	Allow	edit del move
5	Any	VPN	Any	Allow	edit del move

Fig. 40

2.3.8 Laptop Computer Setup

The laptop has been configured to pass the Level-1 Benchmark for Windows 2000 (v1.1.7).

```
Windows 2000 Professional
SSH Sentinel 1.3 VPN Client Software
Norton Internet Security 2002 (Provides firewall and AV protection)
Required business applications
```

Our next step is to configure SSH Sentinel so the laptop can connect to the GIAC firewall using the VPN tunnel. Note: we will not cover software installation.

Our saved "laptop1" X.509 certificate needs to be installed onto laptop1. We can do this by copying the file to a floppy disk and transfer the certificate to laptop1.

From the SSH Sentinel Application, the new certificate must be imported.

To run the policy editor; select the "Key Management" tab, right click on "host keys", and click on "Import".



Fig. 41

After you select the laptop1 file and click "Open", you will be prompted for a password. This password is the passphrase you configured when you created the initial CSR. After you type in the passphrase, click "OK":

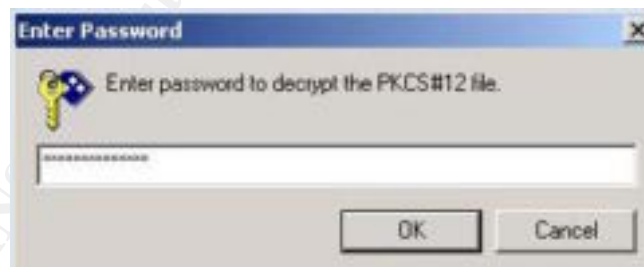


Fig. 42

Click "Yes" to accept the certificate.

You have now imported the laptop1 CERT. From the "SSH Sentinel Policy Editor/Key Management" tab you can view the certificates. The "va certificate" is the one we just imported over:



Fig. 43

To create a new VPN connection, locate the "Security Policy Tab", expand "VPN Connections", and click "Add". The following window will appear:



Fig. 44

The external firewall interface is the termination point of this VPN connection. Type in the IP address assigned to the external interface of the firewall.

Click the "Ellipses" button to configure the remote network. This GIAC user is granted access to the internal LAN. The parameters for this connection are:

Network Name: LAN

IP address: 192.168.0.0
Subnet mask: 255.255.255.0.

After you add the "LAN" entry, the screen will look like this:

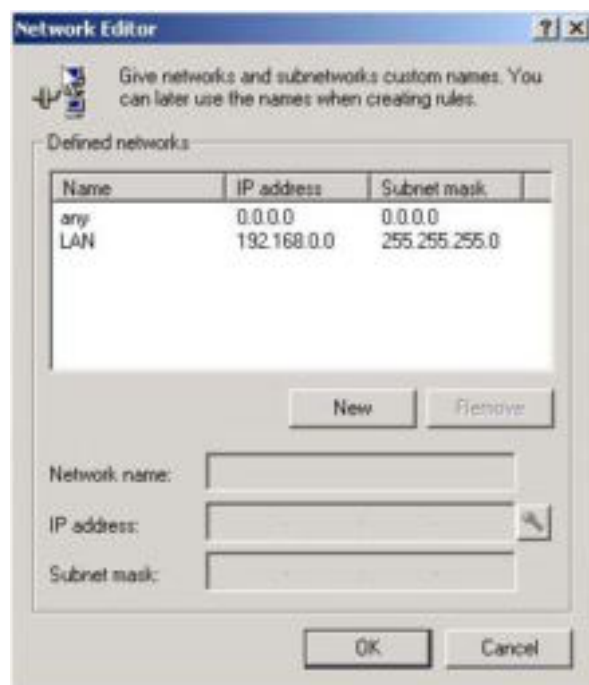


Fig. 45

Click "OK" to close this out, and then click on the "Properties" button.

From the "Add VPN Connection" screen, use the "Authentication" pull down menu and select the certificate we just imported.

Click the "Properties" button.

Click "Settings" in the "Rules Properties" box on the "General" tab under "Proposal Templates". The following window will appear:

© SANS Institute 2000 - 2002

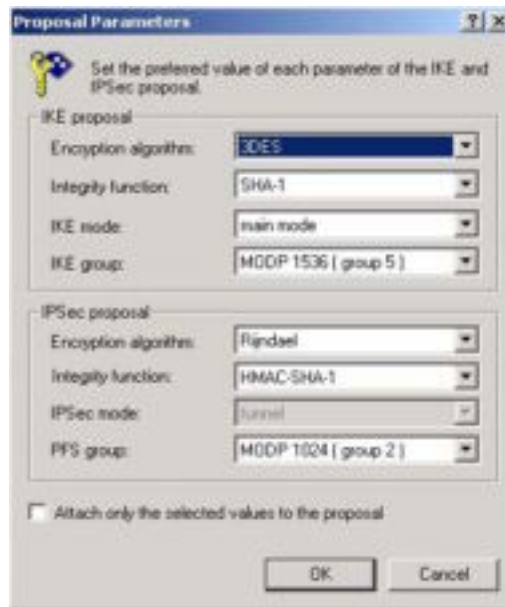


Fig. 46

The parameters for our VPN are:

IKE Proposal
Encryption algorithm: 3DES
Integrity function: SHA-1
IKE Mode: main mode
IKE group: MODP 1536 (group 5)

IPSec proposal
Encryption algorithm: Rijndael
Integrity function: HMAC-SHA-1
IPSec mode: tunnel
PFS group: MODP 1024 (group2)

Click "OK" to keep the changes.

Next, select the "Advanced" tab from the "Rules Properties" window:

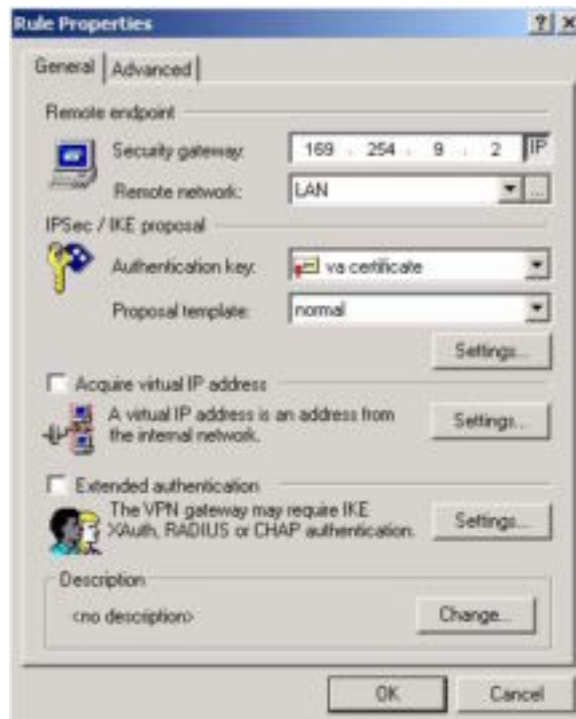


Fig. 47

Click the "Settings" button located in the "Security Association Lifetimes" section:



Fig. 48

Select "Settings" from the "Rule Properties" window.

The Parameters should read:

```
IKE security association
  Lifetime in minutes:    130
  Lifetime in megabytes: 0

IPSec security association
  Lifetime in minutes:    130
  Lifetime in megabytes: 400
```

The time in minutes match the settings for the Laptop1 VPN connection we configured on the firewall. Figure 49 displays our new settings:

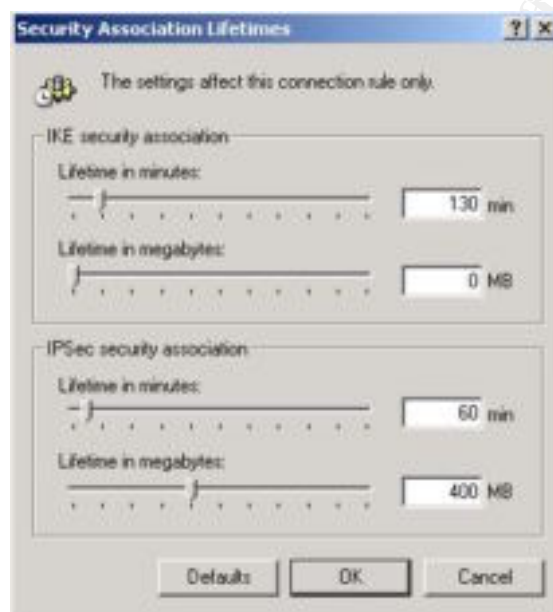


Fig. 49

Click "OK", then save the configuration by clicking "Apply" in the "SSH Sentinel Policy Editor" window as shown in Figure 50:



Fig. 50

To test the VPN connection, establish a dialup connection through your ISP.

From "VPN Connections", select the new VPN connection and then click the "Diagnostics" button. According to the SSH website, "The diagnostics run the complete IKE negotiations (phases 1 and 2) just as they are run when establishing the connection. The security associations are destroyed immediately after the phase 2 is completed." If the following dialog box appears after the diagnostics has run, you will be able to establish a secure VPN connection:



Fig. 51

Next, establish the VPN connection with a right click on the "SSH Sentinel" icon in the task bar. From "Select VPN", choose the connection we just configured. This is demonstrated in Figure 52:

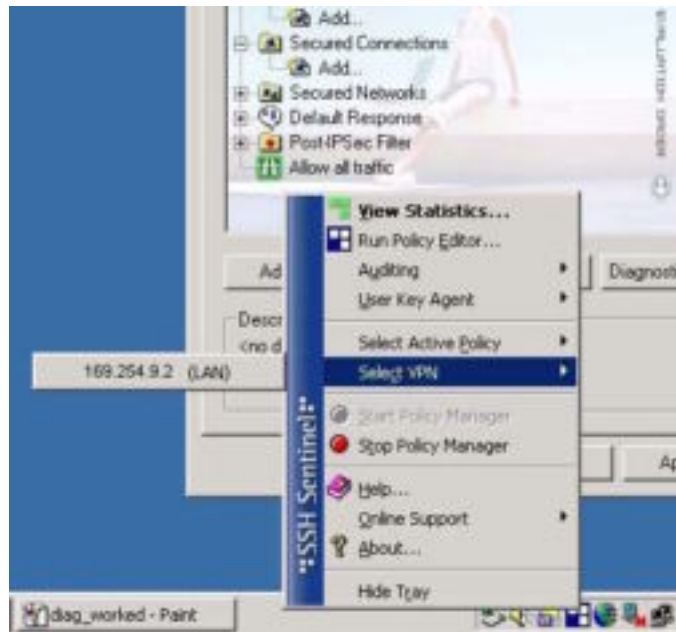


Fig. 52

You will receive an error message if the VPN fails. Once you're connected, you can view stats of the connection:



Fig. 53

2.3.9 Verify Outbound Traffic from Laptop

Now that a VPN connection has been established, we should see if the traffic is indeed leaving as ISAKMP/ESP traffic.

Open a DOS (the other DOS) window and enter "ipconfig" to view the IP address of the PPP connection:



```
C:\WINNT\System32\command.com
C:\>command
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1998-1999.
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter {CB698000-DEC9-43F4-BE6B-C129DB3A9660}:

    Media State . . . . . : Cable Disconnected

Ethernet adapter Local Area Connection:

    Media State . . . . . : Cable Disconnected

PPP adapter earthlink:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 209.244.224.17
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 209.244.224.17

C:\>
```

Fig. 54

2.3.10 Setup Sniffer

We are going to be simulating that we placed the sniffer between the router and the external interface of the firewall. Start the sniffer to capture traffic from 209.244.224.17.

2.3.11 Generate Traffic from Laptop1

To generate traffic, access an internal web server (not servers located in the service network).

2.3.12 Analyze Traffic

Our capture file contains only traffic generated from 209.244.224.17. Note: Sniffing a network other than your own does require permission or a court order. Anything else would be considered illegal. That being said, our capture file contains traffic generated from our laptop.

Figure 55 indicates that all traffic from the laptop appears to be working properly. Only ISAKMP, ESP, and occasional fragmented IP packets existed in the capture file. When we disconnected the VPN connection, traffic terminated as expected. We will simulate that the firewall address is that of the external GIAC firewall.

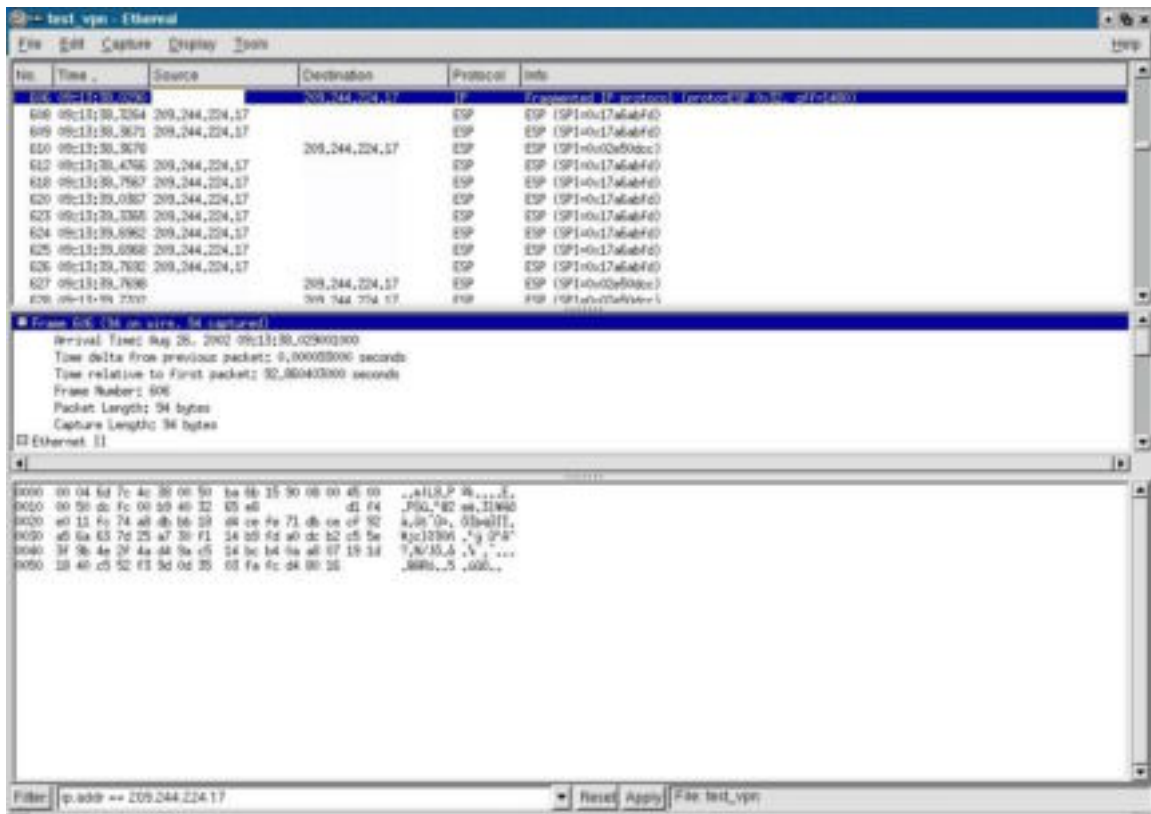


Fig. 55

Since we were able to access the internal web server, we can say that the VPN connection is working correctly. The same steps that were used to verify this connection will also help troubleshoot VPN connections. All VPN connections will be verified the same way.

© SANS Institute

Assignment 3: Verify Firewall

3.1 Plan the Audit

It is important determine what the firewall is configured to do before starting any firewall audit. Without that information, it cannot be determine if the firewall is working correctly. For our purposes, each interface on the firewall will be evaluated against the GIAC policy.

The first part of the audit will verify the rule sets by seeing what packets get by the firewall. One computer will be configured as a sniffer and another will be configured to run Nmap. The second test will consist of running a vulnerability scanner on the external interface. This will determine if the firewall has any known vulnerabilities that could be exploited later. The final test will be verifying the VPN connections.

3.1.1 Ruleset Audit

Nmap will be used to generate traffic through the firewall. A sniffer, in this case Ethereal, will be used to capture packets as they come through the firewall. The sniffer positioning will depend on which interface and direction the traffic is going. If testing inbound rules from the external interface to the service network, the sniffer will be placed in the service network and the Nmap box will be configured to send scans through the external interface to a target on the service network. See Figure 56 for details:

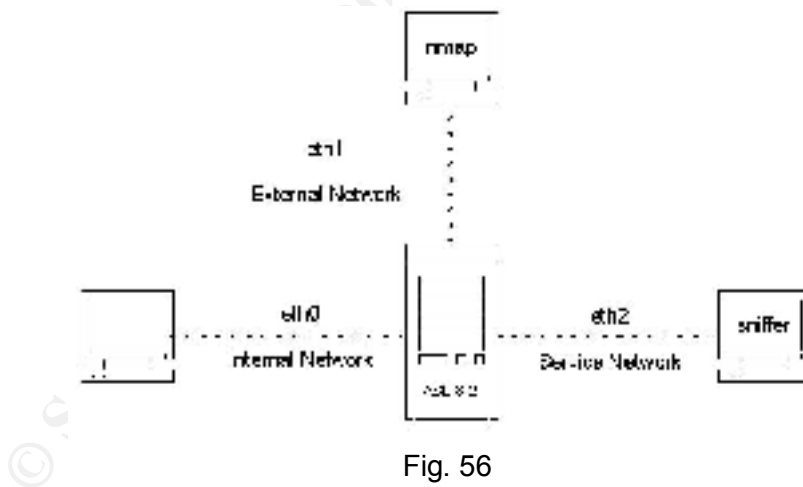


Fig. 56

If possible, simulate the actual environment by configuring a target computer to scan. Better yet, use the actual server. The capture files will verify whether the firewall is working correctly, misconfigured, or malfunctioning. Compare the captured traffic with the ruleset. If unexpected packets make it through or expected packets are not seen, check the firewall configuration.

Test Computers:

The Nmap box and sniffer box are two identical Linux boxes. Since they both have Ethereal and Nmap, it prevents reconfiguring and moving things around. Just run one scan one way and then reverse the process. Things run a lot smoother when using two computers that can do both tasks.

External Interface:

Service	Incoming	Outgoing
http	To webserver only	From Proxy
https	To webserver only	From Proxy
Smtpt	To mail server only	From Mail Server
DNS	To DNS server only	From DNS server
ftp		From LAN
ftp-control		From LAN
ISAKMP	X	
ESP	X	
smb-reject no log	X	X
netbios-reject no log	X	X
255.255.255.255 drop	X	X
192.168.0.255 drop	X	X
ident-reject no log	X	X
Syslog	From Router Only	
Log & drop everything else		

Service Network Interface:

Service	Incoming	Outgoing
http	Ext Only	
https	Ext Only	
Smtpt	Ext & Proxy	
DNS	Ext & Proxy	
SSH	From LAN Only	
smb-reject no log	X	
netbios-reject no log	X	
255.255.255.255 drop	X	
Drop Network Broadcast	X	
ident-reject no log	X	
Ntp	From Router	
Syslog	From Router	
Traffic From VPN Client	From Ext Interface	
Log & reject traffic initiated from service network		X
Log & drop everything else	X	

Internal Interface:

Service	Incoming	Outgoing
http		To Proxy
https		To Proxy
Smtpt		To Proxy
DNS		To Proxy
SSH		To Service Network Only
FTP-Data		X
FTP-Control		X
Traffic from VPN client	From Ext Interface	
smb-reject no log	X	X
netbios-reject no log	X	X
255.255.255.255 drop	X	X
drop network broadcast	X	X
Ntp		
Log & drop everything else	X	

For the external-to-service network scans, a scan was initiated for each server expected to be reached from the Internet in order to verify that the firewall passed certain traffic for certain servers. The syntax is:

```
nmap -sS -P0 -r -p 1-65535 w.x.y.z -oN servername.txt
```

-sS: TCP SYN scan
-P0: Do not ping host before scanning.
-r: nmap will not randomize ports. Easier to maintain log files.
-p: Specifies port, ports, and port ranges you wish to scan. Use -p followed by port numbers.
w.x.y.z: Target you are scanning.
-oN: Saves file in a human-readable format. Follow this syntax with the desired file name.

Any sniffer program will do if Ethereal is not available. Position the sniffer on the target network. Start the sniffer before initializing the scan. Save the capture to a file for analysis when the scan is done.

3.1.2 Vulnerability Scan

The Nessus vulnerability scanner will be used to check for deficiencies at the external interface. Version 1.2.5 will be used to run the vulnerability scans. To expedite the vulnerability checks, we will "enable ICMP" on the external interface of the firewall. (I've always had problems when I tried to disable the "ping" options within Nessus.) Nessus will be configured as follows:

Safe option - Disabled: With the safe option enabled, it won't run scripts that could crash the target under test. We want to crash the firewall if possible.

Enable all plugins - Selected: Will enable all plugins.

Optimize test - Disabled: Launches checks based on existing or required information in the knowledge base. We want to run all the tests regardless of the knowledge base.

Since Nmap is running separately, the Nessus scan can be expedited by reducing the port range to be scanned. Select the open ports found in the Nmap scan for that specific machine to verify initial Nmap scan.

3.1.3 Verify VPN Connection

Using the defined procedure outlined in the GIAC network policy and VPN tutorial, verify the VPN connection.

3.1.4 Cost

The majority of the cost will be spent on “man hours”. The following will provide an estimate based on the requirements of this audit:

Task	Man Hours
Review policy under test	4
Interview Network Administrator	1
Review Architecture	4
Research of device under test	8
Planning Audit	8
Lab Preparation X 2	16
Perform Audit X 2	32
Provide Outbriefing	1
Total Hours	74
Cost Per Hour	\$75.00
Total	\$5,700.00

3.2 Perform Audit

3.2.1 Run Nmap Scans

Perform the following Nmap scans:

- Run Nmap scans through External Interface to:
 - Webserver
 - Mail Server
 - DNS Server
 - Time Server
- Nmap scans from External to Internal LAN.

- Nmap scans through Internal Interface to Service Network.
- Nmap scans from Internal Network through External Interface.
- Nmap scans from Service Network through External LAN.
- Nmap scan of External Interface.
- Nmap scan of Service Network Interface.
- Nmap scan of Internal LAN interface.

3.2.2 Rule Analysis

The firewall worked as expected with the exception of a few configuration errors. The following will provide the errors and recommended changes.

Here is a screen shot from a scan that contains unexpected results:

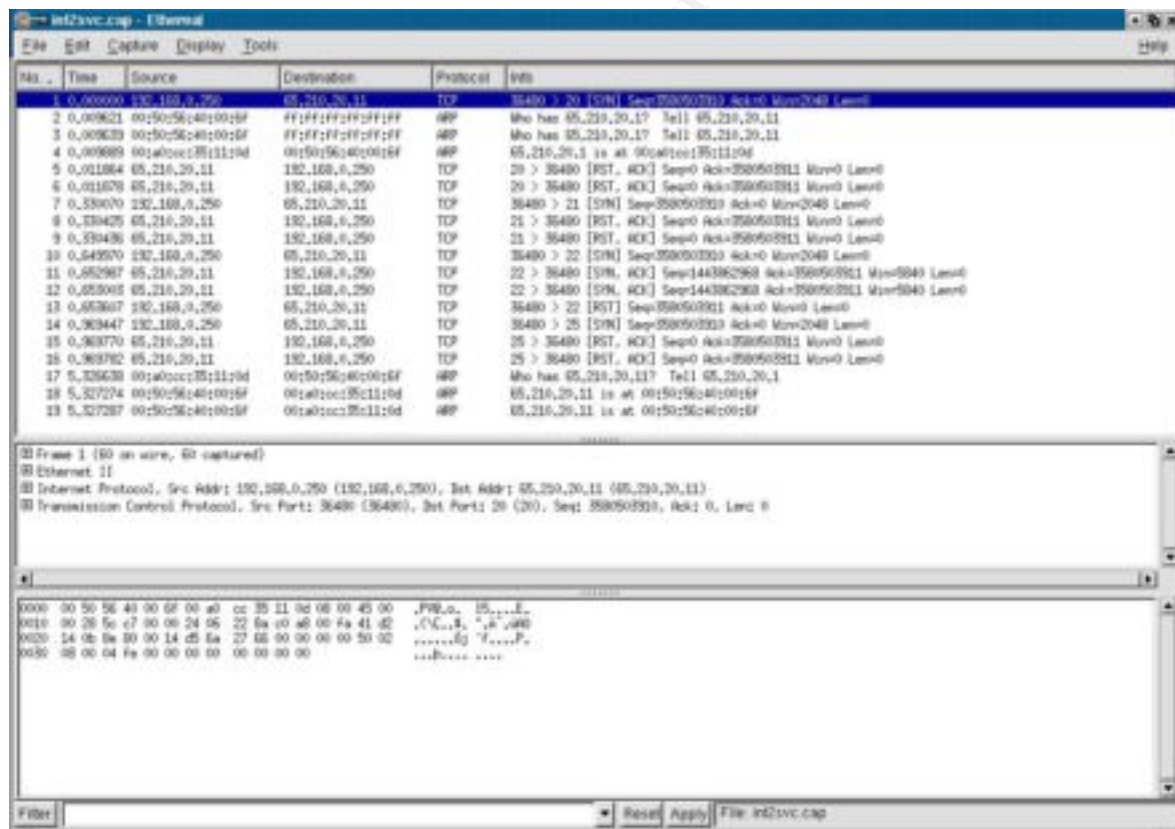


Fig. 57

This scan was done from the internal LAN to the service network. Most of the permitted traffic leaving the internal LAN is processed through a proxy service, except for SSH and FTP. The capture above indicates that SSH is getting

through but so is FTP and SMTP. Port 25 should be handled by the SMTP proxy, while ports 20 and 21 should not be there at all. All file transfers from the LAN and Service machines are done via SFTP.

If you go back to Figure 18, you'll notice that Rule 4 states:

```
Any -> SMTP-> Mail Server -> Allowed
```

The firewall performed exactly as configured. We modified the rule to:

```
External_network -> SMTP -> Mail Server -> Allowed.
```

External_network is a static definition created during interface setup. The firewall external nic is named External. The software creates a "network definition" for that interface, External_network. The new rule states that SMTP traffic originating from the External_network is passed to Mail Server. Scans from the internal network and external network indicate that the new rule is functioning correctly. The SMTP proxy will relay the mail from the internal LAN to the Mail Server.

Rules 5 and 6 state:

```
LAN -> FTP -> ANY -> Allowed
LAN -> FTP-CONTROL -> ANY -> Allowed
```

Again, this misconfiguration worked exactly as it should have. This problem is almost like the previous problem. To correct this problem, the rule was modified to read:

```
LAN -> FTP -> External_network -> Allowed
LAN -> FTP-CONTROL -> External_network -> Allowed
```

This rule prevents LAN users from FTP'ing into the service network, but still allows them to FTP to the Internet. Scans from the internal LAN to the service network did not contain traffic from port 20 or 21. Scans from the internal LAN through the external interface indicated the correct traffic.

Scans targeting each firewall interface were also done to verify all open ports to known services. It would also reveal open ports that we are not aware of. The following TCP ports were open on the following interfaces:

External Interface:

```
25 SMTP Proxy
```

Service Interface:

```
25 SMTP Proxy
```

Internal Interface:

22 SSH access to service network and firewall
25 SMTP Proxy
53 DNS Proxy
443 HTTPS access to the WebAdmin Firewall Interface
8080 HTTP Proxy

Scanning Notes:

All 65535: To scan through the firewall with all 65535 ports took close to an hour, the longest taking 57 minutes. To do all 65535 UDP ports would take even longer. Since we were in a lab environment, it was easy to do a complete TCP scan. A complete audit would include UDP scans. We verified inbound UDP 53 from the external to the DNS Server with the sniffer, but to scan all 65535 UDP ports would take an extremely long time.

If we had more time, the UDP scans could have been done in small chunks over several days. Another problem with scanning for UDP ports is the default drop rule. The way the firewall is configured, performing a UDP scan would indicate that all UDP ports were open. This is due to the firewall not sending ICMP port UNREACHABLE replies.

Service network and external interface logging broadcast address: No rule to drop and not log service network broadcast packets, and external interface network broadcast packets were defined.

3.2.3 Run Nessus Scan

The Nessus scan ran without noticeable problems. This scan did not find any major vulnerability that Nessus could identify. The program did generate the following warnings and notes. Figure 58 indicates a problem with ICMP:



Fig. 58

Nessus indicates that the risk factor for this warning is low, and provides the CVS information for reference. To fix this, disable ICMP on the firewall.

Figure 59 displays an SMTP problem:

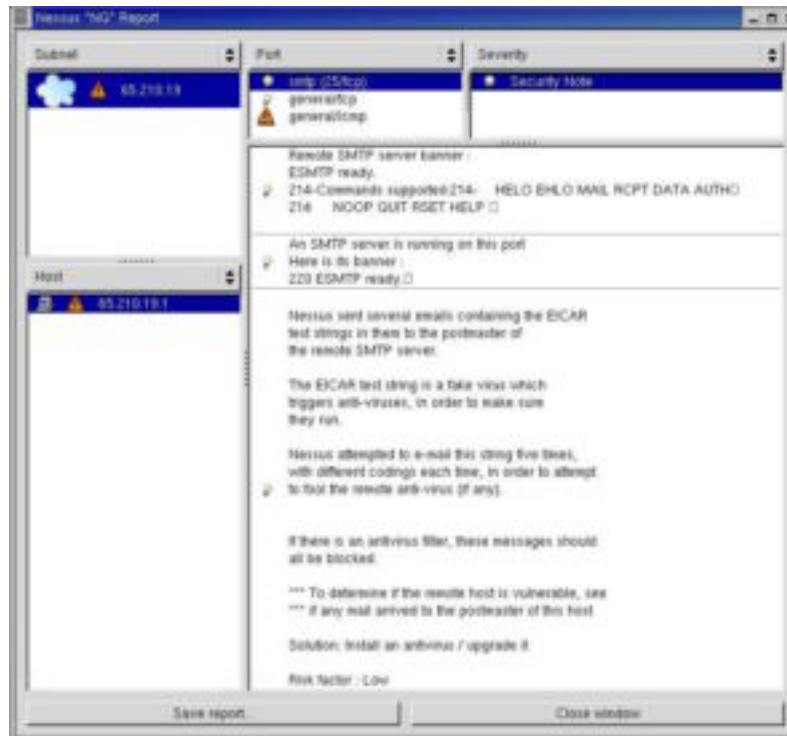


Fig. 59

The following excerpt from the Nessus program describes the plugin "SMTP antivirus filter":

Nessus sent several emails containing the EICAR test strings in them to the postmaster of the remote SMTP server. The EICAR test string is a fake virus which triggers anti-viruses, in order to make sure they run. Nessus attempted to e-mail this string five times, with different codings each time, in order to attempt to fool the remote anti-virus (if any). If there is an antivirus filter, these messages should all be blocked. (Firewall Plugins)

Figure 60 shows the SMTP Mail Relay Queue:

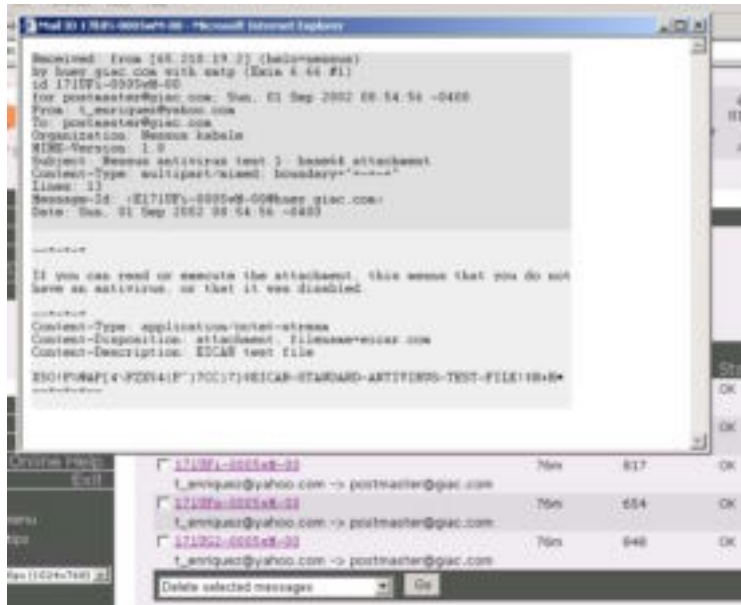


Fig. 60

The virus checker in the SMTP relay identified the test virus each time Nessus sent the infected email.

The "general/tcp" security note displayed in figures 58 and 59 specified the OS of the firewall.

"Nmap found that this host is running Linux Kernel 2.4.0 - 2.5.20"

3.2.4 Verify VPN

As stated in the VPN tutorial, the VPN connections were verified.

3.2.5 Results

With the information from the Ruleset Audit and Vulnerability Scan, the firewall is functioning as required at this point in time. The Ruleset Audit verified initial configuration problems. Subsequent modifications to the filter rules verified that the new rules enforced the policy as expected. The Vulnerability Scan checked for known vulnerabilities that Nessus could identify at the time the scan was performed. The results of that scan indicated no major problems. The SMTP relay virus checker correctly identified the EICAR test virus, and kept the emails in the email queue. The VPN's functioned as configured.

3.3 Recommendations

Security improvements can be made by modifying the VPN policy. Unless partners are trusted not to "roam around" in the service network, I would make all partner connections "Gateway-to-Gateway" only. This change in policy would allow termination to a specific computer instead of a network interface. Enabling

the "PPTP Roadwarrior Access" capability is another option. The Roadwarrior option allows specific termination points to be selected, at the cost of the inherent security problems associated with PPTP technology.

Disabling the VPN function on the firewall and purchasing a stand-alone VPN solution is yet another option. The stand-alone VPN appliance has more flexibility and takes that burden off the firewall.

The SMTP proxy service opens up TCP port 25 on the external interface of the firewall. This would allow an attacker to possibly exploit the firewall using an "exim" exploit. Eliminating the SMTP proxy will remove that risk. I recommend that we setup another PC to function as the SMTP relay to remove that burden from the firewall.

3.4 Overall

Based on the amount of employees, number of computers, and predicted traffic, the firewall as configured is adequate. By monitoring the log and report features on the ASL, it's possible to forecast when it will be necessary to upgrade the firewall.

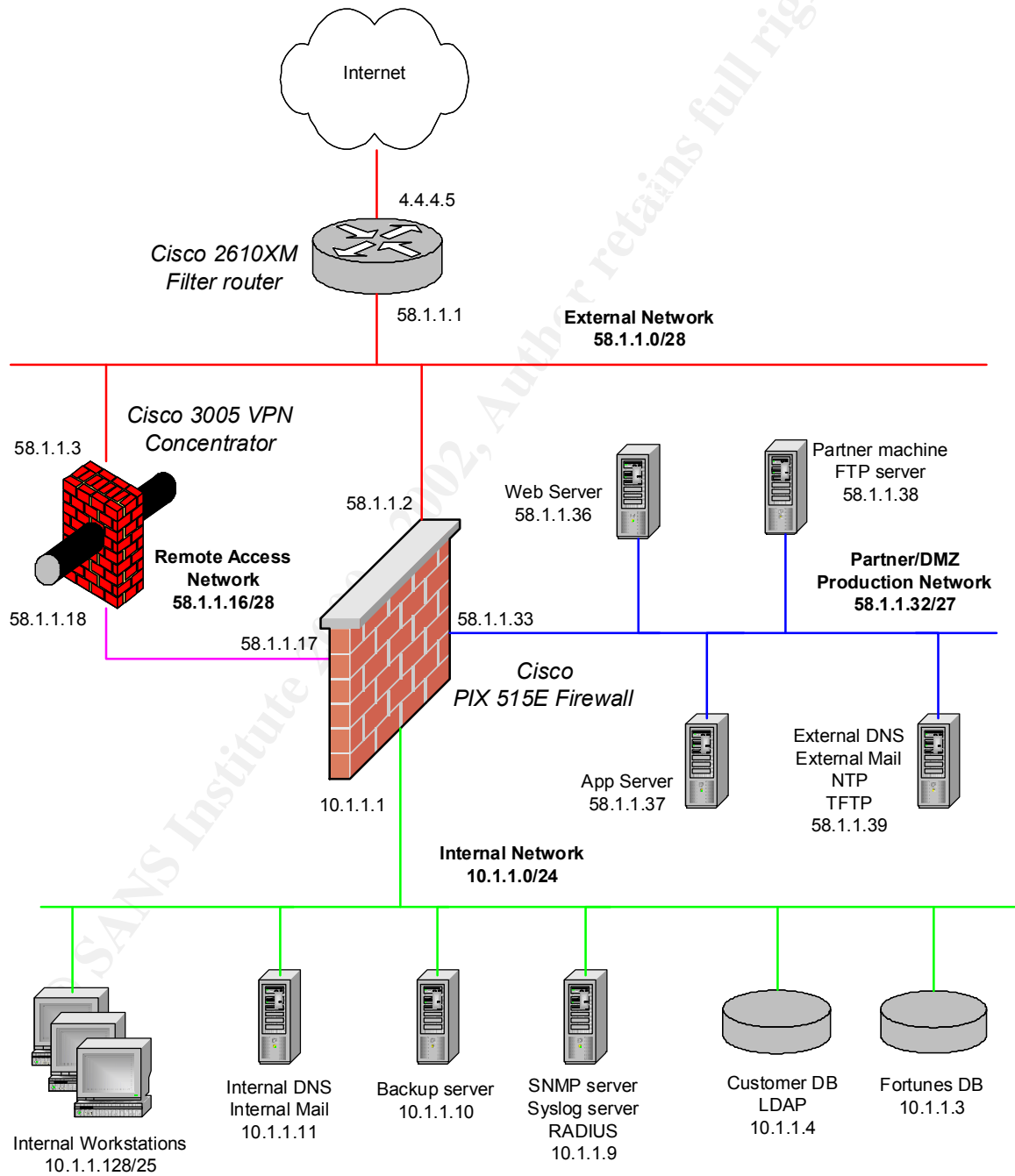
© SANS Institute 2000 - 2002, Author retains full rights.

Assignment 4: Design Under Fire

4.1 Overview

The Network diagram of Steve Keifling will be used for this assignment. His practical can be found at:

http://www.giac.org/practical/Steve_Keifling_GCFW.doc



4.2 Firewall Attack

Steve's design is utilizing the Cisco PIX 515E, running OS Release 6.2(1) and PIX Device Manager Release 2.0(1). The first step was to research and analyze any vulnerability reports. I discovered that Cisco does a great job providing information concerning the products they support. I went to Cisco web to view the latest publicized Cisco Advisories. The most recent PIX Advisory (as of writing this paper) was released on June 27, 2002 concerning a possible DOS vulnerability (<http://www.cisco.com/warp/public/707/SSH-scanning.shtml>) and offers the following description:

"While fixing the vulnerabilities listed in <http://www.cisco.com/warp/public/707/SSH-multiple-pub.html> (Cisco Security Advisory: Multiple SSH Vulnerabilities) an instability is introduced in some products. 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. 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."

Although I'm fairly new to the network security business, it's always advised that you should never use telnet if SSH is available for the obvious reasons (i.e., telnet authenticates in the clear). Although the exploit will not work on Steve's firewall, the fact that we tend to use SSH whenever possible, might cause a configuration mistake on any affected Cisco product.

Unfortunately, while trying to fix one SSH vulnerability, they introduced another one. The Cisco Advisories references Vulnerability Note VU #945216 and VU #13877 at the CERT Coordination website. The Cisco Advisory summary from the Multiple SSH Vulnerabilities is as follows:

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. 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."

I highlighted the first part. That tells me that it has trouble with SSH 1.5. Therefore, my attack will have to attack SSH version 1.5. Following are the details from the Cisco Security Advisory: Multiple SSH Vulnerabilities Advisory that we are concerned with:

"An implementation of SSH in multiple Cisco products are vulnerable to three different vulnerabilities. These vulnerabilities are:

CRC-32 integrity check vulnerability

This vulnerability has been described in a CORE SDI S.A. paper entitled "An attack on CRC-32 integrity checks of encrypted channels using CBC and CFB modes", which can be found at <http://www.core-sdi.com/soft/ssh/ssh.pdf>."

We now know that the vulnerability that they were trying to fix is the CRC-32 integrity check vulnerability. Subsequent searches on the Internet provided several sources of information. A binary that runs the vulnerability check was found at the PacketStorm website (<http://packetstormsecurity.org/0204-exploits/x2.tgz>) and provides the following description:

"X2 exploits the SSH CRC-32 attack detection code buffer overflow vulnerability that exists in SSH1 implementations. The exploit is distributed in binary form and has been encrypted. Includes 45 target types. This code was abandoned in a honey pot and is published under Fair Use Law 17 U.S.C.A 107"

It's important to know that if I did have the chance to run this exploit on a PIX that had SSH enabled running on the external interface, I would have done it in a test/closed environment. No source code was provided for the "x2" program, only a binary. Except for exhaustive testing and analysis of the binary, we didn't know if the binary had any undocumented features. Use it at your own risk. Steve stated in his practical on page 47 that his scans from the Internet did not find any anomalies. That's bad for us because we needed port 22 to be open and running the SSH server. We will simulate that the PIX was running ssh on port 22.

Running the binary with a `-h` flag brought up the following:

```
#./x2 -h

SSHD deattack exploit. By Dvorak with Code from teso (http://www.team-teso.net)

Usage: sshd-exploit -t# <options> host [port]
Options:
  -t num (mandatory)  defines target, use 0 for target list
  -X string            skips certain stages
```

The tarball came with a "targets" file. This file enabled you to select the type of SSH daemon you want to test. Since the PIX is vulnerable with ssh version 1.5, we will have the x2 program execute with that target in mind, using the IP address of the external interface of Steve's PIX firewall. The "1" specifies what version of SSHD to attack.

```
#./x2 -t 1 58.1.1.2 22

SSHD deattack exploit. By Dvorak with Code from teso (http://www.team-teso.net)
```



```
Target: Small - SSH-1.5-1.3.7-10
```

```
Attacking: 58.1.1.2:22
```

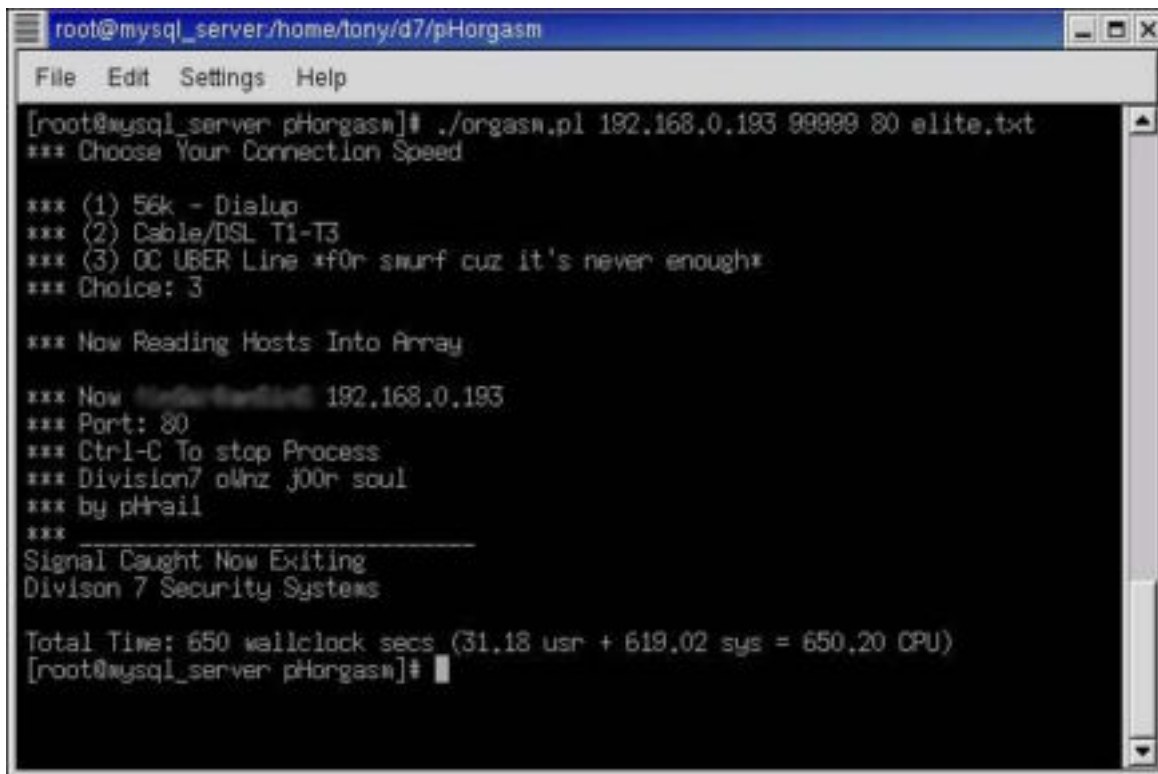
```
Testing if remote sshd is vulnerable # ATTACH NOW
```

After the attack is started, it will prompt you to make an SSH connection to the device under test. If the Cisco PIX was affected, you could not make a connection, and possibly cause it to crash and reboot. If it didn't work, there are 44 other possible targets that the program can attack. Unfortunately, I don't have a PIX firewall to test this on. I would continue to research for exploits concerning the PIX firewall, experimenting when possible.

4.3 Distributed Denial of Service Attack

In the Denial of Service Attack (DDoS) attack, we are simulating that we have 50 compromised cable modems under our control. The DDoS attack will be utilizing Orgasm v 1.0. This program is classified as a Distributed Reflection Denial of Service attack. The attacking machine has a list of known servers that all have the same port open. In our scenario, we will be listing web servers. Each cable modem will initiate a connection to web servers from a designated list of web servers, but spoofing the source address with that of the GIAC target. When the web server receives the spoofed SYN request, it sends a SYN-ACK back to what it thought was the originating IP address. The SYN-ACK packets are sent to the target, effectively using up all the ISP bandwidth to that web site. The following excerpt is from Steve Gibson's paper on Distributed Reflection Denial of Service (DRDoS), "Malicious SYN packets were being "Reflected" off innocent bystanding TCP servers. Their SYN/ACK responses were being used to flood and attack our bandwidth." (13)

Each of our 50 cable modems will each have an original list of valid web servers. The lists can easily be achieved by listing known accessible websites, or scanning the Internet for servers running port 80. Once each cable modem has been configured, all we have to do is run the attack.



```
root@mysql_server/home/tony/d7/phorgasm
File Edit Settings Help
[root@mysql_server phorgasm]# ./orgasm.pl 192.168.0.193 99999 80 elite.txt
*** Choose Your Connection Speed
*** (1) 56k - Dialup
*** (2) Cable/DSL T1-T3
*** (3) OC UBER Line *f0r smurf cuz it's never enough*
*** Choice: 3
*** Now Reading Hosts Into Array
*** Now Reading Hosts 192.168.0.193
*** Port: 80
*** Ctrl-C To stop Process
*** Division7 oMnZ j00n soul
*** by phrail
***
Signal Caught Now Exiting
Division 7 Security Systems

Total Time: 650 wallclock secs (31.18 usr + 619.02 sys = 650.20 CPU)
[root@mysql_server phorgasm]#
```

Figure 61

Figure 61 illustrates the attack finished. The syntax is as follows:

```
#./orgasm.pl 192.168.0.193 99999 80 elite.txt
```

```
<target> <loops> <port> <server list>
```

192.168.0.193 IP address of web server at GIAC.com

99999 Loops - number of times repeated

80 Designates the source port used to initiate contact from the list of servers.

Elite.txt List of web servers.

It will then prompt you to choose your connection speed:

```
*** Choose Your Connection Speed
*** (1) 56k - Dialup
*** (2) Cable/DSL T1-T3
*** (3) OC UBER Line *f0r smurf cuz it's never enough*
*** Choice: 3
```

At the time of the screen shot in Figure 61, we were on a test network. A more appropriate selection would have been 2 for Cable/DSL T1-T3. “2” represents the type of connection for our cable modems. From there, the program initiates the connections.

```
*** Now Reading Hosts Into Array  
  
*** Now XxXxXxXxXxXx 192.168.0.193  
*** Port: 80  
*** Ctrl-C To stop Process  
*** Division7 oWnz j00r soul  
*** by pHrail
```

The Xx's make this paper suitable for all audiences. This gives us 2500 possible reflectors that will send SYN-ACK traffic to our target destination. Whether or not the PIX 515E stops the attack is irrelevant. If each cable modem carried out their attacks at the same time, this would theoretically saturate GIAC's T1.

4.3.1 Countermeasures

Simply adding a rule to your firewall will not mitigate these attacks. The pro's and con's are detailed in the paper. Mr. Gibson suggests a more practical solution:

“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.” (22-23)

For more details about attack, I would suggest reading the Distributed Reflection Denial of Service paper by Steve Gibson (see References for details).

4.4 Internal System Attack

Using Social Engineering, we could try to infiltrate GIAC's internal LAN. How many times have you received an AOL CD in the mail? The method attempted will be along the same lines. We will attempt to attack the perimeter from the inside out.

4.4.1 Finding a Target

To find an unwitting victim, we will have to do a little legwork. To start, we could go to the GIAC website. Good places to start are Contact Us links and employment/career links. Look for any information that would help us.

- Names

- Phone Numbers
- Addresses
- Email Addresses
- External Links

A web page can be a wealth of information. For this case, we can say that the email provided on the website was xxxx@giac.com. Once we have the domain name, we could go to samspade.org to get more information. Our purpose of using the samspade website is to run “giac.com” through the many queries that are available at the web page. There are several interfaces for doing a whois search, use the one your most familiar with.

The information provided can normally supply a mailing address and a Point of Contacts for that particular domain. If we find a name, simply type it into a search engine. You’ll be surprised what you can come up with. (Go ahead and search for yourself). Once you get a few email addresses, you could search the newsgroups for occurrences of that particular user, or just the domain name. In this scenario, we’ll simulate that the POC found on the whois was also found posting several newsgroups for both security newsgroups and a few recreational groups. We will refer to this person as the “target”.

Next, we could post answers to the target’s questions and establish a level of trust. The more you answer the target’s questions; eventually they will trust you for technical information. (Or whatever newsgroup you are interacting in). Once that level of trust is established, we can begin to supply CD’s that cater to the target’s interest. The CD could be run on a PC inside the corporate firewall or on the targets laptop at home. (Where does your network go?) The CD provided would contain a Trojan Program that could potentially provide a covert link into the target machine.

4.4.2 Countermeasures

Concerning the whois Listings: provide a nameless generic email account.

Media: It would be extremely easy to establish a procedure to scan all media before using them on company computers. That same policy should also be in use at home. If the target had children, who knows what the kids are downloading.

Education: It’s also important to educate the users. An occasional threat demo will go along way.

All the security equipment in the world won’t prevent an un-educated user from bypassing all security measures. (Convenience over Security) It’s much easier to appeal to someone’s interest than it is to perform a technical penetration.

References

Antoine, Vanessa, Patricia Bosmajian, Daniel Duesterhaus, Michael Dransfield, Brian Eppinger, James Houser, Andrew Kim, Phyllis Lee, David Opitz, Michael Wiacek, Mark Wilson, Neal Ziring: National Security Agency 's Security Configuration Guide "*Router Security Guidance Activity of the System and Network Attack Center (SNAC)*", Report Number: C4-054R- 00. Version 1.0k March 25, 2002.

Astaro Online Help: Version 3.208. 2002
Definitions: Services Definitions-Online Help
HTTP Proxy: Proxies-HTTP-Online Help
SMTP Relay: Proxies-SMTP Relay Online Help
CA Management: IPsec VPN-CA Management Online Help
Policies: IPsec VPN Policies Online Help
Connections: IPsec VPN Connections Online Help

"Building a Rule Base: Module Two." *Defense In-Depth Day 3: SANS' Track Two*. SANS Institute.

Center for Internet Security Benchmark Version 1.1 For Cisco IOS Routers. April 2002. URL: http://www.cisecurity.org/brnch_cisco.html (31 August 2002).

Cisco Security Advisory: Multiple SSH Vulnerabilities.
<http://www.cisco.com/warp/public/707/SSH-multiple-pub.html>. (4 September 2002).

Firewall Plugins: SMTP Antivirus Filter. Nessus Program Version 1.2.5

Gibson, Steve: "DRDoS: Distributed Reflection Denial of Service".
<http://grc.com/dos/drdo.htm> (4 September 2002).

Ng, Sam: "How to make a sniffing (receive only) UTP cable".
http://www.geocities.com/samngms/sniffing_cable/index.htm (31 August 2002)

"Securing the Internet" *Astaro Security Linux (Product Flyer)*. Germany: Astaro, 2002.

"Security Advisory: Scanning for SSH Can Cause a Crash".
<http://www.cisco.com/warp/public/707/SSH-scanning.shtml> (4 September 2002).

"SSH Sentinel: Usage." SSH Sentinel FAQ's. 2002.
URL: <http://www.ssh.com/faq/index.cfm?id=1101> (31 August 2002).

User Manual for Astaro Security Linux 3.2. 18 July 2002.

x2 Exploit: Packet Storm Website. <http://packetstorm.decepticons.org/0204-exploits>. (4 September 2002).

© SANS Institute 2000 - 2002, Author retains full rights.

Tools

Ethereal: <http://www.ethereal.com>

Nessus: <http://www.nessus.org>

nmap: <http://www.insecure.org>

Orgasm: <http://packetstorm.decepticons.org/distributed/d7-pH-orgasm.tgz>

x2: <http://packetstormsecurity.org/0204-exploits/x2.tgz>

© SANS Institute 2000 - 2002, Author retains full rights.