



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.

Table of Contents.....	1
Lorna_Hutcheson_GCFW.doc.....	2

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

GIAC ENTERPRISES

“FORTUNES FOR THE FUTURE”

By: Lorna J. Hutcheson

Practical Assignment Version: 1.5e



Table of Contents

<u>Assignment 1: GIAC Enterprises Security Architecture Overview</u>	1
<u>Information Requirements</u>	1
<u>GIAC Infrastructure</u>	1
<u>Information Gathering</u>	1
<u>Overall Design</u>	1
<u>IP Addressing Scheme</u>	3
<u>Components Used</u>	3
<u>Border Router</u>	3
<u>Brand</u>	3
<u>Version</u>	3
<u>Implementation</u>	4
<u>Primary Firewall</u>	4
<u>Brand</u>	4
<u>Version</u>	4
<u>Implementation</u>	4
<u>Internal Router</u>	4
<u>Brand</u>	4
<u>Version</u>	4
<u>Implementation</u>	4
<u>U.S. Marketing Firewall</u>	5
<u>Brand</u>	5
<u>Version</u>	5
<u>Implementation</u>	5
<u>International Firewall</u>	5
<u>Brand</u>	5
<u>Version</u>	5
<u>Implementation</u>	5
<u>Server Firewall</u>	5
<u>Brand</u>	5
<u>Version</u>	5
<u>Implementation</u>	5
<u>Storage Area Network (SAN)</u>	6
<u>Brand</u>	6
<u>Version</u>	6
<u>Implementation</u>	6
<u>VPN</u>	6
<u>Brand</u>	6
<u>Version</u>	6
<u>Implementation</u>	6
<u>Intrusion Detection System (IDS)</u>	6
<u>Brand</u>	6
<u>Version</u>	6
<u>Implementation</u>	7
<u>Access Methods</u>	7
<u>Customers</u>	7
<u>Suppliers</u>	7
<u>Partners</u>	7
<u>Assignment 2: GIAC Enterprises Security Policy</u>	8
<u>Overview</u>	8
<u>Security Guidelines</u>	8

<u>Security Policies</u>	8
<u>Extreme Networks Switch Overview</u>	8
<u>IP Access Lists</u>	8
<u>Routing Access Policies</u>	8
<u>Border Router</u>	9
<u>Services and Protocols</u>	9
<u>ACL Implementation</u>	9
<u>Test Procedures</u>	11
<u>Primary Firewall</u>	12
<u>Services and Protocols</u>	12
<u>Rule Set Implementation</u>	12
<u>Host Configuration</u>	13
<u>Rule Set Creation</u>	15
<u>Needed Hosts and rules configuration</u>	17
<u>Test Procedures</u>	18
<u>Internal Switch Summit7i</u>	20
<u>Services and Protocols</u>	20
<u>ACL Implementation</u>	20
<u>Test Procedures</u>	22
<u>U.S. Marketing Firewall</u>	22
<u>Services and Protocols</u>	22
<u>Rule Set Implementation</u>	22
<u>Test Procedures</u>	23
<u>International Firewall</u>	24
<u>Services and Protocols</u>	24
<u>Rule Set Implementation</u>	24
<u>Test Procedures</u>	25
<u>Server Firewall</u>	26
<u>Services and Protocols</u>	26
<u>Rule Set Implementation</u>	26
<u>Test Procedures</u>	27
<u>VPN</u>	27
<u>Services and Protocols</u>	27
<u>Host/VPN creation</u>	27
<u>Filter Implementation</u>	35
<u>Multiple firewalls and VPNs</u>	36
<u>Test Procedures</u>	36
<u>Assignment 3: GIAC Enterprises Security Audit Procedures</u>	37
<u>Overview/Goals</u>	37
<u>Assessment Plan</u>	37
<u>Assessment Implementation</u>	38
<u>Firewall Security Policy Audit</u>	38
<u>Access Control Policy</u>	38
<u>Network Service Access Control Policy</u>	38
<u>Operating System Security Audit</u>	39
<u>Firewall Security Audit</u>	43
<u>Assessment Results</u>	46
<u>Assignment 4: Design Under Fire</u>	48
<u>Overview</u>	48
<u>Perimeter Security Recon</u>	48

<u>Firewall Attack</u>	49
<u>Setting the stage</u>	49
<u>The attack</u>	49
<u>DOS Attack</u>	50
<u>Internal System Compromise</u>	50
<u>Citation of Sources</u>	51

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

Assignment 1: GIAC Enterprises Security Architecture Overview

Information Requirements

GIAC Enterprises is a rapidly growing Internet startup company and as such has many concerns and needs. One of the major overall concerns is security. With their business being Internet based and starting out a small business, the need to get it right the first time is weighing heavy on everyone's mind. After all, this is the opportunity of a lifetime. It is important to design a security plan that protects them now and allows for expansion in the future. It is realized that initial costs may be high, but worth it in the long run. The following areas were causes of concern: customer access; suppliers being able to drop off their "fortunes for the future"; and their overseas partners who translate and then sale their cookies.

GIAC Infrastructure

Information Gathering

It is very important that the very first thing done when designing anything is information gathering. You have to understand and know the entire functionality of the system. If you don't know and understand this, chances are you will create a design that will not meet the overall security needs of the company or provide them with a way to expand. In essence, you will design yourself into a corner. Keep in mind the company hired you as the security expert. While they may know the basics of what needs to be protected, they are looking to you to validate this and ensure their company really is protected. The following are a sample of key questions to ask:

1. What does the organizational chart of the company look like? Who needs to talk to whom?
2. What is the current network design? What is already in place (servers, cabling, fiber, routers etc.).
3. What do they expect to look like in the next five years? Expansion is inevitable, and you need to know this to meet their growing needs.

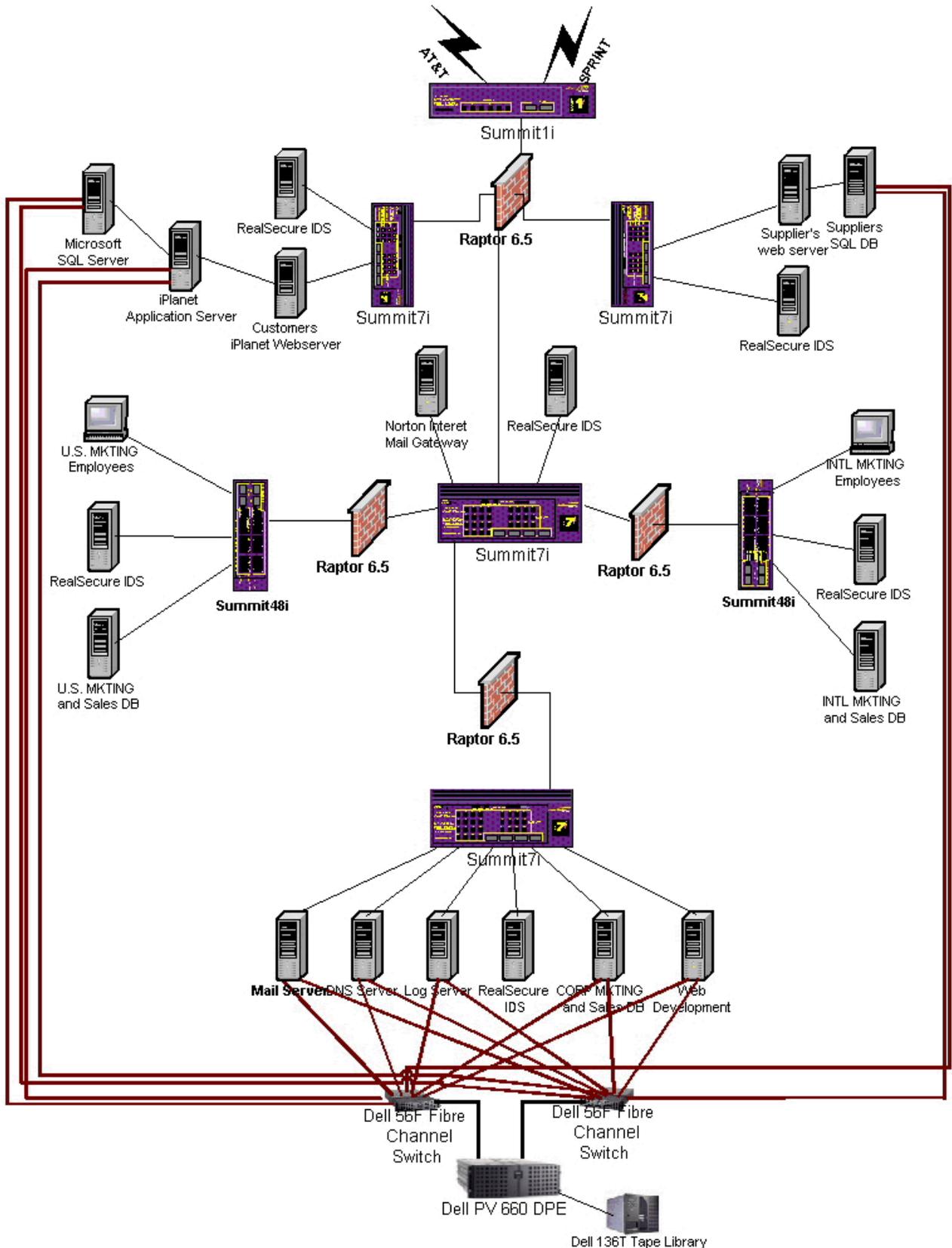
These are only a few of the questions that need to be answered to provide them with a secure system, capable of expanding. For the purposes of this exercise, these two assumptions have been made:

1. Their small Internet business network will not meet the growing needs of the newly merged Enterprise.
2. Expansion in the future is going to be at an explosive rate.

Overall Design

The following diagram in [Figure 1](#) shows the overall network design with security features implemented. Each of these features will be discussed later in greater depth. The design was developed to meet the requirements of GIAC Enterprises and to allow for growth and

Figure 1 expansion in the future. Security needs not expressly stated by the company



were taken into consideration.

IP Addressing Scheme

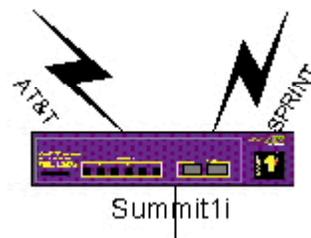
The following addressing scheme will be used in this design. The routable IP addresses are fictitious.

- Border Router:
External Interface: 153.27.210.10/24
- Primary Firewall:
External Interface: 153.27.38.20/24
Internal Interface: 153.27.39.10/24
Suppliers Services Network: 172.16.20.5/24
Customers Services Network: 172.16.21.5/24
- Corporate Internal Router:
External Interface: 153.27.39.15/24
- U.S. Marketing Firewall:
External Interface: 153.27.39.25/24
Internal Interface: 172.16.22.5/24
- International Firewall:
External Interface: 153.27.39.20/24
Internal Interface: 172.16.23.5/24
- Server Firewall:
External Interface: 153.27.39.30/24
Internal Interface: 172.16.24.5/24

Components Used

Border Router

In order to assure customers have access to the web site, two different ISPs will be used. One will be the primary ISP and the second ISP will be the backup. If one ISP goes down for any reason, connectivity will be maintained through the second ISP. The following diagram shows the two connections.



Brand

Extreme Networks was chosen for the border router. In order to meet the growing needs of GIAC Enterprises, Extreme Networks offers Gigabit throughput and implements layer

2 and layer 3 capabilities at wire speed.

Version

The Summit1i switch was chosen for the border router. It has many security features and offers full layer 2 and layer 3 capabilities.

Implementation

The Summit1i will be implemented using ACLs to help filter out the “bad” traffic and help control access at a high level. It also utilizes RADIUS and SSH2 for added management security and/or user authentication.

Primary Firewall

Brand

The Symantec Enterprise Firewall (formally Raptor) was chosen for the primary firewall. It is a proxy firewall, with great flexibility to perform other functions.

Version

The version to be used is 6.5. This latest version not only provides the same great protection and diverse functionality of the previous versions, but also improves upon the GUI interface and makes managing and configuring easier.

Implementation

The firewall will be implemented using rules to control traffic in and out of the corporate network as well as the services network. The proxy capabilities of the firewall will also be used. The firewall will have four NICs installed in it: external, internal, suppliers’ services network and customers’ services network.

Internal Router

Brand

Extreme Networks was chosen again for the internal router. Since Extreme Networks offers Gigabit throughput and implements layer 2 and layer 3 capabilities at wire speed, it also makes it the perfect internal router to handle the growing needs of GIAC Enterprises corporate headquarters.

Version

The Summit7i switch was chosen for the internal router. It has many security features and offers full layer 2 and layer 3 capabilities.

Implementation

The Summit7i will be implemented using ACLs to help filter out the “bad” traffic and help control access at a high level. It also utilizes RADIUS and SSH2 for added management security and/or user authentication. It also allows for easy expansion to

meet the needs of GIAC Enterprises growing company.

U.S. Marketing Firewall

Brand

The Symantec Enterprise Firewall (formally Raptor) was chosen for the U.S. Marketing firewall.

Version

The version to be used is 6.5. This latest version not only provides the same great protection and diverse functionality of the previous versions, but also improves upon the GUI interface and makes managing and configuring easier.

Implementation

The firewall will be implemented using rules to control traffic in and out of the U.S. Marketing division. The proxy capabilities of the firewall will also be used. The firewall will have two NICs installed in it an external and an internal interface.

International Firewall

Brand

The Symantec Enterprise Firewall (formally Raptor) was chosen for the primary firewall. It is a proxy firewall, with great flexibility to perform other functions.

Version

The version to be used is 6.5. This latest version not only provides the same great protection and diverse functionality of the previous versions, but also improves upon the GUI interface and makes managing and configuring easier.

Implementation

The firewall will be implemented using rules to control traffic in and out of the International Marketing Division. The proxy capabilities of the firewall will also be used. The firewall will have two NICs installed in it an external and an internal interface.

Server Firewall

Brand

The Symantec Enterprise Firewall (formally Raptor) was chosen for the primary firewall. It is a proxy firewall, with great flexibility to perform other functions.

Version

The version to be used is 6.5. This latest version not only provides the same great

protection and diverse functionality of the previous versions, but also improves upon the GUI interface and makes managing and configuring easier.

Implementation

The firewall will be implemented using rules to control traffic in and out of the server farm. The proxy capabilities of the firewall will also be used. The firewall will have two NICs installed in it an external and an internal interface.

Storage Area Network (SAN)

Brand

Dell was chosen as the SAN for its ability to provide back up capabilities and eliminate the need for down time.

Version

The Dell PV660 DPE was chosen for the SAN. There will be two Dell 56F Fibre Channel switches used and a Dell 136T Tape Library.

Implementation

The SAN will be implemented to provide redundancy security. All servers will have two interface cards installed for the SAN. Each server will connect to each switch to ensure the path is always present. The Suppliers Database, iPlanet Application Server and Microsoft SQL Server will connect to the SAN. Security will be implemented by using zoning and other features of the SAN.

VPN

Brand

The Symantec Enterprise Firewall also offers VPN capabilities and will be used as the VPN device for the Suppliers and International partners.

Version

The version used will be 6.5 as mentioned above. This allows for multiple encryption capabilities.

Implementation

The VPN will be implemented using filters and different encryption algorithms. The ability for users in one department to safely VPN to another department as permitted and with encryption provides for greater internal security. Rules will be used to control access as well. The International Partners and suppliers will be using Raptor Mobile on their laptops. Our International partners will be using Symantec Enterprise Firewalls as well.

Intrusion Detection System (IDS)

Brand

Internet Security Systems (ISS) RealSecure was chosen as the IDS.

Version

The version to be used is 6.0.

Implementation

The IDS will be customized to each location for what it is to detect. The ability to tailor the IDS makes it more effective for detecting malicious attempts or unauthorized network usage. It will be implemented on each segment of the network (See [Figure 1](#))

Access Methods**Customers**

Customers will have access to only the web server. They will be coming in using HTTPS. This will be enforced by rules set up on the firewall. They will access the web server and using iPlanet's e-commerce suite, will have a secure method of conducting business.

Suppliers

Suppliers will come in and access a secure web server, which will require them to authenticate before gaining access. User accounts will be created and they will only see their necessary information.

Partners

Partners will gain access by means of raptor mobile and a nested VPN tunnel to the International Marketing Subnet. Any other access to other areas in GIAC Enterprises will require authorization.

Assignment 2: GIAC Enterprises Security Policy

Overview

Security Guidelines

The primary rule of thumb is to be secure enough to protect the company, but still allow them to complete their mission. Only those protocols needed to complete the mission will be allowed through. Customers will be allowed access only to the Customer services network. Suppliers will be allowed into both the customer and the supplier services network. Any access into GIAC Enterprises will be by means of a VPN and then only to those resources that are required. Within GIAC Enterprises, access will be granted only to those resources required by the employees. **ENSURE NO MODEMS ARE ALLOWED TO BE USED FROM INSIDE GIAC ENTERPRISES.** If modems are required it is by request and on a stand-alone machine. Modems introduce a backdoor into a network.

Security Policies

Extreme Networks Switch Overview

The Extreme switches have two different ways of controlling traffic. Traffic can be controlled with IP access lists and/or Routing Access Policies. QoS can also be implemented in conjunction with these, but will not be address at this time.

IP Access Lists

IP access lists are created and assigned a name. You can create each list and then apply the rules to it. Access lists are processed sequentially, however precedence numbers can be applied which causes the access lists to be processed in order with the highest precedence being 1. You can have precedence numbers from 1-25,600. The maximum number of rules with precedence established is 255. Rules can be created that overlap if using precedence numbers. **HOWEVER, rules without precedence numbers that overlap rules with precedence numbers with be discarded.** To add a rule, you simple have to assign a unique name and a precedence number if you are using them. To modify an entry, you have to delete it and then retype it or create a new entry and delete the old. It is important to note that a default rule has to be established for each access list to govern what to do if it doesn't match an entry. **If there is no default rule and the packet does not match an access list, the packet will be forwarded. Default rules should be created last because you will lock your self out of the switch if you do not have the correct access in first.** This can be fixed with a reboot, however you will lose all of your changes that have not been saved. ICMP packets can have access lists, but only are effective if used in conjunction with routing access policies.

Routing Access Policies

Routing access policies are used to control what the switch passes. You have the option

of three types of profile modes: permit, deny and none. Permit allows you to enter any permit operation. Any operation not found on this list is denied. Deny allows any deny operation. Any operation no found on this list is permitted. None allows a combination of both permit and deny. Any operation not found on this list is denied. There is no need for a default profile due to the nature of the routing access profile. Sequence numbers can also be used with each profile entry.

Border Router

This device is not the primary source of security and will not be used as such. Its purpose is to help filter out blatant network traffic, known security vulnerabilities and noise that should not be there. The border router will be configured using ACLs to determine how to handle traffic coming into the switch. Only those protocols required will be allowed through. All private IP addresses will be denied. The only IP address allowed to be routed to will be that of the Primary Firewall. Any unnecessary network traffic noise will be filtered out. Any IP address, in the future, determined to be performing questionable activity will be denied access. All ICMP packets coming into the switch from the ingress port will be controlled on a needed basis. You can allow or deny what you want based on an ICMP type and code of 0–255. The switch will also be configured to disable any access to it except for direct connection. The Extreme Networks line of products configures the same across the board for all devices running the same version code.

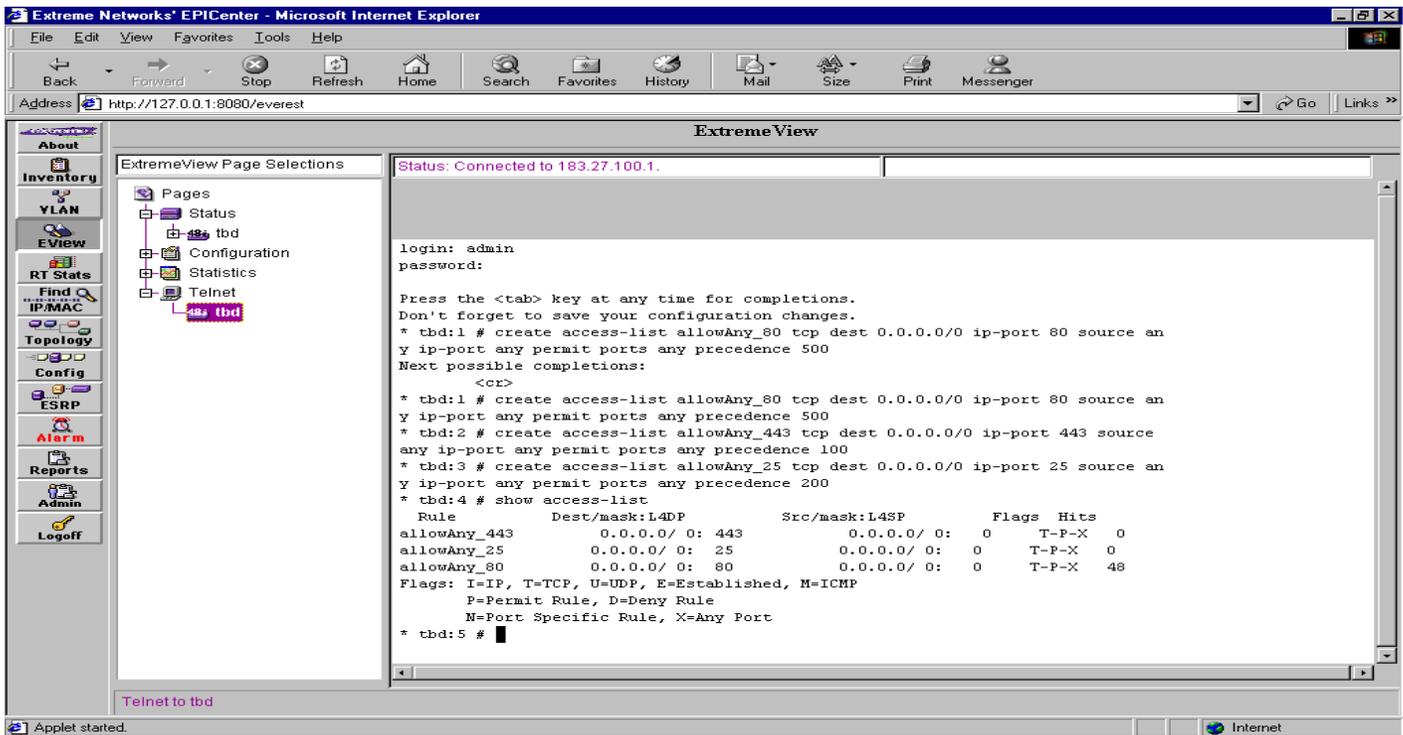
Services and Protocols

The protocols that will be allowed to pass to the GIAC Enterprises primary firewall will be further defined in the implementation section.

ACL Implementation

The following shows the commands to implement the above security policy. Remember, do your default rules last and save your configuration. [Figure 2](#) shows the actual implementation if you were to configure the device. Only a few of the commands are shown, just to give you an idea of Extreme Network's EPICenter.

Figure 2



1. To create your security configuration for access control, use the following commands:

Create access-list denyTelnet_23 tcp dest 153.27.38.20/32 ip-port 23 source any ip-port any deny ports any precedence 100 log
(Denies any telnet session to the firewall's external interface and logs it)

Create access-list denyFTP_21 tcp dest 153.27.38.20/32 ip-port 21 source any ip-port any deny ports any precedence 200 log
(Denies any FTP sessions to the firewall's external interface it and logs it)

Create access-list denyRTR ip dest 153.27.210.10/32 ip-port any source any ip-port any deny ports any precedence 300 log
(Denies any attempt to connect to the router and logs it)

Create access-list denyPing icmp dest 153.27.210.10/32 source any type 8 code 0 deny
(Denies any attempt to ping the router. You cannot set a precedence on ICMP)

Create access-list denyPrivate_10TF tcp dest any source 10.0.0.0/8 deny precedence 20
(Denies tcp from private addresses)

Create access-list denyPrivate_10UF udp dest any source 10.0.0.0/8 deny precedence 21

(Denies udp from private addresses)

```
Create access-list denyPrivate_172TF tcp dest any source 172.16.0.0/12 deny
precedence 22
```

(Denies tcp from private addresses)

```
Create access-list denyPrivate_172UF udp dest any source 172.16.0.0/12 deny
precedence 22
```

(Denies udp from private addresses)

```
Create access-list denyPrivate_192TF tcp dest any source 192.168.0.0/16 deny
precedence 23
```

(Denies tcp from private addresses)

```
Create access-list denyPrivate_192UF udp dest any source 192.168.0.0/16
deny precedence 24
```

(Denies udp from private addresses)

```
Create access-list denyPrivate_10TT tcp dest 10.0.0.0/8 source any deny
precedence 25
```

(Denies tcp from private addresses)

```
Create access-list denyPrivate_10UT udp dest 10.0.0.0/8 source any deny
precedence 26
```

(Denies udp from private addresses)

```
Create access-list denyPrivate_172TT tcp dest 172.16.0.0/12 source any deny
precedence 27
```

(Denies tcp from private addresses)

```
Create access-list denyPrivate_172UT udp dest 172.16.0.0/12 source any deny
precedence 28
```

(Denies udp from private addresses)

```
Create access-list denyPrivate_192TT tcp dest 192.168.0.0/16 source any deny
precedence 29
```

(Denies tcp from private addresses)

```
Create access-list denyPrivate_192UT udp dest 192.168.0.0/16 source any deny
precedence 30
```

(Denies udp from private addresses)

```
Create access-list allowFW ip dest 153.27.38.20/32 source any permit ports
any precedence 500
```

(allows all other IP traffic to pass to the firewall)

2. Create the default rule for each of the following: IP, TCP, UDP, and ICMP as needed:

```
Create access-list denyFW ip dest 0.0.0.0/0 source 0.0.0.0/0 deny ports any
```

(Denies traffic, other than to the firewall. Remember this is the default rule, do not

set the precedence)

Test Procedures

The ability to test and ensure it does what is has configured to do is simple and straightforward. The access list is not large. You can take a machine outside the primary firewall, and after receiving permission to test the configuration, make attempts do the following:

1. Ping the router
2. Ping the firewall
3. Telnet into the firewall
4. Telnet into the router
5. FTP into the firewall
6. FTP into the router
7. Attempt any connection into the router
8. Plug directly into the router and use Nmap or some other tool that will generate IP address and generate those private IP address denied by the list and ensure they are denied
9. Attempt to pass other normal traffic through the router and ensure it is routed

Primary Firewall

Services and Protocols

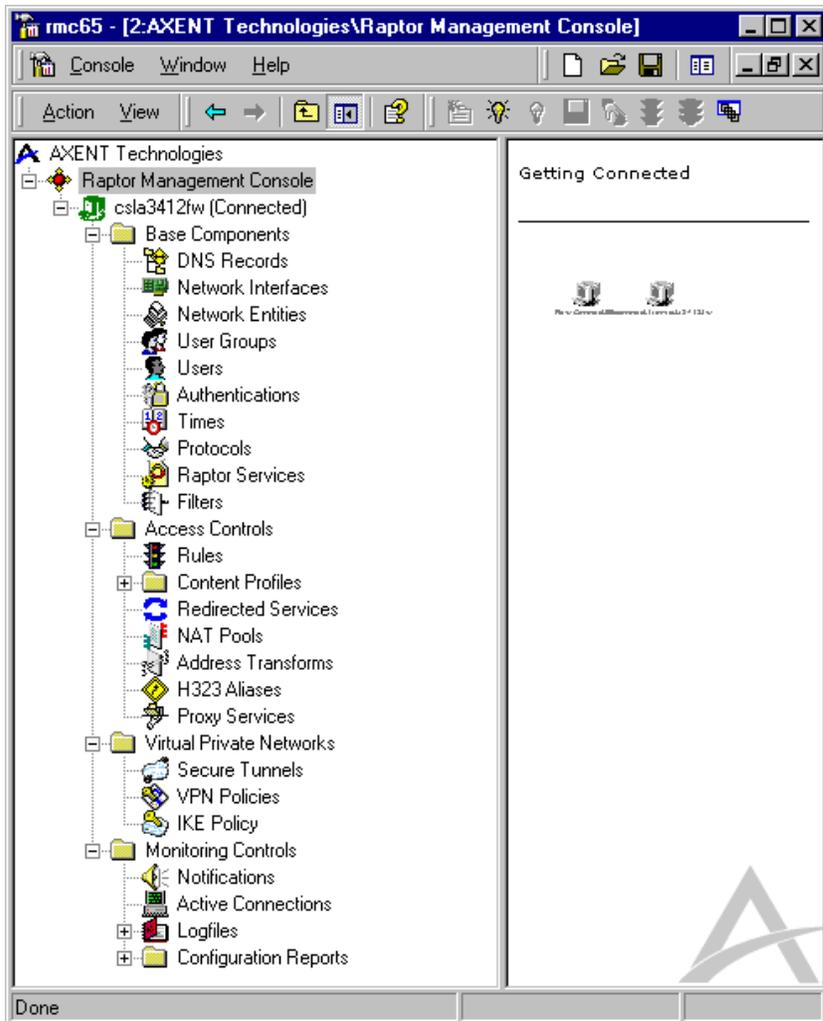
Only those services and protocols that are needed will be used. The major services that are needed are DNS, Mail, and Internet access. All other functionality will be performed through a VPN. VPNs will be discussed in a separate section.

Rule Set Implementation

The rule set implemented will be done on a Symantec Enterprise Firewall (formally Raptor) 6.5. All references to this firewall from here on out will be shortened to Raptor. The OS (WindowsNT) has been properly secured using several references including NSA, SANS and DISC4. (Due to restrictions, only references to SANS in the documentation will exist.) The Raptor system itself has a vulture service running which kills anything not needed by the Firewall and WindowsNT. Since it is impossible to configure the firewall to accurately represent the entire organizational needs, only the major areas and security requirements will be addressed. Raptor has many functionalities imbedded into its design. To give you and idea of its capabilities, here is a screen shot of its capabilities ([Figure 3](#)).

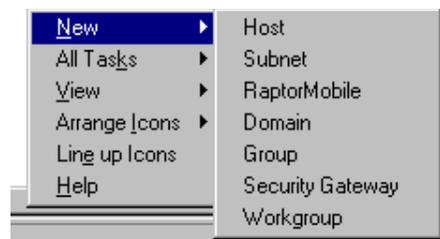
Figure 3

The Raptor firewall supports as many NICs as the OS on which it resides. Using NT we can use five NICs. For our scenario, we will be using all five NICs. Two will be external, one will be our internal network and two will be services networks. By using two external NICs we can use two different ISPs and ensure we have connection to the outside world. For our scenario, we will be showing configuration for one NIC, but all rules will apply to both.



Host Configuration

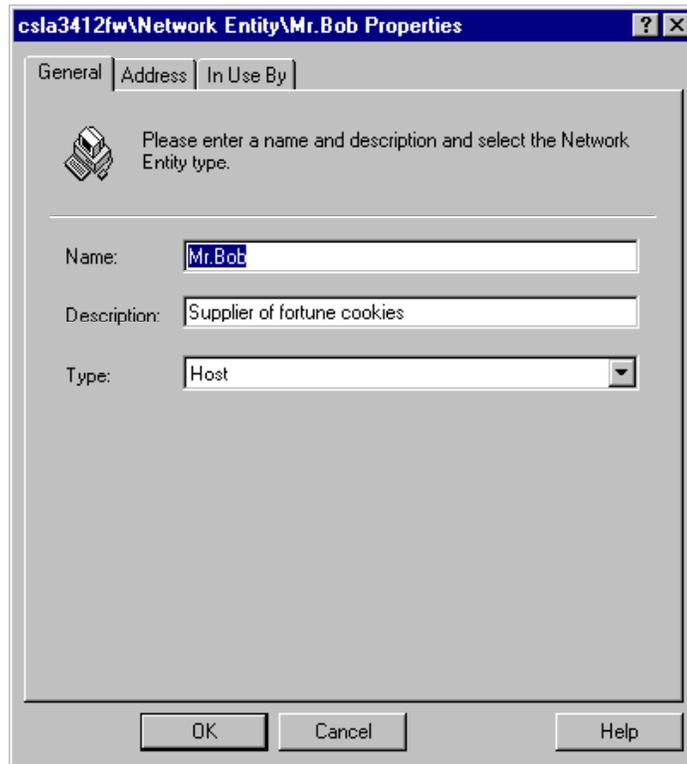
The first thing needed to start configuring your firewall is to create the necessary entities. Raptor uses these entities to identify different machines, subnets, gateways etc.



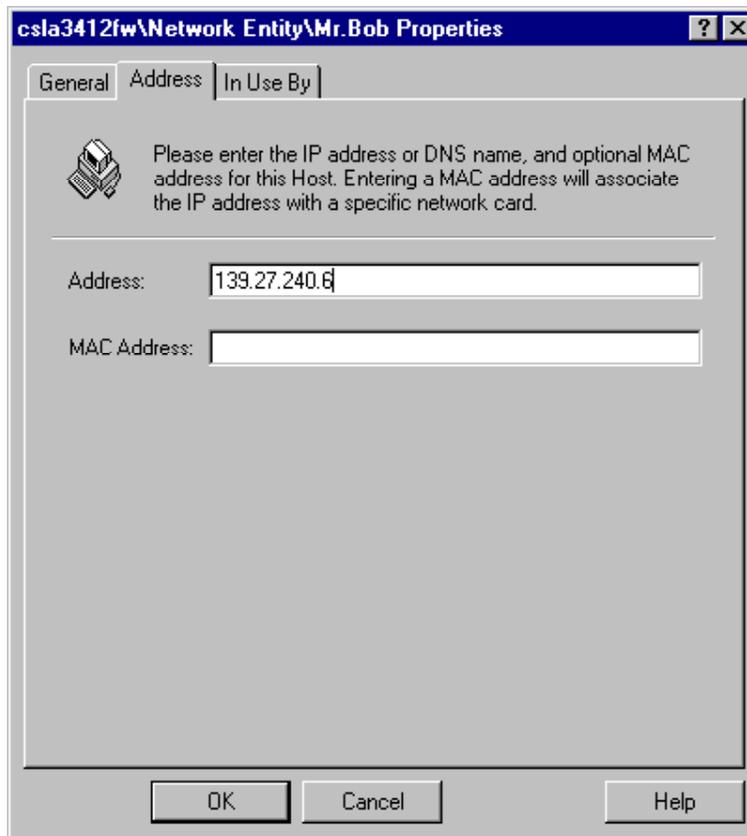
We need to create host entities for each supplier that will be accessing our network. We also need to create host entities for each firewall external NIC and each machine to which users, suppliers, and our partners will require access. This includes E-mail and DNS. To create a host entity, the following steps are needed.

- 1) Under Base Components, go to the network entities tab and right click. Select new and then host.
- 2) Type in the name you wish to give to the entity, a description (this should be explicit

as it will make identify different hosts easier as you start to have several) and the type of entity this is.



- 3) Click the Address tab and fill in the IP address of the machine you are adding a host entry for and an optional MAC address for added security. Then press OK.

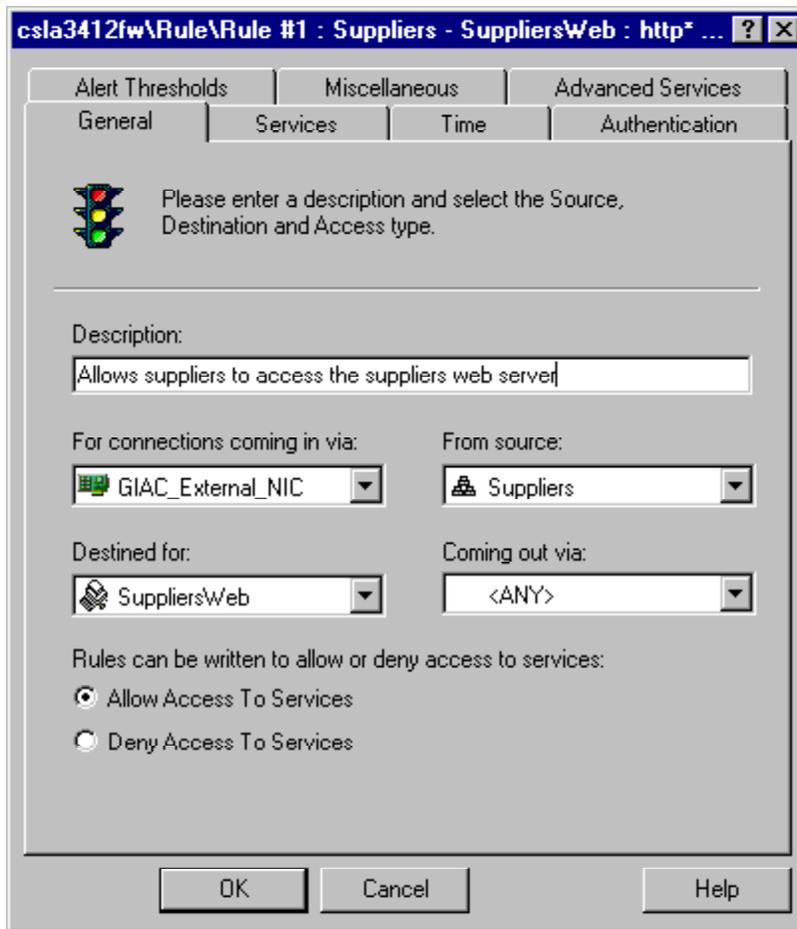


- 4) The next step is to configure your groups. These are important, as it will reduce the number of rules that you have to write. Instead of configuring a rule for each supplier, we will create a single group that will allow all suppliers access to the suppliers services network. You create this the same way as you would for steps 1 and 2 above. Instead of step 3 above, you would click the members tab and add those entities to it that will be included in the group.

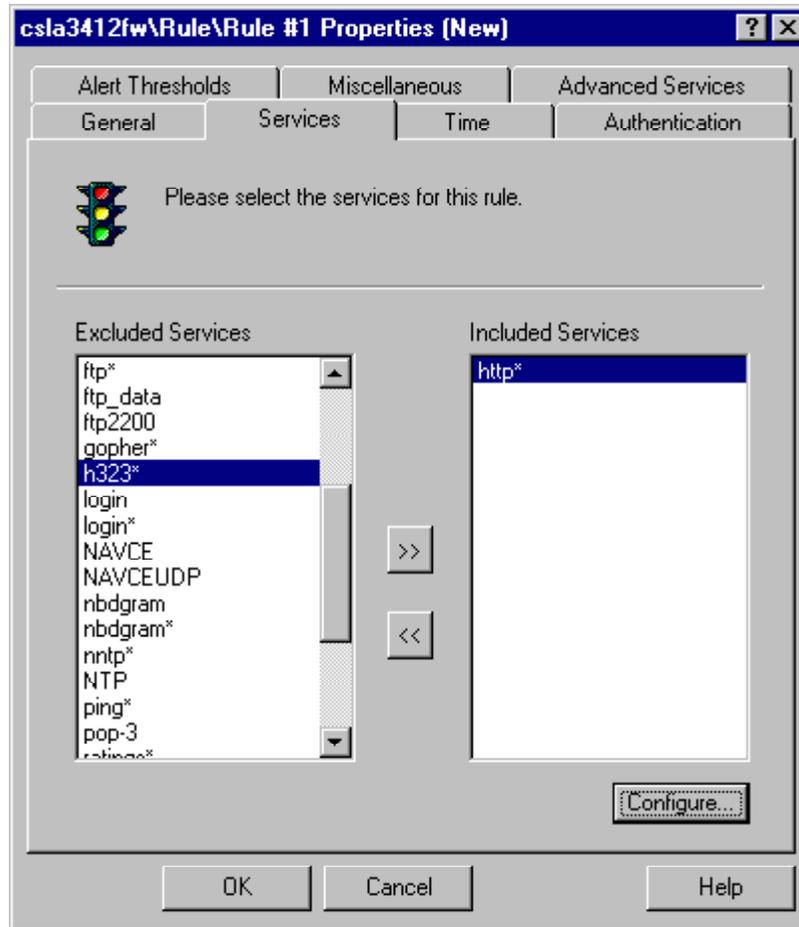
Rule Set Creation

The creation of rules is simple in Raptor. To create a rule, follow the following steps:

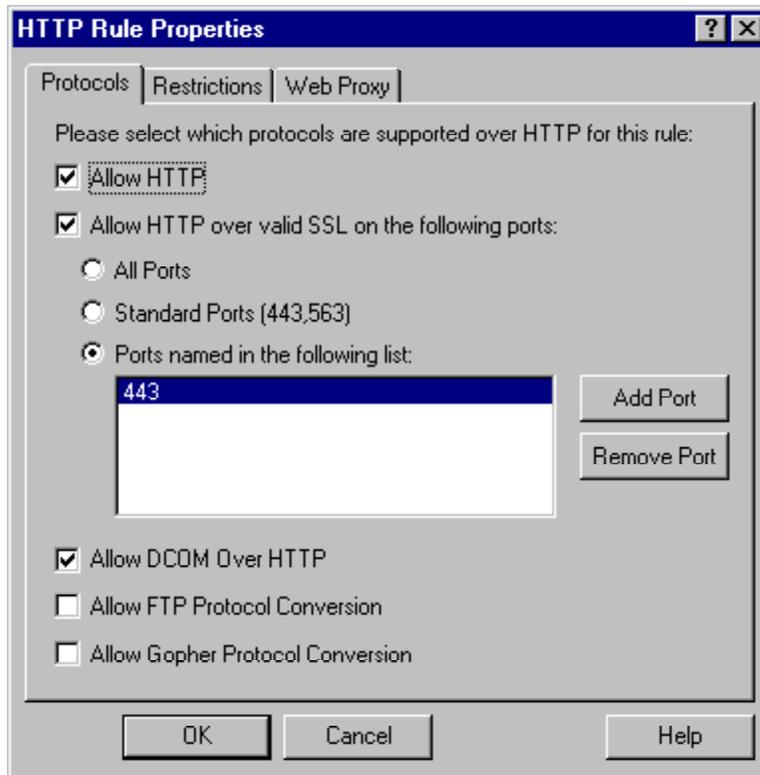
- 1) Under access controls, select rules and then right click. You want to select new and rule to create a new rule.
- 2) You need to fill out the following: Add a very useful and explicit description. Determine how your connections will be coming in to your network that this rule is going to control. We are going to configure the suppliers' rule here. We want the connection to be from the External NIC (Remember, you will have two external interfaces to configure rules for access) The From Source box will contain Network entities that you have created. I already created a group for the suppliers and used it. Then select what your source is destined for. I have a host created for the suppliers' web server. And the connections out via are for where you expect to see the connections returning from. ANY was used here to show one of the options, the correct configuration would be from the suppliers services network interface.



- a) Then you click the services tab to determine which services this rule will allow through. We are going to allow HTTP and then configure the HTTP service. (NOTE: Raptor has several proxy services that allow easier configuration. Ensure the HTTP proxy service is enabled in the Raptor in the Access Control proxy service.



- b) Push the configure button to configure the HTTP service. The * at the end of http denotes it is the raptor built in service. Here you can configure the necessary options for HTTP. We are also allowing SSL on the service to the standard port 443. After configuring, you will push OK twice to accept the rule. (NOTE: No changes to the firewall are accepted until after you save and reconfigure the firewall)



Needed Hosts and rules configuration

Because the interface to Raptor is a GUI interface, I have demonstrated how easy it is to create a host and to add a rule. The following list shows all Entities and rules required by the firewall. Screen shots will not be used here on out due to space requirements. The previously defined steps show how to create all hosts and rules. By default, anything not specifically allowed will be denied. This means you need to watch your firewall closely for the need few weeks to ensure everything functions as possible. We will discuss how to do an audit in the next section, however, an audit may not show complete functionality as a normal user would.

Entities required:

1. Each supplier configured with IP and MAC address (optional, but preferred to prevent spoofing) defined as a host entity
2. A entity configured as a group with each supplier as a member
3. The suppliers' web server
4. The customers' web server
5. The Norton Mail gateway
6. Private address space configured as a subnet
7. Private address space group
8. All internal firewall's external interface
9. Internal Router IP
10. Group containing 8 and 9 above

11. Exchange server configured as a host

Rules Required:

1. Rule for suppliers to access web server: Connection in: External NIC; From Source: suppliers group; Destined for: suppliers' web server; coming out: any (Service HTTP and HTTPS)
2. Rule for customers to access the customer web server: Connection in: External NIC; From Source: universe; Destined for: customers' web server; coming out: any (Service HTTP and HTTPS)
3. Rule for employees to access the customer web server: Connection in: Internal NIC; From Source: universe; Destined for: customers' web server; coming out: any (Service HTTP and HTTPS)
4. Rules for E-mail coming in: Raptor has a built in SMTP wizard that will configure your email access for you. It can be modified after creation. It creates all necessary hosts and a rule for mail in and one for mail out. Ensure the mail server is specified as the Norton Mail Gateway IP address. You have to modify the rule for mail going out and change it to be the host entity of the exchange server.
5. Rule for employees to use the Internet: Connection in: Internal NIC; From Source: universe; Destined for: universe; coming out: any (Service HTTP and HTTPS)
6. Rule to deny private IPs in: Connection in: External NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)
7. Rule to deny private IPs out: Connection in: Internal NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)
8. Rule to deny Internal IPs coming in from the outside: Connection in: External NIC; From Source: Internal IPs; Destined for: universe; coming out: any (explicit deny access)

(NOTE: No Rule for DNS is required as we are allowing the primary firewall to act as the DNS proxy. All DNS requests go to it and it goes and gets them for the users.)

Additional rules need to be created to determine who has FTP privileges, Telnet privileges, files that can be downloaded etc. Raptor has a vast ability to tighten security. The primary focus here was customers, suppliers and internal user's basic functions. VPNs will be addressed in a separate function.

Test Procedures

Rules Required:

1. Rule for suppliers to access web server: **TEST:** Contact a random sampling of suppliers and have them attempt to connect. Monitor the firewall event log to ensure what is happening. Have a few non-authorized users attempt to

- attach and see what happens. **REASON:** This ensures that suppliers have correct access to their web page and no one else does.
2. Rule for customers to access the customer web server: **TEST:** Have a few employees of the network team attempt access from their home machines and monitor the event log. Also attempt a secure session and ensure encryption takes place. **REASON:** This ensures that customers can get to their web pages. You would want to test both paths from each ISP and also test the both rules sets for this. Ensure DNS is configured for both IP addresses. Test the encryption to be sure it is functioning.
 3. Rule for employees to access the customer web server: **TEST:** Have a few employees of the network team attempt access from their office machines and monitor the event log. Also attempt a secure session and ensure encryption takes place. **REASON:** This ensures that employees can get to their web pages. You would want to test both paths from each ISP and also test the both rules sets for this. Ensure DNS is configured for both IP addresses. Test the encryption to be sure it is functioning.
 4. Rules for E-mail coming in/out: **TEST:** Have a random number of users from each department attempt to send email and have some suppliers and international partners attempts to send email. Monitor the firewall log, Norton Mail Gateway log and Exchange server to verify routes. **REASON:** This ensures Email can get to and from everywhere it is suppose to. This is very important as companies tend to do all work electronically these days.
 5. Rule for employees to use the Internet: **TEST:** Have users from inside each department attempt to access the Internet. Monitor events in the firewall log. **REASON:** This ensures that all users can get out to the Internet. This is important since traffic is coming from behind multiple firewalls.
 6. Rule to deny private IPs in: **TEST:** Attempt to send spoofed IP packets from the Border Router to the firewall. The border router should drop them before they ever arrive. **REASON:** RFC1918 governs the use of Private Address Space. These address spaces are not supposed to be forwarded or routed by any means. It is very important that these are dropped. Also, since private IP addresses are in use behind the firewall, it helps to ensure spoofing doesn't occur.
 7. Rule to deny private IPs out: **TEST:** Attempt to send spoofed IP packets from the internal router to the firewall. The internal router should drop them before they ever arrive. **REASON:** RFC1918 governs the use of Private Address Space. These address spaces are not supposed to be forwarded or routed by any means. It also ensures that the firewalls are proxying like they are supposed to do.
 8. Rule to deny Internal IPs coming in from the outside: **TEST:** Send a spoofed IP packet to the outside interface of the firewall with the source being the internal IP addresses. Monitor the firewall logs for actions taken. **REASON:** This is key because we only have five routable internal IP addresses and we want to make sure those don't appear as sources coming in from the outside

interface.

Internal Switch Summit7i

This device is not the primary source of security and will not be used as such. The purpose is to help control network traffic and ensure only the gateways to each of the subnets are used. The internal router will be configured using ACLs to determine how to handle traffic coming into the switch. All private IP addresses will be denied to ensure nothing gets out passed the firewall due to a misconfiguration or other attempts. The only IP addresses allowed to be routed to will be that going to the external interfaces of the firewall. All others will be sent out the default gateway, which is the internal interface of the firewall. Any unnecessary network traffic noise will be filtered out. All ICMP packets coming into the switch will be controlled on a needed basis.

Services and Protocols

The protocols that will be allowed to be routed will be further defined in the implementation section.

ACL Implementation

1. To create your security configuration for access control, use the following commands:

Create access-list denyTelnet_23 tcp dest 153.27.39.10/32 ip-port 23 source any ip-port any deny ports any precedence 100 log
(Denies any telnet session to the primary firewall's internal interface and logs it)

Create access-list denyTelnet_231 tcp dest 153.27.39.25/32 ip-port 23 source any ip-port any deny ports any precedence 110 log
(Denies any telnet session to the U.S. marketing firewall's external interface and logs it)

Create access-list denyTelnet_232 tcp dest 153.27.39.20/32 ip-port 23 source any ip-port any deny ports any precedence 120 log
(Denies any telnet session to the International firewall's external interface and logs it)

Create access-list denyTelnet_233 tcp dest 153.27.39.30/32 ip-port 23 source any ip-port any deny ports any precedence 130 log
(Denies any telnet session to the server firewall's external interface and logs it)

Create access-list denyFTP_21 tcp dest 153.27.39.10/32 ip-port 21 source any ip-port any deny ports any precedence 200 log
(Denies any FTP sessions to the firewall's internal interface and logs it)

Create access-list denyFTP_211 tcp dest 153.27.39.25/32 ip-port 21 source any ip-port any deny ports any precedence 210 log
(Denies any FTP sessions to the U.S. marketing firewall's external interface and logs it)

Create access-list denyFTP_212 tcp dest 153.27.39.20/32 ip-port 21 source any ip-port any deny ports any precedence 220 log
(Denies any FTP sessions to the International marketing firewall's external interface and logs it)

Create access-list denyFTP_213 tcp dest 153.27.39.30/32 ip-port 21 source any ip-port any deny ports any precedence 230 log
(Denies any FTP sessions to the server firewall's external interface and logs it)

Create access-list denyRTR ip dest 153.27.39.15/32 ip-port any source any ip-port any deny ports any precedence 300 log
(Denies any attempt to connect to the router and logs it)

Create access-list denyPrivate_10T tcp dest any source 10.0.0.0/8 deny precedence 20
(Denies tcp from private addresses)

Create access-list denyPrivate_10U udp dest any source 10.0.0.0/8 deny precedence 21
(Denies udp from private addresses)

Create access-list denyPrivate_172T tcp dest any source 172.16.0.0/12 deny precedence 22
(Denies tcp from private addresses)

Create access-list denyPrivate_172U udp dest any source 172.16.0.0/12 deny precedence 22
(Denies udp from private addresses)

Create access-list denyPrivate_192T tcp dest any source 192.168.0.0/16 deny precedence 23
(Denies tcp from private addresses)

Create access-list denyPrivate_192U udp dest any source 192.168.0.0/16 deny precedence 24
(Denies udp from private addresses)

Create access-list allowFW ip dest 153.27.39.10/32 source any permit ports any precedence 500
(allows all other IP traffic to pass to the primary firewall)

Create access-list allowFWU ip dest 153.27.39.25/32 source any permit ports any precedence 600
(allows all other IP traffic to pass to the U.S. marketing firewall)

Create access-list allowFWI ip dest 153.27.39.20/32 source any permit ports any precedence 700
(allows all other IP traffic to pass to the International firewall)

Create access-list allowFWS ip dest 153.27.39.30/32 source 0.0.0.0/0 permit ports any precedence 800

(allows all other IP traffic to pass to the Server firewall)

3. Create the default rule for each of the following: IP, TCP, UDP, and ICMP as needed:

None is created for this router as all other traffic will be sent to the primary firewall's inside interface which is the router's default gateway.

Test Procedures

The test procedures for the internal router are the same as for the primary router. The access list is not large. You can take a machine and plug it directly into the router and after receiving permission to test the configuration, make attempts do the following:

1. Ping the router
2. Ping the firewall
3. Telnet into the firewall
4. Telnet into the router
5. FTP into the firewall
6. FTP into the router
7. Attempt any connection into the router
8. Plug directly into the router and use Nmap or some other tool that will generate IP address and generate those private IP address denied by the list and ensure they are denied
9. Attempt to pass other normal traffic through the router and ensure it is routed

U.S. Marketing Firewall

The purpose of this firewall is to protect and segregate the U.S. Marketing side of GIAC Enterprises from the rest of GIAC Enterprises. To help ensure security, no one should have access to information they do not have a need to know. The firewall will be configured similar to the one above. All machines need to be configured with their gateway on their NICS pointing to their Firewall's internal NIC.

Services and Protocols

The main services that will be needed are Internet access, E-mail and DNS.

Rule Set Implementation

Because of the amount of space required to screen shot each step, I am going to just list the entities and the rules required. For exact steps to configure an entity or a rule, please see the instructions under rule implementation for the primary firewall.

Entities required:

1. The customers' web server
2. The Norton Mail gateway
3. Private address spaces configured as a subnet
4. Private address space group

5. All internal firewall's external interface
6. Group containing 5 above
7. Exchange server as a host

Rules Required:

1. Rule for employees to access the customer web server: Connection in: Internal NIC; From Source: universe; customers web server; coming out: any (Service HTTP and HTTPS) (redirection will be set up)
2. Rules for E-mail coming in: Raptor has a built in SMTP wizard that will configure your email access for you. It can be modified after creation. It creates all necessary hosts and a rule for mail in and one for mail out. Ensure the mail server is specified as the Norton Mail Gateway IP address. Modify the rule in and use the source as the Microsoft exchange server
3. Rule to allow login to the Microsoft exchange server: Connection in: Internal NIC; From Source: universe; Destined for: Microsoft exchange server; coming out: any
4. Rule for employees to use the Internet: Connection in: Internal NIC; From Source: universe; Destined for: universe; coming out: any (Service HTTP and HTTPS)
5. Rule to deny private IPs in: Connection in: External NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)
6. Rule to deny private IPs out: Connection in: Internal NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)

Additional rules need to be created to determine who has FTP privileges, Telnet privileges, files that can be downloaded etc. VPNs will be to access any other portion of GIAC Enterprises to which a user has the permissions to access. The VPN will be firewall to firewall. Configuration of this will be handled in the VPN section.

Test Procedures

Rules Required:

1. Rule for employees to access the customer web server: **TEST:** Have a few employees of the network team attempt access from their home machines and monitor the event log. Also attempt a secure session and ensure encryption takes place. **REASON:** This ensures that employees can get to their web pages. Test the encryption to be sure it is functioning.
2. Rules for E-mail coming in/out: **TEST:** Have a random number of users from in the department attempt to send email and have some suppliers attempt to email to the Marketing employees and have employees in other departments attempt to send email. Monitor the firewall log, Norton Mail Gateway log and Exchange server to verify routes. **REASON:** This ensures

Email can get to and from everywhere it is suppose to. This is very important as companies tend to do all work electronically these days.

3. Rule for employees to use the Internet: **TEST:** Have users in the U.S. Marketing department attempt to access the Internet. Monitor events in the firewall log of both department and primary firewall. **REASON:** This ensures that all users can get out to the Internet. This is important since traffic is coming through multiple firewalls.
4. Rule to deny private IPs in: **TEST:** Attempt to send spoofed IP packets from the internally to the firewall and vice versa. The internal router should drop them before they ever arrive. **REASON:** RFC1918 governs the use of Private Address Space. These address spaces are not supposed to be forwarded or routed by any means. It is very important that these are dropped. Also, since private IP addresses are in use behind the firewall, it helps to ensure spoofing doesn't occur.
5. Rule to deny private IPs out: **TEST:** Attempt to send spoofed IP packets from the internal network to the firewall. The firewall should drop them as they arrive. **REASON:** RFC1918 governs the use of Private Address Space. These address spaces are not supposed to be forwarded or routed by any means. It also ensures that the firewalls are functioning properly.

International Firewall

The purpose of this firewall is to protect and segregate the International Marketing side of GIAC Enterprises from the rest of GIAC Enterprises. To help ensure security, no one should have access to information they do not have a need to know. The firewall will be configured similar to the one above. All machines need to be configured with their gateway on their NICS pointing to their Firewall's internal NIC.

Services and Protocols

The main services that will be needed are Internet access, E-mail and DNS.

Rule Set Implementation

Because of the amount of space required to screen shot each step, I am going to just list the entities and the rules required. For exact steps to configure an entity or a rule, please see the instructions under rule implementation for the primary firewall.

Entities required:

1. The customers' web server
2. The Norton Mail gateway
3. Private address spaces configured as a subnet
4. Private address space group
5. All internal firewall's external interface
6. Group containing 5 above
7. Exchange server as a host

Rules Required:

1. Rule for employees to access the customer web server: Connection in: Internal NIC; From Source: universe; customers web server; coming out: any (Service HTTP and HTTPS) (redirection will be set up)
2. Rules for E-mail coming in: Raptor has a built in SMTP wizard that will configure your email access for you. It can be modified after creation. It creates all necessary hosts and a rule for mail in and one for mail out. Ensure the mail server is specified as the Norton Mail Gateway IP address. Modify the rule in and use the source as the Microsoft exchange server
3. Rule to allow login to the Microsoft exchange server: Connection in: Internal NIC; From Source: universe; Destined for: Microsoft exchange server; coming out: any
4. Rule for employees to use the Internet: Connection in: Internal NIC; From Source: universe; Destined for: universe; coming out: any (Service HTTP and HTTPS)
5. Rule to deny private IPs in: Connection in: External NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)
6. Rule to deny private IPs out: Connection in: Internal NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)

Additional rules need to be created to determine who has FTP privileges, Telnet privileges, files that can be downloaded etc. VPNs will be to access any other portion of GIAC Enterprises to which a user has the permissions to access. The VPN will be firewall to firewall. Configuration of this will be handled in the VPN section.

Test Procedures

Rules Required:

1. Rule for employees to access the customer web server: **TEST:** Have a few employees of the network team attempt access from their home machines and monitor the event log. Also attempt a secure session and ensure encryption takes place. **REASON:** This ensures that employees can get to their web pages. Test the encryption to be sure it is functioning.
2. Rules for E-mail coming in/out: **TEST:** Have a random number of users from in the department attempt to send email and have some suppliers attempt to email to the Marketing employees and have employees in other departments attempt to send email. Monitor the firewall log, Norton Mail Gateway log and Exchange server to verify routes. **REASON:** This ensures Email can get to and from everywhere it is suppose to. This is very important as companies tend to do all work electronically these days.
3. Rule for employees to use the Internet: **TEST:** Have users in the U.S.

Marketing department attempt to access the Internet. Monitor events in the firewall log of both department and primary firewall. **REASON:** This ensures that all users can get out to the Internet. This is important since traffic is coming through multiple firewalls.

4. Rule to deny private IPs in: **TEST:** Attempt to send spoofed IP packets from the internally to the firewall and vice versa. The internal router should drop them before they ever arrive. **REASON:** RFC1918 governs the use of Private Address Space. These address spaces are not supposed to be forwarded or routed by any means. It is very important that these are dropped. Also, since private IP addresses are in use behind the firewall, it helps to ensure spoofing doesn't occur.
5. Rule to deny private IPs out: **TEST:** Attempt to send spoofed IP packets from the internal network to the firewall. The firewall should drop them as they arrive. **REASON:** RFC1918 governs the use of Private Address Space. These address spaces are not supposed to be forwarded or routed by any means. It also ensures that the firewalls are functioning properly.

Server Firewall

The purpose of this firewall is to protect GIAC Enterprises resources.

Services and Protocols

Access to this firewall is severely restricted. Any thing requiring access into this server farm will be via VPN.

Rule Set Implementation

Because of the amount of space required to screen shot each step, I am going to just list the entities and the rules required. For exact steps to configure an entity or a rule, please see the instructions under rule implementation for the primary firewall.

Entities required:

1. Each RealSecure IDS
2. The Norton Mail gateway
3. Private address spaces configured as a subnet
4. Private address space group
5. All internal firewall's external interface
6. Group for all internal firewall's external interfaces
7. Primary firewall's internal interface
8. U.S. Marketing and Sales Database server
9. International Marketing and Sales Database Server
10. Management personnel as needed.
11. Server's as needed

Rules Required:

1. Rules for E-mail coming in: Connection in: External NIC; From Source: Norton Mail Gateway; Destined for: Exchange Mail Server; coming out: any (Service SMTP)
2. Rules for E-mail going out: Connection in: Internal NIC; From Source: Exchange Mail Server; Destined for: Primary Firewall's Internal Interface; coming out: any (Service SMTP)
3. Rule to allow user's to login to the exchange server: Connection in: External NIC; From Source: Firewall group; Destined for: Exchange server; coming out: any
4. Rule to deny private IPs in: Connection in: External NIC; From Source: Private IP group; Destined for: universe; coming out: any (explicit deny access)

Additional rules need to be created to determine who has FTP privileges, Telnet privileges, files that can be downloaded etc. The VPN will be firewall to firewall. Configuration of this will be handled in the VPN section.

Test Procedures

Rules Required:

1. Rule for employee's to log onto exchange server: **TEST:** Have user's attempt to login to the exchange server. **REASON:** Ensure the employee's accounts and permission's are established properly.
2. Rules for E-mail coming in/out: **TEST:** Have a random number of users from in the department attempt to send email and have some suppliers attempt to email to the Marketing employees and have employees in other departments attempt to send email. Monitor the firewall log, Norton Mail Gateway log and Exchange server to verify routes. **REASON:** This ensures Email can get to and from everywhere it is suppose to. This is very important as companies tend to do all work electronically these days.
3. Rule to deny private IPs in: **TEST:** Attempt to send spoofed IP packets from the internally to the firewall and vice versa. The internal router should drop them before they ever arrive. **REASON:** RFC1918 governs the use of Private Address Space. These address spaces are not supposed to be forwarded or routed by any means. It is very important that these are dropped. Also, since private IP addresses are in use behind the firewall, it helps to ensure spoofing doesn't occur.
4. Rule to deny private IPs out: **TEST:** Attempt to send spoofed IP packets from the internal network to the firewall. The firewall should drop them as they arrive. **REASON:** RFC1918 governs the use of Private Address Space. These address spaces are not supposed to be forwarded or routed by any means. It also ensures that the firewalls are functioning properly.

VPN

The Raptor Firewall offer's many functions, one of them being a built in VPN capability.

This offer's the ability to control traffic as one single point.

Services and Protocols

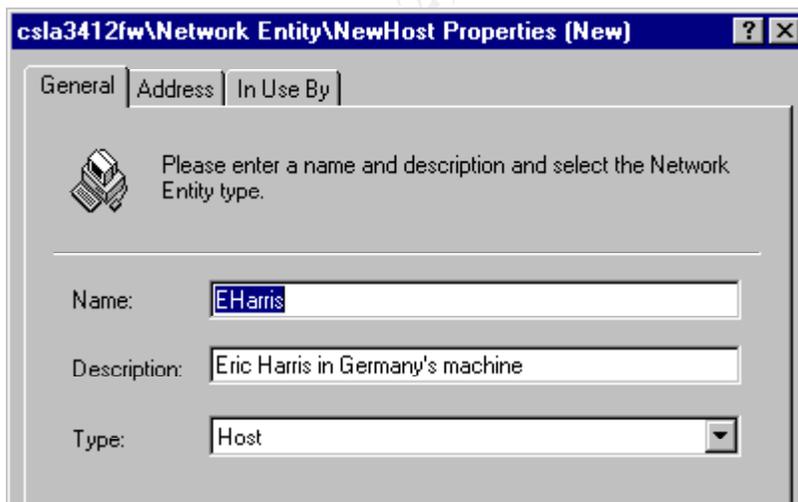
This will be controlled on an individual basis using filters.

Host/VPN creation

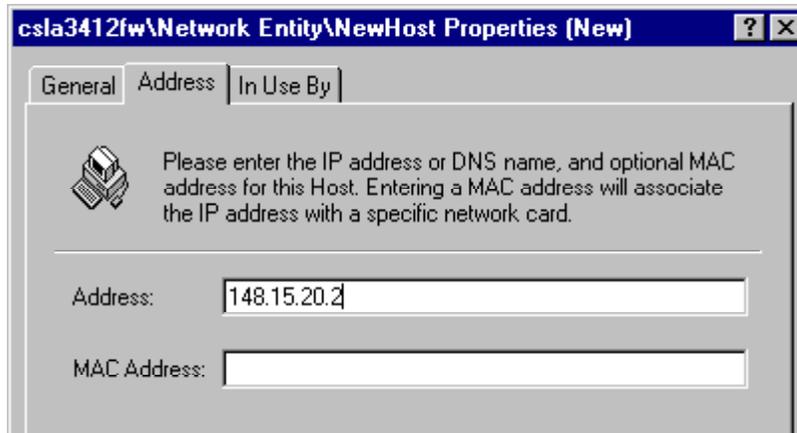
The steps to creating a VPN connection are simple in Raptor. The steps needed will be outlined here.

To create a VPN you have to have four different entities for each side of the VPN. You need an entity that will be your source, gateway for that source, destination gateway, and destination source. The exception to this is using Raptor Mobile where the source and source gateway are one and the same. Complete the steps in the following order:

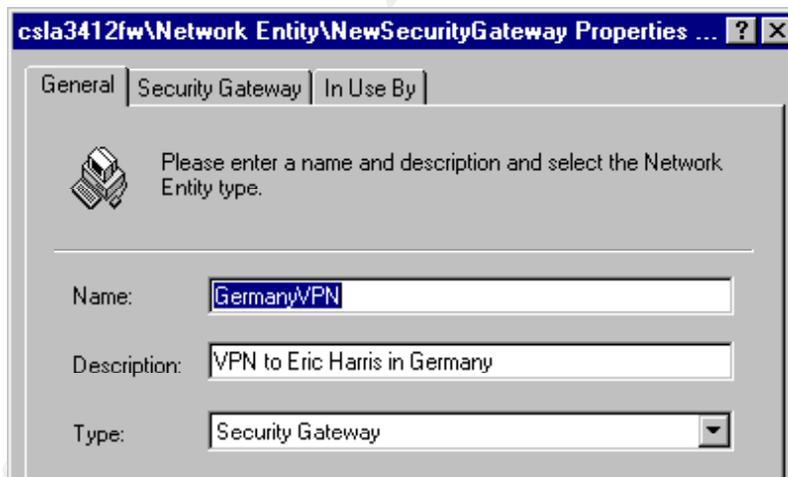
1. You have to create a source entity that is a host, group, subnet etc. For this example we are going to use just a host. Since our local host is already created, we will create one for the machine we are going to talk to over a VPN. First go to the Base Components and click on Network Entities. Then right click and choose host. Ensure it has a meaningful name and description and the type as host.



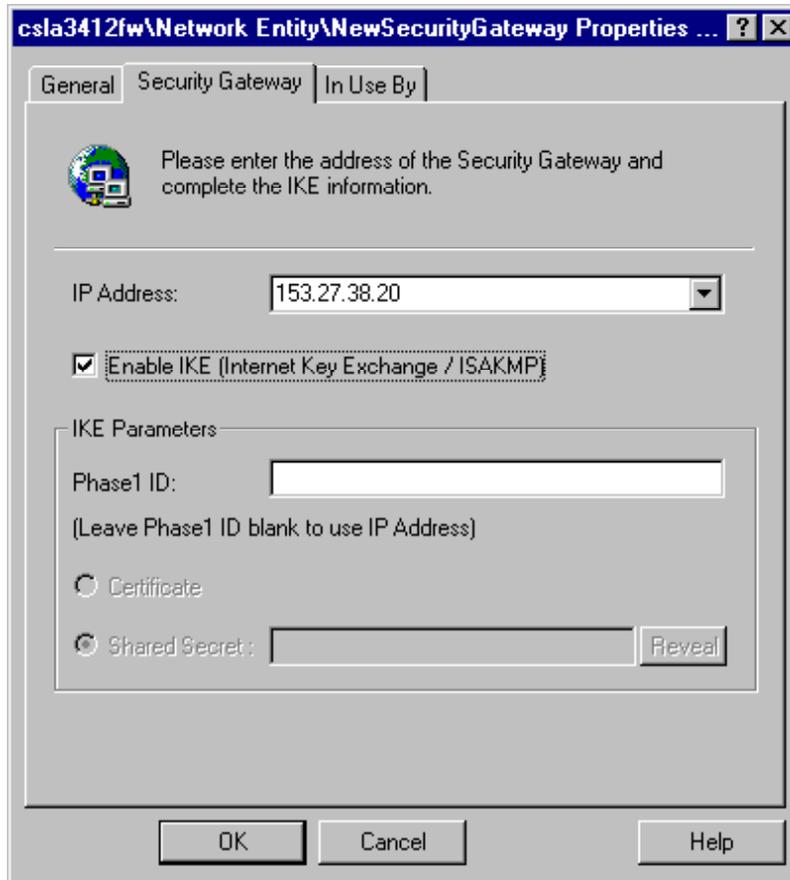
2. Then click on the address tab and enter the IP address of the machine you will be talking to (the MAC address is optional) and then click on enter.



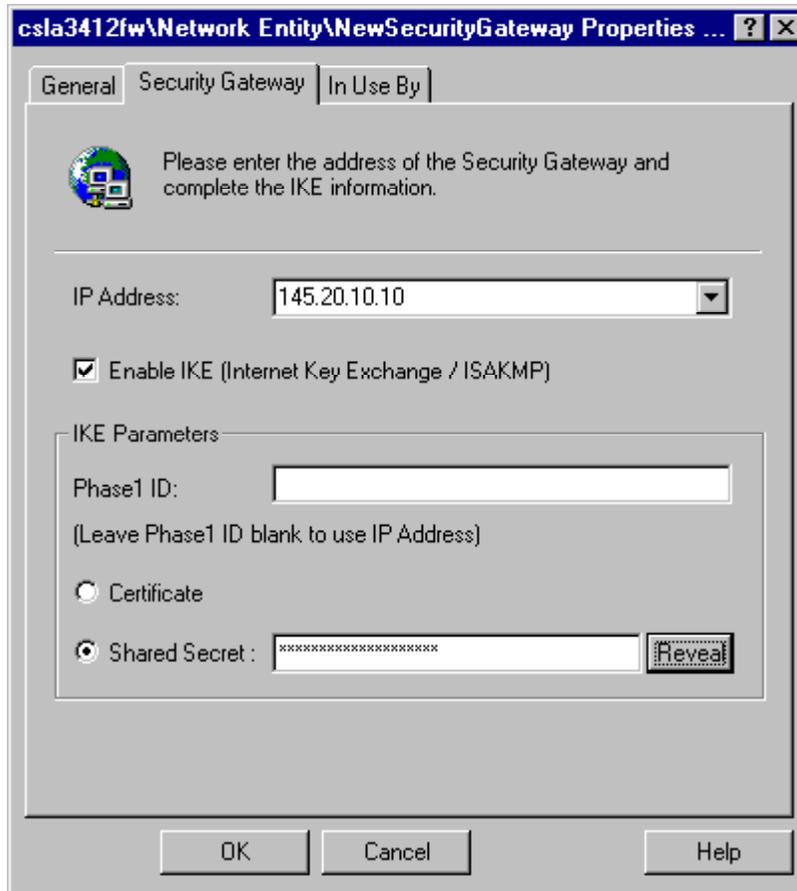
3. You now have to create the local and remote gateway. To create a gateway in the Network Entities right click and select Security Gateway. Give it a meaningful name and description. Ensure the type is Security Gateway.



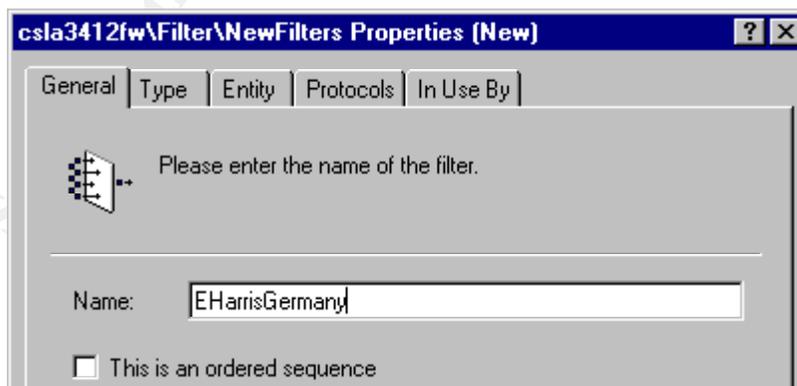
4. Click on the Security Gateway tab and select IP of the local external interface of the firewall. Enable the IKE button and then type in a password or leave blank.



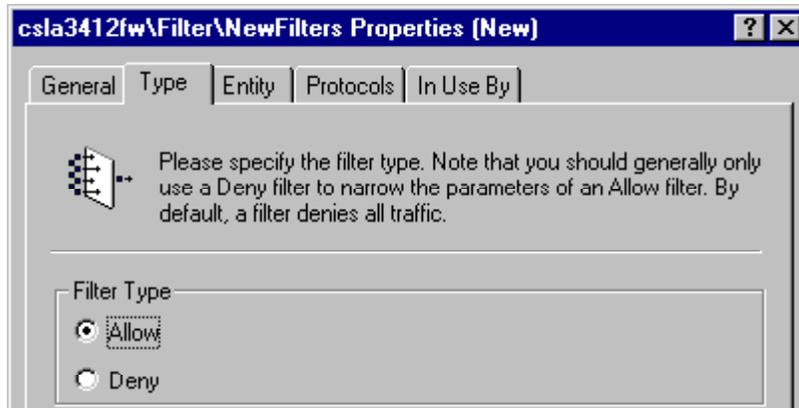
This creates the local gateway. Ensure you choose the outside interface of your firewall as the IP address. To create a remote gateway, repeat steps 3 and 4 above except TYPE IN the IP of the remote gateway, it will not be listed in the drop down box. Then click on the Shared Secret button. Whatever key is put in here has to be the same key typed in on the remote in. You can hide it or reveal as necessary.



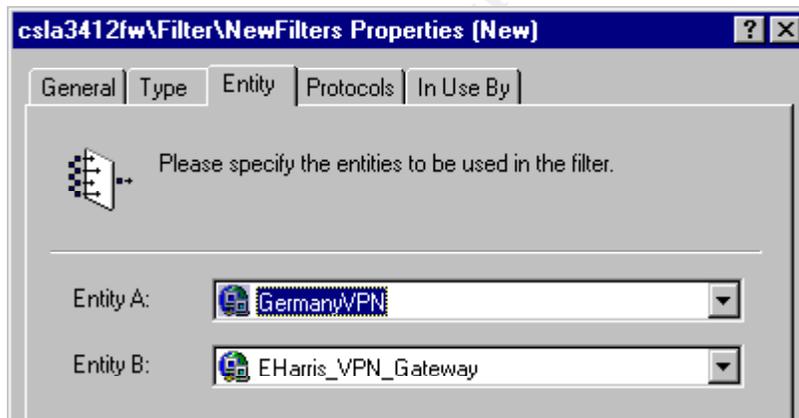
5. Now you need to create filters as required. To create a filter, go to the Base Components and select Filters, right click and select new. Give the filter a meaningful name. Select the ordered sequence button if multiple filters have been created and you want to use them here in a particular order.



6. Click on the type tab and select allow.

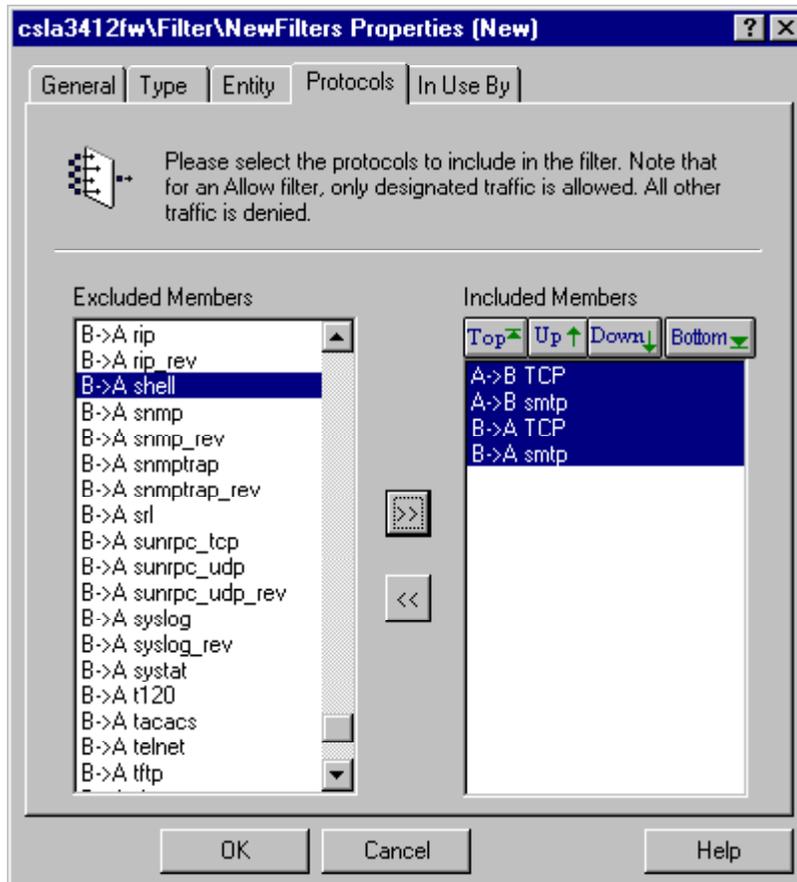


7. Click on the Entity tab and choose Entity A and Entity B to be used. I selected the Gateways so if more employees from that site want to come in, I can apply the filter to them if the same requirements are met. I used GermanyVPN as the name for my local gateway. Probably not the best here as it is confusing. Remember, MEANINGFUL Names!

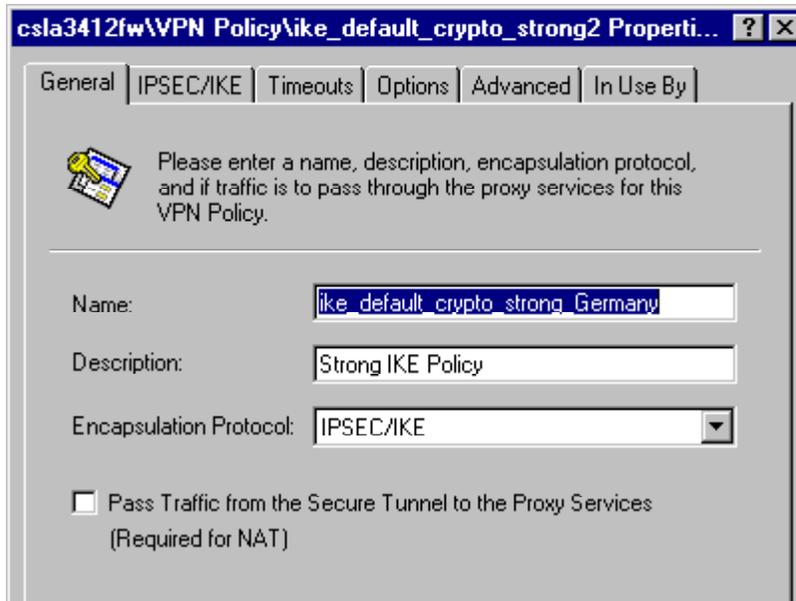


8. Click on the Protocols tab to select what is allowed to pass through the VPN. If

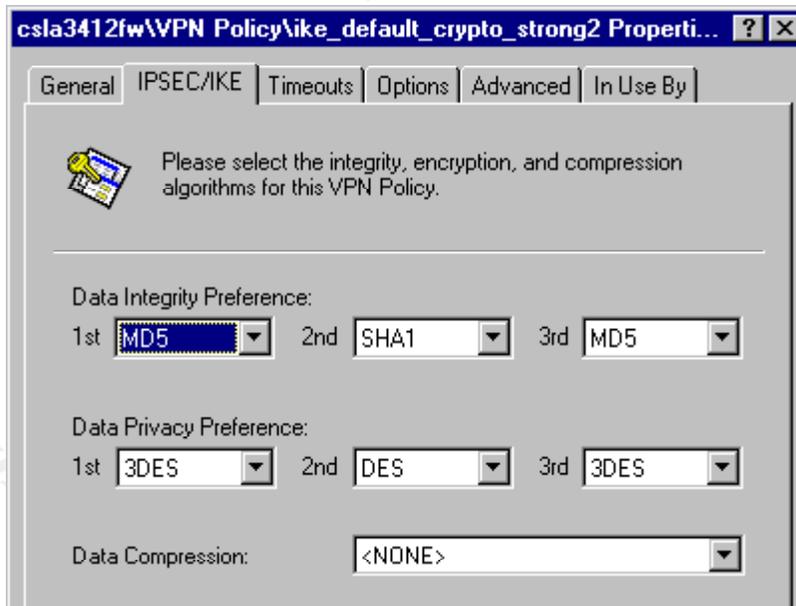
you only select A->B, Entity B will not be able to pass the same protocol back to A! It is very important to select which way you want protocols to pass, depending on what you are doing. Raptor will also let you define your own protocols if what you are looking for is not specified here. You can define the protocol by the type and what are the source and destination ports. After you are finished click OK.



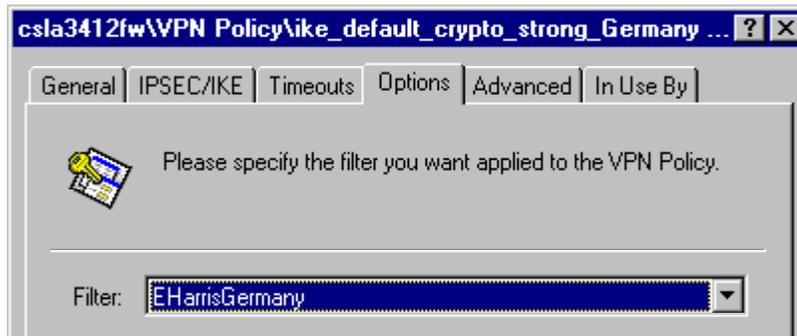
9. Now you need to create a VPN policy to use, which tells us what encryption to use. . Go to the Virtual Private Networks section on the Raptor Management Console and select VPN Policies. In the right pane you will see some already defined policies. You can use these as models and create your own. To do so, select the policy of your choice, right click and select Clone. You need to give it a meaningful name, description and then select the type of encapsulation you want to use. Based on what you select, Raptor grays out options not available with your selection in the rest of the tabs. This really helps to keep you out of trouble if you are new to encryption.



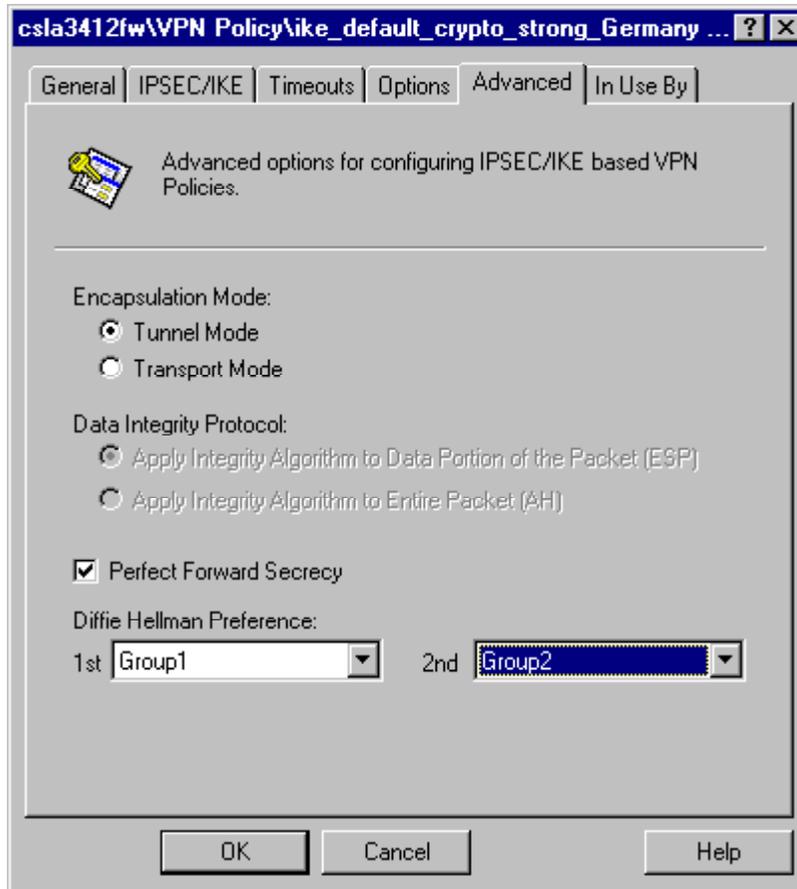
10. Since we selected IPSEC/IKE, we now have a tab for it. Click on it and then select the data integrity Preference and the Data Privacy Preferences. Compression is optional. I chose MD5 as the primary data Integrity and 3DES as the primary Privacy Preference. You have three options that Raptor tries in order in the event of a failure in one. NONE is also an option in all three of these boxes.



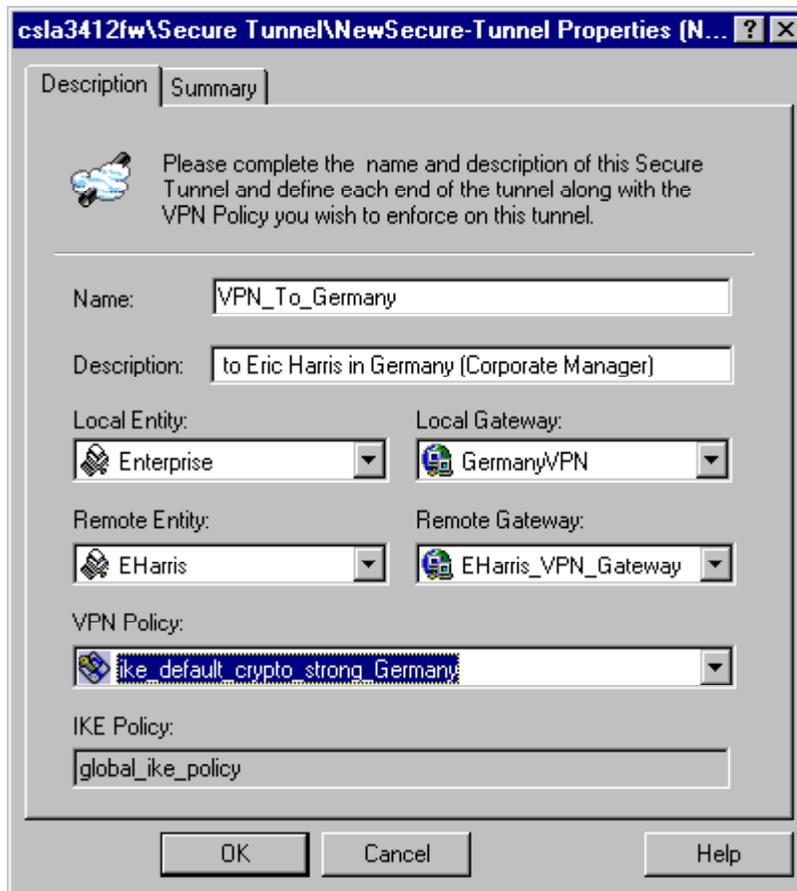
11. Click on the Options tab and here is where you apply the filter you created.



12. Select the Advanced tab and choose your Encapsulation Mode. I chose the Tunnel Mode to encapsulate the entire IP packet in the ESP header. Notice the Data Integrity Protocol is grayed out. This is only an option if you select none on both options under the IPSEC/IKE tab. Raptor does not tell you this. I also enabled Perfect Forward Secrecy to allow the administrators to generate keys and helps to stop hackers by making the keys non successive. Group 2 provides for stronger encryption as it is 1024 bits long, but requires more CPU power. Group 1 is 768 bits. If group one fails, I definitely want group 2 and then I want to know why!



13. We are finally ready to set up the tunnel. To do this, go to Virtual Private Networks, right click on secure tunnel and choose new Secure Tunnel. Give the tunnel a meaningful name and description. Choose the Local Entity as the machine you want to be able to talk to Eric Harris' machine. Choose the local gateway as what you named your local gateway. This is the outside interface of the firewall. The remote entity is the remote machine you want to talk to, in this case Eric Harris. Select the Remote Gateway you created. Finally choose the VPN Policy you created which controls the encryption on the tunnel



Remember what you did on your end, has to be configured on the other end. It is very important to work with the other end to ensure it is set up correctly to work.

Filter Implementation

The above steps 5-8 walk you through how to create a filter. Filters are very important to ensure that only the required connections are allowed and the directions they are allowed. It is very wise to create your own protocols and narrow down the ports used. This will limit what someone is able to gain access to. Multiple filters can be created for e-mail access, database access for different systems etc. This filter's can be combined as you choose and reduce the need to continually create the same filter.

Multiple firewalls and VPNs

Raptor provides the ability to do nested and cascaded VPN tunnels. Both tunnels require IPsec and will not allow swIPe. Nested tunnels allow a tunnel to pass through another tunnel. Cascaded tunnels terminate the tunnel at the remote gateway and then establish a second tunnel to the final destination. For our International Partners, we will use nested tunnels. The only difference is ensuring who knows about whom on the host machines and on the gateways. Raptor documentation provides explicit documentation to configure either one. Since the configuration is the same, but different entities have to have certain entities created on them, it will not be explained here. Nested tunnels was

chosen to ensure the decryption did not take place till it reached its final destination of the International marketing firewall.

Test Procedures

To test the VPN, ideally you will have a test bed set up that will allow you to test patches, configurations etc before deploying. You can test the above configuration in the test bed between two firewalls, if this is not feasible, or currently in place, then use two of the internal firewalls. Set up the configurations to allow access between two controlled machines. Once you establish the VPN and ensure that it functions, test the ability to do things on the network on the remote end. Ensure the VPN only allows you to do what it is you want. If it doesn't or allows you to do more, check the firewall logs and see what is being passed. You may have to use TCPdump or Snort to monitor the packets and see what is missing or in excess.

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

Assignment 3: GIAC Enterprises Security Audit Procedures

Overview/Goals

The purpose this requirement is to audit GIAC Enterprises security architecture and ensure it is functioning as required. We will be looking at the primary firewall in our architecture and validating it meets the criteria. This is a crucial part of the overall security design. The old adage holds true here “It looks good on paper, but will it run?” The request has been made to audit the primary firewall at GIAC Enterprises. The management at GIAC Enterprises, being a new E-commerce company and knowing their livelihood depends the ability of the customers to make purchases 24/7, wants to ensure this will happen. It is very important to them that they can protect their customers and themselves. With a vested interest in the overseas market, and in light of the attack on the World Trade Center and the Pentagon, concern has risen over staying secure. All of the talk of a cyber war being launched as America prepares for action against those accused of perpetrating the attack, has management worried about attacks on their website.

Assessment Plan

In order to plan an assessment, it is important to understand the mission. The management has made that clear: stay operational 24/7 and protect the company and customers against possible attacks or compromise. My task is to audit the primary firewall and ensure it provides the security it was designed to provide. Here are the steps that will be taken to ensure the security of the firewall. A non-disclosure agreement will be signed prior to auditing the firewall.

1. Analyze the firewall security policy. This is by all means the most crucial step. Regardless of how well the firewall’s initial design was implemented, it will not stay in its fine tuned state if there is no policy governing it. Most people install a firewall and then write a security policy. This is completely backwards as to how it should be done. The security policy dictates the configuration of the firewall, not vice versa. Having personally worked with the designer of the firewall and network perimeter security, I know they established a security policy first.

The analysis of the security policy will take two days and will be conducted during business hours as long as it does not interfere with daily operations, otherwise it will be conducted after hours. Approximate cost: \$2000/day x 2 days = \$5,000

2. The next step is to examine the configuration of the OS on which the firewall resides. Having a great firewall is useless if the OS has not been properly hardened. This will be tested against guidance from SANS and NSA and a use a tool that will analyze the system.

The analysis of the OS will take one day and will be conducted after hours to ensure it does not interfere with daily operations. Approximate cost: \$2000/day x 1 day = \$2,000

3. The final step is to examine the firewall and test it to ensure it does only what the security policy says it will do. I will use two different tools to ensure it is properly functioning. I will also examine all the firewall reports for the actual configuration.

The auditing of the firewall will take one day. The first part of the day will be spent during business hours monitoring the traffic and observing the firewall. This will be done mid morning or when the administrators tell me traffic is the heaviest. The rest of the day will be spent using tools to probe the firewall. Approximate cost: \$2000/day x 1 day = \$2000

Assessment Implementation

Firewall Security Policy Audit

The firewall security policy is the very first thing we want to audit. Two days were scheduled for this because it involves two phases. Phase one will be to read and study the firewall security policy. This will be to understand the requirements and ensure the policy is all encompassing, as it should be. There are some very important sections that need to be in the policy.

Access Control Policy

A section needs to be present that defines the access control policy. This should explain the organizational structure of GIAC Enterprises and who needs to talk to whom. It should also examine the different systems with GIAC Enterprises and who has a right to access these systems. A process should also be present that describes how a user requests access to resources and who approves the access. It needs to discuss the international partners. Who they are, what they need access to, and how requests are processed for them. This should also specify for each group or section, the time period for which access is allowed. A section needs to discuss special requests, who authorizes them, for how long etc.

Network Service Access Control Policy

This policy controls the type of services needed. It should list each service and define at the minimum: the protocol used, ports required, how they will be used, which systems use them and exceptions to the policy. This policy takes a lot of time and effort, but is crucial to know what should be present on the network. It is resource intensive to establish, but will save time, effort, and possible security vulnerabilities in the future.

Phase two will be to compare the policy as to what is actually configured on the firewall. The firewall should match the firewall security policy. Any thing that does not match should be annotated and compared to the firewall's logbook to see when the change took place and who made the change. If there are any discrepancies not accounted for, they should be reported as a possible compromise for further investigation. Remember, the majority of compromises are internal!

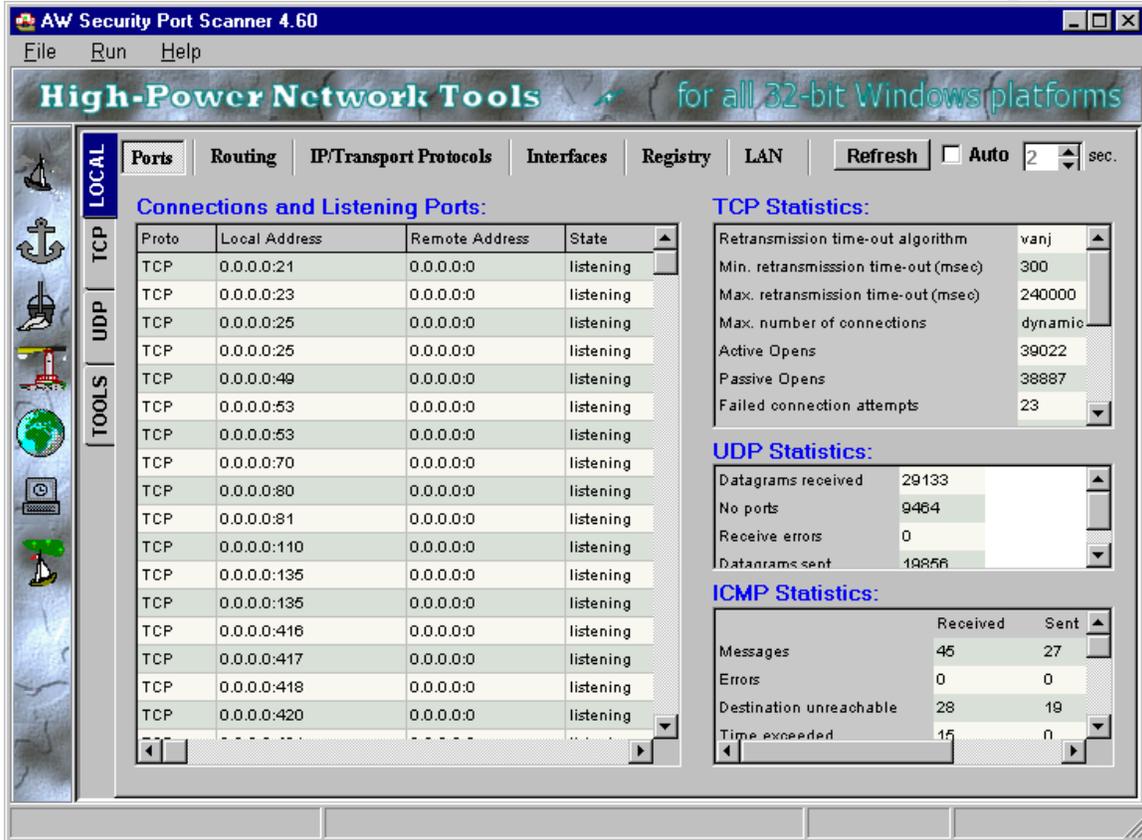
Operating System Security Audit

The operating system audit will take one day. This will be done during the day if time permits and if not, it will be completed after hours. To audit the OS, which in our case is Windows NT workstation, we need to examine several things. Raptor will run on NT workstation or server. In our case, it will be the workstation. We need to ensure the latest patch for the OS has been installed which is service pack 6a. (Note, it is important to check the version of Raptor you are using. Raptor 6.02 requires service pack 5, if the proper Raptor patch has not been installed.) We need to ensure it meets the proper guidelines for securing Windows NT. SANS institute has a step by step guideline that tells you how to secure Windows NT (see <http://www.sansstore.org/>). NSA has also produced guidelines for securing Windows NT. It may be possible to receive a copy by contacting NSA. The OS will be compared against the recommended policies and procedures.

There is also a tool I will use called AW Security Port Scanner. This product gives you the capability of scanning a local hosts as well as a network. It not only scans hosts, but registry settings etc. The following screen shots will show you its capabilities. The screen shots were done on a firewall in an isolated test bed. This will give you an idea of the results you would see.



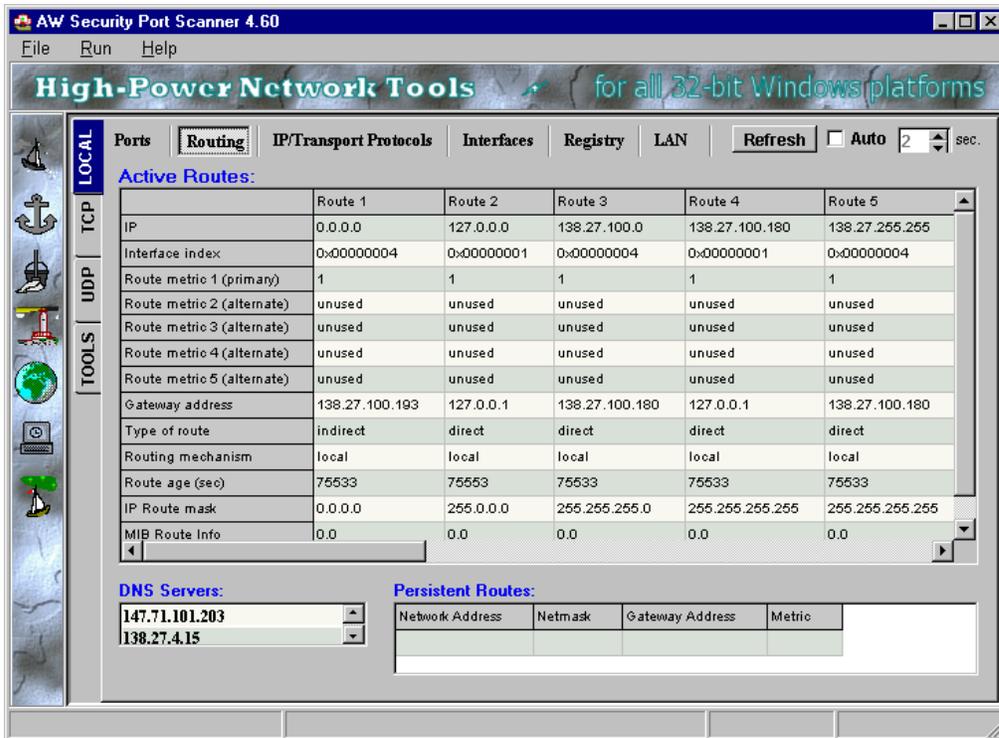
The first thing we want to look at on the OS is for open ports. The tools are simple to use and provides a wealth of information. We want to see what is listening and possible security vulnerabilities it may reveal.



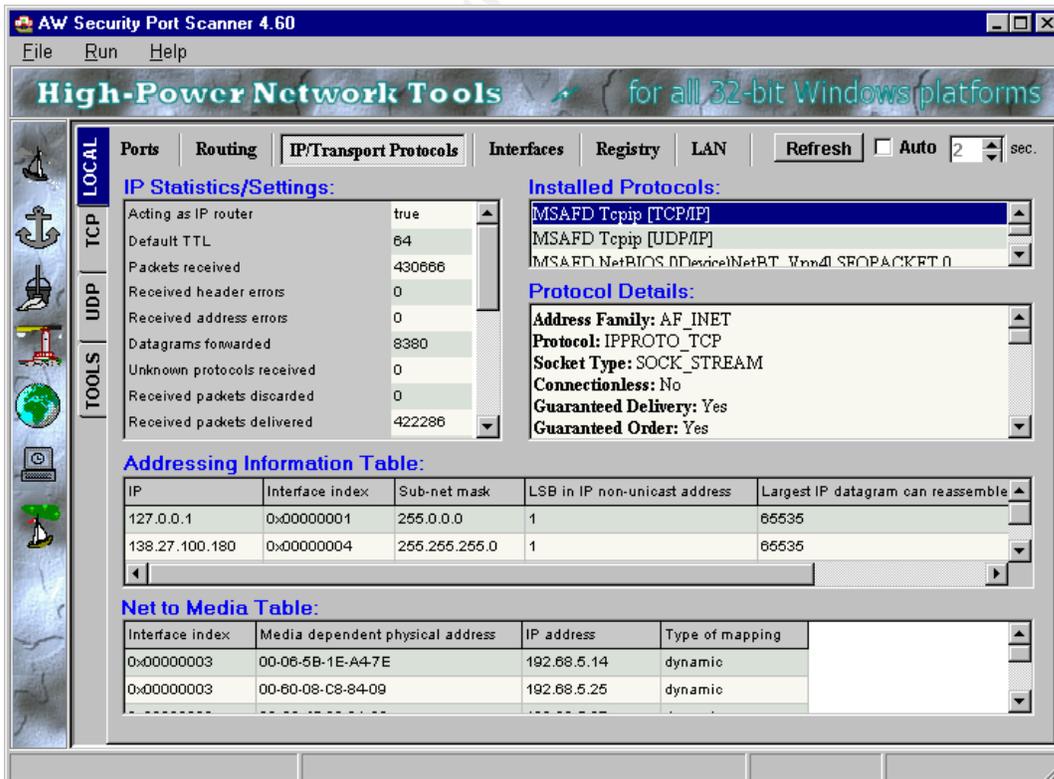
By clicking on any of the ports listed you get a wealth of knowledge about use and possible vulnerabilities.



We now want to look at routing. This is important since Raptor requires IP forwarding to be turned on. We want to know who the OS has routing capabilities for. This can be very revealing.



The next tab will show us the IP protocols and other important information about what the system is using. This will help determine what is necessary and running on the system.



We want to pay close information to the registry section. It reveals information about your system and its vulnerabilities. By clicking on the registry key in question, it shows information at the bottom for what it does and any risks associated with it. Be very careful making registry changes. It can be devastating if you are not very familiar and used to working in it. I recommend strongly all changes be tested on a non-production system and evaluated.

AW Security Port Scanner 4.60
File Run Help

High-Power Network Tools for all 32-bit Windows platforms

Ports Routing IP/Transport Protocols Interfaces **Registry** LAN Refresh Auto 2 sec.

Tcp ARP AFD NetBios Security

Registry Settings

Parameter	Reg Key	Type	Value	Default	Minimum	Maximum	Recommended
BacklogIncrement	HKEY_LO...	Dword	Not present	3	3	20	
DisableRawSecurity	HKEY_LO...	Dword	Not present	0	0	1	
DynamicBacklogGrowthDelta	HKEY_LO...	Dword	Not present	0	0	4294967295	10 for a system under attack
EnableAddrMaskReply	HKEY_LO...	Dword	Not present	0	0	1	0 (1, NT 4, see Q186463)
EnableDeadGWDetect	HKEY_LO...	Dword	Not present	1	0	1	0
EnableDynamicBacklog	HKEY_LO...	Dword	Not present	0	0	1	Under heavy attack, 1
EnableICMPRedirects	HKEY_LO...	Dword	Not present	1	0	1	0
EnablePMTUDiscovery	HKEY_LO...	Dword	Not present	1	0	1	0
EnableSecurityFilters	HKEY_LO...	Dword	0	0	0	1	1
KeepAliveTime	HKEY_LO...	Dword	1800000	7200000	1	4294967295	300000
MaxConnBackLog	HKEY_LO...	Dword	Not present	1000	1	40000	
MaximumDynamicBackl...	HKEY_LO...	Dword	Not present	0	0	4294967295	Under heavy attack, less tha
MinimumDynamicBacklog	HKEY_LO...	Dword	Not present	0	0	4294967295	Under heavy attack, 20
RestrictAnonymous	HKEY_LO...	Dword	Not present	0	0	1	1
RestrictNullSessionAcc...	HKEY_LO...	Dword	Not present	1	0	1	1
TcpMaxConnectRespon...	HKEY_LO...	Dword	Not present	3	0	255	

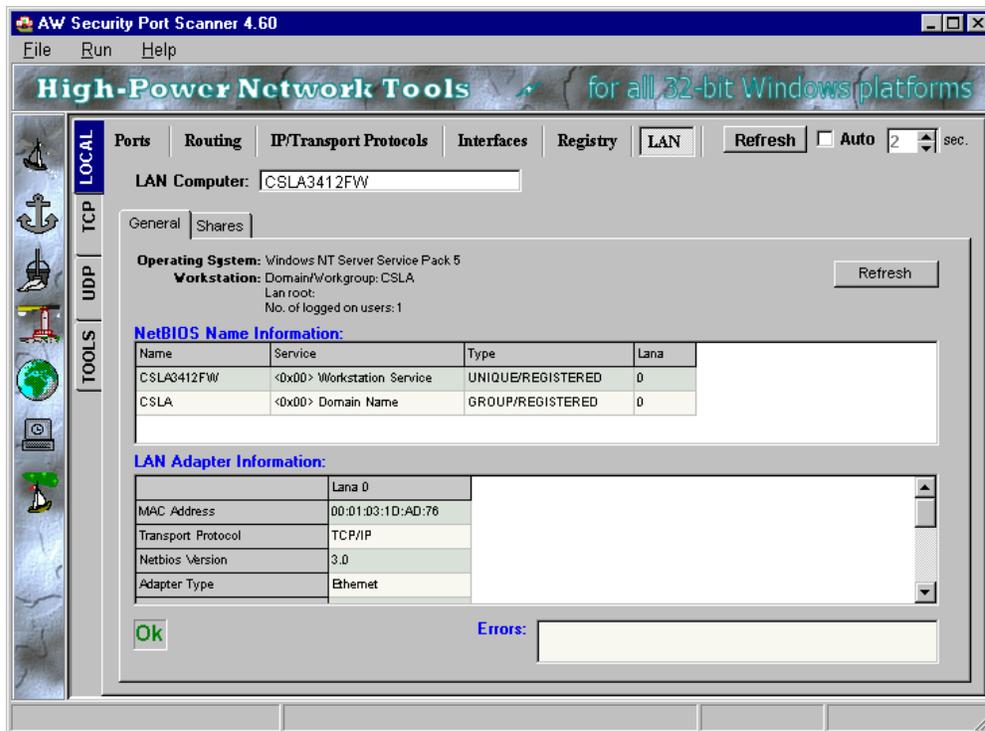
Explanation

Controls the number of free connections to create when additional connections are necessary. Be careful with this value; a large value could lead to explosive free connection allocations. (Although this parameter still exists, the TCP stack itself has been hardened against SYN-ATTACK in Windows 2000; therefore, it should not be necessary to use this feature of AFD.)

WARNING: Editing the Registry can cause serious problems that may require you to reinstall your operating system. Please refer to Microsoft sources or other professional help before proceeding to any changes in the Registry.

The last evaluation

on will be of the LAN settings. Ensure everything is configured the way you thought it was.

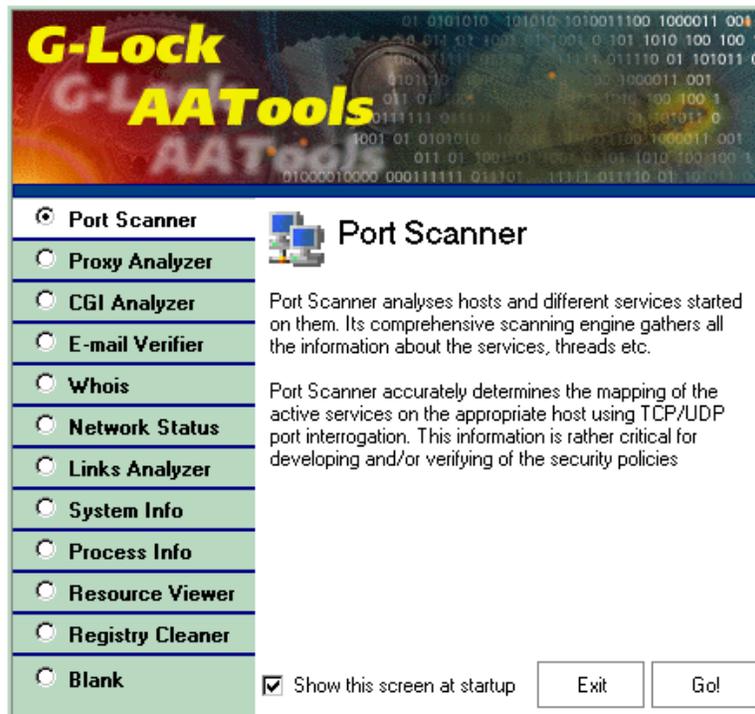


Firewall Security Audit

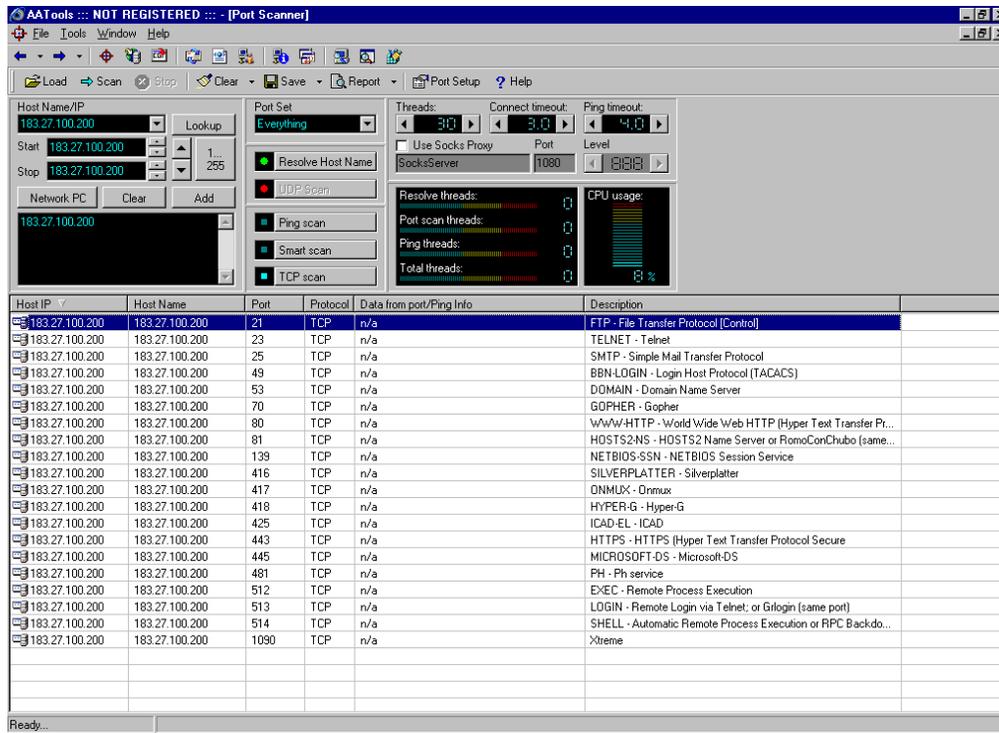
The final audit needs to be done on the Firewall configuration. This will be conducted on a system not attached to the network. This will ensure we do not interfere with business activities. It is easy to move the Raptor configuration; just copy the SG directory to the test system and the same configuration will exist on a non-production system. +We will run a port scan against the firewall. To ensure we are thorough, two different scanners will be used. The one mentioned above and one by G-lock.



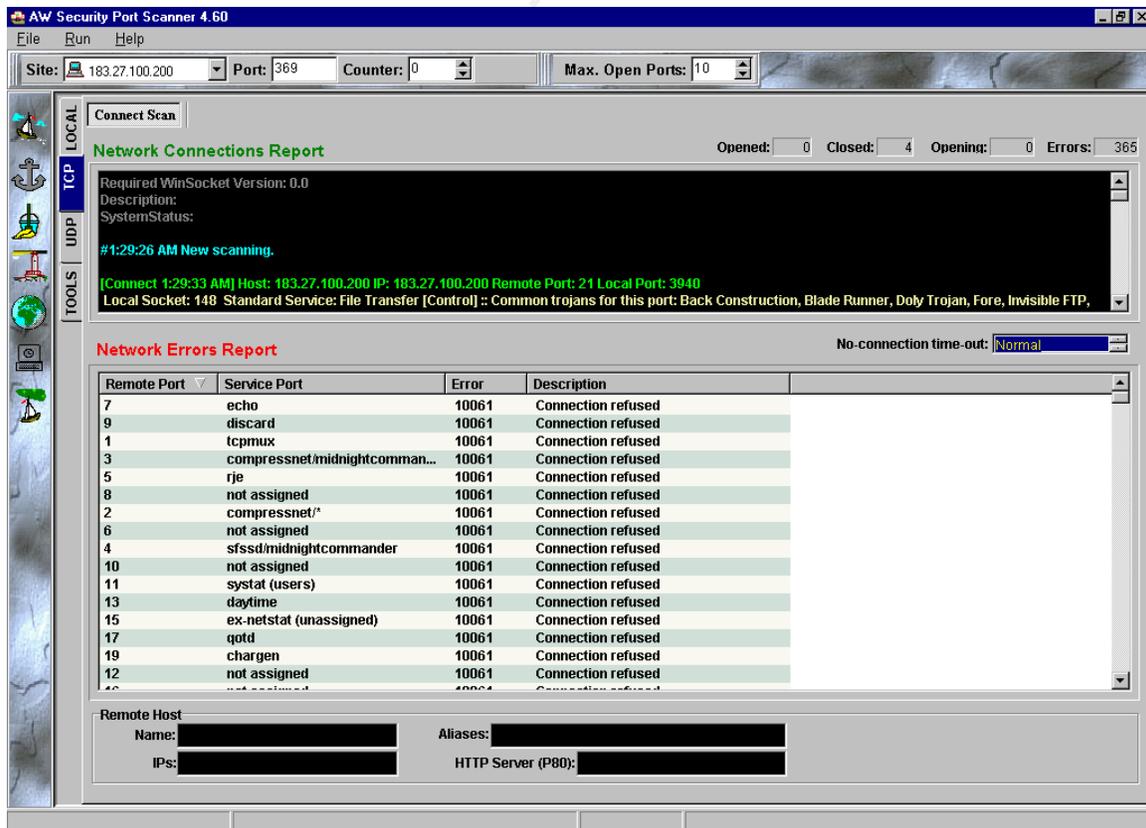
Both tools are simple and will tell us how open the firewall is. This also needs to be compared with the Raptor Firewall logs to validate how raptor handles things. G-lock offers many tools in one. We are interested in the Port Scanner.



Scans will be conducted on all the ports using TCP, UDP and ICMP. The results should be expected and looked at closely to see what was found. We should check the logs to ensure Raptor is handling events correctly and there were no anomalies. Only the necessary ports should be listening on the firewall. Remember, that Raptor has several built in services that require certain ports if enabled. If you don't use the functionality, it should be disabled. The following screen shot shows the results of a port scan by G-lock. Each of the ports found listening need to be verified they are in the Firewall Security Policy. This shows the TCP results.

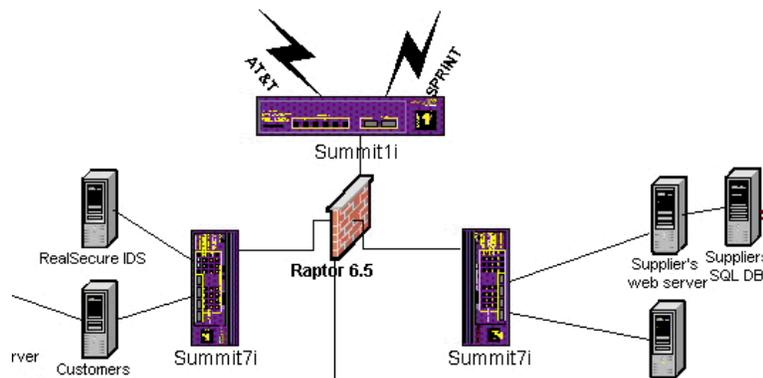


The AW Port Scanner was a little more descriptive in its results as it tells you whether or not it could make a connection. If any connections were established, it should be immediately investigated. This will be compared to the Raptor logs.

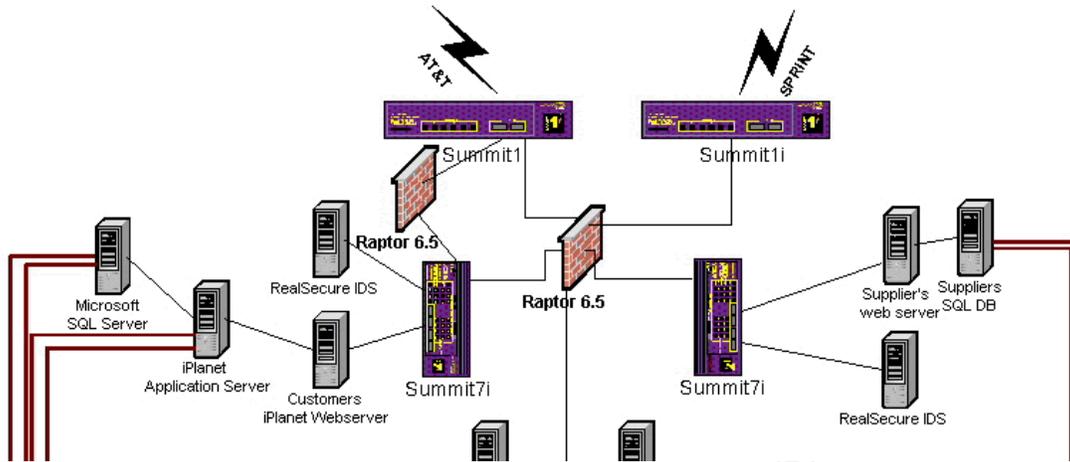


Assessment Results

The results of the actual assessment will be turned over to GIAC Enterprises after a report has been written up with vulnerabilities and recommendations from each of the three areas tested. Initial results indicate that GIAC Enterprises has a good security posture, although there is always room for improvement. The Security policy looked good although, it was already getting out of date. It is important that the differences noted are annotated into the security policy as soon as possible. This should be kept in a location accessible only by designated personnel as it contains in-depth details of GIAC Enterprises configuration. This would be detrimental in the wrong hands. The OS was hardened and no glaring deficiencies were noted, although a thorough analysis of the data collected has yet to be done. One of the things noted was the design of GIAC Enterprises contains a single point of failure, at the router and firewall. If one went down, customers would not be able to get in and that means money lost in E-commerce.



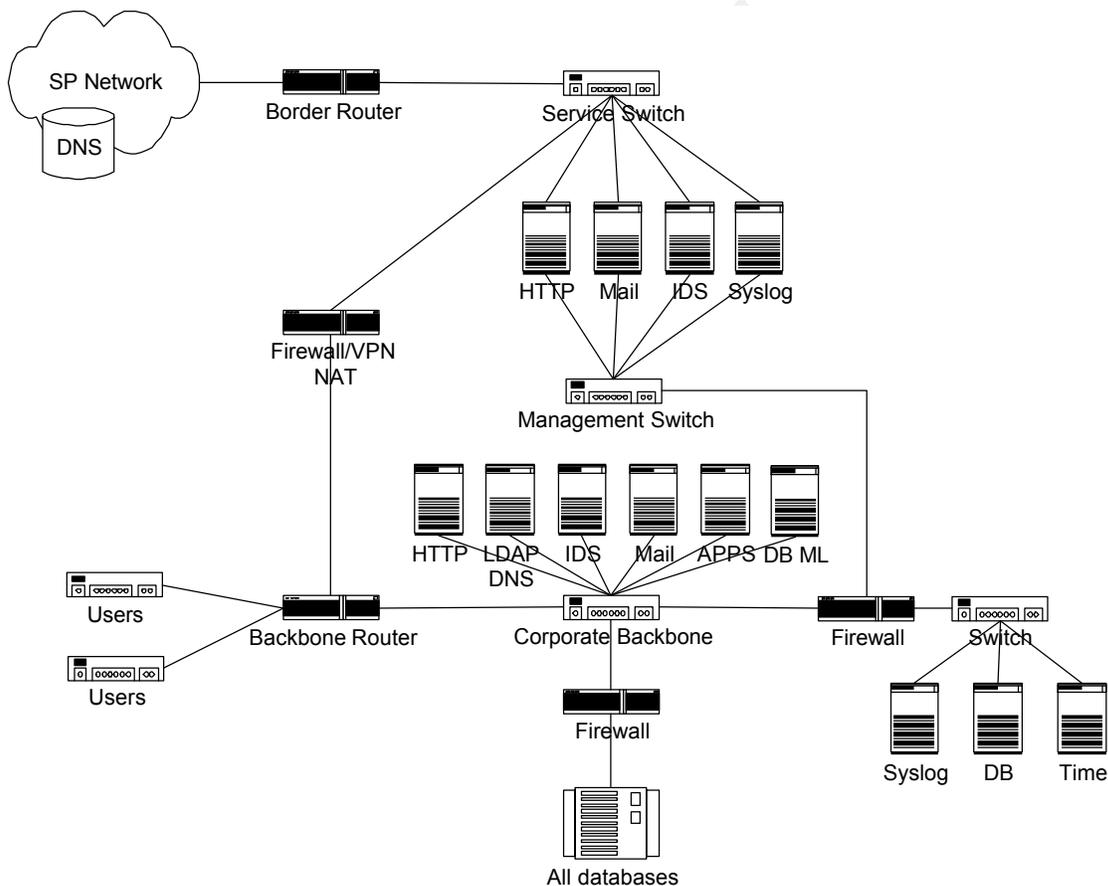
The design calls for two ISP, so connectivity to the Internet has redundancy built in. In order to alleviate the down time if the primary switch died, a spare switch needs to be preconfigured and on hand at all times. Reminder: Changes to one need to be made on the backup. This backup could reside in the test bed replicating the network. The firewall will be covered by a product called iNODE found at www.inodeusa.com. This server allows for self-healing on a machine simply by rebooting. If the firewall died (unless it was hardware) or the software became corrupted, simply reboot the machine and it will restore everything back to the way you configured it. A backup of the SG directory should be made daily. GIAC Enterprises does need to keep a second box configured for the firewall in case of hardware failure. Another option would be to have two routers instead of one for the primary router. This would provide two paths, one to each ISP. Removing the single point of failure in the primary router. An additional firewall added out front would also enable two ways for the customer to get to the web server, ensure it was protected. This new design would allow for greater flexibility for redundancy to other systems as well. The design would look as follows.



Assignment 4: Design Under Fire

Overview

The requirement of this exercise is to get you to think and learn. It is a common thought to believe you're secure and invincible because you have a firewall or something similar. This assignment looks at proposed security designs from the eyes of a hacker. How can I get in or cause a denial of service? If applied to your own network security design, you should have your eyes open to things left undone. For this assignment we were to pick one other student's design and perpetrate an attack against the firewall, a denial of service (DOS) attack and attack to compromise an internal system. I picked my design at random to test my own limited abilities. I have to say, I was amazed at what I found out on the Internet. The design chosen was by Tim Kidder and can be found at http://www.sans.org/y2k/practical/Tim_Kidder_GCFW.zip



Perimeter Security Recon

We have an advantage here to plan our attack. The practical is presented in all of its glory with extensive details about the design. One has to ask how would you go about finding out what is out there on a company you know nothing about. I would be negligent if I didn't address how to find out what is there. There are a few ways to go about this. One

is to use social engineering. You could call the company and pretend to be from the sales department of X company requesting to demo some new products their company has to offer. Most folks are not trained in how to protect their network and how simple information can hurt them. You could also scan the company very stealthily over a long period of time and collect data. You could find out who works in the company's IT department and watch them, just find out where they like to go. Then, casually meet them one day and strike up a conversation. You can find out a lot contact information from www.arin.net and then call them under the pretense one of their boxes has been sending packets to them and wonder if it were misconfigured etc. The possibilities are endless, even if the company is far away. It has to be understood by all who work in the Information Technology arena that the network probes may not come from just the network.

Firewall Attack

Setting the stage

The firewall attack for this assignment turns out to be rather easy. The router in this design is a CISCO 3640 running IOS version 12.1(5)T. There is an exploit released by CISCO on June 27, 2001 and updated September 13, 2001 called IOS HTTP Authorization Vulnerability and can be found at <http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html>. This exploit affects the version of IOS running on the router. Also, by nature of the business, HTTP traffic has to be allowed and both of these combinations present vulnerability. By sending a crafted URL to <http://<device address>/level/xx/exec/> with the level set to 15 (admin rights) and xx being a number between 16 and 99, it is possible to gain full admin privileges to the device. Once obtained, the router is mine. Knowing this is possible, a hacker would probably be very careful about planning the next move. Small changes would go unnoticed on a router with many ACLs, especially if it is configured and then forgotten. They could exploit the company over a long period of time or simply reconfigure the router to pass all traffic and then change the admin password. I am going to be selective because I don't want to draw attention to myself. I will change the last entry from deny to permit. Since Mr. Kidder only denied private addresses, so everything else will now go through. I am also going to turn off logging for the default rule. This should let me go undetected for a while, since all traffic will appear as normal, unless they monitor the configuration regularly. Since the path to the firewall is wide open and the switch in between is not configured to offer any protection, the attack can begin.

The attack

The firewall is a PIX 6.0 and after some research, I found an exploit against the PIX called "Cisco Secure PIX Firewall SMTP Filtering Vulnerability." This was released on September 26, 2001 and can be found at <http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml>. By default, the PIX firewalls that provide access to mail servers are at risk. The command used is "fixup protocol smtp [portnum]." This will allow us to bypass the firewall to the

mail server. This will be discussed more in depth as we look at compromising an internal system. This attack will allow us to pass through the firewall.

DOS Attack

The stage has already been set for our DOS attack against the company. The router is now wide open to allow all traffic to pass. I would have my 50 compromised systems to launch a TCP SYN attack against the customer's web server. All 50 systems would have full access and render the web server useless. This would be devastating to the company since their livelihood depends on the customers' access to the web server. The best way to defend against this is to upgrade the IOS, which is an interim fix and have multiple routes to the web server. Right now, this design has two single points of failure, which are the router and the switch. Also, the web server should be behind a firewall to ensure attacks like this cannot occur. Even if the router were compromised, the firewall would stop a simple attack like TCP SYN.

Internal System Compromise

Before I launched a denial of service attack, I would get what I want from the company. Since we already know how to bypass the router and the firewall we can get to the mail server and access it (especially if it hasn't been hardened, after all its behind a firewall). The mail server has a lot of information on it. There is account information, address lists (to include the company's overseas partners), personal information and company information. Usernames and passwords are there, and as an added bonus, if it is and NT domain, the accounts probably match the accounts on the PDC. It is possible to run code on the mail server. A bug could be planted to transmit out corporate email etc. Once access has been obtained on the web server, the sky is the limit.

Citation of Sources

Northcutt, Stephen; Kessler, Gary; Pomeranz, Hal. Track 2—LevelTwo Firewalls, Perimeter Protection, and Virtual Private Networks. SANS Institute, 2001.

Extreme Networks Quick Reference Guide. 2000.

ExtremeWare Software User Guide V6.1. April 2000.

Sunday, Larry. Information Assurance Raptor Management Console Firewall Training Class Part I and II. 2001.

Symantec Enterprise Firewall and Symantec Enterprise VPN Reference Guide Version 6.5. April 2001.

“Cisco Secure PIX Firewall SMTP Filtering Vulnerability.” Version 1.1, 26 September 2001. URL: <http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml> (3 October 2001).

“Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability.” 27 June 2001. URL: <http://www.securityfocus.com/bid/2936> (3 October 2001).

“Cisco Security Advisory: Cisco Secure PIX Firewall Mailguard Vulnerability.” 5 October 2000. URL: <http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml> (3 October 2001).

“Symantec Enterprise Firewall Formerly Raptor Firewall.” April 2001. URL: http://enterprisesecurity.symantec.com/pdf/axentpdfs/sym_enterprisefw_factsheet.pdf?PID=8535439 (28 August 2001).

“Everything You Need to Know about Network Security.” 1999. URL: <https://enterprisesecurity.symantec.com/content/TrialwareForm.cfm?PID=8535439&PDFID=32&PromoCode=SymEsForm&SSL=YES> (28 August 2001).

“Dell – PowerVault Storage Area Network.” 2001. URL: http://www.dell.com/us/en/fed/products/seriers_sanet_storage.htm (18 September 2001).

Longoria, Gerald. “Resolving Data Storage Demands with SANs.” 2000. URL: http://www.dell.com/us/en/esg/topics/pwer_ps1q00-sans.htm (24 August 2001)

Berlind, Janet. “Vectors Dell Highlight.” March 1999. URL: http://www.dell.com/us/en/bsd/topics/vectors_1999-Storage.htm (24 August 2001).

“Cisco CCIE Fundamentals: Network Design.” 1999. URL:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/index.htm> (24 August 2001).

“SAN Cascading.” 1999-2001. URL:

http://www.dell.com/us/en/esg/topics/products_san_pvaul_006_san_tech.htm (24 August 2001).

“PowerVault Storage Area Network (SAN) Version 4.05.” April 2001. URL:

http://www.dell.com/downloads/us/pvaul/san_405_infobrief.doc (24 August 2001).

“TechBrief: Extreme Networks Migration Guide.” URL:

http://www.extremenetworks.com/technology/whitepapers/Migration_Guide_1-00.asp (24 August 2001).

“TechBrief: Leveraging Redundancy to Build Fault Tolerant Networks.” URL:

<http://www.extremenetworks.com/technology/whitepapers/redundancy.asp> (24 August 2001).

“The Internet and Web-Based Applications Are Creating Monumental Changes in Enterprise Networks.” URL:

<http://www.extremenetworks.com/solutions/enterprise/overview.asp> (24 August 2001).

“Extreme Networks Eliminate Provisioning Hurdles in Service Provider Networks.” URL:

<http://www.extremenetworks.com/homepage/isptools.asp> (24 August 2001).

“Security on IP Networks Countering Denial of Service (DOS) Attacks.” URL:

<http://www.extremenetworks.com/technology/whitepapers/security.asp> (24 August 2001).