Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

SUBMITTED BY: **MATTHEW MITCHELL**

CAPITAL SANS 2000 GIAC LEVELTWO:

FIREWALLS, PERIMETER DEFENSE, AND VPN'S

GIAC CERTIFIED FIREWALL ANALYST CERTFICATION

PRACTICAL ASSIGNMENT

January 30, 2001

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

CONTENTS

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

ASSIGNMENT ONE: SECURITY ARCHITECTURE

GIAC Enterprises requires a perimeter architecture that will provide the maximum level of security as well as allow customers, suppliers, and partners access to the various networks. Partners and suppliers will connect to web-based applications that are made available by web servers on the partners and suppliers private network. GIAC Enterprise employees may access the corporate network from the Internet through the use of VPNs. Customers will be able to purchase products using web-based applications that reside on the public e-commerce network. Figure 1 displays the security architecture including the different networks and the specific equipment used.

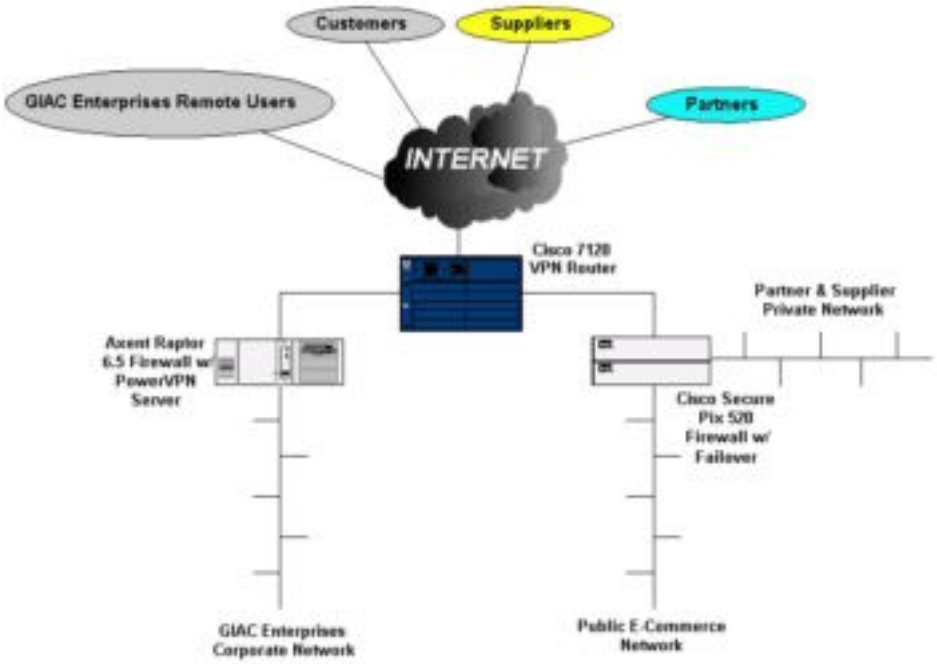

FIGURE 1: GIAC ENTERPRISES PERIMETER SECURITY ARCHITECTURE

CISCO 7120 VPN ROUTER

The Cisco 7120 VPN Router will be used to terminate the connection provided by an Internet Service Provider (ISP). In addition the Cisco 7120 shall perform gateway-to-gateway IPSec VPNs between each supplier to the GIAC Enterprise network and each partner to the GIAC Enterprises network. The VPNs will terminate at this router so that all packets will be decrypted and have to pass through more than one layer of perimeter defense before arriving at the authorized host. Finally the Cisco 1720 VPN Router will perform some packet filtering to ensure that no unauthorized packets enter the various networks. This 7120 router will use Cisco IOS Release 12.1 software with the Enterprise/Firewall/IPSec 3DES feature set. The two primary reasons for selecting the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7120 series router are the VPN feature set and the increase processing power and memory that is that is required to accommodate the processor overhead used to create and negotiate IPSec VPNs.

CISCO SECURE PIX 520 FIREWALLS

The two Cisco PIX firewalls shall be used to perform stateful packet filtering for connections destined for the public e-commerce network and the partner & supplier private network. The firewalls will ensure that only authorized connections can be made to and from the servers on their respective network. The firewalls will use network address translation (NAT) to protect the actual addresses of the servers on each network. Each PIX firewall will be configured to failover to a backup PIX firewall if a hardware or software failure occurs. The failover configuration will maintain state information across both firewalls so that established connections will no be effected if a firewall fails. The PIX firewalls will use PIX v5.5 software. Cisco Secure PIX firewall was chosen over other firewall products for this application because of it's superior speed, high availability configuration features, and because it does not rely on a base operating system.

AXENT RAPTOR 6.5 FIREWALL WITH POWERVPN

The Axent Raptor firewall and PowerVPN Server shall perform proxy based firewall security services for outbound connections from the internal GIAC Enterprises network, provide secure remote access by creating IPSec VPNs with remote users, and deny unauthorized connections to hosts. The Raptor firewall provides many advanced proxy features and services that allow the network administrator to fine tune the firewall at a very granular level as well as integrate it with many identification and authorization mechanisms that exist on the internal corporate network. Using the PowerVPN Server and the RaptorMobile VPN client software easily configurable and very secure VPNs can be created to give remote users secure access to the internal corporate network from any location.

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

ASSIGNMENT TWO: SECURITY POLICIES

For each device that will maintain perimeter defense for GIAC Enterprise's networks requires a security policy. This policy is made up of the rules and polices applied to the configuration of each device. In this section the rules and policies for each router and firewall will be described in detail on a device-by-device basis. The network perimeter designed in section one is a theoretical architecture. No actual IP address information has been defined so the following IP routable address ranges will be used to create configurations:

GIAC Enterprises Network: 5.0.0.0 (publicly seen as 206.105.201.0)
Public E-Commerce Network: 192.168.2.0 (public web server reachable at 206.165.201.4 using NAT)
Partner & Supplier Network: 192.168.1.0 (private web server reachable at 206.165.201.3 using NAT)

Note: These IP addresses were chosen at random, and it is by pure chance that these IP address ranges are owned by an organization.

CISCO 7120 VPN ROUTER SECURITY POLICY:

As stated in section one the Cisco 7120 router will be used to terminate Internet connections, establish gateway-to-gateway VPNs, and perform packet filtering. The following configuration information will show the exact commands used to configure the router along with descriptions of what the command's function is. There will be three portions of this security policy: securing the router, access control lists, and VPN configuration.

SECURING THE ROUTER

Router Configuration Command	**Description**
enable secret *password*	Establishes a password for privileged router mode. The password is hashed using MD5.
service password-encryption	Instructs the IOS to encrypt stored passwords.
no service finger	Will not disclose user information to unauthorized individuals.
no service tcp-small-servers	Disables rarely used services such as echo, chargen, and discard. These services are

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

no service udp-small-servers	rarely used for legitimate purposes.
no ip unreachables	Prevents router from giving out network information.
no cdp running no cdp enable	Cisco uses CDP (Cisco Discovery Protocol) to learn information about neighboring devices. Turning off these devices will avoid the router from releasing information to neighboring devices.
No bootp server	The bootp protocol is not used and therefore should be turned off.
no SNMP	SNMP is not used for network management and is therefore not needed.
no ip directed-broadcast	Prevents the router from acting as a "smurf" amplifier. This must be applied to each interface. Stops ICMP unreachable messages.
transport input ssh	Only allows VTY secure shell connections to configure the router remotely.
exec-timeout 30	This will automatically close VTY connections if they are idle for more than 30 seconds.
banner login *message*	Displays a legal warning each time a user logs into the router.
no ip http server	Turns off the monitoring and configuration services that use HTTP for communications.
ip route 0.0.0.0 0.0.0.0 null 0 255	Drops packets with an invalid destination address.
logging x.x.x.x logging trap debug logging console emergencies	Sends syslog messages to an external syslog server with the IP address x.x.x.x and sends emergency messages to the console.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ACCESS CONTROL LIST CONFIGURATION

Cisco routers have multiple types of IP access lists that can be configured on routers using the IP IOS software. The three most commonly used types are: standard, extended, and reflexive. Standard access lists contain an access list number (1-99), permit/deny, and a source address. Extended access lists enable more granular control over what packets are allowed or denied at the time of inspection. Extended access lists may contain an access list number (100-199) permit/deny, protocol, source (wildcard), destination (wildcard), and protocol options (log). Reflexive access lists monitor the state of the connection in addition to features provided by standard and extended access control lists. Regardless of which type of access control list is used the list must be applied to a specific interface or VTY. After an access list has been created a decision must be made whether to compare packets against a particular access list upon ingress or egress. Only one access list may be applied to an interface for inspection upon ingress and one for inspection upon egress. The placement of a single ACL within a numbered access list is very important because when a packet is compared against an access list the packet will be compared against the first ACL that was entered and if there is no match it will be compared against the second ACL that was entered. This will continue until a match is met.

Router Configuration Command	**Description**
Access-list 105 deny ip host 127.0.0.1 any	Drops packets with the loopback address as the source address.
Access-list 105 deny ip 192.168.0.0 0.0.255.255.255 any	Drops packets that have the source address as a private, non-routable IP address.
Access-list 105 deny ip 172.16.0.0 0.0.15.255.255 any	Drops packets that have the source address as a private, non-routable IP address.
Access-list 105 deny ip 10.0.0.0 0.255.255.255 any	Drops packets that have the source address as a private, non-routable IP address.
Access-list 105 deny ip 5.0.0.0 0.255.255.255 any	Drops spoofed packets that use an internal network IP address as the source IP address.
Access-list 105 deny ip 206.105.201.0 0.0.0.255 any	Drops spoofed packets that use an internal network IP address as the source IP address.
Access-list 105 deny ip 206.165.201.0 0.0.0.255 any	Drops spoofed packets that use an internal network IP address as the source IP address.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Access-list 105 deny ip host 0.0.0.0 any	Drops a packet using an illegal IP address as the source.
access-list 105 deny icmp any any	Drops all ICMP packets when they reach the router.
Access-list 105 permit ip 206.165.201.0 0.0.0.255 200.200.200.0 0.0.0.255	Enable the router to encrypt all traffic between partner's router and the GIAC router.
access-list 105 permit any any	Allows all traffic that has been filtered by previous ACLs to pass through to an internal interface.
interface serial0 access-group 105 in	Defines the external serial interface, used to connect to the Internet, to use ACLs contained in access-list 105 and to make a decision to permit or deny the packet as it enters the external interface of the router.
Access-list 106 permit ip 206.105.201.0 0.0.0.255 any	Permits packets with a source IP address that belongs to the GIAC Corporate network.
Access-list 106 permit ip 206.165.201.0 0.0.0.255 any	Permits packets with a source IP address that belongs to the public e-commerce network and the partner & supplier network.
Access-list 106 deny ip any any	Drops all packets that have not met any previous ACLs in access-list 106.
Interface serial0 Access-group 106 out	Defines the external serial interface to use access-list 106 to filter packets on egress. All packets destined for the Internet that do not originate from an internal network will get dropped when they get to the serial interface.

© SANS Institute 2000 - 2002 Author retains full rights.

VIRTUAL PRIVATE NETWORKS CONFIGURATION

The latest release of Cisco's IOS software includes various feature sets that enhance the basic IP package. The Enterprise/Firewall/IPSec 3DES feature set provides the capability of creating IPSec VPNs between two routers. Partners and suppliers of GIAC Enterprises require an encrypted connection between their networks and selected GIAC Enterprise networks. To meet this need the Cisco 7120 router will be configured to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

create gateway-to-gateway, IPSec compliant, VPNs between the networks utilizing the Internet for connectivity. There are various private connections to suppliers and partners that need to be protected but for brevity's sake only the gateway-to-gateway VPN between the GIAC private network and one partner will be described in the following paragraphs. Following are the IP address information of the routers creating the VPN, exact configurations of each router, and descriptions of the commands.

GIAC Enterprises Router:
External serial interface IP address: 4.5.6.7
GIAC Enterprises router hostname: giac
GIAC Enterprise private network IP addresses: 206.165.201.0

Partner's Router:
External serial interface IP address: 210.210.210.210
Partner router hostname: partner
Partner internal IP addresses: 200.200.200.0

Six steps are required to configure each router for an IPSec tunnel:

1. Define the IKE policies: the type of encryption algorithm, hash algorithm, authentication method, the Diffie-Hellman group identifier, and the security association's timeout will be configured.
2. Configure pre-shared keys or other authentication methods.
3. Create crypto access lists: access control list must be defined in order for the router to know which packets to encrypt.
4. Configure IPSec tunnel mode
5. Configure crypto map information: at each router the peers that make up the VPN must be defined in order to establish a security association (SA)
6. Apply each crypto map to the designated interface at each router.

Defining IKE Policies

The following configurations define identical IKE policies for the GIAC router and the partner's router using triple DES for data encryption, MD5 hash for data integrity, a pre-shared key used for authentication, Diffie-Hellman group 2 (1024 bit), and a 24-hour lifetime for each security association. Triple DES and Diffie-Hellman group two are used for maximum encryption strength.

GIAC Router

```
giac(config)# crypto isakmp policy 1
giac(config-isakmp)# encryption 3des
giac(config-isakmp)# hash md5
giac(config-isakmp)# authentication pre-share
giac(config-isakmp)# group 2   (1024-bit Diffie-Hellman)
giac(config-isakmp)# lifetime 86400  (security association lifetime in seconds)
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Partner Router
partner(config)# crypto isakmp policy 1
partner(config-isakmp)# encryption 3des
partner(config-isakmp)# hash md5
partner(config-isakmp)# authentication pre-share
partner(config-isakmp)# group 2 (1024-bit Diffie-Hellman)

partner(config-isakmp)# lifetime 86400 (security association lifetime in seconds)

Pre-shared Key Configuration

Both peers that make up the VPN decide on an agreed upon pre-shared key which will provide a method of authentication. In this case both parties have agreed on the alphanumeric pre-shared key 2001gcfw in conjunction with the IP address of each router's serial interface.

GIAC Router
giac(config)# crypto isakmp identifiy address
giac(config)# crypto isakmp key 2001gcfw address 210.210.210.210

Partner Router
partner(config)# crypto isakmp identify address
partner(config)# crypto isakmp key 2001gcfw address 4.5.6.7

Crypto Access List

In order for each router to know what packets to encrypt an access list has to be created. This access list will identify the source address and destination address of the packets that will be encrypted. For this VPN all traffic originating from each of the internal IP address blocks of the peers destined for the internal IP address blocks of the other peer will be encrypted. In the fifth step the access list 105 will be referenced which will define which packets will be encrypted.

GIAC Router
giac(config)# access-list 105 permit ip 206.165.201.0 0.0.0.255 200.200.200.0 0.0.0.255

Partner Router
partner(config)# access-list 104 permit ip 200.200.200.0 0.0.0.255 206.165.201.0 0.0.0.255

IPSec Tunnel Mode

The following configurations define which type of tunnel mode will be negotiated between the two peers in the VPN connection.

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

GIAC Router
giac(config)# crypto ipsec transfor-set proposa14 ah-md5-hmac-esp-3des
giac(cfg-crypto-trans)# mode tunnel
Partner Router
partner(config)# crypto ipsec transfor-set proposa14 ah-md5-hmac-esp-3des
partner(cfg-crypto-trans)# mode tunnel

Crypto Map Entries

The following configurations define which type of tunnel mode will be negotiated between the two peers in the VPN connection. These configurations identify which interfaces will be used for the IPSec traffic along with the access list used to define which packets will be encrypted in the IPSec tunnel between the two peers.

GIAC Router
giac(config)# crypto map s4second local-address serial 1/0
giac(config)# crypto map s4second 2 ipsec-isakmp
giac(config)# match address 105
giac(config)# set peer 210.210.210.210
giac(config)# set transform-set proposal14

Partner Router
partner(config)# crypto map s4second local-address serial 1/0
partner(config)# crypto map s4second 2 ipsec-isakmp
partner(config)# match address 105
partner(config)# set peer 4.5.6.7
partner(config)# set transform-set proposal14

Applying Crypto Maps to Interfaces

The final step in configuring an IPSec VPN tunnel between two peers is applying crypto maps to each interface of the routers participating in the VPN. This instructs each router to analyze the packets on the interfaces and to use the previously defined policies during the security association stage of the connections.

GIAC Router
giac(config) interface serial 1/0
giac(config-if)# crypto map s4second

Partner Router
partner(config)# interface serial 1/0
partner(config-if)# crypto map s4second

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

CISCO SECURE PIX 520 FIREWALL SECURITY POLICY

Cisco Secure PIX firewall utilizes the adaptive security algorithm to perform stateful packet filtering. The firewall chooses to drop a packet or pass a packet based on the adaptive security algorithm and the connection state table that is located in memory. By default no packets can pass through the firewall without a connection and a state, all outbound packets are allowed, all inbound packets are denied, all ICMP packets are denied, and all attempts to circumvent these rules will be written to syslog. Each interface of the firewall is given an IP address and a security level. Typically the outside interface is given a security level of zero and the inside interface is given a security level of 100. Packets are not passed from a low security level to a higher security level unless a conduit statement or an access control list has been configured. Packets are allowed to pass from a high security level to a low security level by default.

For all packets destined for either the private network used for Extranet connections to partners and suppliers or the public e-commerce site the Cisco PIX firewalls will perform stateful packet filtering. PIX's use stateful packet filtering in order to allow or deny traffic to the two networks. The two firewalls are configured in a stateful failover configuration. Both firewalls will maintain identical connection state tables. This will enable the firewalls to failover without any interruption of the active connections in the event of a failure on the primary firewall. For simplicity I have only included one web server on each network, public and private. The configurations of the PIX firewalls are very simple. They are configured to only allow http and https connections originating from the Internet. The web servers themselves will not be able open any new connections to destinations on the Internet or any other network directly attached to the firewalls. The only traffic that will be passed to the web servers is from connections originating from the Internet or from a predefined extranet partner. The web servers will only be able to respond to these connection requests. Figure 2 displays the topology and the IP addresses used by the PIX firewalls and the web servers. The following information identifies the configuration for the firewalls.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

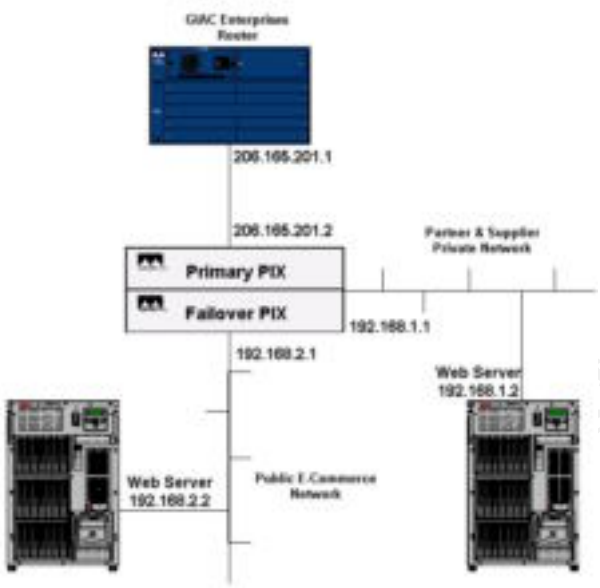

FIGURE 2: CISCO PIX ARCHITECTURE

SECURITY LEVEL CONFIGURATION:

The three Ethernet interfaces of the firewall provide connectivity to the outside (Internet), the public network, and the private partner and supplier network, respectfully. Ethernet0 interface provides connectivity to the router, which provides an Internet connection; this will be named outside and configured with a security level of zero. The ethernet1 interface provides connectivity to the public e-commerce web server and will be named public with a security level of 50. Interface ethernet2 provides connectivity to the private partner and supplier network. It is named private and has been configured with a security level of one hundred.

nameif ethernet0 outside security0
nameif ethernet1 public security50
nameif ethernet2 private security100

IP ADDRESS CONFIGURATION:

The outside interface has been assigned a routable IP address while the public and private interfaces are assigned non-routable private IP addresses. Network address translation (NAT) will be used to enable users on the Internet to connect to servers on the public and private networks. This will be configured in the NAT and Access Control section.

ip address outside 206.165.201.2

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ip address public 192.168.2.1
ip address private 192.168.1.1

NAT & ACCESS CONTROLS:

The following configuration information configures a static IP translation for the public web server and the private web server from non-routable addresses to routable addresses. In addition access control lists have been configured to only allow http and https connections originating from the Internet to connect to the web servers. The last configuration line applies the access control lists to the outside interface and the decision to allow or deny the packet is made upon the packet's ingress to the interface.

static (public,outside) 206.165.201.4 192.168.2.2 netmask 255.255.255.255
access-list acl-in permit tcp any host 206.165.201.4 eq www
access-list acl-in permit tcp any host 206.165.201.4 eq 443

static (private,outside) 206.165.201.3 192.168.1.2 netmask 255.255.255.255
access-list acl-in permit tcp any host 206.165.201.3 eq www
access-list acl-in permit tcp any host 206.165.201.3 eq 443

access-group acl-in in interface outside

Access lists are configured for the private interface to only allow outbound connection requests from the private web server to the partner network mentioned in the previous VPN router configuration section, IP block 200.200.200.0. The access control list is applied to the private interface and packet inspection takes place on ingress.

access-list private-out permit ip 192.168.1.0 255.255.255.0 200.200.200.0 255.255.255.0
access-list private out deny ip any any
access-group private-out in interface private

Access lists are configured for the public interface to allow outbound connection requests from the public web server to the Internet but not the private network or the GIAC Enterprises corporate network. The access control list is applied to the public interface and packet inspection takes place on ingress.

access-list public-out deny tcp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list public-out deny tcp 192.168.2.0 255.255.255.0 5.0.0.0 255.0.0.0

access-group public-out in interface public

REMOTE ACCESS & LOGGING:

The following configuration information only allows secure shell connections from the remote IP address x.x.x0 to the outside interface of the firewall. This will prevent unauthorized users from remotely connecting to the firewall. Secure shell can be used to

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

remotely configure the firewall while protecting the confidentiality of the configuration data by encrypting all packets. In addition all logging information is being sent to a syslog server with the IP address 192.168.1.3.

ssh x.x.x.0 netmask 255.255.255.0 outside
ssh timeout 60

logging host 192.168.1.3
logging trap errors
logging on

AXENT RAPTOR FIREWALL 6.5 W/ POWERVPN SERVER SECURITY POLICY

Axent's Raptor firewall is a proxy-based firewall. All incoming and outgoing connections are terminated at the firewall and the firewall's proxy services perform the connections on behalf of the clients. The Raptor is very easy to configure out of the box and in the hands of a skilled security engineer, who knows all of the configuration files used by raptor, it offers granular control over almost all aspects of incoming and outgoing connections. In addition to the proxy-based security Raptor also has packet-filtering capabilities as well as VPN capabilities when purchased with the PowerVPN option. The default configuration of the Raptor firewall is to deny everything. No traffic will be passed unless a rule has been defined that specifically allows that type of traffic. There are too many configuration possibilities for the Raptor firewall to be described in depth for this practical. For brevity's sake only the most basic configurations and access controls will be described.

The Raptor firewall will be used to protect the GIAC Enterprises corporate network from unauthorized access as well as provide remote access for GIAC users by utilizing the PowerVPN server and RaptorMobile 6.5.1 client software. The IP addressing for the internal hosts consisting of a 5.0.0.0 class A IP block. The external interface of the Raptor firewall has an IP address 206.105.201.4 and is connected to the GIAC router. The following sections detail the configuration of the Raptor firewall and the PowerVPN server.

NETWORK INTERFACE CONFIGURATIONS:

The first step in configuring a Raptor firewall is to configure the interfaces. This will define the internal and external network interfaces and other additional options. The options are very important. They include identifying the internal network, port scan alerts, allow multicast traffic, SYN flood protection, spoof protection, creating packet filters, automatic port blocking, and some protection from denial of service attacks. Most configurations can be done from the GUI Raptor Manager console, but others must be done in configuration files.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Internal interface: named Internal-Interface and configured with the IP address: 5.0.0.1. The following options were selected for this interface (See Figure 3):

- This address is a member of your internal network.
- Enable SYN Flood Protection
- Enable Port Scan Detection

Under the Spoof Protected Networks tab all available networks are to be protected. If any packets are received on the external interface with the IP address of any protected network the packet will be dropped.

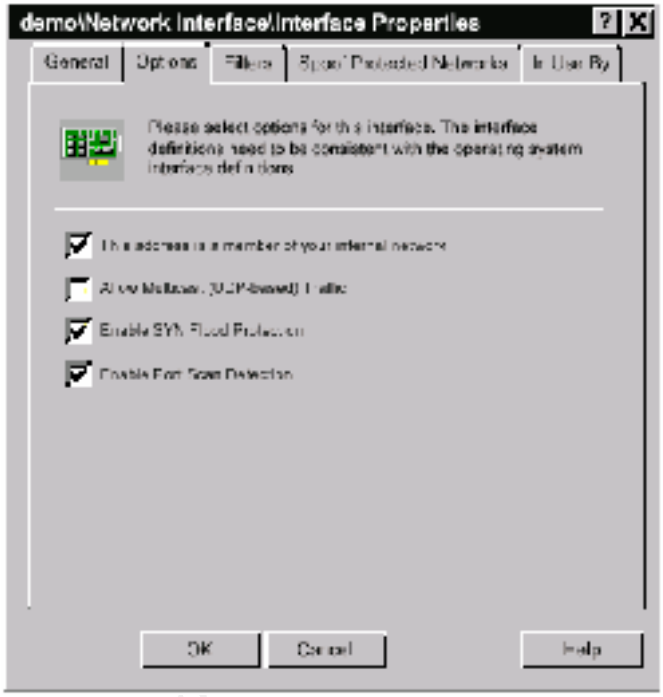

FIGURE 3: NETWORK INTERFACE OPTIONS

External Interface: names Outside-Interface and assigned IP address 206.165.201.4. All of the configurations for the Internal-Interface will be retained for the Outside-Interface except for being a member of the internal network.

DEFINING NETWORK ENTITIES:

The second step in configuring a Raptor firewall is to define the network entities. Raptor bases all configurations on pre-defined network entities. Raptor firewall ships with one predefined network entity, Universe. The Universe network entity is a wildcard entity with IP address 0.0.0.0. For the GIAC corporate network only five entities need to be defined:

- Subnet: Internal-LAN, the subnet used for the entire corporate network; 5.0.0.0 (See Figure 4).
- Host: Mail-Server, the internal mail server, 5.0.0.5
- Host: Virtual-Mail, a virtual server that will be used to redirect smtp connections, 206.165.201.5

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Host: PDC, the Primary Domain Controller on the GAIC corporate network, 5.0.0.6
- Security Gateway: VPN, the endpoint of remote access VPNs; 206.165.201.4

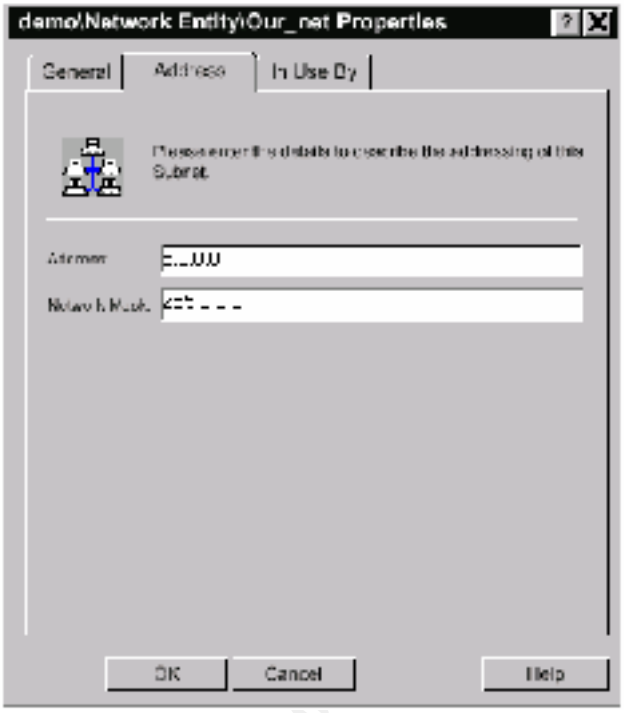

FIGURE 4: SUBNET ENTITY PROPERTIES

DEFINING RULES:

In order for traffic to pass through the firewall a rule has to be defined to specifically allow that type of traffic. Raptor uses a very simple process to define rules. To configure a rule a minimum of six fields need to be defined:

- Connection coming in via: the interface in which the packet will enter first.
- From source: the network entity that sent the packet.
- Destined for: the network entity that is the destination of the packet.
- Coming out via: the interface in which the packet will leave.
- Allow or deny the specific connection.
- Services: the predefined IP, TCP, UDP, and custom port number assignments.

There are many other variables that can be applied to each rule. Authentication services, time definitions for each rule, alerts, advanced services, and miscellaneous other configurations may be configured.

The GIAC corporate network will utilize the following rules:

Name	Connection coming in via	From source	Destined for	Coming out via	Allow/Deny	Services
1	Outside-Interface	Universe	Virtual-	Inside-	Allow	smtp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

			Mail	Interface		
2	Inside-Interface	Internal-LAN	Universe	Outside-Interface	Allow	http,https,ftp
3	Inside-Interface	Mail-Server	Universe	Outside-Interface	Allow	smtp
4	ANY VPN	Universe	Internal LAN	Inside-Interface	Allow	All
5	Inside-Interface	PDC	Universe	Outside-Interface	Allow	Cifs, nbdgram

Rule Descriptions:

Rule	Description
1	The mail server that resides on the corporate network should not be directly accessible from the Internet. A service redirection will be configured to use a virtual server (206.165.201.5) that will listen for smtp requests from the Internet and then the firewall will redirect the requests to the actual mail server (5.0.0.5). This rule will allow requests from the Internet to access the virtual server. Service redirection will be described in more detail in the Defining Service Redirections section.
2	Users on the GIAC corporate network require Internet access in order to perform their jobs. This rule limits the users to access servers on the Internet using http, https, and ftp protocols. See Figure 5.
3	This rule allows the mail server to send mail out to the Internet.
4	The rule allows employees using RaptorMobile VPN software to establish VPNs with the corporate network. These remote users will be authenticated by the VPN software, then the Windows NT Primary Domain Controller, and then given access to all services on the network.
5	This rule allows Microsoft network browsing on the network once a VPN has been established using cifs and netbios datagrams.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

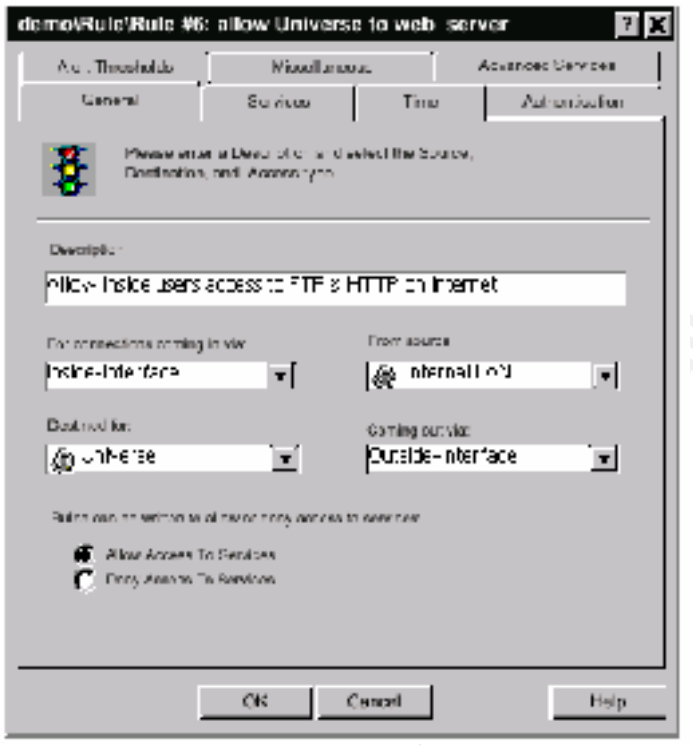

FIGURE 5: RULE DEFININTION

ADDRESS TRANSLATIONS:

Address translations will be configured so that all outgoing connections from the GIAC corporate network (5.0.0.0) will use a NAT pool of 206.105.210.20-206.105.210.40. This will hide the internal host addresses from the Internet.

DEFINING REDIRECTION SERVICES:

The service redirection feature of the Raptor firewall allows a user request to an IP address outside of the internal network be transparently redirected to a server on the inside network. This redirection will maintain the confidentiality of the actual server's IP address. In order to set up a service redirection a network entity with a virtual server address must be created and a rule must be defined to allow communication across the firewall.

For the GIAC Enterprises corporate network a service redirection was configured for the internal mail server. The mail server's IP address is 5.0.0.5. A virtual server was created with an IP address 206.165.201.5. As seen in Figure 6 the redirection is configured so that the virtual mail server would accept incoming smtp connection requests and redirect these to 5.0.0.5.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

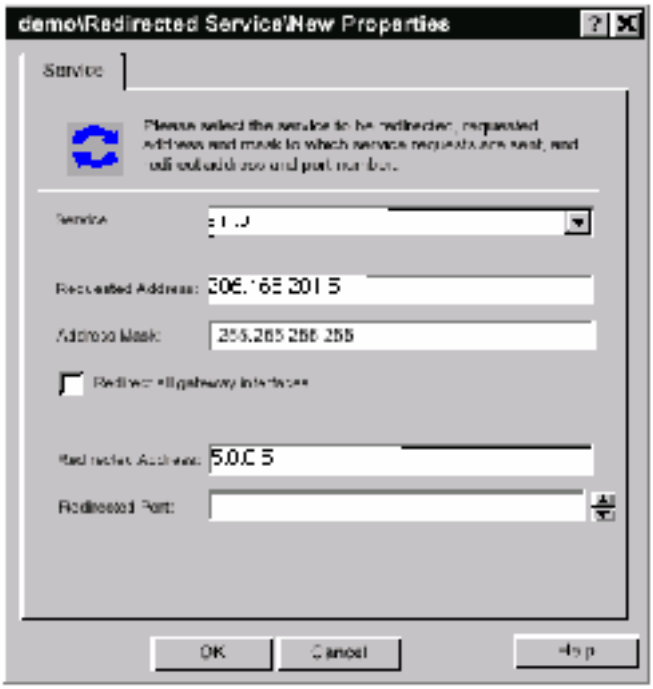

FIGURE 6: SERVICE REDIRECITON CONFIGURATION

CONFIGURING USER GROUPS:

Users and groups can be configured on the Raptor firewall in the same manner as many operating systems. They can be used for many purposes, mainly to authenticate inbound or outbound connections. Adding user and group configurations can give the firewall administrator very granular control of connections.

For the GIAC Enterprises corporate network users and groups are defined in order to authenticate and allow remote VPN access to the corporate network. The user group GIAC-Users was created, see Figure 7. Individual users are created and then made members of the GIAC-Users group. One user was created: default_ike_user. The configuration of the user group contains the following parameters:

- General name and description.
- Users: the individual users that are members of the GIAC-Users user group.
- VPN Authentication: extended authentication methods (none configured).
- VPN Network Parameters: primary/secondary DNS servers, primary/secondary WINS servers, and primary domain controller (5.0.0.6). This will allow remote users who establish a VPN with the Raptor firewall to be authenticated by the internal PDC.
- Automatically negotiate up to 5 tunnels.

Users are created and the following configuration information must be configured:

- Name, description, and User ID.
- Authentication: configure password
- Groups: add the user to the GIAC-Users group.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- VPN: enable IKE, add a Phase1 ID, configure IKE authentication method (for GIAC Enterprises corporate network the shared secret 2001gcfw will be used), and primary IKE user group will be defined (GIAC-Users).

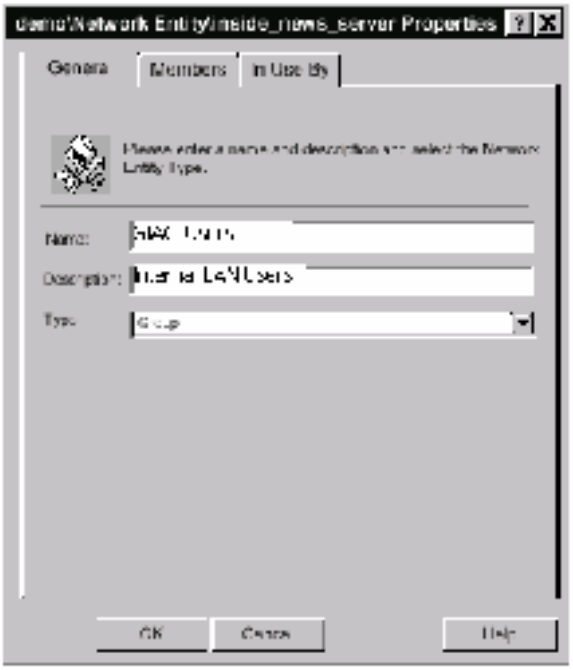

FIGURE 7: CREATING A USER GROUP

VPN SERVICE:

The PowerVPN server that was purchased as an add-on to the Raptor firewall provides the capability to establish IPSec compliant VPNs with remote users and other IPSec compliant gateway devices. The PowerVPN offers an easy to use management console that is built into the Raptor management console. In order to create a VPN six steps must be taken to configure the PowerVPN server:

1. Define network entities: hosts, user groups, subnets, and security gateways must be configured. These will be referenced in rules, policies, and for configuring tunnels.
2. VPN policies need to be defined.
3. IKE policies need to be defined.
4. Secure tunnels need to be created.
5. Rules need to be created to allow VPN connections to pass through the firewall.

For the GIAC Enterprises corporate network step one and six were previously configured in the Defining Network Entities and Defining Rule sections. Steps two through four need to be configured. The configurations are as follows:

Defining VPN Policies:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC Enterprises corporate network will use an IPSec/IKE policy. The following is the VPN policy configuration information:

- Name: GIAC-VPN
- Encapsulation Protocol: IPSEC/IKE
- Pass Traffic from the Secure Tunnel to Proxy Services: Enabled
- Data Integrity Preference: 1st SHA1, 2nd MD5 (See Figure 8)
- Data Privacy Preference: 1st 3DES, 2nd DES (See Figure 8)
- Data Compression: None (See Figure 8)
- Data Volume Timeout: 2100000 kilobytes.
- Lifetime Timeout: 480 minutes
- Inactivity Timeout: 0
- Encapsulation Mode: Tunnel Mode
- Data Privacy Algorithm Preference: Apply Integrity Algorithm to Data Portion of The Packet (ESP)
- Perfect Forward Secrecy: Enabled
- Diffie-Hellman Preference: 1st Group2, 2nd Group1

This configuration will ensure that if possible the most secure VPN will be negotiated.

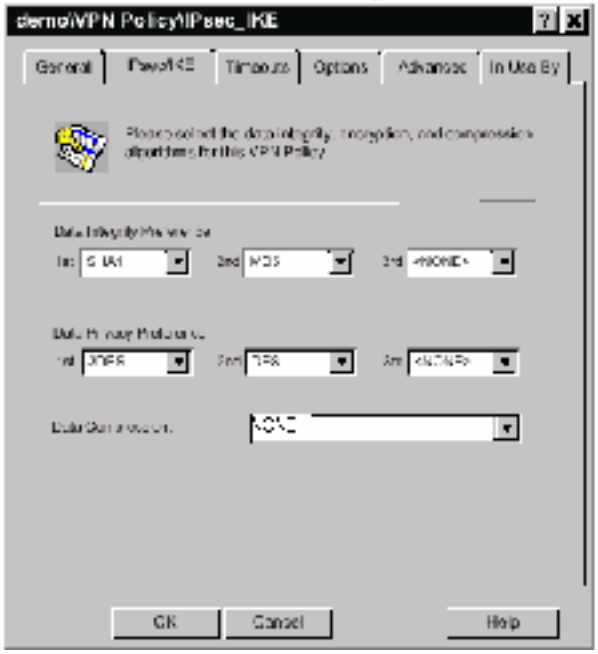

FIGURE 8: IPSEC/IKE CONFIGURATION

Defining IKE Policies:

The Raptor firewall and PowerVPN server comes with a predefined global IKE policy: global_ike_policy. GIAC Enterprises corporate network will use this predefined IKE policy. This is the most secure configuration possible. The following is the global_ike_policy configuration information (see Figure 9):

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Data Integrity Preference: 1st SHA1, 2nd MD5
- Data Privacy Preference: 1st 3DES, 2nd DES
- Diffie-Hellman Preference: 1st Group2, 2nd Group1
- Time Expiration: 1080

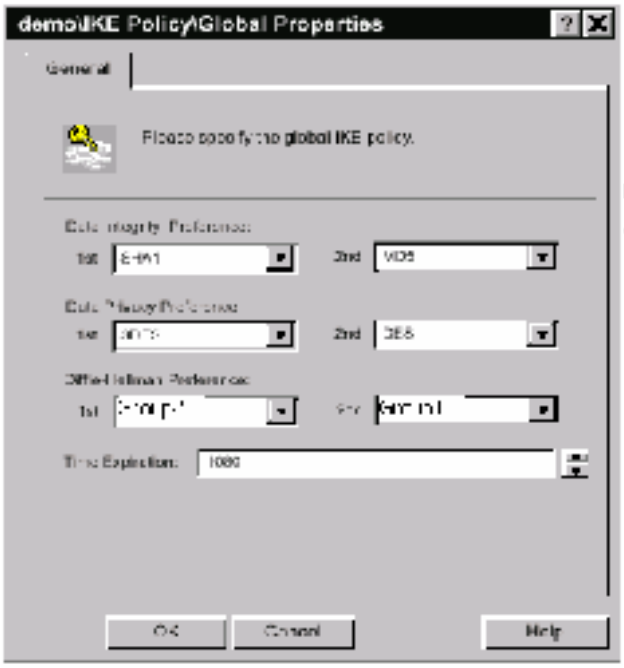

FIGURE 9: IKE POLICY CONFIGURATION

Creating Secure Tunnels:

In order to create a secure tunnel the following information is needed:

- Name and description.
- Local Entity: the destination of the remote VPN connection.
- Local Gateway: the encryption and decryption endpoint of the VPN at the firewall, typically the external interface of the firewall.
- Remote Entity: the network identity that is connecting to the internal network.
- Remote Gateway: the remote encryption and decryption endpoint of the VPN, typically a RaptorMobile client, remote firewall, single user, or a group of users.
- VPN Policy: a predefined VPN policy.
- IKE Policy: a predefined IKE policy.

For the GIAC Enterprises corporate network the configuration is as follows (See Figure 10):

- Name: GIAC-tunnel.
- Local Entity: Internal LAN (GIAC 5.0.0.0 network).
- Local Gateway: VPN (external interface of Raptor firewall, IP address 206.165.201.4).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Remote Entity: GIAC-Users user group.
- Remote Gateway: GIAC-Users user group.
- VPN Policy: the predefined GIAC-VPN policy.
- IKE Policy: the predefined global_ike_policy.

FIGURE 10: CONFIGURING A NEW SECURE TUNNEL.

RaptorMobile Client:

The RaptorMobile client software should be installed on each workstation that requires establishing a VPN connection with the firewall. The software is simple to install and configure. The following are the steps needed to configure the RaptorMobile client software.

- Log on to the client: logging into the RaptorMobile software with a username and a password protects the information stored in the software itself. This has no impact on connecting to the firewall itself. (See Figure 11)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FIGURE 11: RAPTORMOBILE LOGON

- Configuring the gateway information: configuring the security gateway enables the user to define the IP address of the remote gateway and additional client information. For the GIAC Enterprises corporate network the following information is included:(See Figure 12)
  IP Address of gateway: 206.165.201.4
  Shared Secret: 2001gcfw (previously defined)
  Client ID: default_ike_user (user account name)


FIGURE 12: SECURITY GATEWAY CONFIGURATION

- The security gateway is now configured and the user just has to select connect from the Gateways menu to establish the VPN with the firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT THREE: SECURITY ARCHITECTURE AUDIT

When establishing a secure perimeter or a particular network it is not enough to design architecture and configure equipment. It is necessary for the architecture to be tested and analyzed to ensure that the security policy that was created and implemented actually works. This section of the practical will identify and describe how GIAC Enterprise's perimeter will be tested and analyzed. This section will contain three parts: describing the vulnerability assessment, implementing the assessment, and the results of the assessment.

PLANNING THE ASSESSMENT

The purpose of performing an assessment is to ensure that physical and electronic controls that have been put in place to deny unauthorized access by the router and the firewalls actually work. The assessment will take place after normal business hours. This will be done as not to negatively affect the components of the network when clients are using the network. Some network devices may have unpredictable reactions to electronic assessment tools. In order to perform the assessment only two skilled security engineers will be needed for eight hours each to perform the actual assessment and a total of twenty fours hours to write up the assessment report. If the engineers labor category charges $200 per hour the total cost to GIAC Enterprises will be $8000. Each engineer will use various open source software applications that will enable the engineer to identify what services are available on the router, firewalls and servers, identify what packets are allowed to enter each network from the Internet, and what packets are allowed into each network from the internal network. The assessment will take place from both externally and internally.

IMPLEMENTING THE ASSESSMENT

In order to assess the security of the primary firewall and the router used by GIAC Enterprises a few tools will be used inside the network and outside the network. The primary function of the network perimeter is to control packets that are passing in and out of the networks along with being passed between the networks. The following tools will be used for the assessment:

Tool	Description
Nmap	Network mapping application. Nmap can be used to perform TCP connect scanning, TCP SYN scanning, TCP FIN/XMAS/Null scanning, TCP FTP bounce scanning, SYN/FIN fragmented scanning, TCP ACK scanning, UDP ICMP port unreachable scanning, ICMP scanning, TCP Ping scanning, RPC scanning, remote operating system identification, and reverse-ident scanning.
Hping	Network tool, which will enable a user to send custom ICMP, TCP, and UDP packets to a target and display the results. Hping can be used to test firewall rules, port scanning, test network performance, MTU discovery,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	remote operating system identification, TCP/IP stack fingerprinting, and traceroute.
Tcpdump	An application that displays all packet headers of packets traversing the local network segment. This can be used to identify if unauthorized packets are being allowed through security devices such as packet filtering routers and firewalls.
PacketX	Firewall testing tool, which allows the user to create complete TCP/IP packets and send them through a firewall.

From a source outside of the GIAC Enterprises network the following tests will be run to assess the security controls configured on the router and firewalls. During these tests a computer on each GIAC Enterprises network will be will be running Tcpdump and logging the packet activity. This will be used to identify and document which packets were allowed to pass the routers and the firewalls.

1. Using Nmap a port scan of the three interfaces of the router will identify the services that are listening for connections. This will validate the secure configuration of the router.
2. Using Nmap a standard ICMP port scan (ping sweep) of the internal IP blocks will be performed to validate weather ICMP packets are allowed or denied into the networks. The Nmap commands are as follows

Nmap –v –sP 206.165.201.0/24
Nmap –v –sP 206.105.201.0/24

3. Using Nmap a TCP SYN scan (half-open) of the internal IP address blocks will attempt to map the network without using ICMP. In addition the results will show which services are available on internal hosts. The only services that should be listed I the results are the services that have been allowed on the routers and the firewalls. The option for remote operating system identification will be enabled. The commands are as follows.

Nmap –v –sS –O 206.165.201.0/24
Nmap –v –sS –O 206.105.201.0/24

4. The same tests as performed in steps 1-3 will be duplicated with Hping in order to confirm the results of the Nmap scans. The results should be identical.
5. Hping will also be used to create packets with illegal TCP flag settings, SYN floods, and other custom packets to see how the router and firewall handles these situations.
6. Hping will be used to validate which services on which hosts will accept connections from external hosts on the Internet, IP addresses of partners and suppliers, and from internal hosts on the public, private, and corporate network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The results of these tests will validate if the access control lists and firewall rules are configured properly.

7. Using PacketX custom packets will be created and sent across the router and firewalls to test if the packets get dropped or are passed. Packets will be generated using private non-routable IP addresses (192.168.0.x, 172.16.x.x, 10.x.x.x) as the source address. Figure 13 displays the PacketX options for creating custom packets. These tests will be performed from a source outside of the network. In addition packets will be created and sent using arbitrary IP addresses, IP addresses of internal hosts, and IP addresses of partners and suppliers. In order to document the results of these tests the firewall and router logs will be reviewed as well a the Tcpdump output that is running on a computer on each network.
8. In order to verify if the VPN configurations of the Raptor Firewall and the router a packet sniffer such as Tcpdump along with a packet sniffer that can show the actual data, Sniffer Pro, will be run. The results of the packet sniffing should display the IPSec connection negotiation and the actual encryption of the data.

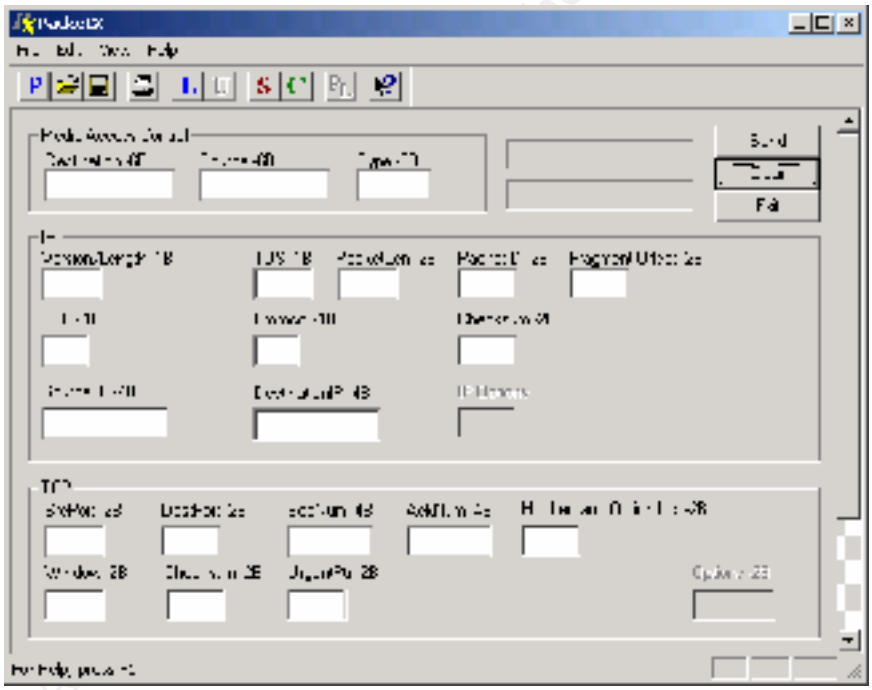

FIGURE 13: PACKETX OPTIONS

RESULTS

The secure perimeter designed in this document is a completely theoretical. Actual output from the scans and test performed using Nmap, Hping, Tcpdump, and PacketX cannot be displayed. If output from the tests were available it should completely validate the configurations made in for the router and the firewalls. If any discrepancies were found the configurations should be scrutinized to see if errors were made in the configurations or if a possible bug in the software exists that needs to be fixed. The architecture that was designed for the GIAC Enterprises networks is a simple design that

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

revolves around a single connection to the Internet. The same router connects all the corporate, private, and public networks. If this router is compromised or the victim of a denial of service attack, all three networks will be affected. An alternative architecture that will be slightly more expensive but more secure architecture would be one in which the three networks had absolutely no connectivity with each other. Figure 14 displays an example of this. Using this alternative architecture all three networks have different IP address blocks and different connections to the Internet. Having three distinct and separate networks will enable the networks to function independently so if one of the networks is compromised or is down for any other reason the other two networks will not be affected. All three networks will have a network-based intrusion detection system that is located after any possible decryption point and will identify and possibly stop an attack. Reverse proxy servers will now protect each network that supports a web server from various attacks. These servers will accept all incoming requests for the web server and control what can and cannot be done. In addition the GIAC Enterprises corporate network will have a second firewall that will add an additional security layer between the corporate network and the Internet.

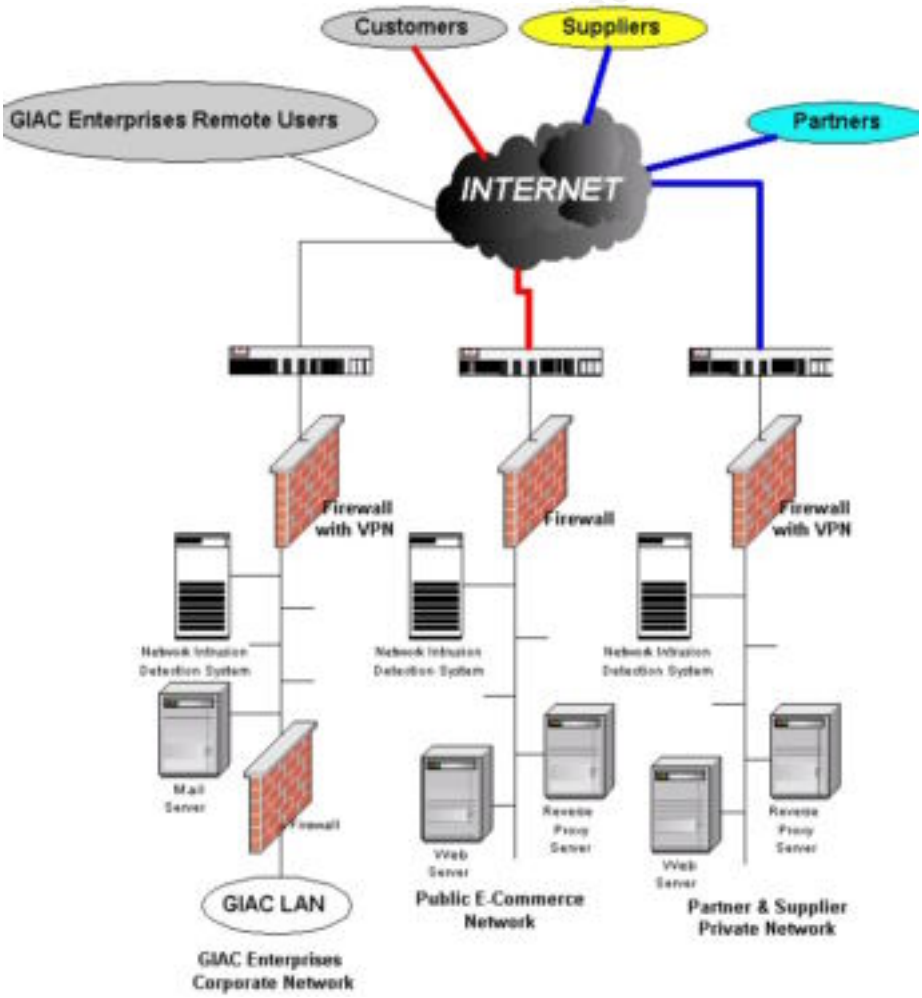

FIGURE 14: ALTERNATIVE ARCHITECTURE

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT FOUR: DESIGN UNDER FIRE

For assignment four Clement Dupuis's practical assignment was chosen as the design under fire. Clement's practical was submitted on September 8, 2000 and is available on the SANS web site at the following URL: http://www.sans.org/y2k/practical/clement_dupuis.doc. Using Clement's architecture in his practical three attacks will be designed to attack the architecture. The network architecture is included below in Figure 15.

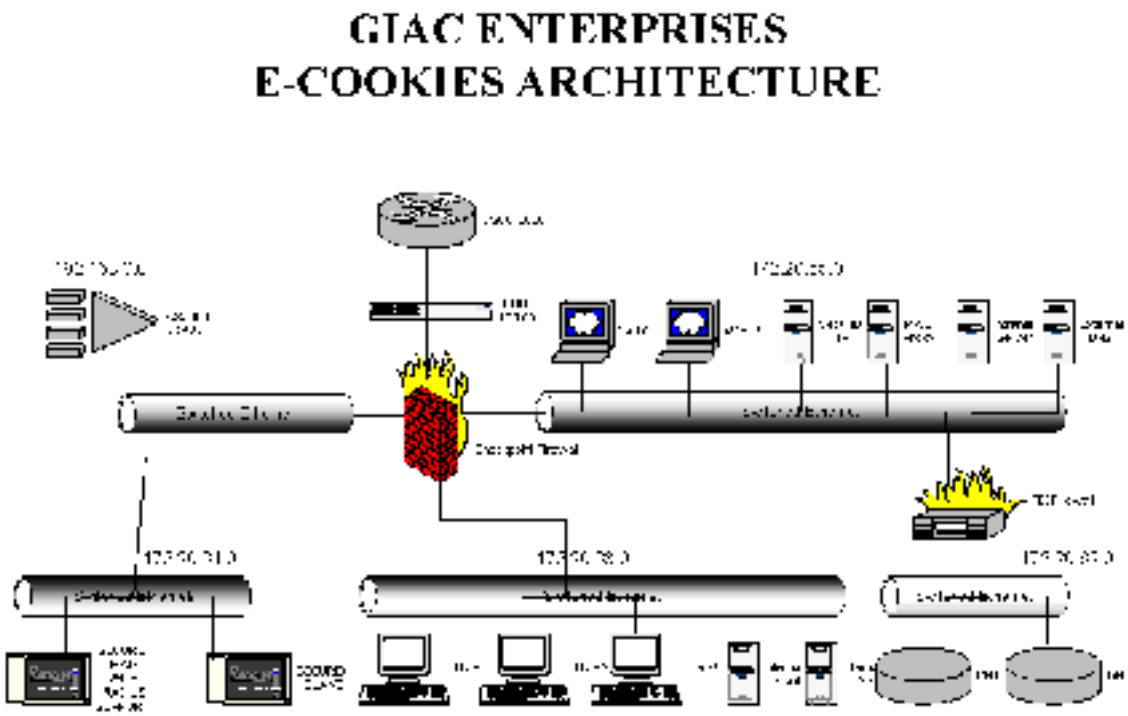

FIGURE 15: CLEMENT DUPUIS'S ARCHITECTURE FOR GIAC ENTERPRISES

ATTACK AGAINST THE FIREWALL

After performing research for specific vulnerabilities associated with various types of firewalls, there are not very many well-known vulnerabilities that are publicly available. The primary firewall chosen by Clement Dupuis for his architecture is the Checkpoint Firewall-1. Checkpoint Firewall-1 has a few vulnerabilities associated with it that were published on the Internet. The architecture shown in figure 15 shows only one firewall in which all traffic must pass through in order to reach one of the five networks connected to the firewall. Using one firewall may lead to a single point of failure. If an attack is directed at the firewall itself and the firewall gets compromised or is rendered useless no traffic will travel into the networks or from the internal networks out to the Internet.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There is a specific vulnerability associated with the Checkpoint Firewall-1 that may cause a denial of service by consuming all of the resources of the firewall itself resulting in all traffic being stopped at the firewall. Firewall-1 reassembles all packets of a datagram before being checked by the rule set defined on the firewall. If a stream of large sized fragmented IP packets are send through the firewall the code which controls the logging of these fragmented packets may consume all available CPU cycles to be consumed. Once all the available CPU cycles are consumed no resources will be available to process traffic and forward, resulting in the failure of the firewall. Details of the vulnerability can be found at http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html. In order to exploit this vulnerability an IP fragment application such as jolt2 can be used to fragment packets and send them to the firewall. Once all the resources are consumed by the packet reassemble logging function of the firewall the firewall will be rendered useless, effectively stopping all traffic from entering or exiting the internal networks from the Internet or destined for the Internet.

DENIAL OF SERVICE ATTACK

During the last year or two there have been numerous, highly publicized, distributed denial of service attacks have been launched against some of the most popular web sites on the Internet. Essentially extremely large volumes of packets are sent to the network that supports the web sites from compromised hosts on the Internet. The bandwidth capacity of the network that supports the web site gets congested and legitimate traffic does not reach the web server to the bandwidth resources being consumed by the attacker traffic. In order for these attacks to take place a large number hosts must be compromised in order to produce the volume of traffic needed to completely congest the bandwidth used to connect to the Internet. These compromised hosts commonly wait for some stimulus before an attack is launched.

In order to subject the design shown in figure 15 to a denial of service attack the Stacheldraht denial service attack tool will be used. The Stacheldraht denial of service attack tool is made up of two parts, a master and a daemon. First, numerous hosts on the Internet are compromised, commonly home connections using permanent cable modem or digital subscriber lines (DSL). Once these systems have been compromised the daemon is installed and configured. The daemon listens for connections from the masters. When the masters connect to the daemon systems using encrypted communications the daemons then initiate the denial of service attack. The Stacheldraht denial service attack tool can be configured to generate an ICMP flood, SYN flood, UDP flood, and smurf style attacks. More information about the Stacheldraht denial of service attack tool can be found at http://staff.washington.edu/dittrich/misc/stacheldraht.analysis. In this example a SYN flood will be generated to create a potential denial of service attack on Clement's architecture. This SYN flood attack is aimed at consuming the resources of the firewall or other host that controls traffic by opening as many half-open sessions.

The Checkpoint Frewall-1 has two features built in the stateful packet inspection engine that can be enabled to defend against a SYN flood attack, SYNDefender Relay and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SYNDefender Gateway. The SYNDefender Relay ensures that an actual TCP three-way handshake is can be completed before the connection is passed onto an internal host. The SYNDefender Relay accepts the SYN from an external host on behalf of the internal host and ensures that an ACK is received before passing on the connection request to the internal host. If an ACK is not received within seconds the connection is immediately terminated. This SYNDefender Relay protection is not enough to protect from a SYN flood attack by itself. The second feature needed to protect against the sheer volume of connection requests in a SYN flood attack is the SYNDefender Gateway. The SYNDefender Gateway controls the backlog queue, which is usually the focus of a SYN flood attack. SYNDefender Gateway moves legitimate connections in which a legitimate ACK packet is received immediately out of the backlog queue and is now considered an open connection to the internal host. If a valid ACK response is not received almost immediately from a host requesting a connection than a RST packet is sent back and the connection attempt is removed from the backlog queue. These two features of the Checkpoint Firewall-1 will working in parallel will protect against SYN flood attacks. Additional information about the SYNDefender Relay and the SYNDefender Gateway can be found at http://www.checkpoint.com/products/firewall-1/syndefender.html.

COMPROMISING AN INTERNAL HOST

Screening routers and firewalls are commonly implemented to protect computer systems and various services from unauthorized access. Coupled with protecting systems with firewalls and screening routers hardening the operating systems can lead to a fairly secure environment. These actions commonly will deny all unauthorized access. But there are computer systems that have services that are designed to be accessible from any location on the Internet, such as web servers, DNS servers, and mail servers. In order to make these systems available to the public holes must be created in firewall and screening router security policies. These services are most commonly attacked and successfully compromised due to their access to the public. Many attacks are successful because the content of packets are not screened at all, IDS signatures are not up to date, operating systems are not up to date, and unknown vulnerabilities that are impossible to defend against. In selecting an internal target to attack in Figure 15 I select the web servers that are located behind the primary firewall. The web servers have been selected due for numerous reasons: 1.) Access is to the web server application is not protected in any way by the firewall or the screening router. 2.) Web server applications are constantly under attack and a great number of exploits in the web sever software along with poor software-programming practices are known and easily found. 3.) The quality, robustness, and functionality of a company web site have a direct effect on the success of a company. If a web server is compromised the results of this can cripple a companies reputation. 4.) For a busy web site it may be possible to hide attempts to compromise the server in legitimate traffic.

The first step taken when attempting to compromise an internal web server is to identify everything about that web server's operating system, web server software, and the type of web application being served by the software. This information is more often than not very easy to acquire. The web server gives much of this information up every time a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

connection is established. The majority of this information is contained within the HTTP header. Other information can be identified by looking at the source code of a web page and noticing if a database is attached in some way, what type of files are being served (html, jsp, asp, dhtml, cfm, etc.). These can tell a great deal of how the web site is supported and run. Once the majority of this information is known it is time to start researching on the web for vulnerabilities. These vulnerabilities can be problems with the operating system, the web server software, the applications that run the site, insecure configuration of the web server, and poor coding practices.

After the vulnerabilities have been researched it is time to select which one will achieve the results that the attacker is looking for. Does the attacker want to render the system useless? Does the attacker want to gain command line access to the system? Does the attacker want the web server to disclose the contents of files that should not be disclosed to the public? Does the attacker want to be able to upload a root kit to the server to enable unlimited control? These are all questions that have to be answered. Once the attacker has chosen a particular vulnerability to exploit the will most likely take steps to perform the attack from a system that will make it nearly impossible to trace the origin of the attack back to the attacker. In many cases an attacker will compromise another host on the Internet and install any tools needed to compromise the web server so that at a later time the attacker can come back and perform the attack.

All that is left is to do is figure out what to do with the web server when it is compromised and select the right time to make the attack.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

REFERENCES

Prentice hall. (1999). IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks. Upper Saddle, NJ: Doraswamy & Harkins.

New Riders Publishing. (1999). Network Intrusion Detection: An Analysts Handbook. Indianapolis, IA: Stephen Northcutt.

O'Reilly & Associates. (1996). Practical Unix and Internet Security. Sebastopol, CA: Simson Garfinkel and Gene Spafford.

Osborne/McGraw-Hill. (1999). Hacking Exposed: Network Security Secrets & Solutions. Berkeley, CA: Stuart McLure, Joel Scambray, and George Kurtz.

Axent Technologies Inc. (2000). Raptor Firewall and PowerVPN 6.5 Configuration Guide for NT. Rockville, MD: Axent Technologies Inc.

Denial of Service Attacks Using TFN2K and Stacheldraht Programs. [On-line]
Available: http://xforce.iss.net/alerts/advise43.php

The "Stacheldraht" Distributed Denial of Service Attack Tool. [On-line]
Available: http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

Cisco VPN: Intranet and Extranet VPN Business Case Scenarios. [On-line]
Available: http://www.cisco.com/univsercd/cc/td/doc/product/core/7100/swcg/6342gre.htm

Cisco Pix 5.3: Installation Guide for the Cisco Secure Pix Firewall Version 5.3. [On-line]
Available:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/install/index.htm

Cisco Pix 5.3: Configuration Guide for the Cisco Secure Pix Firewall Version 5.3. [On-line]
Available:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/config/index.htm

Checkpoint Firewall Alerts Site. [On-line]
Available: http://www.checkpoint.com/techsupport/alerts

Security Focus [On-line]
Available: http://www.securityfocus.com

SecurityPortal [On-line]
Available: http://www.securityportal.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Infosyssec [On-line]
Available: http://www.infosyssec.com

Hack-Net [On-line]
Available: https://www.hack-net.com

Packetstorm [On-line]
Available: http://www.packetstorm.securify.com

Carnegie Mellon Software Engineering Institute CERT Coordination Center [On-line]
Available: http://www.cert.org

Network Security Library [On-line]
Available: http://secinf.net

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.