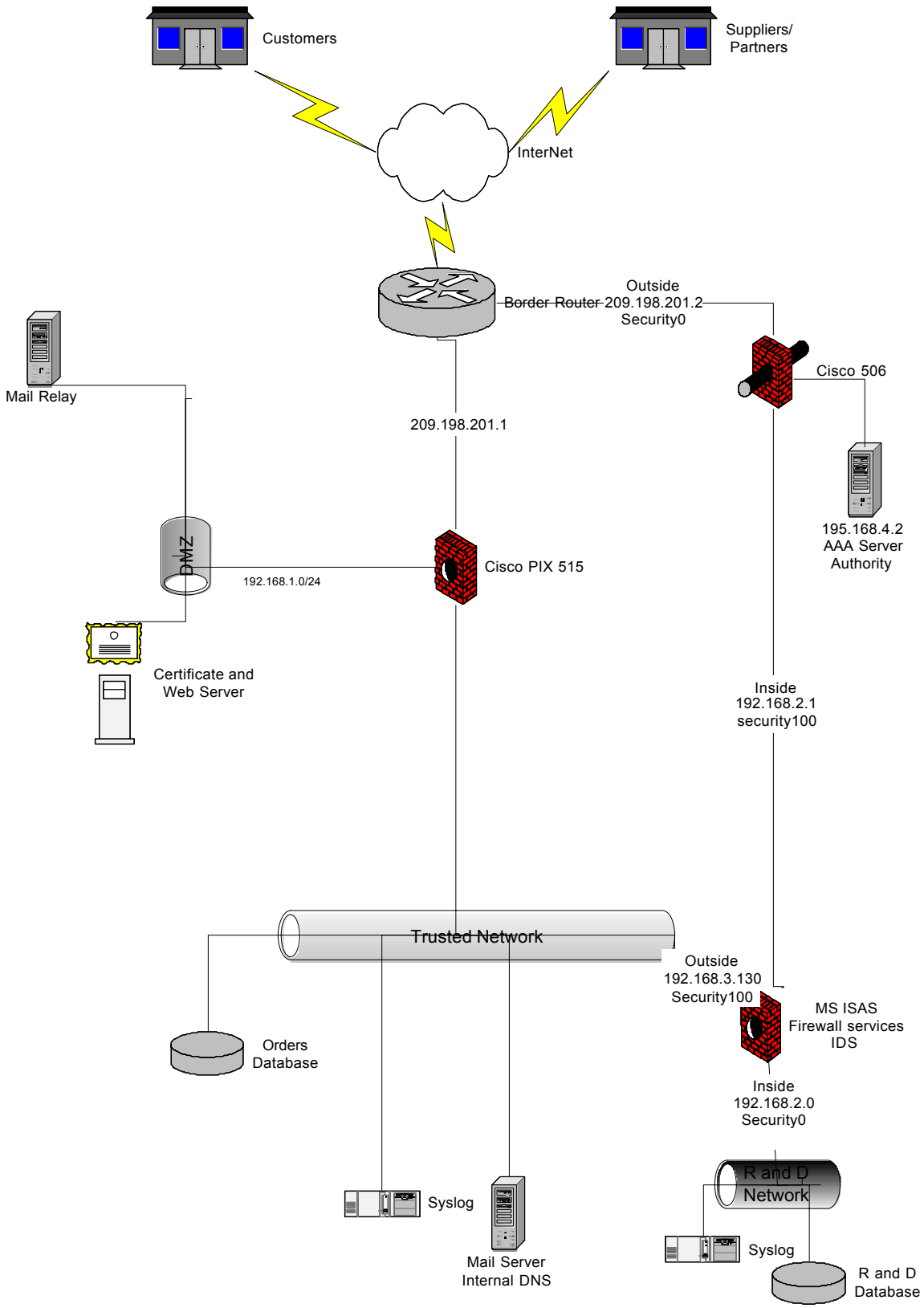
Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst Practical Exam

Prepared By:
Jack Green
October 10, 2001

Version 1.6



Overview

GIAC Enterprises (GE) is in the singular business of authoring fortunes to be included in fortune cookies. These fortunes are then translated into different languages by any of six business partners. Another seven business partners are responsible for printing these fortunes and shipping them to about 12 customers on each continent. GIAC Enterprises, itself, has 30 employees in departments including research and development, accounting, administration and information technology.

Figure 1 shows a summary of the required information for each business partner. Printers/Distributors must retrieve *order* information which includes the specific fortunes to be printed and to whom the order must be shipped. Translators must have access to the *Research and Development* database in order to retrieve, render the fortunes into other languages and insert those newly translated fortune into the pre-production database. Internal employees, authors, create the pre-production fortunes.

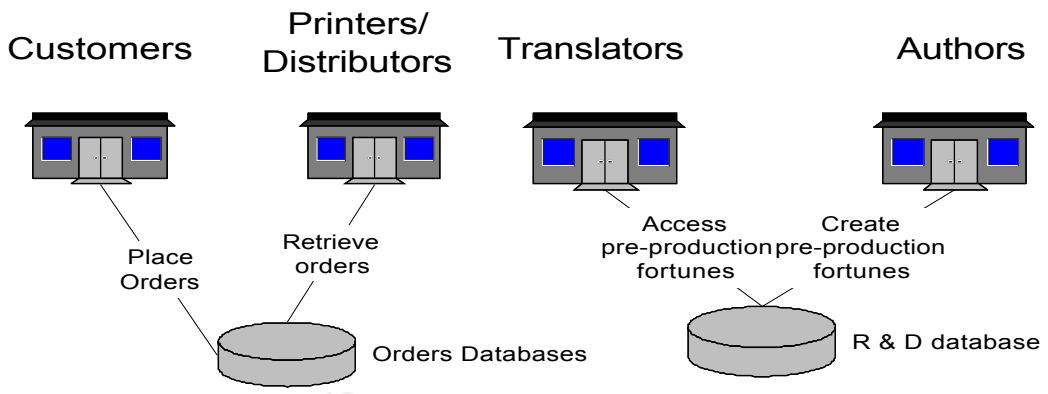


Figure 1 – GIAC Enterprises Business Process Summary

Assignment 1 – Security Architecture (15 points)

Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings. Your architecture must include the following components:

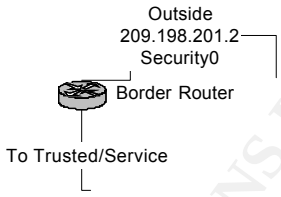
- filtering routers;
- firewalls;
- VPNs to business partners;
- secure remote access; and
- internal firewalls.

Your architecture must consider access requirements (and restrictions) for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

Include a diagram or set of diagrams that shows the layout of GIAC Enterprises' network and the location of each component listed above. Provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

Border Router



Our defense in depth begins with a Cisco 3640 standing as the border router for GE. This router is configured with a one-port high speed serial interface connected to a T1 (1.5 Mbps) line. A T1 connection will provide adequate bandwidth for GE's small business base.

Figure 1

A Four-port Ethernet network module is installed in the second of four slots in the 3640. Figure 2 shows that two of these 100mb ports are connected to the VPN network and the trusted network.

Given the nature of GE's vertical (i.e. small) market, it is logistically possible to implement a static routing table. The 3640 will be responsible for routing packets to each interface based upon the configuration to be described later in the paper**.**

Virtual Private Network (VPN) Concentrator and Firewall

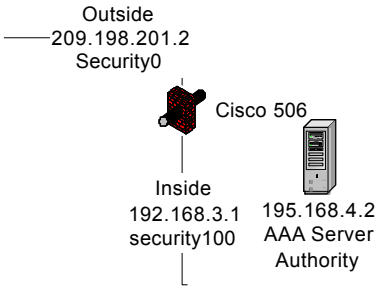
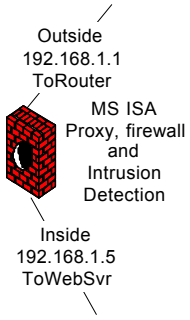


Figure 2 shows that the 192.168.3 network handles VPN communication and access control services for the Suppliers/Partners network. A Cisco PIX 506 was chosen to deliver VPN tunneling services with IPSEC (IKE/DES). Client-side services will be provided by the Cisco VPN Client.
The concentrator was placed on the firewall to allow packet inspection before processing data requests. The AAA server authenticates client requestors.

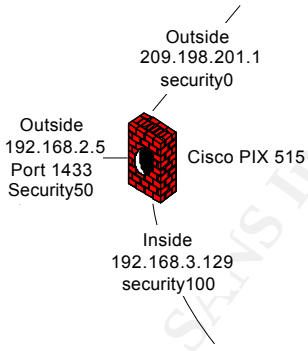
Figure 2



The *Microsoft Internet Security and Acceleration Server (ISAS)* has been placed in front of the research and development department to screen the trusted network and to provide a measure of intrusion detection services.

The use of both Cisco and ISAS firewalls provides an additional level of defense. Should the bad guyz' defeat one set of access controllers they cannot have free reign on the R & D network without defeating the other. As you'll, Suppliers/Partners provide a specific IP address and are permitted access to a specific program
directory on a specific server.

Figure 3

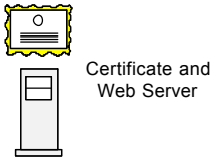


The firewall protecting the trusted network is a Cisco 515R. This router was chosen on the basis of its ability for expansion. Additionally, the common OS between the 506 and the 515 ease IT staff administration problems.

The 515R provides for three Ethernet ports. Of note is the port to the service network providing only MS SQL Server IP connector services to the orders database through only port 1433.

Figure 4

Customer Web Server and Certificate Server



A single web server meets the purchasing needs for this vertical market product. It is an IIS 5.0 running an ASP store. Frequently viewed [ages are stored on the ISAS server. The

server makes calls to the database via a second Ethernet card to the orders database as needed.
Figure 5

Certificates are offered via MS' Certificate Services. These 128 bit SSL certificates are issued by Verisign.

Email Server

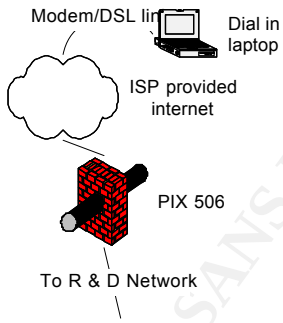
QMail is a *NIX based mail relay agent that has been tested as secure. This unit will reside on the service network. It will be configured to only forward mail from GE's ISP and the trusted network's mail server.

Written by DJ Bernstein, QMail has, to date, been a secure system. In his words,

> *In March 1997, I offered $500 to the first person to publish a verifiable security hole in the latest version of QMail: for example, a way for a user to exploit QMail to take over another account. My offer still stands. Nobody has found any security holes in QMail.*

Figure 6

Remote Access



Partners, Suppliers and employees of the Research and Development department are provided remote access through their local ISP. Like the configuration for VPN, each participating client must also have the Cisco VPN client installed.

Figure 7

Syslog Server

The syslog servers are FreeBSD based. They communicate with the routers/firewalls via syslogd. Logs are written to /var/log/ local*n*.debug. Logs are kept on two machines to ease firewall administration. *Figure 8*

Assignment 2 – Security Policy (35 points)

Part 1 – Define Your Security Policy (25 points)

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific Access Control List (ACL), firewall rule set, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

You **must** include the complete policy (ACL's, rule set, IPSec policy) in your paper. It is not enough to simply state "I would include ingress and egress filtering…" etc. The policies may be included in an Appendix if doing so will help the "flow" of the paper.

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

Border Router Configuration

As the first line of defense, the border router should be secure and should filter unnecessary packets.

First, let's set our global parameters begin by setting the login and a few parameters. Using a rolled cable[1] and a serial communications program like hyperterm ™, Connect to the router and power on.
At the prompt of the router type ***"conf t"*** to enter the global configuration prompt:

[1] Rolled — the colored wires at the end of the cable are in the reverse sequence of the colored wires at the other end of the cable

router (config) #

Name the router

router (config) # Hostname 3640

Set the encrypted the password on the 3640.

3640 (config) # service password-encryption

Set the enable the password on the 3640.

3640 (config) # enable secret (password)

This command warns unauthorized users to stay off.

3640 (config) # banner login #Warning No Unauthorized use permitted#

Secure the router so that only the trusted network can use it.

3640 (config) # access-list 1 permit 192.168.1.0 0.0.0.255
3640 (config) # line vty 0 4
3640 (config) # access-class 1 in

This command will turn on the logging feature of your 3640. The 3640 will first buffer the log so that it can be viewed using the command: “sh log” at the command prompt.

3640 (config) # logging buffered

Set our syslog server.

3640 (config) # logging 192.168.1.131

Define a logging facility (pipe) through which we may communicate with the syslog daemon.

3640 (config) # logging facility local0 (to local 8)

Set a trap for the errors. As listed below, the error levels range from least urgent (debug) to heart stopping (emergency). When trapping events, trap levels are cumulative. That is, if you set the trap for critical, you’ll also get alert and emergency. You won’t get those below. Hence I’ll set trapping for debug and collect everything

emergency	0
alert	1
critical	2
error	3
warning	4
notification	5
informational	6
debug	7

3640 (config) # logging trap debug

Source routed packets are almost always used for spoofing, let's drop them.

3640 (config) # no ip source-route

Disable finger service. It can be used to find who is logged into the router and from where.

3640 (config) # no service finger

The Cisco Discovery Protocol (CDP). CDP is used to find and identify Cisco devices on the network. CDP is blocked to impair reconnaissance.
3640 (config) # no cdp enable

Disable ports below TCP/UDP 20 such as chargen, echo, discard, and etc.

3640 (config) # no service tcp-small servers
3640 (config) # no service udp-small servers

Disable NTP as we're not using it.

3640 (config) # ntp disable

This disables the http server used for administration on the 3640. This command is turned off by default on most 3640s.

3640 (config) # no ip bootp server
3640 (config) # no ip http server

Set up routes to the appropriate networks.

3640 (config) # ip route 209.198.201.1 255.255.255.252 e0
3640 (config) # ip route 209.198.201.2 255.255.255.252 e1

This command will allow you to enter the configuration mode for Serial Interface 0. The following commands are related to other interfaces on the 3640.

3640 (config) # int s0 - Interface Serial0
3640 (config) # int e0 - *Interface Ethernet 0 to VPN*
3640 (config) # int e1 - *Interface Ethernet 1 to Trusted*

After entering the Interface Configuration mode the prompt will change to the Interface Config prompt:

3640 (config-if) #

All commands entered at the config-if prompt will be applied to that given interface. The following commands are interface specific.

Prevent smurf attacks by blocking traffic to the broadcast address

3640 (config-if) # no ip directed-broadcast

To prevent redirect of return traffic:

3640 (config-if) # no ip redirects

SNMP is unnecessary for GE. We will disable it. SNMP v2 offers an MD5-based digest authentication scheme should GE ever choose to implement SNMP.

3640 (config-if) no snmp

Disable CDP on all interfaces.

3640 (config-if) # no cdp enable

ICMP should not give out host unreachable errors to hackers doing reconnaissance.

3640 (config-if) # no ip unreachables

No ip redirects: This command is used to block packets that can be redirected. A malicious user may be able to redirect the path that a packet will take if this command is not applied.

This command will apply the access list 101 on incoming traffic.

Access group 101 in

We will create an access list to block all private addresses, multicast, and loop-back addresses from entering our network from the Internet. These addresses should not be coming into our network. These addresses are usually used for malicious reasons.

The following access list is applied to the Internet 3640:

- blocks and logs all traffic from private address 10.*

3640 (config) # access-list 105 deny 10.0.0.0 0.255.255.255 log

- blocks and logs all traffic from the private addresses range 172.16.*-172.32.*

3640 (config) # access-list 105 deny 172.16.0.0 0.15.255.255 log

- blocks and logs all traffic from private address 192.168.*

3640 (config) # access-list 105 deny 192.168.0.0 0.0.255.255 log

- blocks and logs all traffic from the loop back address 127.*

3640 (config) # access-list 105 deny 127.0.0.0 0.255.255.255 log

- 0.0.0.0 is an invalid address and should be blocked and logged.

3640 (config) # access-list 105 deny 0.0.0.0 log

- blocks and logs all traffic from multicast address range 224.* - 239.*

3640 (config) # access-list 105 deny 224.0.0.0 15.255.255.255 log

- blocks and logs all traffic from experimental address range 240.* - 255*

3640 (config) # access-list 105 deny 240.0.0.0 15.255.255.255 log

- blocks and logs all login services

3640 (config) # access-list 105 deny tcp any any range ftp telnet log
3640 (config) # access-list 105 deny range exec lpd log

Block RPC and NFS and log any activity

3640 (config) # access-list 105 deny udp any any eq sunrpc log

3640 (config) # access-list 105 deny tcp any any eq sunrpc log
3640 (config) # access-list 105 deny udp any any eq 2049 log
3640 (config) # access-list 105 deny tcp any any eq 2049 log
3640 (config) # access-list 105 deny udp any any eq 4045 log
3640 (config) # access-list 105 deny tcp any any eq 4045 log

- Block NetBIOS and log any activity

3640 (config) # access-list 105 deny tcp any any 135 log
3640 (config) # access-list 105 deny udp any any 135 log
3640 (config) # access-list 105 deny udp any any range 137 138 log
3640 (config) # access-list 105 deny tcp any any eq 139 log
3640 (config) # access-list 105 deny tcp any any eq 445 log
3640 (config) # access-list 105 deny udp any any eq 445 log

- Block Xwindows and log any activity

3640 (config) # access-list 105 deny tcp any any range 6000 6255 log

- Allow only ACKed tcp packets to our network

3640 (config) # access-list 105 permit tcp any *a.b.c.d w.x.y.z* gt 1023 established

- Allow SMTP traffic to only the mail server(s)

3640 (config) # access-list 105 permit tcp any *192.168.2*.7 0 eq 25

- Allow DNS traffic to only the name server(s)

3640 (config) # access-list 105 permit tcp any *a.b.c.d* 0.0.0.0 eq 53
3640 (config) # access-list 105 permit udp any *a.b.c.d* 0.0.0.0 eq 53

- Allow HTTP traffic to only the web server(s)

3640 (config) # access-list 105 permit tcp any *192.168.2*.6 0 eq 80

- Access list 105 will be applied to inbound traffic on serial interface 0 with the following command:

3640 (config) # int s0
3640 (config-if) # ip access-group 105 in

- Access list to be applied on the internal interface:

3640 (config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 any
3640 (config)# access-list 101 deny ip any any

The access list above will allow servers on the Service network to access the Internet and deny any other traffic.

We will now want to apply it to the Internal Ethernet interface of the 3640 along with some of the security commands explained earlier**.**

3640 (config)# interface e0
3640 (int-config)# ip access-group 101 in
3640 (int-config)# no ip directed-broadcasts
3640 (int-config)# no ip unreachables
3640 (int-config)# no ip redirects
3640 (int-config)# no snmp
3640 (int-config)# no cdp enable

The GIAC Internet 3640 configuration should look like the following:

no ip source-route
no service tcp-small servers
no service udp-small servers
no service finger
no cdp run
ntp disable

interface serial 0
ip access-group 105 in
ntp disable
no ip directed-broadcasts
no ip unreachables
no ip redirects
no snmp
no cdp enable

interface Ethernet 0
ip access-group 101 in
no ip directed-broadcasts
no ip unreachables
no ip redirects

no snmp
no cdp enable

access-list 105 deny ip 10.0.0.0 0.255.255.255 any log
access-list 105 deny ip 172.16.0.0 0.15.255.255 any log
access-list 105 deny ip 192.168.0.0 0.0.255.255 any log
access-list 105 deny ip 127.0.0.0 0.255.255.255 any log
access-list 105 deny ip 0.0.0.0 0.255.255.255 any log
access-list 105 deny ip 224.0.0.0 15.255.255.255 any log
access-list 105 permit tcp any host 192.168.1.11 eq smtp log
access-list 105 permit tcp any host 192.168.1.12 eq http log
access-list 105 permit tcp any host 192.168.1.12 eq https log
access-list 105 permit udp any host 192.168.1.10 eq domain log
access-list 105 permit tcp host 1.2.3.4 host 192.168.1.10 eq domain log
access-list 101 permit icmp any 192.168.1.0 0.0.0.255 3 4 log
access-list 105 deny ip any any log

Cisco PIX 515

First let's set our passwords:

passwd ******
enable password ********

Set the hostname

hostname Cisco515

The primary internal router supports 3 Ethernet interfaces:

E0 to the border router
E1 to the trusted network
E2 to the web server

After entering config mode, we must name the interfaces:

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50

Explicitly define the interface type and speed

Interface ethernet0 10baset

Interface ethernet1 10baset
Interface ethernet2 10baset

Set the ip addresses

ip address outside 209.198.201.3 255.255.255.0
ip address inside 192.168.3.100 255.255.255.0
ip address dmz 192.168.1.7 255.255.255.0

Enable nat on the named interface to allow trusted users to start connections on to the outside. Assign a pool of routable addresses given us by the ISP.

nat (inside) 1 192.168.1.0 255.255.255.0
global (outside) 1 209.198.201.20-209.198.201.50

These entries allow any host to access our web servers:

access-list inet_acl permit tcp any host 192.168.1.6 eq 80
access-list inet_acl permit tcp any host 192.168.1.6 eq 443
access-list inet_acl deny icmp any any
access-group inet_acl in interface outside

We can, at least, hide the real ip address of our web server. Let's create a static mapping for our web server, the first line for http; the second for ssl:

static(www,outside) 209.198.201.100 192.168.1.6 netmask 255.255.255.255

Set the default route

Route outside 0.0.0.0 0.0.0.0 209.198.201.1 1

For interface e2
To allow access from the web server (192.168.1.6) to the SQL Server database: then deny the rest.

Access-list dmz_acl permit tcp host 192.168.3.100 host 192.168.1.6 eq 1433

To allow return trips back from our web server:

access-list dmz_acl permit tcp host 192.168.1.6 eq 80 any
access-list dmz_acl permit tcp host 192.168.1.6 eq 443 any

Let's allow our trusted hosts access:

access-list dmz_acl permit ip 192.168.1.0 255.255.255.0 192.168.0.0 255.255.0.0
access-group dmz_acl in interface dmz

Set up routes on the firewall among our networks:

Route outside 0 0 209.198.201.3
Route inside 192.168.0.0 192.168.3.100

Configuring the PIX VPN Firewall

Follow these steps to configure the PIX Firewall to interoperate with the Cisco Secure VPN Client:[2]

Configure the interfaces:

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security10

Identify the protocol, the server to provide authentication:

aaa-server TACACS+ protocol tacacs+
aaa-server partnerauth protocol tacacs+
aaa-server partnerauth (dmz) host 192.168.4.2 keyname timeout 5

Enable isakmp for the outside interface

isakmp enable outside

Identify the policy number and set the encryption schema. We must use des (56 bit) to encrypt the data since some of our partners are in restricted countries. The hashing algorithm for ensuring data is md5. We are using a pre-shared key for authentication as our client base is small.

isakmp policy 8 encr des
isakmp policy 8 hash md5
isakmp policy 8 authentication pre-share

Configure the key that is pre-shared between our PIX and its clients. Set the wildcard to restrict to the network we will permit shortly

[2] Command structure adapted from example found at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/basclnt.htm

isakmp key cisco1234 address 192.168.4.0 netmask 255.255.255.0

Create access lists that define the virtual IP addresses for VPN clients:

access-list 80 permit ip host 192.168.2.14 host 192.168.15.10
access-list 80 permit ip host 192.168.2.14 host 192.168.15.11
access-list 80 permit ip host 192.168.2.14 host 192.168.15.12
access-list 80 permit ip host 192.168.2.14 host 192.168.15.13
access-list 80 permit ip host 192.168.2.14 host 192.168.15.14

Configure NAT

nat 0 access-list 80

Configure a transform set that defines how the traffic will be protected: A transform set specifies one or two IPSec security protocols (either ESP or AH or both) and specifies which algorithms to use with the selected security protocol. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

crypto ipsec transform-set standard esp-des esp-sha-hmac

Create a dynamic crypto map. Specify which transform sets are allowed for this dynamic crypto map entry:

crypto dynamic-map cisco 4 set transform-set standard

Add the dynamic crypto map set into a static crypto map set:

crypto map partner-map 20 ipsec-isakmp dynamic cisco

Apply the crypto map to the outside interface:

crypto map partner-map interface outside

Enable extended authorization which lets you prompt for a user name.

crypto map partner-map client authentication partnerauth

Configure IKE Mode Config related parameters:

ip local pool dealer 192.168.15.10-192.168.15.14
isakmp client configuration address-pool local dealer outside
crypto map partner-map client configuration address initiate

Tell PIX Firewall to implicitly permit IPSec traffic:

sysopt connection permit-ipsec

Client Side configuration

The cisco secure client was chosen for use with the 506 Firewall. After installing

the software (MS Windows-based clients only) and avoiding a handful of incompatibilities, the client is ready to be configured.

Step 1 Click **Start**>**Programs**>**Cisco Secure VPN Client**>**Security Policy Editor**.

Step 2 Click **Options**>**Secure**>**Specified Connections**.

Step 3 In the Network Security Policy window, click **Other Connection** and click **Non-Secure** in the panel on the right.

Step 4 Click **File**>**New Connection**. Rename New Connection. For example, **ToGE**

Step 5 Under **Connection Security**, click **Secure**.

Step 6 Under **Remote Party Identity and Addressing,** set the following preferences in the panel on the right:

a. ID Type—Click **IP address**.

b. Enter the IP address of the internal host within the PIX Firewall unit's internal network to which the VPN client will have access. Enter **192.168.2.14**.

c. Click **Connect using Secure Gateway Tunnel**.

d. ID Type—Click **IP address**.

e. Enter the IP address of the outside interface of the PIX Firewall. Enter **209.198.201.2**

Step 7 In the Network Security Policy window, click the plus sign beside the ToGE entry to expand the selection, and click **My Identity**. Set the following preferences in the panel on the right:

a. Select Certificate—Click **None**.

b. ID Type—Click **IP address**.

c. Port—Click **All**.

d. Local Network Interface—Click **Any**.

e. Click **Pre-Shared Key**. When the Pre-Shared Key dialog box appears, click **Enter Key** to make the key field editable. Enter **cisco1234** and click **OK**.

Step 8 In the Network Security Policy window, expand Security Policy and set the following preferences in the panel on the right:

a. Under **Select Phase 1 Negotiation Mode, c**lick **Main Mode**.

b. Select the **Enable Replay Detection** check box.

Leave any other values as they were in the panel.

Step 9 Click **Security Policy**>**Authentication (Phase 1)**>**Proposal 1** and set the following preferences in the panel on the right:

a. Authentication Method—Click **Pre-shared Key**.

b. Encrypt Alg—Click **DES**.

c. Hash Alg—Click **MD5**.

d. SA Life—Click **Unspecified** to accept the default values.

e. Key Group—Click **Diffie-Hellman Group 1**.

Step 10 Click **Security Policy**>**Key Exchange (Phase 2)**>**Proposal 1** and select the following values in the panel on the right:

a. Select the **Encapsulation Protocol (ESP)** check box.

b. Encryption Alg—Click 3**DES**.

c. Hash Alg—Click **SHA-1**.

d. Encapsulation—Click **Tunnel**.

Step 11 Click **File**>**Save Changes**.

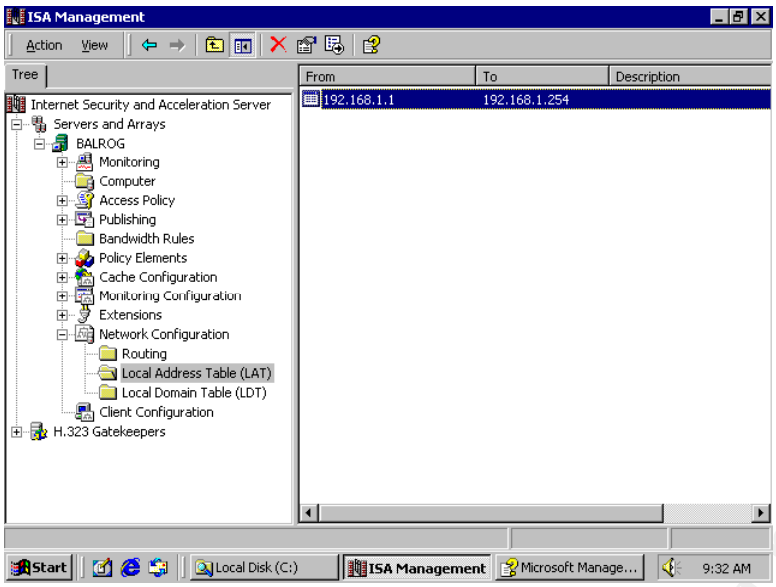
Research and Development Firewall

The Microsoft Internet Security and Accelerator server was chosen for protecting the R& D database.

We will set the following requirements for this firewall:

- Allow all traffic within the R & D network
- Allow http traffic from each of our Suppliers/Partners only
- Allow SMTP out to the trusted network
- Allow POP3 traffic into the R & D network

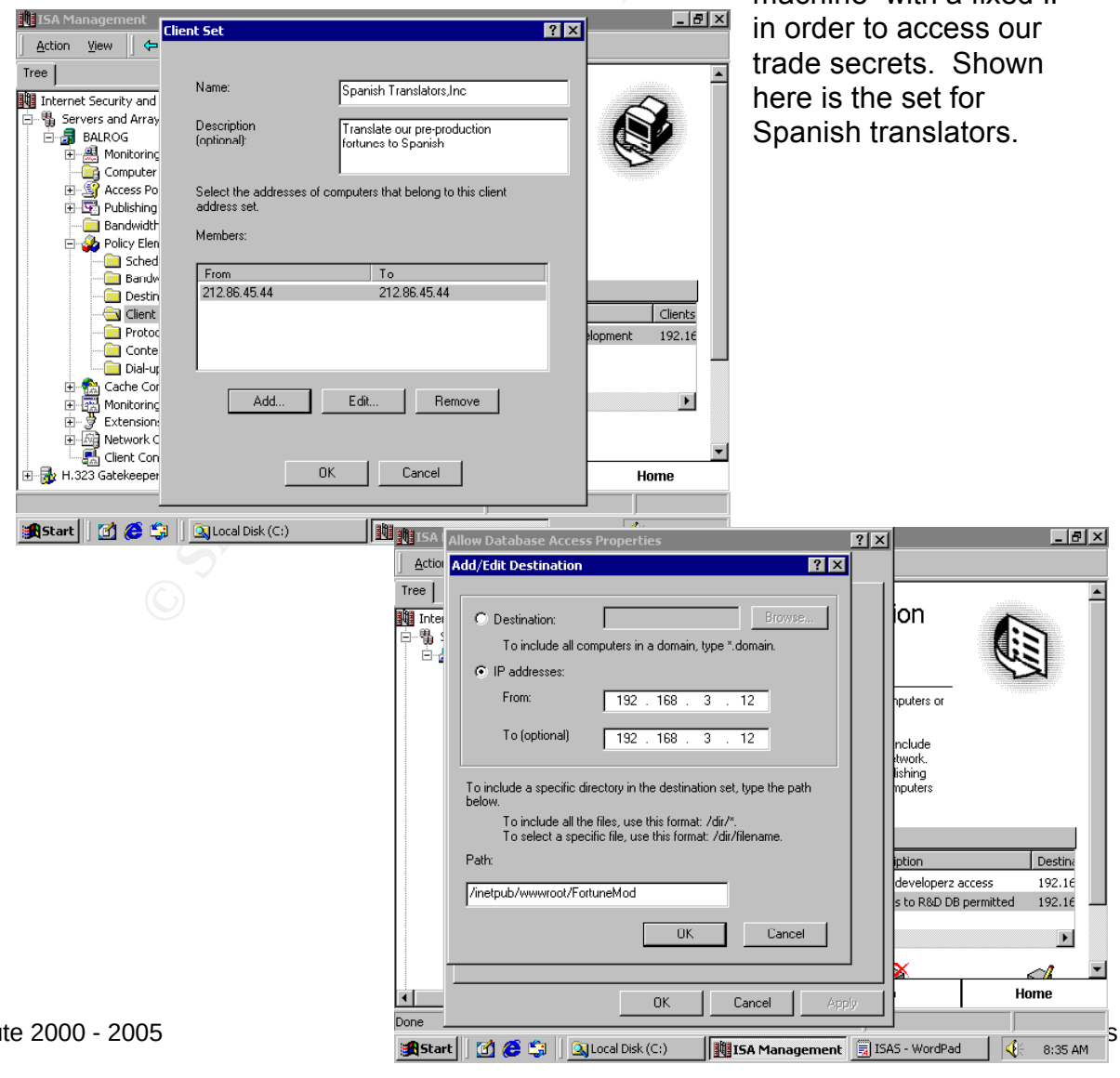
Allow all traffic within the R & D network



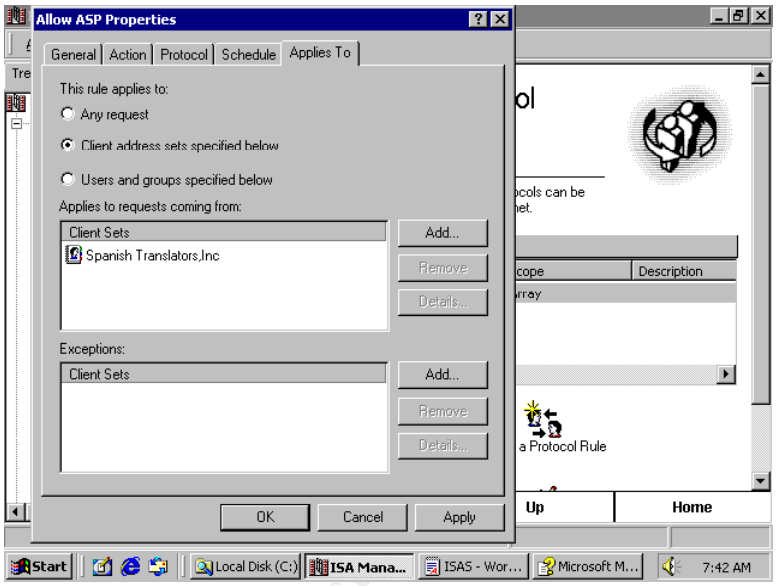
By declaring the R&D network as the local address table, the 192.168.1.0 network is excluded from any external rule that we may apply.

To allow http traffic from each of our Suppliers/Partners

Define *client sets* one for each Supplier/Partner. Each partner must designate a machine with a fixed IP in order to access our trade secrets. Shown here is the set for Spanish translators.



Next we define a destination. The destination reflects not only a single machine but a directory into which the approved requestor may go.



Finally we must create and apply a protocol rule (policy) allowing the Spanish translator through the wall. The general tab allows you to enable the rule. The action tab has an approve/deny choice box. The protocol tab is where the administrator selects from among all defined protocol types. In this case we've chosen HTTP. HTTPS seems unnecessary since we are encrypting upstream with the VPN server.

The last two requirements, providing SMTP and POP3 access from/to the email server on the trusted network (192.168.1.9) are performed with the same procedures as described above.

Assignment 2 – Security Policy (35 points)

Part 1 – Define Your Security Policy (25 points)

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific Access Control List (ACL), firewall rule set, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

You **must** include the complete policy (ACL's, ruleset, IPSec policy) in your paper. It is not enough to simply state "I would include ingress and egress filtering…" etc. The policies may be included in an Appendix if doing so will help the "flow" of the paper.

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

Tutorial

Cisco syntax for a standard access-list is:

access-list <list number 1-99> <permit | deny> <source address> <mask> <log>

Cisco syntax for an extended access-list is:

access-list <list number> <permit | deny> <protocol> <optional keyword host> <to ip address> <to inverse mask> <optional eq port #>

The syntax must be entered while in global configuration mode. The access list must be applied to the interface using interface configuration mode:

ip access-group < list number> <in | out>

Example: **ip access-group 101 in**

Testing the Access List:

To test the above access list we will use a program called Nmap. Nmap is a very powerful network-mapping tool. One of the features of Nmap is that you can spoof the source address when scanning.

To test that we are blocking the private addresses in access-list 105 we will use the Nmap "decoy" command.

nmapnt –sS –D 192.168.1.1 ***Destination IP***

nmapnt – name of scanning program
-sS – scan TCP ports
-D – use decoy address (in this case 192.168.1.1)
192.168.1.1 – private IP we want to spoof

Running this command while monitoring the 3640's log will show attempts made from 192.168.1.1 that were blocked by the access-list.

Output from the 3640's Log:

Oct10 12:04:54 EST: %SEC-6-IPACCESSLOGP: list 105 denied tcp 192.168.1.1(3553) -> a.b.c.d(80), 2 packets

OCT10 12:05:11 EST: %SEC-6-IPACCESSLOGP: list 105 denied tcp 192.168.100.72(4653) -> a.b.c.d(21), 4 packets

Oct10 12:05:16 EST: %SEC-6-IPACCESSLOGP: list 105 denied tcp 192.168.1.10(2513) -> a.b.c.d(25), 2 packets

You may also want to run the command:

3640 # sh access-list 105

The command above will show the hit count or how many access attempts the access list blocked. This command can help you troubleshoot access-list

problems.

deny ip 10.0.0.0 0.255.255.255 any log (50 matches)
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any log (178 matches)
deny ip 127.0.0.0 0.255.255.255 any log
deny ip 0.0.0.0 0.255.255.255 any log
deny ip 224.0.0.0 15.255.255.255 any log
deny ip 192.168.1.0 255.255.255.0 any log

Tips, Tricks and Gotcha's

- The router will do what you tell it to do. If you apply a netmask of 255.255.255.255 on an IP deny statement, it is the same as deny any. Your router is secure but useless.
- A packet being evaluated is processed in sequential order
- The packet is compared with each access item until the first one matches, then it is disposed of accordingly.
- There is an implicit deny at the end of each access-list. One must remember to put in permits, too!
- Each new entry is added to the bottom if the list. Remember that order is important. You can always use a clipboard type application to copy out the lists, edit them, then paste them back in.
- Cisco has a really cool configurator. It is GUI based and will greatly assist you in scripting. It's called *Configmaker* and is available for the downloading.

Assignment 3 – Audit Your Security Architecture (25 points)

You have been asked to conduct a technical audit of the **primary firewall** (described in Assignments 1 and 2) for GIAC Enterprises. In order to conduct the audit, you will need to:

1. Plan the audit. Describe the technical approach you recommend to assess the firewall. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.

2. Conduct the audit. Using the approach you described, validate that the primary firewall is actually implementing GIAC Enterprises' security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

3. Evaluate the audit. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but you must annotate/explain the output.

Audit

Given that GE is a smaller business auditing will be conducted internally. While this is the initial implementation of an audit, further checks will be conducted at least twice monthly and will be expanded to include:

- password checks
- anti-virus readiness
- netbios share ACL's
- scanning of secondary firewalls
- education and subsequent testing of helpdesk staff regarding social engineering hacks

The audit plan will include both external and internal checks on the firewall.

- External audit procedures
  - Network scanning using nmapnt
  - Web Services vulnerability/stress testing
- Internal audit procedures
  - Network scanning using nmapnt
  - Modem auditing – bypassing the firewall THC-scan
  - Firewall updates – IOS current?

The following table outlines the tasks, schedule and expected results.

Task	Schedule	Expected results

Network scanning	Weekend (any time) 1 hours	Ports 25,80 and 443 are open. All else closed.
Network scanning internal	Weekend (any time) 1 hours	Ports 25,80 and 443 are open. All else closed.
Modem auditing	Weekend (after typical working hours 7am-7pm) 1 hours	No modems set to auto answer.
Firewall updates	Sunday 4:00 AM 2 hours. Do not announce.	Audit firewall software releases, check Cisco for patches, and etc.

Permission

It is necessary to obtain written permission before running the audit. An audit can have unintended and terrible consequences. The granting authority may vary, but at the least it should be the CIO or some equivalent.

Method

Network scanning will be conducted using NMAPNT for both external and internal tests. Weekend times were chosen in the case that critical machines were rendered inoperative or vulnerable.

Web services evaluated using the IIS resource kit utilities WCAT.

Modem auditing will be conducted using a war dialer. THS-scan will systematically dial through the companies DID lines to ensure that no employee is bypassing the firewall. This test is conducted during the hours when an employee might be likely to dial in from home.

Firewall updates occur at irregular intervals. It is important to keep current on security patches. Once patches are made available, fixes often require reboots. Hence, these painful hours

Results

Running nmapnt against the firewall, we find that our router is likely doing its just in dropping echo requests on Serial0.

D:\NMAPNT>nmapnt -sT 192.168.3.3

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security (http://www.eEye.com)
based on nmap by fyodor@insecure.org (www.insecure.org/nmap/)

Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds

D:\NMAPNT>nmapnt -sT 192.168.3.3 -P0

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security (http://www.eEye.com)
based on nmap by fyodor@insecure.org (www.insecure.org/nmap/)

Interesting ports on (192.168.3.3):
(The 1522 ports scanned but not shown below are in state: closed)

Port	State	Service
25/tcp	open	smtp
80/tcp	open	http
143/tcp	open	imap2
389/tcp	open	ldap
443/tcp	open	https

An analysis of the firewall logs shows its activity. A sample only is shown:

Date	Type/action	Source	Destination	Protocol	Rule
10/07/2001 20:15:05.880	TCP connection dropped	207.198.111.200, 2771, WAN	192.168.3.3, 773, LAN		20
10/07/2001 20:15:05.880	TCP connection dropped	207.198.111.200, 2776, WAN	192.168.3.3, 113, LAN	'Authentication'	20
10/07/2001 20:15:05.880	TCP connection dropped	207.198.111.200, 2777, WAN	192.168.3.3, 433, LAN		20
10/07/2001 20:15:05.896	TCP connection dropped	207.198.111.200, 2775, WAN	192.168.3.3, 756, LAN		20
10/07/2001 20:15:05.896	TCP connection dropped	207.198.111.200, 2774, WAN	192.168.3.3, 200, LAN		20
10/07/2001 20:15:05.912	TCP connection dropped	207.198.111.200, 2767, WAN	192.168.3.3, 304, LAN		20
10/07/2001 20:15:05.912	TCP connection dropped	207.198.111.200, 2772, WAN	192.168.3.3, 508, LAN		20
10/07/2001 20:15:05.928	TCP connection dropped	207.198.111.200, 2819, WAN	192.168.3.3, 1080, LAN	'Socks'	20

As can be seen the connections from the attacker are being dropped. When the firewall knows the common port usage, it identifies it.

Internal Scan

Running an internal scan revealed the following results.

D:\NMAPNT>nmapnt -sT 192.168.3.3 -P0

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security (http://www.eEye.com)

based on nmap by fyodor@insecure.org (www.insecure.org/nmap/)

Interesting ports on (192.168.3.3):
(The 1520 ports scanned but not shown below are in state: closed)

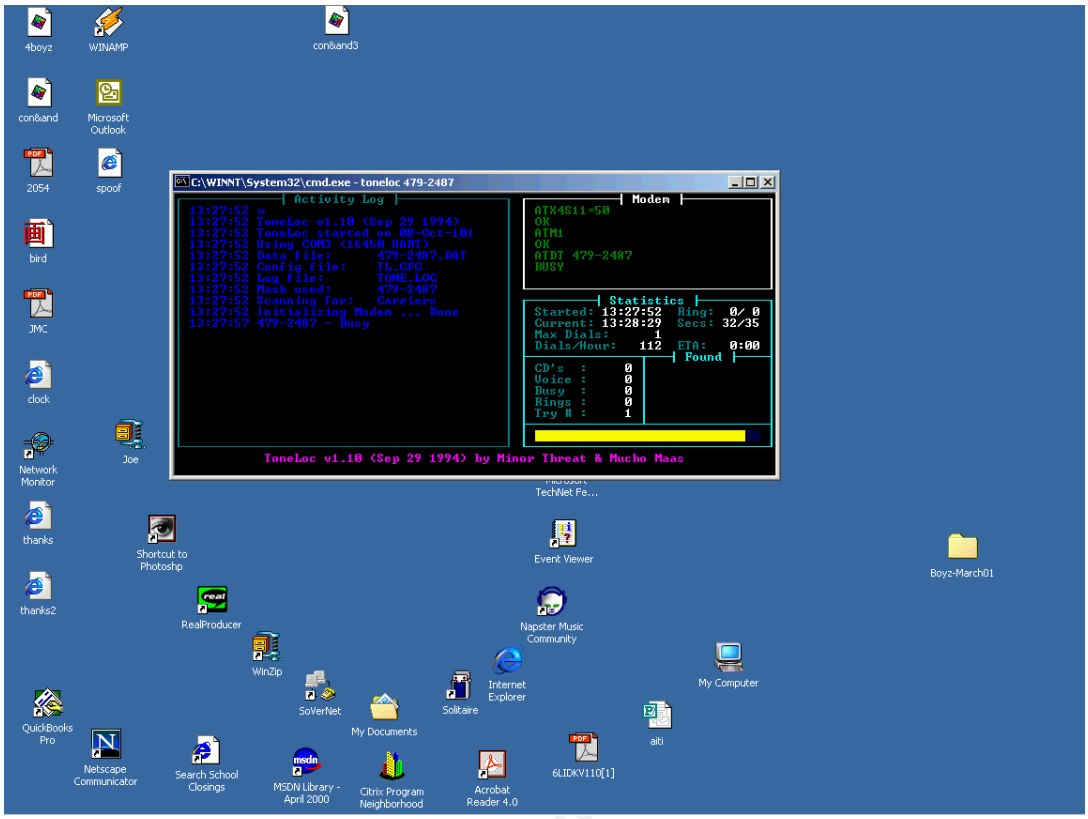
Port	State	Service
23/tcp	filtered	telnet
25/tcp	open	smtp
69/tcp	filtered	tftp
80/tcp	open	http
443/tcp	open	https

Nmap run completed -- 1 IP address (1 host up) scanned in 105 seconds

While ports 23 and 69 appear to be filtered, an analysis of the log shows that sample packets were dropped.

Date	Type/action	Source	Destination	Protocol	Rule
10/08/2001 07:38:05.944	TCP connection dropped	192.168.3.200, 2762, LAN	192.168.3.3, 69, LAN		6
10/08/2001 07:38:06.720	TCP connection dropped	192.168.3.200, 2757, LAN	192.168.3.3, 23, LAN	'Telnet'	6

Dialer Check



Above is a print screen from the DOS-based war dialer *ToneLoc*. Yes, ToneLoc runs from a windows 2000 cmd prompt. We might've scanned against GE's company numbers using the call:

D:\builds> ToneLoc 555-1XXX

This command dials all (100) phone numbers beginning with 555-1000. It should be noted that each modem one uses may get 100 scans completed in one hour. There are commercial war-dialers available that support multiple modems.

A reasonably good manual is located at http://www.textfiles/hacking/tl-user.txt . The software itself is available via a web search. Credit goes out to *Minor Threat* and *Mucho Maas* for their work.

Firewall Updates

To view the version of IOS being run, enter enable mode and type *show version.*

One can review bulletins and download updates from Cisco:
http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml

Other sites that provides useful bulletins:

http://www.sans.org
http://www.cert.org
http://www.inside-security.de/

Conclusions

The external audit showed that GE's primary firewall is behaving as it should behave. Ports 143 (IMAP) and 389 (LDAP) were open. These common ports may have been opened for a reason. They are associated with Microsoft outlook, among others. It's a judgment call, but other administrators should be questioned before closing these ports.

The internal audit revealed two surprises that should be investigated. The open but filtered state of tftp and telnet reveals that the firewall is blocking the ports. This tells a malicious internal scanner that the scanned ip is a firewall. It doesn't show externally because the router has been told "no ip unreachables". It should be fixed internally.

A screening of the company's phone numbers revealed no auto-answer modems. Should we have found auto-answers the matter would've been referred to the IT director for action (such as pulling the modem)

As discussed above additional perimeter audits must be conducted and regular audit routines should be implemented.

Assignment 4 – Design Under Fire (25 points)

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research and describe at least **three** vulnerabilities that have been found for the type of firewall chosen for the design. Choose **one** of the vulnerabilities, design an attack based on the vulnerability, and explain the results of running that attack against the firewall.

2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.

3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

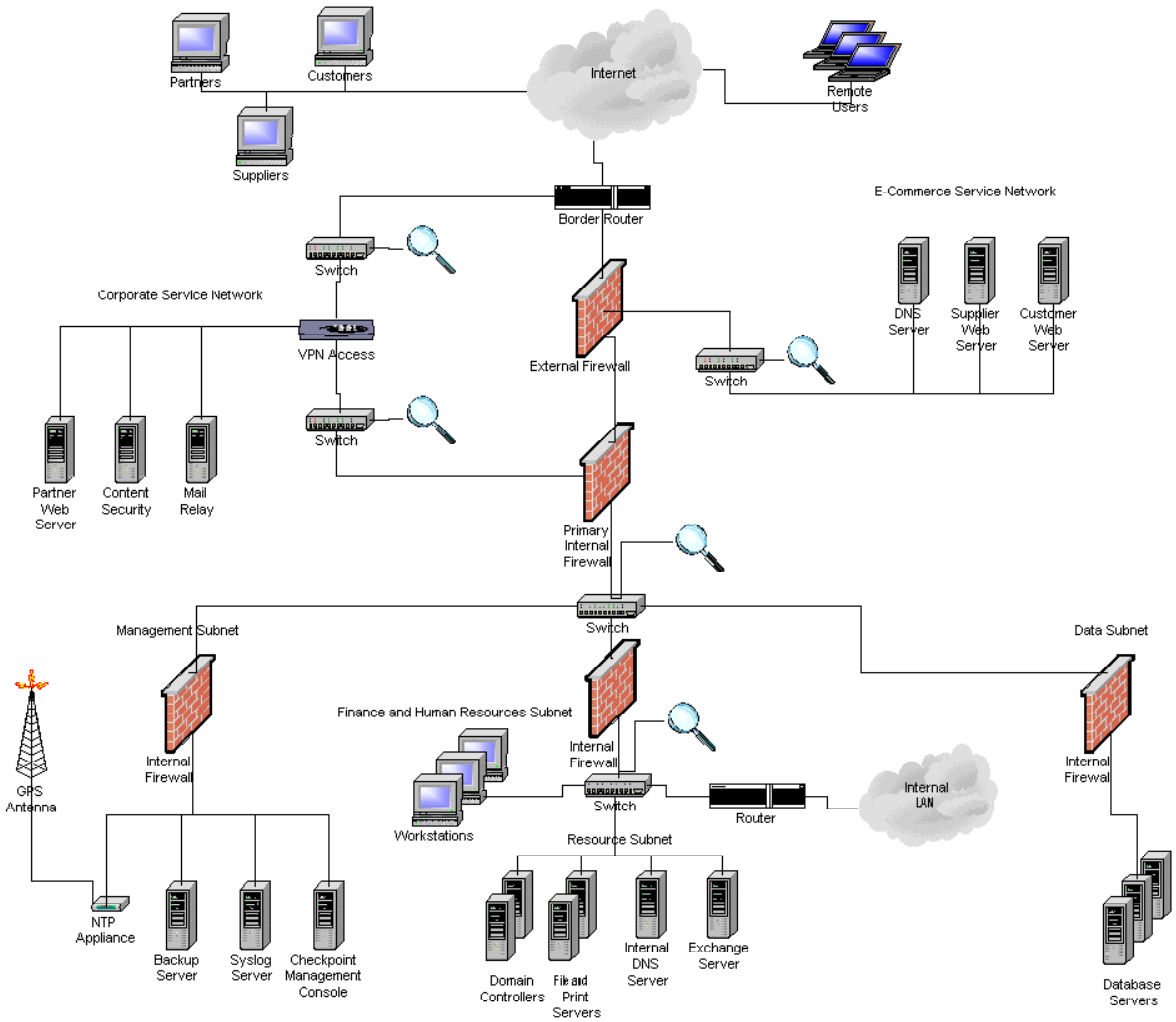
In designing your attacks, keep the following in mind:

- The attack should be **realistic.** The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

- The attack should be **reasonable.** The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should not assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)

- You **must** supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.

- The attack does not necessarily have to succeed (though a successful attack is often the more interesting approach). If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.



Tanya Baccam, http://www.sans.org//y2k/practical/Tanya_Baccam_GCFW.zip , designed the network shown above. She chose the CheckPoint firewall-1.

When service packs are not current, Checkpoint's products are vulnerable to these attacks

- Ip Fragmentation Denial-of-Service Vulnerability
  - Documented by Lance Spitzer, this DOS attack manifests itself *by sending a stream of large IP fragments to the firewall. As the fragments arrive, the mechanism used to log IP fragmentation anomalies can monopolize the CPU on the host machine and prevent further traffic from passing through the firewall*
- Check Point FireWall-1 RDP Bypass Vulnerability
  - *Found* and documented by Jochen Thomas Bauer <jtb@inside-security.de> and Boris Wesslowski bw@inside-security.de, this

`exploit attacks` *FireWall-1 management rules allow arbitrary eitherbound RDP connections to traverse the firewall. Only the destination port (259) and the RDP command are verified by FireWall-1. By adding a faked RDP header to normal UDP traffic any content can be passed to port 259 on any remote host on either side of the firewall*.

- Open ports by default
    - Firewall-1 leaves several ports open by default. These include TCP53, UDP53 (DNS) and UDP 520 (RIP). Additionally for firewall management, it will listen on TCP256, TCP257 and TCP258.

Attacking the Checkpoint FireWall-1

The attack plan for compromising the configuration in question will revolve around the default open ports option. We will attempt to bypass the firewall by:

1. Detect the firewall
2. Scan the firewall for ports in question
3. Attack the web server in the DMZ (attacking an internal system)
4. Install a backdoor listener configured for one of the open ports

Along the way we'll see that defense in depth can thwart this process at many levels, however, we'll be pessimistic and see if everything works. By the way, the names have been changed to protect the innocent.

Given that the firewall is likely to be protecting web server in a DMZ arrangement, let's do a tracert to see what lies in the web server's path.

Let's find the IP of the server with nslookup.

C:\Narya>nslookup www.ge.com
Server: nameserver.somewhere.com
Address: XXX.YYY.ZZZ.???

Name: www.ge.com
Address: AAA.BBB.CCC.DDD

The IP for the server is AAA.BBB.CCC.DDD. now let's find the route to it.

C:\Narya >tracert AAA.BBB.CCC.DDD

Tracing route to www.ge.com [AAA.BBB.CCC.DDD]
over a maximum of 30 hops:

```
  1   <10 ms   <10 ms   <10 ms  AAA.BBB.165.5
  2   <10 ms   <10 ms   <10 ms  AAA.BBB.161.1
  3   <10 ms   <10 ms   <10 ms  AAA.BBB.180.1
  4   <10 ms   <10 ms    16 ms  AAA.BBB.213.128
  5   <10 ms   <10 ms   <10 ms  fa4-0.some-thing.maybe.firewall.us
[FFF.WWW.100.209]
  6   <10 ms   <10 ms   <10 ms  www.ge.com [AAA.BBB.CCC.DDD]

Trace complete.
```

It's likely that the firewall is the next to last route. If the firewall is blocking the return of TTL expired packets then perhaps it will be the last one to return a next hop.

Now let's test to see if it is our Firewall-1. We'll check by hoping that our desired port(s) is open. We'll use NMPANT to find out if our port (TCP256) is open. I'm going to use decoy just to help conceal my identity. I should probably use more spoofed IP's if I were truly doing this.

C:\Narya >nmapnt -sS -D 209.198.222.5 AAA.BBB.CCC.DDD

```
Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Interesting ports on  (192.168.3.1):
(The 1493 ports scanned but not shown below are in state: closed)
Port       State      Service
1/tcp      filtered   tcpmux
23/tcp     open       telnet
55/tcp     filtered   isi-gl
57/tcp     filtered   priv-term
79/tcp     open       finger
256/tcp    open       unknown
257/tcp    open       unknown
258/tcp    open       unknown
```

As we can see port 256 is open and waiting. Its time to launch our attack against www.ge.com. We'll use netcat to ensure we've got an HTTP server available. We enter these commands:

C:\Narya >nc -v www.ge.com 80
www.ge.com [AAA.BBB.CCC.DDD] 80 (http) open

Having identified our IIS server, it is time to try a few things. Likely Ms. Baccam has all Service Packs and hot fixes up to date, but you never know unless you try. I'd try a few things including:

- IISHack
- A few buffer overflows
- Perhaps there is an errant .HTA lying around
- Use netcat to dump the global.asa
- Look for already installed trojans

The point is to be persistent. Given some miracle (She is a GCFW after all) that I get a root login. I would install a netcat listener and configure it to listen on port 256. We patch whatever weakness we found and at that juncture, our mission is accomplished. Lastly, we drop an anonymous note to the administrator and let them know how to clean our compromise!

Countermeasures to this attack

This attack can be thwarted at any step.

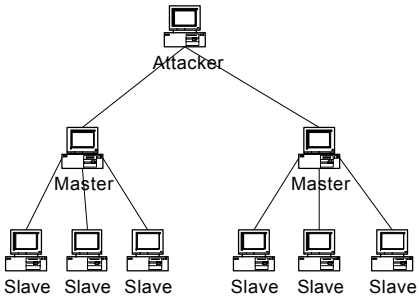
1. Detect the firewall – Deny ICMP traffic at the border router interface. Ms. Baccam did this:

```
!       Log everything else (inbound):
!
access-list 101 deny ip any log
```

2. Scan the firewall for ports in question –
   Close the default ports, log those that are unlogged.
3 Attack the web server in the DMZ –
   The only safe IIS is on a machine that is unplugged from the 100v outlet. That being said, Microsoft readily puts out patches *after* an attack has been discovered.
5. Install a backdoor listener configured for one of the open ports
   Keep patches up to date, keep clean install tapes handy for rebuilds and keep anti-virus scanner DAT files current.

Denial of service attack

There are a number of DDOS attack agents available including Trinoo, TFN2K, and Tribal Flood network. We'll choose Trinoo for this attack. Trinoo is designed as a hierarchy We have our 50 compromised agents. Arrayed like this:



The attacker controls the masters who, in turn, control the slaves. To launch an attack on www.ge.com, the attacker issues a command to the masters like **dos AAA.BBB.CCC.DDD.** The masters may then launch an attack by issuing a command to the slaves like **aaa password AAA.BBB.CCC.DDD.**

The engines will begin flooding our victim with any number of different attacks including land attack , teardrop, or whatever scripts are selected and available on the slave.

Countermeasures

Trinoo is available in *NIX and windows versions. The best countermeasure involves keeping current on patches, anti-virus dat files, and blocking ephemeral ports susceptible to Trinoo.

There are tools and techniques available for detecting the presence of Trinoo. For the Wintrinoo (Windows-based Trinoo) check for service.exe (not service**s**.exe) in the registry under:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run

- For Windows one may download and run
  - http://www.jmu.edu/info-security/engineering/tools/wtrinscan.exe
- For *NIX one may download RID 1.1 from
  - http://www.theorygroup.com/Software/RID/

References:

"Basic VPN Configuration" 26 September 2001
URL:http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/ipsecint.htm#xtocid2614916

"Check Point FireWall-1 RDP Bypass Vulnerability," 14 July 2001
URL: http://www.inside-security.de/advisories/fw1_rdp.html

"Passive FTP Vulnerability," 11 February 2000.
URL: http://www.checkpoint.com/techsupport/alerts/pasvftp.html

Augusti, L. "Setting Up PIX syslog." 12 July 2002 (sic).
URL: http://www.cisco.com/warp/public/110/pixsyslog.html

.Bash, J. "Cisco - Improving Security on Cisco Router." 26 July 1999. URL:
http://www.cisco.com/warp/public/707/21.html

Bernstein, D. J. "Guarantee.html" Publish date unspecified
http://cr.yp.to/qmail/guarantee.html

Boyle, Philip. "Distributed Denial of Service Attack Tools: Trinoo and Wintrinoo A Research Report Submitted in Partial Fulfillment of the SANS GIAC Program"
URL: http://www.sans.org/newlook/resources/IDFAQ/trinoo.htm

Dittrich, David . The DoS Project's "Trinoo" Distributed Denial of Service Attack Tool. 18 April 2000.
URL: http://www.staff.washington.edu/dittrich/misc/trinoo.analysis

Dunlap D. "Configuring Cisco PIX-to-VPN Client Wild-card, Pre-shared, Mode Configuration." 3 April 2001.
URL: http://www.cisco.com/warp/public/110/A.html

Lammle, Todd. CCNA Cisco Certified Network Associate Study Guide Alameda, CA: Sybex, Inc. 1999

Lanza, Jeffrey P. "IP Fragmentation Denial-of-Service Vulnerability in FireWall-1,"
5 April 2001. URL: http://www.kb.cert.org/vuls/id/35958

Pacquet, Catherine and Teare, Diane. Building Scalable Cisco Networks. Indianapolis: Cisco Press. 2001

Scambray, Joel, McClure, Stuart and Kurtz, George. Hacking Exposed, Network Security Secrets and Solutions Second Edition. Berkeley: Osborne/McGraw-Hill, 2001

Simmons, Curt. ISA Configuration and Administration. New York: M & T

Books.2001.

Sonafilippo, Salvatore. “HPING.”
URL: http://www.hping.org

Stevens, W. Richard. TCP/IP Illustrated, Volume 1. Reading: Addison Wesley Longman, Inc, 1994.

Winters, Scott. “Top Ten Blocking Recommendations Using Cisco ACLs Securing the Perimeter with Cisco IOS 12 Routers.” 15 August, 2000.
URL: http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm