GIAC Level Two Firewalls, Perimeter Protection, and VPNs

Practical Assignment for SANS New Orleans

Current as of January 28, 2001

Version 1.5

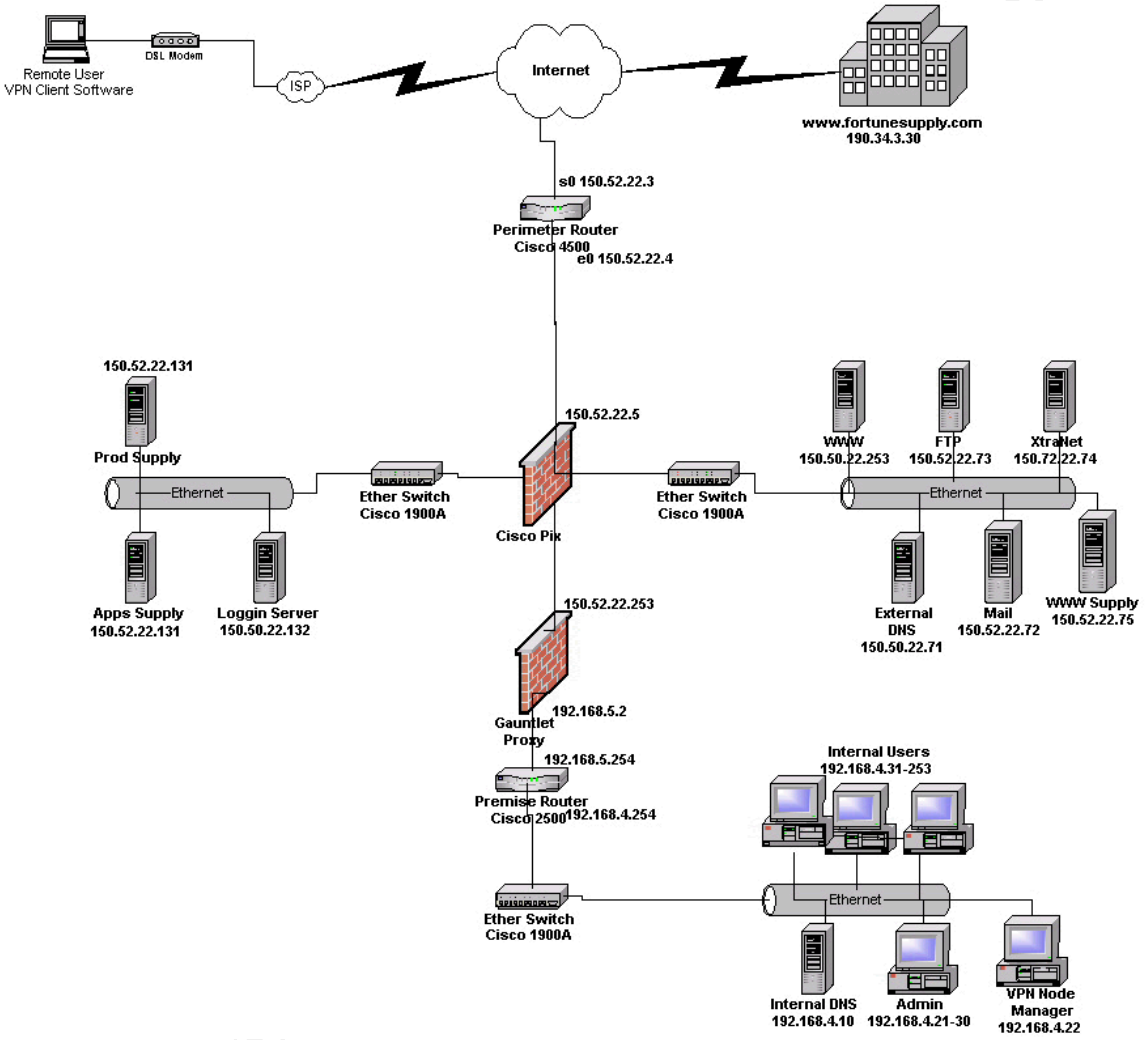
Submitted by:

Joe Livingston

February 19, 2001

Table of Contents

Assignment 1 – Security Architecture – www.fortunecookies.com



Internet traffic will pass through routers and two physical firewalls: A Cisco Pix and a Gauntlet proxy firewall.
The Cisco Pix will provide protection for the Service network and the Production network. The Service network houses all hosts reachable from the Internet. The Production Network houses hosts that are not reachable from the Internet, but provide support for our E-commerce customers. We will accomplish internal network routing with static routes configured on the Cisco Pix.
The Gauntlet firewall will provide application filtering and proxy services.
All inbound traffic from the Internet will be allowed to the Service network only.

All inbound traffic sent directly to the Production network or internal hosts will be blocked by the Cisco pix.
Internet accessible devices will be located on the Service network. These devices will then process requests to an application on the Production network using predefined ports. The Production network systems will call the needed internal systems using static ports and protocols.
Outbound Internet activity from GIAC Enterprises internal systems will be subject to rules sets in both the Gauntlet proxy and the Cisco Pix.
Firewall rules will control access on these paths:

The Cisco Pix will control access as follows:

Internet to Service network
Service network to Production network
Production network to Service network
Production network to Internet
VPN Interface Gateway

The Cisco Pix and Gauntlet proxy will provide redundant screening for the following:

Production network to the Internal network.
Internal network to Production network.
Internal network to Service network.
Internal network to the Internet.

Services provided by the Service network will include:

A corporate World Wide Web server. (WWW.fortunecookies.com)

The external DNS server to resolve external DNS for Internet addressable addresses.

The corporate mail server. This server will host all external Internet mail to and from GIAC Enterprises. Internal network hosts will receive mail from this server using POP.

A FTP server. This will be used to provide non-anonymous FTP services for GIAC's business partners and customers. Access to this system will be by named account only using strong authentication.

An Xtranet server. This server will be used to allow business partners to exchange purchase orders and related documents. Access to this server will require HTTPS.

A logging server. This server will provide centralized logging for all Production network and Service network activities.

Elements on the internal network related to the security environment include:

An Internal DNS server. This will provide all necessary Internal DNS services. This server will forward external DNS requests to the external DNS server in the Service network.

Administrative user systems. These users include system administrators, application administrators, and web content management. All access and restrictions will be illustrated in this document.

Internal network system users. GIAC Enterprises employees that require Internet access to retrieve mail and accomplish other required functions.

Assignment 2: Security Policy

The following general policies will be implemented for the architecture defined above.

The border router will be configured with the standard egress and ingress ACL filtering.
A Cisco Pix firewall will provide stateful packet inspection. The Cisco Pix default policy is to "deny everything". Exceptions are then made for specific application requirements.
A Gauntlet firewall appliance will provide proxy services.
The Gauntlet proxy will be configured to only allow HTTP and HTTPS traffic from internal hosts, it will be configured to deny all other inbound and outbound traffic.
All applications requiring access to systems on either the filtered networks (Service network/Production network). This access will be created as exceptions to the default 'deny any any' rule on the Cisco PIX and the Gauntlet proxy. Traffic will not be routable from the Internet to the production network or the internal network.

Specifics for applying the policy are provided in the following three sections:

Policy application for the Cisco Pix
Inbound traffic
Outbound traffic

Policy application for the Gauntlet proxy
Inbound traffic
Outbound traffic

Policy for IPSec VPN services (for the purposes of this practical, VPN is only defined between Fortunesupply.com, remote users and GIAC fortune cookies).
Inbound traffic
Outbound traffic

General methods for testing policies.

Policy application for the Cisco Pix. (Detailed Cisco Pix commands are available for reference at (http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix).

Each interface must be named and an appropriate security level assigned.

1. The external inteface (facing the Internet) will provide the lowest level of security of "0".
2. The Service network interface will be assigned the security level of "5".
3. The Production network interface will be assigned the security level of "20".
4. The Internal network interface will be assigned the security level of "100".

The syntax to complete this configuration is:

```
nameif ethernet0 outside security0
nameif ethernet3 Service network security5
nameif ethernet2 production network security20
nameif ethernet1 inside security100
```

Inbound traffic rules on the Cisco Pix use lower security to higher security. The Cisco Pix uses a combination of two commands to allow traffic to move from lower security to a higher level of security; static and conduit. The static configuration establishes a link between IP addresses on the lower interface to the higher interface. The conduit command is used to attach a static translation – allowing control of ports and protocols through a potential connection. The following rules are listed in the order they should be applied.

The aggregate Cisco Pix ruleset is:

```
static (Service network, outside) 150.52.22.64 155.72.22.64 netmask 255.255.255.192
0 0
static (Production network,Service network) 150.52.22.130 150.52.22.130 netmask
255.255.255.255 0 0
static (Production network,Service network) 150.52.22.131 150.52.22.131 netmask
255.255.255.255 0 0
static (Production network,Service network) 150.52.22.132 150.52.22.132 netmask
255.255.255.255 0 0
static (inside,Production network) 192.168.4.11 192.168.4.11 netmask
255.255.255.255 0 0
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
timeout xlate 3:00:00 conn 1:00:00 half-closed
0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout unauth 0:05:00 absolute
```

```
sysopt connection tcpmss 1380
sysopt connection permit-ipsec
crypto ipsec transform-set myset ah-md5-hmac esp-des
crypto map mymap 10 set transform-set myset
access-list 10 permit ip host 150.52.22.5 host 190.34.3.30
access-list 10 permit ip host 150.52.22.5 host 192.168.15.1
access-list 10 permit ip host 150.52.22.5 host 192.168.15.2
crypto ipsec transform-set strong-des esp-3des esp-sha-hmac
crypto dynamic-map cisco 4 set transform-set strong des
crypto dynamic-map 20 ipsec-siakmp dynamic cisco
crypto map partner-map interface outside
crypto map partner-map client authentication partnerauth
ip local pool dealer 192.168.15.1-192.168.15.2
isakmp client configuration address-pool local dealer outside
crypto map partner-map client configuration address initiate
sysopt connection permit-ipsec
global (outside) 1 150.52.22.6 – 150.52.22.20
netmask 255.255.255.224
route outside 0.0.0.0 0.0.0.0 150.52.22.5 1
crypto map mymap 10 set session-key inbound ah 400
123456789A123456789A12
crypt0 map mymap 10 set session-key outbound ah 300
123456789A123456789A123456789A12
crypto map mymap 10 set session-key inbound esp 400
cipher abcd1234abcd1234
crypto map mymap 10 set session key outbound esp 300
cipher abcd1234abcd1234
crypto map mymap interface outside
isakmp policy 01
isakmp policy 01 encryption des | 3des
isakmp policy 01 hash md5 | sha
isakmp policy 01 authentication rsa-sig
isakmp policy 01 lifetime 5000
conduit permit tcp host 150.52.22.70 eq 80 any
conduit permit icmp host 150.52.22.70 eq 8 any
conduit permit udp host 150.52.22.71 eq 53 any
conduit permit tcp host 150.52.22.72 eq 25 any
conduit permit icmp host 150.52.22.72 eq 8 any
conduit permit tcp host 150.52.22.73 eq 20 any
conduit permit tcp host 150.52.22.73 eq 21 any
conduit permit icmp host 150.52.22.73 eq 8 any
conduit permit tcp host 150.52.22.74 eq 4000 host 190.34.3.30
conduit permit tcp host 150.52.22.74 eq 443 any
conduit permit icmp host 150.52.22.74 eq 8 any
conduit permit tcp host 150.52.22.130 eq 4000 host 150.52.22.74
conduit permit tcp host 150.52.22.131 eq 3200 host 150.52.22.75
conduit permit tcp host 150.52.22.131 eq 3900 host 150.52.22.75
conduit permit udp host 150.52.22.132 eq 514  host 150.52.22.74 255.255.255.192
conduit permit tcp host 192.168.4.11 eq 3900 host 150.52.22.130
conduit permit tcp host 192.168.4.11 eq 3200 host 150.52.22.131
conduit permit tcp host 192.168.4.11 eq 3900 host 150.52.22.131
conduit deny ip any any
outbound  13 deny 0.0.0.0 0.0.0.0 0 0
outbound  13 except 192.168.4.10 0.0.0.0 53 udp
outbound  13 except 192.168.4.11  0.0.0.0 3200 tcp
outbound  13 except 192.168.4.11  0.0.0.0 3900 tcp
outbound  13 except  150.52.22.253 0.0.0.0 0 tcp
outbound  13 except  150.52.22.253 0.0.0.0 0 udp
outbound 23 deny 0.0.0.0 0.0.0.0 0 0
outbound 23 except 150.52.22.130 0.0.0.0 0 tcp
outbound 33 deny 0.0.0.0 0.0.0.0 0 0
outbound 33 except 150.52.22.72 0.0.0.0 25 tcp
outbound 33 except 150.52.22.71 0.0.0.0 53 udp
outbound 33 except 150.52.22.70 0.0.0.0 0 icmp
outbound 33 except 150.52.22.72 0.0.0.0 0 icmp
outbound 33 except 150.52.22.73 0.0.0.0 0 icmp
apply (inside) 13 outgoing_src
apply (Production network) 23 outgoing_src
apply (Service network) 33 outgoing_src
telnet 150.52.22.253 255.255.255.255
```

The purpose of each rule is explained below.

The Service network is designed specifically to accept traffic from the internet. We will first build a static link allowing the Service network to send and receive packets from the Internet.

This syntax for this rule is:

```
static (Service network,outside) 150.52.22.64 150.52.22.64 netmask 255.255.255.192
0 0
```

The use of the network address and the subnet mask will provide a static for any host placed on the Service Network.

Service network hosts

www host at 150.52.22.70. (Access to the www host from the outside will be exclusively on port 80 using tcp.   To allow this server to be pingable from the internet; include icmp port 8).

The syntax is:

```
conduit permit tcp host 150.52.22.70 eq 80 any
conduit permit icmp host 150.52.22.70 eq 8 any
```

External DNS host at 150.52.22.41.

The External DNS host should be accessible from any host on the Internet. Access will use udp port 53.

The syntax for this conduit is:

```
conduit permit udp host 150.52.22.71 eq 53 any
```

mail host at 150.52.22.72.

We will provide access to the mail host from the Internet on port 25 using tcp. We will also make this host pingable from the Internet using icmp port 8.

The syntax for this conduit is:

```
conduit permit tcp host 150.52.22.72 eq 25 any
conduit permit icmp host 150.52.22.72 eq 8 any
```

FTP host at 150.52.22.73.

We will provide access to the ftp host from the Internet on tcp ports 20 and 21. This host will be accessible from any host on the Internet and we will allow ping to this host using icmp port 8.

The syntax for this conduit is:

```
conduit permit tcp host 150.52.22.73 eq 20 any
conduit permit tcp host 150.52.22.73 eq 21 any
conduit permit icmp host 150.52.22.73 eq 8 any
```

Xtranet host at 150.52.22.74.

Access to the Xtranet host has been programmed by the application developers as tcp (https) on port 4000. Access will only be allowed from select business partners as defined by the Xtranet applications team. For each business partner, we will need a separate conduit command.

The syntax for business partner fortunesupply.com is:

```
conduit permit tcp host 150.52.22.74 eq 4000 host 190.34.3.30
```

www supply host at 150.52.22.75.

The www supply host has been programmed by the application developers as tcp (https) on port 443. This host can be accessed from any Internet host and is pingable using icmp port 8.

The syntax for this conduit is:

```
conduit permit tcp host 150.52.22.75 eq 443 any
conduit permit icmp host 150.52.22.75 eq 8 any
```

Production network hosts:

App Supply host at 150.52.22.130.

The App Supply host access has been programmed by the application developers as tcp on port 4000. Inbound access to this host will be allowed only from the Xtranet host on the Service network at 150.52.22.74. This access will require both a static command and a conduit command.

The syntax for this access is:

```
static (Production network,Service network) 150.52.22.130 150.52.22.130 netmask
255.255.255.255 0 0
conduit permit tcp host 150.52.22.130 eq 4000 host 150.52.22.74
```

Prod Supply host at 150.52.22.131.

The Prod host access has been programmed by the application developers as tcp on ports 3200 and 3900. Inbound traffic will only be allowed from the www supply host on the Service network at 153.72.42.75. This requires a static command and two conduit commands:

The syntax for this access is:

```
static (Production network,Service network) 150.52.22.131 150.52.22.131 netmask
255.255.255.255 0 0
conduit permit tcp host 150.52.22.131 eq 3200 host 150.52.22.75
conduit permit tcp host 150.52.22.131 eq 3900 host 150.52.22.75
```

Loggin at host 150.52.22.132.

Access to the loggin host will be allowed via udp port 514. Inbound traffic will be allowed from systems on the Service network. This access will require a static command and a conduit command:

The syntax for this access is:

```
static (Production network,Service network) 150.52.22.132 150.52.22.132 netmask
255.255.255.255 0 0
conduit permit udp host 150.52.22.132 eq 514  host 150.52.22.64 255.255.255.192
```

Note: The use of the subnet mask on the conduit command allows all hosts on the Service network access to this conduit**.**

Inside hosts

Internal comm host at 192.168.4.11.

Access to this host is required by the app supply and prod supply hosts on the Production Network at 150.52.22.130 and 150.52.22.131. The application developers have defined Xtranet traffic as tcp using port 3900. The application developers have programmed www supply traffic as tcp using ports 3200 and 3900. This requires one static command and three conduit commands:

The syntax for this access is:

```
static (inside,Production network) 192.168.4.11 192.168.4.11 netmask
255.255.255.255 0 0
conduit permit tcp host 192.168.4.11 eq 3900 host 150.52.22.130
conduit permit tcp host 192.168.4.11 eq 3200 host 150.52.22.131
conduit permit tcp host 192.168.4.11 eq 3900 host 150.52.22.131
```

The final rule required to enforce our policy of deny unless explicitly authorized. (deny any any)

The command syntax is:

```
conduit deny ip any any
```

This rule will disallow any packets not specifically authorized in the rules presented, including inbound icmp, upd, and tcp on any port.

Outbound traffic on the Pix (higher security to lower security)

The Cisco Pix uses a combination of two commands to allow traffic from a higher security level to a lower security level: outbound and apply. The outbound command is used to create a labeled set of rules. The apply command is then used to bind a named set of outbound rules to an interface on the Pix.

Inside interface.

This controls traffic from the inside network (including the Gauntlet) out. Because the Gauntlet will be used to proxy all the activity from the inside out, only the Gauntlet and specific other hosts need outbound access. We will allow tcp 3200/3900 for Xtranet and www supply from 192.168.4.11. We will allow the Gauntlet at 150.52.22.253 a full range of tcp and udp ports. We will also allow DNS forwarding requests from the internal DNS at 192.168.4.10 The syntax for this access is:

```
outbound  13 deny 0.0.0.0 0.0.0.0 0 0
outbound  13 except 192.168.4.10 0.0.0.0 53 udp
outbound  13 except 192.168.4.11  0.0.0.0 3200 tcp
outbound  13 except 192.168.4.11  0.0.0.0 3900 tcp
outbound  13 except  150.52.22.253 0.0.0.0 0 tcp
outbound  13 except  150.52.22.253 0.0.0.0 0 udp
apply (inside) 13 outgoing_src
```

Production interface.

This controls traffic leaving the Production network. For this, we have one requirement. The app supply host must be able to make tcp request to the internet to pass purchase documents over a variety of ports. (The app supply host never initiates a connection to external hosts).

The syntax for this access is:

```
outbound 23 deny 0.0.0.0 0.0.0.0 0 0
outbound 23 except 150.52.22.130 0.0.0.0 0 tcp
apply (Production network) 23 outgoing_src
```

Service network interface.

This controls traffic outbound from the Service network. There are three requirements. The mail server needs to be able to make smtp (tcp/25) requests out to the internet. In addition, the External DNS hosts need to make DNS forwarding requests (udp/53) to other nameservers on the internet. Finally, the www, mail, ftp, and www supply hosts must reply to ping requests (icmp/0) allowed in.
The syntax for this access is:

```
outbound 33 deny 0.0.0.0 0.0.0.0 0 0
outbound 33 except 150.52.22.72 0.0.0.0 25 tcp
outbound 33 except 150.52.22.71 0.0.0.0 53 udp
outbound 33 except 150.52.22.70 0.0.0.0 0 icmp
outbound 33 except 150.52.22.72 0.0.0.0 0 icmp
outbound 33 except 150.52.22.73 0.0.0.0 0 icmp
outbound 33 except 153.72.42.75 0.0.0.0 0 icmp
apply (Service network) 33 outgoing_src
```

The VPN solution is based upon a Cisco Pix Firewall v5.x located at our business partners and in our network and the Cisco Secure VPN Client solution used for remote access requirements. We are using a wildcard pre-shared key for IKE authentication solution.

The IKE policy is:

```
Isakmp enable outside
Isakmp policy 01 encr 3des
Isakmp policy 01 hash md5
Isakmp policy 01 authentication pre-share
Isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0 (wildcard pre-share key)
crypto dynamic map partner-map 20 ipsec-isakmp dynamic cisco (dynamic crypto map set)
crypto map partner-map interface outside (apply crypto map to outside interface)
```

```
sysopt connection permit-ipsec (tells Pix to implicitly permit IPSec traffic)
```

Accessing the Cisco Pix
For access other than direct console access, we need to allow firewall administrators telnet access to the CiscoPix. With this architecture firewall administers can only come from the Gauntlet proxy at 150.52.22.253. (They must first telnet to the Gauntlet proxy and then telnet to the Cisco Pix).
The syntax for this access is:

```
telnet 150.52.22.253 255.255.255.255
```

Application of the security policy on the Gauntlet proxy

The Cisco Pix was used to control the majority of the access into the security environment. The Gauntlet proxy will be used to control access out of the GIAC Enterprises internal network. Additional information and complete documentation for the Gauntlet proxy is available at URL http://www.nai.com.

Inbound traffic on the Gauntlet.

The only inbound traffic GIAC Enterprises is allowing is the Xtranet and www supply traffic. All other traffic is outbound. The requirements for each of these inbound application services are:

www supply.

This complements the Cisco Pix rule, whereby Production network host 150.52.22.131 needs to talk to inside host 192.168.4.11 on tcp ports 3200/3900. The steps needed are:
Create a plug gateway for port 3200
Create a plug gateway for port 3900
Create service group consisting of plug gateways 3200 and 3900
Create a source rule for 150.52.22.131 using our service group
Create a destination rule for 192.168.4.11 using our service group

These rules complement the Cisco Pix rule, whereby Production network host 150.52.22.130 needs to talk to inside host 192.168.4.11 on tcp port 3900. The steps needed are:
Create a source rule for 150.52.22.130 using the 3900 plug gateway.
Create a destination rule for 192.168.4.11 using the 3900 plug gateway.

Outbound traffic on the Gauntlet.

The majority of the Gauntlet proxy rules will apply to outgoing traffic.

Internal Users.

GIAC Enterprises employees need access the internet via HTTP, HTTPS, and FTP. We will also need POP3 to the mail server on the Service network. We will use standard Gauntlet proxy services to provide this access.

Follow the examples provided earlier to accomplish each of the following requirements.

Create a network entry for our internal network (192.168.4.*)
Create a network entry for all external addresses (including our Service network hosts)
Create user service group consisting of the desired services
Create a source rule referencing our internal network and our service group
Create a destination rule referencing our service group and our external network group
Create a source rule referencing our internal network and the POP3 service.
Create a destination rule using the POP3 service and 150.52.22.72.

Security Support Users.

The security support users require ssh (tcp/22) and telnet (tcp/23) access (in addition to the standard internal user access) to all systems in the security environment. We will need the IP addresses of the security support user desktops.

The steps needed are: Reference examples provided earlier.

Create a network group of our network security team hosts.
Create a network group of all Service network, Service network, the Cisco Pix, and the border router (Cisco 4500).
Create a plug gateway for tcp/22 (ssh) traffic (reference example provided earlier)
Create a service group that includes our ssh plug gateway and standard telnet
Create a source rule using our security support users group and our ssh-telnet service group.
Create a destination rule using our ssh-telnet service group and our all-security-systems group.

Application Support Users.

Application and Web content managers need access to various Service Network and Production Network hosts to provide support and updates. This is all offered using ssh (tcp/22) in addition to the internal user access provided above. We will need a list of all internal IP addresses assigned to these desktops.

Complete the following steps referencing the examples provided above:

Create a network group of our application administrator hosts.
Create a network group of the Production network and Service network hosts.
Create a source rule using our application administrator group and the ssh plug gateway defined in the 'Security Support Users' section.
Create a destination rule using the shh plug gateway defined in the 'Security Support Users' section and the application administrators group.

Application specific needs.

The proposed architecture will require three application specific outbound rules. The Xtranet process needs to communicate from 192.168.4.11 to 150.52.22.130 over tcp 3900. The web supply process needs to communicate from 192.168.4.11 to 150.52.22.131 over tcp ports 3200/3900. The internal DNS server at 192.168.4.10 needs to pass DNS requests to the internet over udp[port 53.

The steps for Xtranet and web supply:

Create a source rule using 192.168.4.11 and the previously defined 3900 plug gateway.
Create a destination rule using 150.52.22.130 and the 3900 plug gateway.

Create a source rule using 192.168.4.11 and the previous defined 3200/3900 service group.
Created a destination rule using 150.52.22.131 and the 3200/3900 service group.

The DNS traffic requires a different category of rule on the Gauntlet. We need to create a packet filter rule to allow forwarding with reply of udp port 53 traffic.

By applying an access filter of "Forward w/Replies", we restrict inbound udp packets only when an outbound connection was established first.

<u>General methods for testing the rules.</u>

Testing this set of rules can prove to be a challenge. A failure may occur on the Pix or the Gauntlet or both. As such, it will take time, patience, and access to the logs from both firewalls.

In addition, because we need to test connectivity from the internet (or lack there of!), we will need access to an internet connected system. One good way to do this is use a separate machine dialed out to the internet service provider.

The logs for the Pix can be reviewed from the console or telnet command line. To access them, we need to be in 'enable mode' and ensure that logging is on. The commands to turn on full logging are:

```
logging on
logging buffered 7
```

We can then view and clear the log with "show logging" and "clear logging".

The log will show us when a connection is successful or unsuccessful. we can then determine if the firewall is seeing the traffic, and if it is functioning the way we intended.

An example of a success from a Pix log is:

```
301003: Built inbound TCP connection 876 for faddr 150.72.22.74/18557 gaddr
150.52.22.73/4000 laddr 150.52.22.73/4000
```

(This is a tcp connection on port 4000 to the Xtranet box on the SERVICE NETWORK)

An example of a failure from a Pix log is:

```
117001: Inbound TCP connection denied from 150.72.22.74/18557 to 150.52.22.73/23
flags SYN
```

(This is a denial of a telnet (tcp/23) attempt to the Xtranetbox on the SERVICE NETWORK)

Logs for the Gauntlet will be on the Gauntlet server in the syslog messages file. You can view the logs by doing a "tail –f' against the log and watch it scroll.

An example of a success from a Gauntlet log is:

```
Jan 16 11:12:31 gauntlet.giac.com GIAC-3900[903]: permit
host=nodnsquery/150.52.22.73 use of proxy ID=90665
Jan 16 11:12:31 gauntlet.giac.com GIAC-3900[903]: permit destination 192.168.4.11/3900
ID=90665
Jan16 11:12:33 gauntlet.giac.com GIAC-3900[903]: exit
```

(This shows the linkage of the source and destination rules for the GIAC-3900 plug service, lasting approximately 2 seconds)

An example of a failure from a Gauntlet log is:

```
Jan 16 11:58:36 gauntlet.giacfortune.com unix: securityalert: udp if=hme1 from
150.52.22.73.:1079 to 192.168.5.2 on unserved port 162
```

(This shows a udp failure on port 162. Note the 'to' address – this is the inside interface of the Gauntlet.

With logging available, there are several techniques we can use to test each rule set.

For tcp based activity, a quick test can simply be to run the desired application

Another way to test tcp activity is using telnet. Telnet to the host with the desired port. For instance, 'telnet 150.52.22.74 4000'. The behavior of the listening service may vary, but the firewall logs will always show a success or failure.

The DNS udp activity is harder to test. The primary way is to force your internal DNS server to make an external query to an address it has not already cached. Your logs should show activity across the firewalls occurred and was allowed or denied.

For each rule, we should test connectivity. Always test from Internet to Service Network, from Service Network to Production Network, from Production Network to internal, etc.

We want to test the 'deny' side of our rules. For example, since ftp should not be allowed to our mail host (150.52.22.72) from the Internet, try doing an ftp from the internet to that host. Not only should the service not be listening on the machine, we should see an entry on the Pix log showing a denial.

To test outbound connectivity for Application developers and General users, you will need to work with a member of those groups, monitor the log while they perform activity from their desktops.

Assignment 3: Audit of Security Architecture

To audit the security architecture defined in assignment 1 we will follow the following four step process.

1. We will need to review user access to systems as defined by request documents and actual user access files. Normal operating system commands will be used for this review.
2. We review active services for various systems and users. This will include a thorough review of the firewall rules. This will require administrator access to the firewall and the use of standard operating system functions.

3. This step will require network scans to confirm the information available and to validate authorized access to each network segment. To accomplish this we will use a laptop configured with the Linux operating systems and common tools such as nslookup, nmap , and telnet.
4. We will provide an complete analysis to include recommendations for improving the assignment 1 security architecture.

Each process will required different levels of expertise and time expenditure to complete. Estimate for each phase of the audit are as follows:

User access:

We will start this process by examining access documentation generated to grant the required access for each user. This documentation already exists and only needs to be reviewed. This review will be completed in approximately 20 hours by our network administration group. Once this review is completed we will review users and group permissions for each network assets to ensure only the authorized access has been configured and granted in accordance with our security policy. This review will required root access to the servers and an internal host to provide the necessary access. This review will be conducted from the internal network.

Examine the passwd and shadow files for each system. Using the access documents review the password file for:

1. All user user id's should be match and access request document
2. All accounts names should be easily related to the real users name.
3. UID's on the accounts should not be 0
4. All user accounts should have an entry in the shadow password field.
5. The named ftp password files should only contain named accounts.

6. Validate the password and shadow files for strength using crack or another password cracking tool.

7. Verify the listing of authorized users against a current company directory to ensure they are still employed and required access.

Port and Protocol Access

Review of the firewall rules the ensure only authorized services are allowed.

This review will be performed during normal business hours with no impact on performance or activity. This review will also be completed from the internal network.. This review will required approximately 8 hours effort from a firewall security engineer with administrator access to all firewalls.

1. This review will reveal the following:
2. Only required services have been provided.
3. The order in which rules have been applied are correct to allow the authorized services.
4. All wildcards "*" will be validated.

The Cisco Pix.

1. Use the "show config" command to list the relevant static, conduit, outbound, and apply rules.
2. We will review each access authorization document to ensure each requested service has a related rule configured.
3. The rules listed using the "show config" command will be reviewed to ensure the rules are in the proper order to allow all authorized services to function.

The Gauntlet Proxy.

We will review the net-perm-table to ensure only authorized services are authorized and that an access authorization document exists for each service provided:

We will first verify the list of source rules. Each rule should have an access authorization document to match the source rule. We will also ensure that each source rule has an associated access authorization document allowing the service.
In addition, for each source rule, we will verify the following:

The network source. Each entry will address a specific host, a network, or a group.
Verify the list of networks and hosts in each network group.
Ensure the 'May Access' or 'May Not Access' box is checked appropriately for all user/network groups.
The Service. Each entry may be a single service or a group of services. Validate the members of all service groups. Review the actual definition for each service provided.

We will repeat this process for all of the destination rules listed.

Review packet screening rules.
Is there a standard service available for this traffic. If so, use the standard service.
Can the traffic be controlled by a '
"plug gateway" service? (NOTE: Only tcp based traffic can be controlled by "plug gateway" services.
Ensure source and destination IP and ports match exactly with the access and authorization documentation.

<u>Network scans</u>.

Actual network scans are usually the most informative. These scans are invasive and will impact network performance and should be conducted during off-peak hours. These scans will reveal the information that is available to a potential network intruder. To scan the network architecture defined in assignment 1 we will allow approximately 16 hours by one network security engineer.

This scan will require a host on the Internet side of our network. A dialup connection will suffice for this purpose. This scan will validate our router ACLs and firewall configuration. We will use nslookup, nmap, telnet, and netstat to complete our scans. . The nmap manual page is can be located at URL
http://www.insecure.org/nmap/nmap_manpage.html

Nslookup

Nslookup will verify our DNS server is accessible from the internet, and doesn't reveal unnecessary configuration information. Using the information provided we will attempt to resolve to a "general internet host" and we will attempt a "zone transfer" to obtain information about our internal network. Ideally, we don't want to be successful with either attempt.ccessful results from the first two attempts, and failures from the last two.

Telnet

We will also use Telnet to review connectivity originating from the Service Network and Production Networks.
From each host on the Service Network, we will attempt telnet to ports 20, 21,22,23, 25, 43, 53, 79, 80, 512, 513, 514, and 2049. We should get a connection failure and firewall log results for each attempt.

Sample output from this activity is as follows:
Telnet from Xtranet to Apps Supply (Service Network to Production Network)

```
#telnet 150.72.22.74 20
Trying 150.52.22.131...
telnet: Unable to connect to remote host: Connection timed out
```

Cisco Pix log shows:

```
105002: Inbound TCP connection denied from 150.52.22.131/2091 to 150.72.22.74/20
flags SYN
```

– This is normal.

Netstat
The netstat command will be used with the –a switch to verify the exact services are listening on each host. We expect the listening ports to coincide with those required on the authorized access documents.

An example of the netstat output from our ex-dns server is might look like this:

```
netstat -a | grep LISTEN
```

```
    *.sunrpc        *.*          0    0    0    0 LISTEN
    *.telnet        *.*          0    0    0    0 LISTEN
    *.22            *.*          0    0    0    0 LISTEN
    *.ftp           *.*          0    0    0    0 LISTEN
localhost.domain    *.*          0    0    0    0 LISTEN
ex-dns.domain       *.*          0    0    0    0 LISTEN
    *.1080          *.*          0    0    0    0 LISTEN
```

Again review this output against the firewall ruleset and the authorized access documentation and make corrections as necessary.

Analysis and recommendations:

The overall security architecture proposed in assignment 1 provides adequate defense for GIAC Fortune enterprises. Defense in depth is provided using the router ACLs and 2 different firewall implementations. I would recommend installing a second T1 to a second Internet Service provider to reduce the risk of DOS vulnerability. The current architecture is vulnerable to DOS attacks as designed. The VPN solution adds an additional function on the Cisco Pix Firewall and could impact network performance. Recommend this function be moved to a standalone server providing the VPN service only. In addition, we are committed to only using network devices and software certified by ICSA Labs. This agency provides rigorous testing and certification to ensure that products perform to acceptable standards.

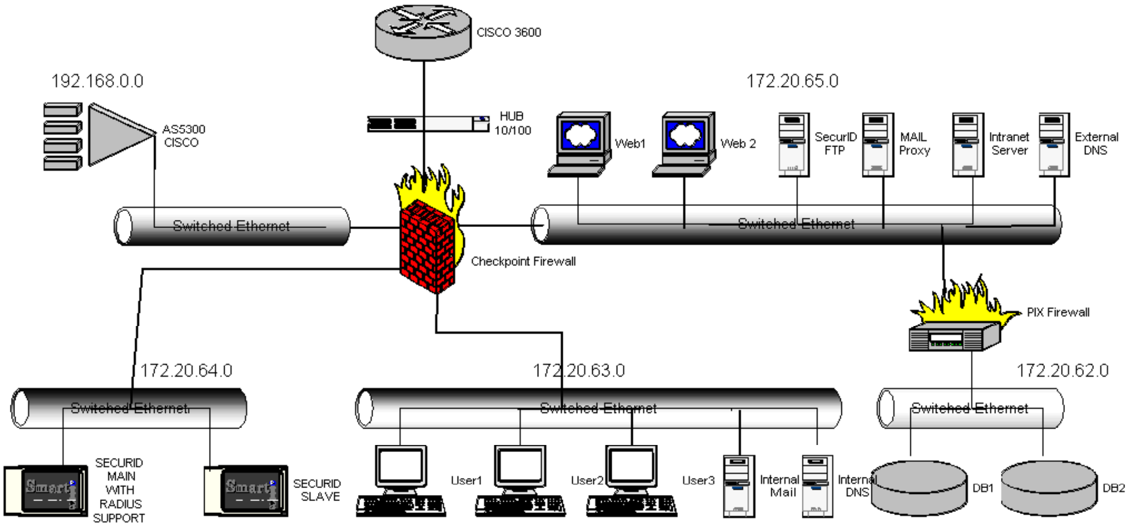
Assignment 4 – Design Under Fire

For this assignment I have selected the practical assignment submitted by Clement Dupuis on September 8, 2000. The complete practical is available at the following URL http://www.sans.org/y2k/practical/clement_dupuis.doc. I will design three attacks against this architecture.

Attack Against the Firewall

There is a published vulnerability for the Checkpoint Firewall-1. The complete vulnerability note can be found at http://www.cert.org/vul_notes/VN-2000-02.html. This vulnerability poses an IP Fragmentation Denial-of-Service threat. This is accomplished by sending a stream of large IP fragments to the firewall (Using jolt2 or a similar tool). As the fragments arrive, the mechanism used to log the IP fragmentation anomalies can monopolize the CPU on the host machine and prevent further traffic (inbound or outbound) from passing through the firewall. This attack could render this network unusable since this is the border firewall for this architecture.

GIAC ENTERPRISES
E-COOKIES ARCHITECTURE



Clement Dupuis's Architecture for GIAC Enterprises

Denial of Service Attack

All systems connected to the Internet are subject to Denial-of-Service attacks. To attack the Clement Dupuis architecture I would use the Stacheldraht denial of service tool. This tool consists of two parts, a master and a daemon. I would scan the Internet and locate as many digital subscriber lines (DSL) and permanent cable modem connections as possible, at least 100. I would then place the daemon on these home computers. The master would be placed on a computer that I have confidence of compromising at will. The attack would be launched from the master, which will direct the daemons to initiate the denial of service attack. The connection between the master and daemon is encrypted during the attack initiation. For this particular attack I will initiate a SYN flood to attempt the denial of service. This attack attempts to consume all resources of the firewall or any other host that controls traffic by opening as many half-port sessions as possible, thus consuming all available resources and denying inbound or outbound services. For additional information on this vulnerability go to URL http://cert.org/advisories/ca2000-01.html.

Web Server

The next attack would attempt to compromise the web server. I would start by gathering as much information as possible about the server. Web servers typically give out an abundance of information whenever a connection is established. I would then research for vulnerabilities based upon the information I collected. I would look at the source code of the web page to determine if a database is attached and what types of files are being served. This could be an indication of how the web site is supported and functions. The next step would be determining the objective of the attack. Once these steps are completed, start the exploit and take the steps necessary to cover my tracks to prevent tracing the attack source.

References

Cisco Pix commands [on-line] Available at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix

Gauntlet Proxy Documentation [on-line] Available at http://www.nai.com

Network Design and Performance, Network Security Conference 2000, Monterey, CA, October 2000, Chris Brenton.

VPNs and Remote Access, Network Security Conference 2000, Monterey, CA, October 2000, Chris Brenton and Dave Elfring.

Sans Level Two Practical Assignment, Clement Dupuis, September 2000, [on-line] Available at http://www.sans.org/y2k/practical/clement_dupuis.doc

Checkpoint Firewall Vulnerabilities [on-line] Available at http://www.cert.org/vul_notes/VN-2000-02.html

Distributed Denial of Service Vulnerability [on-line] Available at http://cert.org/advisories/ca2000-01.html

Nmap manual [on-line] Available at http://www.isecure.org/nmap/nmap_manpage.html

Configuration Guide for the Cisco Secure PIX Firewall Version 5.3, Chapter 5 [on-line] Available at http://www.cisco.com