SANS GIAC Firewall and Perimeter Protection Practical Assignment

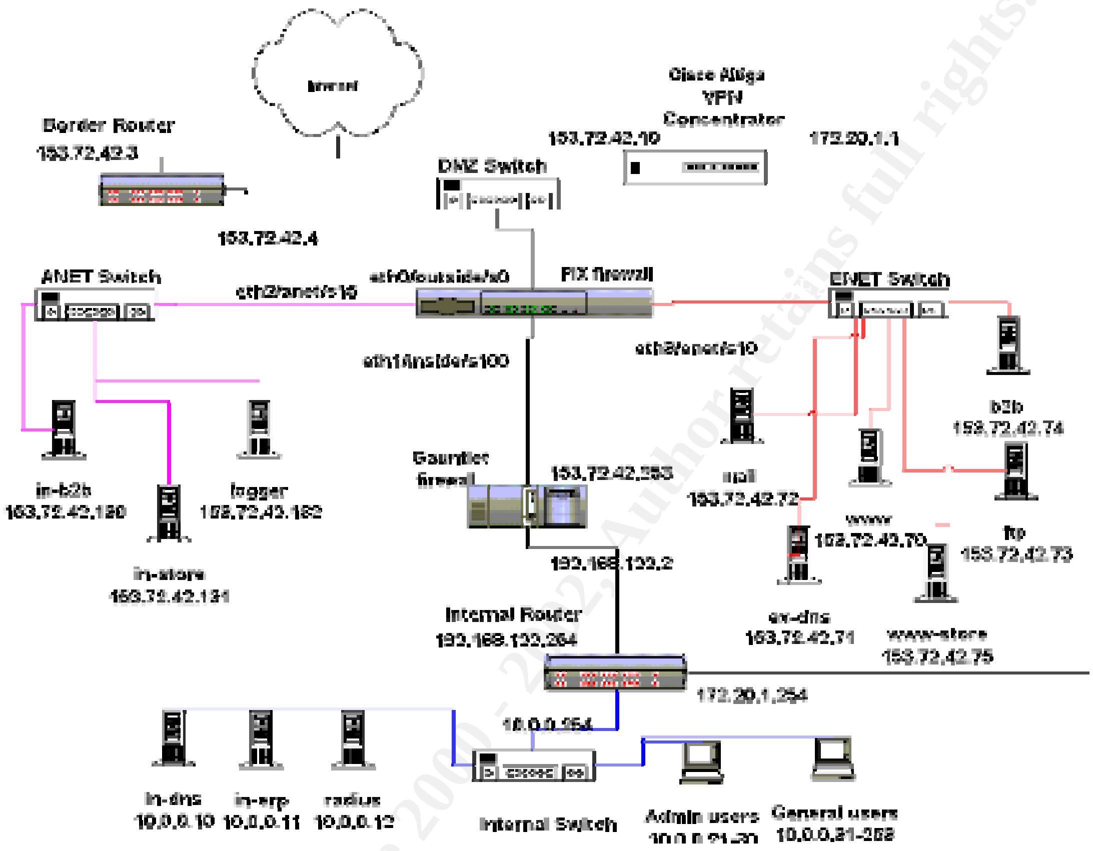
Prepared By Patrick Malone

Based on SANS document Version 1.3 for the Network Security 2000 event.

Contents:

Assignment 1: Security Architecture

The following diagram and explanatory texts are a proposed security architecture for GIAC Enterprises.



The elements and control provided by the diagram above are:

1) Traffic coming through the border router into the security complex is in two general categories: VPN traffic and other traffic.
2) VPN traffic will flow through the Altiga VPN concentrator.
   a) VPN user authentication will be done from an internally hosted Radius server, with host IP addresses assigned by the Altiga. Once connected, the Altiga VPN concentrator will enforce 'split horizon', whereby connected hosts can send and received traffic only over the VPN tunnel. Because the Altiga VPN concentrator is connected to the internal router, any outgoing requests made by VPN clients will pass through the Gauntlet proxy.
3) Non VPN Internet traffic will pass through routers and two physical firewalls: A Cisco Pix stateful firewall and a Gauntlet proxy firewall
   a) The Cisco Pix will provide for two screened networks, know as the ENET and the ANET. The ENET, or External facing network, is the network location for all hosts reachable by the internet. The ANET, or Application facing network, is the network for all internet activity related hosts that are not reachable by the internet. Routing to the internal addresses will be done with static routes on the Pix.
   b) The Gauntlet firewall will provide application filtering and proxy.
4) Two separate firewalls are used to provide diversity and a more complete screening of traffic.
5) All inbound IP traffic from the internet will be allowed to the ENET screened network only.
6) Inbound IP traffic sent directly to the ANET or internal systems will be blocked by the pix.

7) Inbound activity requiring access to GIAC Enterprises internal systems must pass through a transaction brokering 3-tier structure. Web facing components will be on the ENET. These components will then communicate requests to a partner application on the ANET over controlled ports. The ANET systems will then contact any internal systems using defined ports and protocols, controlled by both the Pix and the Gauntlet.
8) Outbound IP activity from GIAC Enterprises internal systems will be screened by both the Gauntlet and the Pix.
9) Firewall rules will control access on these paths:
    a) Internet to ENET - pix
    b) ENET to ANET - pix
    c) ANET to ENET - pix
    d) ANET to internal – pix and gauntlet
    e) ANET to internet - pix
    f) Internal to ANET – gauntlet and pix
    g) Internal to ENET – gauntlet and pix
    h) Internal to internet – gauntlet and pix
10) Elements on the ENET screened network will include:
    a) A corporate world wide web and ftp server. This will provide only public information of static content.
    b) An external dns server. This will only have DNS entries for publicly addressable systems on the ENET. No internal corporate DNS information will be configured on this machine. No zone transfers will be allowed from this DNS server.
    c) A corporate mail server. This will be the mail host for all external internet mail to and from GIAC Enterprises. Internal GIAC employees will read mail from this server via POP.
    d) An external ftp server. This will be used to provide non-anonymous ftp access for GIAC's partners and customers. Access to this system will be by named account.
    e) An external B2B server. This will be used with purchasing partners to exchange XML based purchase orders and related documents. Access will be via HTTPS. This machine is for inbound XML documents sent by external vendors. This system will have a partner system on the ANET.
    f) An external web store front end. This will be used by customer to place and monitor orders for GIAC's products. Access will be via HTTPS only. This system will have a partner system on the ANET.
11) Elements on the ANET screened network will include:
    a) A partner system for the B2B application. This will broker XML documents sent from external purchasing partners. In addition, it will send outbound documents to internet hosts.
    b) A partner system for the web store application. This will broker transactions from the ENET web store server.
    c) A log host. This will be a syslog host used to provide central logging for all ANET and ENET systems.
12) Elements on the internal network related to the security environment include:
    a) An internal DNS server. This will provide all internal DNS services. It will pass off non-internal request to the DNS server in the ENET.
    b) The internal ERP system. This will communicate with the B2B and web store servers in the ANET
    c) An internal Radius authentication server. This will provide authentication for the Altiga VPN concentrator on the DMZ Switch.
    d) Admin user systems. These include system administrators, application administrators, and web content maintainers. Each of these users and the security systems they need access to will be documented.
    e) General user systems. These include the GIAC Enterprises employees that will be browsing the world wide web, as well as reading internet email.

Assignment 2: Security Policy

In order to implement a secure environment using the architecture proposed in assignment one, several general policies will be implemented. Each of the general policy elements will then be demonstrated in detail. Most of the policy element implementation will be presented as it pertains to specific application needs.

1. The border router will implement standard egress and ingress ACL filtering.
2. The stateful firewall will be a Cisco PIX.
3. The default policy on the PIX will be "deny everything". Exceptions are then made for specific application requirements.
4. The proxy firewall will be a Gauntlet firewall.
5. The Gauntlet firewall, by default, will only allow HTTP and HTTPS to the internet from all internal hosts, denying all other inbound and outbound traffic.
6. Each distinct application using systems on either of the screened networks (ENET/ANET) will require a complete and auditable Ports and Protocols document detailing which ports and protocols are required for functionality. This will be used to created exceptions to the default 'deny any any' rule on the PIX and the Gauntlet.
7. No traffic will be allowed from the internet to the ANET or the internal network. Any internet based applications or solutions must be designed to accommodate this policy.
8. Administrative access to the Altiga VPN Concentrator will be enforced in the Altiga setup.
9. Access to all security complex systems must be documented in an auditable Access Request form. This will detail what user coming from what system will access which system. In addition, all accounts on security complex systems must use nicknames not based on existing accounts or user names.

Regarding specific security threats for specific protocols and services, the point of item #3 above is to acknowledge nothing is ever safe. New vulnerabilities show up in old applications on a regular basis. The safest and most prudent way to guard against both old and new threats is to simply deny any traffic we don't expressly need. The same applies for services running on specific hosts. If we don't need a service running on a machine, not only should it be turned off, but it should be de-installed in possible.

Specifics of the policy application will be presented in four major sections:

- Application on the Pix
    - Inbound traffic
    - Outbound traffic
- Application on the Gauntlet
    - Inbound traffic
    - Outbound traffic
- Application on the Altiga VPN Concentrator
- General methods for testing the rules

Application of the security policy on the Pix.

For details on the specifics of Pix commands used in this section, you can reference the on-line command documentation at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix.

The first step is to apply names and security levels to each interface.
The internet facing interface will have the lowest security of 0, the ENET interface will have the next highest at 10, the ANET interface will have the next highest at 15, and the internal interface will have the highest at 100. The commands for this is as follows:

```
nameif ethernet0 outside security0
nameif ethernet3 ENET security10
nameif ethernet2 ANET security15
nameif ethernet1 inside security100
```

Inbound traffic on the Pix (lower security to higher security)
The Pix uses a combination of two commands to allow traffic from a lower security to a higher security: static and conduit. The static command establishes a link between IP addresses on the lower interface and the higher interface. The conduit command attaches to a static translation, controlling the ports and protocols using potential connection.

At this point, no traffic can pass. This is because the default conduit for any inside traffic is a deny of all traffic. We now need to apply rules that allow specific traffic for each inbound host. These rules are presented in the order they should be applied. We start with the outmost zone and work our way in, addressing the needs of each host individually.

Because the ENET screened network is designed specifically to accept traffic from the internet, the first command is to apply a static linking address in the ENET to the outside. This syntax for this is:
static (ENET,outside) 153.72.42.64 153.72.42.64 netmask 255.255.255.192 0 0
The use of the network address and the subnet mask will provide a static for any host put on the ENET.

ENET hosts

1. www host at 153.72.42.70.
   Access to the www host from the outside will be exclusively on port 80 using tcp. We will allow this traffic from any host on the internet. In addition, it has been requested that the www host be pingable from the internet, which is icmp port 8. The conduit commands for this are:
   conduit permit tcp host 153.72.42.70 eq 80 any
   conduit permit icmp host 153.72.42.70 eq 8 any
2. ex-dns host at 153.72.42.41.
   Access to the ex-dns host from the outside will be on udp port 53. We will allow this traffic from any host on the internet. The conduit command for this is:
   conduit permit udp host 153.72.42.71 eq 53 any
3. mail host at 153.72.42.72.
   Access to the ex-dns host from the outside will be on port 25 using tcp. We will allow this traffic from any host in the internet. In addition, it has been requested that the mail host be pingable from the internet, which is icmp port 8. The conduit commands for this are:
   conduit permit tcp host 153.72.42.72 eq 25 any
   conduit permit icmp host 153.72.42.72 eq 8 any
   Note that this host will also need an outbound rule applied. See the outbound section below.
4. ftp host at 153.72.42.73.
   Access to the ftp host from the outside will be on tcp ports 20 and 21. We will allow this traffic from any host on the internet. In addition, it has been requested that the mail host be pingable from the internet, which is icmp port 8. The conduit commands for this are:
   conduit permit tcp host 153.72.42.73 eq 20 any
   conduit permit tcp host 153.72.42.73 eq 21 any
   conduit permit icmp host 153.72.42.73 eq 8 any
5. b2b host at 153.72.42.74.
   Access to the b2b host has been defined by the application developers as tcp (https) on port 4000. We will allow this traffic from only selected business partners as defined by the B2B application team. *For each business partner, we will need a separate conduit command.* The commands for business partner goodstuff.com is:
   conduit permit tcp host 153.72.42.74 eq 4000 host 199.54.23.52
6. www-store host at 153.72.42.75.
   Access to the www-store host has been defined by the application developers as tcp (https) on port 443. We will allow traffic from any host on the internet. In addition, it has been requested that the mail host be pingable from the internet, which is icmp port 8. The conduit commands for this are:
   conduit permit tcp host 153.72.42.74 eq 443 any
   conduit permit icmp host 153.72.42.74 eq 8 any

ANET hosts

7. in-b2b host at 153.72.42.130.

Access to the in-b2b host has been defined by the application developers as tcp on port 4000. Inbound access to this host will be allowed only from the b2b host on the ENET at 153.72.42.74. This requires a combination of a static command and a conduit command:

```
static (ANET,ENET) 153.72.42.130 153.72.42.130 netmask 255.255.255.255 0 0
conduit permit tcp host 153.72.42.130 eq 4000 host 153.72.42.74
```

Note that this host will also need an outbound rule applied. See the outbound section below.

8. in-store host at 153.72.42.131.
   Access to the in-store host has been defined by the application developers as tcp on ports 3200 and 3900. Inbound traffic will only be allowed from the www-store host on the ENET at 153.72.42.75. This requires a static command and two conduit commands:
   ```
   static (ANET,ENET) 153.72.42.131 153.72.42.131 netmask 255.255.255.255 0 0
   conduit permit tcp host 153.72.42.131 eq 3200 host 153.72.42.75
   conduit permit tcp host 153.72.42.131 eq 3900 host 153.72.42.75
   ```
   Note that this host will also need an outbound rule applied. See the outbound section below.
9. Logger at host 153.72.42.132.
   Access to the logger host will be via udp port 514. Inbound traffic will be allowed from systems on the ENET. This requires a static command and a conduit command:
   ```
   static (ANET,ENET) 153.72.42.132 153.72.42.132 netmask 255.255.255.255 0 0
   conduit permit udp host 153.72.42.132 eq 514  host 153.72.42.64 255.255.255.192
   ```
   The use of the subnet mask on the conduit command allows all hosts on the ENET to use this conduit.

Inside hosts

10. in-erp host at 10.0.0.11.
    Access to this hosts is required from both the in-b2b and in-store hosts on the ANET at 153.72.42.130 and 153.72.42.131. The application developers have defined b2b traffic as tcp over port 3900. The application developers have defined www-store traffic as tcp over ports 3200 and 3900. This requires one static command and three conduit commands:
    ```
    static (inside,ANET) 10.0.0.11 10.0.0.11 netmask 255.255.255.255 0 0
    conduit permit tcp host 10.0.0.11 eq 3900 host 153.72.42.130
    conduit permit tcp host 10.0.0.11 eq 3200 host 153.72.42.131
    conduit permit tcp host 10.0.0.11 eq 3900 host 153.72.42.131
    ```

The final default rule

11. The final rules will be to restate the implied deny any any rule. The command is:
    ```
    conduit deny ip any any
    ```
    These will disallow any traffic 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 Pix uses a combination of two commands to allow traffic from a higher security to a lower security: 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.

We will build a set of rules to apply to each interface, starting with the inside most one and working out.

1. Inside interface.
   This controls traffic from the inside network (including the Gauntlet) out. Because the Gauntlet will be used to proxy nearly all the activity from the inside out, only the Gauntlet and specific other host need outbound access. We will allow tcp 3200/3900 for b2b and web store from 10.0.0.11. We will allow the Gauntlet at 153.72.42.253 a full range of tcp and udp ports. We will also allow DNS forwarding requests from the internal name server at 10.0.0.10 The command for building this outbound group is:
   ```
   outbound  13 deny 0.0.0.0 0.0.0.0 0 0
   outbound  13 except 10.0.0.10 0.0.0.0 53 udp
   outbound  13 except 10.0.0.11  0.0.0.0 3200 tcp
   outbound  13 except 10.0.0.11  0.0.0.0 3900 tcp
   ```

```
outbound  13 except  153.72.42.253 0.0.0.0 0 tcp
outbound  13 except  153.72.42.253 0.0.0.0 0 udp
apply (inside) 13 outgoing_src
```

(*A note here on ENET hosts and name resolution. ENET systems will require static host entries for each host on the ANET system need to communicate with. The ex-dns system will not have records for anything on the ANET or the GIAC internal network.*)

2. ANET interface.
   This controls traffic leaving the ANET. For this, we have one requirement. The in-b2b host must be able to make tcp request to the internet to pass XML documents over a variety of ports. (The in-store host never initiates a connection outside, only inside). The commands for building this outbound group are:
   ```
   outbound 23 deny 0.0.0.0 0.0.0.0 0 0
   outbound 23 except 153.72.42.130 0.0.0.0 0 tcp
   apply (ANET) 23 outgoing_src
   ```
   (*A note here on ANET hosts and name resolution. ANET systems will require static host entries for each host they need to communicate with. DNS traffic in/out of the ANET is not open.*)
3. ENET interface.
   This controls traffic leaving the ENET. For this, we have three requirements. The mail server needs to be able to make smtp (tcp/25) requests out to the internet. In addition, the ex-dns machine needs to make dns forwarding requests (udp/53) to other nameservers on the internet. Finally, the www, mail, ftp, and www-store hosts must reply to ping requests (icmp/0) allowed in. The commands for building this outbound group are:
   ```
   outbound 33 deny 0.0.0.0 0.0.0.0 0 0
   outbound 33 except 153.72.42.72 0.0.0.0 25 tcp
   outbound 33 except 153.72.42.71 0.0.0.0 53 udp
   outbound 33 except 153.72.42.70 0.0.0.0 0 icmp
   outbound 33 except 153.72.42.72 0.0.0.0 0 icmp
   outbound 33 except 153.72.42.73 0.0.0.0 0 icmp
   outbound 33 except 153.72.42.75 0.0.0.0 0 icmp
   apply (ENET) 33 outgoing_src
   ```

Access to the Pix itself

Aside from direct console access, we need to allow firewall administrators telnet access to the Pix. In GIAC Enterprises, the firewall administers can only come from the Gauntlet at 153.72.42.253. (They will need to telnet to the Gauntlet, then telnet to the Pix). The command for this is:

```
telnet 153.72.42.253 255.255.255.255
```

The Pix rules all together

Here is a list of all the Pix rules listed together.

```
static (ENET,outside) 153.72.42.64 153.72.42.64 netmask 255.255.255.192 0 0
static (ANET,ENET) 153.72.42.130 153.72.42.130 netmask 255.255.255.255 0 0
static (ANET,ENET) 153.72.42.131 153.72.42.131 netmask 255.255.255.255 0 0
static (ANET,ENET) 153.72.42.132 153.72.42.132 netmask 255.255.255.255 0 0
static (inside,ANET) 10.0.0.11 10.0.0.11 netmask 255.255.255.255 0 0
conduit permit tcp host 153.72.42.70 eq 80 any
conduit permit icmp host 153.72.42.70 eq 8 any
conduit permit udp host 153.72.42.71 eq 53 any
conduit permit tcp host 153.72.42.72 eq 25 any
conduit permit icmp host 153.72.42.72 eq 8 any
conduit permit tcp host 153.72.42.73 eq 20 any
conduit permit tcp host 153.72.42.73 eq 21 any
conduit permit icmp host 153.72.42.73 eq 8 any
conduit permit tcp host 153.72.42.74 eq 4000 host 199.54.23.52
conduit permit tcp host 153.72.42.74 eq 443 any
conduit permit icmp host 153.72.42.74 eq 8 any
conduit permit tcp host 153.72.42.130 eq 4000 host 153.72.42.74
```

```
conduit permit tcp host 153.72.42.131 eq 3200 host 153.72.42.75
conduit permit tcp host 153.72.42.131 eq 3900 host 153.72.42.75
conduit permit udp host 153.72.42.132 eq 514  host 153.72.42.64 255.255.255.192
conduit permit tcp host 10.0.0.11 eq 3900 host 153.72.42.130
conduit permit tcp host 10.0.0.11 eq 3200 host 153.72.42.131
conduit permit tcp host 10.0.0.11 eq 3900 host 153.72.42.131
conduit deny ip any any
outbound  13 deny 0.0.0.0 0.0.0.0 0 0
outbound  13 except 10.0.0.10 0.0.0.0 53 udp
outbound  13 except 10.0.0.11  0.0.0.0 3200 tcp
outbound  13 except 10.0.0.11  0.0.0.0 3900 tcp
outbound  13 except  153.72.42.253 0.0.0.0 0 tcp
outbound  13 except  153.72.42.253 0.0.0.0 0 udp
outbound 23 deny 0.0.0.0 0.0.0.0 0 0
outbound 23 except 153.72.42.130 0.0.0.0 0 tcp
outbound 33 deny 0.0.0.0 0.0.0.0 0 0
outbound 33 except 153.72.42.72 0.0.0.0 25 tcp
outbound 33 except 153.72.42.71 0.0.0.0 53 udp
outbound 33 except 153.72.42.70 0.0.0.0 0 icmp
outbound 33 except 153.72.42.72 0.0.0.0 0 icmp
outbound 33 except 153.72.42.73 0.0.0.0 0 icmp
outbound 33 except 153.72.42.75 0.0.0.0 0 icmp
apply (inside) 13 outgoing_src
apply (ANET) 23 outgoing_src
apply (ENET) 33 outgoing_src
telnet 153.72.42.253 255.255.255.255
```

Application of the security policy on the Gauntlet

The Pix was used to control most of the access into the security environment. The Gauntlet will be used to control access out of the GIAC Enterprises internal network. The Gauntlet has a large number of delivered proxy services to handle various types of applications. We will make use of several that are provided, as well as creating several custom 'plug gateway' services. For information and documentation for the Gauntlet, browse to the site http://www.nai.com.

There will be a blanket set of rules for general users, a tighter set of rules for security and application support personnel, and an even smaller set of rules to accommodate specific applications that require cross-firewall communication.

The Gauntlet works by linking source rules and destination rules by a common service. In order to complete a connection, you must define the addresses of all involved hosts. These can be individual hosts or a group of hosts. You must also define services. Again, these can be individual services or a group of services. Finally, you create source and destination rules using the defined addresses and services. Where services link, traffic is allowed.

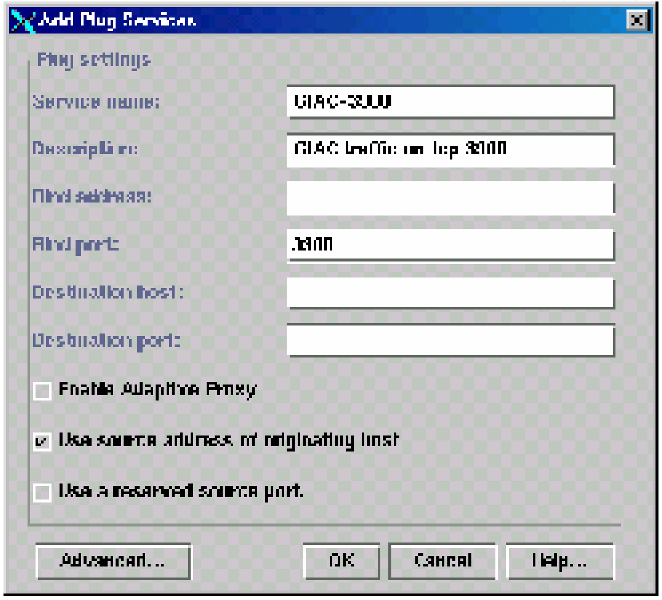
Inbound traffic on the Gauntlet.

The only inbound traffic GIAC Enterprises is allowing is the b2b and www-store traffic. All other traffic is outbound. The components for each of these inbound applications is as follows.

1. www-store.
   This mimics the Pix rule, whereby ANET host 153.72.42.131 needs to talk to inside host 10.0.0.11 on tcp ports 3200/3900. The steps needed are:
   - Create 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 153.72.42.131 using our service group

- Create a destination rule for 10.0.0.11 using our service group

Picture #1 shows the screenshot for creating a plug gateway service for port 3900.



Add Plug Services

Plug settings

Service name: GIAC-3900

Description: GIAC traffic on tcp 3900

Bind address:

Bind port: 3900

Destination host:

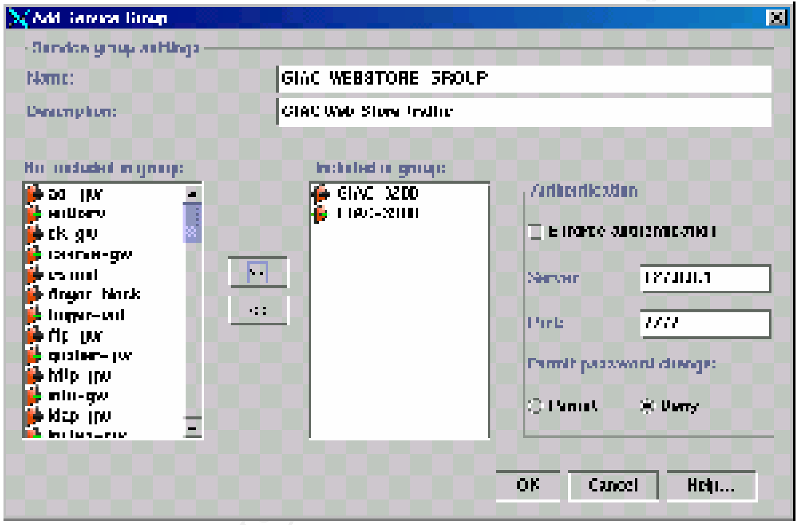
Destination port:

☐ Enable Adaptive Proxy

☑ Use source address of originating host

☐ Use a reserved source port.

Picture #2 shows a screenshot for creating a service group.



Add Service Group

Service group settings

Name: GIAC WEBSTORE GROUP

Description: GIAC Web Store traffic

Not included in group:

aol-gw
auth-srv
ck-gw
cserve-gw
cs-mail
finger-block
finger-srv
ftp-gw
gopher-gw
http-gw
info-gw
ldap-gw
lnotes-gw

Included in group:

GIAC-3200
GIAC-3900

Authentication

☐ Enable authentication

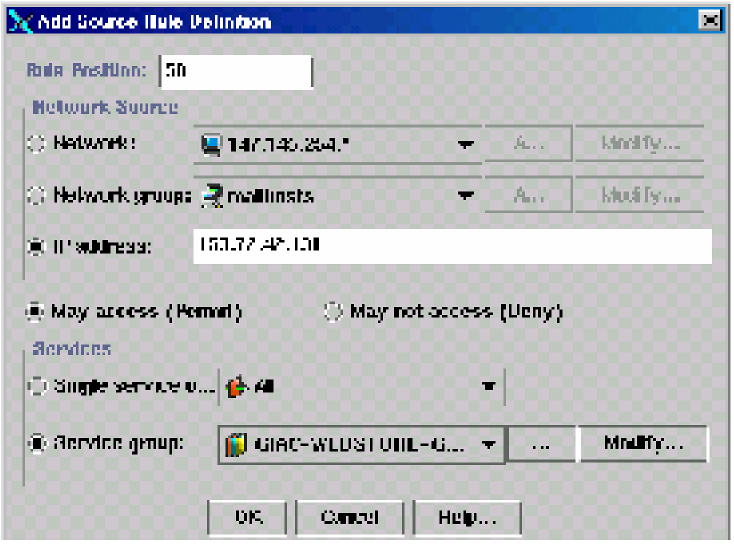
Server 127.0.0.1

Port 7777

Permit password change:

○ Permit ● Deny

Picture #3 shows a screenshot for creating a source rule.



Add Source Rule Definition

Rule Position: 50

Network Source

○ Network: 147.145.254.*

○ Network group: mailhosts

● IP address: 153.72.42.130

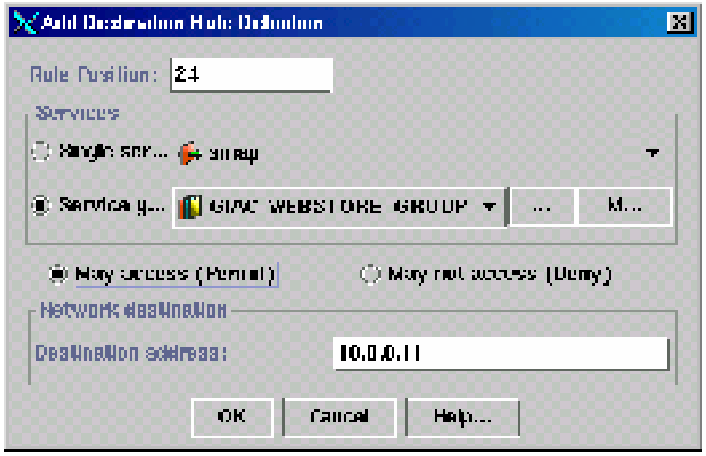
● May access (Permit) ○ May not access (Deny)

Services

○ Single service o...: All

● Service group: GIAC-WEBSTORE-G...

Picture #4 shows a screen shot for creating the destination rule.



Add Destination Rule Definition

Rule Position: 24

Services

○ Single ser...: snmp

● Service g...: GIAC WEBSTORE GROUP

● May access (Permit) ○ May not access (Deny)

Network destination

Destination address: 10.0.0.11

With these rules in place, connectivity from in-store to in-erp are in place.

2. B2B.
This mimics the Pix rule, whereby ANET host 153.72.42.130 needs to talk to inside host 10.0.0.11 on tcp port 3900. The steps needed to provide this are:
   - Create a source rule for 153.72.42.130 using the 3900 plug gateway from above.
   - Create a destination rule for 10.0.0.11 using the 3900 plug gateway

(see screen shots above for examples)

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

3. Internal Users.
The first set of rules we need to build will allow GIAC Enterprises employees to access the internet via HTTP, HTTPS, and FTP. In addition, we need to allow POP3 to the mail server on the ENET. We will use standard Gauntlet services to provide this access. The steps needed are:
   - Create a network entry for our internal network (10.0.0.*)
   - Create a network entry for all external addresses (including our ENET 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 153.72.42.72.

(see screen shots above for examples)

4. Security Support Users.
   The security administration team needs 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's of the network security team desktops. The steps needed are:
   - Create a network group of our network security team hosts.
   - Create a network group of all ENET, ENET, the Pix, and the border router.
   - Create a plug gateway for tcp/22 (ssh) traffic
   - Create a service group that includes our ssh plug gateway and standard telnet
   - Create a source rule using our network security group and our ssh-telnet service group.
   - Create a destination rule using our ssh-telnet service group and our all-security-systems group.

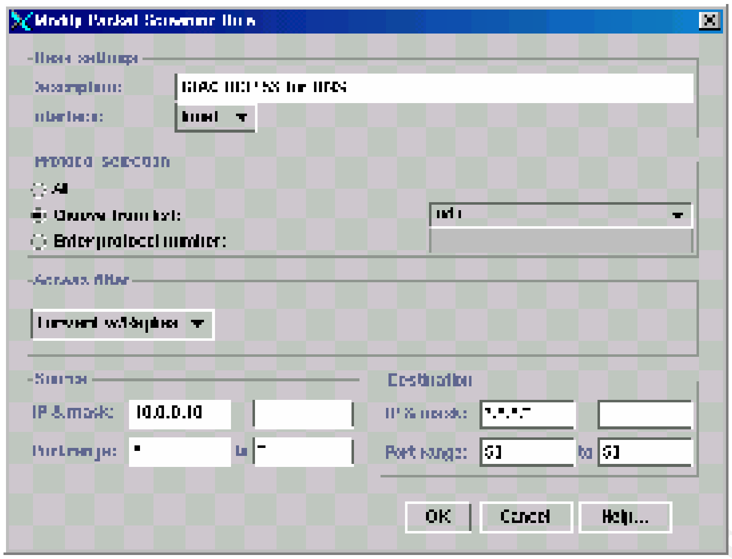
   (see screen shots above for examples)

5. Application Support Users.
   Application and Web administrators need access to various ENET and ANET systems to provide support and updates. This is all offered vi ssh (tcp/22) in addition to the internal user access provided above. We will need a list of all internal IP's these people have on their desktops. The steps needed are:
   - Create a network group of our application administrator hosts.
   - Create a network group of the ANET and ENET systems.
   - 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.

   (see screen shots above for examples)

6. Application specific needs.
   Our environment requires three application specific outbound rules. The b2b process needs to communicate from 10.0.0.11 to 153.72.42.130 over tcp 3900. The web store process needs to communicate from 10.0.0.11 to 153.72.42.131 over tcp ports 3200/3900. The internal DNS server at 10.0.0.10 needs to pass DNS requests to the internet over udp[port 53. The steps for b2b and web store are similar to those above:
   - Create a source rule using 10.0.0.11 and the previously defined 3900 plug gateway.
   - Create a destination rule using 153.72.42.130 and the 3900 plug gateway.
   - Create a source rule using 10.0.0.11 and the previous defined 3200/3900 service group.
   - Created a destination rule using 153.72.42.131 and the 3200/3900 service group.

   The DNS traffic requires a new type of rule on the Gauntlet. There are no proxy services for udp traffic. We need to create a packet filter rule to allow forwarding with reply of udp port 53 traffic. Picture #5 shows a screenshot for creating the forward filter rule.



Basic settings

Description: GIAC ACCESS for DNS

Interface: Inner

Protocol selection

○ All

● Choose from list: udp

○ Enter protocol number:

Access filter

Forward w/Replies

Source

IP & mask: 10.0.0.10

Port range: * to *

Destination

IP & mask: *.*.*.*

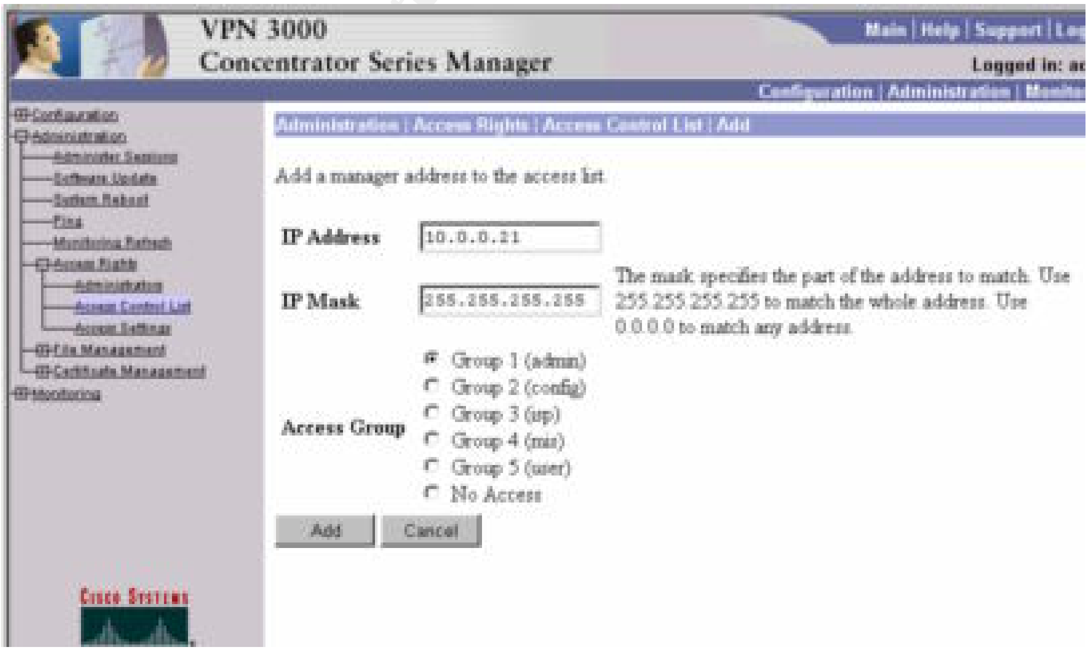
Port range: 53 to 53

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

Application on the Altiga VPN Concentrator.

The Altiga VPN Concentrator enforces 'split horizon'. This is to say that when a VPN connection is active between a host and the concentrator, the host may not send or accept network traffic from any source other than through the VPN tunnel. This option can not be turned off. This is important because it stops a users VPN connection from being used as a tunnel into the internal network. As such, we can depend upon user authentication to control incoming traffic.

The one piece we can not control is administrative access. We could block access using extended ACLS on the border router. However, these can have a significat performance impact. Instead, we will us the Altiga administrative software itself to only allow administrative access to a list of selected internal hosts, thus blocking access from the internet and internal network. Picture #7 is a screen shot of the Altiga web interface showing how to apply a host to the administration access control list.



Administration | Access Rights | Access Control List | Add

Add a manager address to the access list.

IP Address: 10.0.0.21

IP Mask: 255.255.255.255

The mask specifies the part of the address to match. Use 255.255.255.255 to match the whole address. Use 0.0.0.0 to match any address.

Access Group:
- ● Group 1 (admin)
- ○ Group 2 (config)
- ○ Group 3 (isp)
- ○ Group 4 (mis)
- ○ Group 5 (user)
- ○ No Access

This access control list, combined with the administrative password access, will limit administrative access to only our limited set of trusted internal hosts.

General methods for testing the rules.

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 (say a laptop) dialed out to your friendly internet service provider. Of course, having Unix command line access is best.

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 made or denied. With this, we can help determine if the firewall is seeing the traffic, and if it is behaving the way we intended.

An example of a success from a Pix log is:

```
302001: Built inbound TCP connection 949 for faddr 63.227.180.36/19353 gaddr 153.72.42.73/4000 laddr 153.72.42.73/4000
```

(This is a tcp connection on port 4000 to the b2b box on the ENET)

An example of a failure from a Pix log is:

```
106001: Inbound TCP connection denied from 63.227.180.36/19351 to 153.72.42.73/23 flags SYN
```

(This is a denial of a telnet (tcp/23) attempt to the b2b box on the ENET)

Logs for the Gauntlet will be on the Gauntlet server in the syslog messages file (for Unix). A good way to watch this is to do a 'tail –f' against the log and watch it roll.

An example of a success from a Gauntlet log is:

```
Nov 16 12:12:31 gauntlet.giac.com GIAC-3900[904]: permit host=nodnsquery/153.72.42.73 use of proxy ID=90465
Nov 16 12:12:31 gauntlet.giac.com GIAC-3900[904]: permit destination 10.0.0.11/3900 ID=90465
Nov 16 12:12:33 gauntlet.giac.com GIAC-3900[904]: exit
```

(This shows the linkage of the source and destination rules for the GIAC-3900 plug service, lasting apx 3 seconds)

An example of a failure from a Gauntlet log is:

```
Nov 16 12:58:36 gauntlet.giac.com unix: securityalert: udp if=hme0 from 10.0.0.50:1079 to
192.168.122.2 on unserved port 162
```

(This shows a udp failure on port 162. Note the 'to' address – this is the inside interface of the Gauntlet. Request against unserved ports made to the Gauntlet are seen on the receiving interface)

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 (such as a web browser or an ftp session).
- Another quick way to test tcp activity is using telnet. Telnet to the host with the desired port. For instance, 'telnet 153.72.42.74 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. Make sure to test in and out, from internet to ENET, from ENET to ANET, from ANET to internal, etc.
- Don't forget we want to test the 'deny' side of our rules. For example, since ftp should not be allowed to our mail host (153.72.42.72) 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, watching the log while they perform activity from their desktops.
- Note that once regular activity begins across the environment, the amount of information coming out of the logs can be significant. It is helpful to pull a copy off and use various text filters such as grep (or even search in an editor!) to look for specific activity.

Assignment 3: Audit of Security Architecture

In order to audit the Security Architecture GIAC enterprises, we will focus on several areas.

- First will be user access to systems as defined by request documents and actual user access files. Tools used will be standard OS commands.
- Second, we will look at port and protocol access to the various systems as defined by documents and firewall rules. Tools used will be some standard OS commands, as well as command access to the firewalls.
- Third, we well perform a series of network scans to determine of the potential access on each system. Tools used will be a scanning host (Linux), the nslookup command, the nmap port scanning tool, and telnet.
- Fourth, we will provide an analysis with recommendations based on the results of the audit activities.

Each of the process use different methods and will have different impacts on the working environment at GIAC enterprises. As such, estimates of effort and cost, as well as recommended times and potential impacts will be discussed in each section.

1. User access

Based on the policy requirements of documents describing user access to each of the systems, we will need to collect the user access documents and perform a review of accounts on the various systems. The primary items we will be looking for are:

- All user with access are approved for such access
- Usernames are not based on a real persons name
- Passwords are not easily guessed/cracked
- Employees no longer with the company have had their access removed

This activity can be performed during normal business hours with no impact on performance or activity. This should be done from inside GIAC. Once the necessary documents have been provided, this should take no more than 16 hours of effort. It will require root level access to the machines, as well as an internal host that can be used to deploy some tools. This can be performed by a single person.

To begin with, the passwd and shadow files from each system should be retrieved and stored on the work host. In addition, the named ftp passwd files should be obtained as well. With the documents in hand, the password file should be reviewed against the approved user list. Items to check for are:

- All non-system user id's should be on an access request document
- All approved accounts should not be named relative to users real name
- UID's on the accounts should not be 0
- All accounts should have something in the shadow password field
- On the named ftp password files, ensure that these contain only the named accounts and not other accounts.

Once the list of users has been validated, the password and shadow files should be run through crack or some other password cracking tool. We will use a large dictionary. In addition, we will customize the dictionary adding acronyms found commonly at GIAC. Any cracked passwords will be noted.

Finally, the list of active users will be checked against a current company directory. Any active user found that are not in the current company directory will be noted.

At the end of this process, all files will be deleted from the working host.

2. Port and Protocol Access.

Based on the policy requirements of documents describing the port and protocol access to each systems, we will need to collect the documents (referred to as P&P) and perform a review of the firewall rules.

This activity can be performed during normal business hours with no impact on performance or activity. This should be done from inside GIAC. Once the necessary documents have been provided, this should take no more than 8-10 hours of effort. It will require administrative access to both the Pix and the Gauntlet. This can be performed by a single person.

The primary items we will be looking for are:

- Each requested port and protocol has been addressed
- There are no 'extra' open ports and protocols. Special attention will be paid to any rule with a '*' or 'any' value in any field.
- The order in which rules have been applied do not invalidate required restrictions or allowances.

The Pix.
On the Pix, the **show config** command will be used to list the relevant static, conduit, outbound, and apply rules. This list will be captured to a file for review. The **show config** command list the static commands first, followed by the conduit commands, followed by the outbound commands, followed by the apply commands, finally followed by the telnet commands.

We will then check each P&P document, ensuring each requested access has a related rule or set of rules. We will then reverse the process, and make sure each static, conduit, or outbound except (that is not a deny) has a matching line in the documents. We will also ensure that telnet access to the Pix is limited to selective hosts, and that those hosts are documented. Any unmatched P&P request or Pix rule will be noted.

Finally, the list or rules provided will the **show config** command will be examined to ensure there are no holes in the rule order that may cause an early rule to invalidate a later rule.

The Gauntlet.
On the Gauntlet, various sections of the GUI interface will be used to determine a fit with the P&P documents.
(*Gauntlet rules are saved in a text file on the Gauntlet server called netperm-table. However, the complexity of this file does not enable a quick overview of the complexity of the Gauntlet environment. Carefully examining each level within the GUI is the best way to audit a Gauntlet firewall*)

We will start with the list of source rules. First, we will ensure that each P&P request has a matching source rule. Then, we will reverse the process and make sure each source rule has a matching P&P request. For each source rule, we will check the following:

- The network source. Each entry will either be a specific machine, a network, or a network group. Special attention will be paid to the list of networks and hosts in each network group.
- Ensure the 'May Access' or 'May Not Access' box is checked appropriately.
- The Service. Each entry may be a single service or a group of services. Special attention will be paid to the members of a service group. This will require drilling down to the actual service definition for each service.

Next we will examine the destination rules. As with the source rules, we will ensure that each P&P request has a matching destination rule. Then, we will reverse the process and make sure each destination rule has a matching P&P request. For each destination rule, we will check the following:

- The Service. Each entry may be a single service or a group of services. Special attention will be paid to the members of a service group. This will require drilling down to the actual service definition for each service.
- Ensure the 'May Access' or 'May Not Access' box is checked appropriately.
- The Network Destination.????

Next, we will examine each packet screening rule. Because the Gauntlet provides proxies for a wide variety of applications, including the 'plug gateway' service that allows us to define specific tcp based activity, ANY packet screening rule activated should be highly scrutinized. The Gauntlet documentation provides several warnings about the dangers of enabling packet screening rules. This should be heeded. For each packet screening rule, will check the following:

- Is there a provided standard service for this traffic. If so, the standard service should be used.
- Can the traffic be controlled by a 'plug gateway' service. Only tcp based traffic can be controlled by 'plug gateway' services. If the packet screening rule is addressing tcp services, the need for a packet screen should be scrutinized.
- If the packet screening rule passes the previous scrutiny, we need to insure the source and destination IP and ports match exactly with the P&P requests. Remember that many initiated requests use ephemeral ports, so a source port of '*' is not unreasonable. However a destination port of "*' will be considered unacceptable.

Finally, we need to examine the combination or source and destination rules as a whole, paying special attention to the order of the rules. The Gauntlet, because of it's ability to nest network definitions and service groups, requires careful scrutiny. Actual end-to-end connections through the gauntlet occur when source and destination rules link at their service. Because of this, consideration will be given to the effective use of names and comments for networks, network groups, services, and service groups defined in the Gauntlet.

3. **Network scans.**

The performance of actual network scans is the most informative, yet invasive and impacting parts of the audit. This step is not based on reviewing an auditable set of documents. Instead, it is performed from the perspective of a potential intruder wanting any and all knowledge and access of our systems.

The time and resource requirements of this activity are much more restrictive than the previous one.

First, this should be done during a period when little or no activity is occurring on the security environment. Not only does this ensure the auditing activity will not impact business needs, it also ensures the logs we will be reviewing are not filled up with desired traffic. We will perform this activity over a weekend, with ample notice provided to both GIAC employees and customers to expect internet related delays and outages. Because of the large number of scanning requirements, this will take 14-20 hours. Blocking out the entire weekend for this activity is recommended. This can be performed by a single person.

Second, because the primary perspective we want to audit is that of an internet based threat, we need a host outside of our environment from which to perform our scans. There are several avenues for this. For our audit purposes, we plan to temporarily but a switch between the border router and the firewall. We will then put a host on that switch, using it to launch our scans. The host will be turned off once the scans are complete. This has the limitation of not including any border router ACL rules in our audit. However, our primary focus is to check the protection provided by the firewall. One benefit to this approach is it would will be easy to re-apply when changes are made to the security environment in the future.

The primary tools we will use for our scans are nslookup, nmap, telnet, and netstat. Nmap and documentation for it is available from http://www.insucure.org/nmap. (The actual man page is on-line at http://www.insecure.org/nmap/nmap_manpage.html)

- Nslookup
  Nslookup will be used to ensure our DNS server is accessible from the internet, but not configured to provide too much information. We will use the server to try and resolve a general internet host, a GIAC host on the internet, and an internal GIAC host. Finally, we will attempt a zone transfer from the host. We should see successful results from the first two attempts, and failures from the last two.

The following are the results of our nslookup against ex-dns.giac.com:

```
> server 153.72.42.72
Default Server:  ex-dns.giac.com
Address: 153.72.42.72
```

Test 1 worked as desired (success)

```
> sans.org
Name Server: ex-dns.giac.com
Address: 153.72.42.72
Trying DNS
Name:    sans.org
Address:  167.216.133.33
```

Test 2 worked as desired (success)

```
> www.giac.org
Name Server: ex-dns.giac.com
Address: 153.72.42.72
Trying DNS
Name:    www.giac.org
Address: 153.72.42.70
```

Test 3 worked as desired (failure)

```
> in-dns.giac.com
Name Server: ex-dns.giac.com
Address: 153.72.42.72
Trying DNS
looking up FILES
*** No address information is available for "in-dns.giac.com"
```

Test 4 worked as desired (failure)

```
> ls -d giac.com.com
[in-dns.giac.com]
*** Can't list domain giac.com: Unspecified error
```

The final check for DNS will be to ensure the zone transfer error was logged by our DNS server. The results from the syslog were:

Nov 22 10:07:20 ex-dns named[23651]: unapproved AXFR from [205.170.0.10].2327 for "giac.com" (acl)

This shows our logging system capture the attempt.

- Nmap

  Nmap will be used to do both TCP and UPD scans of the hosts from the internet to ensure there are no hosts and services available that we do not want. For each host, will runnmap two times, first scanning TCP , then UDP.

  The nmap results should show only open ports for those that we expect. In addition, we should see logs on the Pix showing denials.

  The nmap commands we will use are:

  - nmap -P0 -p1-65535 <host> . This command will attempt a tcp connect to ports 1-65535 on the target host. It will not attempt a ping before trying a connect.
  - nmap -sU -p1-65535 <host>. This command will attempt a udp connection to ports 1-65535 on the target host.

  We will perform this command against all ENET and ANET . As there will be no route to inside systems from the internet side of the Pix, scanning those host would be counterproductive.

  The following the results of our scan against the b2b server in the ENET.
  The TCP port scan:

```
# nmap -P0 -p1-65535 153.72.42.74
Starting nmap V. 2.52 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on b2b.giac.com (153.72.42.74):
(The 65534 ports scanned but not shown below are in state: filtered)
Port      State      Service
4000/tcp   open       hidden
Nmap run completed -- 1 IP address (1 host up) scanned in 2101 seconds
```

We see that if found port 4000/tcp open, with others filtered. This is what we expected. The Pix logs during the scan are lengthy, but a sample of them is:

```
106001: Inbound TCP connection denied from 153.72.42.10/3559 to 153.72.42.74/787
flags SYN
106001: Inbound TCP connection denied from 153.72.42.10/3560 to 153.72.42.74/2407
flags SYN
106001: Inbound TCP connection denied from 153.72.42.10/3561 to 153.72.42.74/3505
flags SYN
…..
```

The UDP port scan:

```
# nmap -sU -p1-65535 153.72.42.74

Starting nmap V. 2.52 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host b2b.giac.com (153.72.42.74) appears to be up ... good.
Initiating FIN,NULL, UDP, or Xmas stealth scan against b2b.giac.com (153.72.42.74)
The UDP or stealth FIN/NULL/XMAS scan took 1021 seconds to scan 65534 ports.
(no udp responses received -- assuming all ports filtered)
All 65534 scanned ports on b2b.giac.com (153.72.42.74) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 1021 seconds
```

We see that all udp ports are filtered. This is what we expected. Again, the log from the Pix will show the results:

```
106006: Deny inbound UDP from 153.72.42.10/46953 to 153.72.42.74/787
106006: Deny inbound UDP from 153.72.42.10/46953 to 153.72.42.74/654
106006: Deny inbound UDP from 153.72.42.10/46953 to 153.72.42.74/129
106006: Deny inbound UDP from 153.72.42.10/46953 to 153.72.42.74/449
```

- telnet
  Telnet will be used to audit connectivity originating from the ENET and ANET systems. While logged on to each system, we will use telnet with a variety of ports to see the resulting behavior and watch the Pix and Gauntlet logs. While this does not provide as complete a check as nmap, it can be used to ensure the firewall is blocking inbound traffic.

  From each host on the ENET, we will attempt telnet to ports 20, 21,22,23, 25, 43, 53, 79, 80, 512, 513, 514, and 2049. We expect connection failure and firewall log results from each.

  Sample output from this activity is as follows:
  Telnet from b2b to in-b2b (ENET to ANET)

  ```
  #telnet 153.72.42.130 20
  Trying 147.145.42.130...
  telnet: Unable to connect to remote host: Connection timed out
  ```

  Pix logs show:

  ```
  106001: Inbound TCP connection denied from 153.72.42.74/2091 to 153.72.42.135/20
  flags SYN
  ```

This shows what we expected.

However, a telnet from in-b2b to b2b (ANET to ENET) showed ***access we did not expect.***

```
#telnet 153.72.42.74 23
Trying 147.145.42.74...
telnet: Unable to connect to remote host: Connection refused
```

Pix logs show:

```
302001: Built outbound TCP connection 1861 for faddr 153.72.42.74/23 gaddr
153.72.42.130/2356 laddr 153.72.42.130/2356
302001: Built outbound TCP connection 1862 for faddr 153.72.42.74/23 gaddr
153.72.42.130/2356 laddr 153.72.42.130/2356
302001: Built outbound TCP connection 1863 for faddr 153.72.42.74/23 gaddr
153.72.42.130/2356 laddr 153.72.42.130/2356
302001: Built outbound TCP connection 1864 for faddr 153.72.42.74/23 gaddr
153.72.42.130/2356 laddr 153.72.42.130/2356
```

It would seem our Pix rules is allowing outgoing from the in-b2b system not only to the internet, but also our own ENET. Access was denies only because there was not telnet listener running on the b2b system. This access needs to be tightened up.

- Netstat
  The netstat command will be used with the –a switch to audit exactly what services are listening on each host. We expect that the listening ports will match those that required access in the P&P documents.

  An example of the netstat output from our ex-dns server is:

```
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
```

  Here we see that the telnet, sunrpc, ftp and port 1080 are listening beyond the ssh(22) and domain(53) required by the P&P document. While the firewall is not open to allow access to these ports, the system should be reviewed to determine why these extra services are running.

4. Analysis and recommendations.

The overall design of the environment, based on the auditing activity above, provides a good level of defense for GIAC Enterprises. It has several key features built into it:

- Depth of defense implemented by multiple routers and multiple firewalls.
- Diversity of defense, implemented with two separate firewall products.
- Clear definitions of what is supported and allowed.
- Each segment have clearly defined roles and tasks.
- It provides a wide range of possible internet activities with expandability.

Some of the drawbacks are:

- It is complex. This can lead to mistakes.
- Network performance could be a problem for the ENET side.
- The use of 'split horizon' by the Altiga, while offering more security, will cause increased traffic over the boarder router.

We found some obvious problems that should be addressed.

- First, the firewall rule that allows tcp traffic out of the ANET system 153.72.42.130 should be amended to deny traffic to the ENET systems.
- Second, the hosts on each segment need to be reviewed for hardening. The ex-dns system on the ENET had several unnecessary listeners running.

Some other recommendations are:

- Instead of having the mail server act as a POP client for all internal users, build up an internal POP mail server. We can leverage the smap facility on the Gauntlet to pass mail messages to/from the internal and external mail servers. This will eliminate the potential security issue of running POP on the ENET server, as well as cut down on the traffic flowing through both the Gauntlet and the Pix.
- Instead of allowing internal administrative users to ssh and ftp 'through' the Gaunlet, we should enable authorization on the Gauntlet, forcing them to stop there and then be passed on. This provides an additional level of access security to these systems.
- A console server of some type should be included to allow console access to each of the systems. This would make remote management possible, as well as provide a way in should an erroneous firewall rule be introduced or should one of the firewalls go down.