Global Information Assurance Certification Paper

Chris Stevenson
GIAC Firewall and Perimeter Protection
Practical Assignment

Assignment 1 – Egress Filter

Introduction:
All too often the focus of our network defense is outward and we forget about the possibility of an attack originating from within via a compromised machine or a dishonest employee. However, these instances can lead to a great deal of embarrassment for our companies and, in the interest of being good internet neighbors, we should try to deter them. Egress filtering, the process of filtering outbound packets on the network, is a good place to start.

The main advantage of egress filtering is that IP spoofing attacks cannot originate from your network. Smurf and other DoS attacks rely on an attacker sending packets with spoofed source IP addresses. If these packets originate from within your network, but have an external source IP, they will be dropped before they exit your network.

There are few disadvantages to egress filtering. It requires that the network analyst remember that it is there to avoid possible conflicts with other filters. The additional filter and logging may cause a slight performance hit, but it should be minimal.

The Filter:
A simple filter to apply to a Cisco router on a class C network could be defined as follows:

```
access-list 11 permit ip 204.166.62.0 0.0.0.255 any
access-list 11 deny ip any any log
```

In this case we are telling our access-list '11' to let any address from our class C address space (204.166.62.0) out to any external IP address. Packets which fail this test are judged at the second line which will deny packets from any other address and log the incident.

The following commands entered in global configuration mode should apply this filter to your interface (eth0 here):

```
access-list 11 permit ip 204.166.62.0 0.0.0.255 any
access-list 11 deny ip any any log
interface eth0
ip access-group 11 in
```

Testing the filter:
It's a good idea to test the filter to make sure that it is working correctly. First test outgoing packets from your network by using ssh or a web browser to attempt to access an external site. If that works try to spoof another source IP by changing the IP address of a computer in your network and attempt to leave. If your packets are dropped, be sure to check the router logs to be certain that it was your router that blocked your packets. Another method would be to employ a custom designed packet with a bad source IP.

Assignment 2: Firewall Policy Violations

Please Note: I've replaced the hostname of my firewall with 'fwhost' and its IP address with X.X.X.X. I've also replaced the source IP addresses with Y.Y.Y.Y.

Detect #1

Jun 7 11:53:55 fwhost kernel: Packet log: input DENY eth0 PROTO=6 Y.Y.Y.Y:1657 X.X.X.X:23 L=60 S=0x10 I=44861 F=0x4000 T=64 SYN (#8)

Key:

Field	**Description**
Jun 7 11:53:55	Date and Time
fwhost	Firewall hostname
kernel: Packet log	Log facility generating the message
input	Firewall chain to which the rule is applied
DENY	Action taken
eth0	Network interface involved
PROTO=6	Protocol type (TCP)
Y.Y.Y.Y	Source IP address
1657	Source port (unprivileged)
X.X.X.X	Destination IP (firewall)
23	Destination port (Telnet)
L=60	Packet length
S=0x10	Type of service
I=44861	Datagram ID
F=0x4000	Fragment byte offset
T=64	TTL
SYN	This is a SYN packet
(#8)	Firewall rule that caught this packet

This was a telnet attempt that was picked by the following rule, which denies and logs incoming tcp packets destined for port 23:

Target	Protocol	Source	Destination	Ports
DENY	tcp	anywhere	fwhost	1024:65535 -> telnet

Potential damage:
Allowing the telnet protocol would allow clear text ASCII communication to travel on our network, which could result in passwords being compromised. We require ssh instead.

Detect #2

Jun 7 15:16:55 fwhost kernel: Packet log: input REJECT eth0 PROTO=6 Y.Y.Y.Y:1663 X.X.X.X:79 L=60 S=0x00 I=45418 F=0x4000 T=64 SYN (#20)

Key:

Field	**Description**
Jun 7 15:16:55	Date and Time
fwhost	Firewall hostname
kernel: Packet log	Log facility generating the message
input	Firewall chain to which the rule is applied
REJECT	Action taken
eth0	Network interface involved
PROTO=6	Protocol type (TCP)
Y.Y.Y.Y	Source IP address
1663	Source port (unprivileged)
X.X.X.X	Destination IP (firewall)
79	Destination port (finger)
L=60	Packet length
S=0x00	Type of service
I=45418	Datagram ID
F=0x4000	Fragment byte offset
T=64	TTL
SYN	This is a SYN packet
(#20)	Firewall rule that caught this packet

This finger attempt was detected and logged by a rule which rejects and logs incoming tcp packets bound for port 79:

Target	Protocol	Source	Destination	Ports
REJECT	tcp	anywhere	fwhost	1024:65535 -> finger

Potential damage:
We don't allow finger because it allows potential hackers to view accounts and usernames on our machines. Disabling it makes it more difficult to find users who may have easy to guess passwords.

Detect #3

Jun 7 15:17:48 fwhost kernel: Packet log: input REJECT eth0 PROTO=6 Y.Y.Y.Y:1666 X.X.X.X:21 L=60 S=0x00 I=45424 F=0x4000 T=64 SYN (#12)

Key:

Field	**Description**
Jun 7 15:17:48	Date and Time
fwhost	Firewall hostname
kernel: Packet log	Log facility generating the message
input	Firewall chain to which the rule is applied
REJECT	Action taken
eth0	Network interface involved
PROTO=6	Protocol type (TCP)
Y.Y.Y.Y	Source IP address
1666	Source port (unprivileged)
X.X.X.X	Destination IP (firewall)
21	Destination port (FTP)
L=60	Packet length
S=0x00	Type of service
I=45424	Datagram ID
F=0x4000	Fragment byte offset
T=64	TTL
SYN	This is a SYN packet
(#12)	Firewall rule that caught this packet

This ftp attempt was detected and logged by a rule which rejects incoming tcp packets heading for port 21:

Target	Protocol	Source	Destination	Ports
REJECT	tcp	anywhere	fwhost	1024:65535 -> ftp

Potential damage:
There are many documented ftp exploits. The protocol also transmits information in clear text, increasing the possibility of password sniffing.

Detect #4

Jun 7 14:52:11 fwhost kernel: Packet log: input DENY eth0 PROTO=1 Y.Y.Y.Y:8 X.X.X.X:0 L=60 S=0x00 I=31866 F=0x0000 T=128 (#14)

Key:

Field	**Description**
Jun 7 14:52:11	Date and Time
fwhost	Firewall hostname
kernel: Packet log	Log facility generating the message
input	Firewall chain to which the rule is applied
DENY	Action taken
eth0	Network interface involved
PROTO=1	Protocol type (ICMP)
Y.Y.Y.Y	Source IP address
8	Source port (echo request)
X.X.X.X	Destination IP (firewall)
0	Destination port (echo response)
L=60	Packet length
S=0x00	Type of service
I=31866	Datagram ID
F=0x0000	Fragment byte offset
T=128	TTL
(#14)	Firewall rule that caught this packet

This was a ping that was detected by a rule designed to deny and log icmp echo requests:

Target	Protocol	Source	Destination	Ports
DENY	icmp	anywhere	fwhost	echo-request

Potential Damage:
Ping attacks can be used to map network address space. With this information, a potential hacker can learn which IP addresses are used by potential targets.

Detect #5

Jun 7 14:13:01 fwhost kernel: Packet log: input DENY eth0 PROTO=17 X.X.X.X:137 X.X.X.255:137 L=96 S=0x00 I=31463 F=0x0000 T=128 (#2)

Key:

Field	**Description**
Jun 7 14:13:01	Date and Time
fwhost	Firewall hostname
kernel: Packet log	Log facility generating the message
input	Firewall chain to which the rule is applied
DENY	Action taken
eth0	Network interface involved
PROTO=17	Protocol type (UDP)
X.X.X.X	Source IP address (firewall)
137	Source port (netbios naming service)
X.X.X.255	Destination IP (domain broadcast)
137	Destination port (netbios naming service)
L=96	Packet length
S=0x00	Type of service
I=31463	Datagram ID
F=0x0000	Fragment byte offset
T=128	TTL
SYN	This is a SYN packet
(#2)	Firewall rule that caught this packet

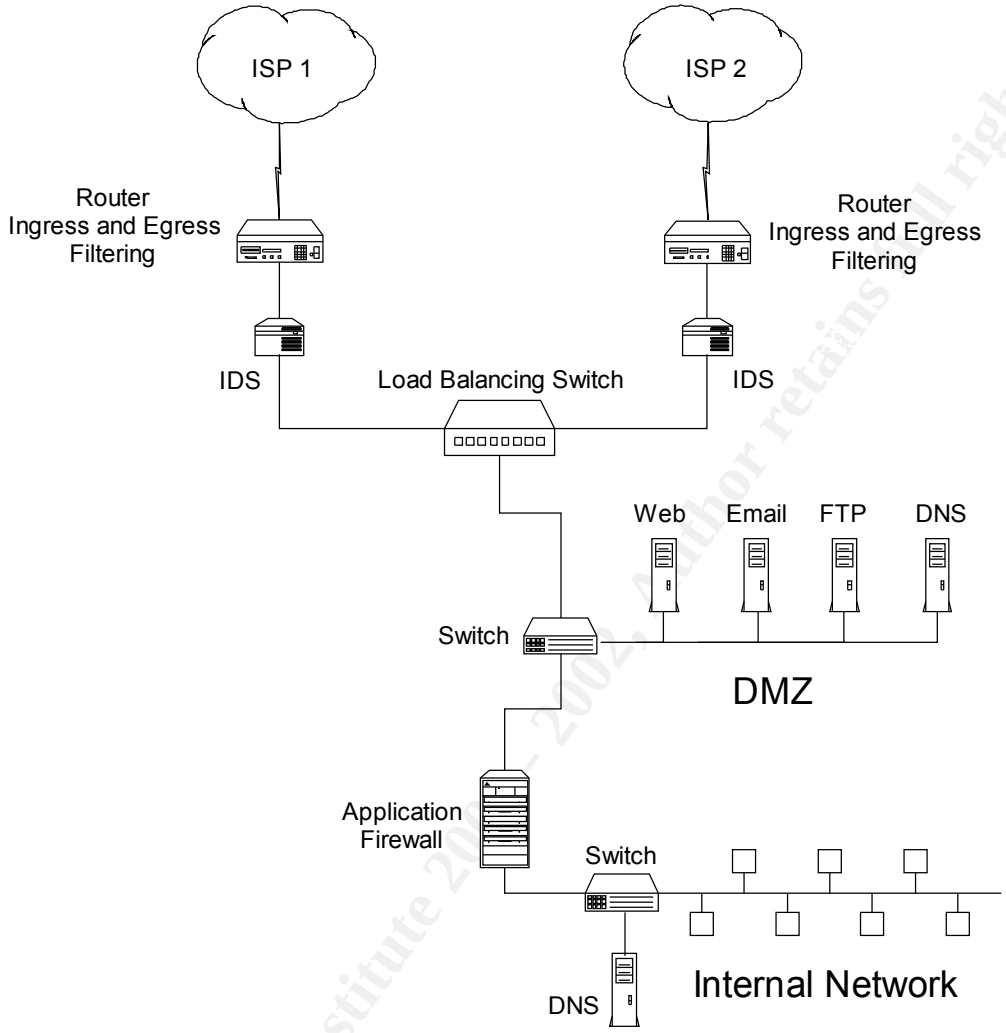
This is a Windows netbios name service broadcast that was picked out and logged by a rule that denies and logs all incoming packets from the firewall's IP address:

Target	Protocol	Source	Destination	Ports
DENY	all	fwhost	anywhere	n/a

Potential damage:
This one is a Windows NetBIOS broadcast reportedly coming in from the same IP address as my *linux* firewall. Someone was apparently attempting to spoof the IP address of the firewall. If a hacker is able to successfully spoof an address in your local domain space, they can potentially gain access to resources that should not available to those outside your local network. An attacker may also spoof an IP address as a prelude to a DoS.

Assignment 3 – Defense in Depth Architecture

Part 1 – Site with two internet connections that is resistant to DoS attacks



Description:

Routers: Both gateway routers are configured with ingress filtering against ICMP packets and proper egress filtering to block IP spoofing attacks originating from within the network. This combination should make the network more resistant to DoS attacks.

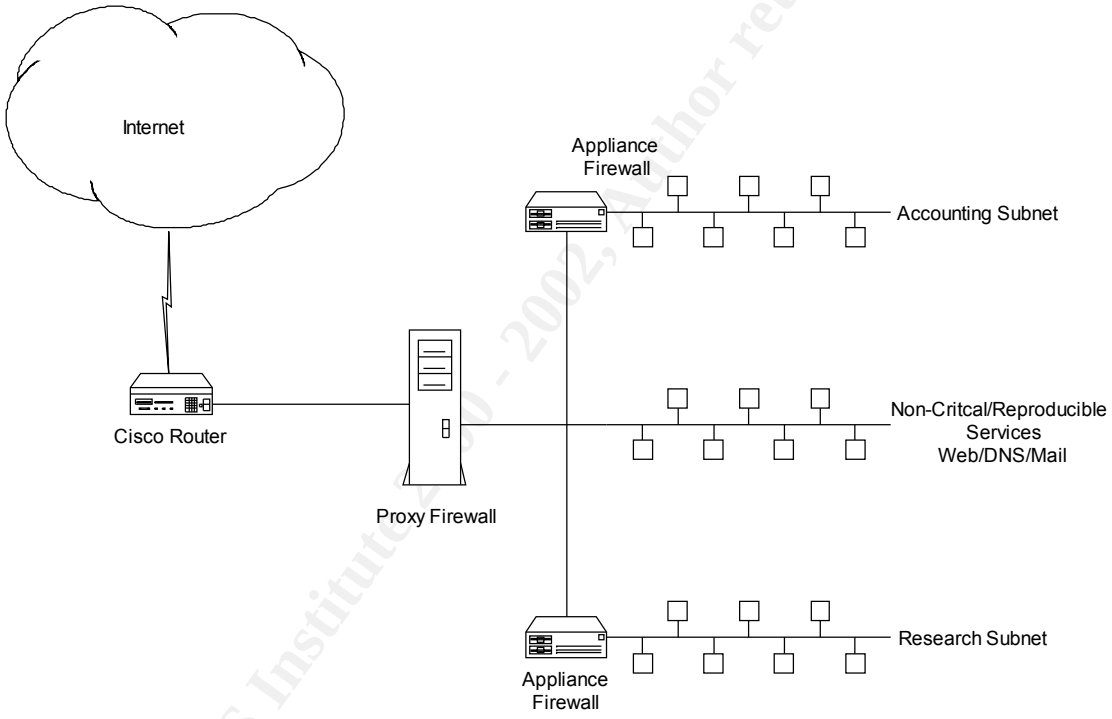
IDS: Two intrusion detection systems such as Network Flight Recorder both log access to the network. Alternatively, these could be firewalls with a small rule set; designed to filter out more unwanted traffic from the DMZ.

Application Firewall: This firewall could be a Checkpoint, a Gauntlet, or another highly secure, stateful system. It would be configured to allow users on the internal network access to the internet and all services except DNS on the DMZ, but would drop packets with bad source IP addresses. All traffic from the DMZ that is not a response to a request from the internal network would be dropped as well as all ICMP traffic.

Split DNS: I have employed a split DNS model in this design. If an intruder is able to access the DNS server in the DMZ, he or she will only gain information about the other servers in the DMZ. The DNS on the internal network contains information about the internal network and the machines in the DMZ, but zone transfers are not allowed through the firewall.

Switching: Both the DMZ and the internal network are switched subnets. In addition, a load-balancing switch is employed to regulate traffic to the two routers.

Part 2 – Site with two critical sub-networks and pre-purchased hardware



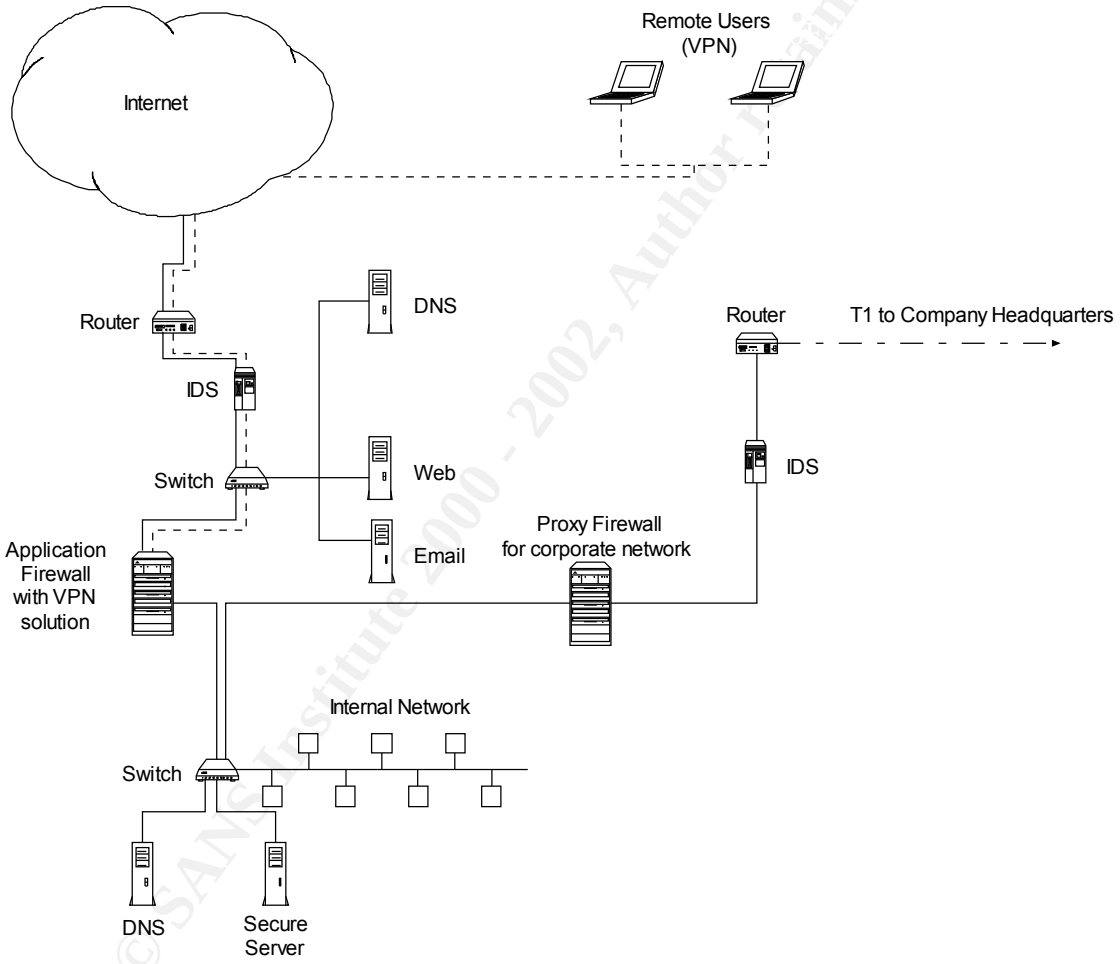
In this case, the Cisco router should perform ingress and egress filtering and the proxy firewall should filter and log packets according to the company's general network security policy.

Appliance firewalls separate the critical Accounting and Research sub-networks. For maximum protection, they should be configured to deny all packets originating from outside their networks except replies from requests for email, DNS, and web services. All three internal subnets should be switched.

Assignment 4 – Create a test that demonstrates knowledge of subject

Your company would like to open a new satellite sales office in another city. This office will have an internet connection for its employees and a leased T1 line back to company headquarters for access to the corporate intranet. You will be hosting a small sales website and email services. The salespeople in your office travel often and will need access to recent updates to the confidential information stored on a server at your site.

Submit a design for this site that will allow the salespeople access to the information they need, but will make your company's information as secure as possible.



Description:
Routers: Both routers are configured with ingress filtering against ICMP packets and proper egress filtering to block IP spoofing attacks originating from within the network. This combination should make the network more resistant to DoS attacks. It is important to remember to properly filter the router to the company intranet to prevent any attacks originating on your network from getting to the main corporate site and to block attacks originating from headquarters.

IDS: Two intrusion detection systems monitor and log access to the network from both the internet, and the company headquarters.

Firewalls: The application firewall is equipped with a VPN solution (the Checkpoint VPN-1 Gateway is one such solution). This provides protection from internet hackers and from machines using your VPN. It is important to filter the traffic from the remote users because their machines can be compromised while away from your internal network.

This firewall is configured to allow users on the internal network access to the internet and services on the DMZ, but it drops packets with bad source IP addresses. All traffic from the DMZ that is not a response to a request from the internal network is dropped as well as all ICMP traffic. After authentication, VPN users are allowed access to the secure server and services in the DMZ.

The proxy firewall is configured to allow local users to access to the intranet at company headquarters, but treats the intranet like a DMZ. Users at corporate headquarters do not have access to services on the local network via the leased line and DNS zone transfers from the intranet are blocked.

Split DNS: DNS is split in this design. The server in the DMZ only contains information about the machines in the DMZ. The internal DNS contains information about computers in the DMZ, all of the computers on the internal network including the secure server, and the proxy firewall. Zone transfers from the internal DNS must be blocked at both firewalls.

The really important thing to remember in this exercise is that you have to protect yourself from your company's main network and your traveling salespeople. If a computer isn't on your local network, you don't really know who is using it or who may have compromised it.