Global Information Assurance Certification Paper

David L. Johnson

Assignment 1: Egress Filtering

Egress filtering has been demonstrated as an effective tool to reduce the possibility of your local network entities being used to support a distributed denial of service (DDoS) attack against a third party. To understand how egress filtering works, it is important to understand the methods used in creating these attacks.

A typical DDoS attack takes the following form. A hacker breaks into several remote systems located on various networks. A client program, which has the ability to generate packets with spoofed IP source addresses, is loaded onto these systems. At some point in time, when the attacker is ready, these client systems are directed by the attacker to send packets to the network entity that he wishes to deny access to. The volume of packets sent to the attacked system prevents legitimate users of the system from gaining access.

The use of spoofed packets makes this sort of attack difficult to trace back to its source. Since the actual source address of the packets has been replaced by another address, tracing has to be done one hop at a time and can only be followed back to the source if the attack continues until the trace is complete. It can also require the cooperation of multiple ISPs, which can be difficult to get. This is where the use of egress filtering can be extremely helpful.

Egress filtering is accomplished by issuing commands to your border router, causing it to drop packets containing IP source addresses that did not originate on your local network. This forces an attacker to use a valid IP address on your local system to generate his attack, making the attack much easier to trace. If we assume a local Class C network address of 207.10.10.0 with interface Ethernet 0 attached to the local network, the commands needed to accomplish this on a Cisco router would be as follows:

```
ROUTER>enable
PASSWORD? ******
ROUTER#config t
ROUTER(config)#access-list 101 permit ip 207.10.10.0 0.0.0.255 any
ROUTER(config)#int e0
ROUTER(config-if)#ip access-group 101 in
```

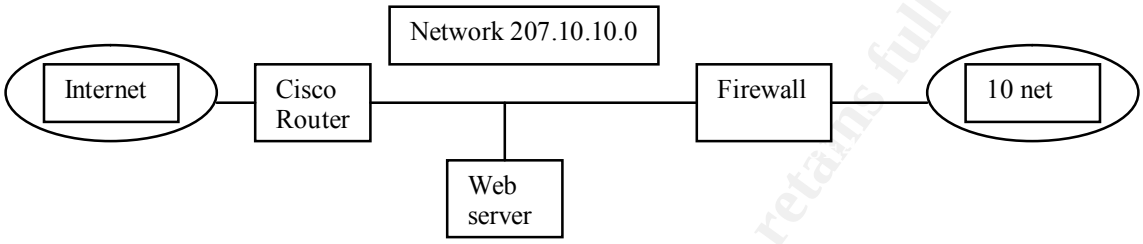
By permitting only the legitimate IP addresses of the local network to enter the router, all other IP source addresses are blocked by the implicit deny rule. The above commands cause the router to drop spoofed packets as they enter the Ethernet interface. The enable command causes the router to ask for the password. Once the correct password is supplied, the config t command is issued to place the router in configuration mode and tells it to accept configuration commands from the terminal. This mode allows the creation of the access list. When the access list is complete, issuing the int e0 command puts the router in config interface mode. The access-group command applies the previously created access list to the Ethernet 0 interface and specifies the in bound direction.

A test should be run to verify that the system is functioning properly. Setup logging on the router's internal Ethernet interface. Use a packet generator to create packets with spoofed IP addresses and direct them through the router. Review the log files for evidence that the packets are being dropped.

Assignment 2: Firewall Policy Violations

Violation 1:

The network I am responsible for consists of one Class C address block attached to the Texas Higher Education Network (THEnet). THEnet provides connectivity and Internet access for a group of state university systems as well as local school districts and state, city and county government agencies. Our local network uses an Axent Raptor Firewall, version 6.0, running on a Windows NT 4.0 server. This is a dual-homed system, which uses NAT to connect a 10 net unregistered network to a DMZ located on a registered Class C network.



A typical rules violation would appear in the log as follows:

Date/Time	Daemon [id]	Message	IP Source/Dest	Protocol	Port S->D
Apr 05 00:44:59.00	firelogd[112]	Possible Port Scan detected on Interface 207.10.10.100	(10.12.26.88->207.10.10.100)	UDP	137->137
Apr 05 00:45:00.00	firelogd[112]	Possible Port Scan detected on Interface 207.10.10.100	(172.16.3.10->207.10.10.100)	UDP	137->137
Apr 05 00:45:00.00	firelogd[112]	Possible Port Scan detected on Interface 207.10.10.100	(207.87.26.43->207.10.10.100)	UDP	137->137

The information recorded is date and time, the daemon that inserted the message in the log, the message itself, IP source and destination addresses, the protocol, and the source and destination ports. In the above messages, several interesting points can be observed. The IP source addresses of the first two entries show private, unregistered network numbers. This indicates that the origins of the packets are most likely within the same ISP as my network. I make this assumption because Internet backbone routers would have dropped the packets. The third entry contains a source address indicating an origin at Digex.net which is a business oriented ISP.

These packets were refused because of the firewall configuration. No specific rule was involved because UDP traffic is denied by default. The basic setup of the Raptor firewall shuts down all traffic through the system. Rules are then created to allow specific protocols to either be passed transparently or redirected to specific IP addresses. A typical scenario involves SMTP. The outside interface of the firewall is listed in the DNS as the email server for the domain. External mail servers deliver mail to the firewall interface, which proxies the mail to the actual server located behind the firewall.

The intent of these packets is unknown. Windows NT uses UDP on port 137 for browsing, printing, logon, domain trusts, and pass through validation. The sources of these packets could be legitimate NT servers on remote networks, which are attempting to locate network resources. They could also be hacking attempts trying to locate vulnerable servers. However, the Windows NT event logs do not show any unsuccessful login attempts, so I suspect they are actually benign.

Similar log entries were found with many different source IP addresses. Because of the difficulty involved in tracing scans like these to their source, I chose to implement packet filtering on the border router to block access at that point and to provide a defense-in-depth. The first step was to decide the configuration of the filter. I chose to block unregistered addresses from entering the network and to block access to the commonly used NetBIOS ports of 135, 137, 138, and 139.

```
access-list 111 deny   ip 192.168.0.0 0.0.255.255 any
access-list 111 deny   ip 172.16.0.0 0.15.255.255 any
access-list 111 deny   ip 10.0.0.0 0.255.255.255 any
access-list 111 deny   ip 127.0.0.0 0.255.255.255 any
access-list 111 deny   tcp any any eq 135
access-list 111 deny   tcp any any eq 137
access-list 111 deny   tcp any any eq 138
access-list 111 deny   tcp any any eq 139
access-list 111 deny   udp any any eq 135
access-list 111 deny   udp any any eq netbios-ns
access-list 111 deny   udp any any eq netbios-dgm
access-list 111 deny   udp any any eq 139
access-list 111 permit ip any any
```

These commands were applied to the serial port of the router in the inbound direction. To reduce the possibility of IP address spoofing, I also blocked IP source routing.

```
no ip source-route
```

Violation 2:

A different type of warning message was found in the logs indicating unusual activity on the internal interface of the firewall directed to the Internet

Date/Time	Daemon [id]	Message	IP Source/Dest	Protocol	Port S->D
Apr 25 07:36:00	firelogd[104]	IP packet dropped: Restricted Port	(10.5.151.15->195.40.6.1	TCP[SYN]	1037 ->6667
Apr 25 07:36:59	firelogd[104]	IP packet dropped: Restricted Port	(10.5.151.15->195.40.6.1	TCP[SYN]	1054 ->6667
Apr 25 07:37:29	firelogd[104]	IP packet dropped: Restricted Port	(10.5.151.15->195.40.6.1	TCP[SYN]	1067 ->6667

Packets matching this pattern began appearing at an alarming rate. Computers on our private network were attempting to reach port 6667, Internet Relay Chat (IRC), at various IP addresses. This was despite the fact that no chat software was installed on any system. The firewall dropped the packets due to the implicit deny all rule as there was no specific rule allowing access to port 6667.

Computers would attempt to attach to port 6667. Since the packets were dropped without reply, the originating port would wait to time out. The computer would move up to the next available local port and try again. This pattern was replicated over and over to the point that the firewall was starting to bog down under the load. A group of six Windows 95 computers were generating enough of these packets to cause all other computers on the network to feel the effects of reduced availability of network resources.

Because many worms and viruses use IRC to either spread or send data about infected machines, I immediately checked to see that the anti-virus packages on the affected systems were operating. All had McAfee Virus Shield installed and functioning. All of the virus signature files had been updated recently. The newest signature file was 5 days old and the oldest was two weeks. All of the machines were updated with the latest available signature file and rescanned but McAfee found no infections. McAfee was removed from one of the computers and replaced by Norton Anti-virus. The system was rescanned but still nothing was found. The next step taken was to shut down background processes running on the machines and observe the effects. No relief to the network traffic congestion was noted.

A comparison was made between these systems and a similar machine that was not contributing to the problem. The only thing different on these six machines compared to others on the network was a free software application named Webshots. Webshots is a program used to automatically change the Windows desktop background. This program had been downloaded off of the Internet and installed by this group of

users. Shutting down the operation of Webshots had no effect on the network traffic, nor did removing it completely from the affected computers. The packets continued to pour out onto the network.

More research was conducted into the problem. A packet sniffer was used to examine a sampling of the packets. Data contained in several of these packets contained the names adsoftware.com and aureate.com. Upon researching these names, the following web site was located: http://grc.com/optout.htm.

Steve Gibson has created this site to inform people about a problem that has been termed "Spyware." Details can be located on the web site but at its most basic level, spyware is attached to distributions of freeware and shareware to report back to the author or advertiser information about the users of the product. Mr. Gibson distributes a free program, called Optout, which will locate and remove spyware software. Optout was run on each of the six affected machines. It located spyware from a company named Aureate on each of them. Optout was allowed to remove all instances of the spyware and network traffic returned to normal.

This situation was strange in that the firewall behavior actually contributed to the network traffic congestion. If port 6667 had been open, the computers would have successfully transmitted their data to the IRC server and only a minimal amount of traffic would have been generated. With port 6667 closed, potentially damaging personal data was prevented from being distributed but availability of network resources was impacted.

Violation 3:

The following log entries were generated intentionally by attacking the external firewall interface.

Date/Time	Daemon [id]	Message	IP Source/Dest	Protocol	Port S->D
Jun 07 13:51:25	firelogd[105]	Possible Port Scan detected on Interface 207.10.10.100	(207.10.10.1->207.10.10.100	UDP	137 ->137
Jun 07 13:51:27	firelogd[105]	Possible Port Scan detected on Interface 207.10.10.100	(207.10.10.1->207.10.10.100	UDP	137 ->137
Jun 07 13:51:28	firelogd[105]	Possible Port Scan detected on Interface 207.10.10.100	(207.10.10.1->207.10.10.100	UDP	137 ->137

Using the Windows NT "net use" command, I attempted to attach to a nonexistent network share on the firewall:

```
NET USE R: \\FIREWALL\SHARE
```

I issued the above command from a computer on the same network as the firewall while monitoring the firewall logs. This command simulates the actions of several viruses now in the wild, which attempt to exploit unprotected network shares on Windows systems. All file sharing is disabled by default on the Axent Raptor Firewall for NT. Access to port 137 is also disabled by default. If file sharing was not disabled and such a share had actually existed a hacker could gain access to any information located there.

Violation 4:

The following log entries were generated intentionally by attacking the external firewall interface.

Date/Time	Daemon [id]	Message	IP Source/Dest	Protocol	Port S->D
Jun 07 14:07:20	firelogd[105]	IP packet dropped Restricted Port	(207.10.10.1->207.10.10.100	TCP[SYN]	1180->81
Jun 07 14:07:22	firelogd[105]	IP packet dropped Restricted Port	(207.10.10.1->207.10.10.100	TCP[SYN]	1180->82
Jun 07 14:07:24	firelogd[105]	IP packet dropped Restricted Port	(207.10.10.1->207.10.10.100	TCP[SYN]	1180->83

Using a browser I attempted to attach to a nonexistent web server on ports 81 through 83. I issued the command from a computer on the same network as the firewall while monitoring the firewall logs. This allowed me to simulate a TCP port scan, using the browser to vary the destination port. The firewall immediately detected the probe and logged it as an attempt to connect to a restricted port. All access to protected areas is disabled by default in the Raptor setup. A transparent proxy is used to redirect HTTP services to a destination defined by rule. In our particular situation, a rule has been set up to allow HTTP connections to port 80 to be redirected to an intranet server located on the private network. User accounts with valid passwords must exist on the server to obtain access. Connections to any port not specifically defined and permitted are dropped and logged by the firewall.

Violation 5:

The following log entries were generated intentionally by attacking the external firewall interface.

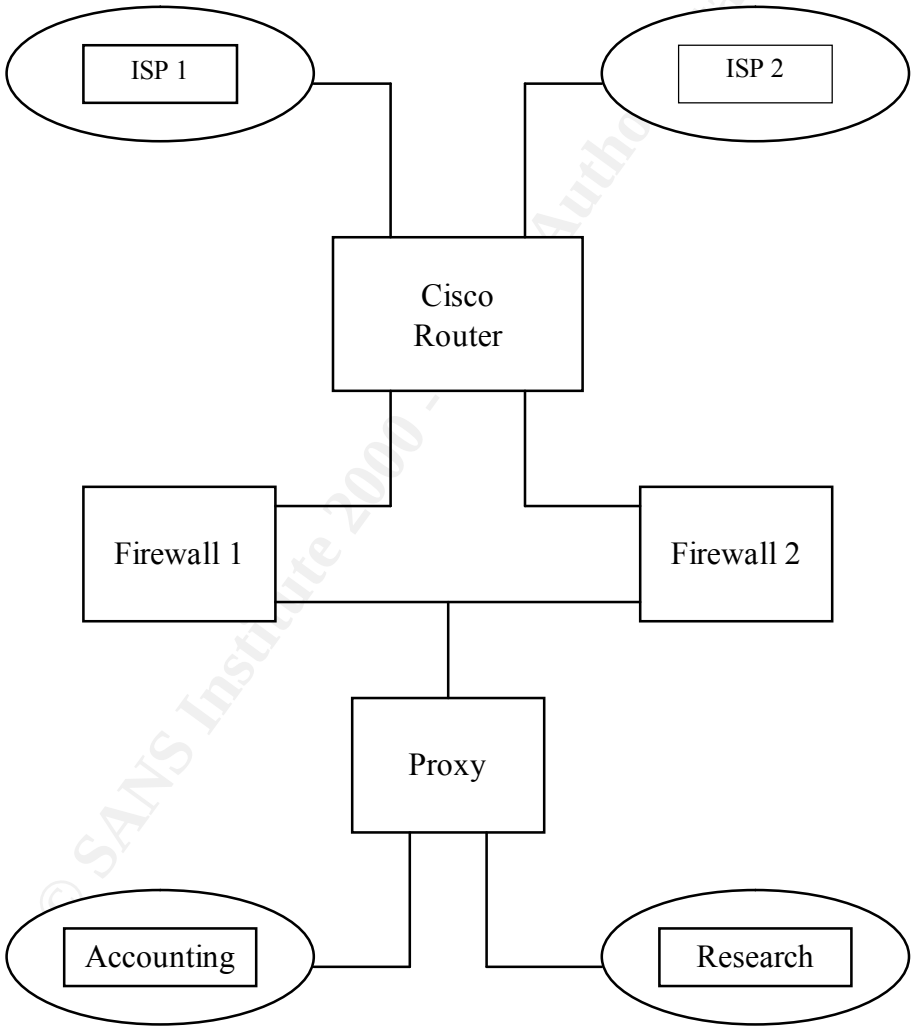
Date/Time	Daemon [id]	Message	IP Source/Dest	Protocol	Port S->D
Jun 07 14:10:13	firelogd[105]	IP packet dropped Restricted Port	(207.10.10.1->207.10.10.100	TCP[SYN]	1184->21
Jun 07 14:10:14	firelogd[105]	Possible Port Scan detected on Interface 207.10.10.100	(207.10.10.1->207.10.10.100	TCP[SYN]	1184->21

Again, using a browser, I attempted to attach to an FTP server on port 21. I issued the command from a computer on the same network as the firewall while monitoring the firewall logs. No FTP proxy has been defined on this firewall. The firewall immediately detected the probe and logged it as an attempt to connect to a restricted port and as a possible port scan. Connections to any port not specifically defined and permitted are dropped and logged by the firewall.

Assignment 3 - Defense in Depth Architecture

The scenario describes a requirement for a network with dual Internet connection that is optimized for resistance to DDoS attack. The following equipment is available for use in designing the network architecture: One Cisco router, one proxy firewall, and two appliance type firewalls with two 10/100 NIC's, capable of performing bridging.

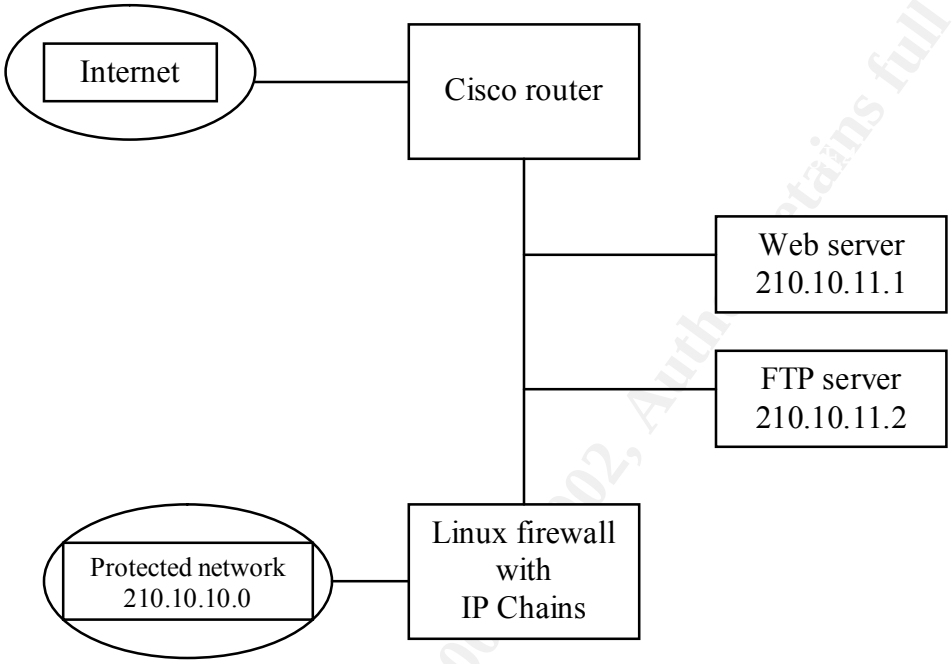
Use a Cisco router with two serial and two Ethernet interfaces to connect to the ISPs. The appliance firewalls then are connected to the Ethernet ports on the router. The remaining Ethernet ports on the appliance firewalls are bridged together and are connected to the proxy firewall. The accounting and research subnets are then attached to separate interfaces on the proxy. The bridge functions of the appliance firewalls allow traffic to be redirected to either ISP in case of a DDoS attack. The proxy separates the two departments, protecting them from each other. Defense in depth is achieved through packet filtering on the Cisco router and the multi-layer effect of the appliance and proxy firewalls.



Assignment 4 - Create a Test

You are responsible for security of the network shown in Diagram A. Analyze and describe the setup and make two recommendations for improving security without major budget expenditures. Include a diagram of the network showing the proposed changes.

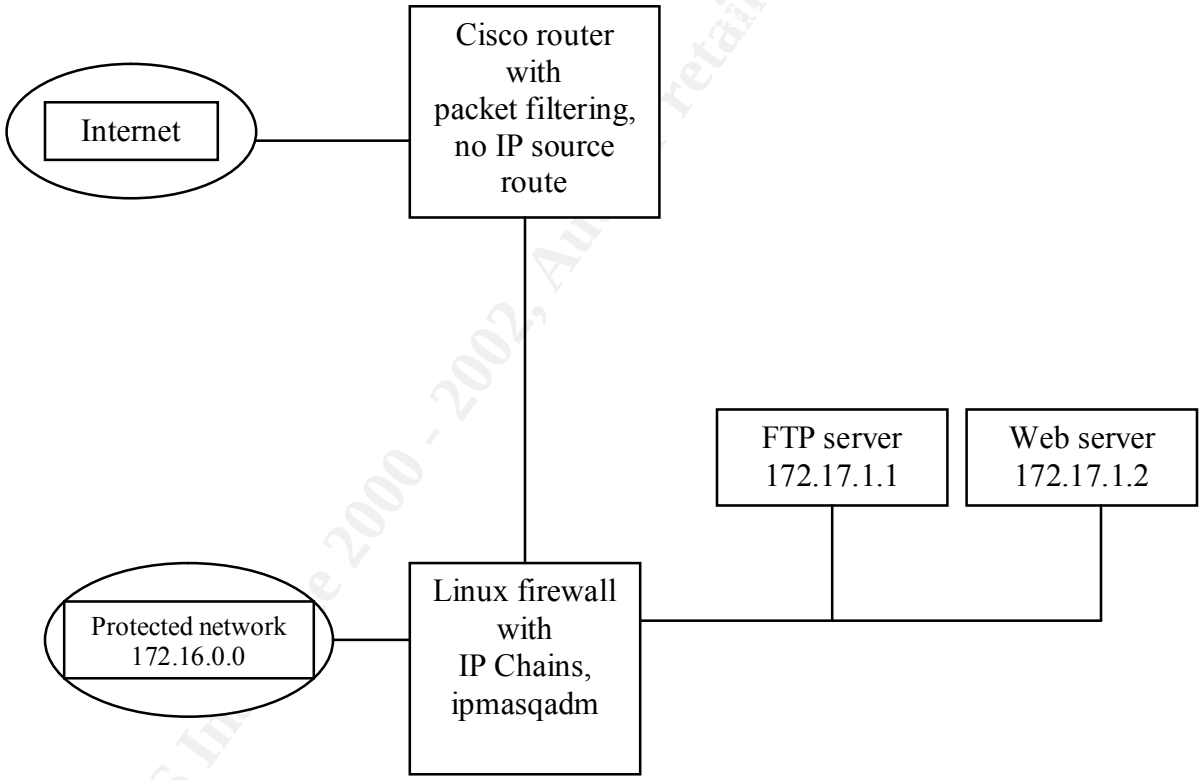
Diagram A



Solution:

The network in Diagram A consists of two registered Class C IP address blocks joined by a Linux firewall running IP Chains. A web server and an ftp server are located in the unprotected DMZ area. Only machines located on the 210.10.10.0 network are protected by the firewall. Many different solutions could be proposed to provide better security at minimum expense.

1. Enable IP Masquerade on the protected network to hide addresses of individual machines.
2. Use private addressing on the protected network.
3. Create a screened subnet off of the firewall and relocate the web and FTP servers there.
4. Enable packet filtering on the router.
5. Block IP source routed packets at the router.



Test Questions

Section 3.1

1) NetBIOS uses which common ports?
   a) 80, 443, 8080
   b) 21,22
   c) 135, 137, 138, 139
   d) any available port over 1024

2) To request establishment of a tcp connection, a computer sends a
   a) SYN packet
   b) ACK packet
   c) REQ packet
   d) None of the above

3) Well known ports are
   a) Numbered between 1 and 1023
   b) Remain constant on the host on which they are offered
   c) Identified with specific services
   d) All of the above

4) Packet fragmentation occurs when
   a) Packets collide on a network
   b) Too many users request the same service
   c) The MTU of a network segment is smaller that the size of the datagram
   d) Connecting private address blocks to registered address blocks

5) T/F Fragmentation can be used in DDoS attacks.

6) DNS zone transfers
   a) Can be used by an attacker to gather information about the hosts on your network.
   b) Should be restricted to authorized systems only
   c) Take place on port 53 using tcp
   d) All of the above

7) ICMP
   a) Uses port numbers like all protocols
   b) Provides reliable delivery of data
   c) Requires an exclusive client/server relationship
   d) Is used to communicate error conditions.

8) T/F DNS responses always use UDP.

9) Distance vector routing protocols include
   a) RIP, IGRP, and EIGRP
   b) RIP, GRIP, and RGRP
   c) IGRP, UGRP, WEGRP
   d) None of the above

10) The tribe flood network attack is an example of
   a) A distributed denial of service attack
   b) An Internet worm
   c) A self replicating virus
   d) None of the above

Section 3.2

1) Firewalls are
   a) Hardware devices
   b) Software only
   c) a & b
   d) none of the above

2) Packet filters
   a) Are low end firewalls
   b) Can enhance security
   c) Are very fast
   d) All of the above

3) The acronym NAT stands for
   a) Novell administration technology
   b) Network address translation
   c) Network address transfer
   d) Normal address translation

4) Packet filters and firewalls are
   a) Perimeter security devices
   b) Only useful on intranets
   c) Mandated by InterNIC
   d) Not important with current technology

5) Firewalls
   a) Can be a challenge to a hacker
   b) Provide a measure of protection for all protected hosts
   c) Should be employed with other security mechanisms
   d) All of the above

6) T/F A security policy should be developed before a firewall is selected.

7) Egress filtering
   a) Prevents outbound spoofing
   b) cannot help you detect an intrusion
   c) is usually implemented outbound on the router serial interface
   d) can only be implemented on Cisco routers

8) Routers can filter network traffic based on
   a) Protocol and port
   b) Source and destination
   c) Inbound and outbound
   d) All of the above

9) IPCHAINS rule types include
   a) Accept, deny, refuse
   b) Accept, deny, reject
   c) Accept, reject, hide
   d) Accept, redirect, refuse

10) T/F Firewalls are used to create security policy.

Section 3.3:

1) T/F Cisco routers use acceptance control lists to create packet filter rules.

2) Cisco IP access list types include
   a) Default, custom, and stateful
   b) Standard, enhanced, and receptive
   c) Standard, extended, and reflexive
   d) Stateful, enhanced, and reflexive

3) Which of the following is a valid ACL entry?
   a) Access-list 11 permit any any
   b) Access-group 11 permit any any
   c) Access-list 11 any any permit in
   d) Access-list 11 permit host 192.168.1.100 in

4) A standard Cisco access list has an identification number
   a) Between 1 and 49
   b) Between 1 and 100
   c) Between 1 and 99
   d) Between 0 and 99

5) 5) An extended Cisco access list has an identification number
   a) Between 100 and 200
   b) Between 100 and 150
   c) Between 0 and 99
   d) Between 100 and 199

6) T/F Reflexive ACLs use a state table to keep track of where traffic is going.

7) Cisco access lists can
   a) Filter traffic
   b) Restrict access to router services such as telnet
   c) Restrict which routes are sent and accepted
   d) All of the above

8) Firewalls can be used to control traffic between
   a) A DMZ and a trusted network
   b) A screened network and a trusted network
   c) Internal department networks
   d) All of the above

9) T/F Implementing a split DNS involves creating an external DNS server for requests from the Internet and an internal DNS server for use by systems behind the firewall.

10) T/F Nslookup, Dig, and Sam Spade are all tools that can be used to test a DNS setup.