Stallings and Brown Chapter 9 Review Questions:

Review Question 9.11: What is a DMZ network and what types of systems would you expect to find on such networks?

DMZ is a computer network or a host that is in between the external and internal firewall. It prevents the direct access from external users to server. The types of systems are Corporate Websites, Email Servers, and Domain Name System Servers.

(Page 301)

Review Question 9.13: How does an ISP differ from a firewall?

IPS is capable of detecting or blocking the traffic by discarding the packet. It also monitors the ports and sends commands to firewall to stop the traffic. It also adds IDS to block the traffic.

Stallings and Brown Chapter 9 Problems:

Problem 9.1: As was mentioned in Section 9.3, one approach to defeating the tiny fragment attack is to enforce a minimum length of the transport header that must be contained in the first fragment of an IP packet. If the first fragment is rejected, all subsequent fragments can be rejected. However, the nature of IP is such that fragments may arrive out of order. Thus, an intermediate fragment may pass through the filter before the initial fragment is rejected. How can this situation be handled?

It can be handled by a reassembly algorithm that will help detect the fragments that have overlap portions and will overwrite them, creating a new fragments that will be in order. The lowest fragment will contain safe data to allow the packet to pass the filter and this will have a packet following with a non-zero offset that will overlap header information and it will be modified. The the subsequent will pass the filters because it doesn't have a non-zero offset.

Problem 9.5: SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

Rule	Direction	Scr Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

a. Describe the effect of each rule.

-Rule A permits the inbound SMTP connection since is defining the remote host receiving the incoming email from external server.

-Rule B permits the inbound SMTP connection since is defining the external server receiving the incoming email from remote host.

-Rule C permits the outbound SMTP connection since it defines the external server transmitting the outgoing email to remote host.

-Rule D permits the outbound SMTP connection since it defines the remote host transmitting the outgoing email to external server.

-Rule E is a default rule that is only applied when the other rules do not apply, it defines the direction as ”in” or ”out” and the action is to deny.

b. Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets from this scenario are as shown:

Packet	**Direction**	**Src Addr**	**Dest Addr**	**Protocol**	**Dest Port**	**Action**
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP	1234	?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

Indicate which packets are permitted or denied and which rule is used in each case.

Packet	**Direction**	**Src Addr**	**Dest Addr**	**Protocol**	**Dest Port**	**Action**
1	In	192.168.3.4	172.16.1.1	TCP	25	Permit (A)
2	Out	172.16.1.1	192.168.3.4	TCP	1234	Permit (B)
3	Out	172.16.1.1	192.168.3.4	TCP	25	Permit (C)
4	In	192.168.3.4	172.16.1.1	TCP	1357	Permit (D)

c. Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Typical packets are as follows:

Packet	**Direction**	**Src Addr**	**Dest Addr**	**Protocol**	**Dest Port**	**Action**
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

Will the attack succeed? Give details.

The attack would succeed because in the original filter set, rules B and D permits all connections that ends with transmission ports above 1023.

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	Permit (B)
6	Out	172.16.3.4	10.1.2.3	TCP	5150	Permit (D)

Problem 9.6: To provide more protection, the rule set from the preceding problem is modified as follows:

Rule	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	Action
A	In	External	Internal	TCP	> 1023	25	Permit
B	Out	Internal	External	TCP	25	> 1023	Permit
C	Out	Internal	External	TCP	> 1023	25	Permit
D	In	External	Internal	TCP	25	> 1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

a. Describe the change.

The only difference is that now a bound is being added with the Src Port and the Dest Port. So it would be as follows:

-Rule A permits the inbound SMTP connection since is defining the remote host receiving the incoming email from external server from Src Port greater than 1023 to Dest Port of 25.

-Rule B permits the inbound SMTP connection since is defining the external server receiving the incoming email from remote host, from Src Port of 25 to Dest Port greater than 1023.

-Rule C permits the outbound SMTP connection since it defines the external server transmitting the outgoing email to remote host, from Src Port greater than 1023 to Dest Port of 25.

-Rule D permits the outbound SMTP connection since it defines the remote host transmitting the outgoing email to external server, from Src Port of 25 to Dest Port greater than 1023.

-Rule E is a default rule that is only applied when the other rules do not apply, it defines the direction as "in" or "out" and the action is to deny.

b. Apply this new rule set to the same six packets of the preceding problem. Indicate which packets are permitted or denied and which rule is used in each case.

Packet 1 :: Permit (A)
Packet 2 :: Permit (B)
Packet 3 :: Permit (C)
Packet 4 :: Permit (D)
Packet 5 :: Deny (E)
Packet 6 :: Deny (E)

Problem 9.11: You are given the following "informal firewall policy" details to be implemented using a firewall such as that in Figure 9.2:

1. E-mail may be sent using SMTP in both directions through the firewall, but it must be relayed via the DMZ mail gateway that provides header sanitization and content filtering. External e-mail must be destined for the DMZ mail server.
2. Users inside may retrieve their e-mail from the DMZ mail gateway, using either POP3 or or POP3S, and authenticate themselves.
3. Users outside may retrieve their e-mail from the DMZ mail gateway, but only if they use the secure POP3 protocol and authenticate themselves.
4. Web requests (both both insecure and secure) are allowed from any internal user out through the firewall but must be relayed via the DMZ Web proxy, which provides content filtering (noting this is not possible for secure requests), and users must authenticate with the proxy for logging.
5. Web request (both insecure and secure) are allowed from anywhere on the Internet to the DMZ Web server.
6. DNS lookup requests by internal users are allowed via the DMZ DNS server, which queries to the internet.
7. External DNS requests are provided by the DMZ DNS server.
8. Management and update of information on the DMZ servers is allowed using secure shell connections from relevant authorized internal users (may have different sets of users on each system as appropriate).
9. SNMP management requests are permitted from the internal management hosts to the firewalls, with the firewalls also allowed to send management traps (i.e., notification of some event occurring) to the management hosts.

Design suitable packet filter rule sets (similar to those shown in Table 9.1) to be implemented on the "External Firewall" and the "Internal Firewall" to satisfy the aforementioned policy requirements.

Next page ...

Not Est = Not Established

:::::EXTERNAL::::

Action	**Source**	**Port**	**Destination**	**Port**	**Flags**	**Comments**
Permit	DMZ mail gateway	Any	Any	SMTP (25)	Not Est	Sanitizing the header
Permit	Any	Any	DMZ mail gateway	SMTP (25)	Not Est	Filtering the Content
Permit	Any	Any	DMZ mail gateway	POP3S (995)	Not Est	User Authentication
Permit	DMZ web Proxy	Any	Any	HTTP/S(80/443)	Not Est	Content Filtered, User Authentication
Permit	DMZ DNS Server	DNS (53)	Any	DNS(53)	Not Est	TCP and UDP
Permit	Any	DNS (53)	DMZ DNS Server	DNS(53)	Not Est	TCP and UDP
Permit	Any	Any DMZ	Any	Any	Est	Return Traffic Flow
Permit	Any	Any	Any	Any	Not Est	Block All Else

:::::INTERNAL::::

Action	**Source**	**Port**	**Destination**	**Port**	**Flags**	**Comments**
Permit	Any Int	Any	DMZ mail gateway	SMTP (25)	Not Est	Sanitizing the header
Permit	Any Int	Any	DMZ mail gateway	POP3/S(110,995)	Not Est	Content Filtered
Permit	Any Int	Any	DMZ Web Proxy	HTTP/S(80,443)	Not Est	User Authentication
Permit	Any Int	DNS (53)	DMZ DNS Server	DNS (53)	Not Est	Content Filtered, User Authentica
Permit	DMZ DNS server	DNS (53)	Any Internal	DNS (53)	Not Est	TCP and UDP
Permit	Any	Any	Any DMZ server	SSH (22)	Not Est	TCP and UDP
Permit	Management User Host	Any	Any DMZ server	SNMP (161)	Not Est	Return Traffic Flow
Permit	Permit	Any	Management User Host	SNMP TRAP (162)	Not Est	Block All Else