SMTP 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:

Firewall Exercise Rule Set

Firewall rule	Direction	Source addr	Dest addr	Dest port	Protocol	Action
A	In	external	internal	25	TCP	permit
B	Out	Internal	external	*	TCP	permit
C	Out	Internal	external	25	TCP	permit
D	In	External	internal	*	TCP	permit
E	Either	*	*	*	*	deny

질문 1

0.48 pts

Rule A allows inbound traffic from external sources that has a destination port of 25 and uses a TCP protocol.

- (•) True
- ( ) False

질문 2

0.48 pts

Rule B allows an inbound connection from internal to external on any port with TCP protocol.

- ○ True
- ◉ False

질문 3 **0.48 pts**

Rule C denies an outbound connection from internal to external on port 25 with TCP protocol.

- ◉ True
- ○ False

질문 4 **0.48 pts**

Rule D allows inbound traffic from external sources that has any destination port and uses a TCP protocol.

- ○ True
- ◉ False

질문 5 **0.48 pts**

Rule E denies all other traffic.

- ◉ True
- ○ False

질문 6 **3.9 pts**

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 that a user on your

host tries to send e-mail to the SMTP server on the remote system. Four typical packets on this scenario are as shown below in the table.

Indicate which packets are permitted or denied and which rule is used in each case. So for each packet, make sure you specify if it is permitted or denied followed by the rule in brackets (). **For this exercise to be graded correctly, you must spell permitted or denied correctly, followed by a space, then the rule in parenthesis, letter only. For example: Denied (D) - OR - Permitted (B)**

Packet	Src Addr	Dest Addr	Protocol	Source Port	Dest Port	ACK	Action
1	192.168.3.4	172.16.1.1	TCP	1234	25	0	Permitted (A)
2	172.16.1.1	192.168.3.4	TCP	25	1234	1	Permitted (B)
3	172.16.1.1	192.168.3.4	TCP	1432	25	0	Permitted (C)
4	192.168.3.4	172.16.1.1	TCP	25	1432	1	Permitted (D)

질문 7

2.95 pts

Someone from the outside world (10.1.2.4) 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.

Indicate which packets are permitted or denied. **For this to be graded, only write permitted or denied. No spaces, or a rule in parenthesis for this particular question. Spell it correctly!**

Packet	Direction	Src Addr	Dest Addr	Protocol	Source Port	Dest Port	Action
5	In	10.1.2.4	172.16.1.1	TCP	5150	8080	Permitted

6	Out	172.16.3.4	10.1.2.4	TCP	8080	5150	Permitted

To increase protection the rule set is changed as follows:

Firewall rule	Direction	Source addr	Dest addr	Src Port	Dest port	Protocol	Action
A	In	external	internal	>1023	25	TCP	permit
B	Out	Internal	external	25	*	TCP	permit
C	Out	Internal	external	>1023	25	TCP	permit
D	In	External	internal	25	*	TCP	permit
E	Either	*	*	Any	*	*	deny

질문 8

10.75 pts

Apply this new rule set to the same six packets used before. Indicate which packets are permitted or denied and which rule is used in each case. So for each packet, make sure you specify if it is permitted or denied followed by the rule in brackets (). **For this exercise to be graded correctly, you must spell permitted or denied correctly, followed by a space, then the rule in parenthesis, letter only. For example: Denied (D) - OR - Permitted (B)**

Packet	Src Addr	Dest Addr	Protocol	Source Port	Dest Port	ACK	Action
1	192.168.3.4	172.16.1.1	TCP	1234	25	0	
2	172.16.1.1	192.168.3.4	TCP	25	1234	1	

3	172.16.1.1	192.168.3.4	TCP	1432	25	0	
4	192.168.3.4	172.16.1.1	TCP	25	1432	1	

Packet	Direction	Src Addr	Dest Addr	Protocol	Source Port	Dest Port	Action
5	In	10.1.2.4	172.16.1.1	TCP	5150	8080	
6	Out	172.16.3.4	10.1.2.4	TCP	8080	5150	