Write firewall packet filtering rules for a corporate network with IP addresses 219.33.*.*. The firewall should permit all outgoing connections, incoming connections to the web servers with IP addresses 219.33.12.2 and 219.33.3.4 for both HTTP and HTTPS, incoming connections to the email server with IP address 219.33.12.2, and incoming SSH connections to machines with IP addresses 219.33.49.12 and 219.33.3.8.

Incoming from HTTP (Port 80) and HTTPS (Port 443)

ALLOW TCP * : * -------> 219.33.12.2 : 80

ALLOW TCP * : * -------> 219.33.12.2 : 443

ALLOW TCP * : * -------> 219.33.3.4 : 80

ALLOW TCP * : * -------> 219.33.3.4 : 443

Incoming from SMTP (Port 25)

ALLOW TCP * : * -------> 219.33.12.2 : 25

Incoming from SSL (Port 22)

ALLOW TCP * : * -------> 219.33.49.12 : 22

ALLOW TCP * : * -------> 219.33.3.8 : 22

Outgoing

Any machine from our internal network can access any ip address outside our network

ALLOW TCP 219.33.*.*:* -------> * : *

Internal network to any external IP, a handshake must take place in which a ACK from external IP must be accepted and not dropped.

ALLOW TCP * : * -------> 219.33.*.* : * (if ACK = 1)

DROP * * : * -------> *:*

If none of the rules above match, then drop.