CSS 337: Assignment 5

Firewalls

Qn. 1: You are given the following "informal firewall policy" details to be implemented using a firewall shown in the following figure:

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 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 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 requests (both insecure and secure) are allowed from anywhere on the Internet to the DMZ Web server.

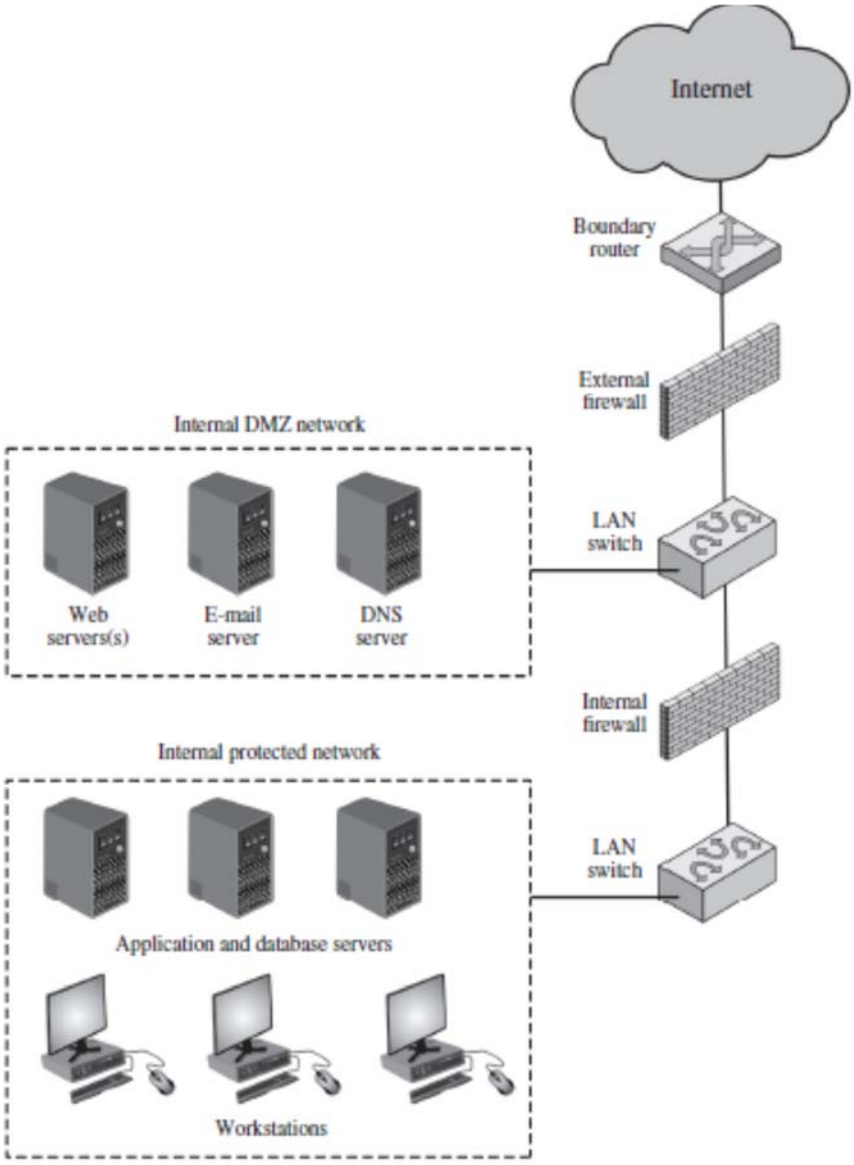
6. DNS lookup requests by internal users are allowed via the DMZ DNS server, which queries to the Internet.

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).

Design suitable packet filter rule sets to be implemented on the "External Firewall" and the "Internal Firewall" to satisfy the aforementioned policy requirements.

NOTE: Ports are SMTP: 25, DNS 53, POP3 110, POP3S 95 HTTP 80, HTTPS 443



Qn2: Complete the Firewall tools exercise given in class. Answer all the questions in the document.

Submit both Qn 1 and 2 in the same word or pdf document.