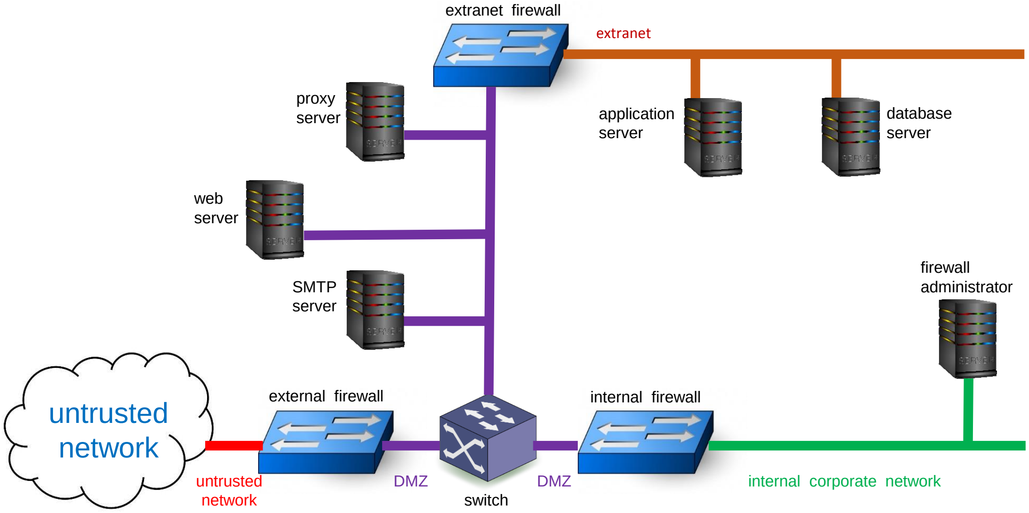
homework 5 - firewalls

50 pts. – due date: Wed. 10/25

Please finish reading chapter “6”, pages 297 - 354 of Whitman and Mattord (5th edition), review the firewall slide deck and then answer the following questions. Please note that the goal of this exercise is to familiarize you with the basic process of writing rules for packet-filtering firewalls, not to provide a cook-book answer for all cases. Many specific firewalls are different, and may require or not require rules to follow specific formats or patterns.



device	interface	IP address	alias address
external firewall	untrusted network	20.22.20.1	
	DMZ	20.22.20.2	
extranet firewall	DMZ	20.22.20.3	
	extranet	20.22.20.4	
internal firewall	DMZ	20.22.20.5	
	internal network	192.168.0.1	20.22.20.6
SMTP server	DMZ	20.22.20.7	
web server	DMZ	20.22.20.8	
proxy server	DMZ	20.22.20.9	
application server	extranet	20.22.10.11	20.22.20.11
database server	extranet	20.22.10.12	20.22.20.12
firewall admin.	internal network	192.168.0.2	20.22.20.20

port	service
25	SMTP
80	http (web)
107	internal application
156	database session

One common extension to a corporate network is an “extranet.” (Note that this term has evolved in meaning, so you may encounter it being used in different contexts.) One application of an extranet is as an extension off the DMZ where additional services are offered, usually to trusted business partners. This provides access to shared resources between the businesses without creating direct vulnerabilities on the internal network.

1. **[20 pts.]** Create firewall rules for the untrusted network port on the external firewall which will:
    - block spoofing of internal network addresses
    - allow traffic from the untrusted network into the DMZ for the
        - SMTP server;
        - web server (http);
        - proxy server (internal application port);
        - and, extranet database server.
    - allow response traffic to the extranet database server and all internal network devices
    - explicitly disallow any inbound ping or telnet traffic
    - disallow all other traffic

2. **[10 pts.]** Create firewall rules for the DMZ port on the extranet firewall which will:
    - allow traffic from the proxy server to the application server for the internal application service
    - allow traffic to the database server from these specific sources only (representing preferred customers):
        - network 42.40.0.0
        - network 77.7.77.0
        - host 112.92.4.3
    - disallow all other traffic

3. **[20 pts.]** Create firewall rules for the internal network port on the internal firewall which will:
    - specifically deny traffic spoofing the firewall ports
    - deny traffic to the firewall ports, except from the local firewall administrator (allow that traffic)
    - allow all outbound traffic out
    - deny all other traffic