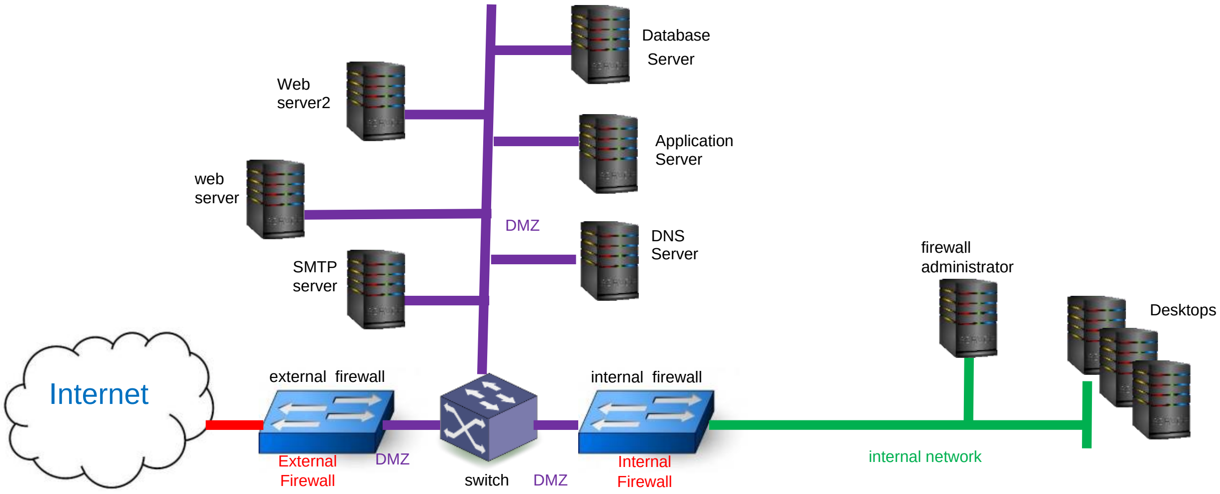
Homework 2 - Firewalls

60 pts. – Due date: Friday Nov. 11th at 7:00PM EST

The goal of this exercise is to make you familiar with the basic process of writing rules for packet filtering firewalls, not to provide an actual rule base for any specific vendor's production firewall. Use the spreadsheet titled "Homework_02-FWRuleMatrix.xlsx" as your answer sheet for the questions below.



Device	INTERFACE DETAILS by Network	IP Address
External firewall	Untrusted (internet) interface	98.138.5.1
External firewall	DMZ interface	120.32.20.2
Internal firewall	DMZ interface	120.32.20.5
Internal firewall	internal network / management Interface	192.168.20.1
DNS server	DMZ	120.32.20.6
SMTP server	DMZ	120.32.20.7
web server	DMZ	120.32.20.8
web server2	DMZ	120.32.20.9
application server	DMZ	120.32.20.10
database server	DMZ	120.32.20.11
firewall admin station	internal network	192.168.20.2

Port	Service
22	ssh
25	smtp
53	DNS
80	http
107	proprietary application
156	database session

	NETWORK DEFINITIONS	
Network		**IP Address**
DMZ		120.32.20.0/24
internal network		192.168.20.0/24

1. **[27 pts.]** Create firewall rules on the external firewall which will: (You will have 9 rules)
   - This rule is to block known malicious traffic first. Disallow traffic to the SMTP server from:
     - The internet host 202.125.17.28 on the SMTP service
     - The internet host 12.30.30.25 on the SMTP service
   - allow traffic from the internet into the DMZ to the:
     - SMTP server on the SMTP service only
     - DNS server on the DNS service only
     - web server on http only
     - web server2 on the proprietary app port only
     - extranet database server on the database session only
   - allow all outbound traffic from any DMZ address out to any site
   - disallow all other traffic

2. **[21 pts.]** Create firewall rules on the internal firewall which will: (You will have 7 rules)
   - specifically deny all internal network traffic to web server 2
   - allow all internal network outbound traffic to the Application server via the proprietary application port
   - deny traffic on the internal network to the internal firewall management interface IP using ssh, except from the local firewall administrator (allow that traffic using ssh)
     - Hint: This will be 2 different rules; remember rules are matched from the top down and when traffic matches a rule it stops at that rule and the action of the rule is performed on it
   - Allow internal network outbound traffic out to the DNS server on the DNS service only
   - allow all other internal network outbound traffic out to the internet via HTTP
   - disallow all other traffic

3. **[12 pts.]** Create firewall rules for the internet firewall which will: (You will have 4 rules)
   - allow any traffic to the database server on the database session port from these specific sources only (representing preferred customers):
     - network 42.41.1.0/24
     - network 77.77.7.0/24
     - host 113.92.44.3
   - disallow all other traffic