

Directed Work N° 3

Exercise 1:

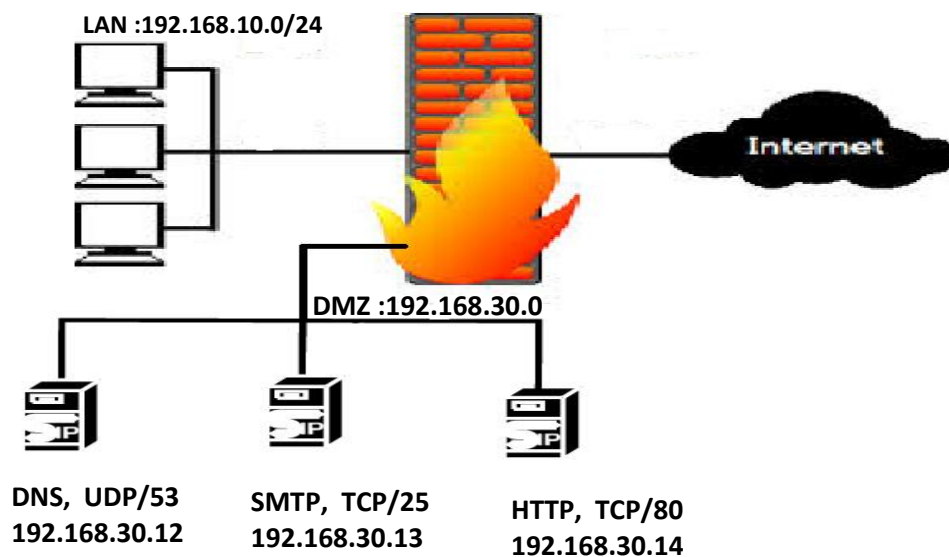
Complete the comparison table (Stateless vs Stateful Firewall)

Parameter	Stateless Firewall	Stateful Firewall
Philosophy		
Filtering decision		
Memory & CPU intensive		
Security		
Connection status		
Performance		

Exercise 2:

A company has a firewall to restrict access to and from machines on its internal network. The company's network architecture also includes a demilitarized zone (DMZ) for deploying the company's own SMTP, HTTP, and DNS servers.

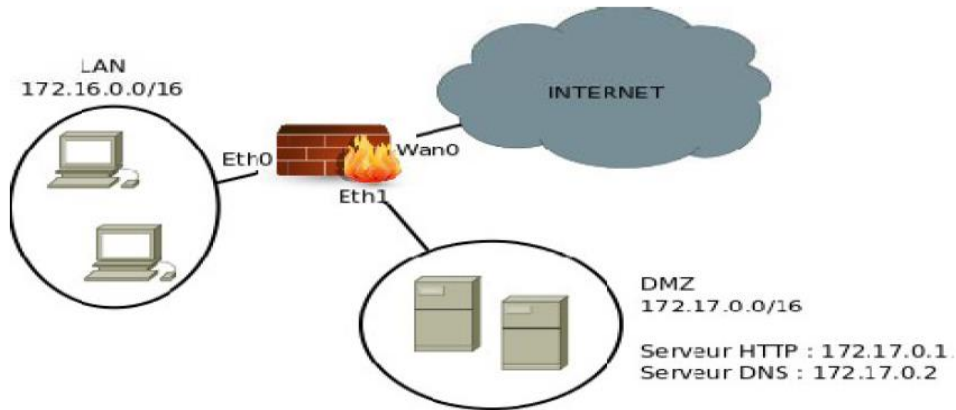
- The company's network is represented by the following diagram:



Write the firewall filtering rules corresponding to the following policies:

1. Allow external users to access the DNS servers of the local network.
2. Allow internal users to access the HTTP servers of the local network.
3. Allow internal users to access SMTP servers on the internet.
4. All other types of communication must be denied.

Exercise 3:



A company has a firewall to restrict access to and from machines on its internal network. The company's network architecture also includes a demilitarized zone (DMZ) for deploying the company's own Web and DNS servers.

- The company's network is represented by the diagram above.
- The security policy enforced by the firewall is described by the following table:

Rule	Src IP	Dst IP	Src Port	Dst Port	Protocol	Action
1	172.16.0.0	172.17.0.1	*	80	TCP	Allow
2	172.17.0.1	172.16.0.0	80	*	TCP	Allow
3	172.16.0.0	172.17.0.2	*	53	UDP	Allow
4	172.17.0.2	172.16.0.0	53	*	UDP	Allow
5	*	172.17.0.1	*	*	TCP	Allow
6	172.17.0.1	*	80	*	TCP	Allow
7	172.16.0.0	*	*	80	TCP	Allow
8	*	172.16.0.0	80	*	TCP	Allow
9	*	*	*	*	*	Deny

1. Give the policy corresponding to each pair of rules (1-2), (3-4), (5-6) and (7-8).
2. Specify which rule will match each of the following packets and state whether the packet will be accepted or rejected:
 - **p1** – Src IP: 172.16.0.30 Dst IP: 12.230.24.45 Proto: TCP Src Port: 1045 Dst Port: 443
 - **p2** – Src IP: 172.16.10.5 Dst IP: 172.17.0.2 Proto: UDP Src Port: 6810 Dst Port: 53
 - **p3** – Src IP: 140.10.2.1 Dst IP: 172.17.0.1 Proto: TCP Src Port: 8000 Dst Port: 80
 - **p4** – Src IP: 17.14.3.3 Dst IP: 172.17.0.2 Proto: UDP Src Port: 6000 Dst Port: 53
 - **p5** – Src IP: 172.17.0.1 Dst IP: 1.2.3.4 Proto: TCP Src Port: 80 Dst Port: 9999