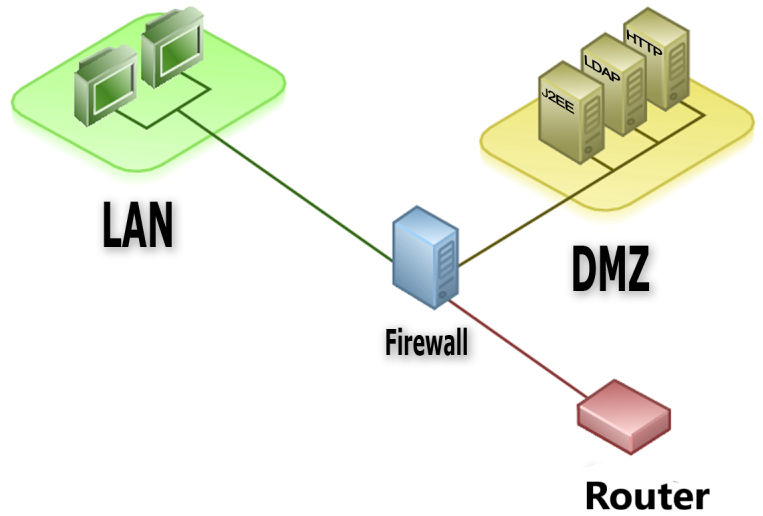
**FIREWALL&DMZ**

**I. Introduce**

Firewall is a network security system, can be based on hardware or software, using rules to control traffic entering and leaving the system. A firewall acts as a barrier between a secure network and an insecure network. It controls access to network resources through an active control model. That is, only traffic that conforms to the policy defined in the firewall can access the network, all other traffic is rejected.

DMZ is a word very commonly used in military zones and the computer field. DMZ stands for Demilitarized Zone. Understood as the demilitarized zone, military frontier, or demilitarized zone. Areas with no military activity took place, so this was also where peaceful urban areas were away from gang territories. However, DMZ is also an acronym used in informatics. In computing a DMZ is a networked device (range of networked devices or subnets), for example a computer, placed outside of a firewall or other security measures on the network.



**Purpose of DMZ:**

In computer security, for the small and medium networks, we setup a firewall that processes all the requests from the internal network (LAN) to the Internet, and from the Internet to the LAN.

This firewall is the only protection the internal network has in these setups; it handles any NAT (Network Address Translation), by forwarding and filtering requests as its configuration.

For small companies, this is usually a good choice. But for the large system, putting all servers behind a firewall is poor security.

That’s why DMZs (demilitarized zone networks) are used to separate the internal network from the outside world. This way, outsiders can access the public information in the DMZ, while the private, proprietary information is kept safely behind the DMZ, into the internal network.

The DMZ Network exists to secure the hosts (internal network) from most vulnerable to attack. These hosts usually involve services that extend to users outside of the local area network, the most common examples being email, web servers, and DNS servers. Because of the increased potential for attack, they are placed into the monitored subnetwork to help protect the rest of the network if they become compromised.

Here are a few examples of services that you can keep in the Demilitarized Zone Network:  
 - webservers with public information  
 - the front-end of your application (the back-end should be kept safely behind the DMZ)  
 - mail server  
 - authentication services  
 - services like HTTP for general public usage, secure SMTP, secure FTP, and secure Telnet  
 - VoIP servers  
 - VPN endpoints  
 - application gateways  
 - test and staging servers

**II. Construction architecture of DMZ&Firewall**

The basic components that make up the DMZ are: IP addresses and firewalls.

Two important identifiers of the DMZ:

- It has a different network ID than the internal network.

- It is separated from the Internet and the internal network by the firewall(s).

1. IP addresses in DMZ:

DMZ can use public IP or private IP for servers depending on the configuration on the firewall and the DMZ structure.

When we use a public IP for the DMZ, you will need to subnet the block of IP addresses that ISP gives us to get two separate network IDs. Then one network ID is used for the external interface (network card directly connected to the ISP) of the firewall and the other network ID is used for the DMZ network. However, remember when subnet this public IP block, must configure router so that packets from outside Internet can reach the DMZ.

We can also create a DMZ with the same network ID as the internal network by using VLAN Tagging (IEEE 802.1q) while ensuring the DMZ and the internal network are separation. In this case, the servers in the DMZ and the workstations on the internal network are all plugged into a switch (or different switches but these switches are connected together) and assigned to the different VLANs.

In case using private IP for the DMZ, need NAT (some firewalls already support this feature) to convert these private IPs to a public IP (which is assigned to the external interface of the firewall between the Internet and the DMZ).

2. DMZ models

a. components:

The components in the network model include:

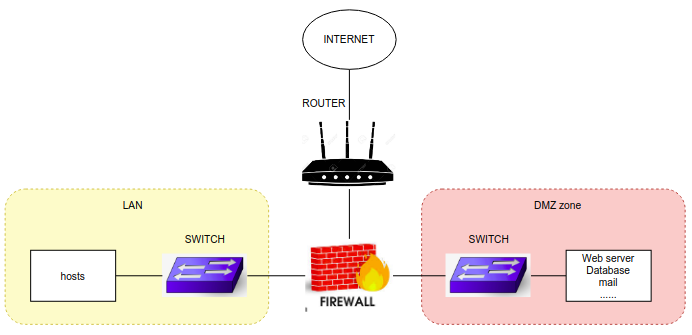
- Local area network(LAN): the place where network devices, workstations and servers belong to the internal network of the unit.

- DMZ zone: a neutral network zone between the internal network and the Internet, which contains information allowing users from the Internet to access and accept risks from Internet attacks. Services commonly deployed in the DMZ are: Web server, Mail server, DNS server, FTP server, ... - Server Farm: the place where servers don’t directly provide services to the Internet. Usually to deploy Database Server, LDAP Server, …

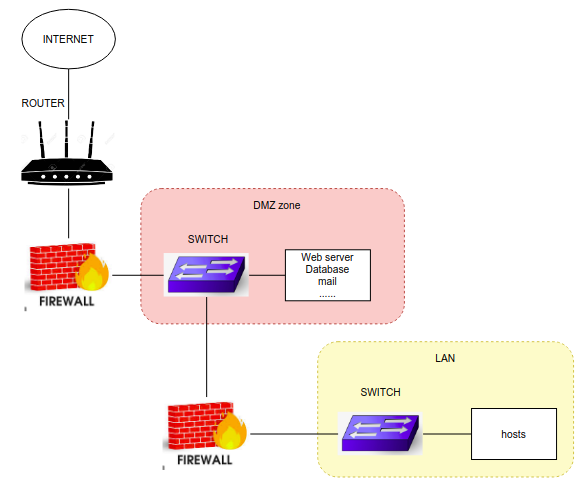
- Internet: Also known as external network, connects to the global Internet. The security network model organization to ensure security has a great impact on the safety of network systems and other Web portal. This is the first base for the construction of defense and protection systems. In addition, the organization of a secure network model can effectively limit internal and external attacks.

b. Models:

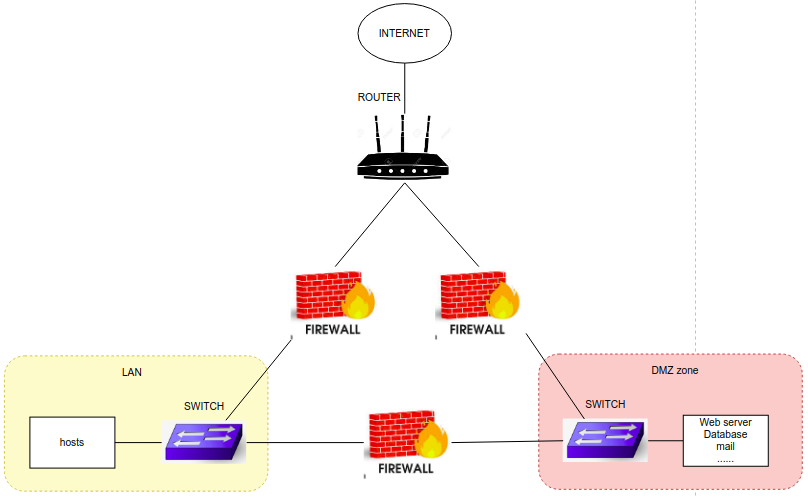
In this model, the Internet area, intranet area, and DMZ area are designed separately. In addition, we put a firewall between network zones to control the flow of information between network zones and protect the network areas from unauthorized attacks.



Put a firewall between the Internet area and the DMZ area and a firewall between the DMZ area and the internal network area.



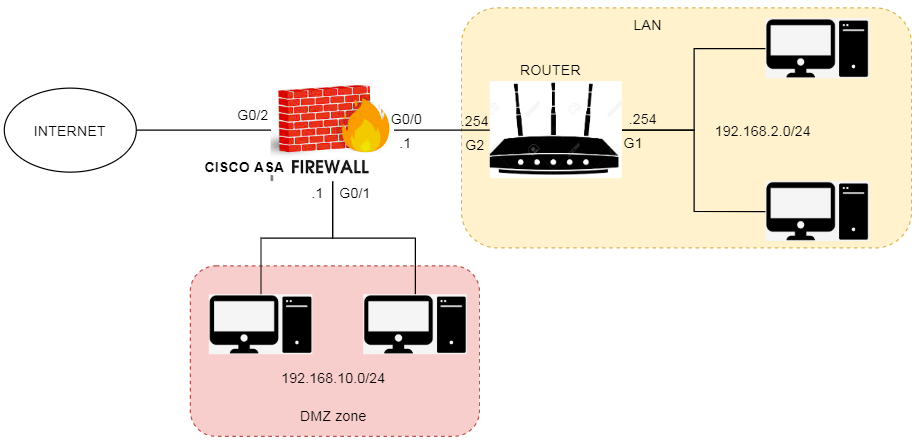
Put a firewall between the Internet area and the DMZ network area, a firewall between the DMZ area and the internal network area, and a firewall between the internal network area and the Internet zone. Thus, each access between regions is controlled by a firewall as shown in the figure.



III. How to configure a DMZ area

For example, I use the CISCO ASA to configure a single firewall DMZ.

## Lab topology setup



Step 1. Configure interface port of CISCO ASA(firewall)   
  
LAN area

|  |
| --- |
| interface GigabitEthernet0/0 nameif inside security-level 100 ip address 192.168.0.1 255.255.255.0 |

DMZ

|  |
| --- |
| interface GigabitEthernet0/1 nameif DMZ security-level 50 ip address 192.168.10.1 255.255.255.0 |

Internet

|  |
| --- |
| interface GigabitEthernet0/2 nameif outside security-level 0 ip address dhcp setroute  //auto insert route default to ip route table after receive IP |

Step 2. Configure routing:  
Set default-route on router. Configure static route on CISCO:

|  |
| --- |
| route inside 192.168.2.0 255.255.255.0 192.168.0.254 |

After configuration, the DMZ can be accessed from inside(LAN)  
Note: By default, CISCO ASA doesn’t allow ICMP to pass between zones, to ping from the Inside zone you need to configure more:

|  |
| --- |
| ciscoasa(config)# policy-map global\_policy  ciscoasa(config-pmap)# class inspection\_default  ciscoasa(config-pmap-c)# inspect icmp |

Step 3. Configure SSH on CISCO ASA:

|  |
| --- |
| ciscoasa(config)# username NAME password PASS  ciscoasa(config)# crypto key generate rsa general-keys ciscoasa(config)# ssh 192.168.2.10 255.255.255.255 inside  ciscoasa(config)# ssh version 2 ciscoasa(config)# aaa authentication ssh console LOCAL |

After completed this step, SSH from PC(192.168.1.10) is available

Step 4.  Configure static NAT and ACL to allow remote Desktop service in DMZ:  
4.1: Configure Object Network:

|  |
| --- |
| object network DMZ\_10.10 host 192.168.10.10 |

4.2: Configure Object Service:

|  |
| --- |
| object service RDP service tcp source eq 3389 |

4.3: Configure NAT:

|  |
| --- |
| nat (inside,outside) source static DMZ\_10.10 interface service RDP |

4.4: Configure ACL to allow outside access to DMZ:

|  |
| --- |
| access-list POLICY extended permit tcp any host 192.168.10.10 eq 3389 access-group POLICY in interface outside |

Then, Remote Desktop Services from Outside(192.168.1.67) is ready.

Step 5. Configure PAT to allow user from inside(LAN) can access to Internet:

B1: Configure Object:

|  |
| --- |
| object network USER subnet 192.168.2.0 255.255.255.0 |

B2. Configure PAT:

|  |
| --- |
| nat (inside,outside) source dynamic USER interface // Ip-address of user who NAT to outside interface address |

REFERRENCES:

https://www.cisco.com/c/dam/global/en\_ca/assets/pdf/sc-01\_fw-ips-cvd\_designguide\_en.pdf

https://www.speaknetworks.com/cisco-asa-dmz-configuration-example/

http://cs.lewisu.edu/mathcs/msis/projects/msis595\_KevinKeay.pdf

https://perpetuastudents.wordpress.com/2007/12/05/firewall/