As your teacher requirement, your presentation will follow the format like the website: [www.pechakucha.com](http://www.pechakucha.com).

I attached the presentation.pptx, you’ll need to slideshow every slide and read the paragraph that I wrote below. You also need record your voice and monitor screen while you present. After that, submit the **video** which you recorded and **research.docx**.

Remember read the paragraph below following the slide number. Don’t forget record and monitor screen.

**SLIDE1:**

Today, I’ll present about topic “Firewall&DMZ”. The first, we need to understand “what is firewall?”.

By definition, 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.

 Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices. For example, “Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it’s further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

Ok, We know the definition of firewall, next we’ll find out “what is DMZ?”

**SLIDE2:**

DMZ is a word very commonly used in military zones and the computer field. DMZ stands for Demilitarized Zone.

Because systems that are most vulnerable to attack are those that provide services to users outside of the local area network, such as e-mail, Web and DNS servers, they are quarantined inside a DMZ, from where they have limited access to the private network.

**SLIDE3:**

As you see in the picture, The DMZ is isolated using a security gateway (i.e. firewall) to filter traffic between the DMZ and the private network. The DMZ itself also has a security gateway in front of it to filter incoming traffic from the external network.

At here, you’ll wonder why we need DMZ while firewall can also prevent the attack from outside?

The truth is: 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 of internal network. For small companies, this is usually a good choice. But for the large system, putting all servers behind a firewall is poor security.

So, The DMZ Network exists to secure the hosts (internal network) from most vulnerable to attack

**SLIDE4:**

First, we need to understand about the components in the secure network model.

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.

Next, we’ll research about the DMZ models in next slide

**SLIDE5:**

I’ll introduce some DMZ models that we usually set up. Remember, there are many DMZ models you can set up, it depends on your requirements and budget.

The first model I introduce, the single firewall DMZ

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. So there is only a firewall to protect the servers and control line between DMZ and LAN.

**SLIDE6:**

The double firewall DMZ.

it’s same the first model but we’ll put a firewall between the Internet area and the DMZ area and a firewall between the DMZ area and the internal network area.

So, there are two firewalls in this model, the firewall between DMZ and internet to prevent the attack from outside and the firewall between DMZ and LAN to ensure no suspicious action from LAN can harm the DMZ.

**SLIDE7:**

The triple firewall DMZ.

We 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.

Every connection has a firewall to prevent the attacking.

So, there are still many DMZ configuration methods.

Next slide, I’ll present how to configure a DMZ.

**SLIDE8:**

I choose CISCO ASA 5500s to configure firewall&DMZ in single firewall DMZ model.

As you see in this picture, it’s lab topology. There only a firewall-CISCO ASA in this model, Cisco ASA is deployed as an Internet gateway, providing outbound Internet access to all internal hosts. In addition, there are Local Area Network and the servers (in DMZ).

**SLIDE9:**

I configure the ethernet ports on CISCO ASA like this picture.

The Cisco ASA Firewall uses so called “security levels” that indicate how trusted an interface is compared to another interface. The higher the security level, the more trusted the interface is. Each interface on the ASA is a security zone so by using these security levels we have different trust levels for our security zones

So, set ip address 192.168.0.1 netmask 255.255.255.0 and security-level 100 at GigabitEthernet0/0 interface, set ip address 192.168.10.1 netmask 255.255.255.0 and security-level 50 at GigabitEthernet0/1 interface. The last, set dhcp and security-level 0 at GigabitEthernet0/2 interface

We also configure route inside to set default-route on router

After configuration, the DMZ can be accessed from inside(LAN)

**SLIDE10:**

By default, CISCO ASA doesn’t allow ICMP to pass between zones, to ping from the Inside zone you need to configure more, like the first picture.

Then we configure SSH on CISCO ASA to allow ssh service as the second picture.

After completed this step, you can SSH from PC with ip 192.168.1.10 to DMZ.

**SLIDE11:**

We also need to configure static NAT and ACL to allow remote Desktop service in DMZ.

First, Configure Object Network, name DMZ\_10.10 with host 192.168.10.10

Second, Configure Object Service: object service RDP  
and service tcp source

Third, configure Network address translation like image,

nat inside or outside source static DMZ\_10.10 and interface service is RDP

Final, Configure ACL to allow outside access to DMZ:

access-list POLICY extended permit tcp, I permit tcp from host 192.168.10.10 in access-group POLICY I configured.

Then, You have Remote Desktop Services from Outside with ip 192.168.1.67

Next step, Configure PAT to allow user from inside(LAN) can access to Internet:

Configure Object:

object network USER, type your user name and subnet with ip 192.168.2.0 netmask 255.255.255.0

then, Configure PAT:

nat inside or outside source dynamic USER interface

source is Ip-address of user who NAT to outside interface address

So, I presented the Reseach about Firewall&DMZ, maybe there are many miss knowledge while presentation, hope you forgive the minor mistakes.

**DONE!!!!**

Thanks for listening