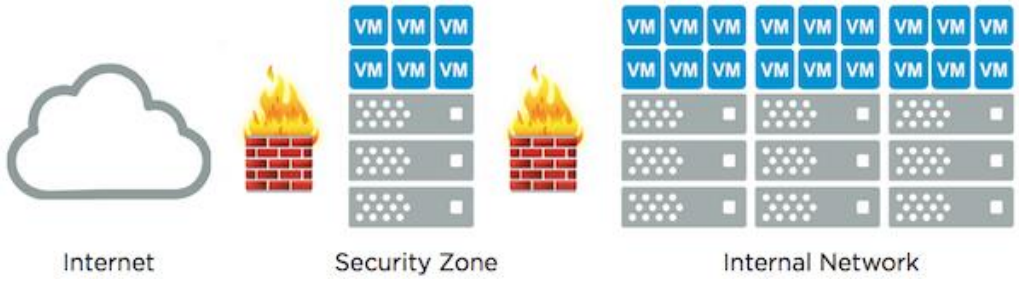
1. Brief paragraph

a. security zone

Also known as "*DMZ*", it is a sub-network used to separate the organization's internal network from external applications and requests. Security zones are logical network segmentations which one or more interfaces are bound. We can define several security zones as the internet needs.



Ideally, the security zones should be self-contained and includes the necessary computing, network and storage resources with little or no dependency on an organization's internal infrastructure.

reference:

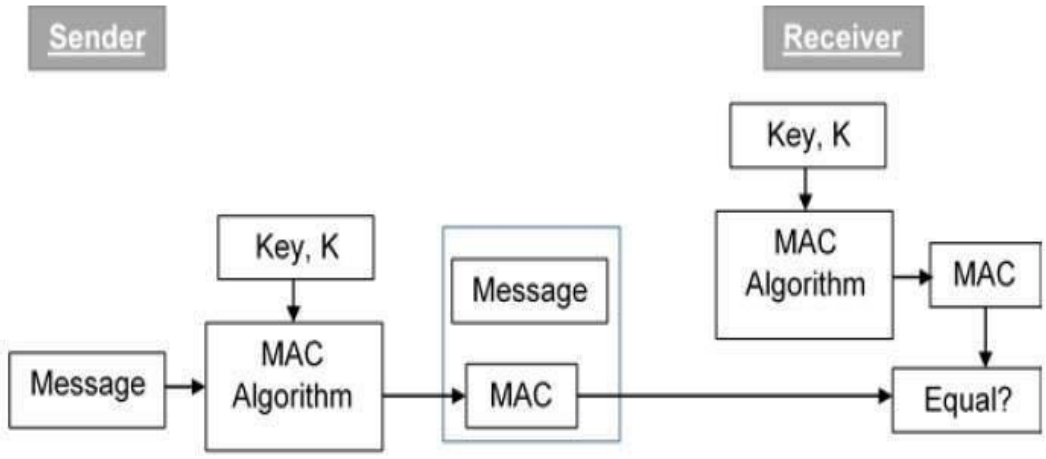
https://blogs.vmware.com/virtualblocks/2016/01/11/vsan-for-security-zones/

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-zone-configuration.html

b. message authentication

Also called *data origin authentication* or *data integrity authentication.* It is a circumstance that sender's message hasn't been altered in transmission and the receiver can verify the data integrity of the message.

Message authentication is generally achieved by using message authentication codes (MAC). Following figure is the example of message authentication.



Message authentication doesn't always meet the property of non-repudiation and confidentiality. Sometimes the message authentication process will include the MAC algorithm and asymmetric encryption/decryption algorithm.

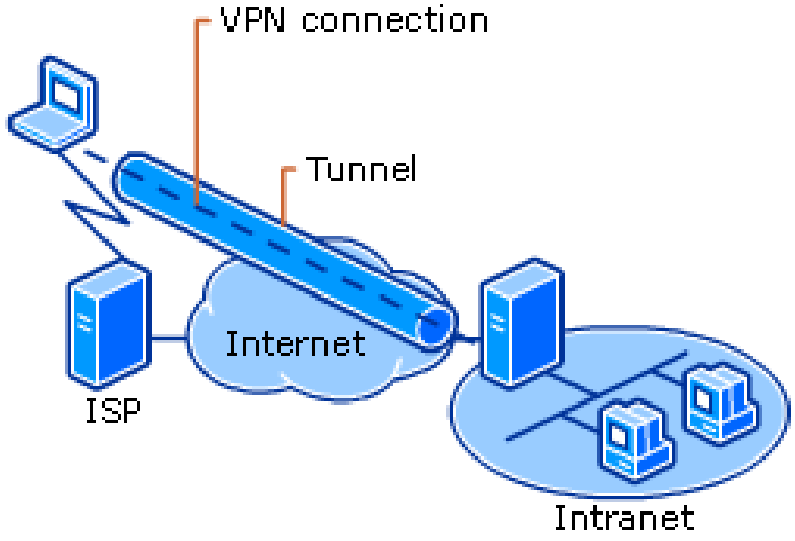
Reference:

https://en.wikipedia.org/wiki/Message_authentication

https://en.wikipedia.org/wiki/Message_authentication_code

c. VPN

Virtual private network (VPN) builds a private network across a public network. The users send and receive data through the VPN as if their electronic devices were directly connected to the private network. Running applications across the VPN may increase the security and anonymity in the internet communication.



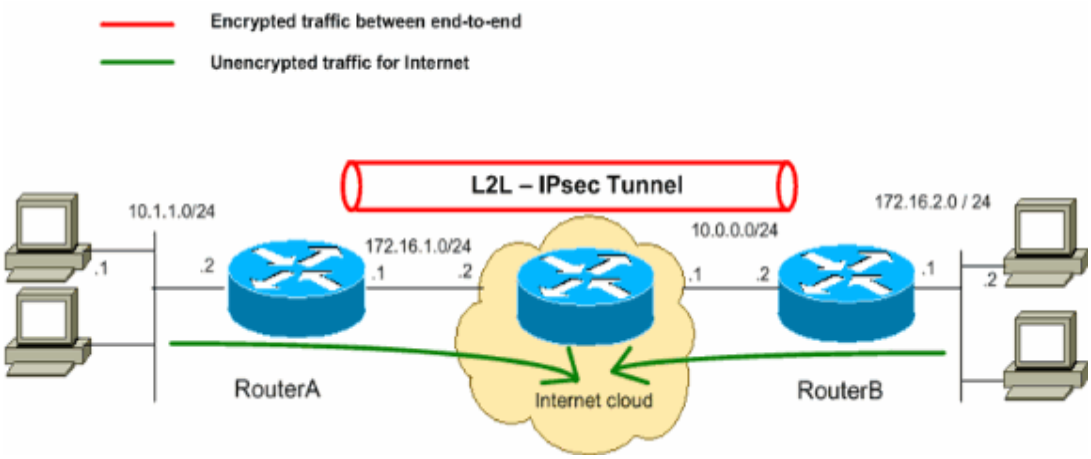
Before we build a secure VPN tunnel, the tunnel endpoints must be authenticated. VPN cannot guarantee the complete anonymity of internet connection. However, they might enhance the privacy and security

Reference:

https://en.wikipedia.org/wiki/Virtual_private_network

d. IPsec

Internet Protocol Security (IPsec) is a network protocol that verify (authenticate) and provide the confidentiality (encrypt) of packets sent over the network. Generally, it is used in VPN. It can protect the data flows between host-to-host, network-to-network, or network-to-host. IPsec uses cryptography method to protect communications over networks and supports network-level authentication, data integrity, data confidentiality, and replay protection…etc.



Encryption/Decryption algorithm used in IPsec usually includes:

HMAC-SHA1/SHA2: for integrity and authentication

3DES-CBC: for confidentiality

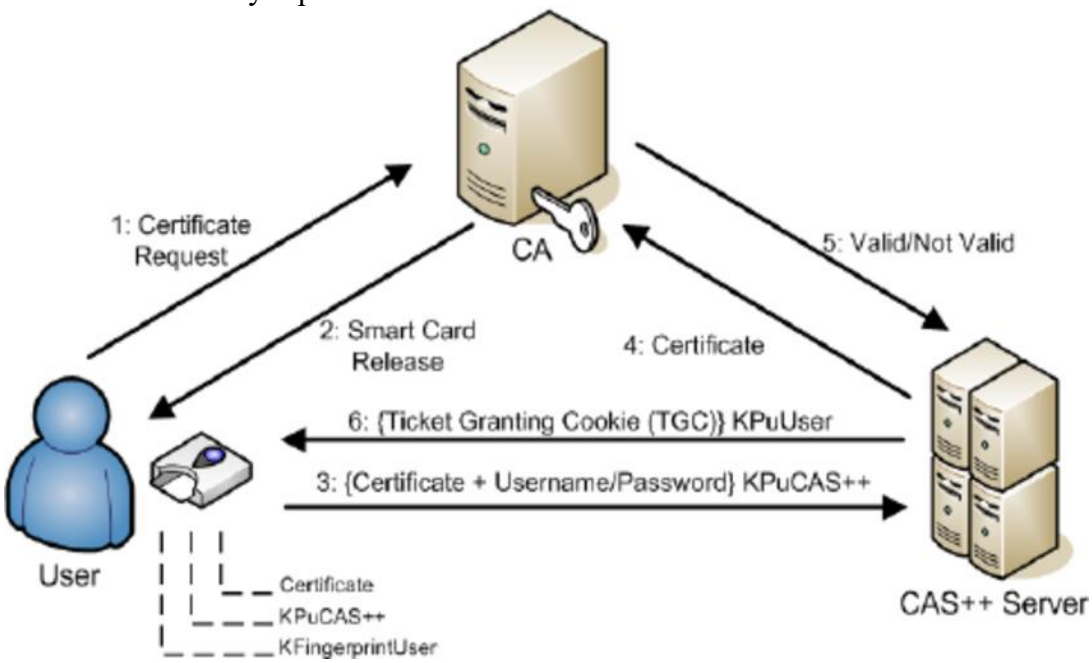
AES-GCM: for confidentiality and authentication

Reference:

https://en.wikipedia.org/wiki/IPsec

e. certificate-based authentication

The main purpose of adapting *certificate-based authentication* is to ensure that only approved users and devices can get access to the systems. That is for the information security aspect.



Certificate-based authentication involves the use of digital certificates to identify the users, machines, or devices before granting access to the resources, networks and application…etc. Usually, it is in coordination with traditional methods such as username and password authentication.

Some authentication examples

- Identifying on-location/in-field machines that need to communicate with back-end services (e.g. payment kiosks located in convenience stores)
- Identifying all employee laptops and mobile devices before allowing access to WiFi, VPNs, Gateways, etc
- Identifying all servers within the enterprise to enable mutual authentication

2. Explain Scripts

a. switch & vlan

Because I can't find a 48-port switch, I adjust the scripts a little bit. Following is my implementation about the switch.

// That is the basic initial configuration

```
Switch>enable

Switch#configure terminal
```

// Here we rename the switch to Switch-B and change the mode to vtp transparent

```
Switch(config)#hostname Switch-B

Switch-B(config)#vtp mode transparent
```

// We separate the first virtual LAN 10 and rename it to Engineering

```
Switch-B(config)#vlan 10

Switch-B(config-vlan)#name Engineering

Switch-B(config-vlan)#exit
```

// The same, we separate the second virtual LAN 20 and rename it to Sales

```
Switch-B(config)#vlan 20

Switch-B(config-vlan)#name Sales

Switch-B(config-vlan)#exit
```

// Similar, we separate the second virtual LAN 30 and rename it to Marketing

```
Switch-B(config)#vlan 30

Switch-B(config-vlan)#name Marketing
```

Switch-B(config-vlan)#exit

// After we separate the VLAN, we have to grant the access right of that VLAN

Switch-B(config)#interface range fastEthernet0/1-8

Switch-B(config-if-range)#switchport mode access

Switch-B(config-if-range)#switchport access vlan 10

Switch-B(config-if-range)#exit

// VLAN 20

Switch-B(config)#interface range fastEthernet0/9-16

Switch-B(config-if-range)#switchport mode access

Switch-B(config-if-range)#switchport access vlan 20

Switch-B(config-if-range)#exit

// VLAN 30

Switch-B(config)#interface range fastEthernet0/17 - 24

Switch-B(config-if-range)#switchport mode access

Switch-B(config-if-range)#switchport access vlan 30

Switch-B(config-if-range)#exit

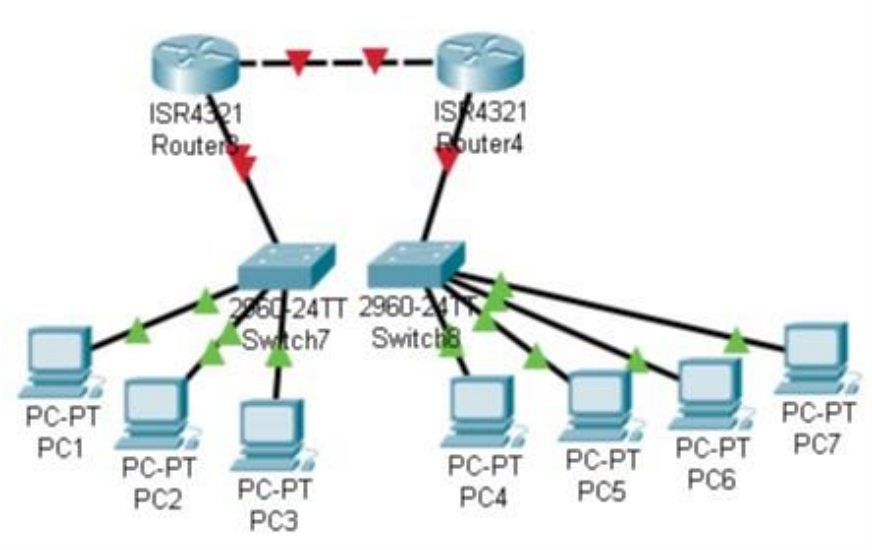
// Now, we assign the IP address for the VLAN 10

Switch-B(config)#interface vlan 10

ip address 192.168.10.1 255.255.255.0

Switch-B(config-if)#exit

b. switches & routers



I think this network consist of two routers, and each router connected to a switch that including several computers.

// first we configure switch-A and assign it IP addresses

```
! L3-Switch-A Configuration
hostname L3-Switch-A
ip routing
ip multicast-routing
interface fastEthernet0/1
 no switchport
 ip address 10.2.1.1 255.255.0.0
 ip pim dense-mode
interface fastEthernet0/2
 no switchport
 ip address 10.3.1.1 255.255.0.0
 ip pim dense-mode
interface fastEthernet0/3
```

```
 no switchport
 ip address 10.1.1.1 255.255.0.0
 ip pim dense-mode
```

// Now we declare Switch-B

```
router eigrp 10
 network 10.0.0.0
! L3-Switch-B Configuration
hostname L3-Switch-B
ip routing
ip multicast-routing
interface fastEthernet0/1
 no switchport
 ip address 10.2.1.2 255.255.0.0
 ip pim dense-mode
interface fastEthernet0/2
 no switchport
 ip address 10.4.1.2 255.255.0.0
 ip pim dense-mode
interface fastEthernet0/3
 no switchport
 ip address 10.5.1.2 255.255.0.0
 ip pim dense-mode
interface fastEthernet0/4
 no switchport
 ip address 10.6.1.1 255.255.0.0
 ip pim dense-mode
```

// Now we declare router B

```
router eigrp 10
 network 10.0.0.0
! Router-B Configuration
hostname Router-B
ip routing
interface fastEthernet0/0
 no shutdown
 ip address 10.6.1.10 255.255.0.0
 ip igmp join-group 239.1.1.1
```

// Now we declare router C

```
router eigrp 10
 network 10.0.0.0
! Router-C Configuration
hostname Router-C
ip routing
interface fastEthernet0/0
 no shutdown
 ip address 10.5.1.10 255.255.0.0
 ip igmp join-group 239.1.1.1
router eigrp 10
 network 10.0.0.0
```

3. Application