Components of network :

Router

- Router emits the wifi signals
- These are given by ISP providers, your devices will connect to this wifi, to this local network
- Internet Gateway:
    - Router act as default gateway to the internet, the internet which comes from outside needs to enter into your router, to enter into router there is a gate which is in router called as internet gateway through this it needs to enter inside.
    - since we call router is default gateway to internet.
- when ever a device connected to the router, it gets an ip address
- which component of router is gives out the ip address is DHCP service.
- it stands for *Dynamic host configuration protocol*
- Router assigns ip address to devices through Dynamically, the time period will be 24 hrs, after 24 hrs it will assign one more.
- there is a term `Lease` refers to this time period.
- can i assign a static ip :
    - every internet accesing device is having a network componet called as NIC(network interface card).
    - There is one unique hardware address assigned to NIC called as MAC address.
    - we will make an ip address static means that we will associate our ip with MAC address this make static ip.

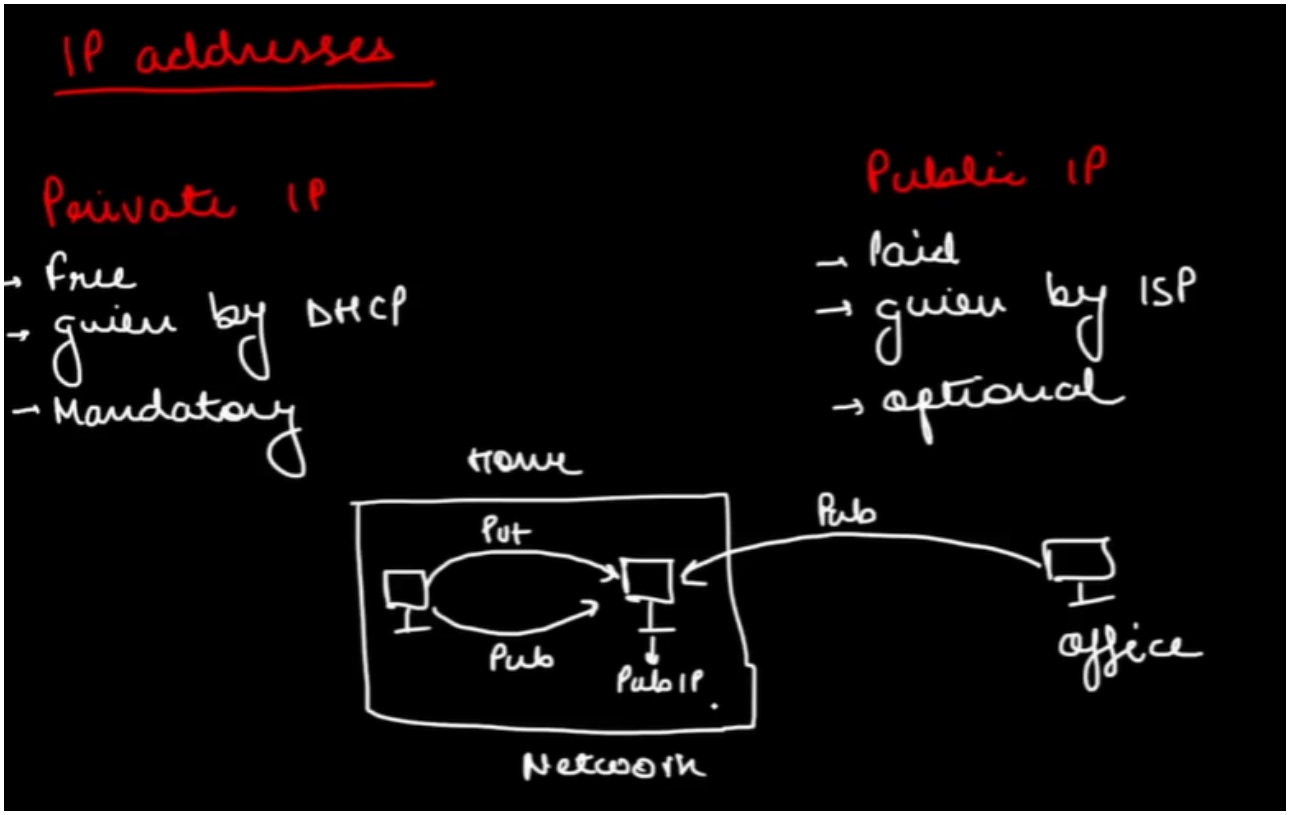
DNS(Domain Name Server)

- if you want to access google.com , we will type google.com in browser how is that happennig ?
- we know that every website are hosted in servers, these server will be having ip address, to access a website through ip address is difficult. because there are lots of ips we use daily.
- To make it easy, we have DNS we will associate a name for these ips in DNS records, whenever you type the name google.com it search in DNS server for associated ip address and sends request to that server.
- if you want to find out the google ip
    - go to cmd and type `nslookup google.com` and hit on enter this will provide you ip address of google
- similar you can find for any domain, github.com, instagram.com..etc
- IN IP we have types:
    - ipv4 - stores as 'A record'
    - ipv6 - stores as 'AAAA record'
    - Mail servers - stores as 'Mx record'
    - Text information - 'TXT record'

- Alias infomation - stores as 'CNAME reocord' (www.facebook.com --> fb.com)

IP Address

- when ever you are inside fo network you can connect to other devices through private ip and public ip.
- if you want to connect from outside you need to connect only through public ip.
- every device should have a private ip given by router to the machine through DHCP server/service.
- if two devices are connected through home wifi network, they can communicate through public ip and private ip.
- if a device from out side needs to connect to your device, your device must have public ip.
- Private ip are free and these are provided by the DHCP, public ip are paid and these are provided by the ISP.
- Have a look at image below.



CIDR

- you might have seen some where like 10.0.0.0/16 ,10.0.0.0/24, 10.0.0.0/20.
- 10.0.0.0/16
- 10.0.0.0/24
- 10.0.0.0/20
- The ip adress will have 4 bytes seperated by .
- each byte has 8 bits that means it has totally 4*8 =32 bits
- Min number : 00000000.00000000.00000000.00000000 = 0.0.0.0
- maximun number : 11111111.1111111.11111111.11111111 = 255.255.255.255

- ```
    1   1  1  1  1  1  1   1
  2^7               2^1 2^0  = 128+64+32+16+8+4+2+0 = 255
  ```

```
* how to calculate no.of ip addresses for a given ip
    * 10.0.0.0/24
        *  2^32-24 = 2^8 = 256.

* the number which represented after ip states those many bits are freezed, and
remaining is variable.
* 10.0.0.0/16 states 16 bits are frozen, 16 are variable
    * 10.0.x.x (x is variable)
    * 10.0.1.0/16:
        * 10.0.0.0/16
        * 10.0.0.1/16
        * 10.0.0.255/16
        * 10.0.1.0/16
        * 10.0.2.0/16
        * 10.0.255.0/16
        * 10.0.255.1/16
        * 10.0.255.255/16
```

- if you take 10.0.0.0/24 you will get 256 , you can't use 256 ip there are reserved ip's
    - 10.0.0.0 - network address
    - 10.0.0.1 - Default gateway
    - 10.0.0.2 ,10.0.0.3 - Virtual DNS server
    - 10.0.0.5 - Broadcast
- Subnet:
    - when we divide a large part of network into small networks these each small network is called as subnet.
    - for a large network 10.0.0.0/16(10.0.255.255) we will have (255*255 = 65536 ip's)
    - is 10.0.1.0-10.0.1.255 is a part of this large network 10.0.0.0 - 10.0.255.255 ? yes.

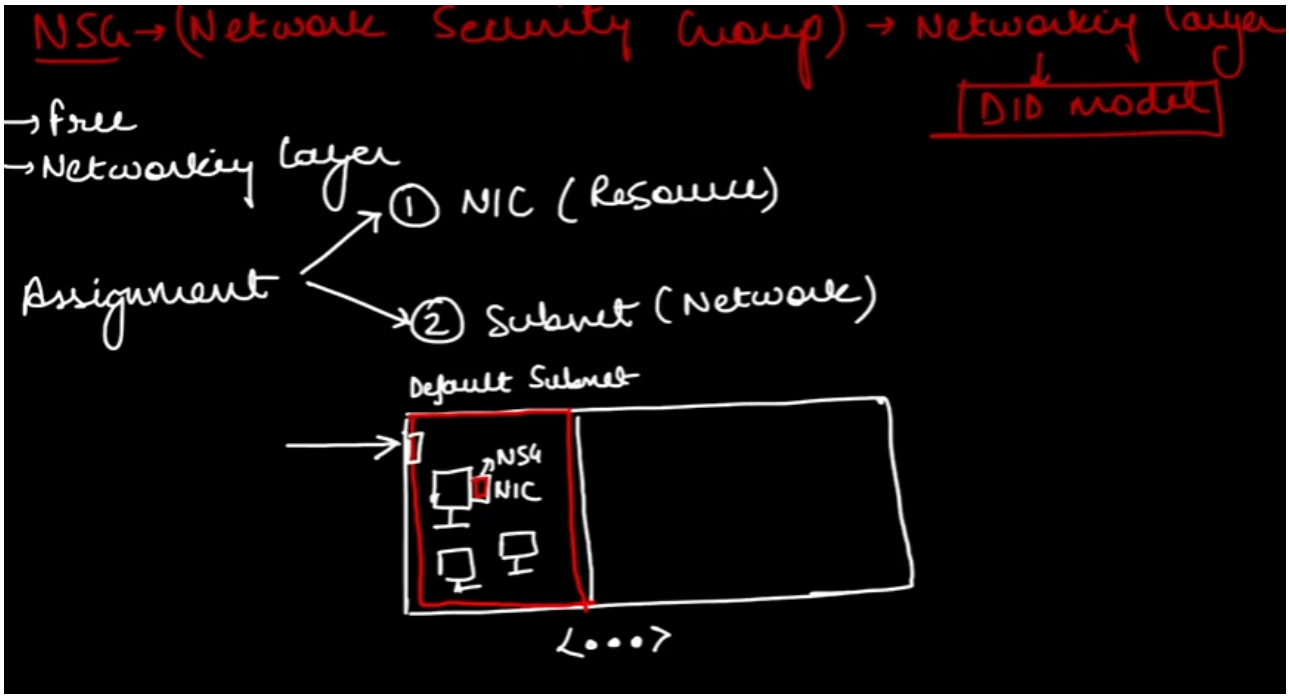
Azure Virtual Network <...>

- it is a regional resouce, we will create vnet for a region.
- private is free and public ip is paid
- there are 2 SKU's for public ip
    - Basic:
        - Static/Dynamic
        - No Zone redundancy
    - Standard:
        - Static
        - Zone redundancy
```

- if you want you can de-allocate public ip for your VM.

NSG (Network security Groups)

- To controll the traffic which is coming in and going out to your resource.
- to solve this we have NSG, this allows you to controll traffic for your resource
- This work in network layer in Defence in depth model
- it is free.
- Assignment is on two levels
    - NIC(resource)
    - Subnet (network)
- in a Vnet i have a default subnet and other subnet now we are focused on default subnet
- from image the default subnet is having 3 vms, and for one of the vm NSG is associated at NIC level, which is going to stop the traffic for that vm
- the arrow mark shows the NSG configured at subnet level which stops trafic to enter into subent level. this can enter to other two vms not for the vm associated nsg at nic level.



- How to control traffic:
- To control traffic we have somthing like Security rules and they are two types
    - Inbound Security Rule : (Traffic which is coming inside)
    - Outbound Security Rule : (Traffic which is going out)
- Inbound rule:
    - Fixed rules
        - 65000 - within Vnet

        - 65001 - Azure Load baclencer
        - 65500 - All other connections is denied.

- Outbound rule:
    - Fixed rules
        - 65000 - Allow all outbound
        - 65001 - Allow all load balencer
        - 65500 - Deny all outbound.

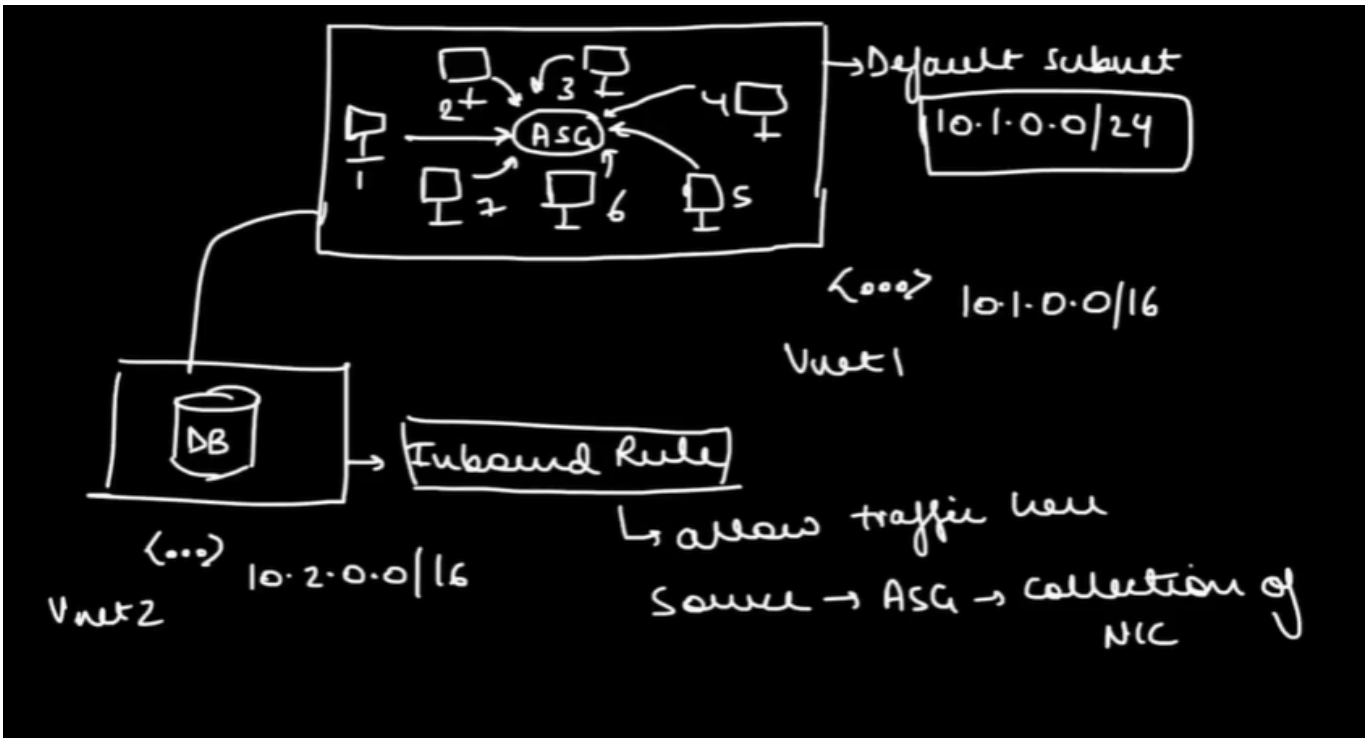
- Priority :
    - the rules will work according to priorities, lower the priority will be evaluated first checking.

- Source & Destination :
    - here we will mention that details of entering or going traffic by providing
        - through Ip range
        - can provide 1 ip
        - Any to Any
        - Application security group (ASG)
        - Service tag -> ip for PAAS - these are having fully qualified domainname

- Protocol :
    - we can select protocols
        - TCP, UDP, RDP, HTTP, HTTPS.

- Action :
    - Allow
    - Deny

- ASG (Application security group):
    - I have 2 vnets and in vnet1 i have 4 vms associated to subnet1 and in vnet2 i have a DB now to connect all the 4vms to DB, we can use a ASG as assigning all the NICs to ASG to create a inbound rule mentioning ASG, this will allow vms to access the db.



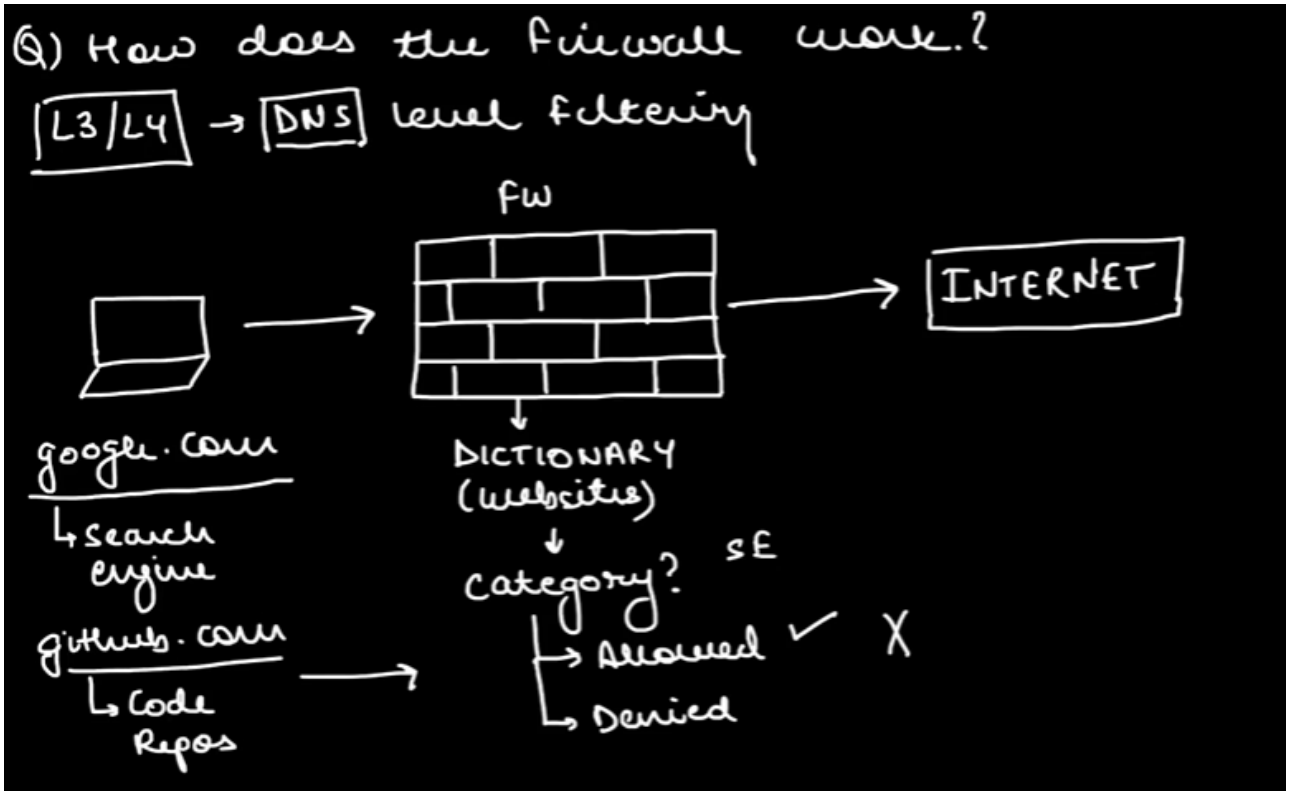
Azure Firewall

- Paid stateful firewall as a services
    - hours of usage
    - how much data you process
- SKU's:
    - Basic
        - small business
        - Filtering:
            - L3/L4(DNS)
    - Standard
        - Medium business
        - Filtering:
            - L3/L4(DNS)
    - Premium
        - MNC/Large
        - Filtering:
            - L3/L4 + L7 (DNS+ App Layer)
- How does the firewall work ?

In L3/L4 level:(DNS level Filtering) * suppose you want to access google.com from a browser, the request goes from your laptop to Firewall there , its having a dictionary there the sites are listed in catagories, now iam trying to access google.com it comes under search engines it will check whether it needs to allow or deny.

- if it is allowed then it will allow to search in internet else it will deny.
- This is called DNS level filtering.

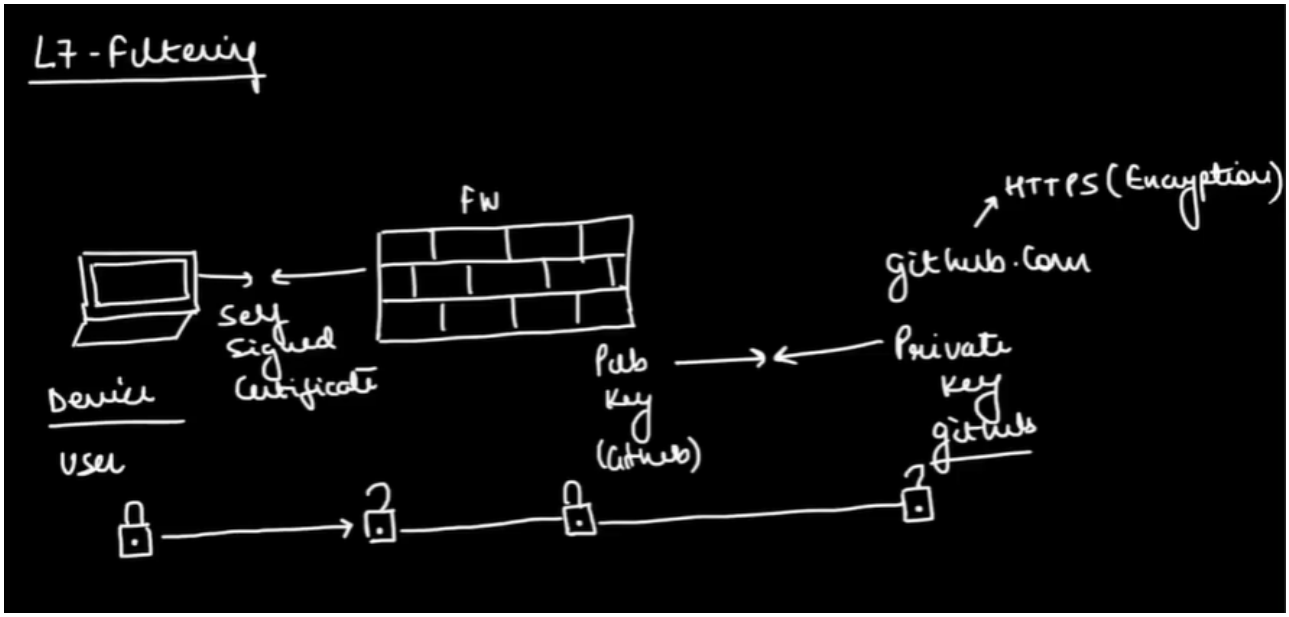
- it works on perimeter layer in defence in depth layer.



L7 Filtering

- We use L7 layer filtering to know the data which we have sent is allowed or not, this allows us to read the data at firewall if it is allowed it will be encrypted and sent to any site.
- How SSL Certificates work :
    - from our side we will create a CSR file (Certificate signing request) and we will send this to certificate authorities, which has our public key and our organisation details.
    - Using these details they will create a certificate by binding digicert private key and public key we sent, and they will give certificate to us.
    - now we will bind this to our website
    - whenever a user try to access the website our certificate will create a key on session with user and to decrypt the data user browser is having public key of certificate authorities like digicert. using this it will decrypt so user can access data.
- Now coming to firewall, when you access github.com the request will be sent from your device by encrypting using public key to the firewall (here your device and firewall is binded with self signed certificate), Firewwall can decrypt the data since private is with firewall.
- now other hand fire will be holding the github public key again the data is encryted at firewall and sent to github it will decrypt there.this is called L7 filtering

- This process we call SSL Termination/TLS interception[encrypt-decrypt-encrypt-decrypt].




```
* L7 Filtering

L7 layer filtering, or Layer 7 filtering, examines the application layer data to
determine if the transmitted data is permitted. If the data is allowed, it will be
encrypted and sent to the destination site.

* How SSL Certificates Work:

A CSR (Certificate Signing Request) file is created, which includes the public key
and organizational details. This file is sent to a Certificate Authority (CA).
The CA uses its private key and the provided public key to generate a certificate,
which is then issued back to the requester.
The certificate is then bound to the website.
When a user accesses the website, a session key is created using the website's
certificate. The user's browser, which holds the public keys of trusted CAs like
DigiCert, uses this to decrypt the data, enabling secure access.

* L7 Filtering with SSL:

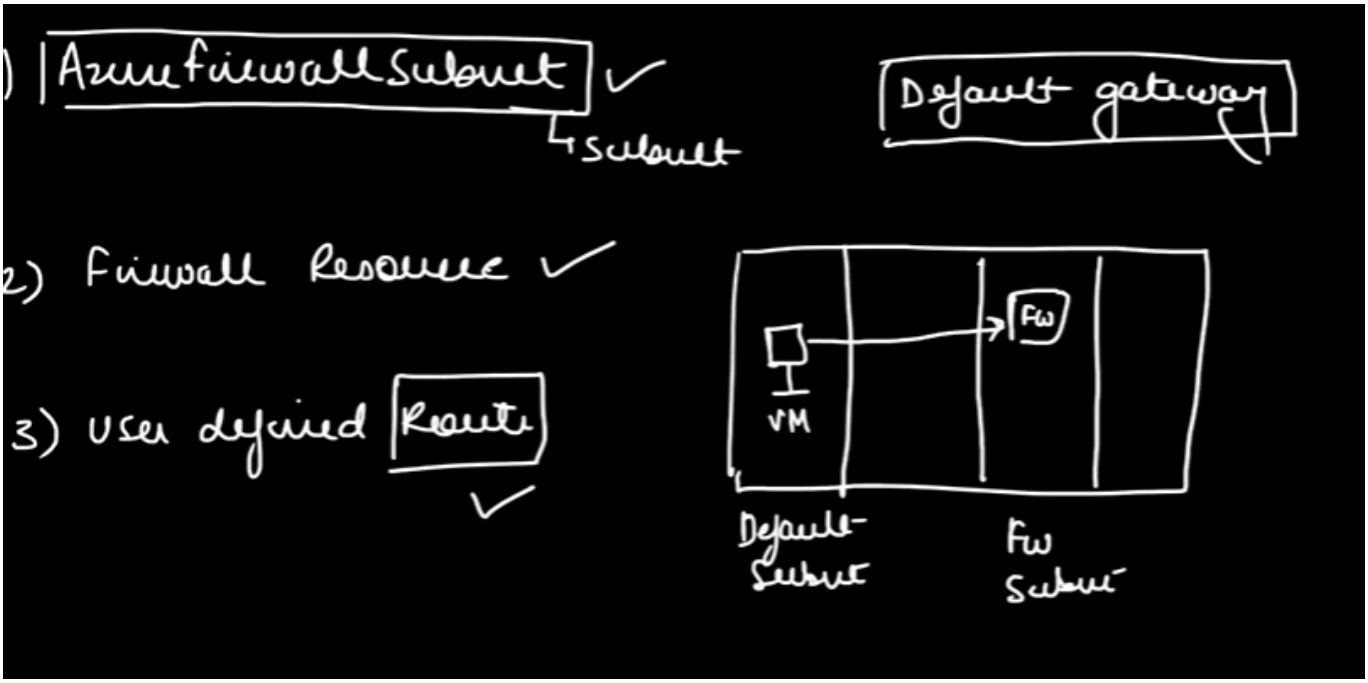
When you access a site like GitHub, your device sends an encrypted request to the
firewall using the firewall's public key (assuming a self-signed certificate setup
between your device and the firewall).
The firewall decrypts the data using its private key.
The firewall then re-encrypts the data using GitHub's public key and sends it to
GitHub.
GitHub decrypts the data using its private key. This process is known as L7
filtering.

* Certificate Authority Trust:

Websites like GitHub use SSL/TLS certificates issued by trusted Certificate
Authorities (CAs).
These certificates include the public key of the website (GitHub, in this case).
The list of trusted CAs and their public keys is pre-installed in most browsers
```

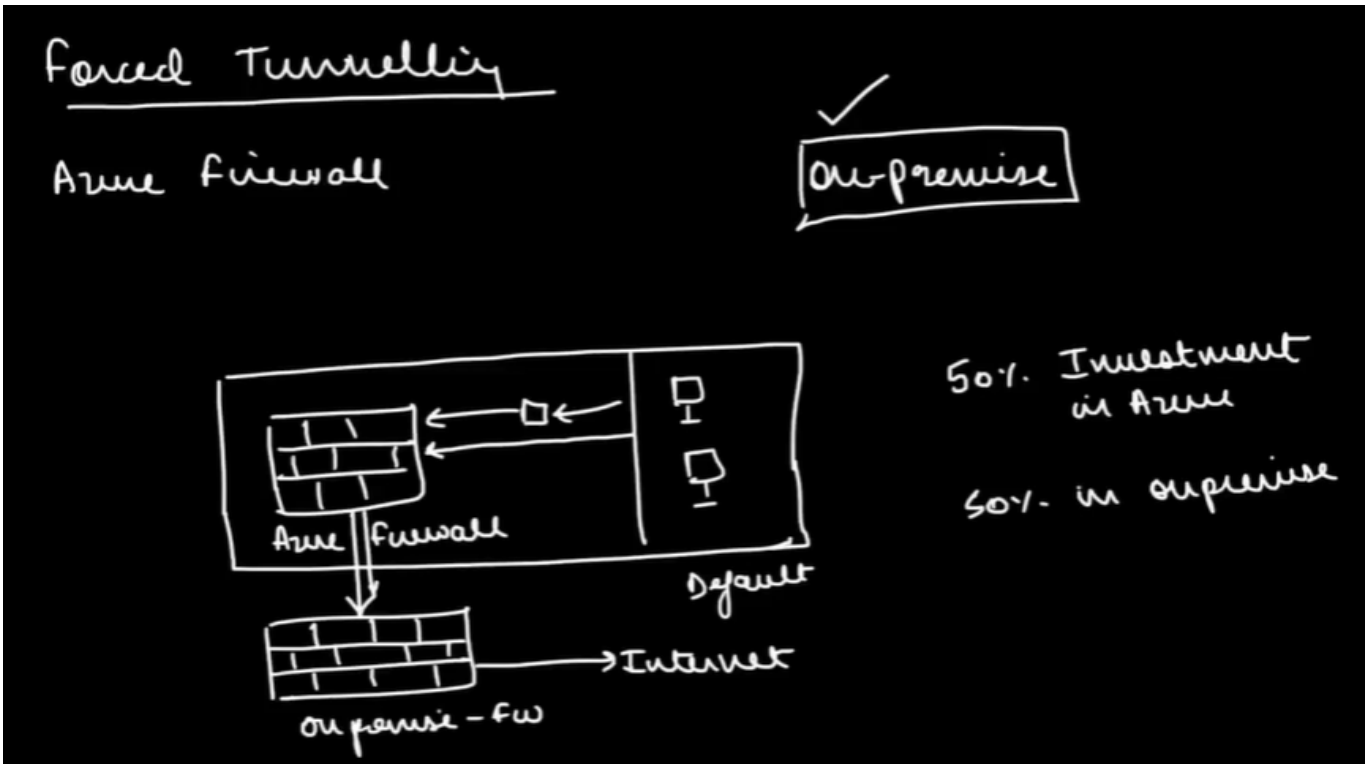
```
and operating systems. Firewalls performing SSL inspection also have access to
this list.
```

- How to create a firewall
- first we need to create Azure firewall subnet(firewall will be created in this subnet only)
- Fire wall resource
- User defined route
- scenario :
    - we have two subnets and inside of default subnet we have a vm and we have created a new subnet for Firewallsubnet
    - the traffic which is coming or going t i need to sent it through fire wall subnet since we need to create a route, else it will go normally without firewall involved.



Fourced Tunnelling

- here the traffic coming from the firewall is sent to opremise firewall and from there it sent to internet, have look at picture you will get it.



DNAT Rule(Destination Network address Translation)

- Mapping firewall Ip with ports, to hide public ip's of vms.