DAY 05 28-12-2024

* Different Parts of IP Address

- An IP address is made up of different parts, each serving a specific purpose in identifying a device on a network.
- In an IPV4 address, there are four parts, called "octets", which are seperated by dots. (e.g 192.168.1.1) Here's what each part represents.
- Network Portion : The first few sections (octets) of an IP address identify the network that the same network, allowing them to communicate with each other and share resources.
- Host Portion: The remaining Sections of the IP address specify the individual device, or "host", within that network.
- This part makes each device unique within the network, allowing the router

to distinguish b/w different devices.

The 32-bit IP address is divided into sub-classes. These are given below.

> Class A : The network ID is 8 bits long and the host ID is 24 bits long.

> Class B : The network ID is 16 bits long and the host ID is 16 bits long.

> Class C : The network ID is 24 bits long and the host ID is 8 bits long.

* How Does Subnetting Work?

- The working of Subnets starts in such a way that firstly it divides the subnets into smaller subnets.
- For communicating between subnets, routers are used.
- Each subnet allows its linked devices to communicate with each other.

- Subnetting for a network should be done in such a way that it does not affect the network bits.
- In class C the first 3 octets are network bits so it remains as it is.
- For Subnet 1: The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part (i.e)., 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.

Thus the range of Subnet 1 is: 193.1.2.0 to 193.1.2.127

Subnet id of Subnet -1 = 193.1.2.0

The direct Broadcast id of Subnet -1 is: 193.1.2.127

The total number of hosts possible is: 126 (out of 128, 2 id's are used for subnet id & direct broadcast id)

The Subnet mask of Subnet -1 is: 255.255.255.128

- For Subnet 2: The first bit chosen from the host id part is one and the range will be from (193.1.2.10000000) till you get all 1's in the host ID part (i.e) 193.1.2.11111111).
- Thus, the range of subnet-2 is : 193.1.2.128 to 193.1.2.255
- Subnet id of Subnet-2 is : 193.1.2.128
- The direct Broadcast id of Subnet-2 is: 193.1.2.255
- The total number of hosts possible is : 126 (out of 128, 2 id's are used for subnet id & Direct Broadcast id)
- The Subnet mask of Subnet-2 is: 255.255.255.12
- The best way to find out the Subnet mask of a subnet is to set the fixed bit of host-id to 1 and the rest to 0.
- finally, after using the subnetting the total number of usable hosts is reduced from 254 to 252.

Note:

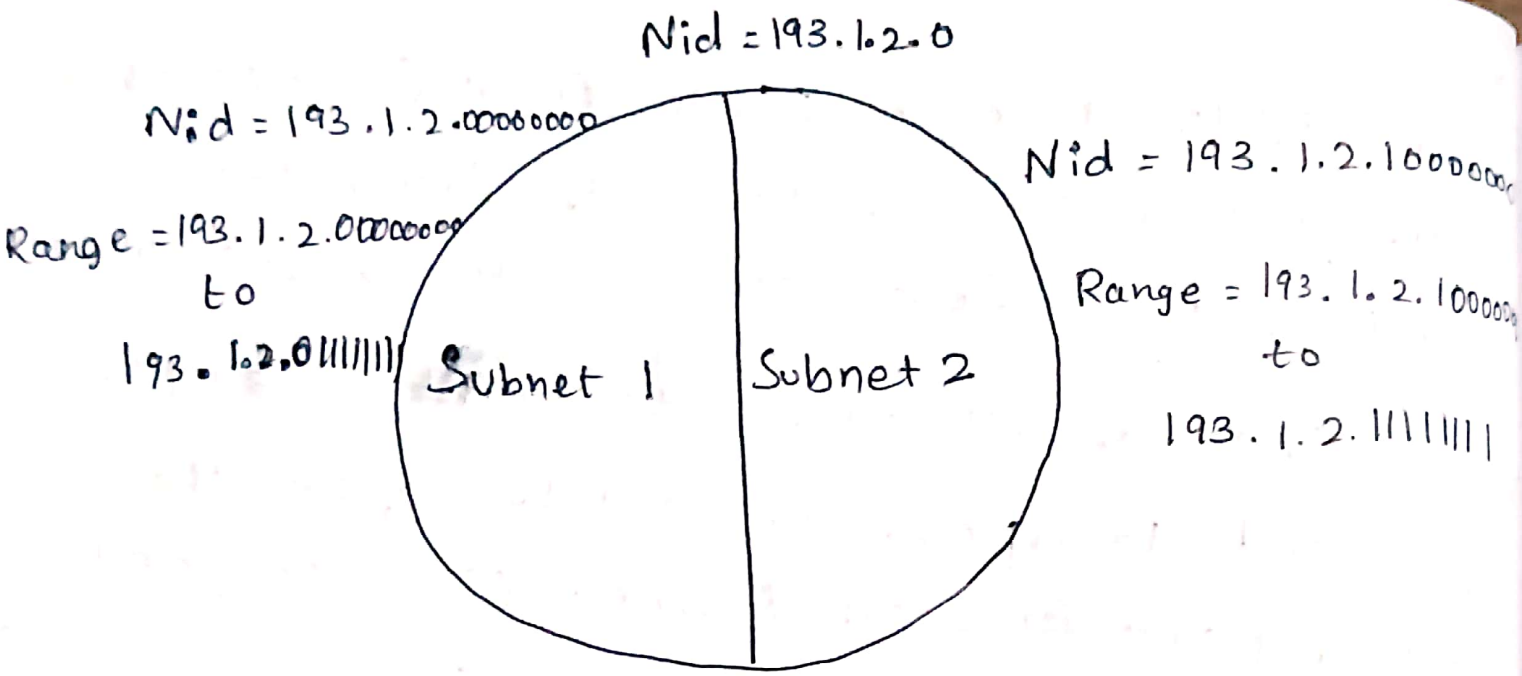
2. To divide a network into four (2^2) parts you need to choose two bits from the host id part for each subnet i.e., (00, 01, 10, 11)

3. To divide a network into eight (2^3) parts you need to choose three bits from the host id part for each subnet (i.e) (000, 001, 010, 011, 100, 101, 110, 111) and so on.

4. We can say that if the total no of subnets in a network increases the total number of usable hosts decreases.

- The network can be divided into two parts
- To divide a network into two parts, you need to choose one bit for each subnet from the host ID part.
- In the below diagram, there are two subnets.

Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.



★ Difference b/w classful and classless addressing

Parameter	classful Addressing	Classless Addressing
Basics	In classful addressing IP addresses are allocated according to the classes A to E.	Classless addressing came to replace the classful add. and to handle the issue of rapid exhaustion of IP address.
Practical	• It is less practical	• More practical
Network ID & Host ID	• It changed the network ID & host ID depends on the class.	• There is no such restriction of class in classless addressing.
VLSM	• It does not support the variable Length Subnet Mask (VLSM)	• It supports the VLSM.

Expense	Expensive as compared to classless addressing	expensive as compared to classful addressing
CIDR	It does not support classless Inter-Domain Routing (CIDR).	It supports classless Inter-Domain Routing.
updates		Triggered updates
Troubleshooting and Problem detection	Troubleshooting & Problem detection are easy than classless addressing because of the division of network, host & subnet parts in the address	It is not as easy compared to classful addressing
Division of address	• Network • Host • subnet	• Host • subnet

★ Introduction of classful IP Addressing.

- An IP Address is an address that has information about how to reach a specific host, especially outside the LAN.
- An IPaddress is a 32-bit unique address having an address space of 2^{32}.
- classful IP addressing is a way of organizing and managing I.P addresses, which are used to identify devices on a network.
- Think of IP addresses like street addresses for houses, each device on a network needs its unique address to communicate with other devices.

★ What is an IPV4 Address?

- An IPV4 address is an unique number assigned to every device that connects, to the internet or a computer network.
- It's like a home address for your Computer, Smartphone, or any other devia,

allowing it to communicate with other devices.

- Format : An IPV4 address is written as four numbers seperated by periods, like this: 192.168.1.1. Each number can range from 0 to 255.
- The IPV4 address is divided into two parts: Network ID & Host ID.
- Purpose : The main purpose of an IPV4 address is to identify devices on a network and ensure that data sent from one device reaches the correct destination.

Example : When you type a website address into your browser, your device uses the IPV4 address to find and connect to the server where the website is hosted.

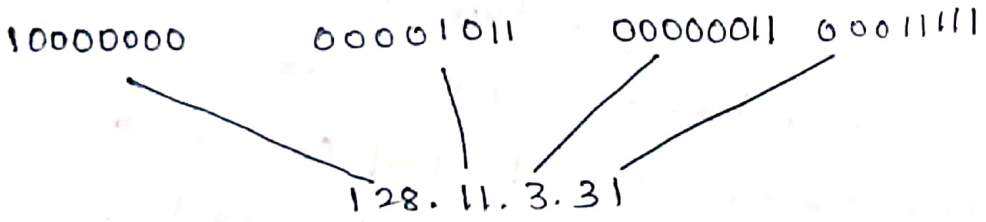
- Host ID.
- Think of an IPV4 address as a phone number for your device. Just as you dial a specific number to reach a particular person,

devices use IPV4 addresses to connect and share information.

> Two Notations - i. Dotted decimal
ii. Hexadecimal notation

Some points to be noted about (i)

- The value of any segment (byte) is blw 0 and 255 (both included).
- No zeros are preceding the value in any segment (054 is wrong, 54 is correct)



Hexadecimal Notation

01110101	00011101	10010101	11101010
75	1D	95	EA

0x751D95EA

* Need for Classful Addressing

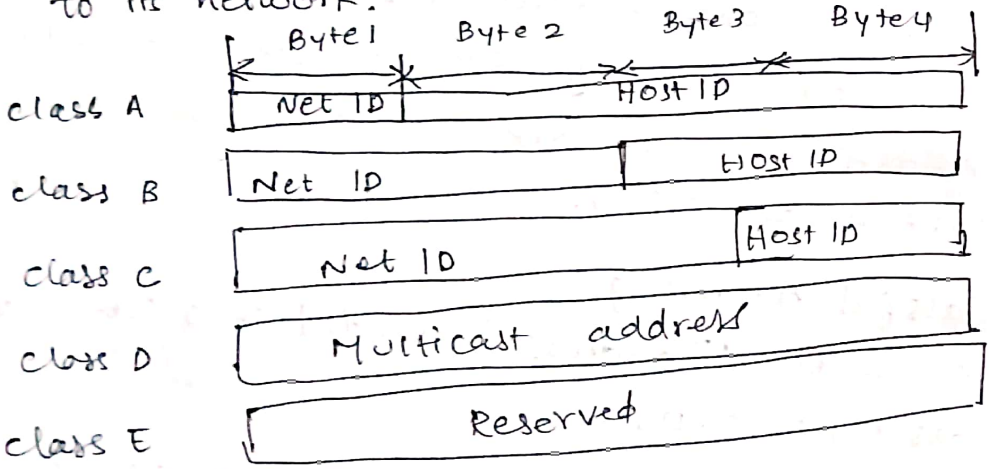
- Initially in 1980's IP address was divided into two fixed part i.e., NID (Network ID) = 8 bit, and HID (Host ID) = 24 bit.
- So, there are 2^8 that is 256 total network are created and 2^{24} that is 16M Host per network.
- There are one 256 Networks & even a small organization must buy 16M computer (Host) to purchase one network. That's why we need classfull addressing.

* Classful Addressing

The 32-bit IP address is divided in 5 sub-classes

- Class A, B, C, D, E
- Each of the classes has a valid range of IP addresses.
- Class D and E are reserved for multicast and experimental purpose.
- The order of bits in the first octet determines the classes of IP address.

- The class of IP address is used to determine the bits used for network ID & host ID and the no of total networks and hosts possible in that particular class.
- Each ISP or network administrator assigns an IP address to each device that is connected to its network.



* Range of Special IP Addresses

169.254.0.0 – 169.254.0.16 : link-local addresses

127.0.0.0 – 127.255.255.255 : Loop-back addresses

0.0.0.0 – 0.0.0.8 : used to communicate within the Current network.

* Rules for

- Host IDs are used to identify a host within a network.
- The host ID is assigned based on the following rules
- Within any network, the host ID must be unique to that network.
- A host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broad cast address to send packets to all the hosts present on that particular network.

* Rules for Assigning Network ID

- Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is

assigned the same network ID, ~~as all host on the same physical network is assigned.~~

Rules:

i. The network ID cannot start with 127 because 127 belongs to the class A address & is reserved for internal loopback functions.

ii. All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.

iii. All bits of network ID set to 0 are used to denote a specific host on the local network & are not routed and therefore aren't used.

★ CIDR Notation

- Class less Inter domain routing.

/16 /17 /18 /19 /20 /21 /22

/23 /24 /25 /96 /27 /28

eg1): VPC1 – 10.0.0.0/22 – 1024 IP addresses

Tot. no. of bits in IPv4 – 32

Bits in CIDR IP address (reserved) – 22

32 – 22 = 10, 2^{10} = 1024 IP addresses

VPC2 – 10.0.0.0/23 – 512 addresses

Tot no of bits – 32

Bits in CIDR (reserved) – 23

32 – 23 = 9, 2^9 = 512 addresses

VPC3 – 10.0.0.0/24 – 256 addresses

Tot. no of bits – 32, bits reserved – 24

32 – 24 = 8, 2^8 = 256 addressed

VPC4 – 10.0.0.0/25 – 128 addresses

Tot. ~~not~~ bits – 32, Bits reserved – 25

32 – 25 = 7, 2^7 = 128 addressed

VPC5 – 10.0.0.0/26 – 64 addresses

Tot. no. of bits = 32 bits reserved – 26

32 – 26 = 6, 2^6 = 64 address

VPC 6 - 10.0.0.0/27 - 32 addresses

Tot. no. of bits = 32

reserved = 27 => 32 - 27 = 5 so, 2^5 = 32

VPC 7 - 10.0.0.0/28 - 16 addresses

Tot = 32 reserved = 28 => 32 - 28 = 4, 2^4 = 16

VPC 8 - 10.0.0.0/21 - 2048 address

Tot. no. of bits = 32

reserved = 21 so, 32 - 21 = 11, => 2^{11} = 2048 address

VPC 9 - 10.0.0.0/20 - 4096 addresses

VPC 10 - 10.0.0.0/19 - 8192 addresses

VPC 11 - 10.0.0.0/18 - 16,384 addresses

VPC 12 - 10.0.0.0/17 - 32,768 addresses

VPC 13 - 10.0.0.0/16 - 65,536 addresses

EG1: VPC 1 - 10.0.0.0/24 - 256 IP addresses

Tot. no. of bits in IPV4 - 32

Bits in CIDR IP Address - 24

32 - 24 = 8, 2^8 = 256 IP addresses

10.0.0.0, 10.0.0.1, 10.0.0.2 .... 10.0.0.255,

EG2: VPC 2 - 10.0.0.0/23 - 512 addresses

Tot. no. of bits in IPV4 - 32

bits in CIDR IP address - 23

Bits in CIDR IP address - 23

32 - 23 = 9, 2^9 = 512 IP addresses

10.0.0.0, 10.0.0.1, 10.0.0.255][10.0.1.0, 10.0.1.1

.... 10.0.1.255;

EG: VPC - 10.0.0.0/22 - 1024 IP address

Total no. of bits in IPV4 - 32

Bits in CIDR IP address - 22

~~Bits in~~ 32 - 22 = 10, 2^{10} = 1024 IP addresses

[[10.0.0.0, 10.0.0.1, ... 10.0.0.255], [10.0.1.0, ...

10.0.1.1, ... 10.0.1.255], [10.0.2.0, ...

10.0.2.255], [10.0.3.0, 10.0.3.1, ... 10.0.3.255]

~~EG3: 10.0.0.0/21~~

~~Total = 32, bits in CIDR = 21~~

~~32 - 21 = 11, 2^{11} = 2048 IP address~~

EG3: 10.0.0.0 /21

Total = 32, bits in CIDR = 21

32 - 21 = 11 = 2^{11} => 2048 IP address

[[10.0.0.0, ... 10.0.0.255], [10.0.1.0, ... 10.0.1.255], 1024
[10.0.2.0, ... 10.0.2.255], [10.0.3.0, ... 10.0.3.255] 1024
[10.0.4.0, ... 10.0.4.255], [10.0.5.0, 10.0.5.255] 2048
[10.0.6.0, ... 10.0.6.255], [10.0.7.0, 10.0.7.255]]

EG4: 10.0.0.0 /23 - 512 address

[10.0.0.0, ... 10.0.0.255], [10.0.1.0, ... 10.0.1.255]
~~[10.0.2.0, ... 10.0.2.255], [10.0.3.0, ... 10.0.3.25~~
~~[10.0.4.0, ... 10.0.4.255], [10.0.5.255, ... 10.0.5~~
~~255]~~

EG5: 10.0.0.0/22

10.0.0.0 ... 10.0.0.255 to
10.0.1.0 ... 10.0.1.255 to
10.0.2.0 ... 10.0.2.255 to
10.0.3.0 ... 10.0.3.255

EG6: 10.0.0.0 /25 -> 128 address

10.0.0.0 to 1.0.0.0.127

EG7: 10.0.0.0/26 -> 64 address

10.0.0.0 to 10.0.0.63

EG8: 10.0.0.0 /27 -> 32 address

10.0.0.0 ... 10.0.0.31

EG9: 10.0.0.0 /28 -> 16 address

~~invalid cidr~~ 0.0 .... 10.0.~~15~~0.15

EG10: 10.0.0.0 /21

2^{11} = 2048

10.0.7.0 to 10.0.7.255

EG11: VPC 9 = 10.0.0.0 /20

10.0.0.0 to 10.0.15.255

EG12: VPC 10.0.0.0 /23

32 - 23 = 9 = 512

10.0.0.0 to 10.0.1.255

DO PAGE

EG13: VPC : 10.0.0.0 /16

10.0.0.0 to 10.0.255.255

EG14: VPC : 10.0.0.0 /17

10.0.0.0 to 10.0.127.255

EG15: VPC : 10.0.0.0 /18

10.0.0.0 to 10.0.63.255

EG16: VPC : 10.0.0.0 /19

10.0.0.0 to 10.0.31.255

30/12/2024

DAY 06

VPC 2 - 20.15.0.0 /23

Tot. no. of bits = 32, Bits in CIDR - 23 =) 32-23=9

2^9 = 512 addresses

[20.15.0.0 to 20.15.1.255]

VPC 3 - 20.15.0.0/24 - 256 addresses

[20.15.0.0 to 20.15.0.255]

VPC 4 - 20.15.0.0/25 → 128 addresses

[20.15.0.0 to 20.15.0.127]

VPC 5 - 20.15.0.0/26 → 64 address

[20.15.0.0 to 20.15.0.63]

VPC 6 - 20.15.0.0/27 → 32 address

[20.15.0.0 to 20.15.0.31]

VPC 7 - 20.15.0.0/28 → 16 address

[20.15.0.0 to 20.15.0.15]

VPC 8 - 20.15.0.0/22 - 1024 address

[20.15.0.0 to 20.15.3.255]

VPC 9 - 20.15.0.0/21 - 2048 address

[20.15.0.0 to 20.15.7.255]

VPC 10 - 20.15.0.0/20 - 4096 address

[20.15.0.0 to 20.15.15.255]

VPC 11 - 20.15.0.0/19 - 8192 address

[20.15.0.0 to 20.15.31.255]

VPC 12 - 20.15.0.0/18

[20.15.0.0 to 20.15.63.255]

VPC 13 - 20.15.0.0/17

[20.15.0.0 to 20.15.127.255]

VPC 14 - 20.15.0.0/16

[20.15.0.0 to 20.15.255.255]

EG1: VPC 1 - 20.15.0.0/22 -

Subnet 1 - 256 IP's - 20.15.0.0/24

Subnet 2 - 256 IP's - 20.15.1.0/24

Subnet 3 - 256 IP's - 20.15.2.0/24

Subnet 4 - 256 IP's - 20.15.3.0/24

EG2: VPC 2 - 20.15.0.0/21 -

Subnet 1 - 512 IP's - 20.15.0:0/23

Subnet 2 - 512 IP's - 20.15.2.0/23

Subnet 3 - 512 IP's - 20.15.4.0/23

Subnet 4 - 512 IP's - 20.15.6.0/23

EG3: VPC 3 - 20.15.0.0/20

Subnet 1 - 1024 IP's - 20.15.0.0/22

Subnet 2 - 1024 IP's - 20.15.4.0/22

Subnet 3 - 1024 IP's - 20.15.8.0/22

Subnet 4 - 1024 IP's - 20.15.12.0/22

EG4: VPC 4 - 20.15.0.0/19

Subnet 1 - 2048 IP's - 20.15.0.0/21

Subnet 2 - 2048 IP's - 20.15.8.0/21

" 3 - 2048 IP's - 20.15.16.0/21

" 4 - 2048 IP's - 20.15.24.0/21

EG5: VPC 5 - 20.15.0.0/18

Subnet 1 - 4096 IP's - 20.15.0.0/20

" 2 - 4096 IP's - 20.15.16.0/20

" 3 - 4096 IP's - 20.15.32.0/20

" 4 - 4096 IP's - 20.15.48.0/20

EG6: VPC 6 - 20.15.0.0/17

Subnet 1 - 8192 IP's - 20.15.0.0/19

" 2 - 8192 IP's - 20.15.32.0/19

" 3 - 8192 IP's - 20.15.64.0/19

" 4 - 8192 IP's - 20.15.96.0/19

EG7: VPC 7 - 20.15.0.0/16

Subnet 1 - 16384 IP's - 20.15.0.0/18

" 2 - 16384 IP's - 20.15.64.0/18

" 3 - 16384 IP's - 20.15.128.0/18

" 20.15.192.0/18

EG8: VPC 8 - 20.15.0.0/18

Subnet 1 - 4096 IP's - 20.15.0.0/20

Subnet 2 - 2048 IP's - 20.15.16.0/21

Subnet 3 - 1024 IP's - 20.15.24.0/22

Subnet 4 - 2048 IP's - 20.15.28.0/19

Subnet 5 - 1024 IP's - 20.15.36.0/22

Subnet 6 - 2048 IP's - 20.15.40.0/19

Subnet 7 - 4096 IP's - 20.15.48.0/20

EG9: VPC 9 - 20.15.0.0/16

Subnet 1 - 4096 IP's - 20.15.0.0/20

" 2 - 16384 IP's - 20.15.16.0/18

" 3 - 4096 IP's - 20.15.80.0/20

" 4 - 2048 IP's - 20.15.96.0/21

" 5 - 1024 IP's - 20.15.104.0/22

" 6 - 8192 IP's - 20.15.108.0/19

" 7 - 4096 IP's - 20.15.140.0/20

EG10: VPC 10 - 20.15.0.0/18

Subnet 1 - 2048 IP's - 20.15.0.0/21

Subnet 2 - 4096 IP's - 20.15.8.0/18

Subnet 3 - 512 IP's - 20.15.24.0/23

Subnet 4 - 1024 IP's - 20.15.26.0/22

Subnet 5 - 512 IP's - 20.15.30.0/23
Subnet 6 - 4096 IP's - 20.15.32.0/18
Subnet 7 - 1024 IP's - 20.15.48.0/22
Subnet 8 - 2048 IP's - 20.15.52.0/21

EG10: VPC 10 - 10.0.0.0/16 -

Subnet 1 - 4096 IP's - 10.0.0.0/20
Subnet 2 - 1024 IP's - 10.0.16.0/22
Subnet 3 - 8192 IP's - 10.0.20.0/19
Subnet 4 - 4096 IP's - 10.0.52.0/20
Subnet 5 - 2048 IP's - 10.0.68.0/21
Subnet 6 - 4096 IP's - 10.0.76.0/20

DAY 07 DATA CENTER TECHNOLOGY 31/12/2024

★ Data Center

- A data center is a facility of one or more buildings that house a centralized computing infrastructure, typically servers, storage and networking equipment.
- In this world of apps, big data, and digital everything, you can't stay on top of your industry without cutting-edge computing infrastructure.
- If you want to keep things in-house, the answer is the data center.
- Its primary role is to support all the crucial business applications and workloads that all organizations use to run their business.

★ Role of Data Center

- A data center is designed to handle high volumes of data and traffic with minimum latency, which makes it particularly useful for the following use cases:

> Private cloud: Hosting in-house business productivity applications such as CRM, ERP etc

> Processing big data, powering machine learning and artificial intelligence.

> High-Volume eCommerce transactions.

> Powering online gaming platforms and communities.

> Data Storage, backup, recovery and manageme

* Types of Data centers

1. Colocation

- A colocation center - also known as "carrier hotel" - is a type of data center where you can rent equipment, space, and bandwidth from the data center's owner.

For example, instead of renting a virtual machine from a public cloud provider, you can just straight-up rent a certain amount of their hardware from specified data centers.

2. Enterprise

- An Enterprise data center is a fully company-owned data center used to process internal data and host mission-critical applications.

3. Cloud

By using third-party cloud services, you can set up a virtual data center in the

cloud.

- This is a similar concepts to colocation, but you may take advantage of specific services rather than just renting the hardware and configuring it yourself.

4. Edge data center

- An Edge data center is a smaller data center that is as close to the end user as possible.
- Instead of having one massive data center, you instead have multiple smaller ones to minimize latency and lag.
- when IOT devices and low-latency data demands are high, organizations are deploying Edge computing facilities.

5. Micro Data Center

- A micro data center is essentially an edge data center pushed to the extreme.
- It can be a as small as office room, just handling the data processed in a specific region.
- Large enterprise data centers are still the most popular, but experts foresee continued growth in colocation and micro data centers.

★ Data center tier rating Breakdown

- Companies also rate data centers by tier to highlight their expected uptime and reliability.

Let's break it down:

i. Tier 1: A Tier 1 data center has a single Path for power and cooling and few, if any, redundant and backup components. It has an expected uptime of 99.671% (28.8 hrs of downtime annually).

ii. Tier 2: A Tier 2 data center has a single path for power and cooling and some redendant and backup components.

- It has an expected uptime of 99.741% (22 hrs of downtime annually).

iii. Tier 3: A Tier 3 data center has multiple paths for power and cooling and systems in place to update and maintain it without taking it offline. It has an expected uptime of 99.982%. (1.6 hrs of downtime annually).

iv. Tier 4: A Tier 4 data center ~~has~~ is built to be completely fault-tolerant and has redundancy for every component. It has an expected uptime of 99.995% (26.3 minutes of downtime annually)

* Choosing your data center locations is crucial

Here are just some of the things you must consider:

- Proximity to major markets and customers:
  - Latency and reliable connections play a major factor in running an efficient facility that meets customer demand.
- Labor costs and availability:
  - While labor costs may be good in a particular region, is there enough talent (across disciplines) needed to run and maintain your data center?
- Environmental conditions:
  - Temperature and humidity variances wreak havoc on environmental systems and forecasting.
  - Earthquakes, hurricanes, blizzards, and tornadoes are unpredictable and can shut down a facility indefinitely, keep this in mind.

- Airport and highway accessibility and quality:
  - You need large equipment and service equipment to build and maintain the data center.
  - It must also be readily accessible for delivery, services and employees.

- Availability and cost of real estate options:
  - Build versus buy requires considering building costs and quality of construction, versus incentives from landlord and local governments
  - Amount of local and state economic development incentives:
  - Beyond construction considerations, local jurisdiction may provide development incentives in rural or development areas, and less inviting in densely populated or over-resourced data areas. On the counter side of this are the taxes and

regulatory requirements that can be costly and restrictive.

- Availability of telecommunications infrastructure:
  - Make sure local providers can meet your future bandwidth demands and that there are not only redundant systems from your provider, but that you have multiple providers available.

- Cost of utilities:
  - Costs vary globally and in some and, some countries, you may not have an option of where you place your data center and considering alternative power sources is prudent and, in some countries, required.

NOTE: Cloud Related characteristics

- Scalability - Increasing the capacity of the resources. ability to increasing the

- Elasticity: The ability to increase the capacity

or decrease the capacity of the resources is known as Elasticity.

- Reliability: The ability of the resources to overcome a failover situation and continue its operations.
- Availability: copying and moving the resources to new locations for lower latency accessibility for users around that location.
- Redundancy: The ability of the resources to withstand any adverse factors and still continue its operations.

* Data center physical Security: How to keep your data safe

There are three important concepts to keep in mind when designing a policy to keep your data safe and available at all times - data security, service continuation & personnel and asset safety.

- Data security

- Data Security Systems include physical and telemetric Systems, rigid security policy adherence, and highly available redundancy make up the data protection foundation.
- These protect against physical intrusion, cyber breaches, human and environment events.

- Service Continuation

- Set up the proper architecture of power & networking systems, including redundancy, disruption simulations, and automated workflows.
- That way, you can deliver on SLAs & protect yourself against unforeseen incidents.

- Personnel and asset Safety and Preservation

- Use proven data center design practices to monitor weight and Power distribution, cable management systems to alert before

reaching safety thresholds.

* Asset Integrity Monitoring: Improve your data Center Security

- Asset integrity monitoring is a cornerstone practice for any major computing infrastructure.
- It continuously monitors your system for anomalies, and alerts you immediately for Power and environmental incidents.

> Data center teams can use them to

i. Reduce, predict, and plan for power and thermal anomalies.
ii. Identify at-risk firmware and software.
iii. Identify human errors outside security and CMP policies.
iv. Detect unauthorized hardware or software on the network.

> operations and security teams benefit from increased visibility and a simplified audit process with an accurate asset data set.

i. Automated discovery of assets and attributes
ii. Traceable lifecycle management and workflows
iii. Logged user access, date and time.
iv. Identification of unknown and non-compliant hardware and software.
v. Critical incidents and custom report queries

* How does data center Infrastructure Management (DCIM) Software Improve the data center?

- DCIM bridges the gap between facilities and IT, coordinating planning and managing through automation and transparent communication, leveraging a "single source of truth".
- What does that actually mean? All the data and controls you need to manage your data center are available in one place.

reaching safety thresholds.

* Asset Integrity Monitoring: Improve your data Center Security

- Asset integrity monitoring is a cornerstone practice for any major computing infrastructure.
- It continuously monitors your System for anomalies, and alerts you immediately for Power and environmental incidents.

>Data center teams can use them to

i. Reduce, predict, and plan for power and thermal anomalies.
ii. Identify at-risk firmware and software.
iii. Identify human errors outside security and CMP Policies.
iv. Detect unauthorized hardware or Software on the network.

> operations and Security teams benefit from increased visibility and a simplified audit process with an accurate asset dataset.

i. Automated discovery of assets and attributes
ii. Traceable lifecycle management and workflows
iii. Logged user access, date and time.
iv. Identification of unknown and non-compliant hardware and Software.
v. Critical incidents and custom report queries

* How does data center Infrastructure Management (DCIM) Software Improve the data center?

- DCIM bridges the gap between facilities and IT, Coordinating planning and managing through automation and transparent communication, leveraging a "Single Source of truth".
- What does that actually mean? All the data and controls you need to manage your data center are available in one place

(And most of the time, it controls itself perfectly without any of your input).

i. Asset Management

- From the receiving dock to decommissioning, Nlyte DCIM maximizes the production value of your assets over time.
- Capturing change at its source, Nlyte DCIM facilities timely onboarding of equipment at the time of receiving, and streamlining the decommissioning of older equipment.

ii. Workflow Automation

- Optimize your resources and personnel with measurable, repeatable, intelligent processes making individual more efficient.
- Support cross-team assignment for multi team tasks. Extend the adoption of ITIL and COBIT into the data center without any additional development or services.

iii. Bi-lateral Systems Communication

- Nlyte becomes your single source of truth for all assets, sharing information between facilities, IT, and business systems.

iv. Infrastructure and Workflow Optimization

- Designed to support your operation efficiently goals and reduce the number of ad-hoc processes at play in your data center.
- Unlock unused and under-utilized workload, space and energy capacity to maximize your ROI.

v. Space and Efficiency Planning

- Forecast and predict the future state of your data center's physical capacity based on consumption management.
- "What if" models forecast the exact capacity impact of data center projects on space, power, cooling and networks.

vi. Risk, Audit, Compliance and Reporting:

- Power failure simulations and automated workflow reduce the risk of the unknown and human error.
- Audit and reporting tools improve visibility help achieve compliance requirements.

STORAGE

★ Types of Data Center Storage - Introduction

- Data center storage, a part of data center architecture, is a collective term for the devices, software technologies, and processes that design, manage and monitor data storage within a data center.
- Apart from the devices and software technologies, data center storage also includes the policies and procedures used to govern the process of data storage and retrieval,
- for ex: Data storage security, data collection, data availability, and so on.
- Besides, data center storage must abide by the government laws and regulations related to data storage and security under some circumstances.

★ Types of Data Center Storage

- With the advancement of information technologies, companies are provided with a variety of options on data center storage, such as solid-state drives (SSDs), Cloud storage, software-defined storage etc.
- However, many data centers still rely on three traditional ways of data center storage: direct-attached storage, network-attached storage, and storage area network.
- Three types of data center storage
  i. DAS (Direct Network Storage)
  ii. NAS (Network attached storage)
  iii. SAN (Storage Area Network)

★ Direct Attached Storage (DAS)

- Direct attached storage typically refers to hard disk drives (HDDs) or Solid-state drives (SSDs) and is the most common type of data center storage.
- Just as its name shows, DAS is attached directly to a host server, instead of connecting through a network, like Ethernet.
- Besides, DAS usually connects to a computer through small computer system Interface (SCSI)
- Whether connected to a computer internally or externally, DAS is controlled by the host computer.

★ Advantages of DAS

i. cost-saving

- DAS is cheaper and the price per GB for these types of storage devices is very low, which continues to trend downward. Because of this, it is more popular in small- to medium sized businesses.

ii. Better Performance

- Compared with other networked storage solutions, DAS cannot affected by network bottlenecks such as network congestion. Therefore, the data hosted on DAS can be accessed without hindrance.

★ Disadvantages of DAS

i limited Scalability

- Because the overall configuration is too simple, DAS is easily influenced by the server.
- A server can only support few expansion slots or external ports.
- Besides, if the server fails, the data cannot be accessed.

ii. Not Shareable enough

- Since data on DAS cannot be connected through the internet, data sharing can be

a big problem.

- If the users want to share data with Someone, they have to do this through each other's computer or find another way out.

DAS

★ Network Attached Storage (NAS)

- Network Attached storage is a file-level data center storage device that supports multiple users to retrieve data from centralized disk capacity over a TCP/IP network.
- It usually has its node on the local area network (LAN), without the intervention of the application server, allowing users to access on the network.
- As a dedicated data storage server, NAS includes storage devices (such as disk arrays, CD/DVD drivers) and embedded system software supporting cross-platform file sharing.
- Besides it also supports a variety of system protocols, including Network file Protocol (NFS), common Internet file System (CIFS), file transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), etc.

★ Advantages of NAS:

i. High-efficient file sharing

- NAS enables users and applications to access and edit the files on the same hard drive easily through the network, which improves the efficiency of work a lot.

ii. Easy deployment and operation

- It can provide reliable file-level data Consolidation since file locking is handled by the device itself.

- It can also distribute NAS hosts and other devices across an enterprise's network environment.

★ Disadvantages of NAS

1. Poor Performance
2. Lack of scalability

★ Storage Area Network (SAN)

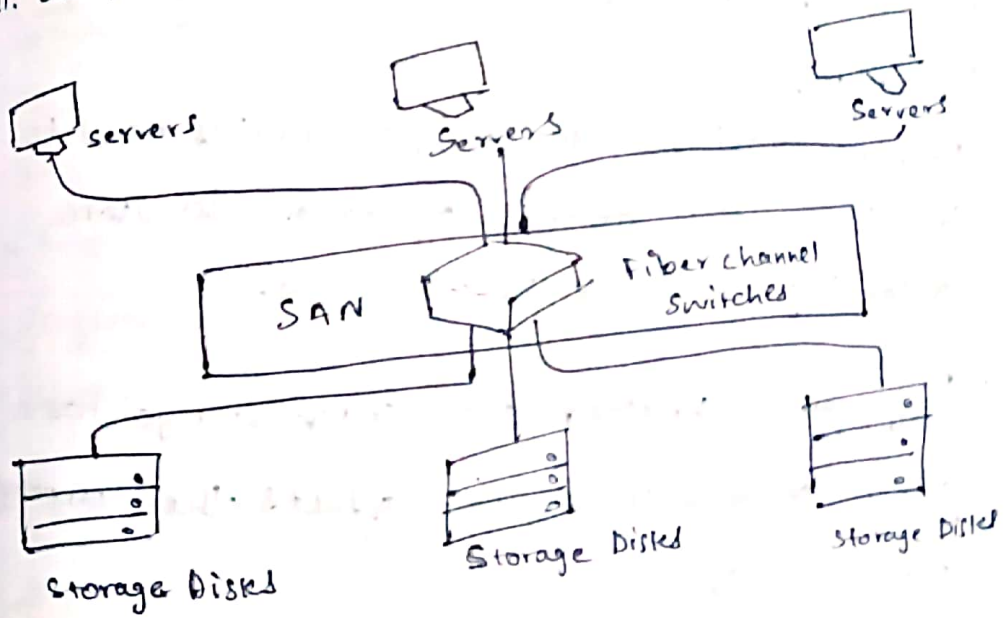
- Storage Area Network (SAN) is a dedicated and high-speed network established for Storage that is independent of the TCP/IP network.
- It connects servers to their logical disk units (LUNs) and provide block-level network access to data center storage.
- SAN typically adopts a high-end RAID array, which makes it ideal for mission-critical applications requiring high performance, data redundancy, and fault tolerance.

★ Advantages

i. High Scalability
ii. High Security

★ Disadvantages

i. High cost
ii. Complex and difficult installation.



SAN

DAY 08 01/01/2025

★ How to choose Suitable Data Center Storage?

> Scalability: The Scalability of data center storage is an important element that influences the business.

- Compared with NAS and SAN, DAS has very limited Scalability.
- Before making a decision, companies need to investigate the amount of data to store according to their requirements.

> Performance: Whether data center storage has a good performance or not affects the company's choices a lot.

- Then NAS is not a good choice if the company takes the performance of data center storage seriously.

> IT staff: Some companies may prefer data center storage which is easy to manage and deploy.

- Deploy Due to the complexity of SANs, professional IF staff is required to maintain the device, which can be a burden for some companies.

> Usage case: Because of its low price and limited IT resources, DAS is more suitable for small-to-medium-sized businesses.

- For those large enterprises looks for better performance and Scalability, NAS and SAN can better meet their needs.

FIREWALL

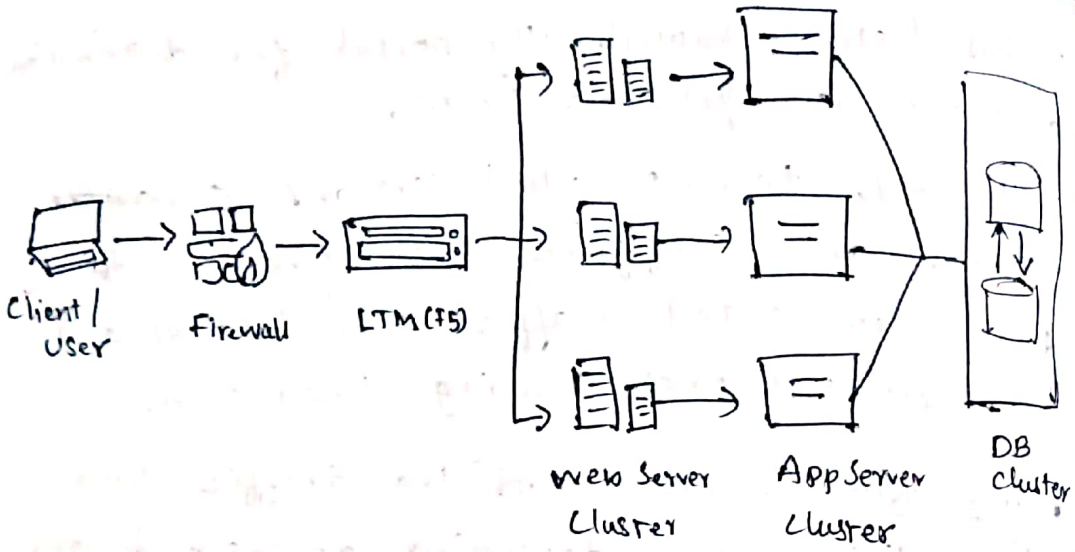
★ What is a data center firewall?

- A data center firewall is a software or hardware device that is used by data centers for maximizing security.
- It is a 5-tuple network layer that serves as a multitenant software designed networking (SDN) device.

- The purpose of a firewall is to monitor the traffic entering and exiting an organization's network.
- In the industry jargon, this network is called a perimeter.
- For fragmented network perimeter, the firewall can work at subsequently smaller levels down to the workload level, filtering out external threats.

★ How does a data center firewall work?

- Data center administrators install and configure the firewall by creating access control lists (ACLs) which are applied to a network interface or a subnet.
- They implement the firewall policies at the switch port of each tenant VM (Virtual Machine), and the network controller pushes these through the portal for distribution amongst all applicable hosts.
- This way, tenant administrators can enable and configure the firewall to divert unwanted traffic from internet and intranet networks securing their own.
- The firewall can control the traffic flow in multiple ways depending on their designs.
- Legacy architectures typically offer static packet filtering, stateful inspection, and proxy services.
- Modern-day firewalls have supplemented the architecture with advanced thread analysis, intrusion detection (IDS/IPS), and application context.
- These modern analytics make it much easier to evaluate the content of incoming traffic.



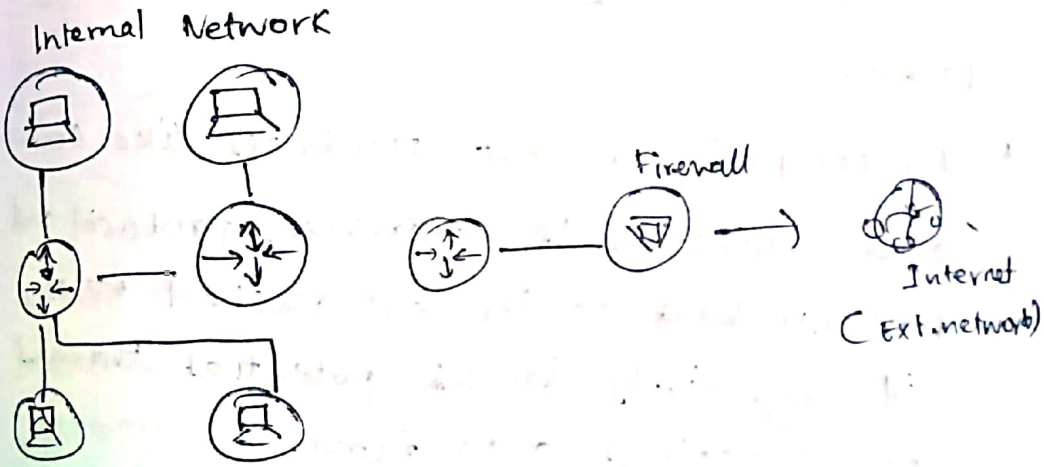
★ Types of Firewalls

- There are many types of firewalls, often categorized by system protected, form factor, network placement, and data filtering method, including

1. Network firewall
2. Host-based firewall
3. Hardware "
4. Software "
5. Internal "
6. Distributed "
7. Perimeter firewall
8. Next-generation "
9. Packet filtering "
10. circuit level gateway
11. web application "
12. Proxy "
13. Stateful inspection "

- Data filtering method – Proxy, circuit level, web app, Packet filtering, Next Generation (NG FW), Stateful inspection.
- form factors – Hardware, Software
- Network placement – Internal, distributed, Perimeter
- System Protected – Network, host-based

★ Network firewall



→ Firewall types by systems protected

1. A network firewall is positioned at the juncture between trusted and untrusted networks, such as internal systems and the internet.

2. Its primary role is to monitor, control and decide on the validity of incoming and outgoing traffic based on a predefined set of rules.

3. These rules are designed to prevent unauthorized access and maintain network integrity.

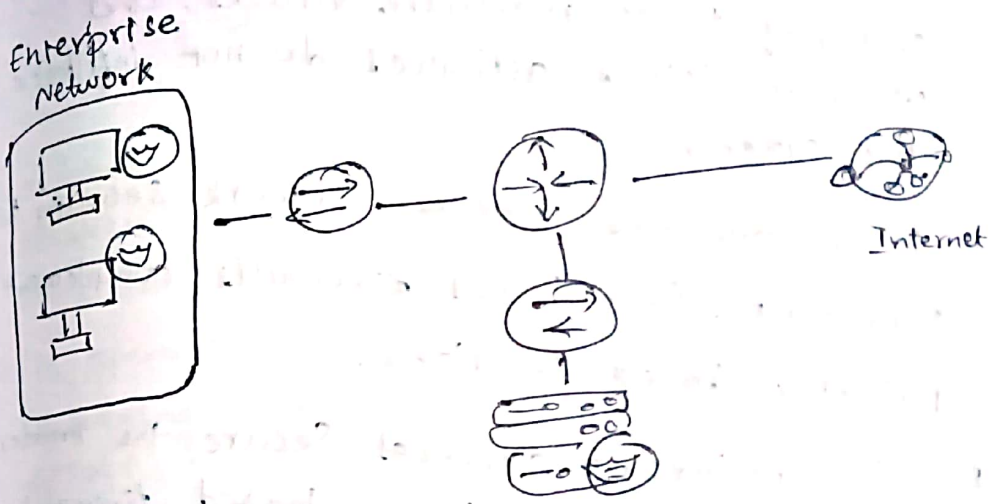
4. The operational function of a network firewall lies in its ability to scrutinize each data packet.

5. By comparing packet attributes like source and destination IP addresses, protocol and port numbers to its established rules, it effectively blocks potential threats or undesired data flow.

6. Whether implemented as hardware, software or both, its placement ensured comprehensive traffic screening.

7. Beyond simple traffic regulation, network firewalls offer logging capabilities. Logs assist administrators in tracking and probing suspicious activities.

* Host - based firewall



1. A host - based firewall is software that operated on a singular device within a network.

2. It is installed directly onto individual computers or devices, offering a focused layer of protection against potential threats.

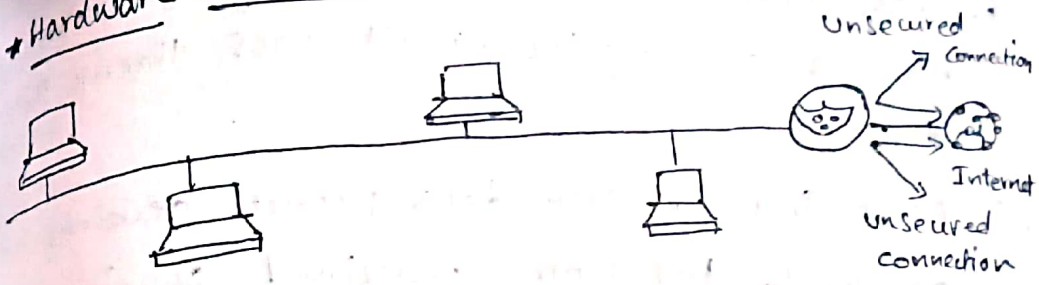
3. By examining the incoming and outgoing traffic of that specific device, it effectively filters harmful content, ensuring that malware viruses, and other malicious activities do not infiltrate the system.

4. In environments where network security is paramount, host-based firewalls complement perimeter-based solutions.

5. While perimeter defenses secure the broader network's boundaries, host-based firewalls bolster security at the device level.

6. This dual protection strategy ensures that even if a threat surpasses the network's primary defenses, individual computer remain shielded.

*Hardware firewall



LAN

1. A hardware firewall is a physical device placed between a computer or network and its connection to the internet.

2. It operates independently of the host device, examining inbound and outbound traffic to ensure compliance with set security rules.

3. By actively analyzing packets of data, the hardware firewall can identify and block threats, providing a robust barrier against potential cyber intrusions.

4. The operation of a hardware firewall involves connecting it directly between the internet source and the target network or system.

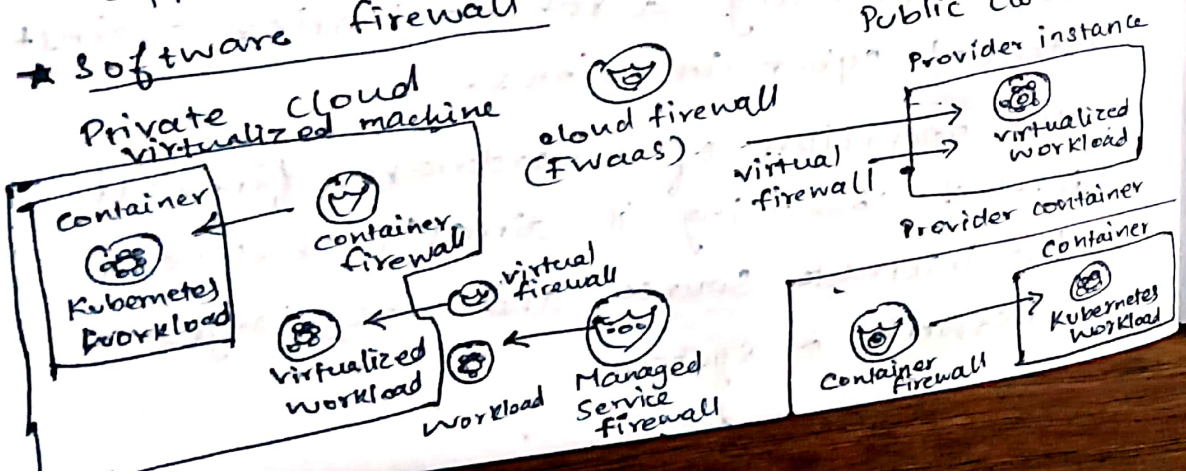
5. Once implemented, all internet traffic, whether incoming or outgoing, must pass through this device.

6. As it inspects each data packet, decisions are made based on predefined security policies.

7. Malicious or suspicious traffic is blocked, so only safe and legitimate data reaches the internal network.

8. Threats are intercepted before reaching internal systems, offering a proactive approach to network security.

★ Software firewall



★ A software firewall is a firewall in a software form factor rather than a physical appliance, which can be deployed on servers or VM to secure cloud env.

ii. Software firewall are designed to protect sensitive data, workloads and apps in env wherein it is difficult or impossible to deploy physical firewalls.

iii. Software firewalls embody the same firewall technology as hardware firewalls Called known as next-generation firewalls or NGFWs)

iv. They offer multiple deployment options to match the needs of hybrid/multi-cloud env and modern cloud app.

v. Software firewalls can be deployed into any VM or cloud environment

★ Types of Software firewalls

- Container, virtual, Cloud & managed service firewalls.

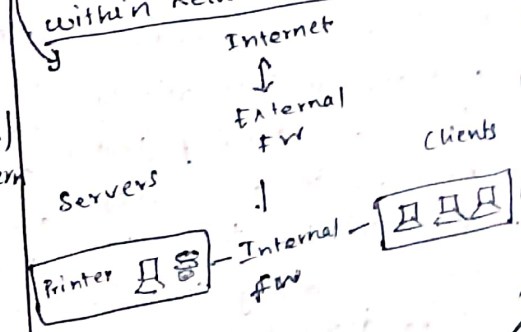
★ Hardware vs Software firewall

1. A hardware firewall is a standalone physical device positioned b/w the network & its connected devices.

2. This type of firewall runs on a security-centric OS, typically layered over generic hardware resources.

★ Internal firewall

> Firewall types by placement within network infrastructure



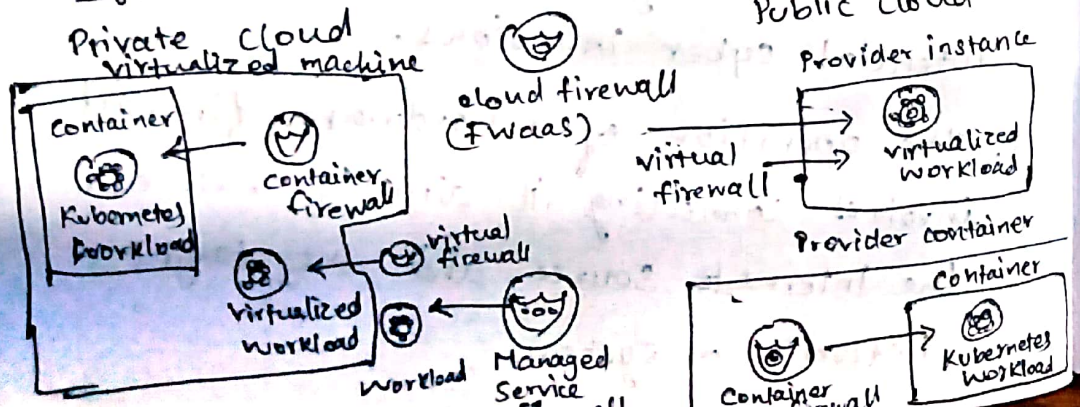
5. Once implemented, all internet traffic, whether incoming or outgoing, must pass through this device.

6. As it inspects each data packet, decisions are made based on predefined security policies.

7. Malicious or suspicious traffic is blocked, so only safe and legitimate data reaches the internal network.

8. Threats are intercepted before reaching internal systems, offering a proactive approach to network security.

★ Software firewall



i. A software firewall is a firewall in a software form factor rather than a physical appliance, which can be deployed on servers or VM to secure cloud env.

ii. Software firewall are designed to protect sensitive data, workloads and apps in env wherein it is difficult or impossible to deploy physical firewalls.

iii. Software firewalls embody the same firewall technology as hardware firewalls (also known as next-generation firewalls or NGFWs)

iv. They offer multiple deployment options to match the needs of hybrid/multi-cloud envn and modern cloud app.

v. Software firewalls can be deployed into any VM or cloud environment

★ Types of Software firewalls

- Container, virtual, Cloud & managed service firewalls.

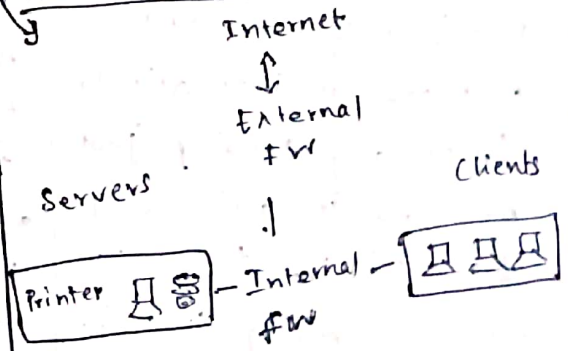
★ Hardware vs Software firewall

1. A hardware firewall is a standalone physical device positioned b/w the network & its connected devices.

2. This type of firewall runs on a security-centric OS, typically layered over generic hardware resources.

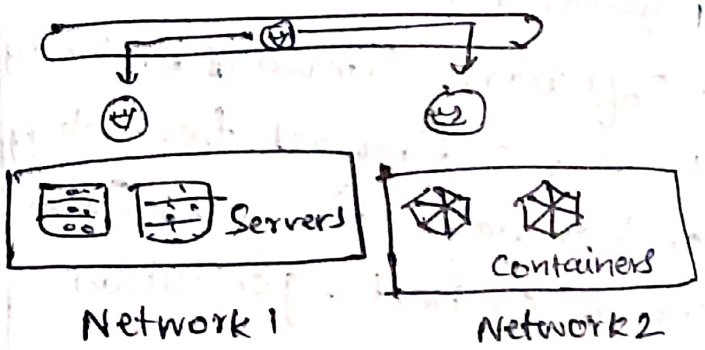
★ Internal firewall

> Firewall types by placement within network infrastructure



- An IF, functions primarily within a network's confines, targeting security threats that may have alread penetrated the perimeter defenses.
- It focuses on the traffic b/w devices within a n/w.
- This is relevant coz not all threats originate from the internet.
- Issues can arise from within an organization, be it unintentional employee errors or malicious intention.
- It operates under the Principle of zero trust.
- It doesn't automatically trust any activity just because it originates from within the n/w.
- By segmenting the n/w into distinct zones, each with its specific security measures, the firewall ensures potential threats don't spread unchecked across the entire system.
- Microsegmentation for instance, is a technique wherein the n/w is divided into smaller isolated zones, enhancing security.

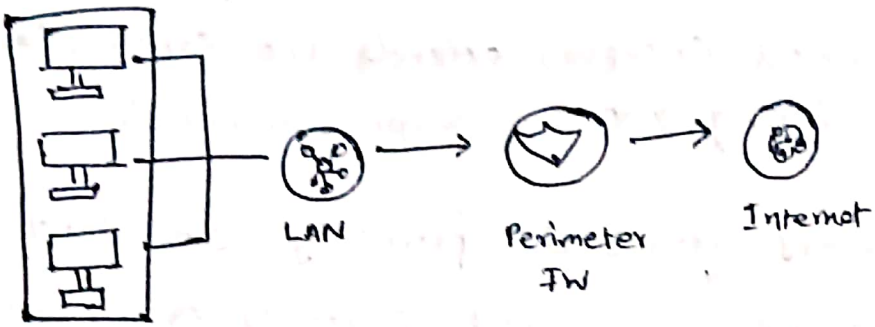
★ Distributed firewall



- A distributed firewall is a n/w security mechanism designed to safeguard an organization's entire infrastructure.
- unlike traditional firewalls, which are typically concentrated on a single node or device, distributed firewalls operate across a n/w.
- They harness the capabilities

- One primary advantage of distributed firewall is their ability to monitor both internal and external traffic.
- Distributed firewalls examine traffic both within and entering the n/w, thus offering a more comprehensive security layer.

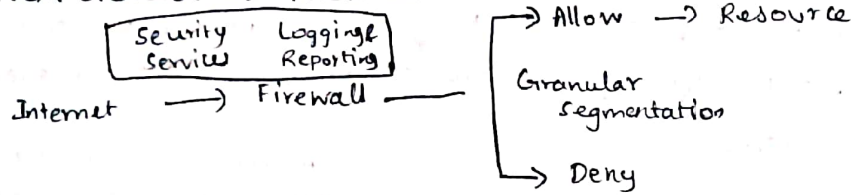
★ Perimeter Firewall



- A Perimeter Firewall establishes the boundary b/w a private n/w and the public domain of the internet.
- Functioning as the primary defense, this type of firewall meticulously inspects every data byte attempting to pass through.
- This safeguards the private n/w from unwarranted and potentially harmful data.
- A significant role of a perimeter firewall involves differentiating and subsequently allowing or disallowing traffic based on pre-defined parameters, ensuring only legitimate and safe data gain entry.
- The efficacy of a perimeter firewall hinges on its ability to recognize and discern the nature of data packets.
- It examines both the header info and the payload of each packet to determine intent.
- This level of examination aids in the identification of potential threats, like malware or indications of a looming cyberattack, facilitating timely preventive action.

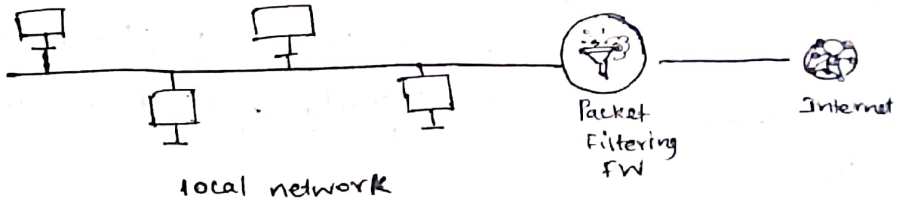
★ Firewall Types by Data filtering Method

> Next Generation Firewall



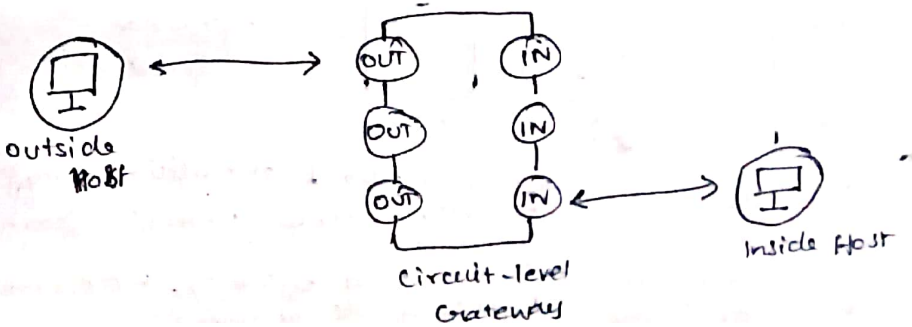
- A next-generation Firewall (NGFW) extends the capabilities of traditional firewalls, offering more comprehensive security solutions.
- Unlike their predecessors focused primarly on stateful inspection, NGFWs provide enhanced features to understand and control application traffic, integrate intrusion prevention mechanisms, and utilize cloud-sourced threat intelligence.
- This evolved approach ensures a more meticulous inspection of data packets, accounting for the intricate nuances of modern cyber threats.
- Beyond access control, NGFWs are adept at addressing modern challenges like advanced malware and sophisticated application-layer attacks.
- They delve deeper into the data, examining the nature of the traffic and identifying patterns that could signal potential threats.

★ Packet Filtering Firewall



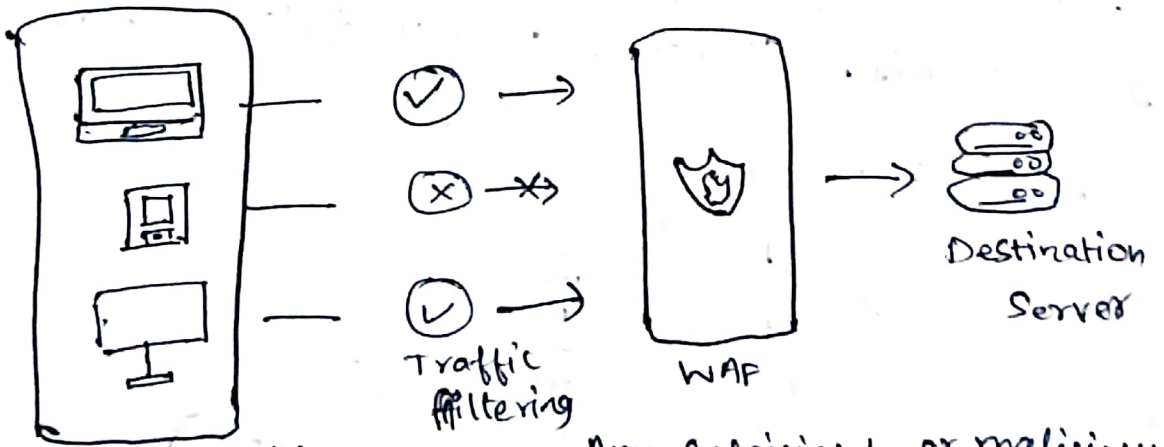
- Packet filtering firewalls operate at the network layer responsible for regulating the flow of data packets between networks.
- These firewalls rely on pre-defined rules that evaluate specific attributes of the packets such as source IP, destination IP, Ports and protocols.
- If the attributes match the established rules, the packet is allowed to pass through.
- If not, the packet is blocked.
- Types of packet filtering firewalls can be further broken down into static packet-filtering firewalls, dynamic packet-filtering firewalls, stateless packet filtering firewalls, stateful packet filtering firewalls.

★ Circuit Level Gateway



- A circuit-level gateway functions primarly at the session layer of the OSI model.
- Its role is to oversee and validate the handshaking process between packets, specifically for TCP and UDP connections.
- By examining the handshake process and the IP addresses associated with packets, this firewall identifies legitimate traffic and deters unauthorized access.
- A circuit-level gateway primarly focuses on header information, ensuring the traffic aligns with the firewall's rule set without delving into the actual content of the data packets.
- when a user seeks to initiate a connection with a remote host, the circuit level gateway establishes a circuit, which is essentially a virtual connection b/w the user and intended host. This gateway then supervises the traffic traversing this circuit.

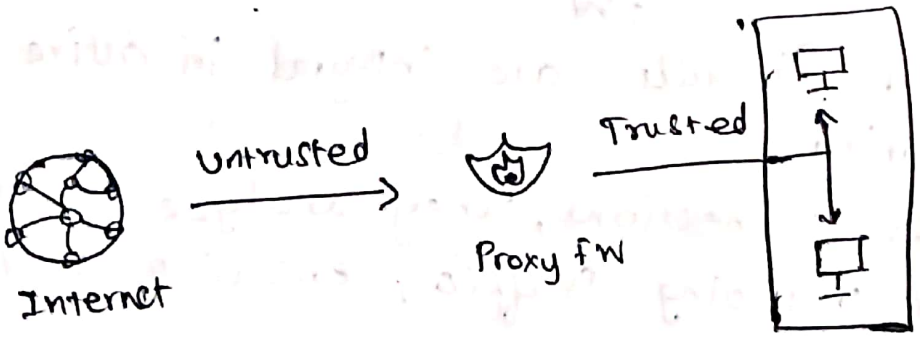
★ Web Application Firewall



- These rules discern b/w benign & Potential traffic.
- Any suspicious or malicious traffic is promptly blocked, preventing potential attacks.
- To maintain efficiency, WAFs employ Policies or sets of rules.

- A web application firewall, commonly reffered to as WAF, Serves as a specialized layer of protection of web applications, web servers, and APIs.
- It functions by examining and filtering HTTP traffic, thereby safeguarding web applications from threats like cross-site scripting (XSS), SQL injection, and file inclusion.
- WAFs differentiate themselves by operating at layer 7, specifically targeting application layer threats.
- Positioned in front of web applications, WAFs act as reverse proxies.
- This means that they intercept and inspect requests bound for the web applications, ensuring only legitimate traffic passes through.

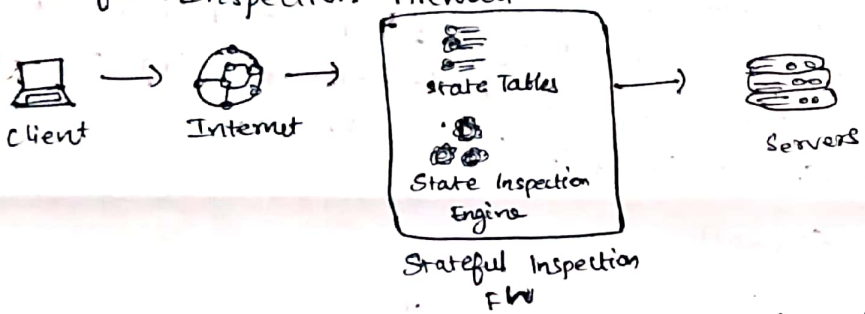
★ Proxy firewall



- A proxy firewall stands as a vital defense mechanism for networks, operating at the application layer.
- Also referred to as an application firewall or gateway firewall, it primarily functions as intermediary, filtering messages between computer systems and external servers.

- By doing so, it safeguards network resources from potential cyber threats.
- Unlike conventional firewalls, which do not decrypt or extensively inspect application protocol traffic, proxy firewalls, delve deeper.
- They scrutinize traffic entering and leaving a network, identifying signs of potential cyberattacks or malware.

★ Stateful Inspection firewall



Stateful Inspection FW

- Stateful inspection firewalls are integral in active n/w connection monitoring.
- By tracking these connections, they analyze the context of incoming and outgoing traffic, ensuring only safe packets traverse the network.
- Located at Layer 3 and 4 of the Open System Interconnection (OSI) model, their primary function is to filter traffic based on its state and context.
- This method is more thorough than mere packet-level protection because it understands the broader context of data exchanges.
- The underlying technology of a stateful firewall is its ability to perform packet inspection.
- It scrutinizes the contents of each data packet to determine if it matches the attributes of previously recognized safe connections.

★ Layer 3 vs Layer 7 Firewall

- A Layer 3 firewall functions at the network layer of the Open Systems Interconnection (OSI) model.
- It primarily focuses on filtering traffic based on parameters like IP addresses, port numbers, and specific protocols, making its approach broad and akin to router's operations.
- This type of firewall offers efficient and wide-ranging coverage, providing protection by allowing or denying packets based on their source and destination details.
- Conversely, a Layer 7 firewall operates at the application layer of the OSI model.
- Its main advantage lies in its ability to deeply inspect the content within data packets.
- By analyzing the specific contents, it can discern between benign and malicious application-specific traffic, effectively guarding against threats like SQL injection or other application layer attacks.

★ How to select or choose the right firewall for a Business Network

- It requires a clear understanding of the network architecture, protected assets, and specific organizational needs.
- Start by defining the technical objectives of the firewall.
- Determine if the network requires a comprehensive solution or if a more straightforward firewall suffices.
- It's crucial to consider the type of network, importance of assets, budget and expected traffic, for starters.
- Assess how firewall products integrate into existing infrastructure.
- Finally, be sure to consider compliance requirements and relevant data protection laws.

★ what are the 3 types of firewalls in cyber security?

- Classification of firewalls can vary based on criteria & context.

i. Packet - Filtering Firewalls: operate at the network level and use rules to allow or block data based on source and destination IP addresses, ports and protocols.

ii. Stateful inspection Firewall: Also known as dynamic packet filtering Firewalls, they not only examine packets but also keep track of active sessions and determine if the packet is part of an established connection.

iii. Proxy firewall: operate at the application layer, acting as intermediaries between users & the services they wish to access, filter data based on incoming data is a legitimate source.