**Networking**

**Network Types**

1. Personal area networks (PAN)
2. Local area networks (LAN)
3. Metropolitan area networks (MAN)
4. Wide area networks (WAN)

**Network Topologies**

1. Bus
2. Ring
3. Mesh
4. Star

**Network Standard**

Network standards are designed to ensure that hardware and software made by different vendors work seamlessly together.

**Media Access Control (MAC) Address**

* Unique identifier assigned to every network-enabled device at the time of manufacture.
* Referred to as the burned-in address, the Ethernet hardware address, or a physical address.
* Has a standard composition of six hexadecimal numbers separated by a colon or dash, for example, AA-6A-BA-2B-68-C1.
* The first three numbers of the MAC address define the manufacturer's organizationally unique identifier (OUI). The remaining three numbers uniquely identify the device.

**Network Devices**

* Repeaters
* Hubs
* Bridges
* Switches
* Routers

Nearly all of these devices depend on a media access control or an Internet Protocol (IP) address to deliver data on the network

**Repeater:**

* Regenerates Signal
* Doesn't modify or interpret data packets
* Doesn't amplify the signal. Instead, it regenerates the data packet at the original strength, bit by bit.

**Hub:**

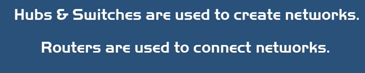
* It does not filter data.
* When a data packet comes from one device, it broadcast to multiple devices connected on this hub.
* They allow multiple Ethernet-based network-enabled devices to communicate with each other.
* It does not read MAC address of network devices. So it shares signal with all devices connected with hub which is security concern

**Switches:**

* Able to read MAC address
* Filter data based on MAC address
* Data is being sent only to matching MAC address device
* Reduces security concerns compare to Hub.

**Router:**

* Both Hub and Switch used to create LAN network, does not connect Internet. So Router comes into picture
* Used for routing data from one network to another based on IP.
* When data with IP comes to router which matches IP of data packet with intended network. If it matches, it sends data. Otherwise it routes to another different network.



**Network Address**

1. Media Access Control (MAC) address that identifies the network interface on the hardware level.

2. Internet Protocol (IP) address that identifies the network interface on a software level.

**Routing**

Routing, in the context of networks, refers to the mechanism used to make sure that data packets follow the correct delivery path between the sending and receiving device on a network.

**What is a subnet?**

A subnet defines one or more logical networks within the class A, B, or C network. Without subnets, you're restricted to a single network in each of the class A, B, or C networks. Subnets allow multiple subnetworks to exist within one network.

**Classless Interdomain Routing (CIDR) notation**

* Common way to define the subnet and the routing prefix is to use the Classless Interdomain Routing (CIDR) notation.
* CIDR applies to the IP address as the number of bits you want to allocate to your subnet.
* Using CIDR notation, at the end of the IP address, add a "/" and then the number of bits.
* For example, 198.51.100.0/24 is the same as using the dotted-decimal format subnet mask 255.255.255.0. It offers an address range of 198.51.100.0 to 198.51.100.255.

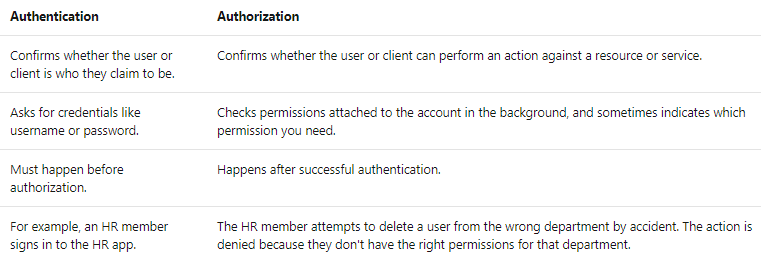
**DNS**

The Domain Name System is a decentralized lookup service that translates a human-readable domain name or URL into the IP address of the server that's hosting the site or service.

**Network Clien**t

A network client is a lightweight computer or device that can't run programs on its own. This type of client is typically used to access and interact with a mainframe computer / Server. This server is located elsewhere and is accessed through a network.

**Authentication Vs Authorization**



**Firewall**

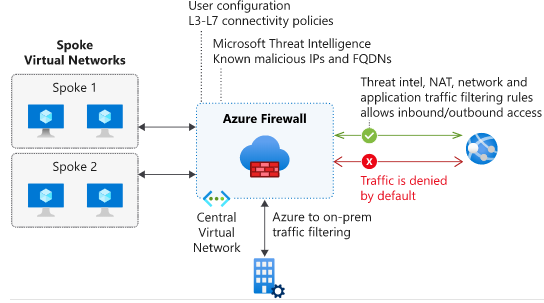
A network firewall is a security appliance that blocks or remedy unauthorized access into your network. Network firewalls also monitor and make logs of all traffic across your network.

**Network Security Group (NSG)**

* Filters traffic through security rules that you specify to deny or permit different types of traffic across your VNETs.
* You can also log all the traffic flowing through your network security groups for analysis.
* Use the Azure Network Watcher service and enable NSG flow logs.
* Your logs will then be stored for use in a JSON file in a storage account.

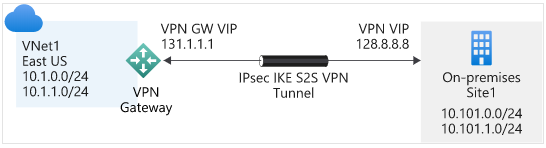
**Azure Firewall**

Azure Firewall is a fully managed firewall that you can use to protect the resources that are inside your Azure virtual networks.



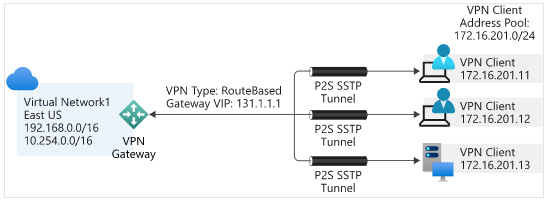
**Site-to-Site VPN**

You connect your on-premises network to your Azure virtual networks by configuring a site-to-site VPN connection with Azure. Use a VPN gateway (which is a VPN appliance from Azure), along with your local VPN device, to establish a VPN tunnel for communication. Your cloud and on-premises resources then communicate across the VPN tunnel.



**Point-to-Site VPN**

You can also set up a point-to-site VPN connection between Azure and your on-premises network. Here, individual users and clients can connect to your Azure resources through a secure tunnel.



**Network Monitor**

Network monitoring means monitoring all the components of a network, like switches, routers, servers, and firewalls. You monitor the network for performance and faults and continuously analyze the information you gather.