**Azure Virtual Network**

**Agenda:**

1. Introduction of VNet
2. Key Concepts
3. VNet Components
4. Launch an Instance using Azure VNet
5. **Introduction of Vnet:**

What Is Azure Virtual Network?

An [Azure](https://www.simplilearn.com/tutorials/azure-tutorial/what-is-azure) Virtual Network (VNet) is a network or environment that can be used to run VMs and applications in the cloud.

When it is created, the services and Virtual Machines within the Azure network interact securely with each other.

1. **Key Concepts:**

* A virtual network (VNet) allows you to specify an IP address range for the VNet, add subnets, associate network security groups, and configure route tables.
* A subnet is a range of IP addresses in your VNet. You can launch Azure resources into a specified subnet. Use a public subnet for resources that need to connect to the Internet and a private subnet for resources that won’t be connected to the Internet.
* To protect the Azure resources in each subnet, use network security groups.

**3 )Why use an Azure virtual network?**

Key scenarios that you can accomplish with a virtual network include:

* Communication of Azure resources with the internet.
* Communication between Azure resources.
* Communication with on-premises resources.
* Filtering of network traffic.
* Routing of network traffic.
* Integration with Azure services.

### Communicate with the internet:

All resources in a virtual network can communicate outbound with the internet, by default. You can also use a [public IP address](https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-public-ip-address), [NAT gateway](https://learn.microsoft.com/en-us/azure/nat-gateway/nat-overview), or [public load balancer](https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview) to manage your [outbound connections](https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections). You can communicate inbound with a resource by assigning a public IP address or a public load balancer.

When you're using only an [internal standard load balancer](https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview), outbound connectivity is not available until you define how you want outbound connections to work with an instance-level public IP address or a public load balancer.

Communicate between Azure resources:

Azure resources communicate securely with each other in one of the following ways:

* **Virtual network**: You can deploy VMs and other types of Azure resources in a virtual network. Examples of resources include App Service Environments, Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets. To view a complete list of Azure resources that you can deploy in a virtual network, see [Deploy dedicated Azure services into virtual networks](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services).
* **Virtual network service endpoint**: You can extend your virtual network's private address space and the identity of your virtual network to Azure service resources over a direct connection. Examples of resources include Azure Storage accounts and Azure SQL Database. Service endpoints allow you to secure your critical Azure service resources to only a virtual network. To learn more, see [Virtual network service endpoints](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview).
* **Virtual network peering**: You can connect virtual networks to each other by using virtual peering. The resources in either virtual network can then communicate with each other. The virtual networks that you connect can be in the same, or different, Azure regions. To learn more, see [Virtual network peering](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview).

Communicate with on-premises resources:

You can connect your on-premises computers and networks to a virtual network by using any of the following options:

* **Point-to-site virtual private network (VPN):** Established between a virtual network and a single computer in your network. Each computer that wants to establish connectivity with a virtual network must configure its connection. This connection type is useful if you're just getting started with Azure, or for developers, because it requires few or no changes to an existing network. The communication between your computer and a virtual network is sent through an encrypted tunnel over the internet. To learn more, see [About point-to-site VPN](https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about?toc=/azure/virtual-network/toc.json).
* **Site-to-site VPN**: Established between your on-premises VPN device and an Azure VPN gateway that's deployed in a virtual network. This connection type enables any on-premises resource that you authorize to access a virtual network. The communication between your on-premises VPN device and an Azure VPN gateway is sent through an encrypted tunnel over the internet. To learn more, see [Site-to-site VPN](https://learn.microsoft.com/en-us/azure/vpn-gateway/design?toc=/azure/virtual-network/toc.json#s2smulti).
* **Azure ExpressRoute**: Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic doesn't go over the internet. To learn more, see [What is Azure ExpressRoute?](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction?toc=/azure/virtual-network/toc.json).

Filter network traffic:

You can filter network traffic between subnets by using either or both of the following options:

* **Network security groups**: Network security groups and application security groups can contain multiple inbound and outbound security rules. These rules enable you to filter traffic to and from resources by source and destination IP address, port, and protocol. To learn more, see [Network security groups](https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview) and [Application security groups](https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups).
* **Network virtual appliances:** A network virtual appliance is a VM that performs a network function, such as a firewall or WAN optimization. To view a list of available network virtual appliances that you can deploy in a virtual network, go to [Azure Marketplace](https://azuremarketplace.microsoft.com/marketplace/apps/category/networking?page=1&subcategories=appliances).

Route network traffic:

Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the internet, by default. You can implement either or both of the following options to override the default routes that Azure creates:

* **Route tables**: You can create [custom route tables](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#user-defined) that control where traffic is routed to for each subnet.
* **Border gateway protocol (BGP) routes**: If you connect your virtual network to your on-premises network by using an [Azure VPN gateway](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview?toc=/azure/virtual-network/toc.json) or an [ExpressRoute](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-routing?toc=/azure/virtual-network/toc.json#dynamic-route-exchange) connection, you can propagate your on-premises BGP routes to your virtual networks.

Integrate with Azure services:

Integrating Azure services with an Azure virtual network enables private access to the service from virtual machines or compute resources in the virtual network. You can use the following options for this integration:

* Deploy [dedicated instances of the service](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services) into a virtual network. The services can then be privately accessed within the virtual network and from on-premises networks.
* Use [Azure Private Link](https://learn.microsoft.com/en-us/azure/private-link/private-link-overview) to privately access a specific instance of the service from your virtual network and from on-premises networks.
* Access the service over public endpoints by extending a virtual network to the service, through [service endpoints](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview). Service endpoints allow service resources to be secured to the virtual network.

1. **VNet Components:**

* NAT Gateway
* Allows your virtual network resources to have an outbound-only connection.
* A NAT gateway resource can use up to 16 static IP addresses.
* You can use multiple subnets in a NAT gateway.
* Route tables are used to determine where network traffic is directed.
* A subnet can only be associated with one route table.
* If multiple routes contain the same address prefix, the selection will be based on the following priority: User-defined route, BGP route, and System route.
* You can connect VNets to each other using VNet peering.
* If you need to connect privately to a service, you can use Azure Private Endpoint powered by Azure Private Link.

**VNet Use Case:**

* VNet with a single public subnet.
* VNet with public and private subnets (NAT).

**Subnets:**

* When you create a VNet, you must specify a range of IPv4 addresses for the VNet in the form of a CIDR block (example: 10.0.0.0/16).
* A CIDR block must not overlap with any existing CIDR block that’s associated with your VNet.
* You can add multiple subnets in each Availability Zone of your VNet’s region.
* Types of subnets:
  + Public subnet
  + Private subnet
  + Gateway subnet
* Private - Instances can access the Internet with NAT (Network Address Translation) gateway that is present in the public subnet.
* Public - Instances can directly access the internet.
* The CIDR block size of an IPv4 address is between a /16 netmask (65,536 IP addresses) and /29 netmask (8 IP addresses).
* The 5 reserved addresses in each CIDR block is not available for you to use, and cannot be assigned to any virtual machines.
* You can delegate a subnet to be used by a dedicated service.

**Security:**

* Network Security Groups – controls the inbound and outbound traffic of Azure resources.
  + The rules are processed from lowest to highest numbers.
  + You can set a number between 100 and 4096.
  + The rules can be applied to both inbound or outbound traffic.
  + You can allow or deny incoming or outgoing traffic.
  + When you create a network security group, Azure assigns default security rules for inbound and outbound traffic.
  + Can be attached to a subnet or a network interface. Refrain from attaching a network security group to both subnet and network interface.
* You may use service tags on network security rules to minimize the complexity of frequent updates.
* Augmented security rules allow you to create a single rule with multiple source and destination IPs.
* Application Security Group – allows you to define a VMs group network security policy.
* You can use IP flow verify of Azure Network Watcher to check which network security rule allows or denies the traffic.
* With VNet service endpoint policy, you can filter the egress VNet traffic to Azure Storage.

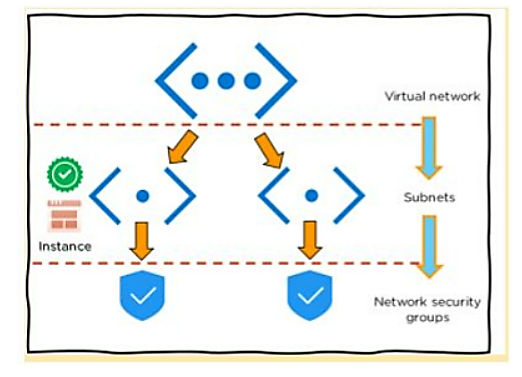
**Routing:**

* It delivers the data by choosing a suitable path from source to destination.
* For each subnet, the virtual network automatically routes traffic and creates a routing table.

**Network Security Groups:**

* It is a firewall that protects the virtual machine by limiting network traffic.
* It restricts inbound and outbound network traffic depending upon the destination [IP addresses](https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-an-ip-address), port, and protocol.

1. **How to Launch an Instance using Azure VNet?**

****

* First, create a virtual network in the [Azure cloud](https://www.simplilearn.com/azure-cloud-services-and-its-importance-article)
* Next, create subnets into each virtual network
* Now, assign each subnet with the respective instance or Virtual Machine
* After which you can connect the instance to a relevant Network Security Group
* Finally, configure the properties in the network security and set policies
* As a result, you will be able to launch your instance on Azure
* Moving forward, we will see a demonstration on creating an Azure virtual machine and virtual network step-by-step.