Azure Virtual Network in AVD

Agenda:

Section 2:

1) Introduction of VNet
2) Key Concepts
3) VNet Components
4) Launch an Instance using Azure VNet
5) Manage connectivity to the internet and on-premises networks
6) Understanding Azure Virtual Desktop network connectivity

1) Introduction of Vnet:

What Is Azure Virtual Network?

An 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.

2) 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, NAT gateway, or public load balancer to manage your 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, 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.
- **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.
- **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.

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.
- **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.
- **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?.

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 and 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.

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 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 or an ExpressRoute 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 into a virtual network. The services can then be privately accessed within the virtual network and from on-premises networks.
- Use Azure Private Link 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. Service endpoints allow service resources to be secured to the virtual network.

3) 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.

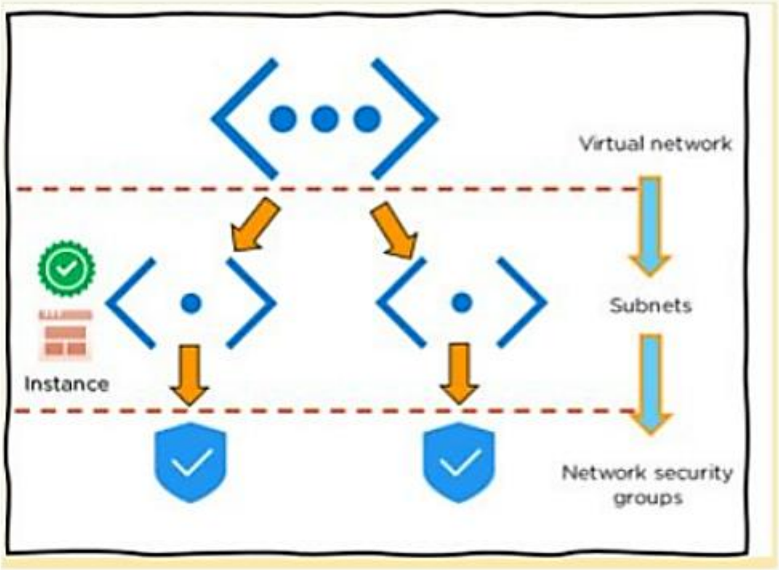
Routing:

- 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, port, and protocol.

4) How to Launch an Instance using Azure VNet?



- First, create a virtual network in the Azure cloud
- 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.

5) Manage connectivity to the internet and on-premises networks:

You can connect your on-premises computers and networks to a virtual network using any combination 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.
- Ideal for just getting started with Azure, or for developers, because it requires little or no changes to your existing network.
- The communication between your computer and a virtual network is sent through an encrypted tunnel over the internet.
- **Site-to-site VPN**: Established between your on-premises VPN device and an Azure VPN Gateway that is deployed in a virtual network.
- 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.
- **Azure ExpressRoute**: Established between your network and Azure, through an ExpressRoute partner.
- This connection is private. Traffic does not go over the internet.

Filter network traffic

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

- **Network security groups (NSGs)**: Network security groups and application security groups can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.
- **Network virtual appliance (NVA)**: A network virtual appliance is a VM that performs a network function, such as a firewall, WAN optimization, or other network function

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 Azure creates:

- **Route tables**: You can create custom route tables with routes 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 using an Azure VPN Gateway or ExpressRoute connection, you can propagate your on-premises BGP routes to your virtual networks.

Virtual network integration for Azure services

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

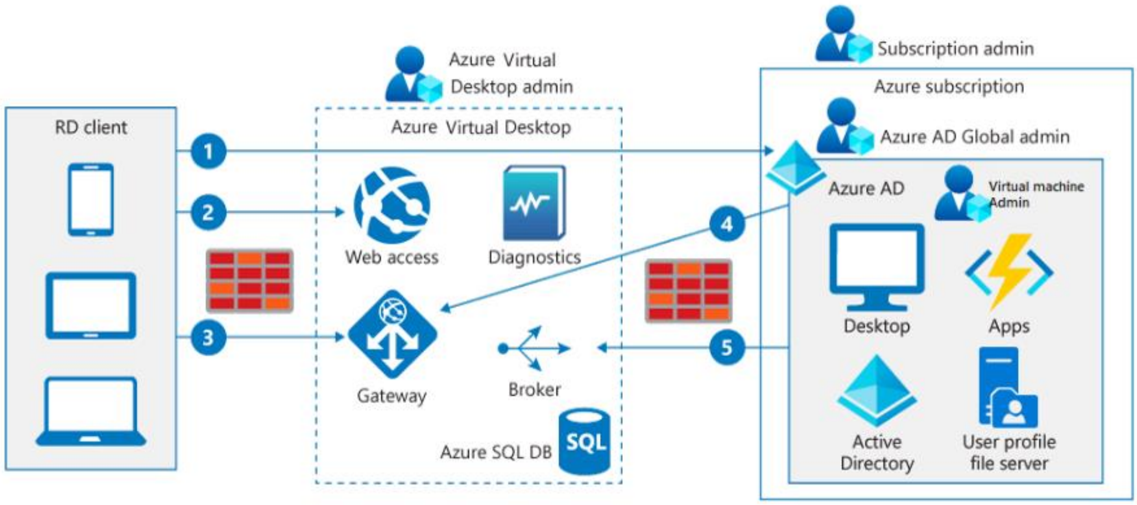
- Deploying dedicated instances of the service into a virtual network. The services can then be privately accessed within the virtual network and from on-premises networks.
- Using Private Link to access privately a specific instance of the service from your virtual network and from on-premises networks.
- You can also access the service using public endpoints by extending a virtual network to the service, through service endpoints. Service endpoints allow service resources to be secured to the virtual network.

6) Understanding Azure Virtual Desktop network connectivity

Azure Virtual Desktop uses Remote Desktop Protocol (RDP) to provide remote display and input capabilities over network connections.

The connection data flow for Azure Virtual Desktop starts with a DNS lookup for the closest Azure datacenter.

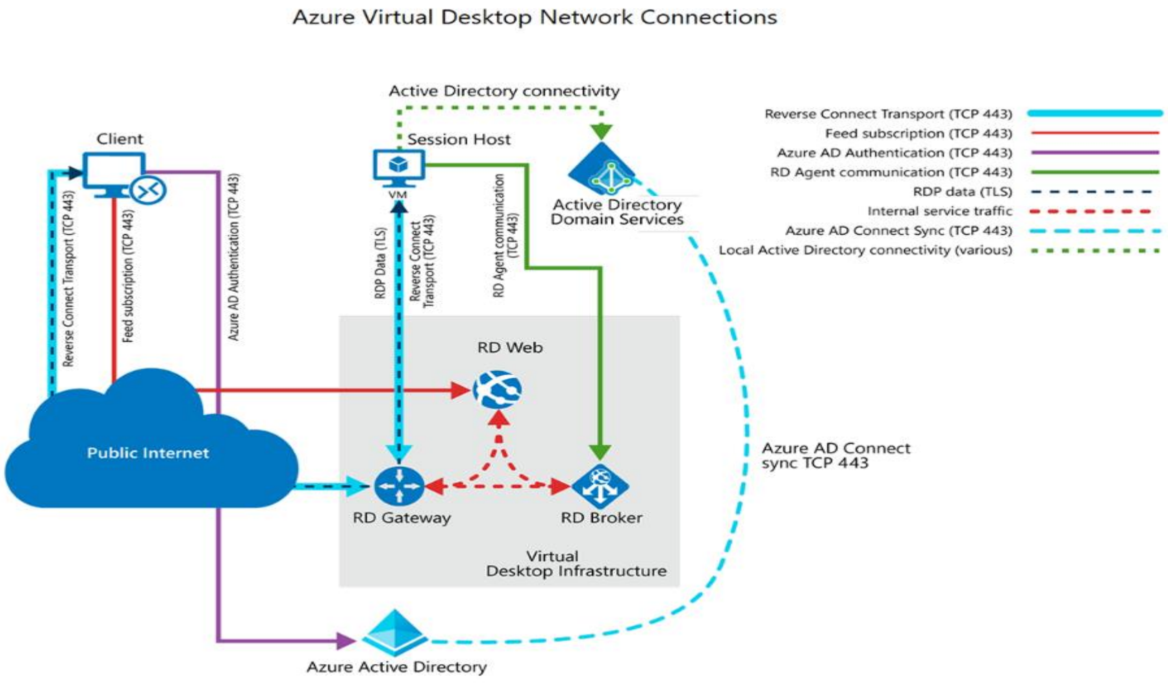
The following image shows the five-step connection process for Azure Virtual Desktop running in Azure.



- When authenticated in Microsoft Entra ID, a token is returned to the Remote Desktop Services client.
- The gateway checks the token with the connection broker.
- The broker queries the Azure SQL database for resources assigned to the user.
- The gateway and the broker select the session host for the connected client.
- The session host creates a reverse connection to the client by using the Azure Virtual Desktop gateway.

The inbound ports aren't opened and the gateway is acting as an intelligent reverse proxy. The gateway manages all session connectivity.

Azure Virtual Desktop hosts the client on the session hosts running on Azure. Microsoft manages portions of the services on the customer's behalf and provides secure endpoints for connecting clients and session hosts. The diagram below gives a high-level overview of the network connections used by Azure Virtual Desktop


Azure Virtual Desktop Network Connections
Active Directory connectivity
Session Host
VM
Client
Active Directory Domain Services
Reverse Connect Transport (TCP 443)
Feed subscription (TCP 443)
Azure AD Authentication (TCP 443)
RD Agent communication (TCP 443)
RDP data (TLS)
Internal service traffic
Azure AD Connect Sync (TCP 443)
Local Active Directory connectivity (various)
RDP Data (TLS)
Reverse Connect Transport (TCP 443)
RD Agent communication (TCP 443)
RD Web
Public Internet
RD Gateway
RD Broker
Virtual Desktop Infrastructure
Azure AD Connect sync TCP 443
Azure Active Directory

Session connectivity

Azure Virtual Desktop uses Remote Desktop Protocol (RDP) to provide remote display and input capabilities over network connections. RDP has initially released with Windows NT 4.0 Terminal Server Edition and was continuously evolving with every Microsoft Windows and Windows Server release. From the beginning, RDP developed to be independent of its underlying transport stack, and today it supports multiple types of transport.

Reverse connect transport

Azure Virtual Desktop is using reverse connect transport for establishing the remote session and for carrying RDP traffic. Unlike the on-premises Remote Desktop Services deployments, reverse connect transport doesn't use a TCP listener to receive incoming RDP connections. Instead, its'using outbound connectivity to the Azure Virtual Desktop infrastructure over the HTTPS connection.

Session host communication channel

Upon startup of the Azure Virtual Desktop session host, the Remote Desktop Agent Loader service establishes the Azure Virtual Desktop broker's persistent communication channel. This communication channel on a secure Transport Layer Security (TLS) connection serves as a bus for service message exchange between the session host and Azure Virtual Desktop.

Client connection sequence

Client connection sequence described below:

1)Using supported Azure Virtual Desktop client user subscribes to the Azure Virtual Desktop Workspace.

2) Microsoft Entra authenticates the user and returns the token used to enumerate resources available to a user.

3) Client passes token to the Azure Virtual Desktop feed subscription service.

4) Azure Virtual Desktop feed subscription service validates the token.

5) Azure Virtual Desktop feed subscription service passes the list of available desktops and RemoteApps back to the client with a digitally signed connection.

6) Client stores the connection configuration for each available resource in a set of rdp files.

7) When a user selects the resource to connect, the client uses the associated rdp file and establishes the secure TLS 1.2 connection to the closest Azure Virtual Desktop gateway instance.

8) Azure Virtual Desktop gateway validates the request and asks the Azure Virtual Desktop broker to orchestrate the connection.

9) Azure Virtual Desktop broker identifies the session host and uses the previously established persistent communication channel to initialize the connection.

10) Remote Desktop stack initiates the TLS 1.2 connection to the same Azure Virtual Desktop gateway instance as used by the client.

11) After both client and session host connected to the gateway, the gateway starts relaying the raw data between both endpoints. Establishing the base reverse connect transport for the RDP.

12) After the base transport is set, the client starts the RDP handshake.

Connection security

TLS 1.2 is used for all connections initiated from the clients and session hosts to the Azure Virtual Desktop infrastructure components.

For reverse connect transport, both client and session host connect to the Azure Virtual Desktop gateway. With the TCP connection in place, the client or session host validates the Azure Virtual Desktop gateway's certificate.

RDP establishes a nested TLS connection between client and session host using the session host's certificates.

By default, the certificate used for RDP encryption is self-generated by the OS during the deployment.

Azure Virtual Desktop RDP Shortpath for managed networks

RDP Shortpath for managed networks is a feature of Azure Virtual Desktop that establishes a direct UDP-based transport between Remote Desktop Client and Session host. RDP uses this transport to deliver Remote Desktop and RemoteApp while offering better reliability and consistent latency.

- RDP Shortpath transport is based on the Universal Rate Control Protocol (URCP). URCP enhances UDP with active monitoring of the network conditions and provides fair and full link utilization. URCP operates at low delay and loss levels as needed by Remote Desktop.
- RDP Shortpath establishes the direct connectivity between the Remote Desktop client and the session host. Direct connectivity reduces dependency on the Azure Virtual Desktop gateways, improves the connection's reliability, and increases available bandwidth for each user session.
- The removal of extra relay reduces round-trip time, which improves user experience with latency-sensitive applications and input methods.
- RDP Shortpath brings support for configuring Quality of Service (QoS) priority for RDP connections through Differentiated Services Code Point (DSCP) marks.
- RDP Shortpath transport allows limiting outbound network traffic by specifying a throttle rate for each session.