AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Monitor and manage performance and health
14. Plan and implement updates, backups, and disaster recovery

Microsoft

Implement and manage networking for Azure Virtual Desktop

Introduction

In this module, you will learn to:

- Describe Azure Virtual Desktop network connectivity
- Analyze connection quality in Azure Virtual Desktop
- Describe Remote Desktop Protocol (RDP) bandwidth requirements Managed
- Configure RDP Shortpath for Azure Virtual Desktop sample scenarios ←
- Plan and implement Quality of Service for Azure Virtual Desktop
- Plan an Azure Private Link solution for Azure Virtual Desktop
- Create an RDP connection to a Windows VM using Azure Bastion

:443

SH
:3389

Understanding Azure Virtual Desktop network connectivity

VPN Device

IPsec
TLS

Virtual GW

Azure

You can connect your on-premises computers and networks to a virtual network using any combination of:

- **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 doesn't go over the internet.

AZ-700

Analyze connection quality in Azure Virtual Desktop

Connection network and graphics data

- The connection network and graphics data that Azure Log Analytics collects can help you discover areas that impact your end user's graphical experience.
- The service collects data for reports regularly throughout the session.
- You can also use RemoteFX network performance counters to get some graphics-related performance data from your deployment, but they're not as comprehensive as Azure Log Analytics.

Azure Virtual Desktop connection network data reports have the following advantages:

- Each record is connection-specific and includes the correlation ID of the connection that can be tied back to the user.
- The round-trip time measured in the table is protocol-agnostic and will record the measured latency for TCP or UDP connections.

Connection network data

The network data you collect for your data tables using the *NetworkData* table includes the following information:

- **Estimated available bandwidth (kilobytes per second)** is the average estimated available network bandwidth during each connection time interval.
- **Estimated round-trip time (milliseconds)** is the average estimated round-trip time during each connection time interval. Round-trip time is how long a network request takes to go from the end -user's device to the session host through the network, then return from the session host to the end-user device.
- **Correlation ID** is the *ActivityId* of a specific Azure Virtual Desktop connection that's assigned to every diagnostic within that connection.
- **Time generated** is a timestamp in UTC time that marks when an event the data counter is tracking happened on the VM. All averages are measured by the time window that ends at the marked timestamp.
- **Resource ID** is a unique ID assigned to the Azure Virtual Desktop host pool associated with the data the diagnostics service collects for the table.
- **Source system**, **Subscription ID**, **Tenant ID**, and **type** (table name).

Remote Desktop Protocol (RDP) bandwidth requirements

RDP uses compression algorithms for different types of data.

Type of Data	Direction	How to estimate
Remote graphics	Session host to client	See the detailed guidelines.
Heartbeats	Bidirectional	~ 20 bytes every 5 seconds.
Input	Client to session host	Amount of data is based on the user activity, less than 100 bytes for most of the operations.
File transfers	Bidirectional	File transfers are using bulk compression. Use .zip compression rates for an approximation.
Printing	Session host to client	Print job transfer depends on the driver and using bulk compression, use .zip compression rates for an approximation.

Other scenarios can have their bandwidth requirements depending on how you use them, such as:

- Voice or video conferencing
- Real-time communication
- Streaming 4K video

Estimating Bandwidth Used by Remote Graphics

RDP delivers the graphics generated by the remote server to display it on a local monitor.

- A 1080p desktop image in its uncompressed form is about 8Mb in size.
- Displaying this image on the locally connected monitor with a modest screen refresh rate of 30Hz requires bandwidth of about 237 Mbps.

To reduce the amount of data transferred over the network, RDP uses the combination of multiple techniques:

- Frame rate optimizations
- Screen content classification
- Content-specific codecs
- Progressive image encoding
- Client-side caching

RDP Shortpath for Azure Virtual Desktop

RDP Shortpath is used in two ways:

Managed networks: direct connectivity is established between the client and the session host when using a private connection, such as a virtual private network (VPN). A connection using a managed network is established in one of the following ways:

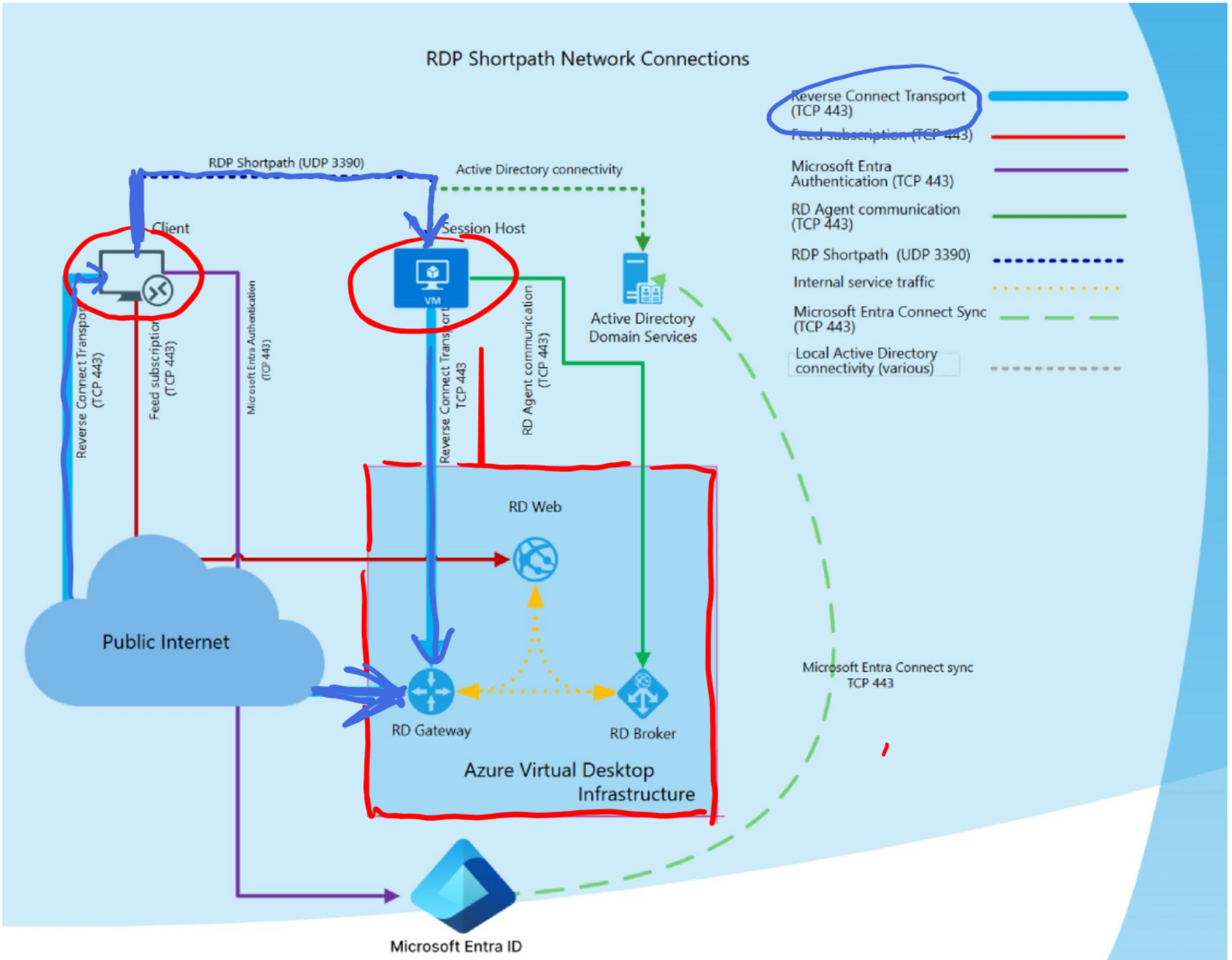
- A *direct* UDP connection between the client device and session host, where you need to enable the RDP Shortpath listener and allow an inbound port on each session host to accept connections.
- A *direct* UDP connection between the client device and session host, using the Simple Traversal Underneath NAT (STUN) protocol between a client and session host. Inbound ports on the session host aren't required to be allowed.

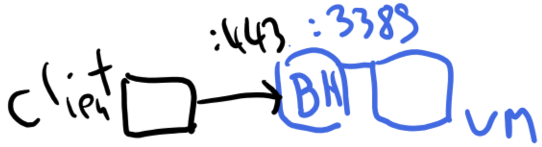
Public networks: direct connectivity is established between the client and the session host when using a public connection. There are two connection types when using a public connection:

- A direct UDP connection using the Simple Traversal Underneath NAT (STUN) protocol between a client and session host.
- An indirect UDP connection using the Traversal Using Relay NAT (TURN) protocol with a relay between a client and session host.

How RDP Shortpath works for managed networks = VPN

1. The session host sends the list of its IPv4 and IPv6 addresses to the client.
2. The client starts the background thread to establish a parallel UDP-based transport directly to one of the session host's IP addresses.
3. While the client is probing the provided IP addresses, it continues to establish the initial connection over the reverse connect transport to ensure there's no delay in the user connection.
4. If the client has a direct connection to the session host, the client establishes a secure connection using TLS over reliable UDP.
5. After establishing the RDP Shortpath transport, all Dynamic Virtual Channels (DVCs), including remote graphics, input, and device redirection, are moved to the new transport.
   - If a firewall or network topology prevents the client from establishing direct UDP connectivity, RDP continues with a reverse connect transport.

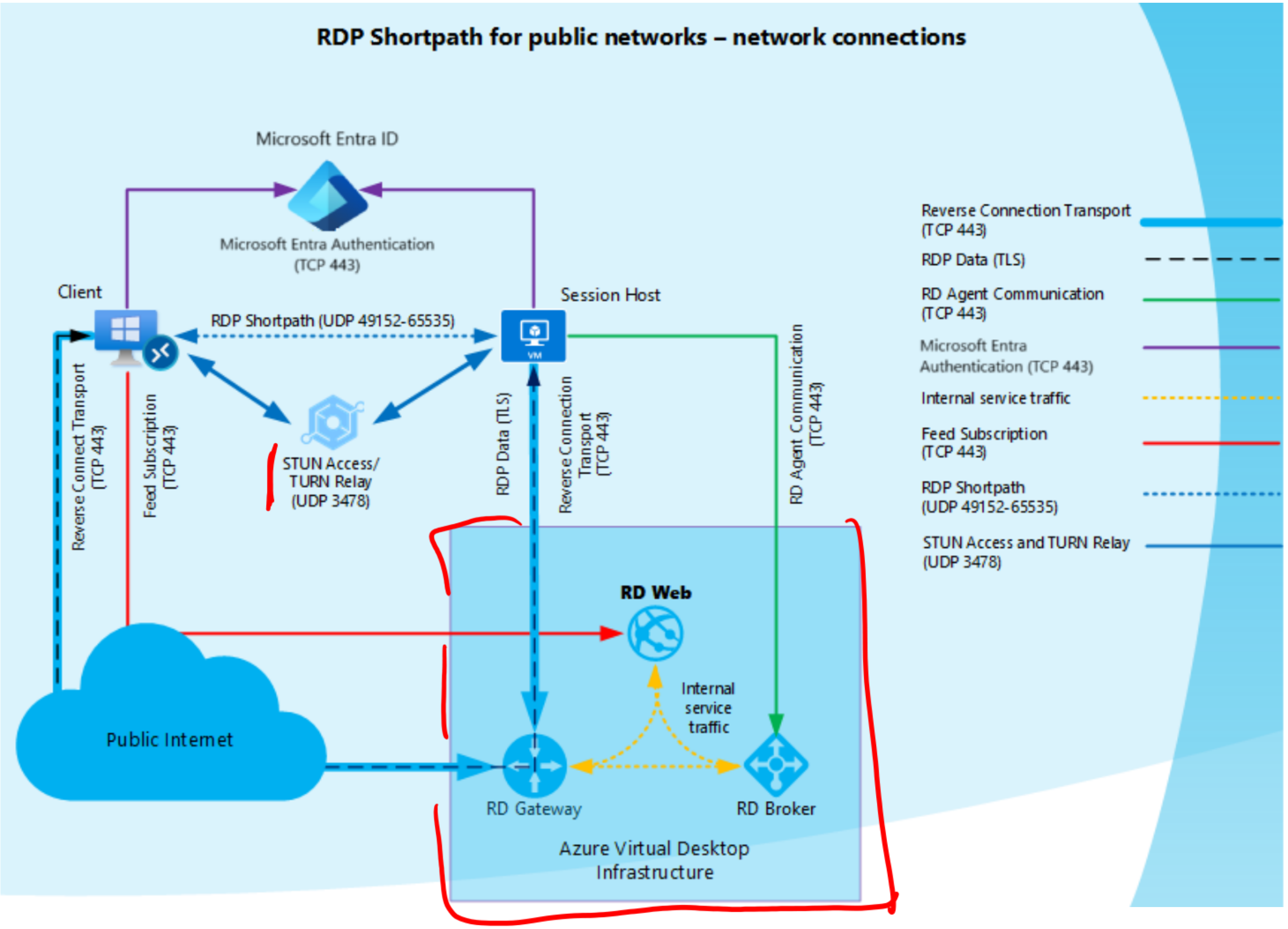

RDP Shortpath Network Connections
Reverse Connect Transport (TCP 443)
~~Feed subscription (TCP 443)~~
Microsoft Entra Authentication (TCP 443)
RD Agent communication (TCP 443)
RDP Shortpath (UDP 3390)
Internal service traffic
Microsoft Entra Connect Sync (TCP 443)
Local Active Directory connectivity (various)
RDP Shortpath (UDP 3390)
Active Directory connectivity
Client
Session Host
VM
Active Directory Domain Services
Reverse Connect Transport (TCP 443)
Feed subscription (TCP 443)
Microsoft Entra Authentication (TCP 443)
Reverse Connect Transport TCP 443
RD Agent communication (TCP 443)
RD Web
Public Internet
RD Gateway
RD Broker
Azure Virtual Desktop Infrastructure
Microsoft Entra Connect sync TCP 443
Microsoft Entra ID



How RDP Shortpath works for public networks

When a connection is being established, Interactive Connectivity Establishment (ICE) coordinates the management of STUN and TURN to optimize the likelihood of a connection being established, and ensure that precedence is given to preferred network communication protocols.

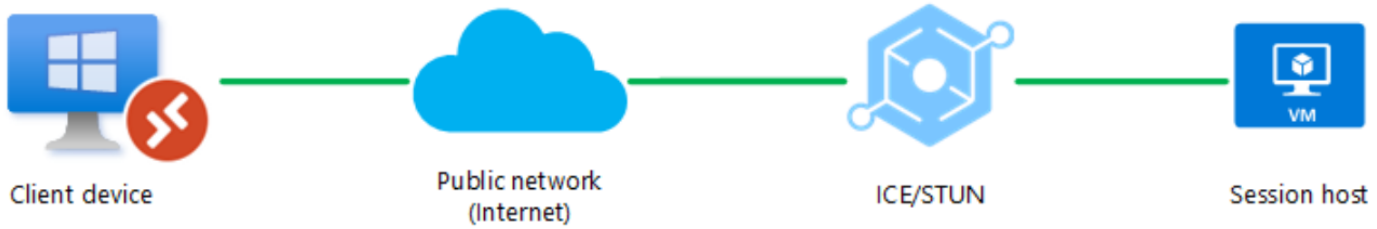
Each RDP session uses a dynamically assigned UDP port from an ephemeral port range (49152 to 65535 by default) that accepts the RDP Shortpath traffic. Port 65330 is ignored from this range as it is reserved for use internally by Azure.



RDP Shortpath for Azure Virtual Desktop sample scenarios

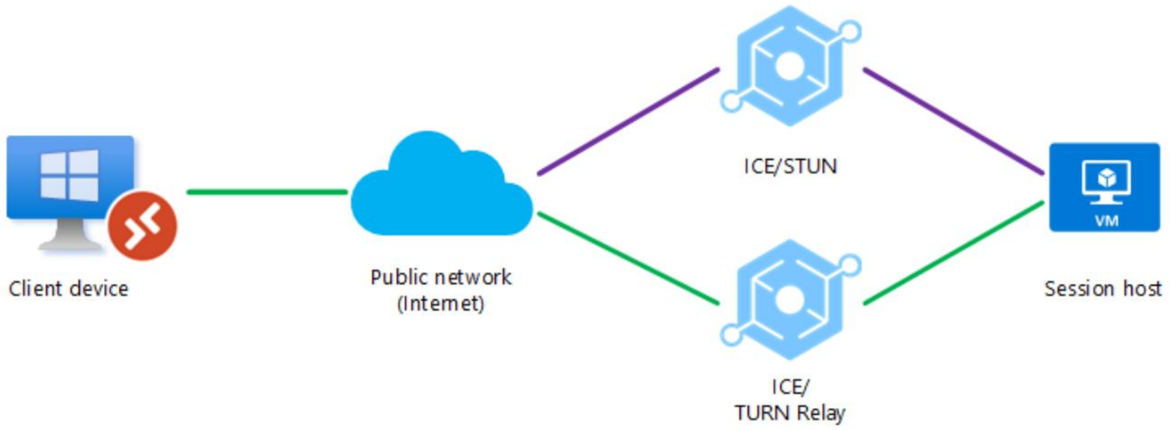
Scenario 1

A UDP connection can only be established between the client device and the session host over a public network (internet). A direct connection, such as a VPN, isn't available. UDP is allowed through firewall or NAT device.



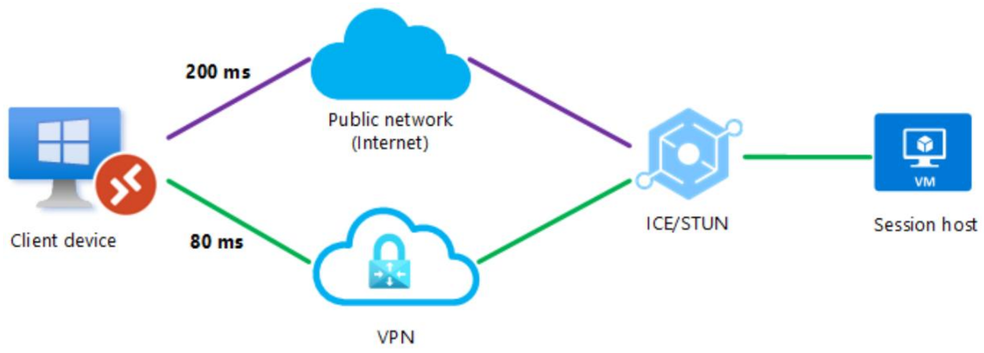
Scenario 2

A firewall or NAT device is blocking a direct UDP connection, but an indirect UDP connection can be relayed using TURN between the client device and the session host over a public network (internet). Another direct connection, such as a VPN, isn't available.



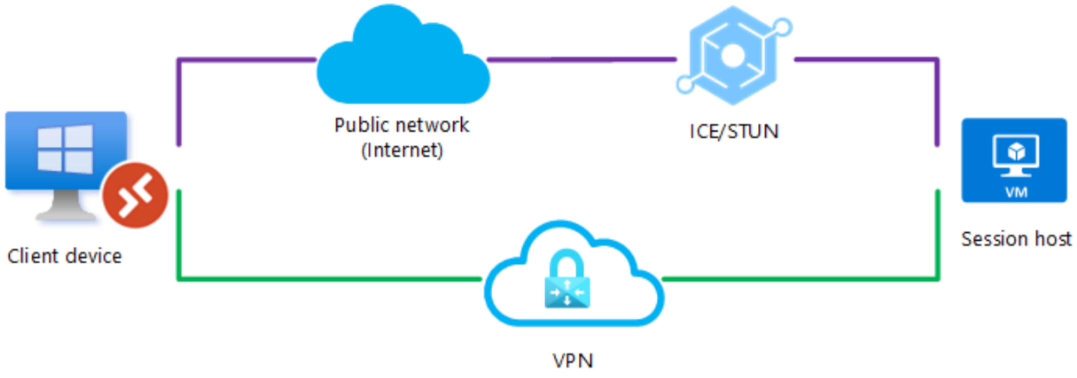
Scenario 3

A UDP connection can be established between the client device and the session host over a public network or over a direct VPN connection, but RDP Shortpath for managed networks isn't enabled. When the client initiates the connection, the ICE/STUN protocol can see multiple routes and will evaluate each route and choose the one with the lowest latency.



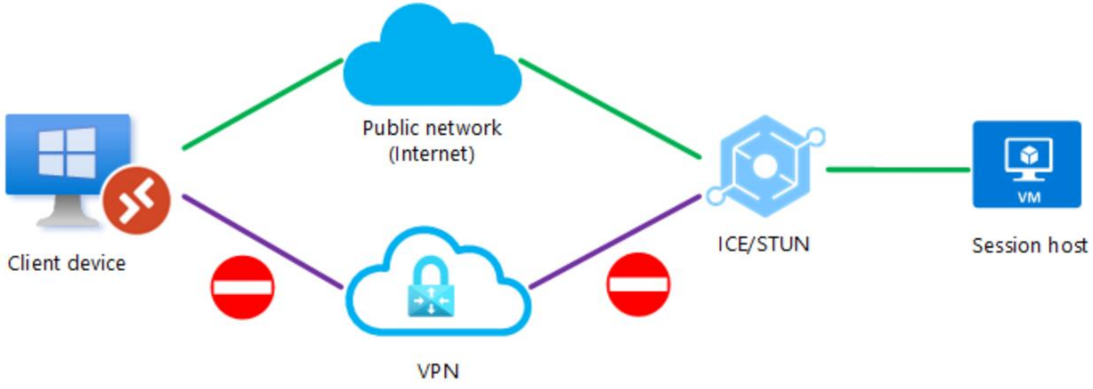
Scenario 4

Both RDP Shortpath for public networks and managed networks are enabled. A UDP connection can be established between the client device and the session host over a public network or over a direct VPN connection. When the client initiates the connection, there are simultaneous attempts to connect using RDP Shortpath for managed networks through port 3390 (by default) and RDP Shortpath for public networks through the ICE/STUN protocol.



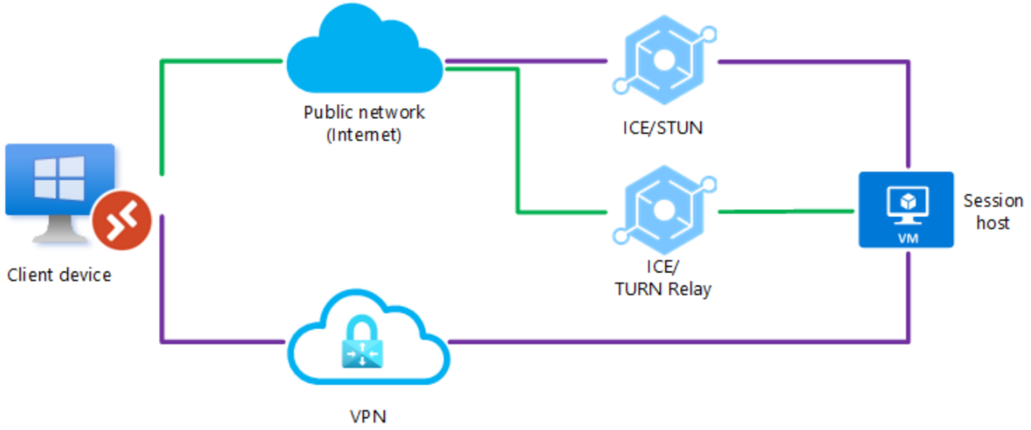
Scenario 5

A UDP connection can be established between the client device and the session host over a public network or over a direct VPN connection, but RDP Shortpath for managed networks isn't enabled. To prevent ICE/STUN from using a particular route, an admin can block one of the routes for UDP traffic. Blocking a route would ensure the remaining path is always used.



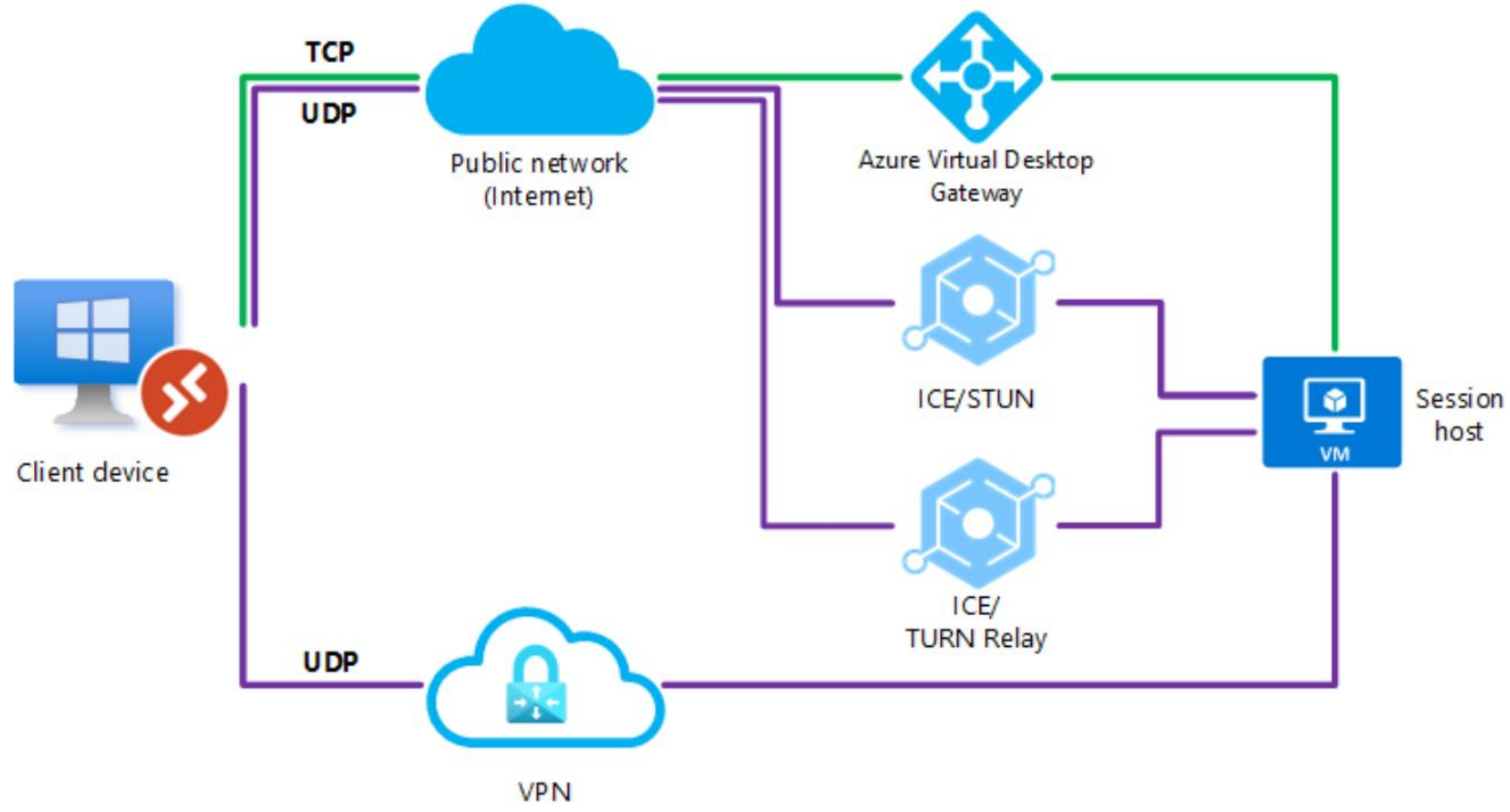
Scenario 6

Both RDP Shortpath for public networks and managed networks are configured, however a UDP connection couldn't be established using direct VPN connection. A firewall or NAT device is also blocking a direct UDP connection using the public network (internet), but an indirect UDP connection can be relayed using TURN between the client device and the session host over a public network (internet).



Scenario 7

Both RDP Shortpath for public networks and managed networks are configured, however a UDP connection couldn't be established. In this instance, RDP Shortpath will fail and the connection will fall back to TCP-based reverse connect transport.



Plan and implement Quality of Service for Azure Virtual Desktop

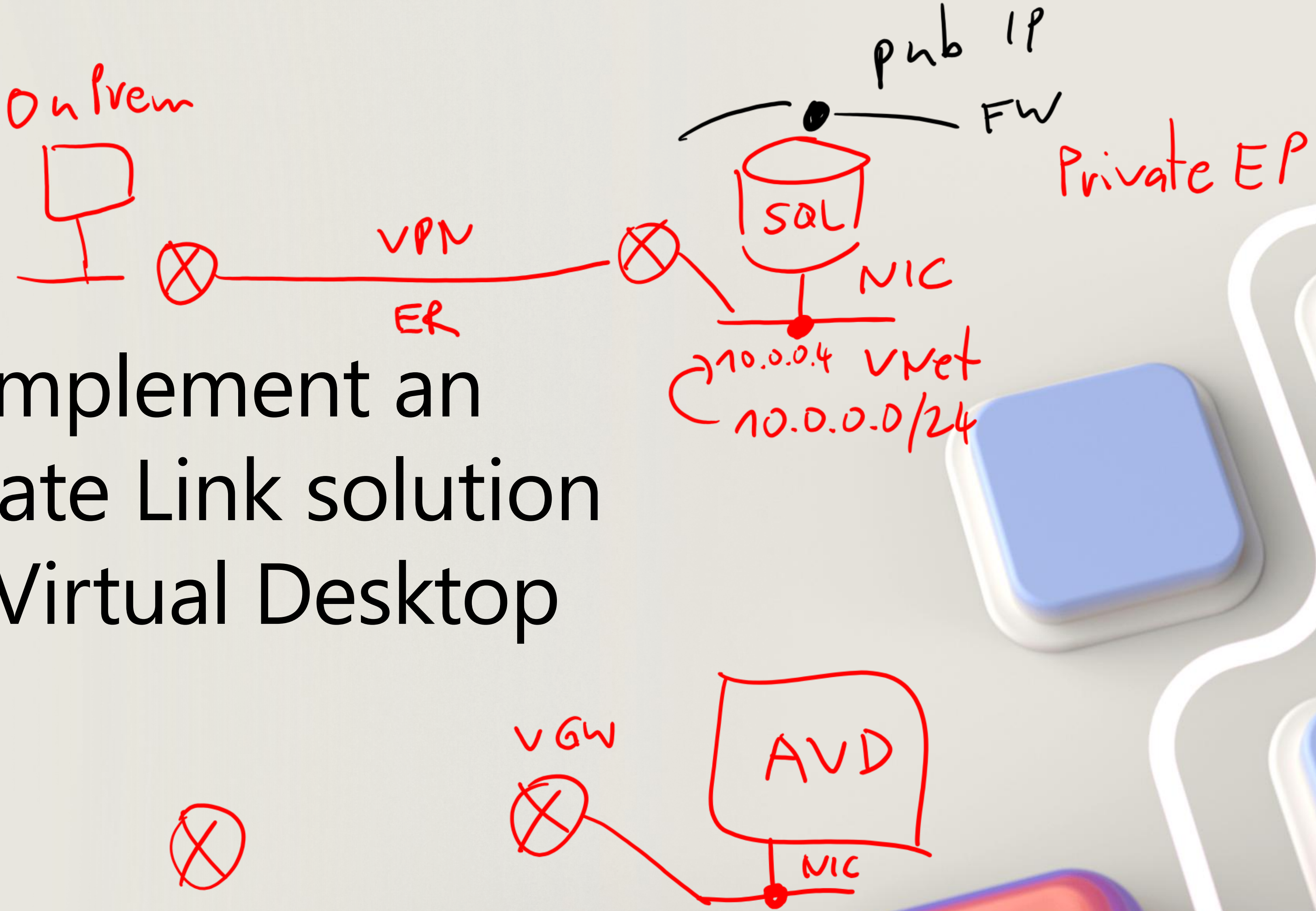
Quality of Service for Azure Virtual Desktop

- RDP Shortpath for managed networks provides a direct UDP-based transport between Remote Desktop Client and Session host.
- RDP Shortpath for managed networks enables configuration of Quality of Service (QoS) policies for the RDP data.
- QoS in Azure Virtual Desktop allows real-time RDP traffic that's sensitive to network delays to "cut in line" in front of traffic that's less sensitive.
- Windows Group Policy Objects to identify and mark all packets in real-time streams and help your network to give RDP traffic a dedicated portion of bandwidth.

Quality of Service queues
To provide QoS, network devices must have a way to classify traffic, and must be able to distinguish RDP from other network traffic.

An analogy is that QoS creates virtual "carpool lanes" in your data network. Some types of data never or rarely encounter a delay. Once you create those lanes, you can adjust their relative size, and much more effectively manage the connection bandwidth you have while still delivering business-grade experiences for your organization's users.

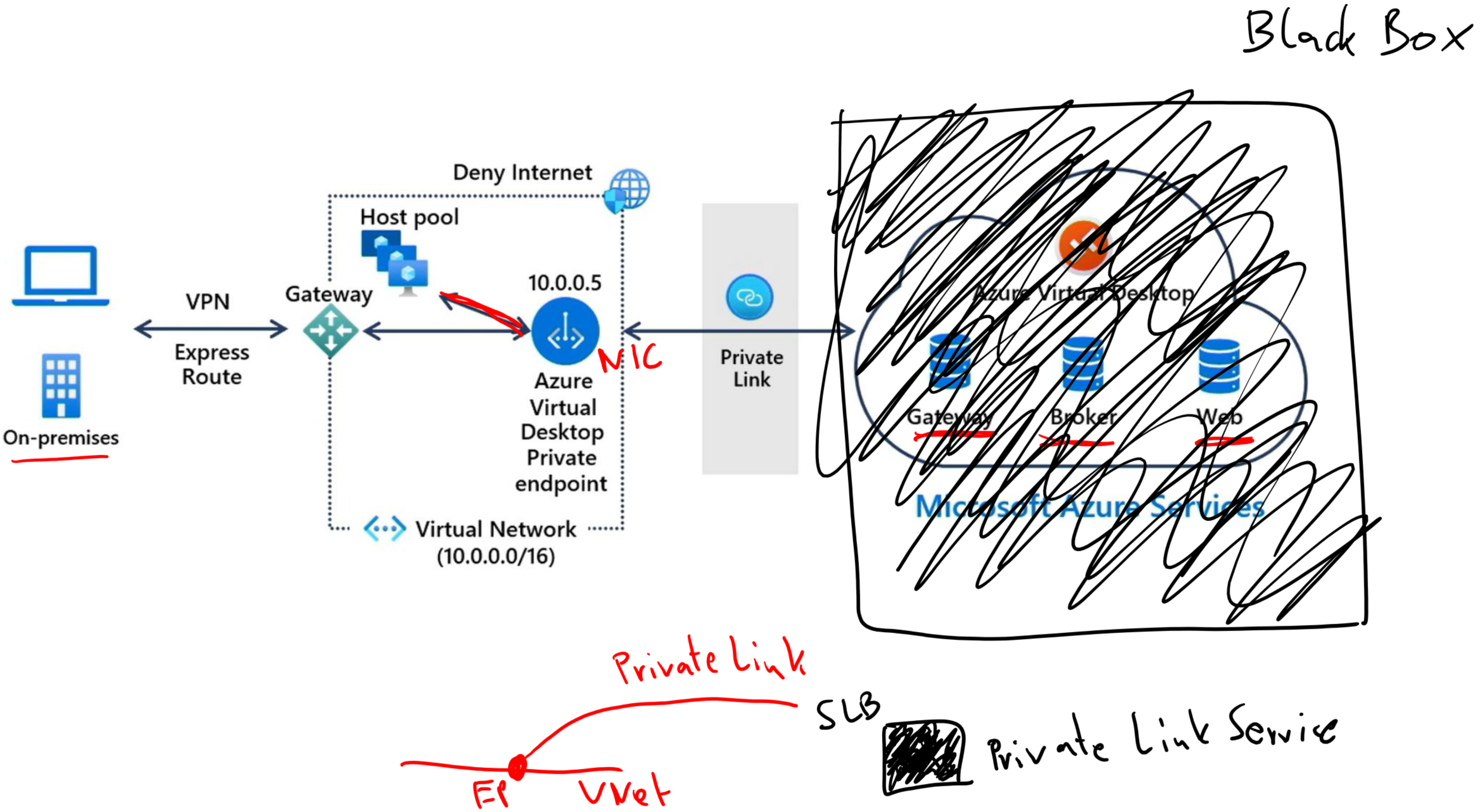
Plan and implement an Azure Private Link solution for Azure Virtual Desktop



Azure Virtual Desktop has three workflows with three corresponding resource types to use with private endpoints.

- **Initial feed discovery:** allows the client discover all workspaces assigned to a user. To enable this process, you must create a single private endpoint to the global sub-resource to any workspace.
  - You can only create one private endpoint in your entire Azure Virtual Desktop deployment. This endpoint creates DNS entries and private IP routes for the FQDN needed for initial feed discovery. This connection becomes a single, shared route for all clients to use.
- **Feed download:** the client downloads all connection details for a specific user for the workspaces that host their application groups. You create a private endpoint for the feed sub-resource for each workspace you want to use with Private Link.
- **Connections to host pools:** every connection to a host pool has two sides - clients and session hosts. You need to create a private endpoint for the connection sub-resource for each host pool you want to use with Private Link.

How does Private Link work with Azure Virtual Desktop?



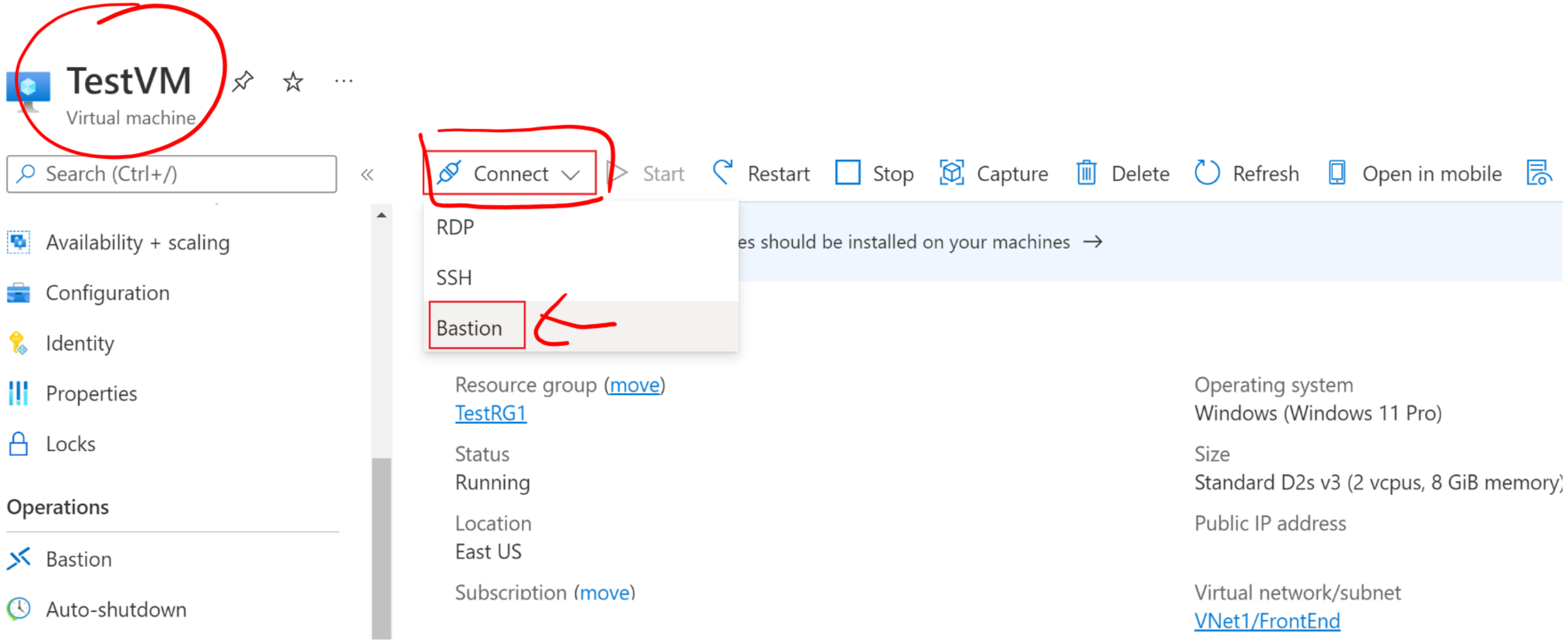
Create an RDP connection to a Windows VM using Azure Bastion

Azure Bastion provides secure connectivity to all of the VMs in the virtual network in which it's provisioned.

Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

New :

shareble lik



Resource group (move)
TestRG1

Status
Running

Location
East US

Subscription (move)

Operating system
Windows (Windows 11 Pro)

Size
Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address

Virtual network/subnet
VNet1/FrontEnd

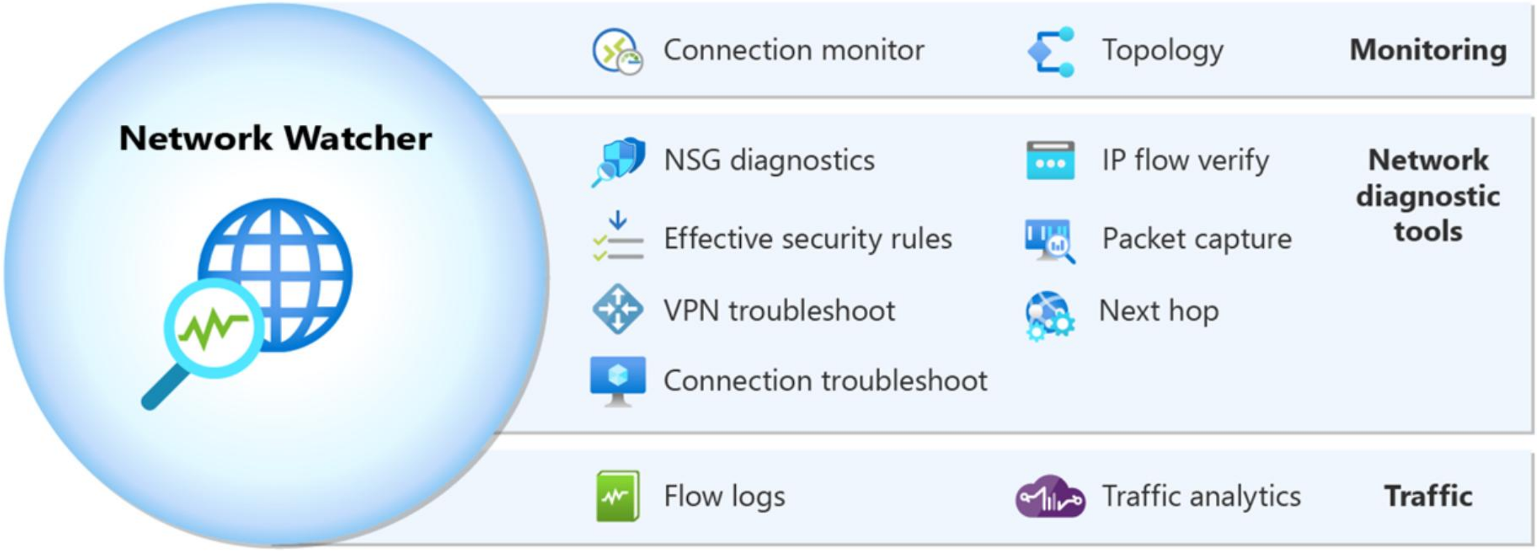
Monitor and troubleshoot network connectivity for Azure Virtual Desktop

Azure Network Watcher provides a suite of tools to monitor, diagnose, view metrics, and enable or disable logs for Azure IaaS (Infrastructure-as-a-Service) resources.

Network Watcher enables you to monitor and repair the network health of IaaS products like virtual machines (VMs), virtual networks (VNets), application gateways, and load balancers.

Network Watcher has three sets of tools and capabilities:

- Monitoring
- Network diagnostic tools
- Traffic



Knowledge check

Knowledge check

What is used to secure connectivity and prevent exposing Remote Desktop Protocol Secure Shell (RDP/SSH) ports all virtual machines in a virtual network?

Choices:

1. [✓ Azure Bastion]
2. Azure Load Balancer
3. Network security groups (NSGs)

Knowledge check

A system administrator is setting up a remote desktop protocol for Azure Virtual Desktop. They want to improve the connection's reliability and increase available bandwidth for each user session. Which feature should they use?

Choices:

1. Reverse connect transport ✗
2. Quality of Service (QoS) ✗

[✓ 3. RDP Shortpath] ✓

Knowledge check

A system administrator is tasked with improving the performance of a remote desktop application hosted on Azure Virtual Desktop. The administrator is considering using RDP Shortpath. What does RDP Shortpath enable?

Choices:

1. It enables the deployment of applications in a virtualized environment, isolating them from each other and from the host system

2. It enables the automation and validation of the creation and teardown of environments to help deliver secure and stable application hosting platforms

[✓ 3.] It establishes a direct UDP based transport between a local device and session host in Azure Virtual Desktop, offering better connection reliability and more consistent latency ✓

Knowledge check

A network administrator needs to limit the RDP outbound network traffic by specifying a throttle rate in QoS Policy. What should they do to implement throttle rate limiting on session host using Group Policy?

Choices:

✗ 1. They should create a new policy in the root directory of Group Policy Management.

2. They should modify the existing policy in the Session Hosts OU.

[✓ 3.] They should create a new GPO in the Session Hosts OU, specify the outbound throttle rate, and apply it to svchost.exe. ✓

Summary

Summary

What you learned:

- Describe Azure Virtual Desktop network connectivity
- Analyze connection quality in Azure Virtual Desktop
- Describe Remote Desktop Protocol (RDP) bandwidth requirements
- Configure RDP Shortpath for Azure Virtual Desktop sample scenarios
- Plan and implement Quality of Service for Azure Virtual Desktop
- Plan an Azure Private Link solution for Azure Virtual Desktop
- Create an RDP connection to a Windows VM using Azure Bastion