

AZ-140

Configuring and Operating Azure Virtual Desktop



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. Plan for disaster recovery
14. Automate Azure Virtual Desktop management tasks
15. Monitor and manage performance and health

Implement and manage networking for Azure Virtual Desktop



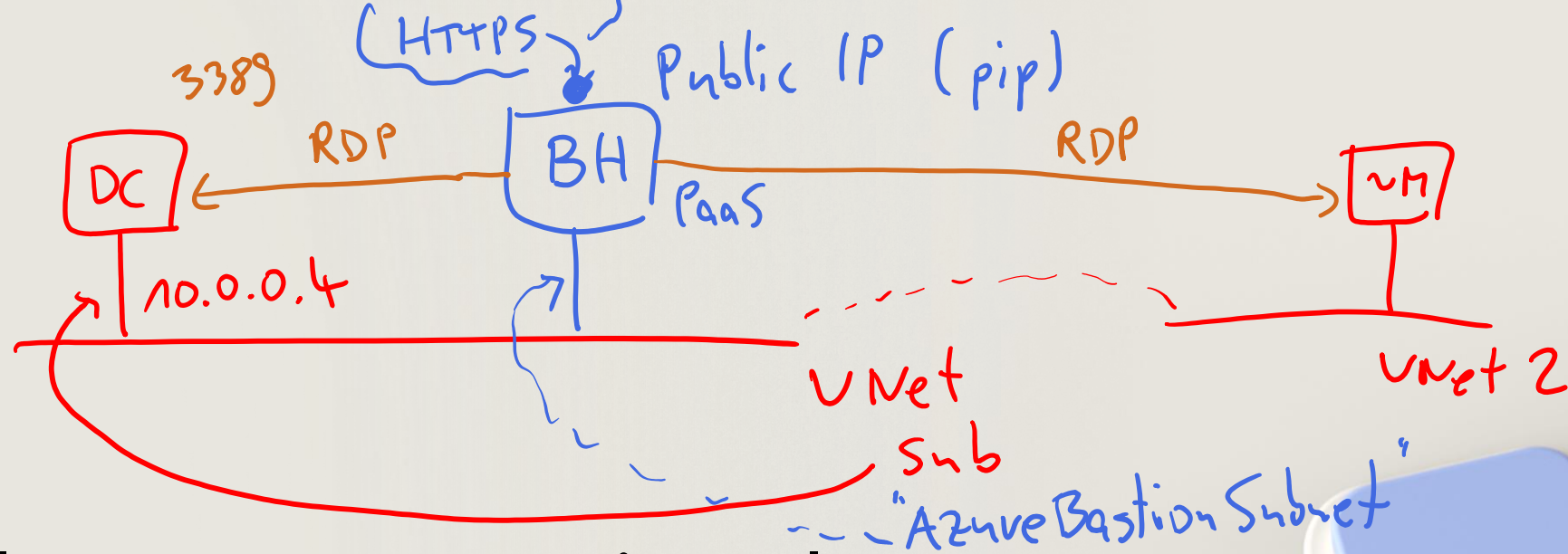
Introduction

- 1 Implement Azure virtual network connectivity
- 2 Manage connectivity to the internet and on-premises networks
- 3 Understanding Azure Virtual Desktop network connectivity
- 4 Implement and manage network security
- 5 Configure Azure Virtual Desktop session hosts using Azure Bastion
- 6 Azure Network Watcher
- 7 Knowledge check and Summary

AZ-140: Implement an Azure Virtual Desktop infrastructure (25-30%)

Implement and manage networking for Azure Virtual Desktop

- Conceptual knowledge of Azure compute solutions.
- Working experience with virtual machines, virtual networks, and app service.

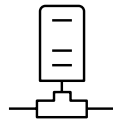


Implement Azure virtual network connectivity

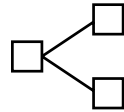
Communication between Azure resources is done by one of the following:



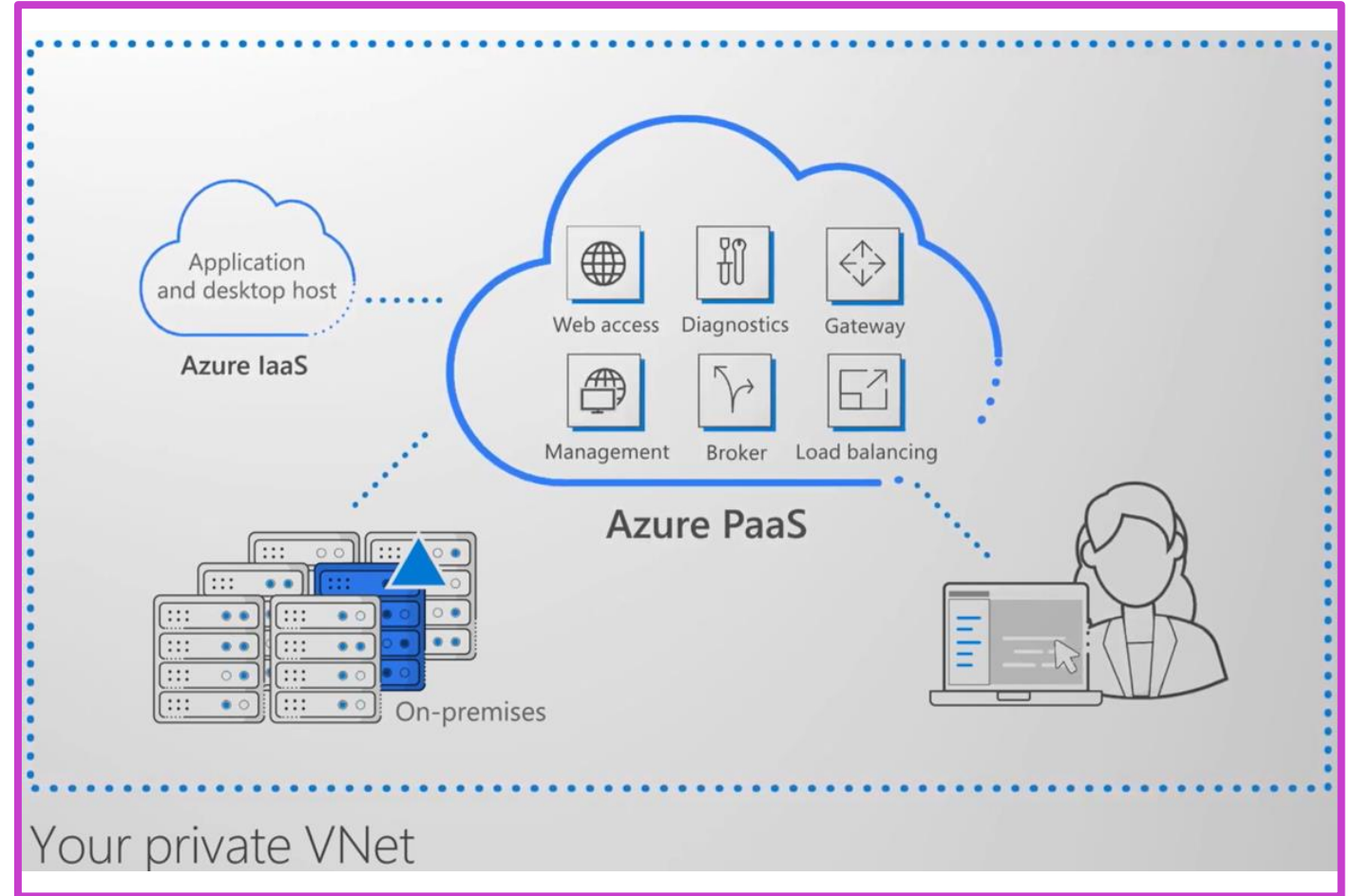
Through a virtual network: Deploy VMs, and several other types of Azure resources to a virtual network



Through a virtual network service endpoint: Extend your virtual network private address space and the identity of your virtual network to Azure service resources over a direct connection.



Through VNet Peering: Connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering



Manage connectivity to the internet and on-premises networks



Point-to-site virtual private network (VPN):

- Each computer that wants to establish connectivity with a virtual network must configure its connection.
- The communication between a computer and a virtual network is sent through an encrypted tunnel over the internet.

Site-to-site VPN: Established between 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 an on-premises VPN device and an Azure VPN gateway is sent through an encrypted tunnel over the internet.

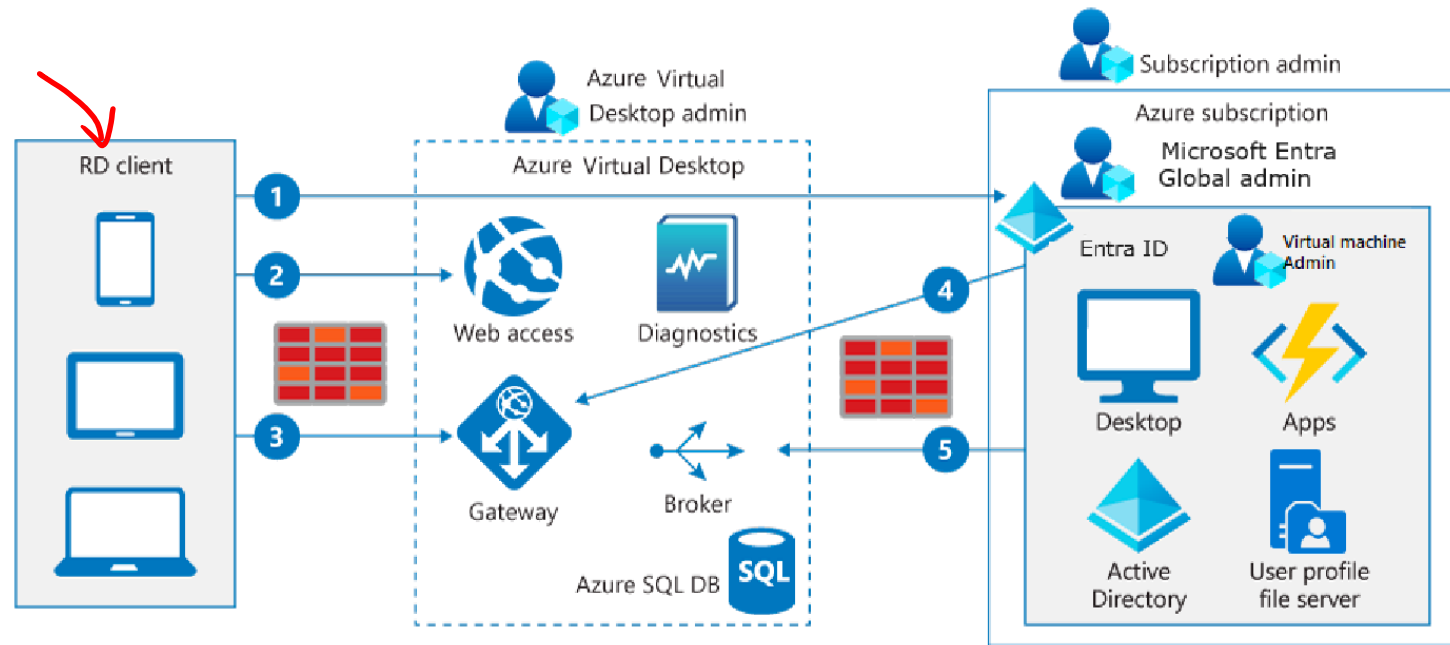
Azure ExpressRoute: Established between your network and Azure, through an ExpressRoute partner.

- This connection is private.
- Traffic does not go over the internet.

Understanding Azure Virtual Desktop network connectivity

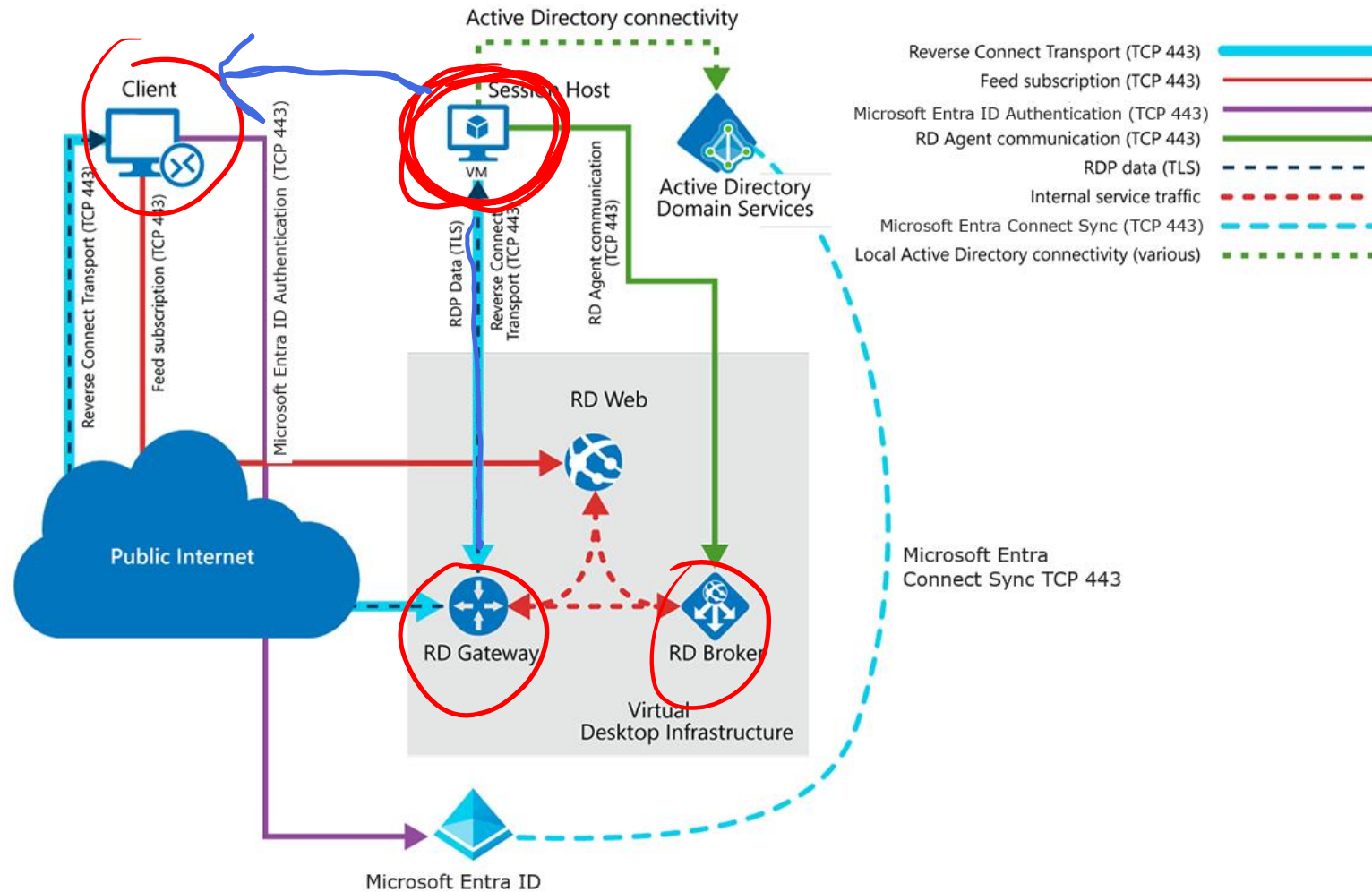


1. When authenticated in Microsoft Entra ID, a token is returned to the Remote Desktop Services client.
2. The gateway checks the token with the connection broker.
3. The broker queries the Azure SQL database for resources assigned to the user.
4. The gateway and the broker select the session host for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



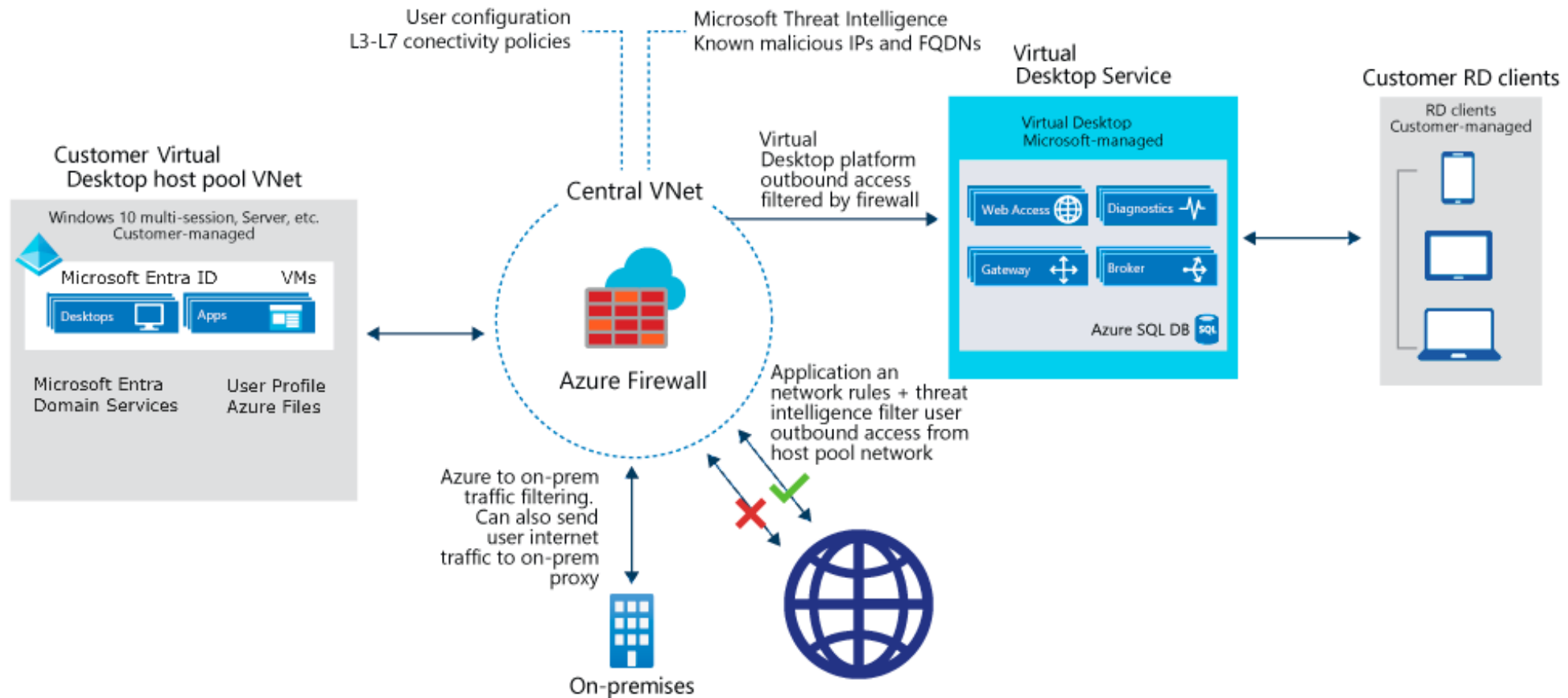
Azure Virtual Desktop networks

Azure Virtual Desktop Network Connections



Implement and manage network security





- A host pool is a collection of Azure virtual machines that register to Azure Virtual Desktop as session hosts.
- These virtual machines run in your virtual network and are subject to the virtual network security controls.
- They need outbound Internet access to the Azure Virtual Desktop service to operate properly and might also need outbound Internet access for end users.
- Azure Firewall can help you lock down your environment and filter outbound traffic.

Configure Azure Virtual Desktop session hosts using Azure Bastion



Microsoft Bastion provides secure connectivity to all VMs in a virtual network in which it is provisioned.

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

Microsoft Azure

Home >

TestVM | Bastion
Virtual machine

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size
- Security

Connect using Azure Bastion
Azure Bastion Service enables you to securely and seamlessly RDP & SSH

Using Bastion: **TestVNet1-bastion**, Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

☒ Open in new window

Username * ⓘ

Password * ⓘ

Connect

Key board

ping
tracert

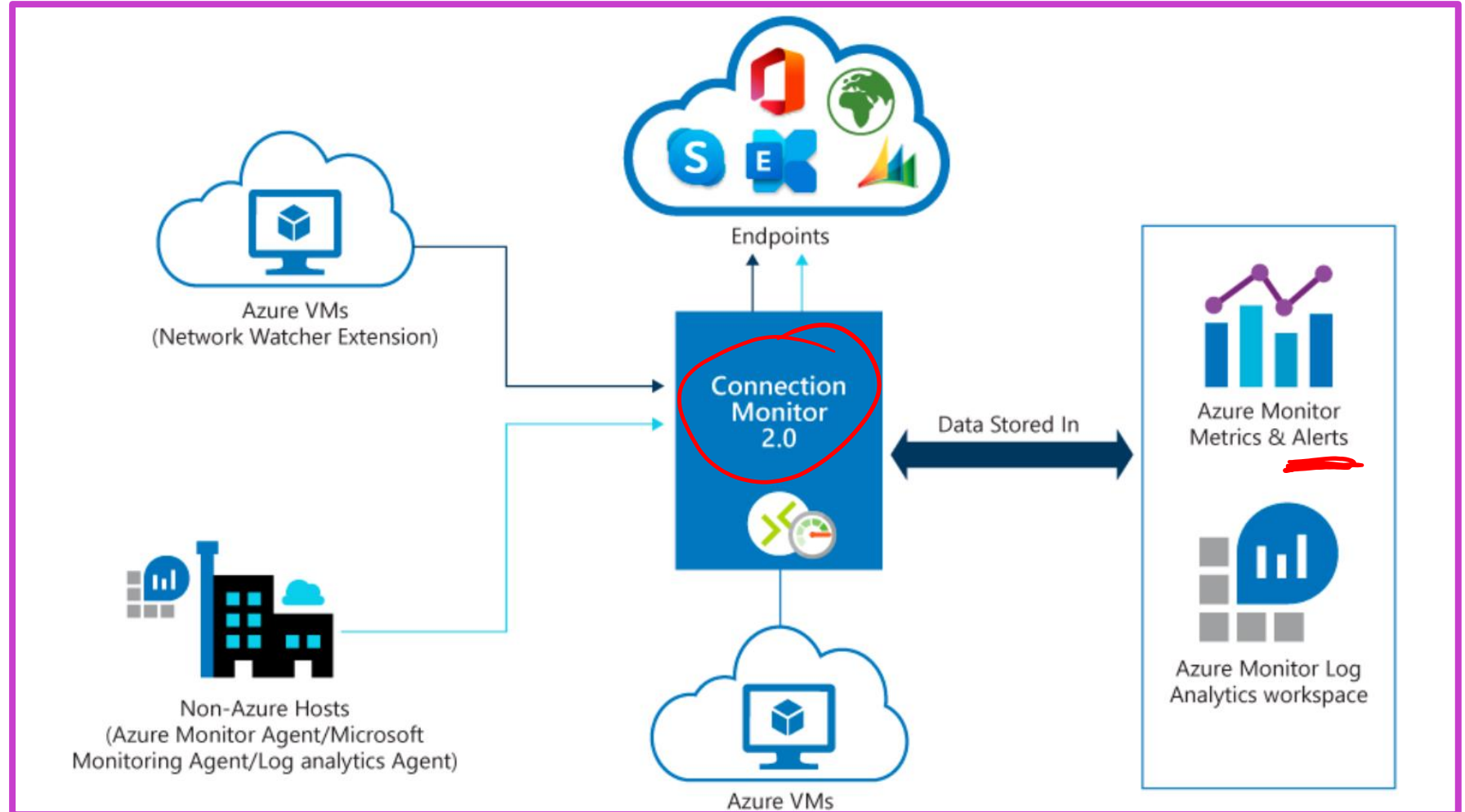
Azure Network Watcher



Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.

Connection Monitor 2.0 monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint.

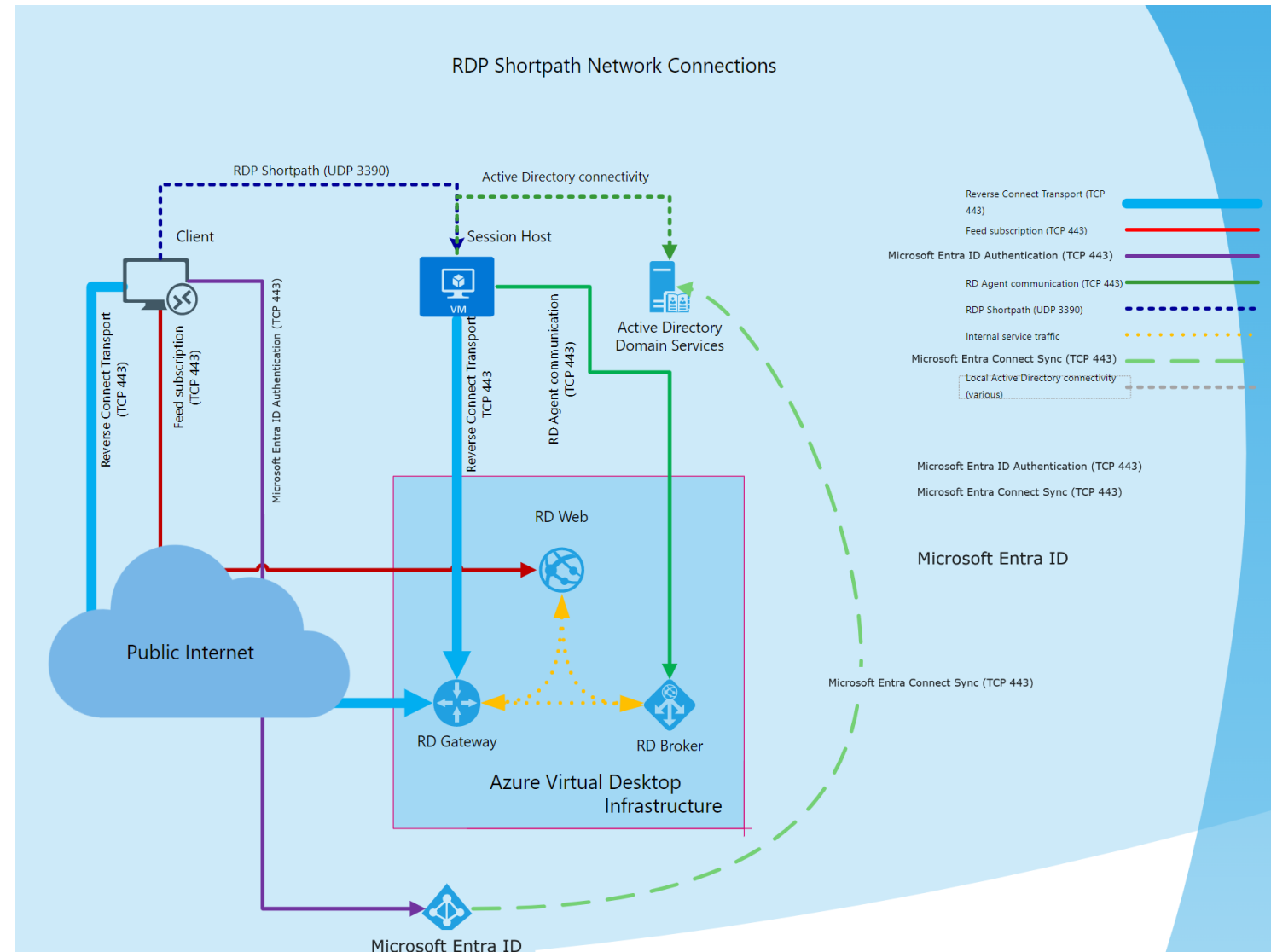
If an endpoint becomes unreachable, connection troubleshoot informs you of the reason.



Plan and implement Remote Desktop Protocol Short path



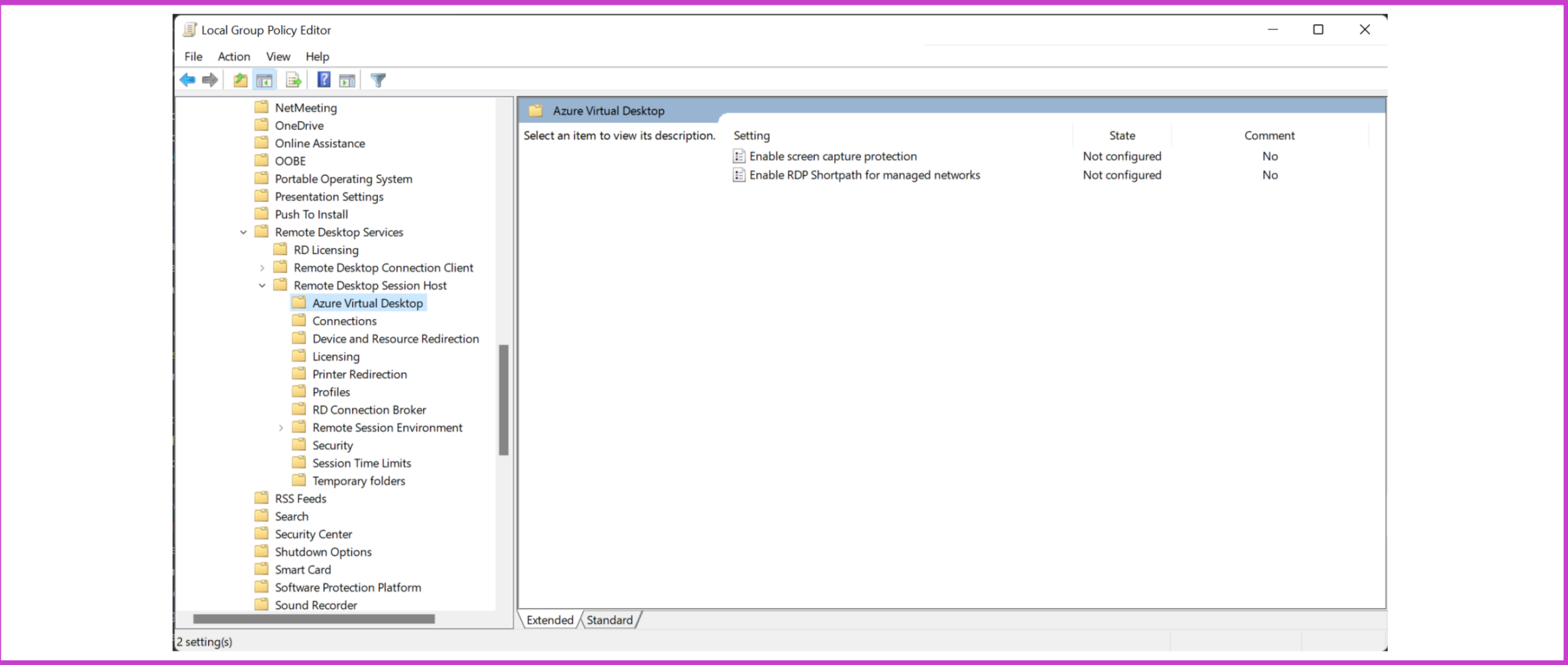
1. The session host sends the list of its private and public IPv4 and IPv6 addresses to the client.
2. The client starts the background thread to establish a parallel UDP-based transport directly to one of the host's IP addresses.
3. Initial connection establishment over the reverse connect transport to ensure no delay in the user connection.
4. If the client has a direct line of sight, the client establishes a secure TLS connection with the session host.
5. RDP moves all Dynamic Virtual Channels (DVCs).
6. If a firewall or network topology prevents the client from establishing direct UDP connectivity, RDP continues with a reverse connect transport.



Configure Remote Desktop Protocol Shortpath for managed networks



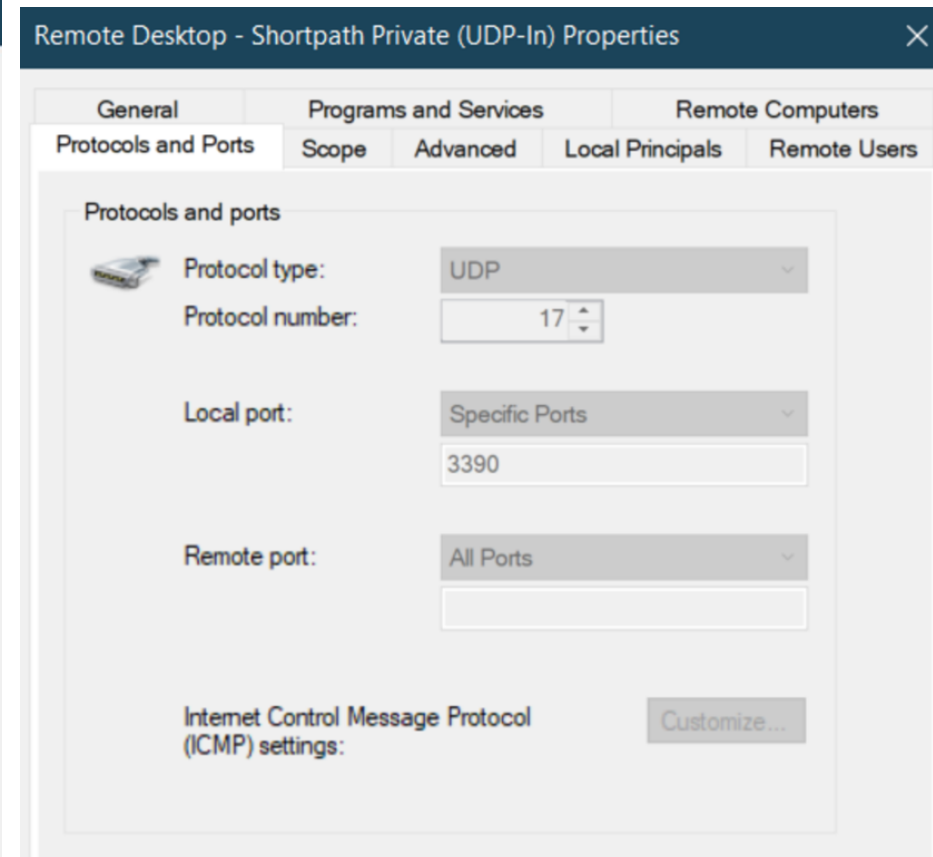
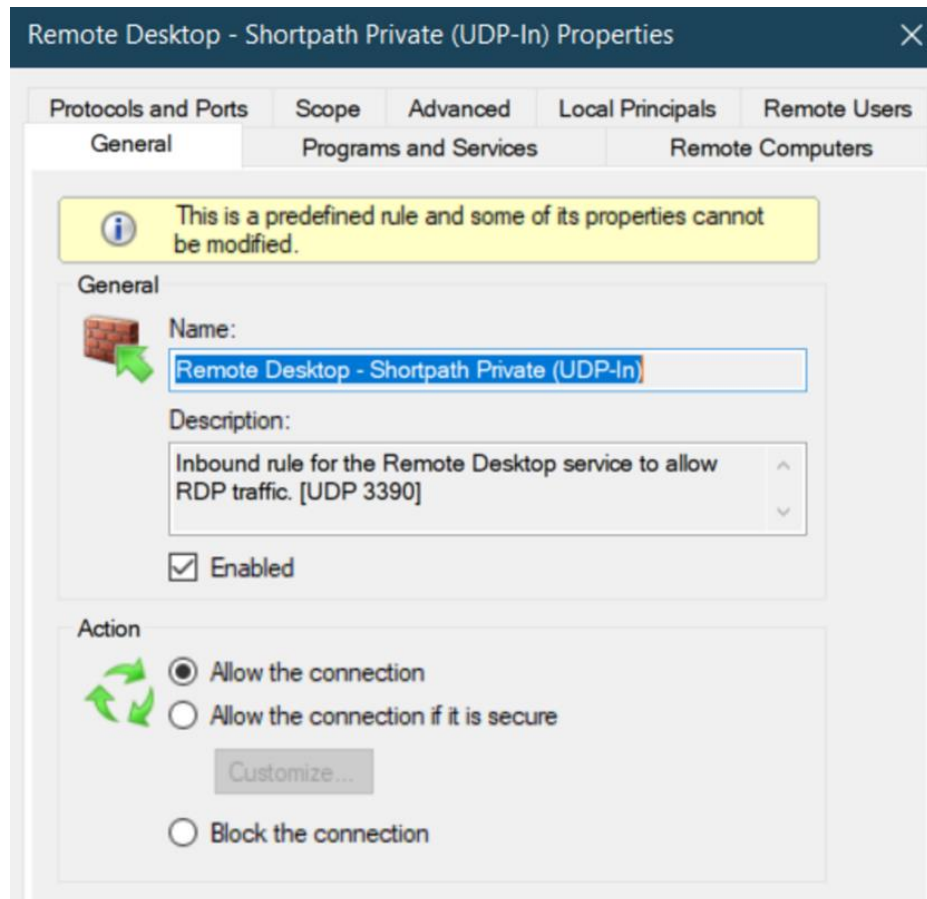
To enable RDP Shortpath for managed networks, you enable the RDP Shortpath listener on the session host.



Configure Windows Defender Firewall with Advanced Security for RDP Short path



To allow inbound network traffic for RDP Shortpath, use the Microsoft Defender Firewall with Advanced Security node in the Group Policy Management MMC snap-in to create firewall rules.



Plan and implement Quality of Service for Azure Virtual Desktop



RDP Shortpath for managed networks enables configuration of Quality of Service (QoS) policies for the RDP data.

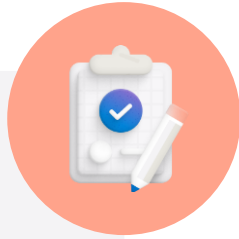
- QoS in Azure Virtual Desktop allows real-time RDP traffic that's sensitive to network delays to "cut in line" in front of traffic that's less sensitive.
- QoS uses Windows Group Policy Objects to identify and mark all packets in real-time streams and help your network to give RDP traffic a dedicated portion of bandwidth.

Without some form of QoS, you might see the following issues:

- **Jitter** – RDP packets arriving at different rates, which can result in visual and audio glitches.
- **Packet loss** – Packets dropped, which results in retransmission that requires another time.
- **Delayed round-trip time (RTT)** – RDP packets taking a long time to reach their destinations, which result in noticeable delays between input and reaction from the remote application.

Knowledge check and Summary

Check your knowledge



What you learned:

- Recommend a solution for Azure Virtual Desktop network connectivity.
- Implement Azure virtual network connectivity for Azure Virtual Desktop.
- Describe network security for Azure Virtual Desktop.
- Configure Azure Virtual Desktop session hosts using Microsoft Bastion.
- Monitor communication between a virtual machine and an endpoint.

