Hub Spoke Configuration for MI

Last updated by | Charlene Wang | Feb 8, 2021 at 10:36 PM PST

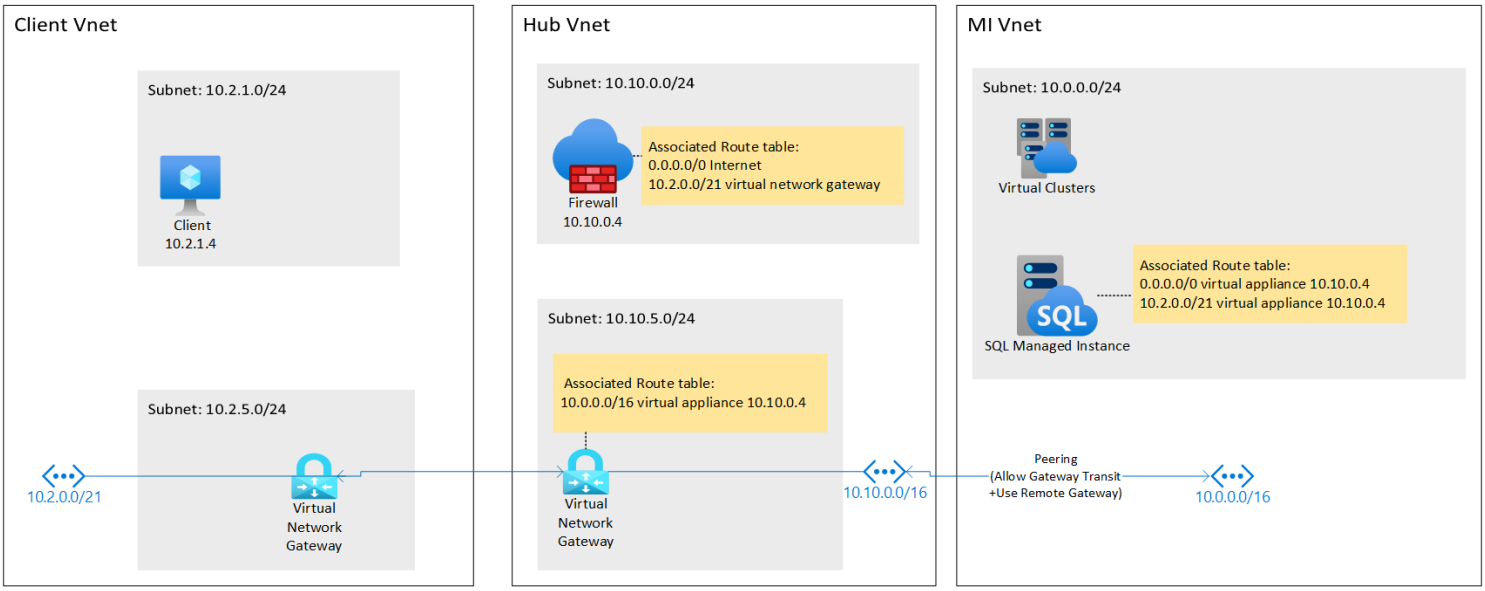
Contents

Architecture

Hub-spoke virtual network setting is commonly used when customers connect their on-premises network to an Azure virtual network to create a hybrid networr and they want to control access to the Azure network resources in a centralized way.

Azure Firewall is an important part in this architecture to control network access in a hybrid network using rules that define allowed and denied network traffic.

Azure SQL Database and Azure SQL Managed Instance can be part of the Azure resources which resids in the hub virtual network, but due to special private cluster deployment for Azure SQL Managed Insance, you need some special configurations like UDR to make the connections work.



- Client VNet: represents on-premise network which is the client who will access Azure cloud resources
- Hub VNet: represents the centralized hub virtual network where Azure firewall resides.
- MI VNet: represents one kind of spoke virtual network. Since we are using Azure SQL Managed Instance as the target resource type, this means the virtual network where MI is deployed.

Configuration

How to set up hub-spoke virtual network for Managed Instance step by step

In this sample, I am using Azure virtual network to simulate on-premise network (client VNet).

Prerequistes

Expect you already have one Azure SQL Managed Instance deployed. In this sample, my MI Vnet is 10.0.0.0/16, MI subnet is 10.0.0.0/24.

Detail steps

1. Create the firewall hub virtual network First, create the resource group to contain the resources for this tutorial:
    - Sign in to the Azure portal at https://portal.azure.com.
    - On the Azure portal home page, select Resource groups > Add.
    - For Subscription, select your subscription.
    - For Resource group name, type FW-Hybrid-Test.
    - For Region, select (US) East US. All resources that you create later must be in the same location.
    - Select Review + Create.
    - Select Create.

    Now, create the VNet:

    Note: The size of the AzureFirewallSubnet subnet is /26. For more information about the subnet size, see Azure Firewall FAQ.

- From the Azure portal home page, select Create a resource.
- Under Networking, select Virtual network.
- Select Create.
- For Resource group, select FW-Hybrid-Test.
- For Name, type VNet-hub.
- Select Next: IP Addresses.
- For IPv4 Address space, delete the default address and type 10.10.0.0/16.
- Under Subnet name, select Add subnet.
- For Subnet name type AzureFirewallSubnet. The firewall will be in this subnet, and the subnet name must be AzureFirewallSubnet.
- For Subnet address range, type 10.10.0.0/26.
- Select Add.
- Select Review + create.
- Select Create.

2. Create the on-premises virtual network

- From the Azure portal home page, select Create a resource.
- In Networking, select Virtual network.
- For Resource group, select FW-Hybrid-Test.
- For Name, type VNet-OnPrem.
- For Region, select (US) East US.
- Select Next : IP Addresses
- For IPv4 address space, delete the default address and type 10.2.0.0/21.
- Under Subnet name, select Add subnet.
- For Subnet name type ClientSubnet.
- For Subnet address range, type 10.2.1.0/24.
- Select Add.
- Select Review + create.
- Select Create.

Now create a second subnet for the gateway.

- On the VNet-Onprem page, select Subnets.
- Select +Subnet.
- For Name, type GatewaySubnet.
- For Subnet address range type 10.2.5.0/24.
- Select OK.

3. Configure and deploy the firewall Now deploy the firewall into the firewall hub virtual network.

- From the Azure portal home page, select Create a resource.
- In the left column, select Networking, and search for and then select Firewall.
- On the Create a Firewall page, use the following table to configure the firewall:

Setting	Value
Subscription	<your subscription>
Resource group	FW-Hybrid-Test
Name	AzFW01
Region	East US
Choose a virtual network	Use existing: VNet-hub
Public IP address	Add new: AzureFirewallPIP.

- Select Review + create.
- Review the summary, and then select Create to create the firewall.
- This takes a few minutes to deploy.
- After deployment completes, go to the FW-Hybrid-Test resource group, and select the AzFW01 firewall.
- Note the private IP address. You'll use it later when you create the default route.

4. Configure network rules First, add a network rule to allow traffic to MI.
   - On the AzFW01 page, Select Rules.
   - Select the Network rule collection tab.
   - Select Add network rule collection.
   - For Name, type RCNet01.
   - For Priority, type 100.
   - For Action, select Allow.
   - Under Rules, for Name, type AllowClient2MI.
   - For Protocol, select TCP.
   - For Source type, select IP address.
   - For Source, type 10.2.1.0/24 which is the on-premises ClientSubnet.
   - For Destination type, select IP address.
   - For Destination address, type 10.6.0.0/16 which is the MI VNet.
   - For Destination Ports, type 1433.
5. Create and connect the VPN gateways The hub and on-premises virtual networks are connected via VPN gateways.

   Create a VPN gateway for the hub virtual network

   - From the Azure portal home page, select Create a resource.
   - In the search text box, type virtual network gateway.

- Select Virtual network gateway, and select Create.
- For Name, type GW-hub.
- For Region, select the same region that you used previously.
- For Gateway type, select VPN.
- For VPN type, select Route-based.
- For SKU, select Basic.
- For Virtual network, select VNet-hub.
- For Public IP address, select Create new, and type GW-hub-pip for the name.
- Accept the remaining defaults and then select Review + create.
- Review the configuration, then select Create.

Create a VPN gateway for the on-premises virtual network

- From the Azure portal home page, select Create a resource.
- In the search text box, type virtual network gateway and press Enter.
- Select Virtual network gateway, and select Create.
- For Name, type GW-Onprem.
- For Region, select the same region that you used previously.
- For Gateway type, select VPN.
- For VPN type, select Route-based.
- For SKU, select Basic.
- For Virtual network, select VNet-Onprem.
- For Public IP address, select Create new, and type GW-Onprem-pip for the name.
- Accept the remaining defaults and then select Review + create.
- Review the configuration, then select Create.

Create the VPN connections

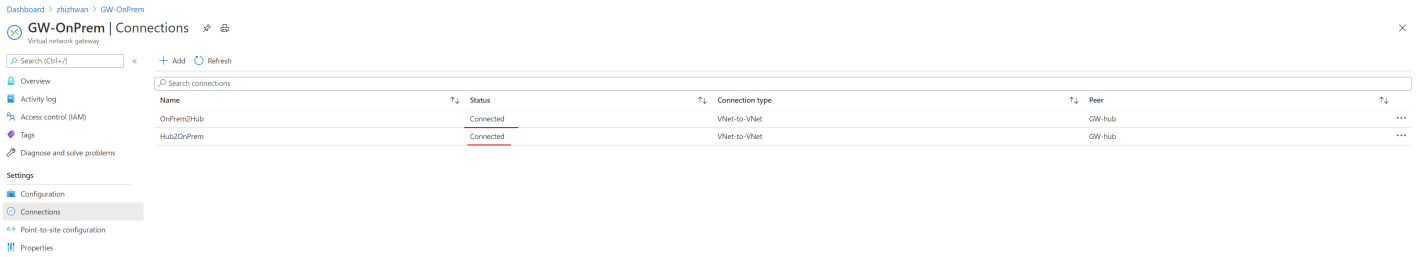
Now you can create the VPN connections between the hub and on-premises gateways.

In this step, you create the connection from the hub virtual network to the on-premises virtual network. You'll see a shared key referenced in the examples. You can use your own values for the shared key. The important thing is that the shared key must match for both connections. Creating a connection can take a short while to complete.

- Open the FW-Hybrid-Test resource group and select the GW-hub gateway.
- Select Connections in the left column.
- Select Add.
- The the connection name, type Hub2OnPrem.
- Select VNet-to-VNet for Connection type.
- For the Second virtual network gateway, select GW-Onprem.
- For Shared key (PSK), type AzureA1b2C3.

- Select OK.
- Open the FW-Hybrid-Test resource group and select the GW-Onprem gateway.
- Select Connections in the left column.
- Select Add.
- For the connection name, type OnPrem2Hub.
- Select VNet-to-VNet for Connection type.
- For the Second virtual network gateway, select GW-hub.
- For Shared key (PSK), type AzureA1b2C3.
- Select OK.

Verify the connection After about five minutes or so, the status of both connections should be Connected.



6. Peer the hub and MI virtual networks Now peer the hub and spoke virtual networks.
   - Open the FW-Hybrid-Test resource group and select the VNet-hub virtual network.
   - In the left column, select Peerings.
   - Select Add.
   - Under This virtual network:

Setting name	Value
Peering link name	HubtoSpoke
Traffic to remote virtual network	Allow (default)
Traffic forwarded from remote virtual network	Allow (default)
Virtual network gateway	Use this virtual network's gateway

   - Under Remote virtual network:

Setting name	Value
Peering link name	SpoketoHub
Virtual network deployment model	Resource manager
Subscription	<your subscription>
Virtual network	<your MI VNet>
Traffic to remote virtual network	Allow (default)
Traffic forwarded from remote virtual network	Allow (default)
Virtual network gateway	Use the remote virtual network's gateway

- Select Add.

Add peering

VNet-hub

For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.

This virtual network

Peering link name *

HubtoSpoke

Traffic to remote virtual network

- (•) Allow (default)
- ( ) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

- (•) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

Virtual network gateway

- (•) Use this virtual network's gateway
- ( ) Use the remote virtual network's gateway
- ( ) None (default)

Remote virtual network

Peering link name *

SpoketoHub

Virtual network deployment model

- (•) Resource manager
- ( ) Classic

[ ] I know my resource ID

Subscription *

V

Virtual network *

VNet-Spoke

Traffic to remote virtual network

- (•) Allow (default)
- ( ) Block all traffic to the remote virtual network

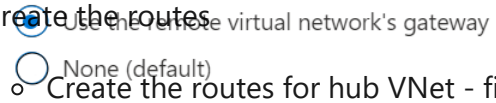
Traffic forwarded from remote virtual network

- (•) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

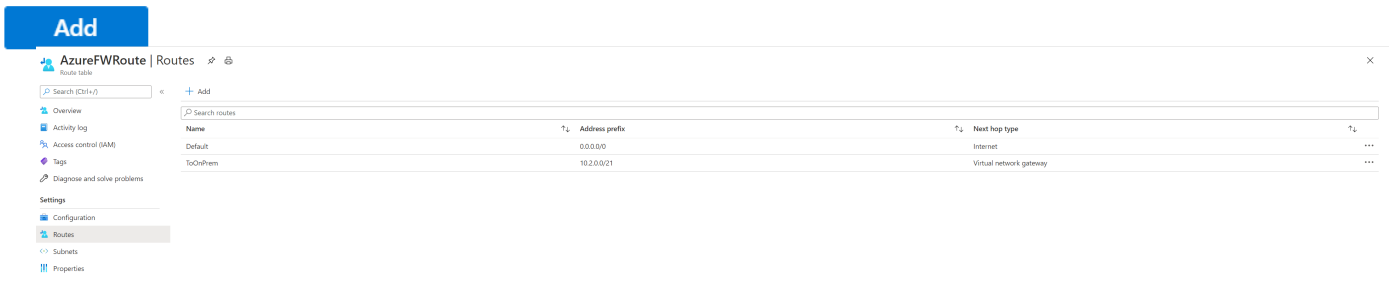
Virtual network gateway

- ( ) Use this virtual network's gateway

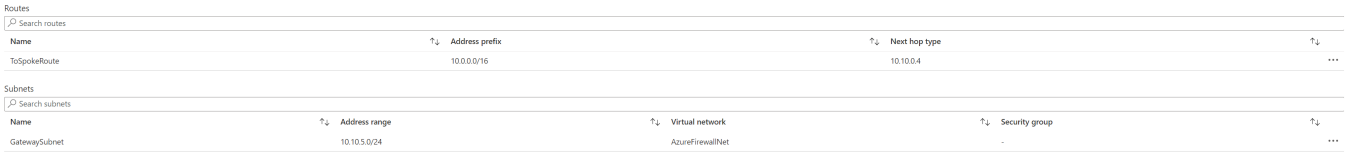
7. Create the routes



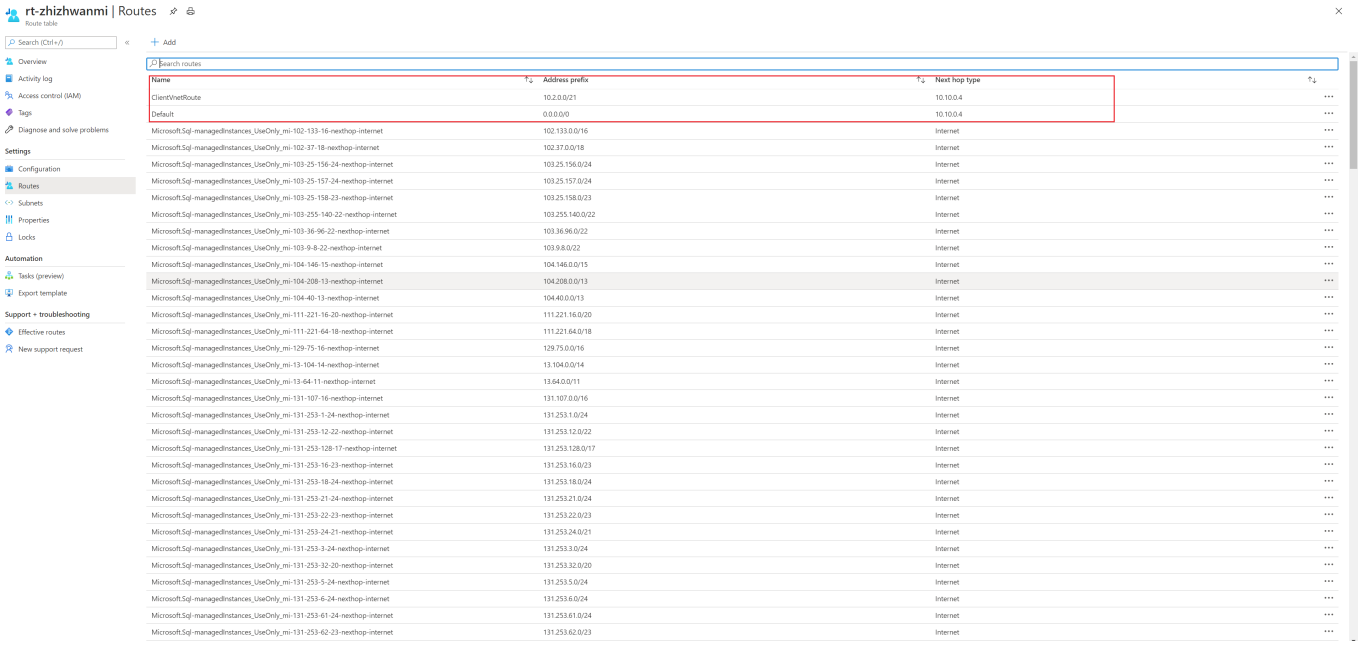
   - Create the routes for hub VNet - firewall subnet Route table for firewall subnet need default route 0.0.0.0/0 to internet and another route for On-premises VNet traffic through virtual network gateway.



   - Create the routes for hub VNet - Gateway subnet Route table for hub gateway subnet need to have route for MI traffic through azure firewall private IP address.



   - Modify the routes for MI subnet. Default 0.0.0.0/0 need to route to Azure firewall private IP address, while another route for client VNet traffic throught Azure firewall private IP address.



8. Test connection You can use any client which resides in on-premise Vnet to test the connection to MI using private connections.

Key things to take care

1. While in step 6, it's quite important that peering from spoke network (MI VNet) to set "Virtual network gateway" to "Use the remote virtual network's gateway" since connections from MI to on-premise need go through the hub network and use the hub gateway to communicate successfully.

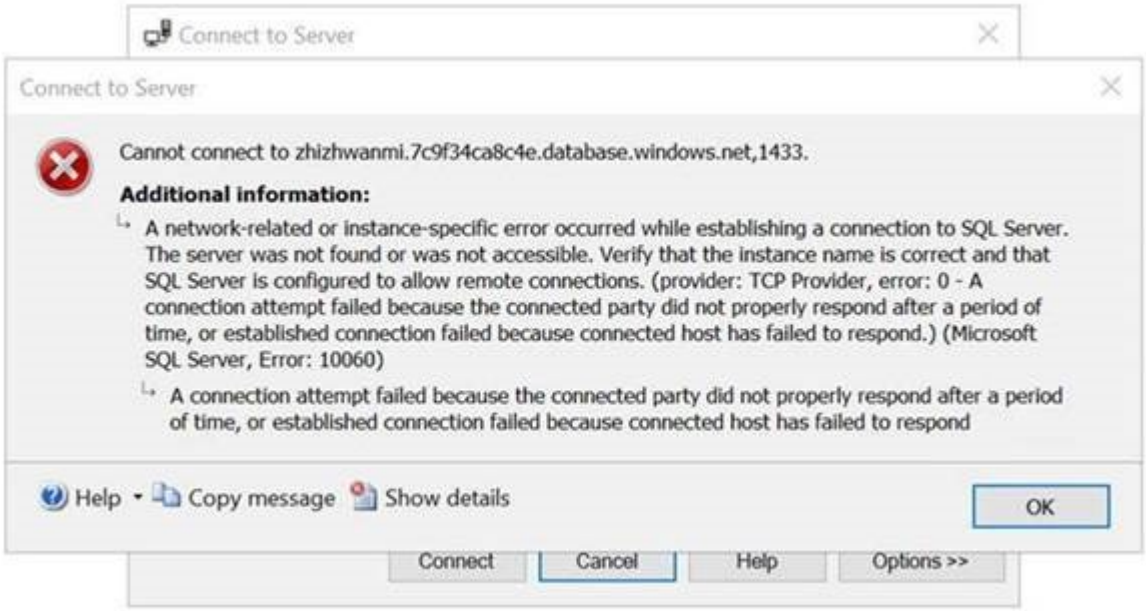
2. It is also important to know that you don't need any route table on client VNet because it can learn the routes automatically from gateway. However, for MI (or any other spoke network), you need special route

table to make sure connections pass through the Azure firewall for security validation. Take care of step 7 in above section.

3. In above sample, I didn't configure specific NSGs for client VNet, hub VNet. MI subnet is using default NSG with no additional inbound/outbound rules. If you want to configure any NSG for client VNet or hub VNet, make sure the connections are allowed through NSGs.

Common Errors

You may receive error 10060 when connect to MI from on-premise network.



Troubleshooting

This error message indicates client is unable to reach managed instance. This is usually caused by incorrect network settings like NSG, route table, gateway, virtual network peering settings.

Capture network trace on Client

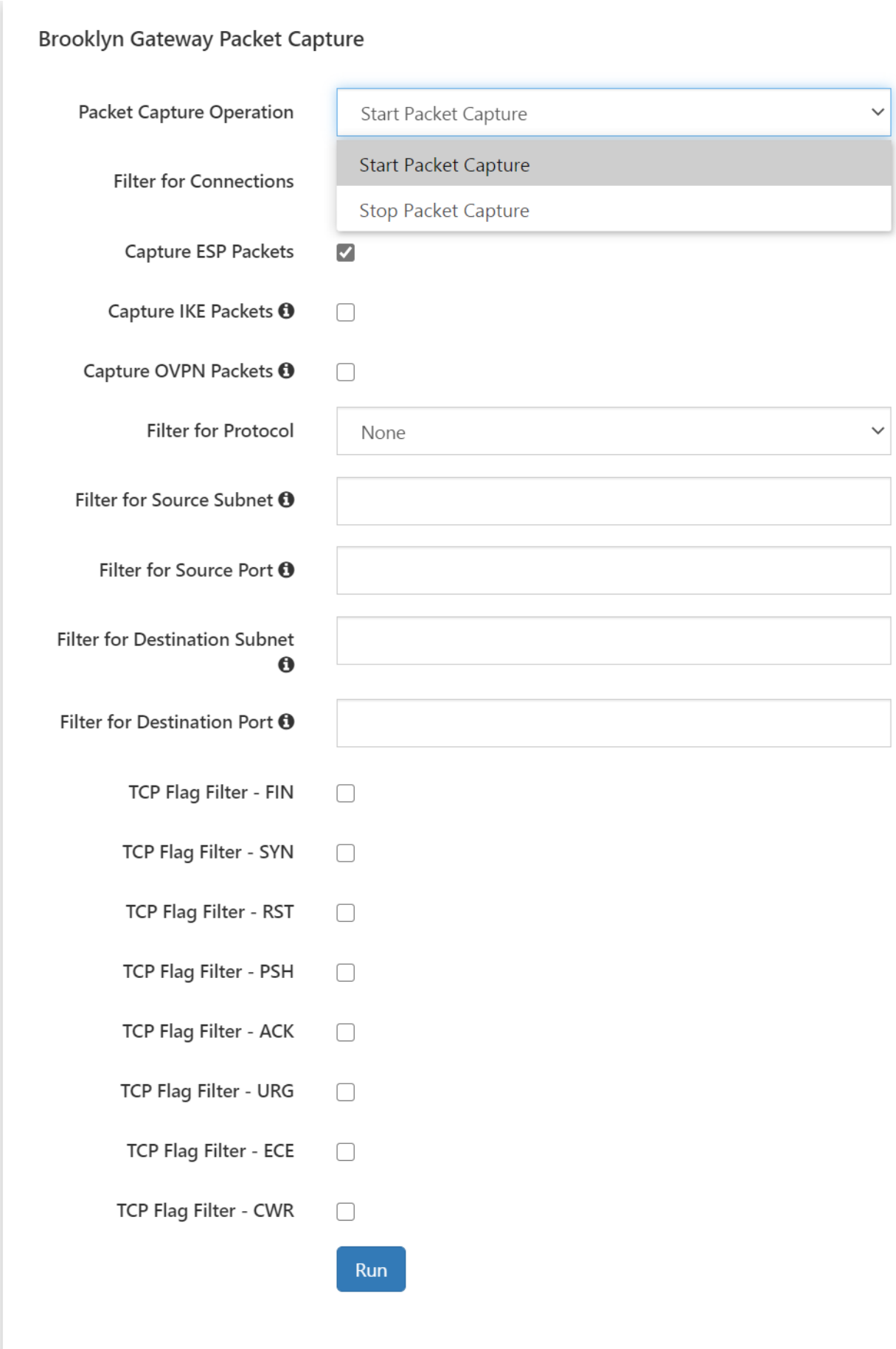
You can capture network trace on client using Netmon or nestsh or WireShark to verify in which phase the connection fails.

Capture network trace on Gateway

If you see there is no response packet from managed instance and want to further verify whether there is network packets passing through the gateway device. You can use ASC to capture network trace on Gateway.

1. Open ASC -> Resource Explorer -> Microsoft.Network -> virtualNetworkGateways - find your gateway device like "GW-OnPrem" in above sample
2. Select "Diagnostics" tab and "Brooklyn Gateway Packet Capture" subtab to start the packet capture on Gateway.


GW-OnPrem
Microsoft.Network/virtualNetworkGateways
Properties
Visual Debugging
Brooklyn Findings
Diagnostics
Brooklyn Logs
Operations
Resource Crud Troubleshooter
Insights
Access Control
Health
Host Packet Capture
Brooklyn Gateway Packet Capture
Brooklyn Gateway Flow Logging
Gateway Tenant Resource
Brooklyn Diagnostics



3. Reproduce the connection issue
4. Stop the network capture from same place in step 2.

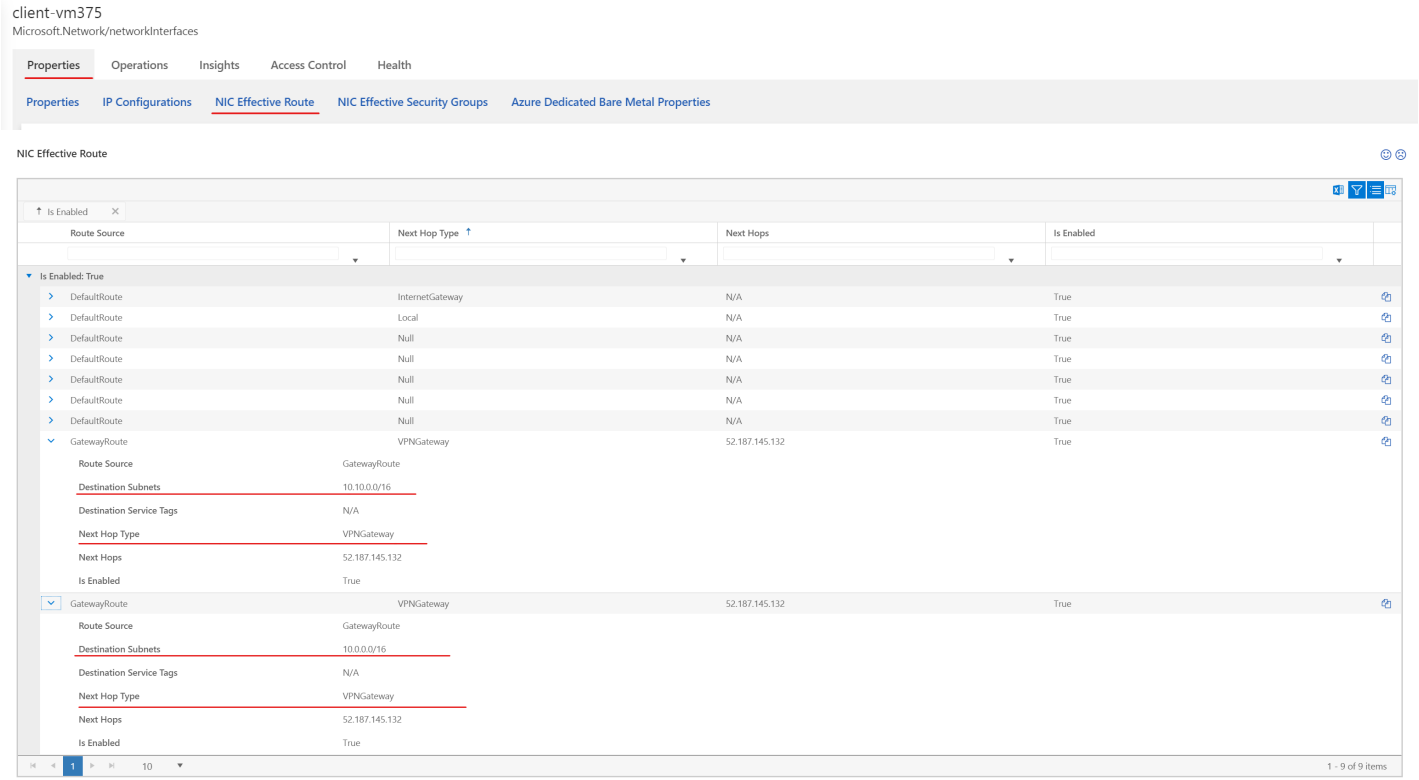
More information refer to Brooklyn Gateway Packet Captures & Diagnostics.

If you find any packet loss or packet not reaching gateway, you can open a collaboration task to Gateway CSS team.

Verify if client learn the routes correctly

Since my simulated on-premises client is on Azure VM. I am able to verify if it learns the routes correctly from ASC.

1. Open ASC -> Resource Explorer -> Microsoft.Network -> networkInterfaces - find your VM NIC device like "client-vm375" in my sample.
2. Select "Properties" tab and "NIC Effective Route" subtab to check the routes. In the hub-spoke architecture, you should see there are two routes learned automatically from Gateway that destination is hub network and spoke network (MI Vnet).



If you find there is no routes to spoke network, then the issue happens on VNET peering setting between hub and spoke network. Please check tip 2 in "Key things to take care" section. You have to recreate the VNET peering and reset the VPN Gateway after that.

For route or VNET peering issue, you can reach Azure Networking CSS for collaboration.

Public Doc Reference

General hub-spoke setup not specific to MI

How good have you found this content?