How to set up Site-to-Site VPN between Synology Router and Microsoft Azure

Site-to-Site VPN, powered by Synology VPN Plus, allows multiple networks in geographically different locations to establish secure connections to each other over the Internet.

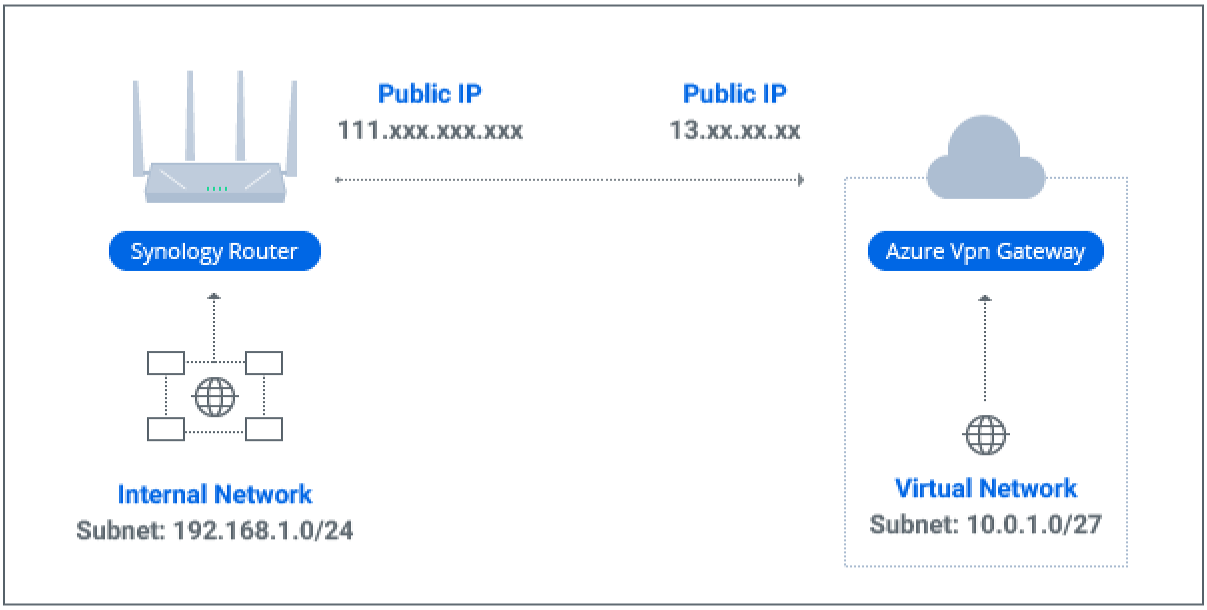
Aside from the benefits you may experience when using a Site-to-Site VPN tunnel between two Synology Router products, you may also implement a hybrid cloud solution by setting up such tunnel between a Synology Router and **Microsoft Azure Virtual Network** service.

This tutorial will guide you through the setup of Site-to-Site VPN between Synology Router and Microsoft Azure Virtual Network.

Contents

1. Before you start

Before you proceed with the Site-to-Site VPN setup, please make sure you have already had an adequate environment as described below.



- Set up your Synology Router **RT2600ac** or **RT1900ac**, and make sure it is running on SRM 1.1.5 or above.
- Install **VPN Plus Server** 1.2.0 or above.
- In VPN Plus Server, activate the **Site-to-Site VPN** feature.

  Note: For more information on our licensing plan, please refer to this **webpage**.

This tutorial is based on the scenario described below.

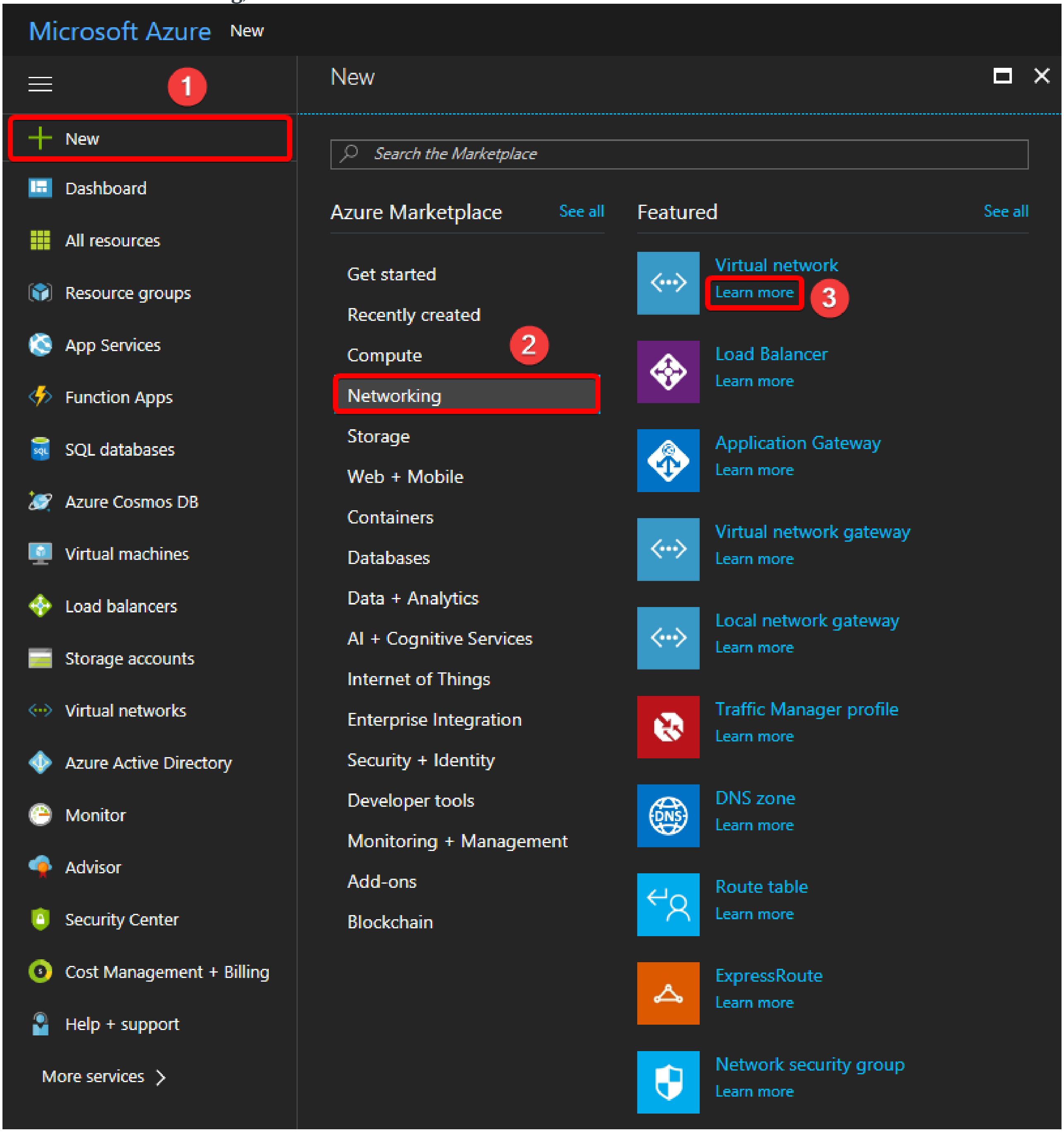
- **Synology Router** (**RT2600ac** or **RT1900ac**) site
  - Internal subnet: 192.168.1.0/24
  - Gateway: 111.xxx.xxx.xxx
- **Microsoft Azure** site
  - Internal subnet: 10.0.1.0/27
  - Gateway: 13.xx.xx.xx
- Pre-shared key: 123456789
- Encryption configuration:
  - Phase 1:
    - Encryption: AES128
    - Authentication: SHA-256
    - Key life: 28800
    - DH Group: 2 (modp 1024)
    - DPD (Dead Peer Detection): disable
  - Phase 2:
    - Encryption: AES128
    - Authentication: SHA-256
    - Key life: 27000
    - DH Group: 2 (modp 1024)

2. Site-to-Site VPN configuration on Microsoft Azure

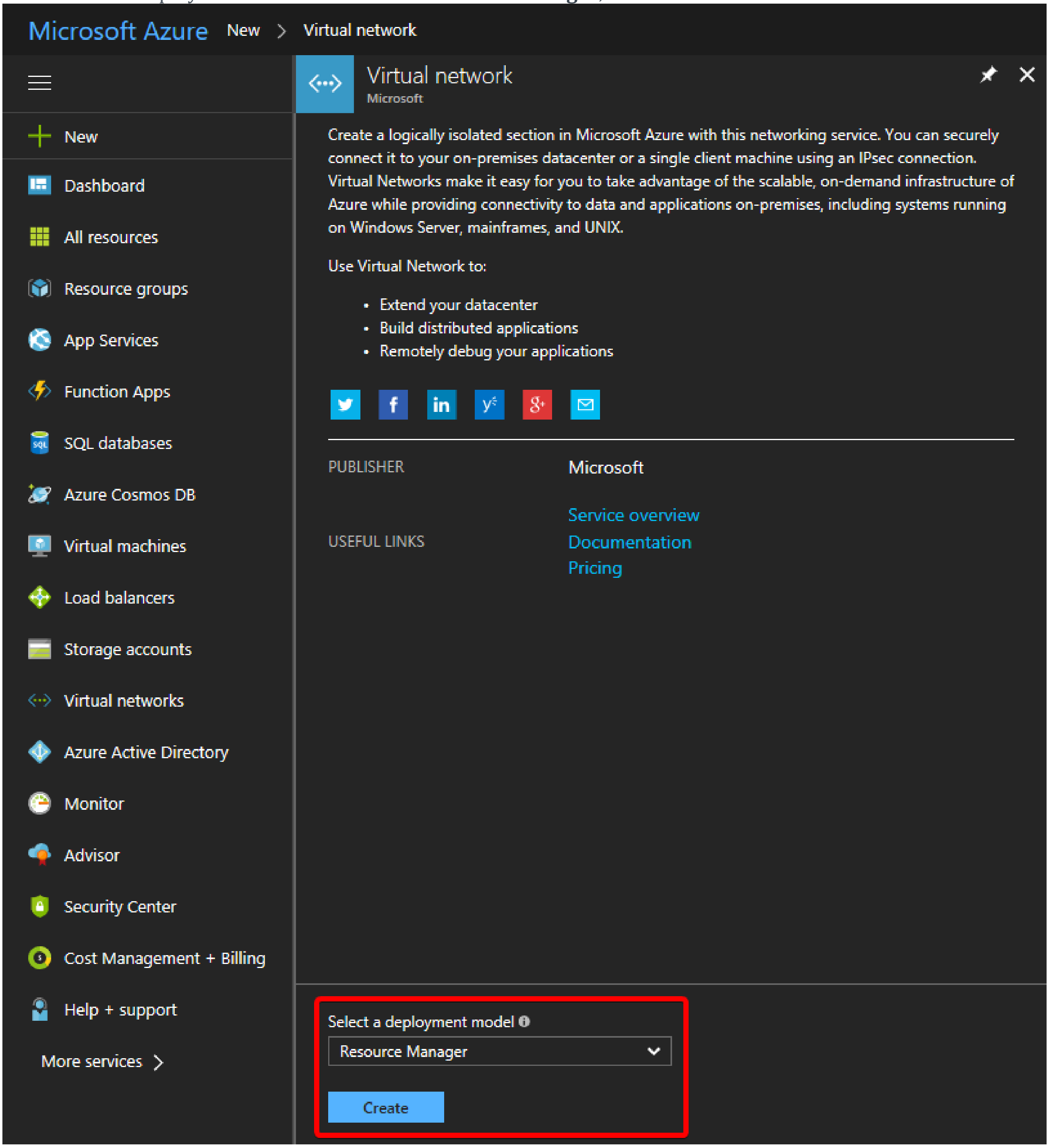
2.1 Create a virtual network

1. Log in to your **Microsoft Azure** account.

2. Go to **New** > **Networking**, and click **Learn more** under **Virtual network**.



3. Make sure the deployment model remains at **Resource Manager**, and click **Create**.



Create a logically isolated section in Microsoft Azure with this networking service. You can securely connect it to your on-premises datacenter or a single client machine using an IPsec connection. Virtual Networks make it easy for you to take advantage of the scalable, on-demand infrastructure of Azure while providing connectivity to data and applications on-premises, including systems running on Windows Server, mainframes, and UNIX.

Use Virtual Network to:

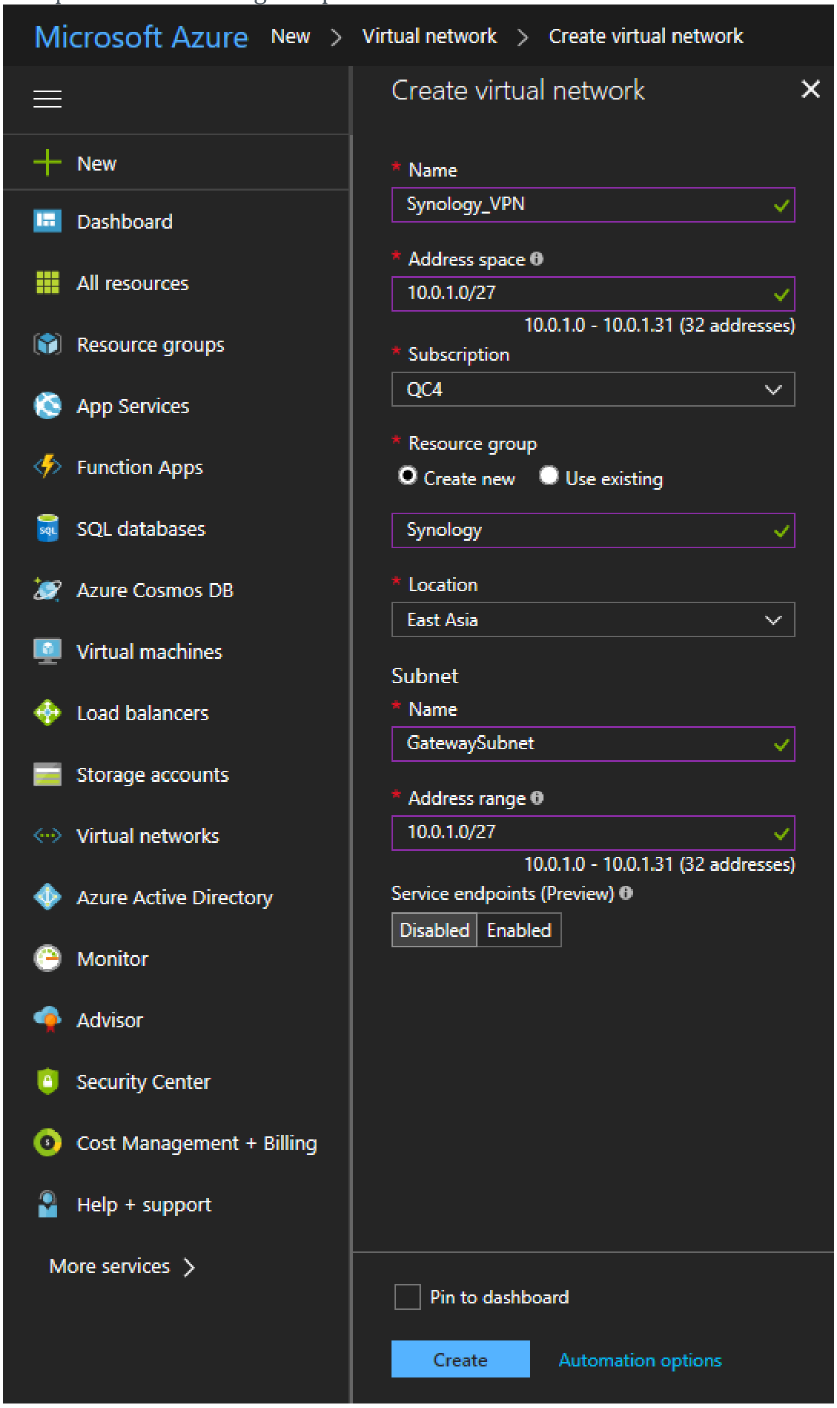
- Extend your datacenter
- Build distributed applications
- Remotely debug your applications

PUBLISHER Microsoft

USEFUL LINKS Service overview, Documentation, Pricing

Select a deployment model: Resource Manager

4. Complete the following setup to create a virtual network:



Create virtual network

* Name
Synology_VPN

* Address space
10.0.1.0/27
10.0.1.0 - 10.0.1.31 (32 addresses)

* Subscription
QC4

* Resource group
● Create new ○ Use existing
Synology

* Location
East Asia

Subnet
* Name
GatewaySubnet

* Address range
10.0.1.0/27
10.0.1.0 - 10.0.1.31 (32 addresses)

Service endpoints (Preview)
Disabled | Enabled

□ Pin to dashboard

Create   Automation options

a. **Name**: Here, we enter "*Synology_VPN*".

  b. **Address space**: Specify the address range for the virtual network. Here, we enter *10.0.1.0/27*.

  c. **Subscription**: Select your subscription to Microsoft Azure service.

  d. **Resource group**: Here, we select **Create new** and enter "*Synology*".

  e. **Location**: Select the location of your virtual network.

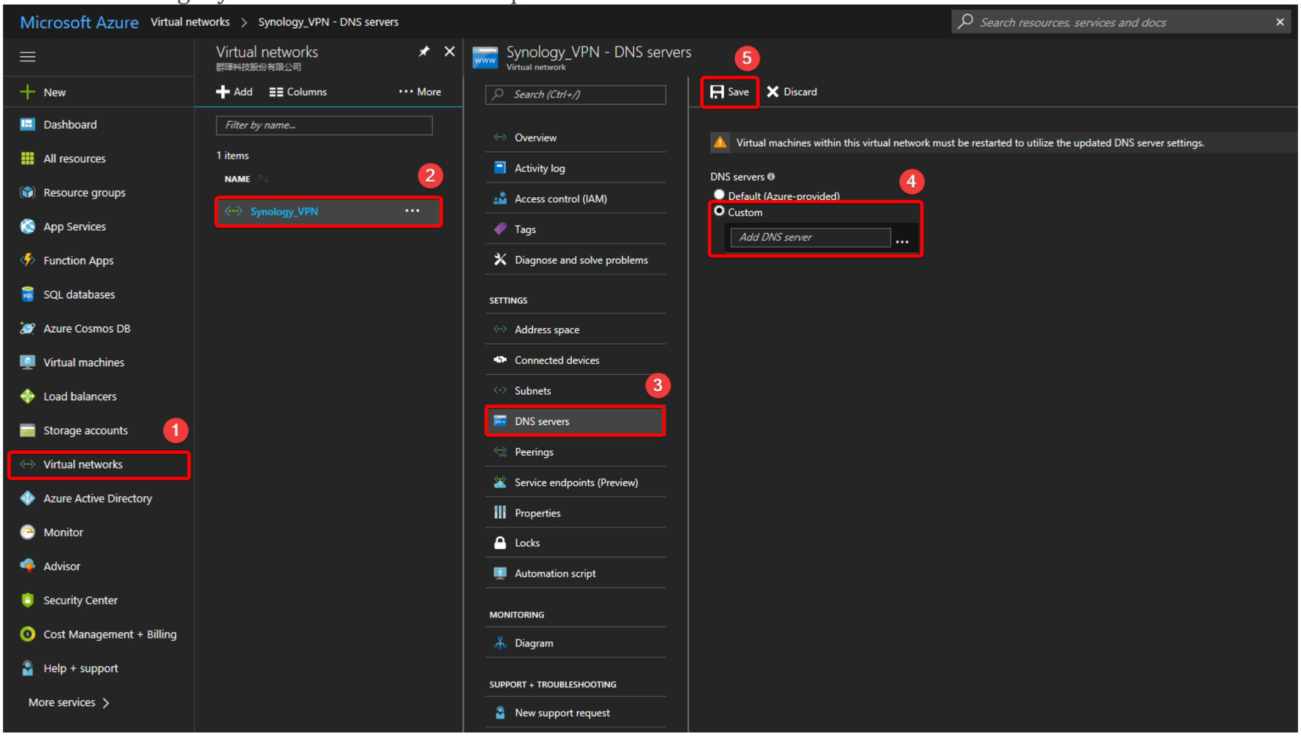
  f. Specify the properties of the **Subnet**:

    a. **Name**: Here, we enter "*GatewaySubnet*".

    b. **Address range**: Specify the address range for the subnet. This range must be within or equal to the **Address space** configured above. Here, we enter *10.0.1.0/27*

    g. Click **Create** when the setting is complete.

5. Do the following if you wish to connect to a specific DNS server:



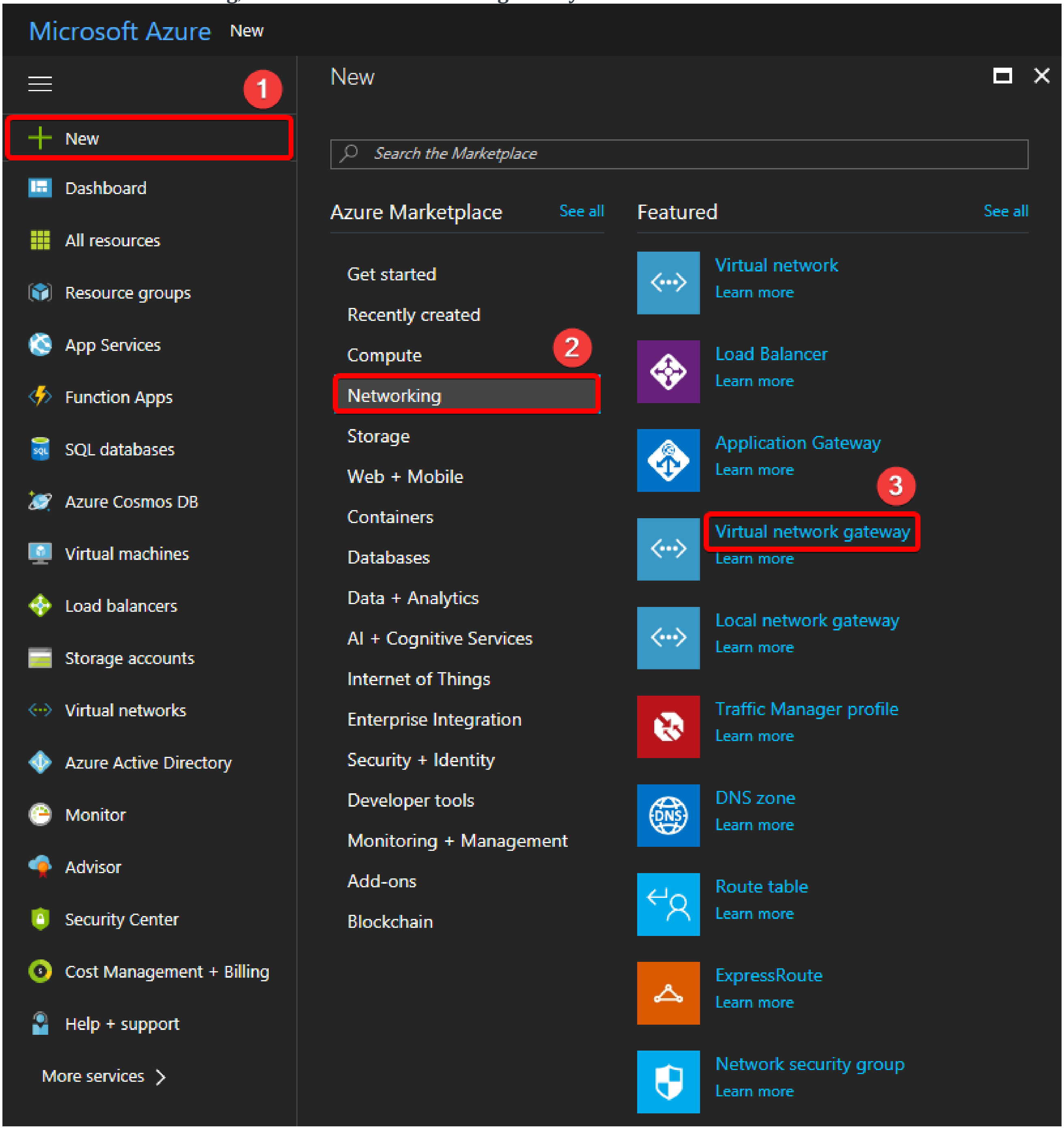
Virtual machines within this virtual network must be restarted to utilize the updated DNS server settings.

. In the just now created *Synology_VPN*, go to **DNS servers** under **SETTINGS** section.

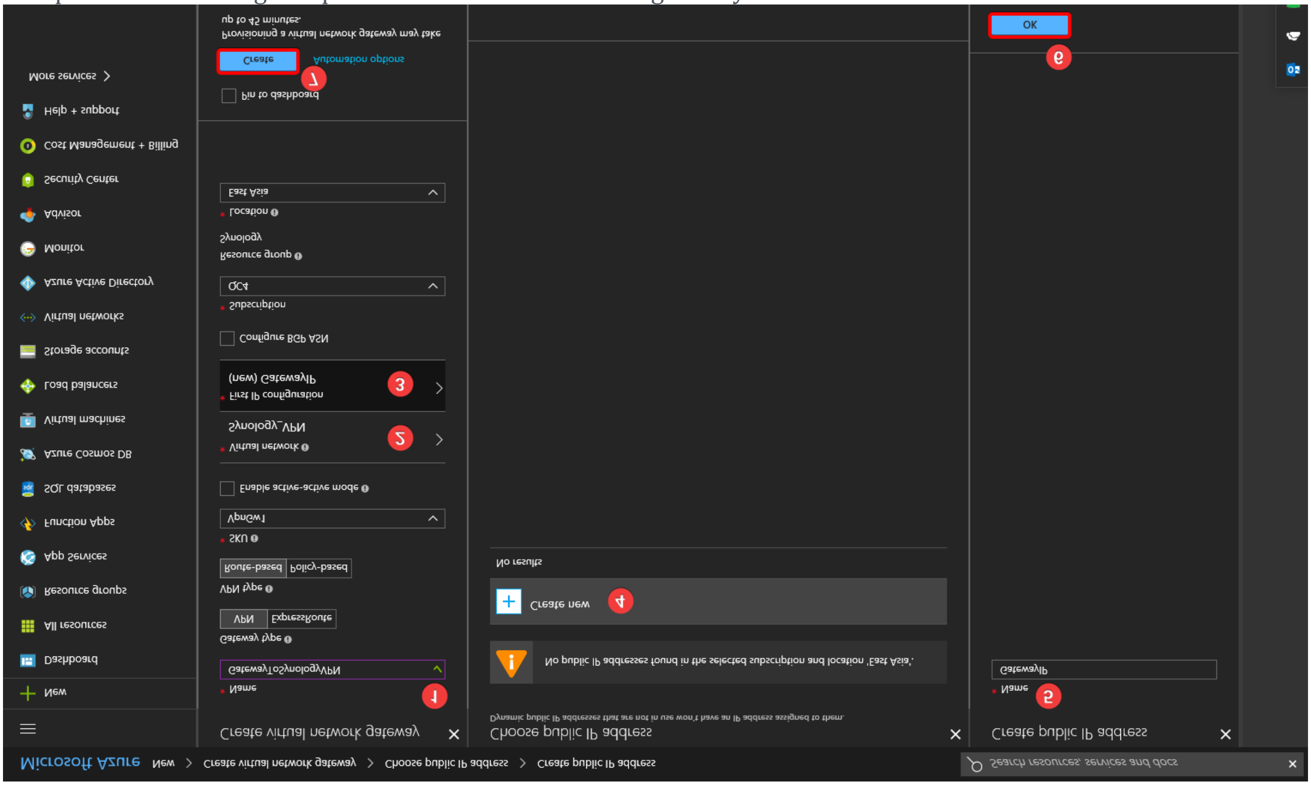
  a. Select **Custom**, and specify the DNS server address.

2.2 Create Virtual Network Gateway

1. Go to **New** > **Networking**, and click **Virtual network gateway**.



2. Complete the following setup to create a virtual network gateway:



Microsoft Azure New > Create virtual network gateway > Choose public IP address > Create public IP address

Create virtual network gateway

- Name: GatewayToSynologyVPN
- Gateway type: VPN | ExpressRoute
- VPN type: Route-based | Policy-based
- SKU: VpnGw1
- □ Enable active-active mode
- Virtual network: Synology_VPN
- First IP configuration: (new) GatewayIP
- □ Configure BGP ASN
- Subscription: QC4
- Resource group: Synology
- Location: East Asia
- □ Pin to dashboard
- Create | Automation options
- Provisioning a virtual network gateway may take up to 45 minutes.

Choose public IP address

Dynamic public IP addresses that are not in use won't have an IP address assigned to them.

No public IP addresses found in the selected subscription and location 'East Asia'.

Create new

No results

Create public IP address

- Name: GatewayIP
- OK

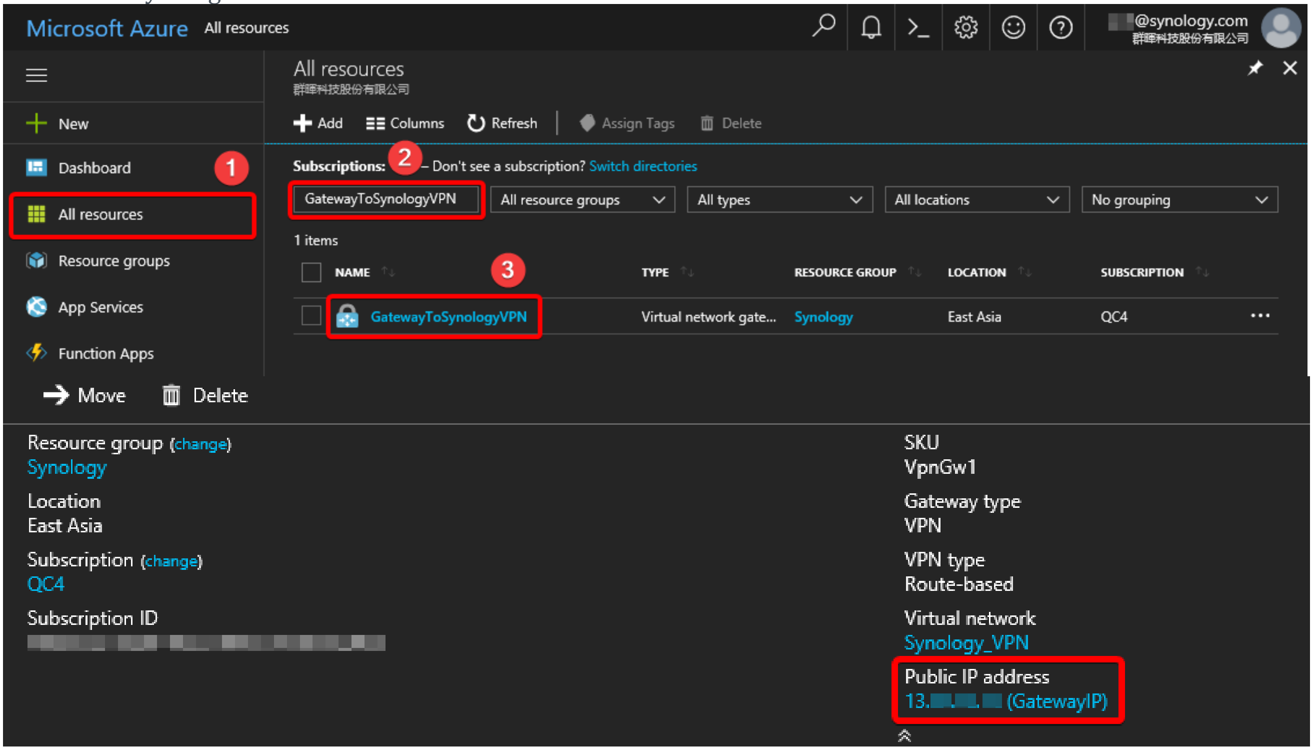
a. **Name**: Here, we enter "*GatewayToSynologyVPN*".

b. Click **Virtual network**, and select the just now created *Synology_VPN*.

c. Click **First IP configuration** > **Create new**, and here, we enter *Gateway IP*.

d. Click **Create** when the setting is complete.

3. Go to **All resources**, and search for the just now created "*GatewayToSynologyVPN*". You will then find the automatically assigned **Public IP address**.



Microsoft Azure All resources

All resources
群暉科技股份有限公司

Subscriptions: – Don't see a subscription? Switch directories

GatewayToSynologyVPN | All resource groups | All types | All locations | No grouping

1 items

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
GatewayToSynologyVPN	Virtual network gate...	Synology	East Asia	QC4

Resource group (change)
Synology

Location
East Asia

Subscription (change)
QC4

Subscription ID
[redacted]

SKU
VpnGw1

Gateway type
VPN

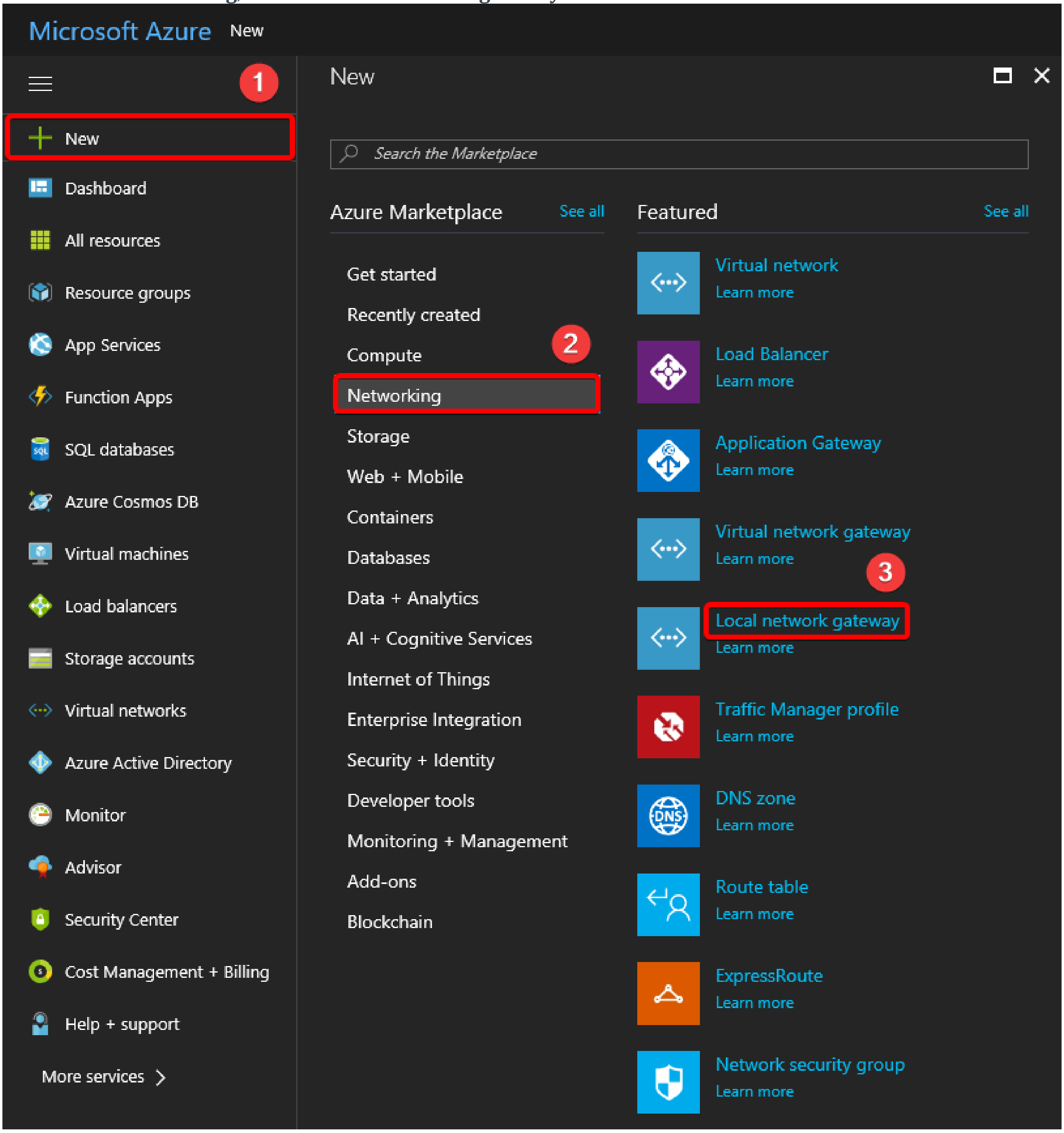
VPN type
Route-based

Virtual network
Synology_VPN

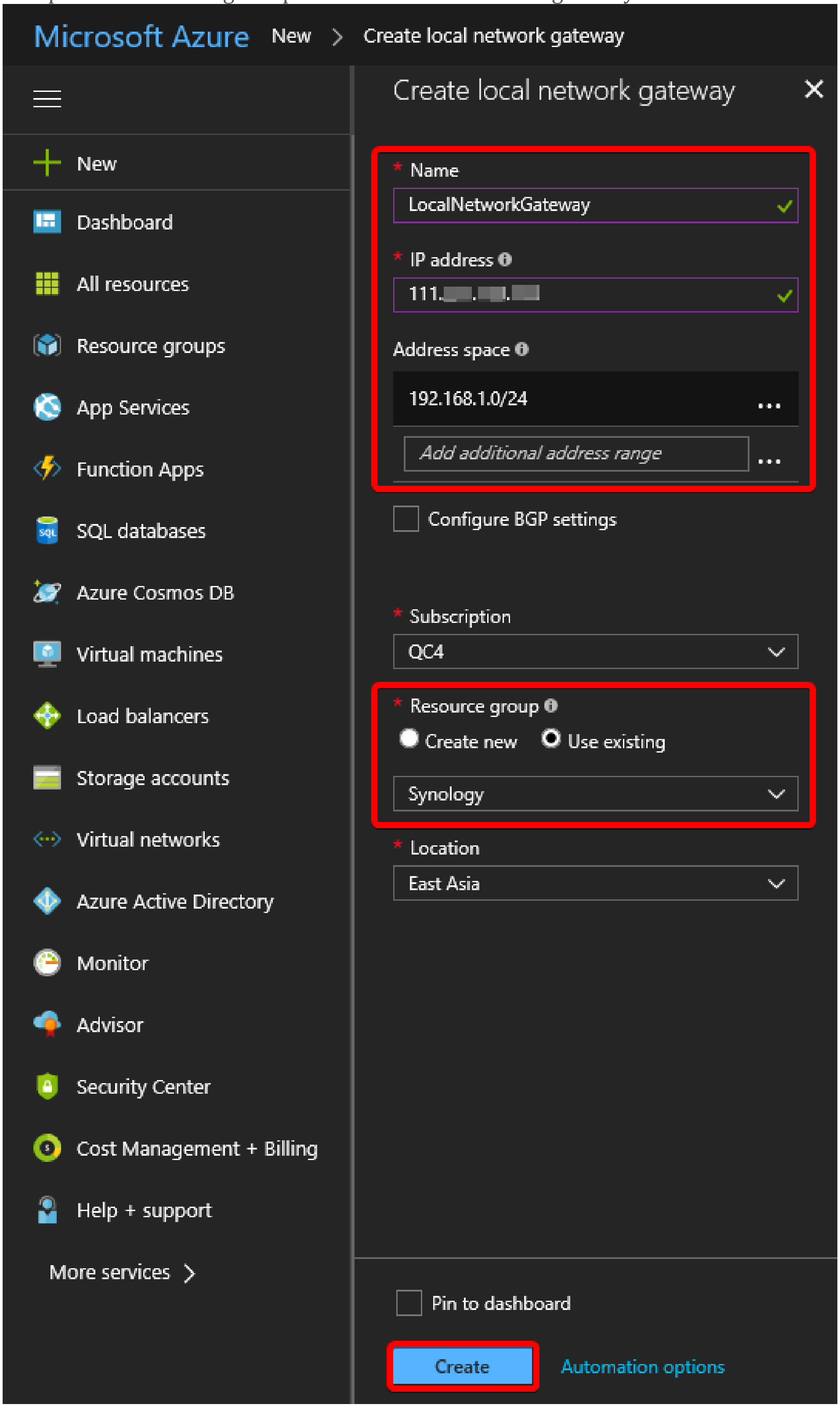
Public IP address
13.[redacted].[redacted].[redacted] (GatewayIP)

2.3 Create Local Network Gateway

1. Go to **New** > **Networking**, and click **Local network gateway**.



2. Complete the following setup to create a local network gateway:



Create local network gateway

* Name: LocalNetworkGateway

* IP address: 111.[redacted]

Address space: 192.168.1.0/24

Add additional address range

□ Configure BGP settings

* Subscription: QC4

* Resource group: ○ Create new ● Use existing

Synology

* Location: East Asia

□ Pin to dashboard

Create Automation options

a. **Name**: Here, we enter "*LocalNetworkGateway*".

b. **IP address**: Enter the IP address of your Synology Router.

c. **Address space**: Specify the internal subnet of your Synology Router. Here, we enter "*192.168.1.0/24*".

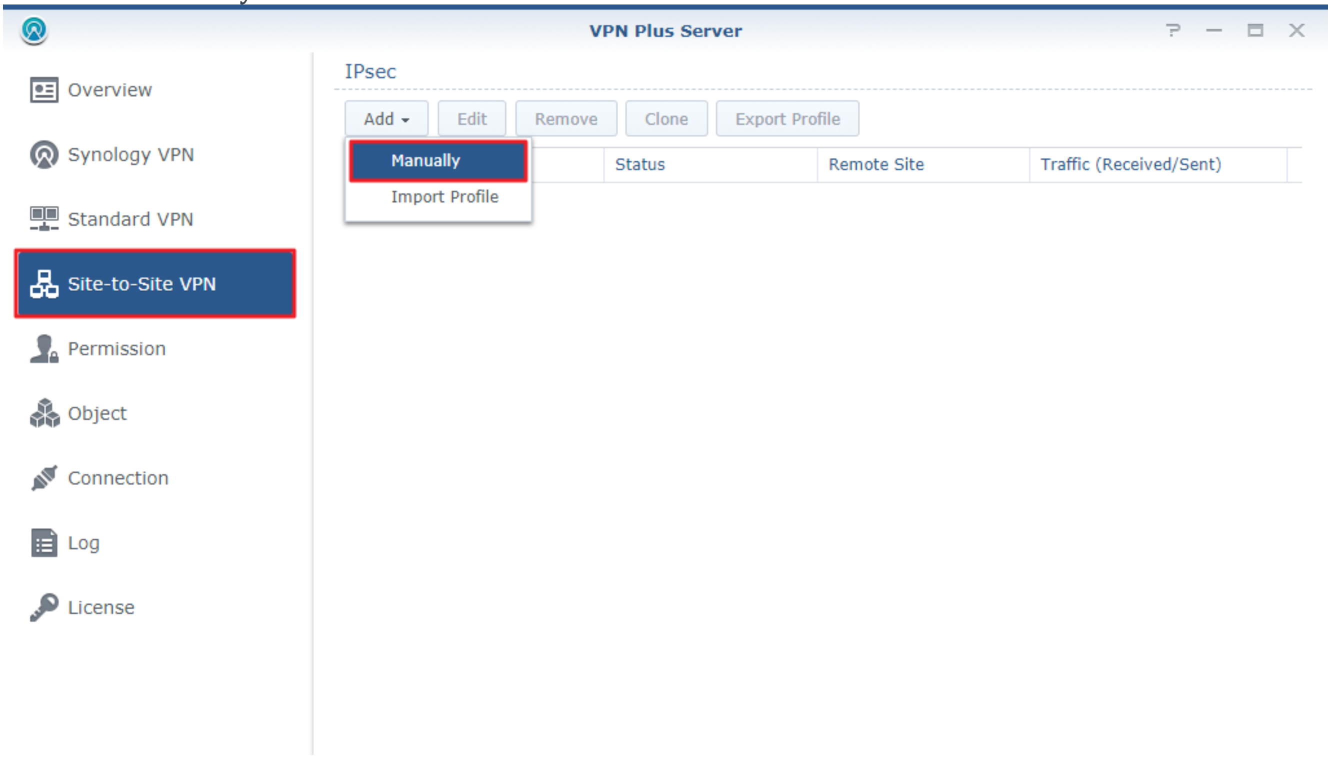
d. **Resource group**: Select **Use existing**, and select the previously created **Synology** from the drop-down list.

e. Click **Create** when the setting is complete.

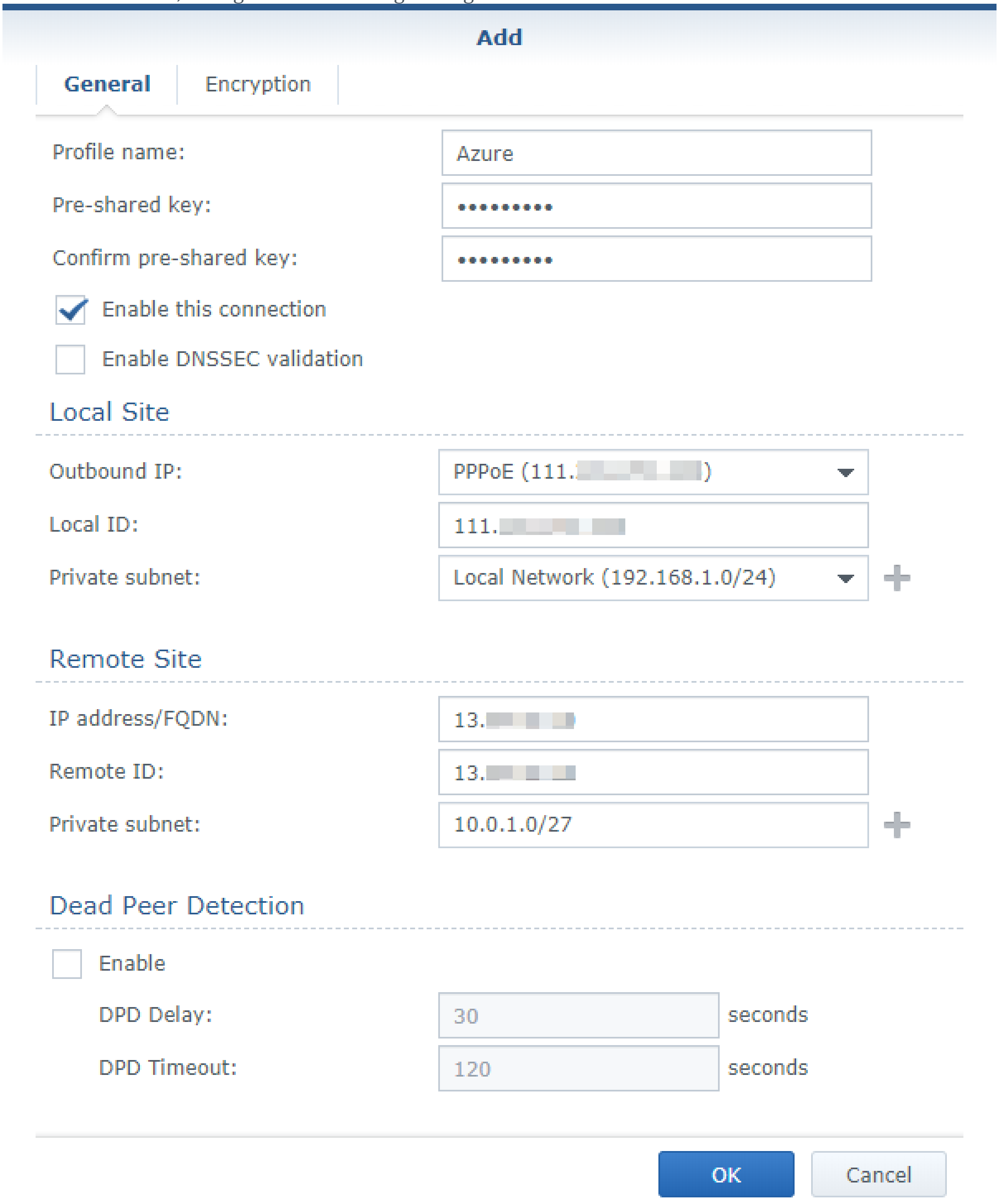
3. Site-to-Site VPN configuration on Synology Router

Sign in to SRM on your Synology Router, and follow the steps below.

1. Go to **VPN Plus Server** > **Site-to-Site VPN**.
2. Click **Add** > **Manually**.



3. In the **General** tab, configure the following settings:



Add

General | Encryption

Profile name: Azure

Pre-shared key: •••••••••

Confirm pre-shared key: •••••••••

☑ Enable this connection

□ Enable DNSSEC validation

Local Site

Outbound IP: PPPoE (111.[redacted])

Local ID: 111.[redacted]

Private subnet: Local Network (192.168.1.0/24)

Remote Site

IP address/FQDN: 13.[redacted]

Remote ID: 13.[redacted]

Private subnet: 10.0.1.0/27

Dead Peer Detection

□ Enable

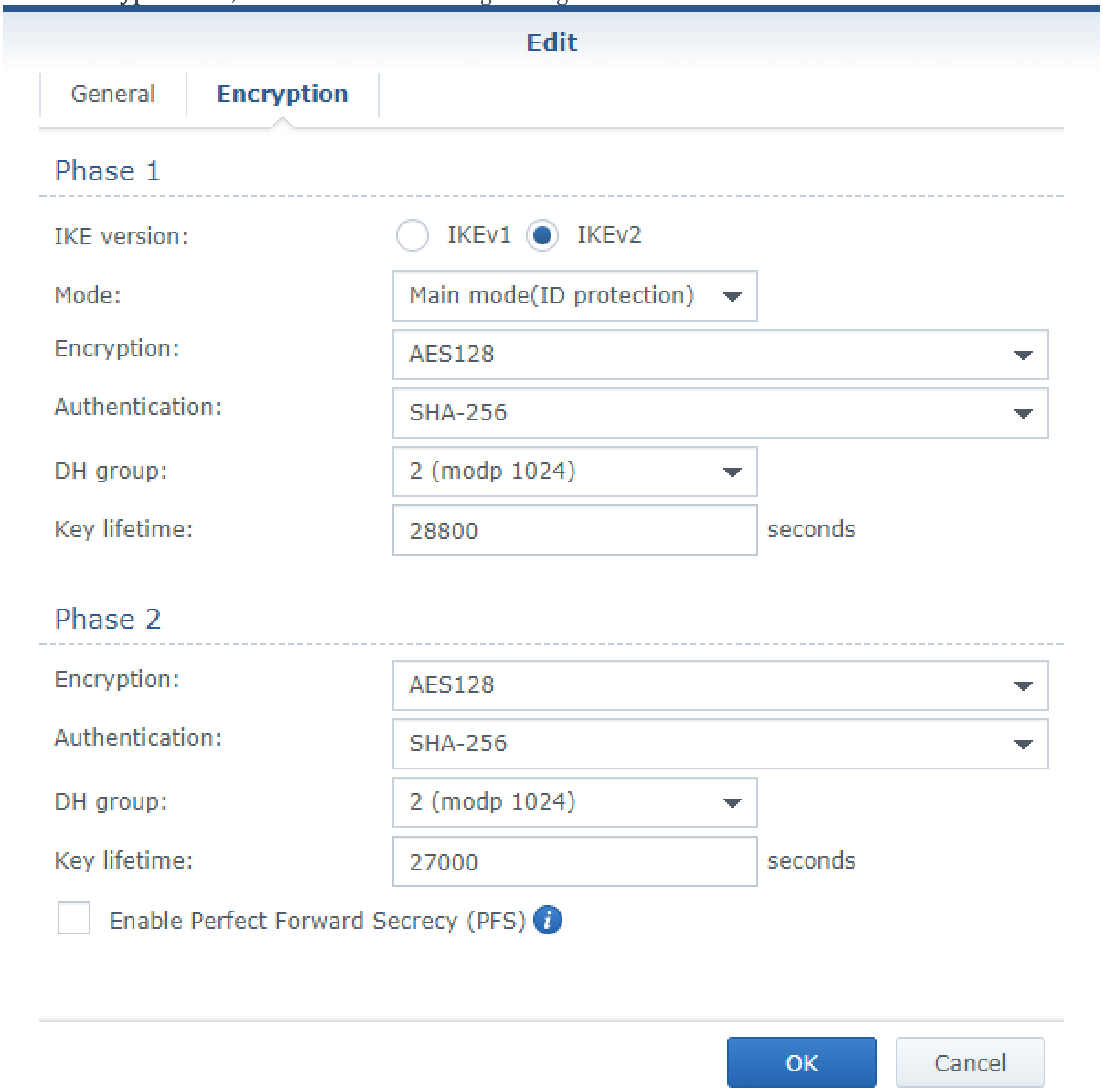
DPD Delay: 30 seconds

DPD Timeout: 120 seconds

- **Profile name**: Enter a customized name for the profile. Here, we enter "*Azure*".
- **Pre-shared key**: Here, we enter "*123456789*".
- Under **Local Site** section, configure the following settings:
  - **Outbound IP**: Enter Synology Router's IP address. Here, we enter *111.xxx.xxx.xxx*.
  - **Local ID**: You can enter a public IP address or FQDN to specify the Local ID. Here, we enter *111.xxx.xxx.xxx*.
  - **Private subnet**: Specify the local network under the private subnet of Synology Router. Here, we select *Local Network (192.168.1.0/24)*.
- Under **Remote Site** section, configure the following settings:

    - **IP address/FQDN**: Enter the public IP address of Microsoft Azure site. Here, we enter *13.xx.xx.xx*.
    - **Remote ID**: You can enter a public IP address or FQDN to specify the Remote ID. Here, we enter *13.xx.xx.xx*.
    - **Private subnet**: Specify the local network under the private subnet of Microsoft Azure. Here, we enter *10.0.1.0/27*.
  - Under **Dead Peer Detection** section, make sure the checkbox remains unticked.

4. In the **Encryption** tab, make sure the following settings are identical with those on the other site:



Phase 1

IKE version: ○ IKEv1 ● IKEv2

Mode: Main mode(ID protection)

Encryption: AES128

Authentication: SHA-256

DH group: 2 (modp 1024)

Key lifetime: 28800 seconds

Phase 2

Encryption: AES128

Authentication: SHA-256

DH group: 2 (modp 1024)

Key lifetime: 27000 seconds

□ Enable Perfect Forward Secrecy (PFS)

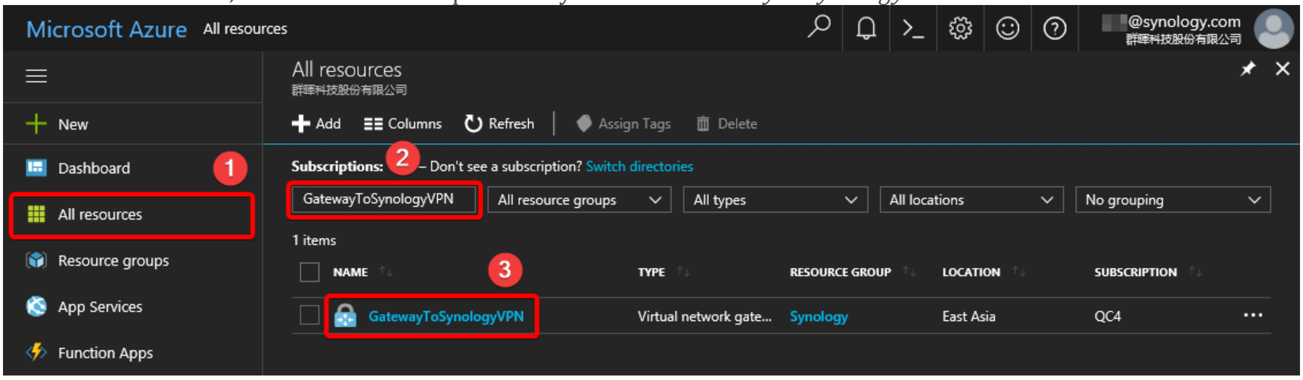
  - Under **Phase 1** section:
    - **IKE version**: Select **IKEv2**.
    - **Mode**: Select **Main mode (ID protection)**.
    - **Encryption**: Select **AES128**.
    - **Authentication**: Select **SHA-256**.
    - **DH group**: Select **2 (modp 1024)**.

- **Key lifetime**: Select **28800** seconds.

- Under **Phase 2** section:
  - **Encryption**: Select **AES128**.
  - **Authentication**: Select **SHA-256**.
  - **DH group**: Select **2 (modp 1024)**.
  - **Key lifetime**: Select **27000** seconds.
  - Make sure the **Enable Perfect Forward Secrecy (PFS)** checkbox remains unticked.

4. Establish connection between Synology Router and Microsoft Azure

1. Go to **All resources**, and search for the previously created "*GatewayToSynologyVPN*".



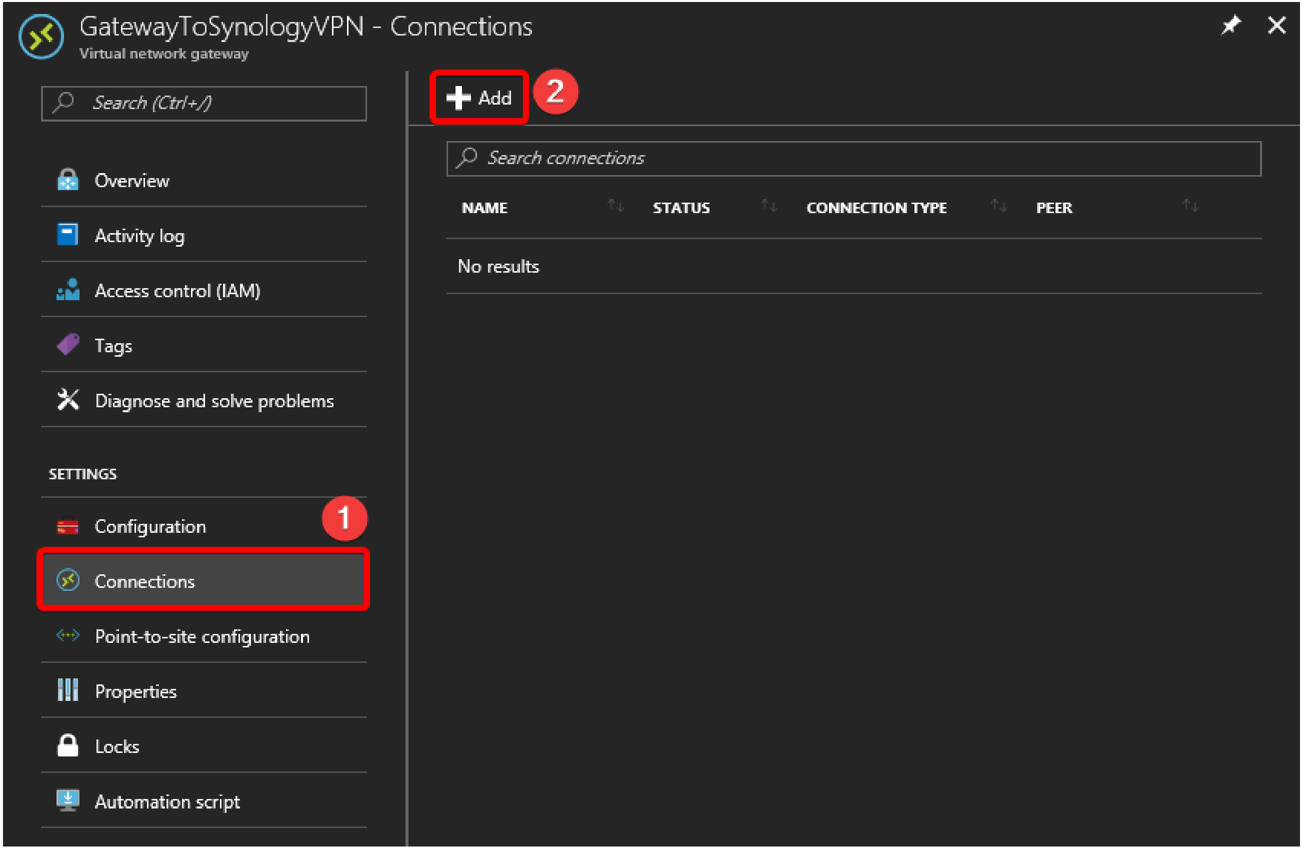
Subscriptions: – Don't see a subscription? Switch directories

GatewayToSynologyVPN	All resource groups	All types	All locations	No grouping

1 items

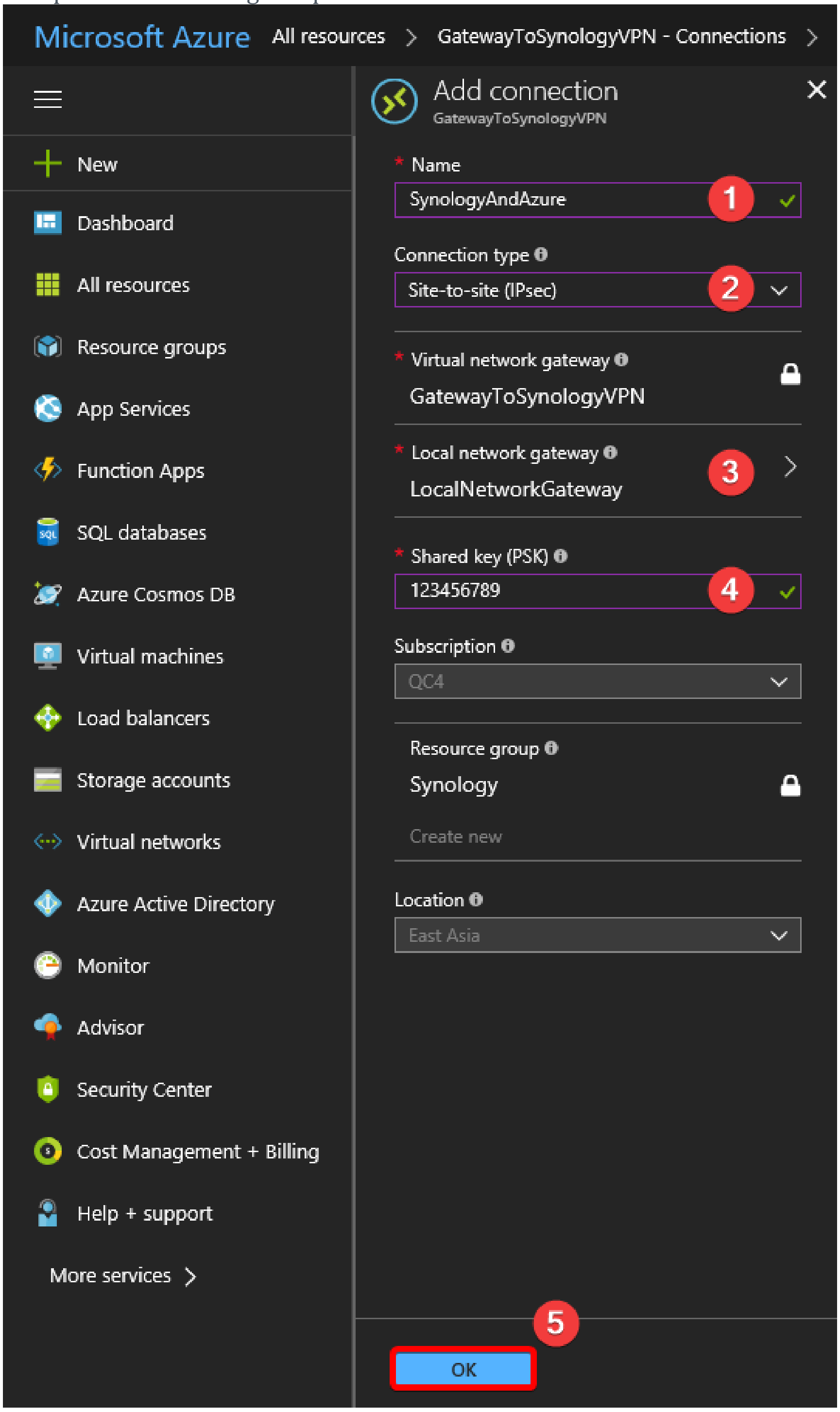
NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
GatewayToSynologyVPN	Virtual network gate...	Synology	East Asia	QC4

2. Go to **Connections**, and click **Add**.



NAME	STATUS	CONNECTION TYPE	PEER
No results			

3. Complete the following setup to create the Site-to-Site VPN connection:



Add connection
GatewayToSynologyVPN

* Name: SynologyAndAzure

Connection type: Site-to-site (IPsec)

* Virtual network gateway: GatewayToSynologyVPN

* Local network gateway: LocalNetworkGateway

* Shared key (PSK): 123456789

Subscription: QC4

Resource group: Synology

Location: East Asia

a. **Name**: Here, we enter *SynologyAndAzure*.

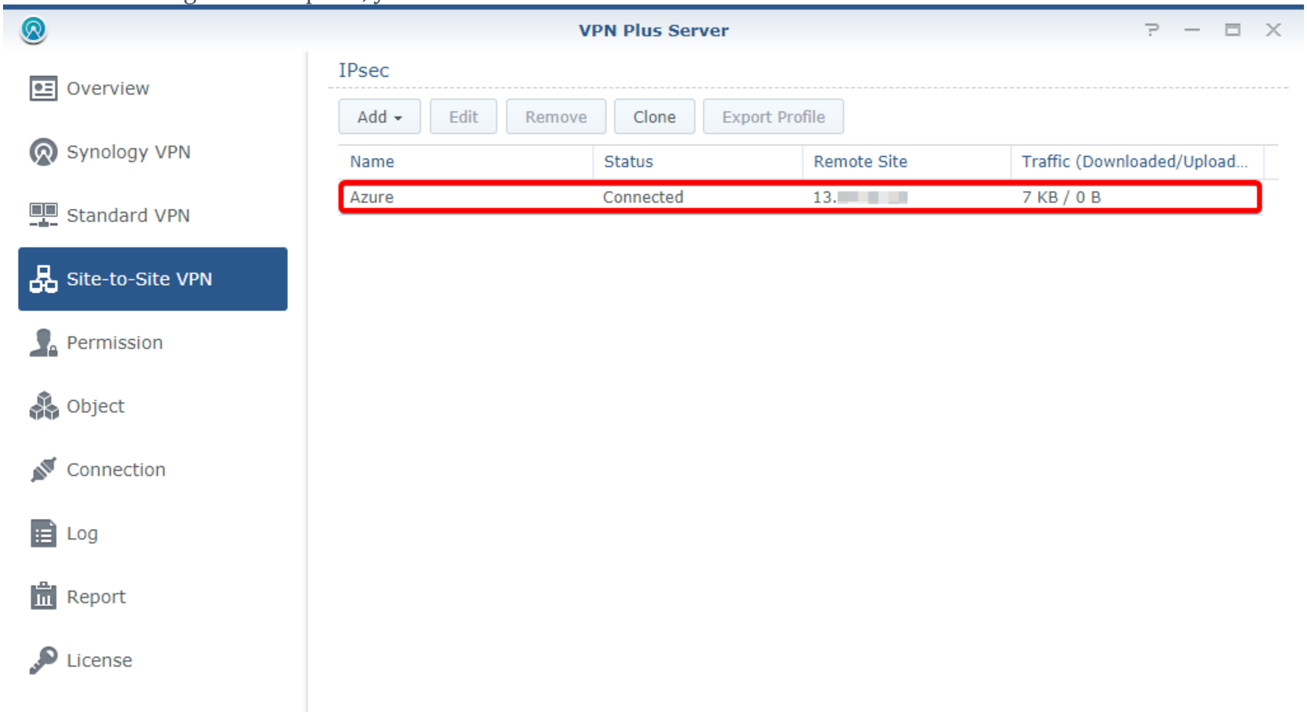
b. **Connection type**: Select **Site-to-site (IPsec)**.

c. Click **Local network gateway** to select the previously created *LocalNetworkGateway*.

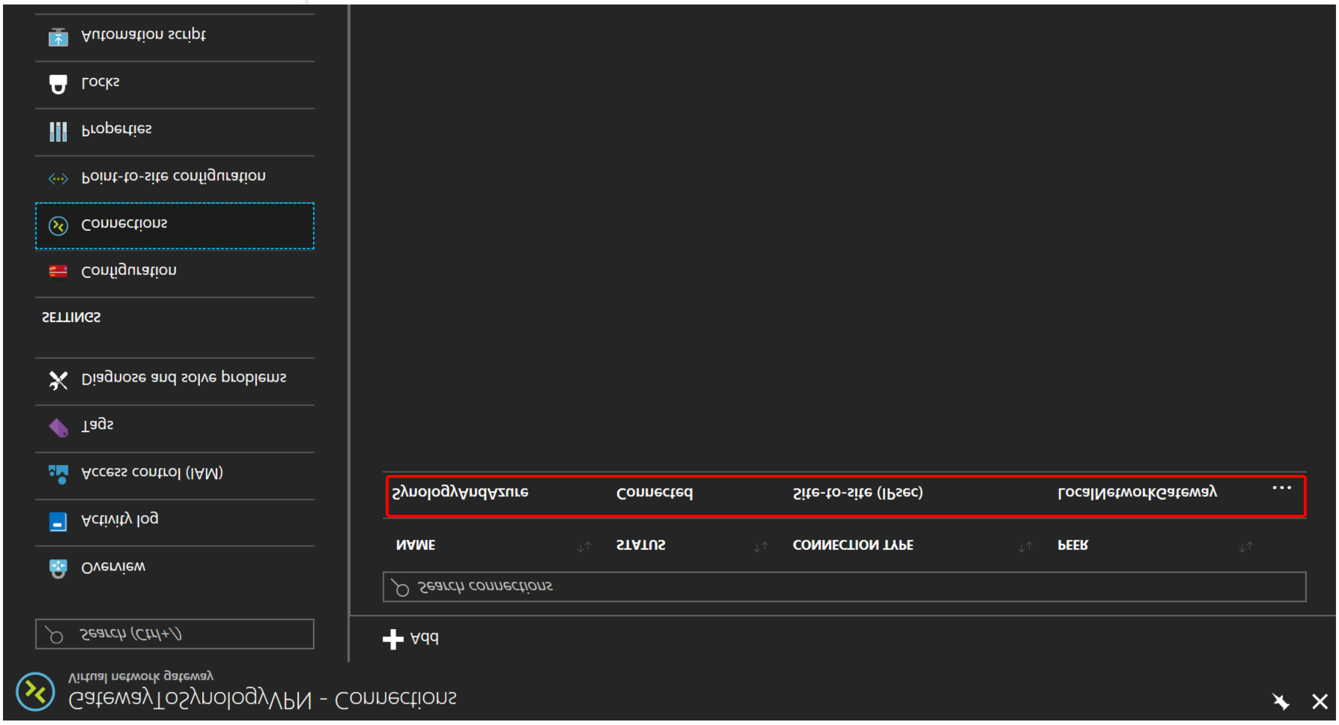
d. **Shared key(PSK)**: Specify the same pre-shared key as on Synology Router. Here, we enter "*123456789*".

e. Click **OK** when the setting is complete.

4. When the settings are complete, you will see the status of Site-to-Site VPN tunnel on each of the two sites.



Name	Status	Remote Site	Traffic (Downloaded/Upload...
Azure	Connected	13.[redacted]	7 KB / 0 B



NAME	STATUS	CONNECTION TYPE	PEER
SynologyAndAzure	Connected	Site-to-site (IPsec)	LocalNetworkGateway