Technical Guide

AMF Plus Cloud on Microsoft Azure Installation Guide

Installation Guide

Introduction

AMF Plus Cloud is a scalable cloud-based network management platform. It supports Allied Telesis switching, firewall, and wireless products, as well as a wide range of third-party devices.

This installation guide enables you to install and configure your AMF Plus Cloud in a Microsoft Azure cloud environment.

Note: This document contains a lot of Azure-specific terminology. For more detailed information about Azure terms and concepts, please refer to the Azure documentation. Also, the screen-shots shown were current at the time of creation, but are subject to change.

Related documents

For details about the AMF Plus Cloud system requirements, please refer to the AMF Plus Cloud Datasheet.

For more information about AMF Plus Cloud, refer to the AMF Plus Cloud documentation.

Contents

Procedure overview

The general procedure for setting up this product on Azure is as follows:

1. "Create an Azure image"

Upload the VHD image file of this product to Azure to create an Azure image.

2. "Create an SSH key pair"

Create an SSH key pair to be used for SSH access.

3. "Create an instance"

Create an instance (virtual machine) of this product from the image created in Step 1.

4. "SSH connection settings"

Access the instance using an SSH client (for example, PuTTY).

5. "Connection to user network (single mode)"

In single mode, an IPsec VPN is established between the user network to allow this product to communicate securely with AMF-compatible devices on the user network.

6. "Connection with tenant networks (multi-tenant mode)" (optional)

In multi-tenant mode, an L2TPv3 + IPsec VPN is established between each tenant network to allow AMF containers on this product to communicate securely with AMF-compatible devices on the tenant network.

Create an Azure image

The standard way to create virtual machines on Azure is to use a Virtual Machine Image. A virtual machine image is a **template** containing all the information needed to create instances of a specific type.

To allow the creation of AMF Plus Cloud instances on Azure, an AMF Plus Cloud virtual machine image is needed.

The following section covers downloading AMF Plus Cloud from the Allied Telesis Download Center, and the requirements to upload the Virtual Hard Disk (VHD) image to your Azure account as a virtual machine image.

Prerequisites

To create an Azure AMF Plus Cloud image, you will need access to the following:

- A PC, connected to the Internet.
- An Azure account.
- An Azure AMF Plus Cloud VHD image. This can be downloaded from the Allied Telesis Download Center.
- The Microsoft Azure CLI. This can be downloaded from https://docs.microsoft.com/en-us/cli/azure/install-azure-cli.

Note: This process was tested with version 2.51. Later versions of the Microsoft Azure CLI will likely also work, but have not been specifically tested.

Uncompress the VHD image

The VHD image downloaded from the Allied Telesis Download Center will be in a compressed .gz format. Before it can be used, it must be uncompressed.

Using gunzip

On platforms where it is supported, such as Unix and Linux, the .gz file can be uncompressed using the **gunzip** command. To uncompress the file, use the following command:

```
gunzip <name_of_file.gz>
```

Using 7-Zip

On platforms where gunzip is not available, such as Windows, use 7-Zip to uncompress the file. 7-Zip can be downloaded from http://www.7-zip.org.

Install the Microsoft Azure CLI

The following steps require the use of the Microsoft Azure CLI. This can be downloaded from https://docs.microsoft.com/en-us/cli/azure/install-azure-cli. For instructions on how to install Microsoft Azure CLI, and documentation of its functionality, refer to https://docs.microsoft.com/en-us/cli/azure/overview.

Login to Azure

To configure your Azure account and upload the VHD, it is necessary to log in to the Azure account using the Azure CLI.

1. At the command line, enter the following command:

```
az login
```

2. This will open a web browser to authenticate your connection. Log in using your Azure credentials.

Create the Azure resource group

An Azure Resource Group is required to associate all of your Azure resources.

Note: If you already have an existing Resource Group that you want to use, you may skip this step.

Enter the following command at the Azure CLI command line:

```
az group create --location <region> --name <group>
```

The following parameters are required:

Table 1: az group create Command Parameters

<region>	The Azure region for the Resource Group.
<group>	The name for the Resource Group.

Example:

```
az group create --location westus --name myresourcegroup
```

Note: For a list of an account's supported regions, use the following command:

```
az account list-locations --output table
```

Create the Azure storage account

An Azure Storage Account is required to store the uploaded AMF Cloud VHD.

Note: If you already have an existing Storage Account that you want to use, you may skip this step.

Enter the following command at the Azure CLI command line:

```
az storage account create --resource-group <group> --name <account> --sku
Standard_LRS
```

The following parameters are required:

Table 2: az storage account create Command Parameters

<group>	The name of the Resource Group where the Storage Account will be created.
<account>	The name for the Storage Account. Must be globally unique across all Azure accounts.
Standard_LRS	An Azure Standard Managed Disk using Locally Redundant Storage.

Example:

```
az storage account create --resource-group myresourcegroup
--name mystorageaccount --sku Standard_LRS
```

Create the Azure storage container

An Azure Storage Container is required as a specific area for your Azure resources. This storage container will hold the uploaded AMF Cloud VHD.

Enter the following command at the Azure CLI command line:

```
az storage container create --account-name <account> --name <container>
```

The following parameters are required:

Table 3: az storage container create Command Parameters

<account>	The name of the Storage Account where the Storage Container will be created.
<container>	The name for the Storage Container.

Example:

```
az storage container create --account-name mystorageaccount
--name mycontainer
```

Upload the VHD to Azure

The AMF Cloud VHD needs to be uploaded to the Storage Container. From there, it will be used to create the AMF Cloud image.

Enter the following command at the Azure CLI command line:

```
az storage blob upload --account-name <account> --container-name
<container> --name <vhd> --type page --file <path>
```

The following parameters are required:

Table 4: az storage blob upload Command Parameters

<account>	The name of the Storage Account.
<container>	The name of the Storage Container.
<vhd>	The destination name of the VHD to create.
page	VHD files must be uploaded as page blobs.
<path>	The path to the VHD file on your local machine.

Example:

```
az storage blob upload --account-name mystorageaccount
--container-name mycontainer --name vaa_azure-5.5.3-1.3.vhd --
type page --file "C:\VHD\vaa_azure-5.5.3-1.3.vhd"
```

Determine the VHD URL

To create the AMF Cloud image, it is necessary to determine the blob URL of the uploaded VHD.

Enter the following command at the Azure CLI command line:

```
az storage blob url --account-name <account> --container-name <container>
--name <vhd>
```

The following parameters are required:

Table 5: az storage blob url Command Parameters

<account>	The name of the Storage Account.
<container>	The name of the Storage Container.
<vhd>	The name of the VHD file.

Example:

```
az storage blob url --account-name mystorageaccount --container-
name mycontainer --name vaa_azure-5.5.3-1.3.vhd
```

Note: Make note of the URL returned by this command, as it will be used in the next part of the process.

Create the Azure image

Now create the Azure AMF Cloud image, using the blob URL of the VHD.

Enter the following command at the Azure CLI command line:

```
az image create --resource-group <group> --name <image> --os-type Linux --
source <url>
```

The following parameters are required:

Table 6: az storage blob url Command Parameters

<group>	The name of the Resource Group.
<image>	The name for the image being created.
Linux	Operating system type. This must be Linux for AMF Cloud.
<url>	The blob URL for the VHD, from the previous step.

Example:

```
az image create --resource-group myresourcegroup --name
vaa_azure-5.5.3-1.3 --os-type Linux --source
"https://mystorageaccount.blob.core.windows.net/vhds/
vaa_azure-5.5.3-1.3.vhd"
```

Create an SSH key pair

Since Azure does not provide console access to instances (virtual machines), configuration and management of this product on Azure must be done via SSH (Secure Shell).

When creating an Azure virtual machine, you can choose between public key authentication and password authentication for the SSH authentication method. For security reasons, we will use public key authentication. If you use public key authentication, you will need to specify the public key for the manager account when creating the virtual machine. Before that, you need to create an SSH key pair (public key pair) by following the steps below before creating the virtual machine.

Note: If you are using an SSH key pair that you have already created, you can go to the next section, “Create an instance”.

SSH key pair

A cryptographic method that uses different keys for data encryption and decryption is called **asymmetric cryptography**, and the two keys used in that method are collectively called a **key pair** or **public key pair**. In asymmetric cryptography, data encrypted with one key of a key pair can only be decrypted with the other key of the pair.

SSH supports **public key authentication** using this property, and the key pair used in this authentication method is called an **SSH key pair**.

An SSH key pair consists of two keys:

- Public Key

A **public key** is a key that does not need to be kept secret. With SSH public key authentication, the user's public key is installed in advance on the access destination host (server, etc.). Public keys can be made public, so it's okay to install the same public key on multiple hosts.

In this product, the public key of the key pair set at the time of instance creation is automatically installed as the public key for the manager user at the time of initial startup. You can log in to this product as a manager user.

- Private Key

A **private key** is a key that is kept securely by its owner and should never be disclosed to anyone else. Since the private key is the only key that can decrypt data encrypted with the public key, the server takes advantage of this property in SSH public key authentication. This allows the server to compare the accessing user’s key with the public key installed on the server, determine whether they possess the correct private key, and grant or deny access based on that result.

To access an instance of this product via SSH, you need to configure your SSH client software to authenticate using the private key that corresponds to the public key you entered when creating the instance.

Creating an SSH key pair with PuTTYgen

The following explains how to create an SSH private key in PuTTY, a typical SSH client for Windows.

For more details, please refer to the user guides for Azure and PuTTY.

Prerequisite

Download and install PuTTY from putty.org. The MSI installer or ZIP archive contain PuTTY and all of its companion utilities. You can also download each program individually. You will need to download at least the following programs:

- putty.exe (used for SSH connection)
- puttygen.exe (used to create a private key file)

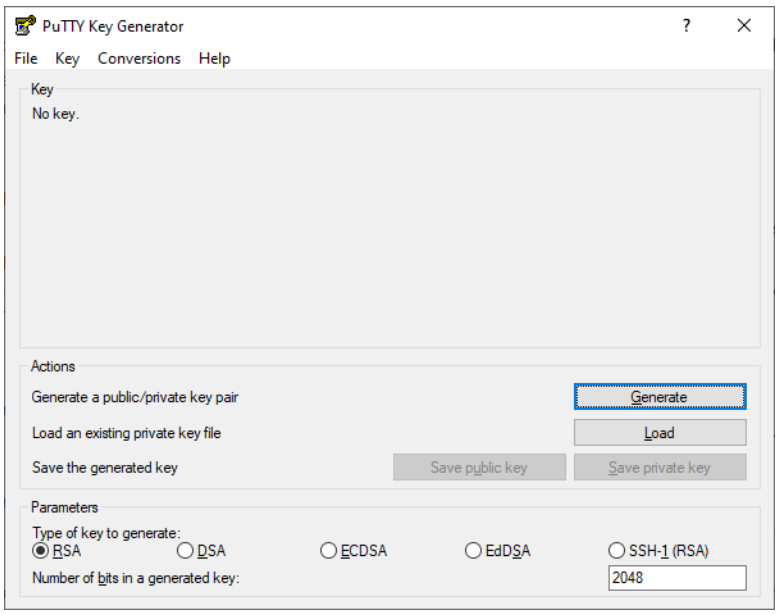
Create an SSH key pair with PuTTYgen

You need a private key pair, created using a utility called PuTTYgen.

1. Start PuTTYgen by one of the following methods:

- In the Start menu, click **All Programs** > **PuTTY** > **PuTTYgen**
- At the Run prompt, enter “c:\Program Files\PuTTY\puttygen.exe”

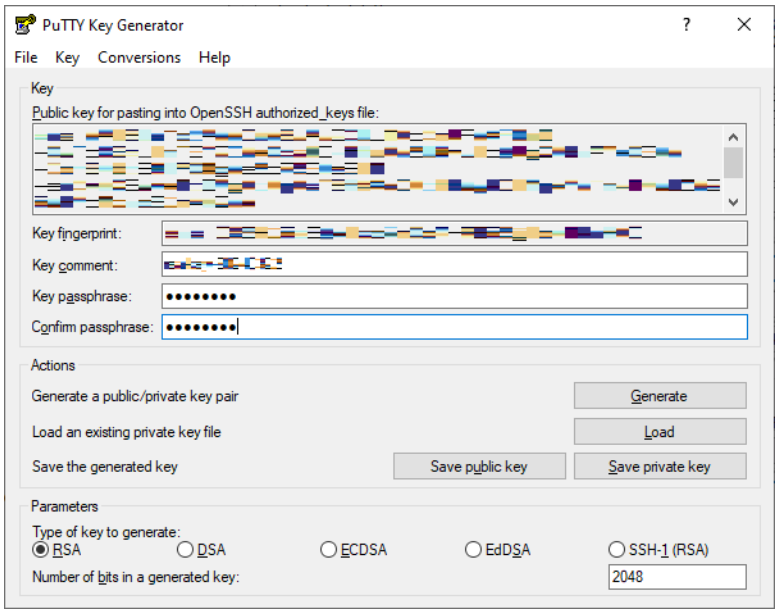
The PuTTY Key Generator window will appear.



2. Make sure that the **RSA** radio button is selected under **Parameters**. Click the **Generate** button.
3. Move your mouse in the blank area below the progress bar until the progress bar is filled. This may take some time.
4. Change the **Key comment** to identify the new key.
5. Set a passphrase.

Enter a passphrase to protect your private key in the **Key passphrase** field.

If you set a passphrase here, even if someone else obtains the private key, they will not be able to use it unless they enter the passphrase.



6. Export public and private key files

Click the **Save public key** button above. A new window will open. Specify the save destination and file name of the public key.

Click the **Save private key** button. Repeat the process, and the save the destination and file name of the private key.

You now have a public and private SSH key pair that can be used with PuTTY.

Creating an SSH key pair with ssh-keygen

The following explains how to create an SSH key pair using the OpenSSH key pair generation tool, the **ssh-keygen** command, which is standard on many UNIX-based operating systems including Linux.

For more details, please refer to the manual page for the **ssh-keygen** command.

1. In the command shell, execute the **ssh-keygen** command as follows:

Example:

```
ubuntu@ubuntu-pc:~/tmp$ ssh-keygen -f id_rsa_vaa
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Enter same passphrase again: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Your identification has been saved in id_rsa_vaa.
Your public key has been saved in id_rsa_vaa.pub.
The key fingerprint is:
SHA256:rV9heYHFxoN2mSj5rZk/LzcAnrjsgI04KnCO7m2uWOM
ubuntu@ubuntu-pc
The key's randomart image is:
+---[RSA 2048]----+
| . =.o |
| or +oO |
|           +.+.. |
|          . ..... |
|        S + *+.  |
|. . . + o +++ |
|.+yes or yes . ... |
|+o+o. .+ . +..|
|==Eo... =o|
+----[SHA256]-----+
```

Note: Enter your passphrase to protect your private key at the “Enter passphrase (empty for no passphrase)” and “Enter same passphrase again” prompts. Your passphrase will not be shown; the Xs here are for illustration only.

2. This will generate a private key “id_rsa_vaa” and a public key “id_rsa_vaa.pub” in the current directory.

Example:

```
ubuntu@ubuntu-pc:~/tmp$  ls -l rsa_id*
-rw-------+ 1 free free 1766 Jul 11 12:55 id_rsa_vaa
-rw-r--r--+ 1 free free 396 Jul 11 12:55 id_rsa_vaa.pub
```

You now have a public and private SSH key pair.

Create an instance

The next step in the process is to create an instance (virtual machine).

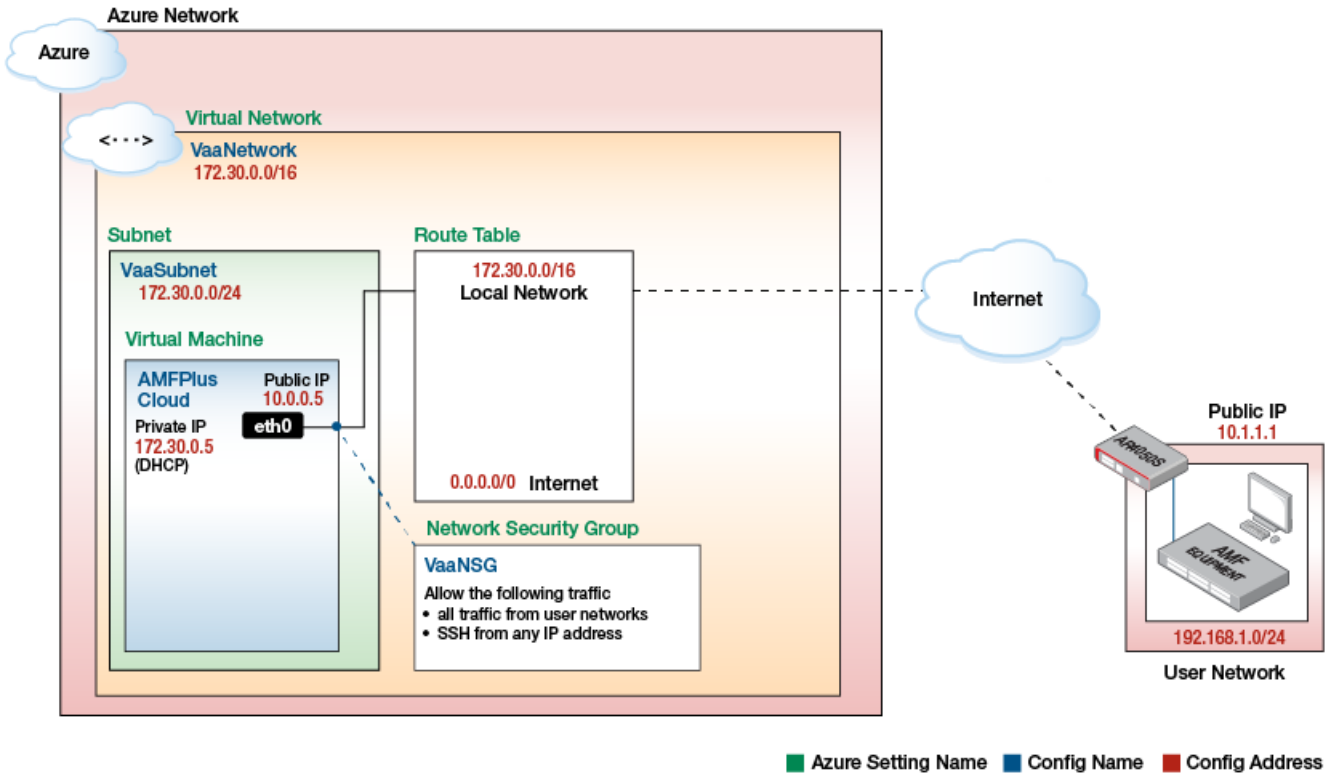
Prerequisites

To create an instance, you need an Azure image as a template. This section assumes that you have already completed the “Create an Azure image” section.

You will also need an SSH key pair. This section assumes that you have already completed the “Create an SSH key pair” section.

Network configuration, access control, and so on also need to be planned in advance. This document assumes these have already been completed.

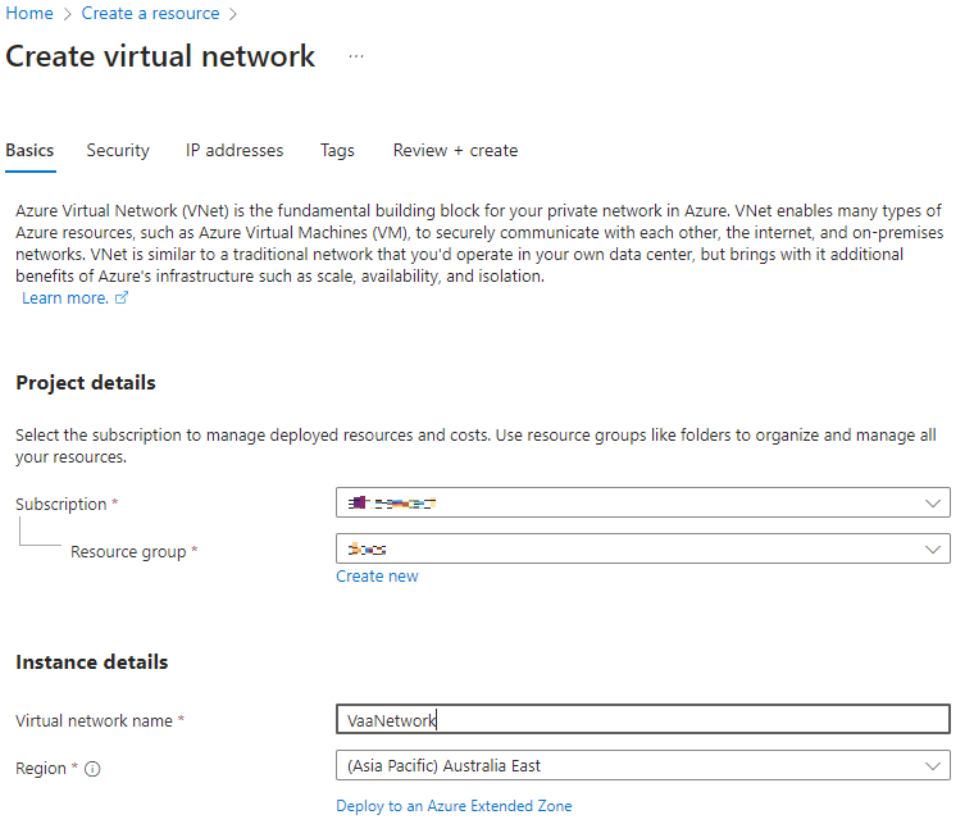
The following diagram summarizes the various settings information handled when creating a virtual machine. In the following explanation, we will use the names and addresses shown in this diagram. When configuring your instance, use the settings from your own environment.



Create the virtual network

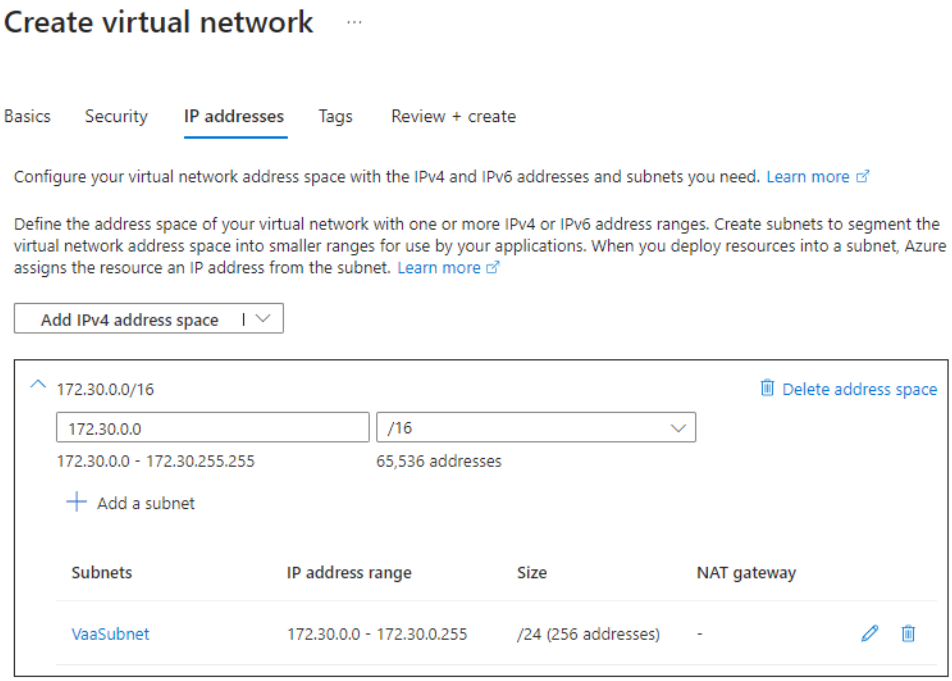
First, you need to create a virtual network and subnet for the virtual machine. To create a virtual network and subnet, follow the steps below.

1. From the Azure portal, select **Create a Resource > Networking > Virtual Network**.
2. On the **Basics** tab in the **Create virtual network** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Virtual network name	VaaNetwork
Region	Choose the appropriate region for your installation

3. Click on the **IP addresses** tab, and enter appropriate values for each item.



Address space	172.30.0.0/16
Subnet name	VaaSubnet
Subnet address range	172.30.0.0/24

4. Click on the **Review + Create** tab, and click on the **Create** button.
5. After a few moments, when the creation is complete, you'll see a “Your deployment is complete” notification.

This completes the creation of the virtual network.

Create a network security group

A network security group is a virtual firewall that applies to virtual machine communications.

By default, a network security group denies all external (inbound) communications and allows all internal (outbound) communications, so settings are required to allow necessary external communications.

Here, we will create a new network security group and add inbound security rules that allow all traffic from the user network and only SSH from any address. Below is an overview of the security rules added in this procedure.

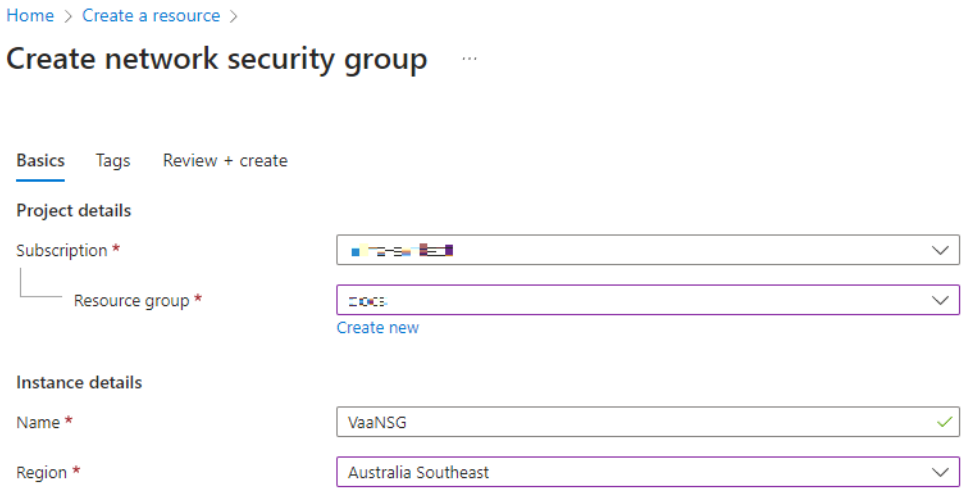
Table 7: Inbound security rules

PRIORITY	NAME	SOURCE	ADDRESS	PROTOCOL	ACTION
100	AllowFromUserNetwork	192.168.1.0/24	all	all	Allow
110	AllowSSH	all	all	SSH (22/TCP)	Allow

Note: By default, the security rules of a network security group have some implicit rules defined at the end, which are set to allow communication within a virtual network (including networks connected via VPN) and deny other communication. Therefore, a rule with a priority of **100** is not actually necessary, but it is explicitly set here for the sake of clarity.

Note: Here, SSH access to this product is open, but in practice we recommend limiting access by specifying the source IP address.

1. From the Azure portal, select **Create a Resource > Networking > Network Security Group**.
2. On the **Basics** tab in the **Create network security group** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Name	VaaNSG
Region	Choose the appropriate region for your installation

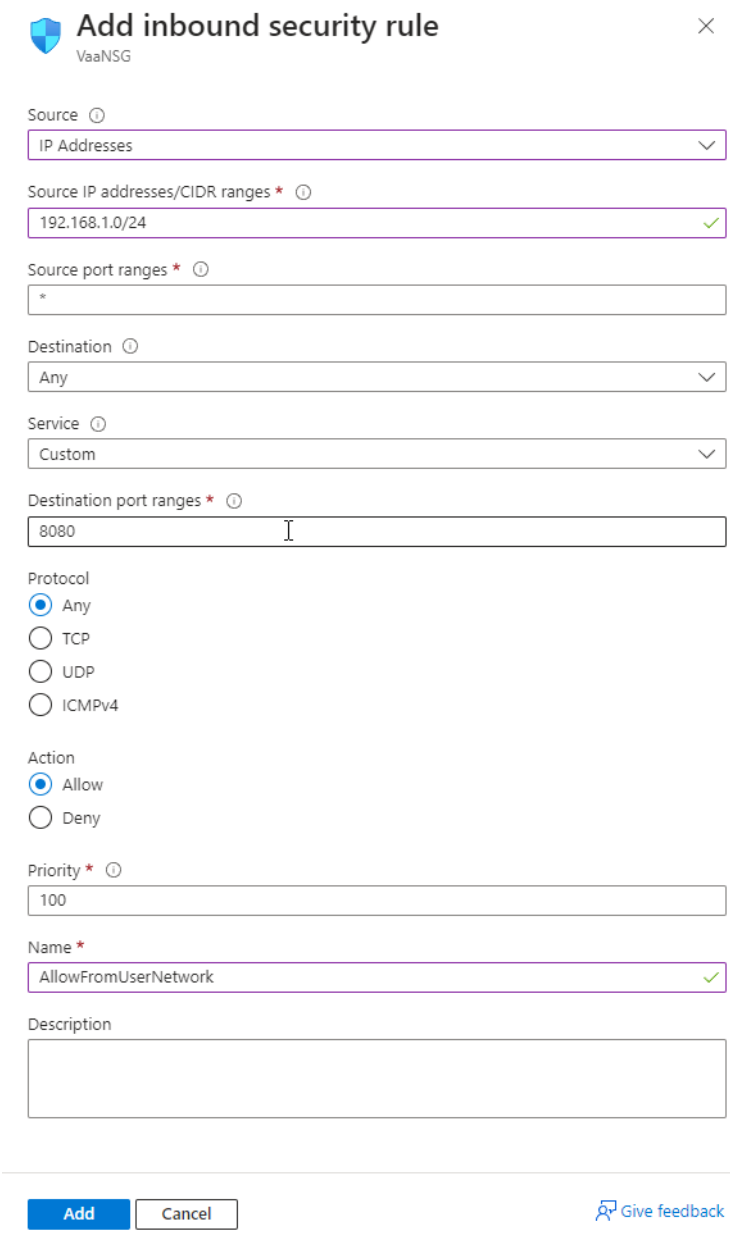
3. Click on the **Review + Create** tab, and click on the **Create** button.
4. After a few moments, when the creation is complete, you'll see a “Your deployment is complete” notification.

5. Next, to allow traffic from the user network, you need to add inbound security rules to the newly created network security group “VaaNSG”.

To find your newly created security group:

- On the Deployment complete screen, click on the **Go to resource** button, or
- From the Azure portal, enter “VaaNSG” in the **Search resources** field, then click on it.

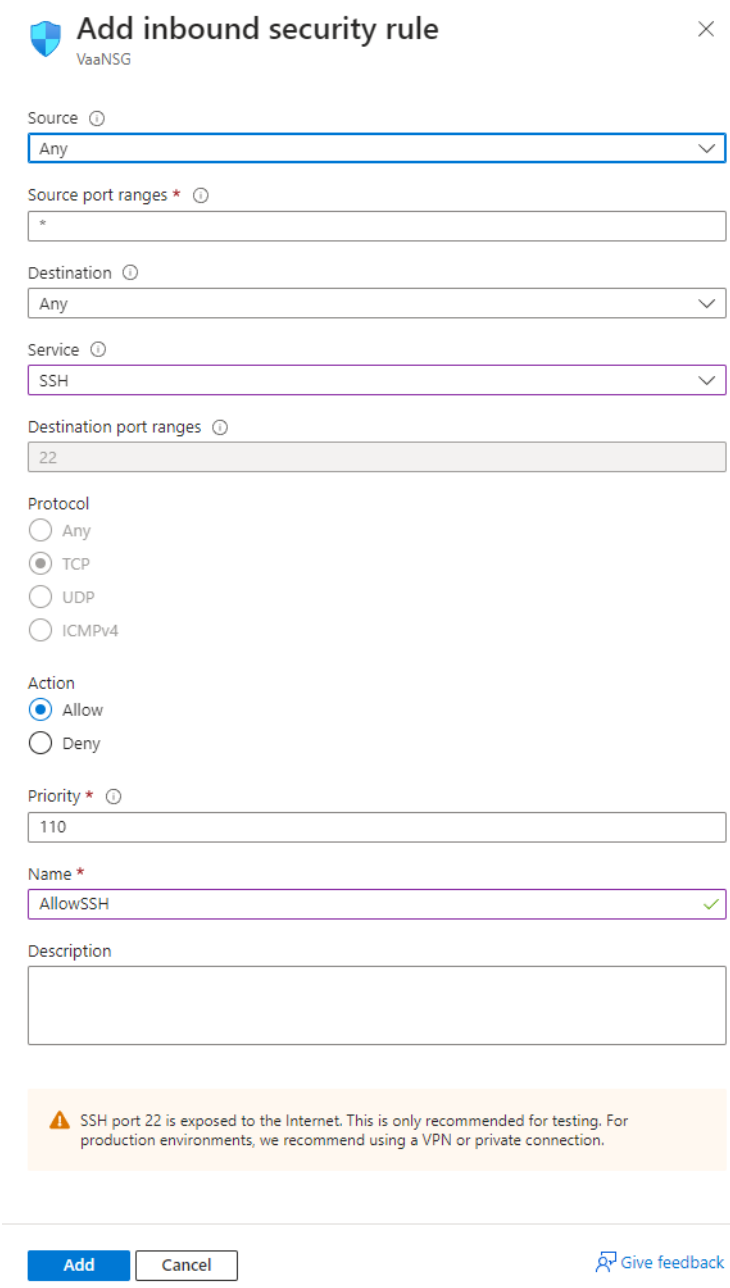
6. From the side menu, select **Settings > Inbound security rules**, and click **Add**.
7. In the **Add inbound security rule** dialog, enter appropriate values for each field and click the **Add** button.



Source	IP addresses
Source IP addresses/CIDR ranges	192.168.1.0/24
Source port ranges	*
Destination	Any
Service	Custom
Destination port ranges	8080
Protocol	Any
Action	Allow
Priority	100
Name	AllowFromUserNetwork

8. After a few moments, when creation is complete, you'll see a notification that says “Created security rule”.
9. Next, add another inbound security rule to allow SSH from any address. From the side menu, select **Settings > Inbound security rules**, and click **Add**.

10. In the **Add inbound security rule** dialog, enter appropriate values for each field and click the **Add** button.



Source	Any
Source port ranges	*
Destination	Any
Service	SSH
Destination port ranges	22
Protocol	TCP
Action	Allow
Priority	110
Name	AllowSSH

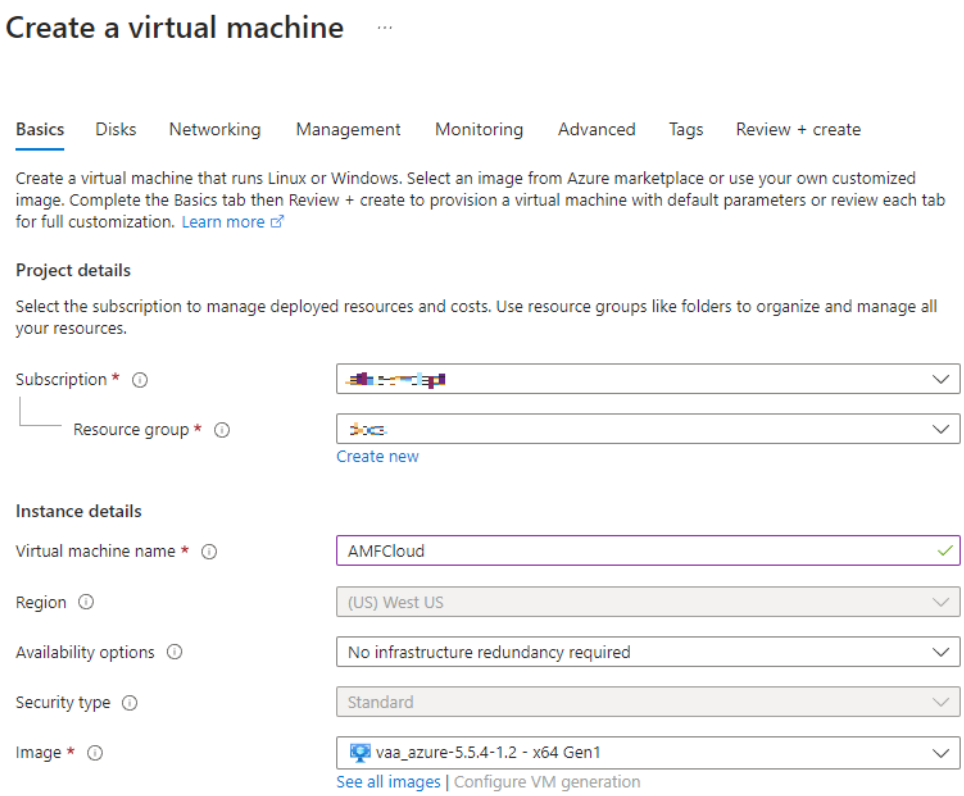
11. Once creation is complete, you will see the notification “Created security rule “again.

This completes the creation of the network security group.

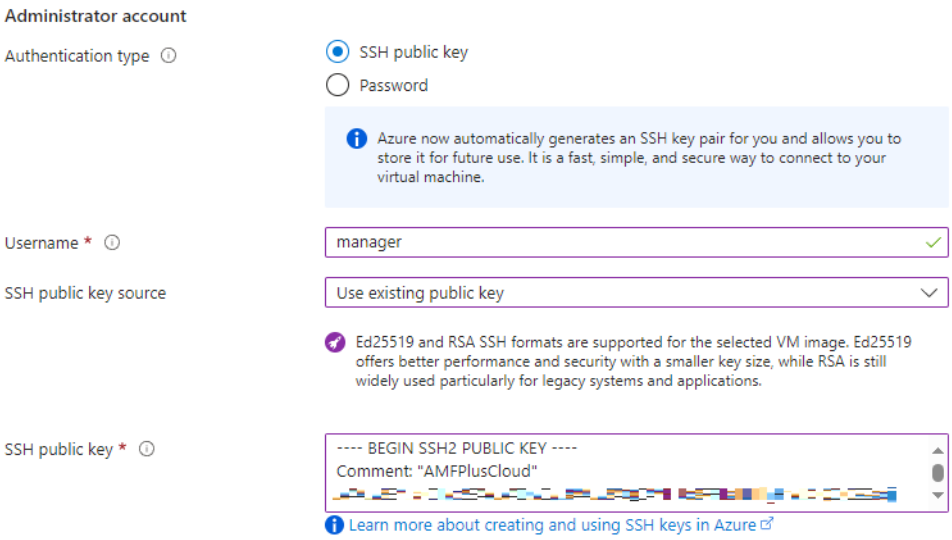
Creating a Virtual Machine

With the previous steps completed, now you can create the virtual machine.

1. From the Azure portal, enter “Vaa” in the **Search resources** field, then select the image you uploaded earlier. Click **+Create VM**.
2. On the **Basics** tab of the **Create a virtual machine** dialog, enter appropriate values for each field.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Virtual machine name	AMFCloud
Region	Defaults to the image location
Image	The name of the image



Authentication type	SSH public key
Username	manager
SSH public key source	Use existing public key
SSH public key	Copy and paste the contents of your public key created in the "Create an SSH key pair" section

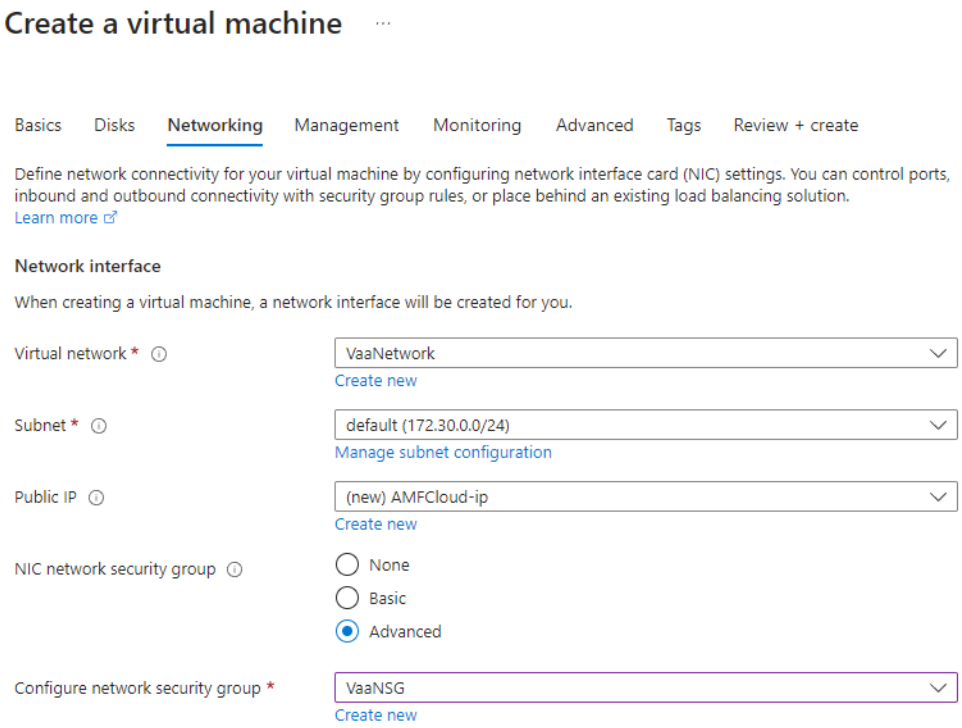
Note: When the virtual machine is started for the first time, the **Virtual machine name** specified here will be automatically set as the hostname.

3. Click on the **Disks** tab, and specify the size of the virtual machine.

Requirements vary depending on your environment. Please refer to the AMF Plus Cloud Datasheet to select the appropriate size.

Note: The initial virtual disk size of the created virtual machine is set to a default size. If you need to increase this after creating your virtual machine, follow the steps in the "Changing the Virtual Disk Size" section.

4. Click on the **Networking** tab and enter appropriate values for each field.



Virtual network	VaaNetwork
Subnet	VaaSubnet (172.30.0.0/24)
Public IP	(new) AMFCloud-ip (this name is generated automatically)
NIC network security group	Advanced
Configure network security group	VaaNSG

5. Click on the **Review + create** tab, and verify your settings are correct. Then click the **Create** button.
6. After a few moments, when the creation is complete, you'll see a “Deployment successful” notification.

This completes the creation of the virtual machine.

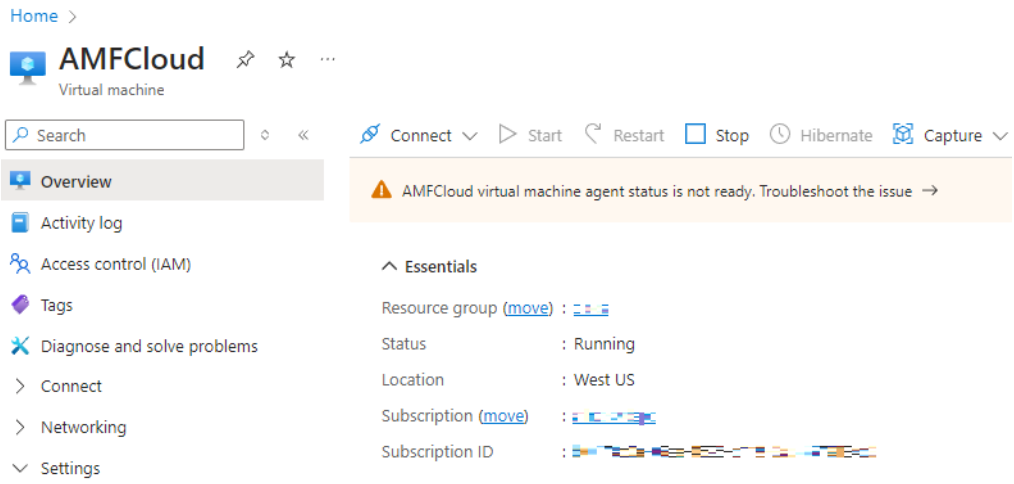
After the details are displayed, you will be able to SSH log in to the displayed public IP address with the public key. The process for testing this is described in the “SSH connection settings” section.

Changing the Virtual Disk Size

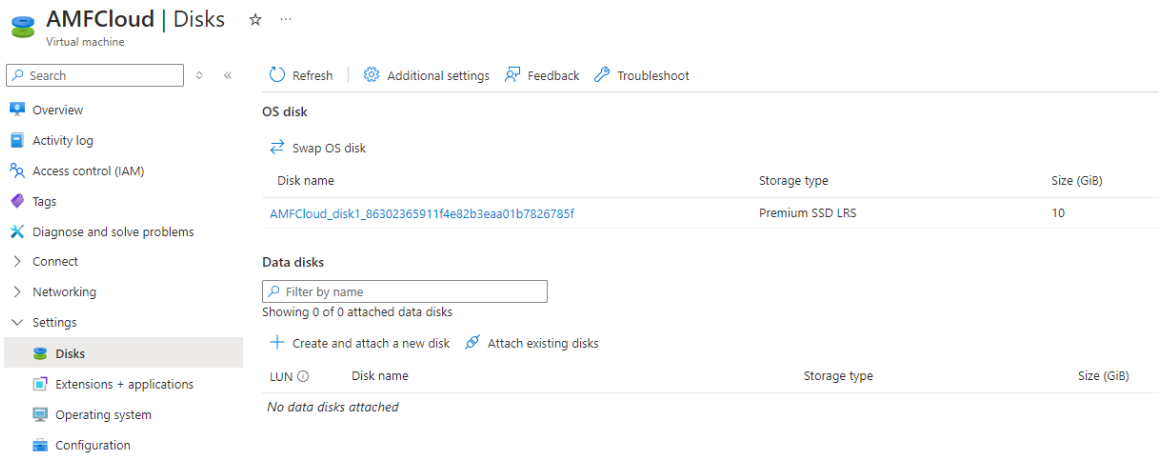
The virtual machine you create will have a default initial virtual disk size. If you need to increase this, you can expand the size of the virtual disk using the following procedure.

1. To change the virtual disk size, stop the virtual machine.

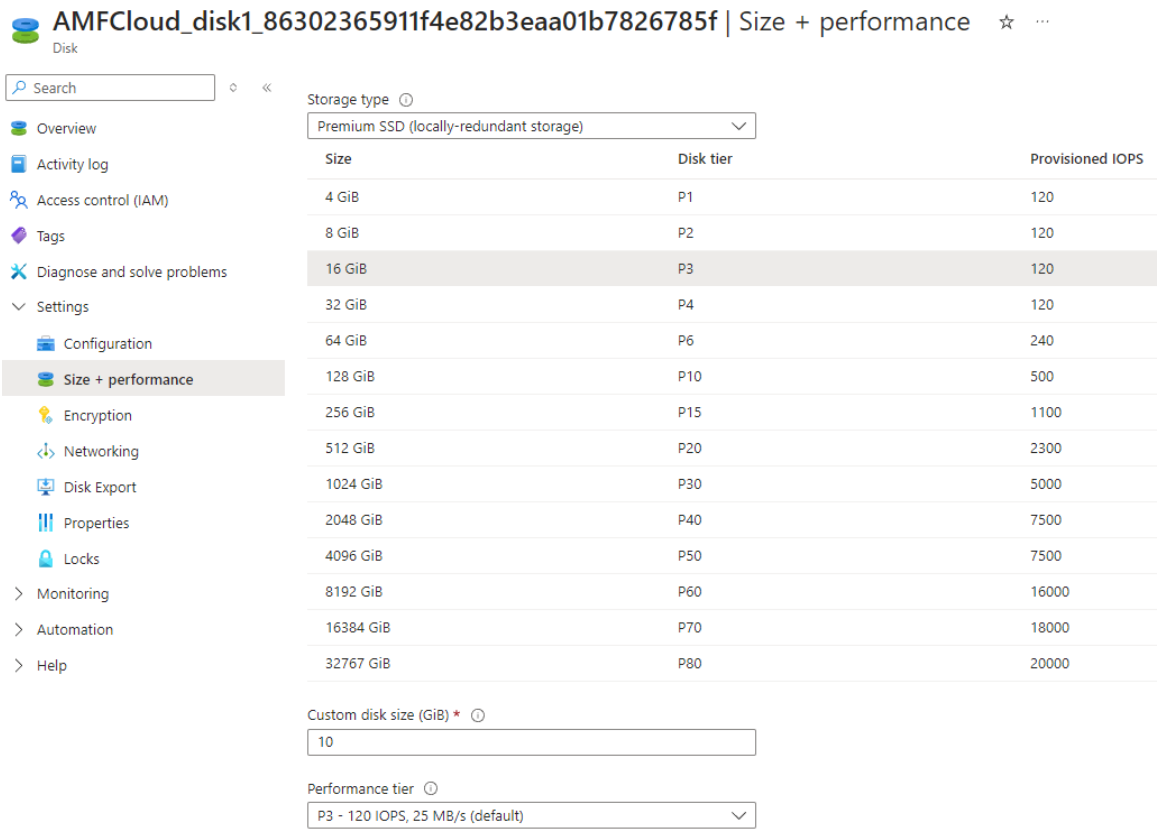
From the Azure portal, enter “AMFCloud” in the **Search resources** field, then select the virtual machine you created earlier. Next, click the **Stop** button on the **Overview** screen. After a while, the virtual machine will stop and a notification will be displayed.



2. From the menu at the left, click on **Settings > Disks**. Click the disk displayed under **OS Disk**. The disk name in this example will be formatted like “AMFCloud_Disk1_xxxxxx”.



3. Enter the required size in the **Custom disk size (GiB)** field and click **Save**.



4. You will see a notification that says “Disk updated successfully”.

5. Return to the **AMFCloud Virtual Machine** screen and click **Start**. The virtual machine will start with the new disk size.

SSH connection settings

Since Azure does not provide console access to instances (virtual machines), configuration and management of this product on Azure must be done via SSH (Secure Shell).

Note: You should already have created your key pair in the “Create an SSH key pair” section.

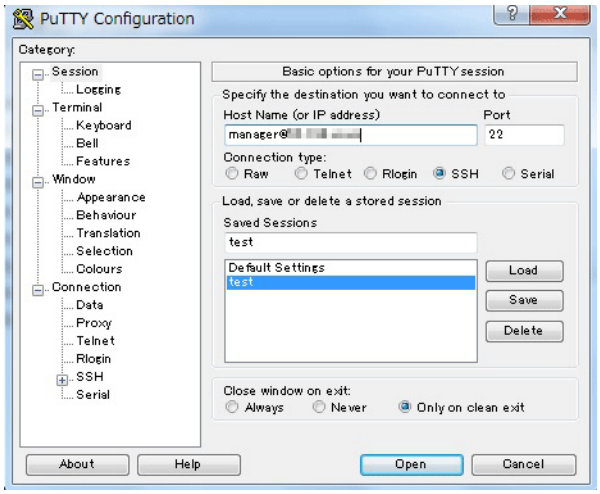
This section describes how to access the CLI of this product with public key authentication using an SSH key pair, using “PuTTY” for Windows and the ssh command for Ubuntu (Linux) as an SSH client.

Make an SSH connection to Vista Manager using PuTTY and private key

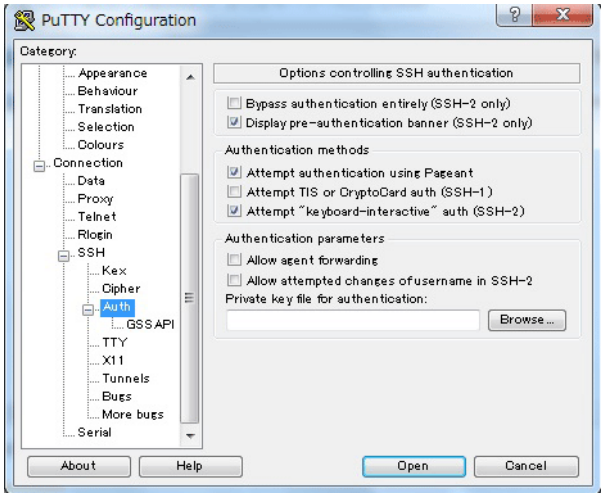
Once you have configured SSH, you can connect to your instance using PuTTY.

1. When PuTTY is opened, a window like the one shown below will be displayed. Enter “manager@ (the public IP address of this instance)” in the **Host Name** field.

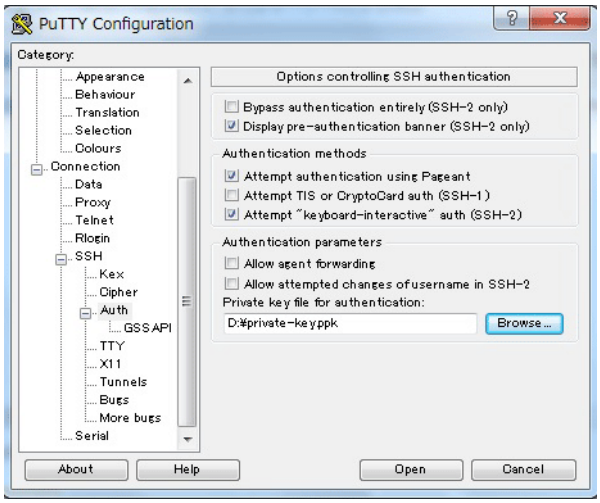
Note: You can check the public IP address from the instance screen of the EC2 dashboard.



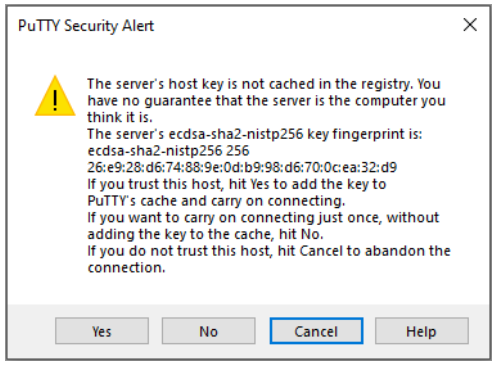
2. Next, click **Connection** > **SSH** > **Auth** in the left panel.



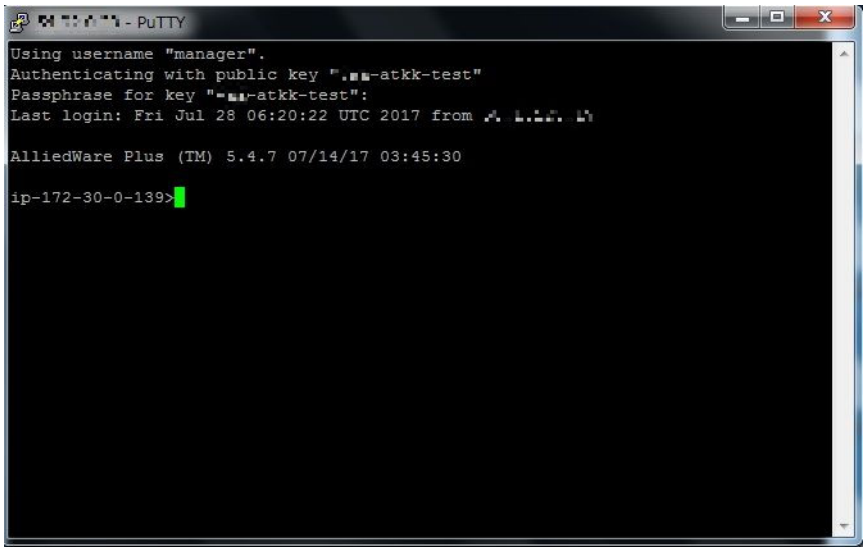
3. Click the **Browse** button. Specify the private key saved earlier. Click **Open** to start an SSH session.



4. If this is your first time connecting to an instance of the product, a security alert dialog box will appear asking if you trust the host you are connecting to. Click **Yes** to save the key to your cache.



5. This completes the SSH connection to this product and displays the AlliedWare Plus CLI screen.



Make an SSH connection to Vista Manager using SSH client of Ubuntu (Linux)

The following describes how to SSH into this product using the standard OpenSSH SSH client in many Linux and UNIX-like environments.

See the man page for the ssh command for more information.

1. In the command shell, move the current directory to the location of the private key file you created earlier.

```
ubuntu@ubuntu-pc:~/tmp$ cd ~/.ssh
```

Note: For security reasons, it is recommended that you set the permissions on the private key file to be read-only for the file owner and inaccessible for everyone else. You can do so with the following commands:

```
ubuntu@ubuntu-pc:~/.ssh$  chmod 400 amf-plus-cloud-atkk-test.pem
ubuntu@ubuntu-pc:~/.ssh$  ls -la amf-plus-cloud-atkk-test.pem
-r-------- 1 vaa vaa 1696 Jul 15 15:06 amf-plus-cloud-atkk-test.pem
```

2. Make an SSH connection to the product with the **ssh** command. Use the **-i** option to specify the PEM file downloaded when creating the key pair on AW. **manager** is the default user name, and **XX.XXX.XX.XXX** is the public IP address of the product instance.

Note: You can check the public IP address of the product instance from the instance screen of the EC2 dashboard.

```
ubuntu@ubuntu-pc:~/.ssh$ ssh -i amf-plus-cloud-atkk-test.pem
manager@XX.XXX.XX.XXX
```

3. When connecting to the server for the first time, you will be asked to confirm the public key of the server. Type “yes” and press the **Enter** key.

```
The authenticity of host 'XX.XXX.XX.XXX (XX.XXX.XX.XXX)' can't be established.
ECDSA key fingerprint is 7f:4e:5c:04:e2:bc:b1:dc:e5:27:b4:86:17:33:9c:0c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'XX.XXX.XX.XXX' (ECDSA) to the list of known hosts.
```

4. This completes the SSH connection to this product and displays the AlliedWare Plus CLI screen.

```
Last login: Mon Jul 31 05:27:39 UTC 2017 from xx.x.xxx.xx

AlliedWare Plus(TM) 5.5.2 XX/XX/XX XX:XX:XX

ip-172-30-0-139>
```

Connection to user network (single mode)

In single mode, to use this product from a user network, you need to connect the Azure virtual network to the user network. There are two ways to do this:

- “How to use AMF Cloud's VPN function”

Build an IPsec tunnel between AMF Cloud itself and the VPN router of the user network.

- “How to use Azure's VPN function”

Build an IPsec tunnel between the Azure virtual network gateway and a VPN router on your network.

We will explain each method using an example where our AT-AR4050S (referred to as the “AR router”) is used as the VPN router on the user network side.

Note: The following are the minimum settings required to connect Azure to your network. During actual operation, please add appropriate access control and security settings using functions such as network security groups according to the requirements of your environment. Also, please design the network configuration appropriately to suit your actual environment.

How to use AMF Cloud's VPN function

The basic configuration for connecting AMF Cloud to a user network using the VPN function of AMF Cloud is described below.

In this configuration, AMF Cloud itself becomes a VPN router and builds an IPsec tunnel between it and the VPN router on the user network side. Therefore, the VPN connection is configured on the AMF Cloud itself. This means there is minimal configuration on the Azure side, except for the network security group, which requires rules to allow VPN communication from the AR router.

Note: The following is a reference example, so please adjust the settings as appropriate in your actual environment.

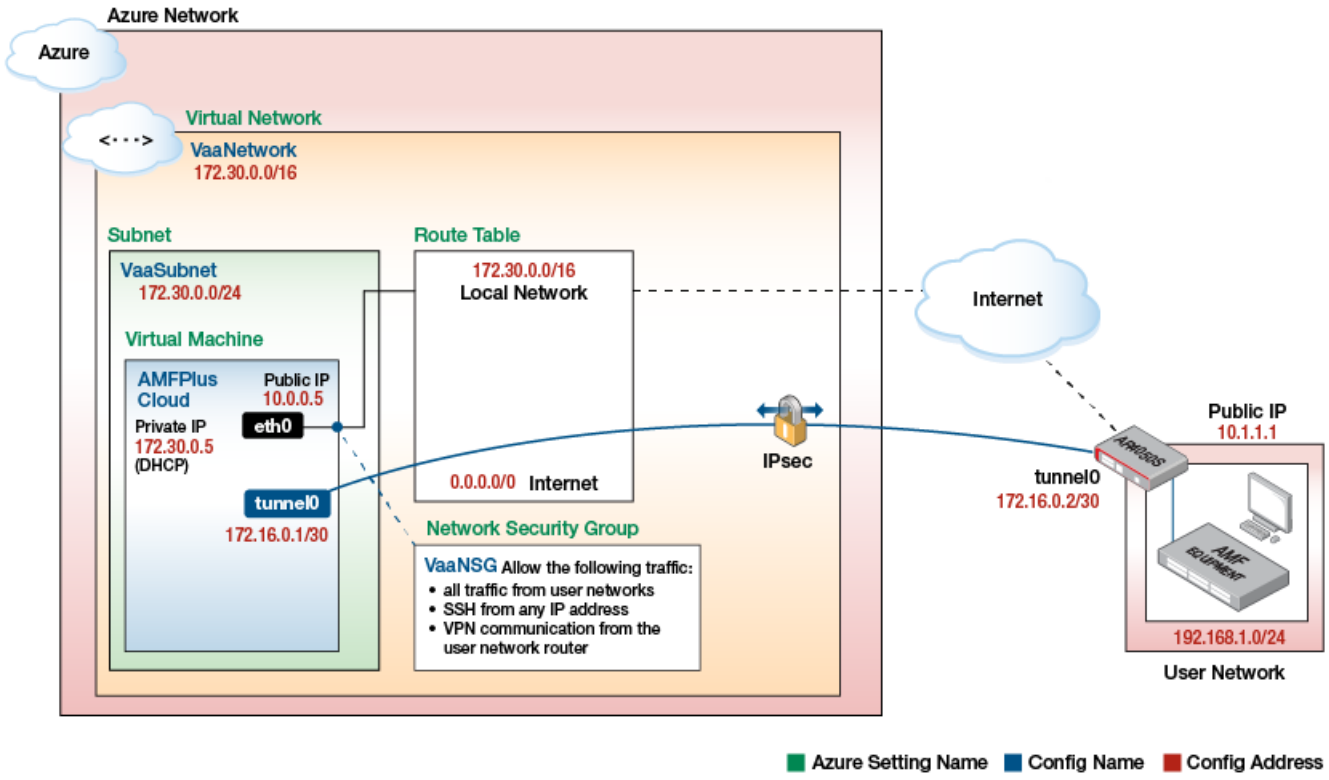


Table 8: User network connection parameters

	AMF CLOUD	AR ROUTER
Tunnel Interface Name	tunnel0	tunnel0
Tunnel Operation Mode	IPsec (IPv4)	IPsec (IPv4)
Tunnel end address (as seen from AMF Cloud)	172.30.0.5 (the private IP of eth0)	10.1.1.1 (public IP)
Tunnel end address (as seen from the AR router)	10.0.0.5 (Virtual Machine Public IP)	10.1.1.1 (public IP)
Address to be set for the tunnel I/F	172.16.0.1/30	172.16.0.2/30
ISAKMP Phase 1 ID	vaa0 (hostname format string)	10.1.1.1 (IP address)
ISAKMP pre-shared key	abcdefghijklmnopqrstuvwxyz1234	

Note: The public IP address of the AMF Cloud virtual machine can be confirmed in Azure, for example from the virtual machine's **Overview**, **Network**, or **Properties** screen.

Azure side settings

Add an inbound security rule to the network security group applied to the AMF Cloud virtual machine to allow VPN communication from the AR router.

Table 9: Inbound security rule parameters

SOURCE	DESTINATION PORT RANGE	PROTOCOL	ACTION	EXPLANATION
10.1.1.1 (the public IP address of the AR router)	500	UDP	license	ISAKMP
10.1.1.1 (the public IP address of the AR router)	4500	UDP	license	NAT-T (UDP-encap ISAKMP/ESP)

AMF Cloud side settings

AMF Cloud has the same VPN function as the AR router, so the settings are similar to those of the AR router described below.

However, since:

- AMF Cloud itself is set to a private IP address (172.30.0.5), and
- AMF Cloud's public IP address (10.0.0.5) is converted by the Azure NAT function,

it is necessary to set the tunnel local name to send the name of the device itself (host name format string) so that the AR router can correctly identify the AMF Cloud during ISAKMP connection.

1. Set the ISAKMP pre-shared key to be used with the AR router (10.1.1.1). To do this, use the **crypto isakmp key** command.

Example:

```
crypto isakmp key abcdefghijklmnopqrstuvwxyz1234 address 10.1.1.1
```

2. Create an IPsec tunnel interface **tunnel0**.

To do this, create a tunnel interface with the interface command and set the following information.

- Local side tunnel end address (**tunnel source**) - Specify the eth0 interface of the AMF Cloud
- Remote side tunnel end address (**tunnel destination**) - Specify the public IP address of the AR router
- ISAKMP local name (**tunnel local name**) - Specify an arbitrary string so that the AR router can identify the AMF Cloud
- Tunnelling method (**tunnel mode ipsec**)
- Application of IPsec protection to the tunnel interface (**tunnel protection ipsec**)
- IP address of the tunnel interface (**ip address**)
- MTU of the tunnel interface (**mtu**)

Example:

```
interface tunnel0
 tunnel source eth0
 tunnel destination 10.1.1.1
 tunnel local name vaa0
 tunnel mode ipsec ipv4
 tunnel protection ipsec
 ip address 172.16.0.1/30
 1300 people
```

3. Set a route to the user network (192.168.1.0/24). To do this, use the **ip route** command. However, set it so that the route cannot be used until the VPN connection is activated.

Example:

```
ip route 192.168.1.0/24 tunnel0
ip route 192.168.1.0/24 null 254
```

AR router settings

Next, we will explain the VPN settings on the AR router, which is the VPN router on the user network side.

Here, we assume that the AR router is connected to the Internet via the ppp0 interface. We also assume that the Internet connection settings and the settings on the AMF Cloud side have been completed. As mentioned above, a private IP address (172.30.0.5) is set for the AMF Cloud itself, and the public IP address (10.0.0.5) of the AMF Cloud is converted by the Azure NAT function, so on the AR router side, you need to specify the same string as that set on the AMF Cloud side in the tunnel remote name so that the AMF Cloud can be correctly identified during the ISAKMP connection.

1. Set the ISAKMP pre-shared key to be used with AMF Cloud. To do this, use the **crypto isakmp key** command. Since the public IP of AMF Cloud is NAT translated, here we identify AMF Cloud by a string ID in the form of a hostname.

Example:

```
crypto isakmp key abcdefghijklmnopqrstuvwxyz1234 hostname vaa0
```

2. Create an IPsec tunnel interface **tunnel0**.

To do this, create a tunnel interface with the interface command and set the following information.

- Local side tunnel end address (**tunnel source**) - Specify the ppp0 interface of the AR router
- Remote side tunnel end address (**tunnel destination**) - Specify the public IP address of the AMF Cloud
- ISAKMP local name (**tunnel local name**) - Specify the same string as set in the AMF Cloud to identify the other party via NAT
- Tunnelling method (**tunnel mode ipsec**)
- Application of IPsec protection to the tunnel interface (**tunnel protection ipsec**)
- IP address of the tunnel interface (**ip address**)
- MSS rewrite setting on the tunnel interface (**ip tcp adjust-mss**)
- MTU of the tunnel interface (**mtu**)

Example:

```
interface tunnel0
 tunnel source ppp0
 tunnel destination 10.0.0.5
 tunnel remote name vaa0
 tunnel mode ipsec ipv4
 tunnel protection ipsec
 ip address 172.16.0.2/30
 ip tcp adjust-mss 1260
 1300 people
```

3. Set up a route to AMF Cloud (172.30.0.5/32) using the **ip route** command, but set it so that the route cannot be used until the VPN connection is activated.

Example:

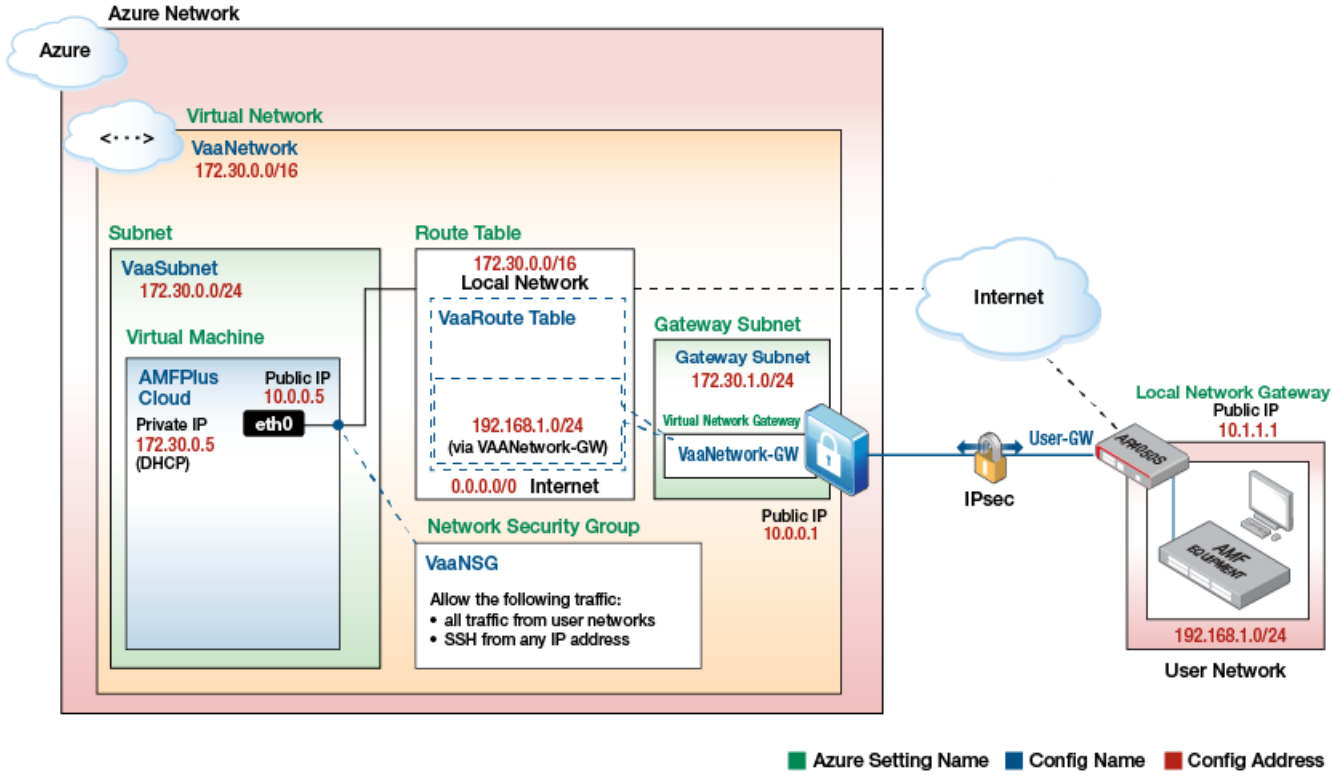
```
ip route 172.30.0.5/32 tunnel0
ip route 172.30.0.5/32 null 254
```

At this point, IP communication between this product on Azure and the user network is possible.

Note: This installation guide does not cover AMF configuration. For information on setting up virtual links between this product and the AMF network, see the AMF Feature Overview and Configuration Guide.

How to use Azure's VPN function

The basic configuration for connecting Azure and a user network using Azure's VPN function is as follows:



In this configuration, the virtual network gateway provided by Azure is used as a VPN router. Therefore, the VPN connection settings are made for Azure. No settings are required on the AMF Cloud side.

Azure side settings

The following Azure components are required to establish a VPN connection between Azure and your network:

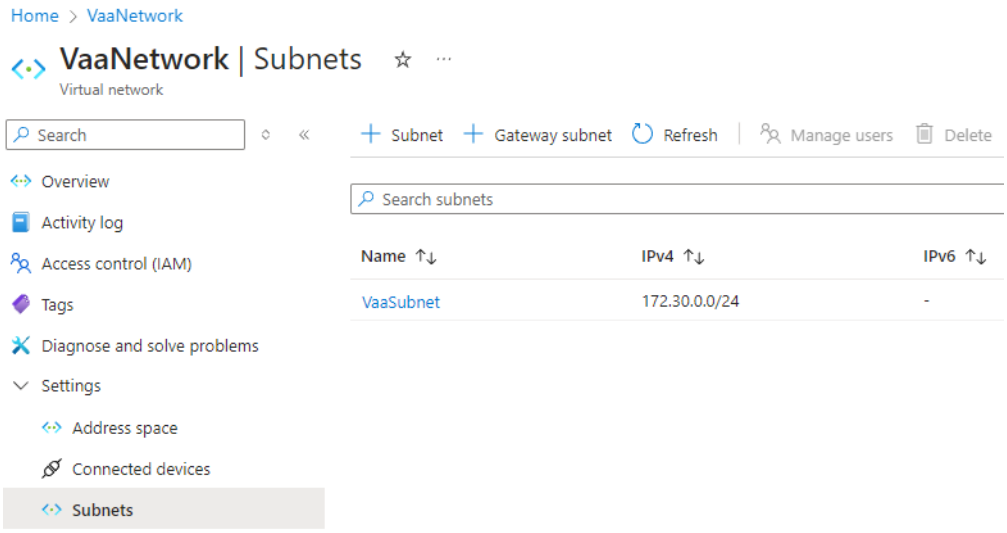
- Gateway subnet - A subnet for placing the Azure side virtual VPN router. For instructions, refer to the "Create a gateway subnet" section.
- Virtual network gateway - A virtual VPN router on the Azure side. For instructions, refer to the "Create a virtual network gateway" section.
- Local network gateway - The VPN router on the user network side as seen from Azure. For instructions, refer to the "Create a local network gateway" section.
- Site-to-site connection - A summary of the information required for VPN connection between Azure and your network. For instructions, refer to the "Create a site-to-site connection" section.
- Route table - A table used to add user-defined routes to an Azure virtual network. For instructions, refer to the "Add a route table and associate it with a subnet" section.

For more information about VPN terminology in Azure, see the Microsoft user guide.

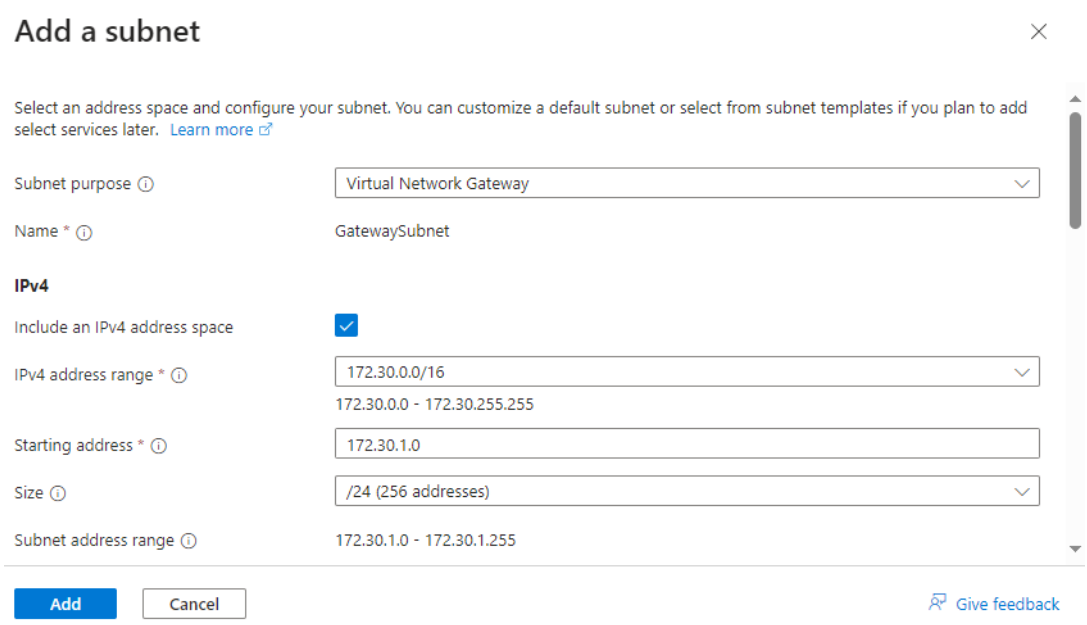
Create a gateway subnet

To set up a VPN router (virtual network gateway) on the Azure side, you must create a gateway subnet in the virtual network. To create a gateway subnet, follow these steps:

1. From the Azure portal, enter “VaaNetwork” in the **Search resources** field, then select the virtual network you created earlier.
2. From the side menu, select **Settings > Subnets**, and click **+Gateway subnet**.



3. On the **Add a subnet** blade, accept the default values and click the **Add** button.



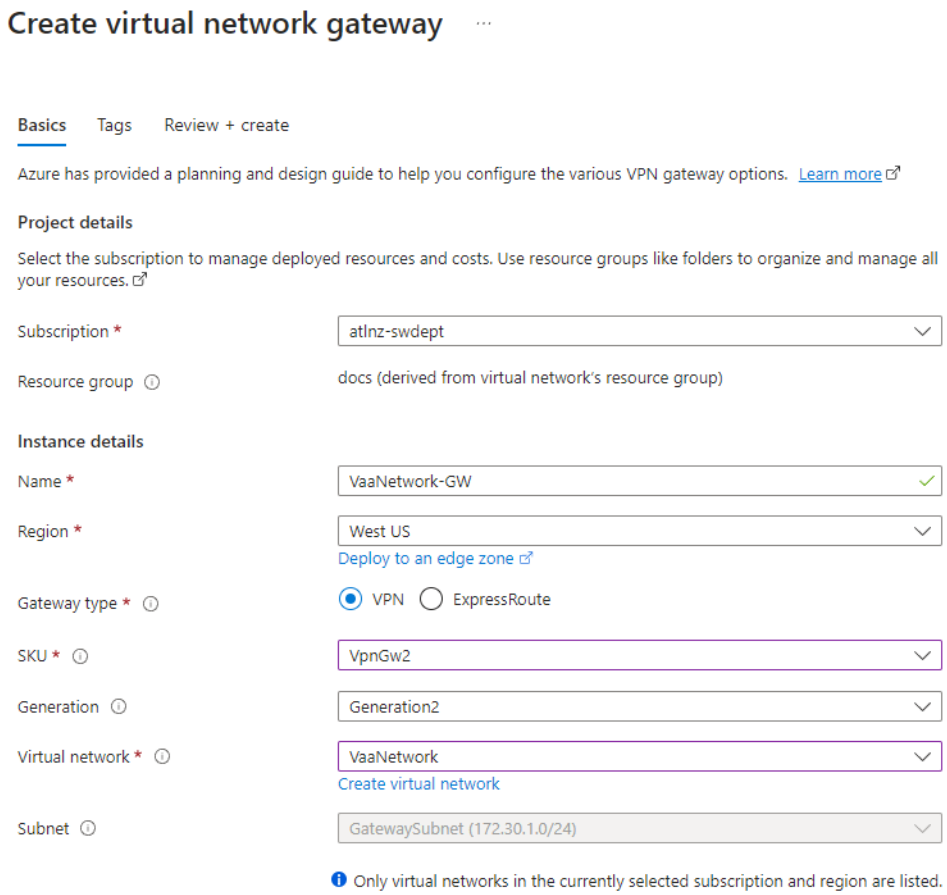
4. After a few moments, you'll see a notification that the creation is complete.

This completes the creation of the gateway subnet.

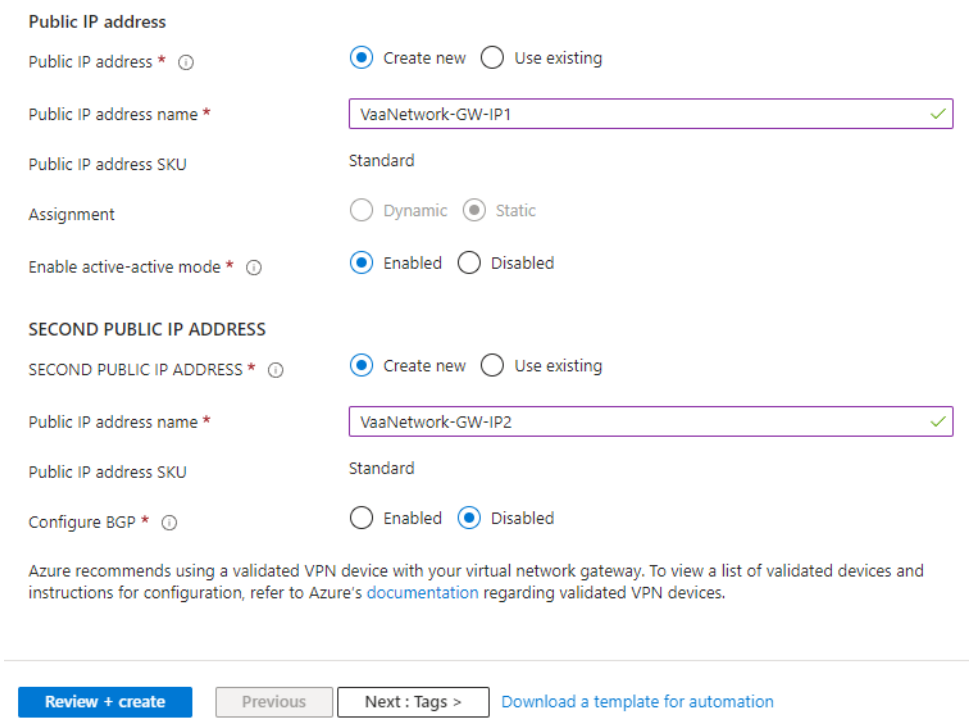
Create a virtual network gateway

After you create the gateway subnet, you next create a virtual network gateway, which is the VPN router on the Azure side.

1. From the Azure portal, select **Create a Resource > Networking > Virtual network gateway**.
2. On the **Basics** tab in the **Create virtual network** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Name	VaaNetwork-GW
Region	Choose the appropriate region for your installation
Gateway Type	VPN
Virtual network	VaaNetwork



Public IP address	Create new
Public IP address name	VaaNetwork-GW-IP1
Second public IP address	Create new
Second public IP address name	VaaNetwork-GW-IP2

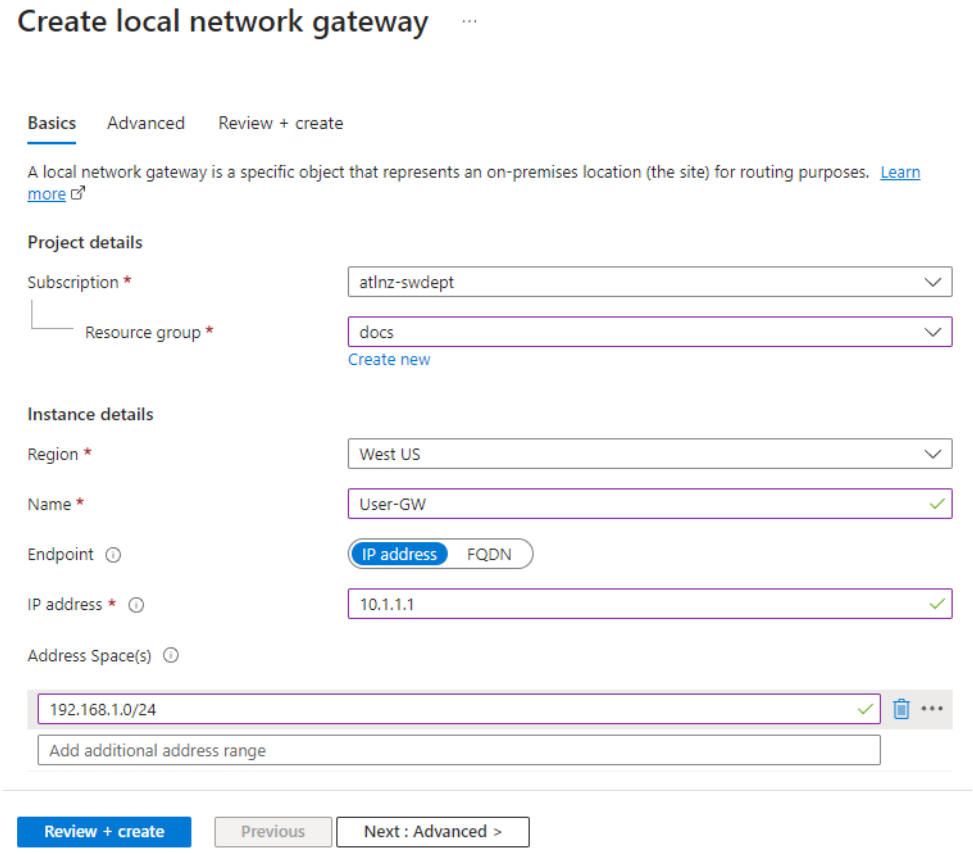
3. Click on **Review + create**, and make sure the settings are correct. Once you have confirmed the settings, click on **Create**.
4. It may take up to 45 minutes for the virtual network gateway to be created, after which you will see a “Deployment succeeded” notification.

This completes the creation of the virtual network gateway.

Create a local network gateway

Next, define the information about the VPN router of the user network, which will be the opposite VPN router of Azure, as the local network gateway. The address range (prefix) on the user network side is also specified here.

1. From the Azure portal, select **Create a Resource > Networking > Local network gateway**.
2. On the **Basics** tab in the **Create local network gateway** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Region	Choose the appropriate region for your installation
Name	User-GW
IP address	10.1.1.1
Address Space	192.168.1.0/24

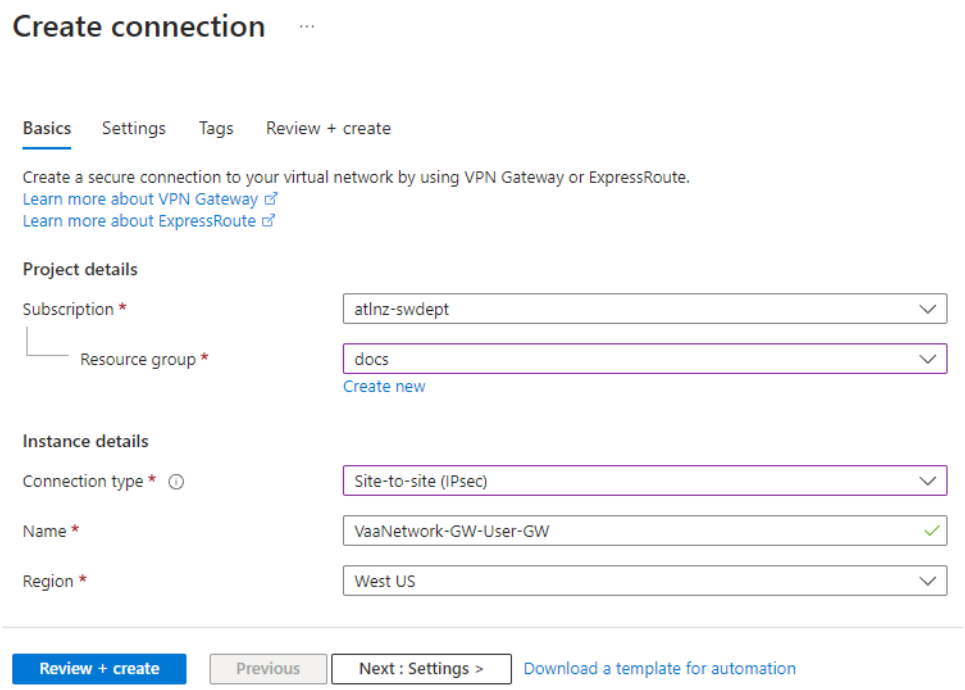
3. Click on **Review + create**, and make sure the settings are correct. Once you have confirmed the settings, click on **Create**.
4. Once the creation is complete, you will see a “Deployment succeeded” notification.

This completes the creation of the local network gateway.

Create a site-to-site connection

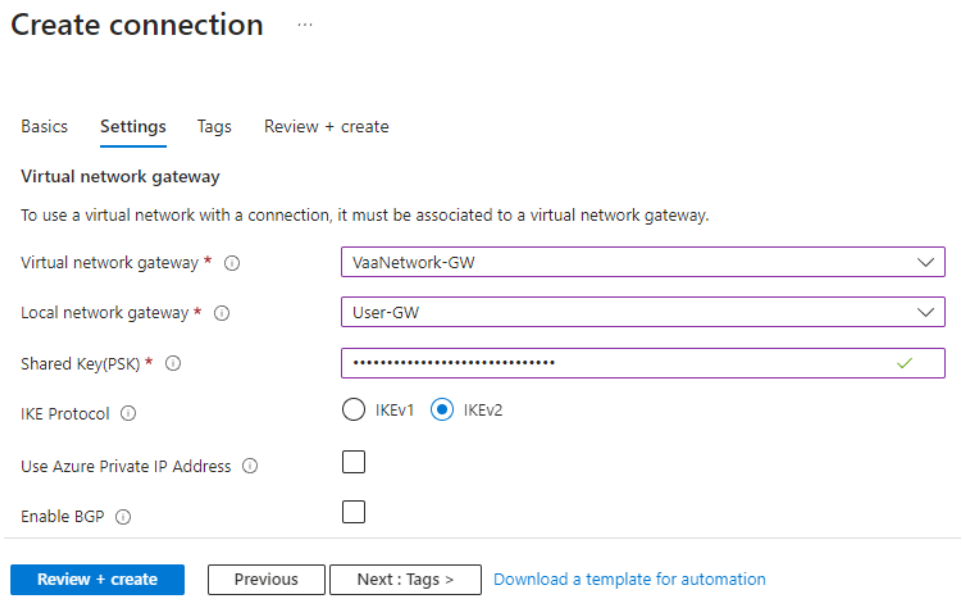
Finally, you create a site-to-site connection to define the information for the VPN connection.

1. From the Azure portal, select **Create a Resource > Networking > Connection**.
2. On the **Basics** tab in the **Create connection** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Connection type	Site-to-site (IPsec)
Name	VaaNetwork-GW-User-GW
Region	Choose the appropriate region for your installation

3. On the **Settings** tab in the **Create connection** dialog, enter appropriate values for each item.



Virtual network gateway	VaaNetwork-GW
Local Network Gateway	User-GW
Shared Key	abcdefghijklmnopqrstuvwxyz1234

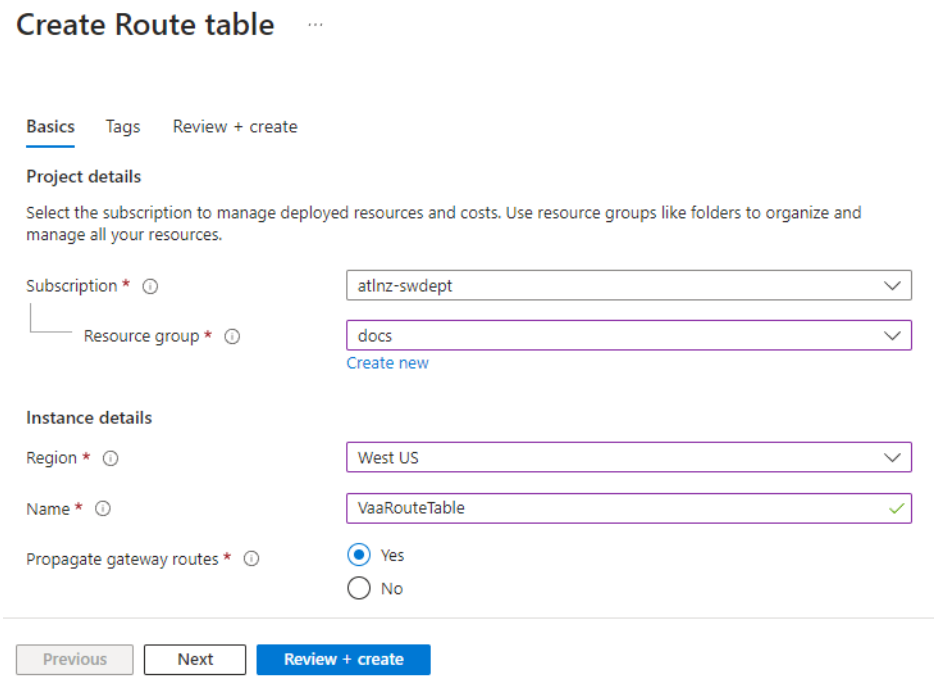
4. Click on **Review + create**, and make sure the settings are correct. Once you have confirmed the settings, click on **Create**.
5. Once the creation is complete, you will see a “Deployment succeeded” notification.

This completes the creation of the site-to-site connection.

Add a route table and associate it with a subnet

Next, register routes to the user network in the route table and associate them with each subnet in the Azure virtual network.

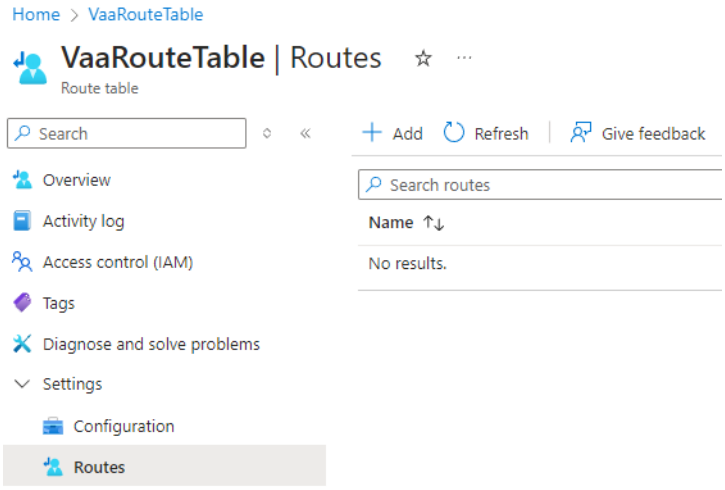
1. From the Azure portal, select **Create a Resource > Networking > Route table**.
2. On the **Basics** tab in the **Create Route table** dialog, enter appropriate values for each item.



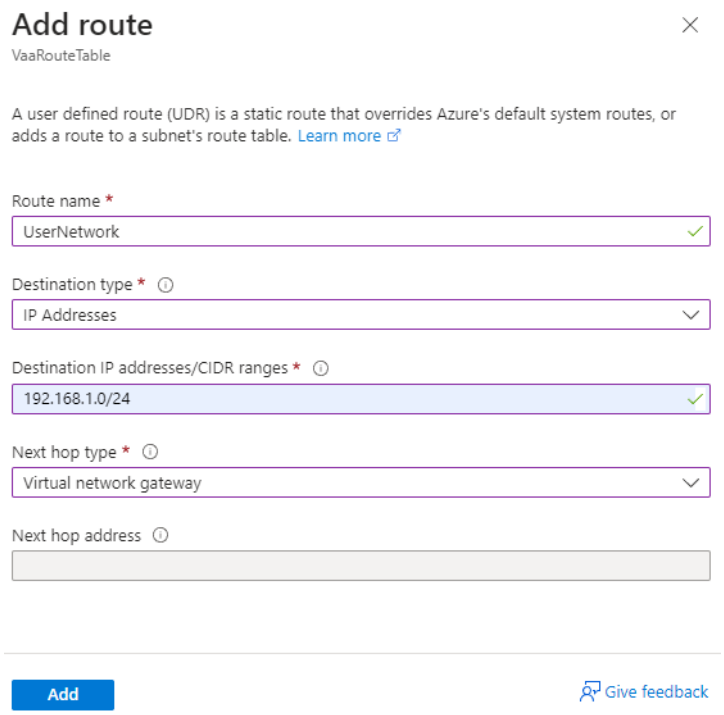
Subscription	Your Azure subscription
Resource group	The resource group you have created
Region	Choose the appropriate region for your installation
Name	VaaRouteTable

3. Click on **Review + create**, and make sure the settings are correct. Once you have confirmed the settings, click on **Create**.
4. Once the creation is complete, you will see a “Deployment succeeded” notification.
5. From the Azure portal, enter “VaaNetwork” in the **Search resources** field, then select the virtual network you created earlier.

6. From the side menu, select **Settings > Routes**, and click **+Add**.



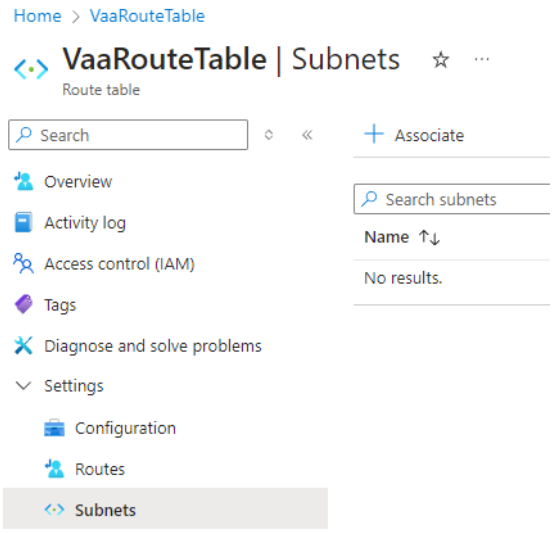
7. On the **Add route** dialog, enter appropriate values for each item and click **Add**.



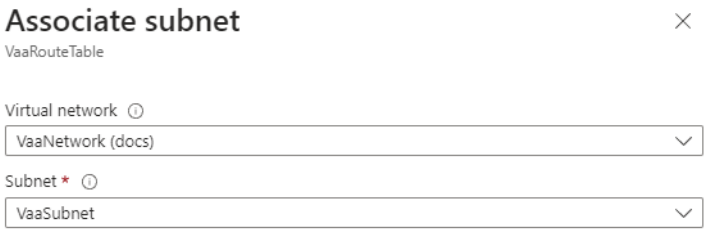
Route name	UserNetwork
Destination type	IP Addresses
Destination IP addresses/CIDR ranges	192.168.1.0/24
Next hop type	Virtual network gateway

8. After a few moments, the addition will be completed and you will see a notification that says “Route added successfully”.

9. Next, associate the route table with the subnets. From the side menu, select **Settings > Subnets**, and click **+Associate**.

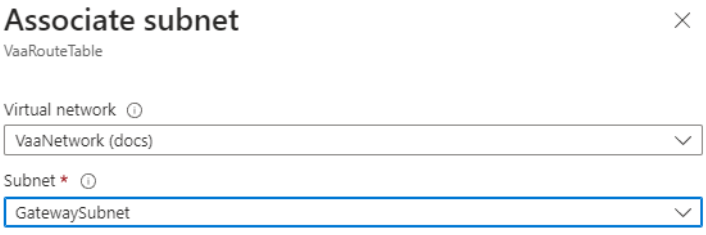


10. Enter appropriate values for each item in the **Associate subnet** dialog, and click the **OK** button.



Virtual network	VaaNetwork
Subnet	VaaSubnet

11. After a few moments, the association is complete and you'll see a notification that says “Subnet route table saved”.
12. Return to the **VaaRouteTable > Subnet** dialog, and click **+Associate**.
13. Enter appropriate values for each item in the **Associate subnet** dialog, and click the **OK** button.



Virtual network	VaaNetwork
Subnet	GatewaySubnet

14. After a few moments, the association is complete and you'll see a notification that says “Subnet route table saved”.

This completes the process of adding a route table and associating it with a subnet.

This completes the basic configuration of a single-mode configuration that does not use the AMF multitenant function.

AR router settings

Next, we will explain the IPsec-related settings of the AR router, which is the VPN router on the user network side. For information on the network configuration, refer to the single mode network configuration. Here, we assume that the AR router is connected to the Internet via the ppp0 interface. We also assume that the settings on the Azure side have been completed.

Note: The following is a reference example, so please adjust the settings as appropriate in your actual environment.

The following parameters are used for the VPN connection with Azure:

Table 10: ISAKMP settings

IKE PHASE 1 (ISAKMP) SETTINGS	
Authentication Method	Pre-shared key
IKE version and exchange mode	IKEv2
Diffie-Hellman Groups	Group2 (1024-bit MODP)
Encryption algorithm	AES256
Authentication Algorithm	SHA-1
SA validity period	28800 seconds (8 hours)

Table 11: IPSEC settings

IKE PHASE 2 (IPSEC) SETTINGS	
SA mode	Tunnel Mode
Security Protocol	ESP (Encryption + Authentication)
Encryption algorithm	AES256
Authentication Algorithm	SHA-1
SA validity period	3600 seconds (1 hour)

Table 12: Other settings

UNIQUE SETTINGS IN THIS EXAMPLE	
Pre-shared key	abcdefghijklmnopqrstuvwxyz1234

ISAKMP Settings

ISAKMP Profile

```
awplus(config)# crypto isakmp profile Azure-Phase-1
awplus(config-isakmp-profile)# version 2
awplus(config-isakmp-profile)# lifetime 28800
awplus(config-isakmp-profile)# transform 1 integrity sha1 encryption aes256 group
2
awplus(config-isakmp-profile)# exit
awplus(config)#
```

Pre-shared key

```
awplus(config)# crypto isakmp key abcdefghijklmnopqrstuvwxyz1234 address 10.0.0.1
```

ISAKMP Peer (Specify the ISAKMP profile to use for connecting to the Azure Virtual Network Gateway)

```
awplus(config)# crypto isakmp peer address 10.0.0.1 profile Azure-Phase-1
```

IPsec settings

IPsec Profile

```
awplus(config)# crypto ipsec profile Azure-Phase-2
awplus(config-ipsec-profile)# lifetime seconds 3600
awplus(config-ipsec-profile)# transform 1 protocol esp integrity sha1 encryption
aes256
awplus(config-ipsec-profile)# exit
```

Tunnel interface settings

Tunnel0 interface

```
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source ppp0
awplus(config-if)# tunnel destination 10.0.0.1
awplus(config-if)# tunnel protection ipsec profile Azure-Phase-2
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# ip address 169.254.0.1/32
awplus(config-if)# ip tcp adjust-mss 1260
awplus(config-if)# exit
```

Routing Settings

Static Routes

```
awplus(config)# ip route 0.0.0.0/0 ppp0
awplus(config)# ip route 172.30.0.0/16 tunnel0
awplus(config)# ip route 172.30.0.0/16 null 254
```

At this point, IP communication between this product on Azure and the user network is possible.

Note: This installation guide does not cover AMF configuration. For information on setting up virtual links between this product and the AMF network, see the AMF Feature Overview and Configuration Guide.

Connection with tenant networks (multi-tenant mode)

Note: The following explanation assumes that the basic settings for single mode in the "Connection to user network (single mode)" section have been completed. If a connection between AMF Cloud and the user network is not required, that part can be omitted.

In multi-tenant mode, to use this product from each tenant network, you need to configure communication between the AMF container for the relevant tenant and the tenant network. There are two ways to do this:

- "How to use AMF Cloud's VPN function"

Build an L2TPv3 tunnel protected by IPsec between AMF Cloud itself and the VPN router of the tenant network, and use AMF Cloud's bridge function to bridge the L2TPv3 tunnel to each container.

- "How to use Azure's VPN function"

Build an IPsec tunnel between the Azure virtual network gateway and a VPN router on the tenant network.

We will explain each method using an example where our AT-AR4050S (referred to as the "AR router") is used as the VPN router on the tenant network side.

Note: The following are the minimum settings required to connect Azure to your network. During actual operation, please add appropriate access control and security settings using functions such as network security groups according to the requirements of your environment. Also, please design the network configuration appropriately to suit your actual environment.

How to use AMF Cloud's VPN function

The basic configuration for connecting AMF Cloud to a tenant network using the VPN function of AMF Cloud is described below.

In this configuration, AMF Cloud itself acts as a VPN router and bridge. You build an L2TPv3 + IPsec tunnel between the tenant network VPN router and bridging the L2TPv3 tunnel to each container using the bridge function of AMF Cloud.

Therefore, the VPN connection is configured for AMF Cloud itself. There is no configuration on the Azure side, such as the virtual network gateway, but for the network security group, you add a rule to allow VPN communication from the AR router.

In addition, in this configuration, the communication paths between each container and the tenant network are completely separated. Each tenant can specify its own IP address (IP addresses can overlap between tenants).

Note: The following is a reference example, so please adjust the settings as appropriate in your actual environment.

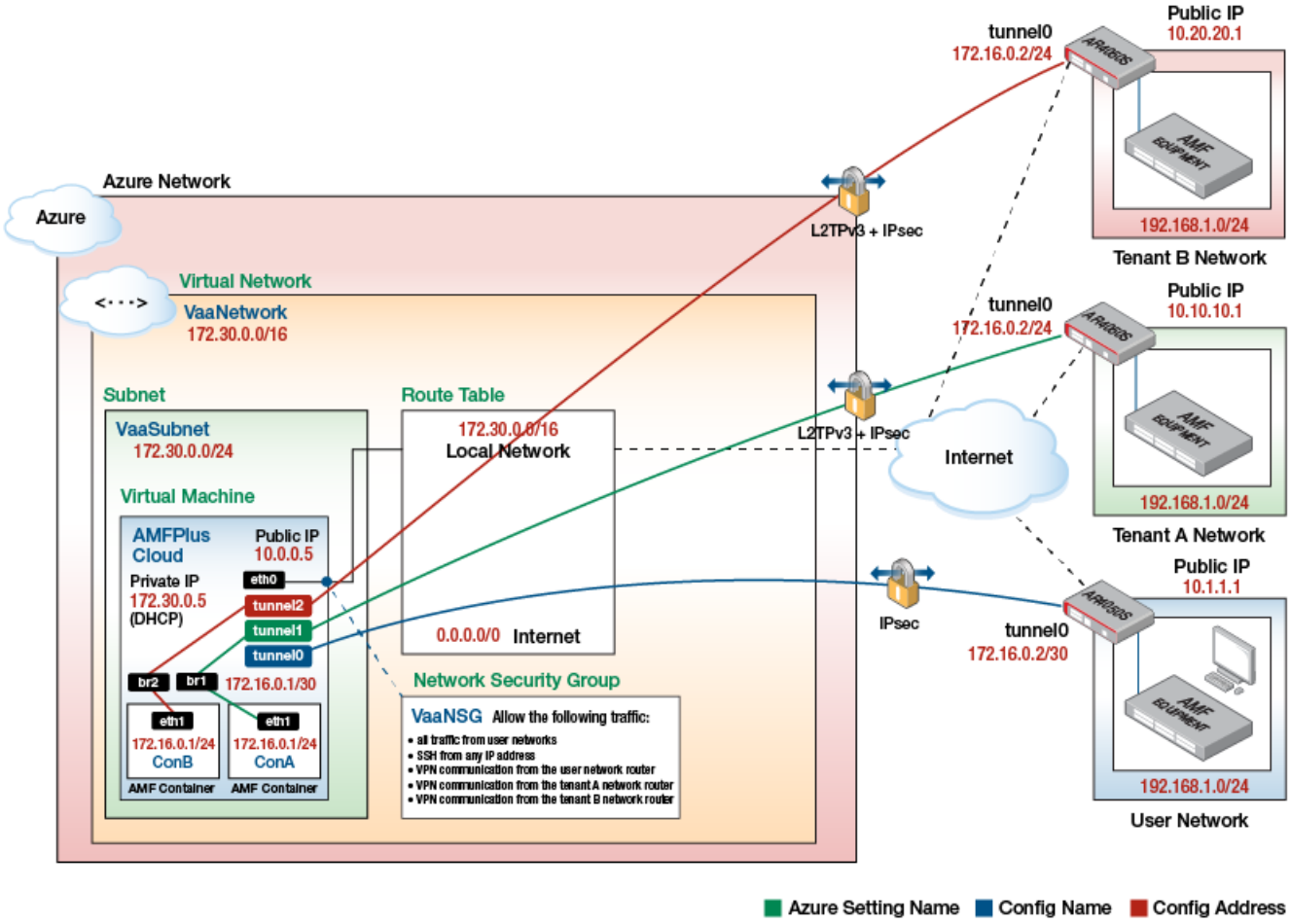


Table 13: Tenant A network connection parameters

	AMF CLOUD	AR ROUTER
Tunnel Interface Name	tunnel1	tunnel0
Tunnel Operation Mode	L2TPv3 + IPsec (IPv4)	L2TPv3 + IPsec (IPv4)
Tunnel end address (as seen from AMF Cloud)	172.30.0.5 (the private IP of eth0)	10.10.10.1 (public IP)
Tunnel end address (as seen from the AR router)	10.0.0.5 (the public IP of the instance)	10.10.10.1 (public IP)
Container Name (Bridge)	ConA (br1)	-
Address to be set for the tunnel I/F	-	172.16.0.2/24
Address to be set on eth1 of the container	172.16.0.1/24	-
ISAKMP Phase 1 ID	vaa1 (hostname format string)	10.10.10.1 (IP address)
ISAKMP pre-shared key	efghijklmnopqrstuvwxyz1234abcd	
L2TPv3 ID	11	12

Table 14: Tenant B network connection parameters

	AMF CLOUD	AR ROUTER
Tunnel Interface Name	tunnel2	tunnel0
Tunnel Operation Mode	L2TPv3 + IPsec (IPv4)	L2TPv3 + IPsec (IPv4)
Tunnel end address (as seen from AMF Cloud)	172.30.0.5 (the private IP of eth0)	10.20.20.1 (public IP)
Tunnel end address (as seen from the AR router)	10.0.0.5 (the public IP of the instance)	10.20.20.1 (public IP)
Container Name (Bridge)	ConB (br2)?	-
Address to be set for the tunnel I/F	-	172.16.0.2/24
Address to be set on eth1 of the container	172.16.0.1/24	-
ISAKMP Phase 1 ID	vaa2 (hostname format string)	10.20.20.1 (IP address)
ISAKMP pre-shared key	ijklmnopqrstuvwxyz1234abcdefgh	
L2TPv3 ID	21	22

Note: The public IP address of the AMF Cloud virtual machine can be confirmed in Azure, for example from the virtual machine's **Overview**, **Network**, or **Properties** screen.

Note: In this configuration, to show that the networks of each AMF container are independent, the same IP addresses are set for the AMF containers **ConA** and **ConB**, and the networks of Tenants A and B. However, this is to show that it is possible to configure overlapping VLANs and IP addresses between AMF containers, and is not a required setting.

Note: The following explanation assumes that the basic settings for single mode in the "Connection to user network (single mode)" section have been completed. If a connection between AMF Cloud and the user network is not required, that part can be omitted.

Azure side settings

You need to add inbound security rules to the network security group applied to the virtual machines in AMF Cloud to allow VPN communication from each tenant's AR router.

Table 15: Inbound security rules

SOURCE	DESTINATION	PROTOCOL	ACTION	EXPLANATION
10.10.10.1 (Tenant A router's public IP address)	500	UDP	license	ISAKMP A
10.20.20.1 (Tenant B router public IP address)	500	UDP	license	ISAKMP B
10.10.10.1 (Tenant A router's public IP address)	4500	UDP	license	NAT-T (UDP-encap ISAKMP/ESP) A
10.20.20.1 (Tenant B router public IP address)	4500	UDP	license	NAT-T (UDP-encap ISAKMP/ESP) B

AMF Cloud side settings

AMF Cloud has the same VPN function as the AR router, so the configuration is similar to that of the AR router, which will be described later.

However, since the AMF Cloud has a private IP address (172.30.0.5), and the AMF Cloud's public IP address (10.0.0.5) is converted by the Azure NAT function, the AR router must be configured to send the name of its own device (hostname format string) in **tunnel local name**. This means it can correctly identify the AMF Cloud during ISAKMP connection. This section shows the configuration for establishing an L2TPv3 + IPsec tunnel between the AMF Cloud and the VPN routers of the Tenant A and B networks.

1. Using the **crypto isakmp key** command, set the ISAKMP pre-shared key to be used between the AR routers (10.10.10.1 and 10.20.20.1) of Tenant A and Tenant B.

Example:

```
crypto isakmp key efghijklmnopqrstuvwxyz1234abcd address 10.10.10.1
crypto isakmp key ijklmnopqrstuvwxyz1234abcdefgh address 10.20.20.1
```

2. Create L2TPv3 tunnel interfaces tunnel1 (for Tenant A) and tunnel2 (for Tenant B).

To do this, create a tunnel interface with the **interface** command and set the following information:

- Local side tunnel end address (**tunnel source**) - Specify the eth0 interface of the AMF Cloud
- Remote side tunnel end address (**tunnel destination**) - Specify the public IP address of the AR router
- ISAKMP local name (**tunnel local name**) - Specify an arbitrary string so that the AR router can identify the AMF Cloud
- L2TPv3 local ID (**tunnel local id**) - Assign an arbitrary number so that it is paired with the opposite side
- Tunnelling method (**tunnel mode ipsec**)
- Application of IPsec protection to the tunnel interface (**tunnel protection ipsec**)

Example:

```
interface tunnel1
 tunnel source eth0
 tunnel destination 10.10.10.1
 tunnel local name vaa1
 tunnel local id 11
 tunnel remote id 12
 tunnel mode l2tp v3
 tunnel protection ipsec

interface tunnel2
 tunnel source eth0
 tunnel destination 10.20.20.1
 tunnel local name vaa2
 tunnel local id 21
 tunnel remote id 22
 tunnel mode l2tp v3
 tunnel protection ipsec
```

AR router settings

Next, we will explain the VPN settings on the AR router, which is the VPN router on the tenant network side. Here, we assume that the AR router is connected to the Internet via the ppp0 interface. We also assume that the Internet connection settings and the settings on the AMF Cloud side have been completed.

As mentioned above, a private IP address (172.30.0.5) is set for the AMF Cloud itself, and the public IP address (10.0.0.5) of the AMF Cloud is converted by the Azure NAT function. On the AR router side, you need to specify the same string as that set on the AMF Cloud side in tunnel remote name so that the AMF Cloud can be correctly identified during ISAKMP connection.

Tenant A side AR router

1. Set the ISAKMP pre-shared key to be used with AMF Cloud. To do this, use the **crypto isakmp key** command. Since the public IP of AMF Cloud is NAT translated, we identify AMF Cloud by a string ID in the form of a hostname.

Example:

```
crypto isakmp key efghijklmnopqrstuvwxyz1234abcd hostname vaa1
```

2. Create an L2TPv3 tunnel interface tunnel0.

To do this, create a tunnel interface with the **interface** command and set the following information:

- Local side tunnel end address (**tunnel source**) - Specify the ppp0 interface of the AR router
- Remote side tunnel end address (**tunnel destination**) - Specify the public IP address of the AMF Cloud
- ISAKMP remote name (**tunnel remote name**) - Specify the same string as set in the AMF Cloud to identify the other party via NAT
- L2TPv3 local ID (**tunnel local id**) - Assign an arbitrary number so that it is paired with the opposite side
- L2TPv3 remote ID (**tunnel remote id**) - Assign an arbitrary number so that it is paired with the opposite side
- Tunnelling method (**tunnel mode ipsec**)
- Application of IPsec protection to the tunnel interface (**tunnel protection ipsec**)
- IP address of the tunnel interface (**ip address**)

Example:

```
interface tunnel0
 tunnel source ppp0
 tunnel destination 10.0.0.5
 tunnel remote name vaa1
 tunnel local id 12
 tunnel remote id 11
 tunnel mode l2tp v3
 tunnel protection ipsec
 ip address 172.16.0.2/24
```

Tenant B side AR router

1. Set the ISAKMP pre-shared key to be used with AMF Cloud. To do this, use the **crypto isakmp key** command. Since the public IP of AMF Cloud is NAT translated, we identify AMF Cloud by ISAKMP remote name.

Example:

```
crypto isakmp key ijklmnopqrstuvwxyz1234abcdefgh hostname vaa2
```

2. Create an L2TPv3 tunnel interface tunnel0.

To do this, create a tunnel interface with the **interface** command and set the following information.

- Local side tunnel end address (**tunnel source**) - Specify the ppp0 interface of the AR router
- Remote side tunnel end address (**tunnel destination**) - Specify the public IP address of the AMF Cloud
- ISAKMP remote name (**tunnel remote name**) - Specify the same string as set in the AMF Cloud to identify the other party via NAT
- L2TPv3 local ID (**tunnel local id**) - Assign an arbitrary number so that it is paired with the opposite side
- L2TPv3 remote ID (**tunnel remote id**) - Assign an arbitrary number so that it is paired with the opposite side
- Tunnelling method (**tunnel mode ipsec**)
- Application of IPsec protection to the tunnel interface (**tunnel protection ipsec**)
- IP address of the tunnel interface (**ip address**)

Example:

```
interface tunnel0
 tunnel source ppp0
 tunnel destination 10.0.0.5
 tunnel remote name vaa2
 tunnel local id 22
 tunnel remote id 21
 tunnel mode l2tp v3
 tunnel protection ipsec
 ip address 172.16.0.2/24
```

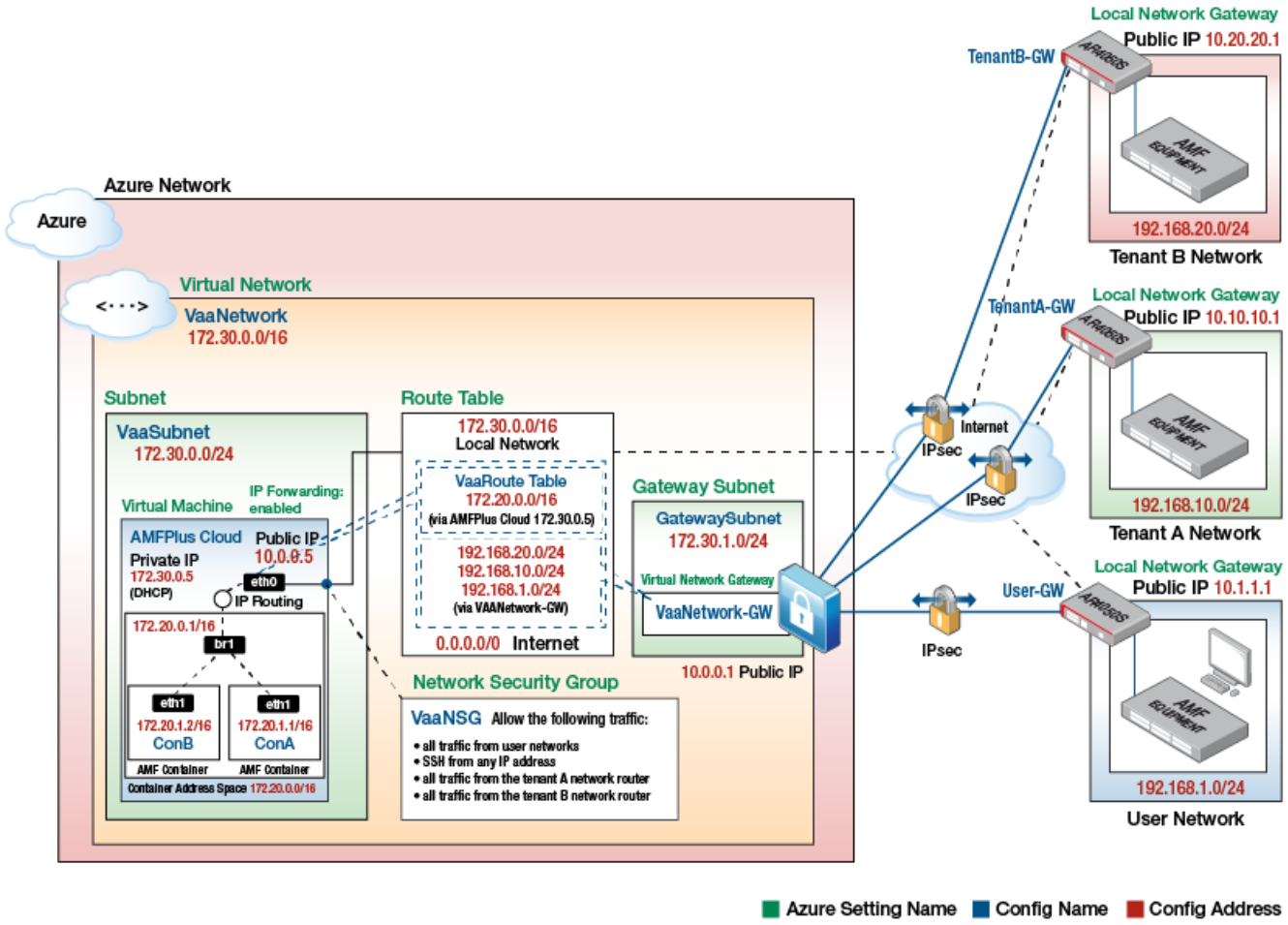
Note: For further settings, see the AMF Feature Overview and Configuration Guide.

How to use Azure's VPN function

The basic configuration for connecting Azure and a tenant network using Azure's VPN function is as follows.

In this configuration, the virtual network gateway provided by Azure is used as a VPN router. Therefore, the VPN connection is configured in Azure. No configuration is required on the AMF Cloud side.

In this configuration, the communication path from the virtual network gateway to the AMF Cloud (multitenant controller) and each container is a shared IP network. This means each tenant cannot specify its own IP address. You need to design the network taking into account everything from the virtual network to the AMF Cloud, AMF container, user network, and tenant network so that IP addresses do not overlap.



Note: The following explanation assumes that the basic settings for single mode in the "Connection to user network (single mode)" section have been completed. If a connection between AMF Cloud and the user network is not required, that part can be omitted.

Azure side settings

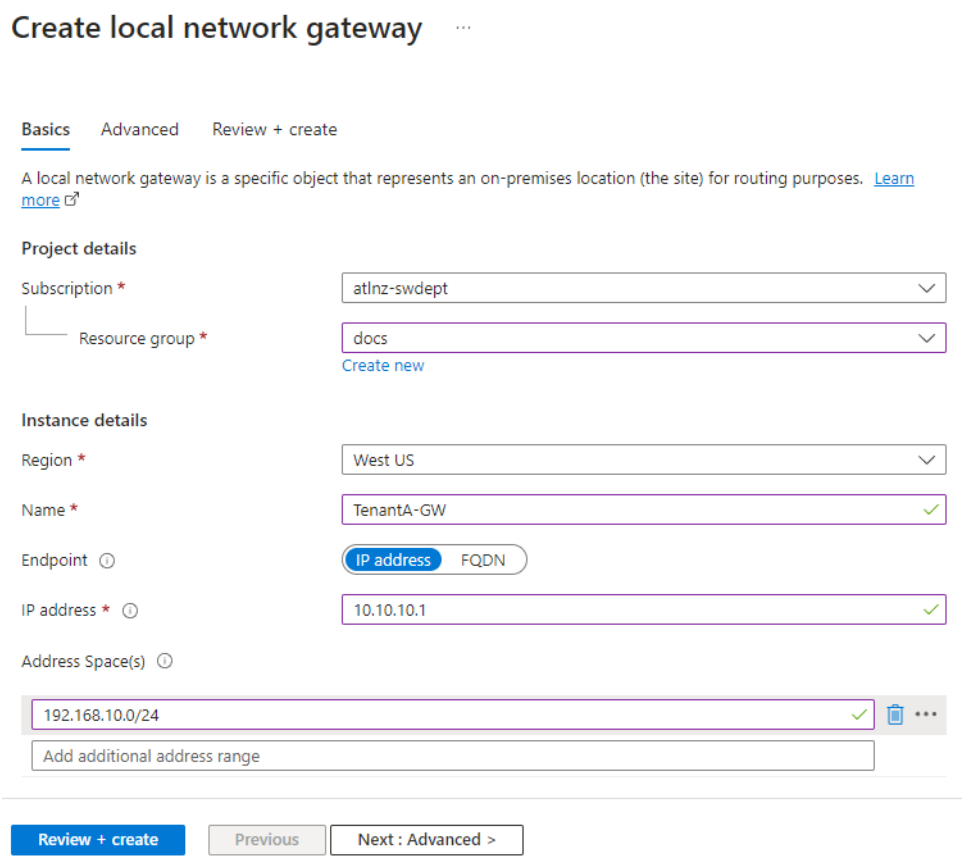
Create local network gateways

If you use the AMF multi-tenant function, you must also connect the Azure virtual network and each tenant network via VPN.

Here, you will add information about the VPN routers for Tenant A and Tenant B as local network gateways. You will also specify the address range (prefix) on the tenant network side here.

1. First, create a local gateway for Tenant A. From the Azure portal, select **Create a Resource > Networking > Local network gateway**.

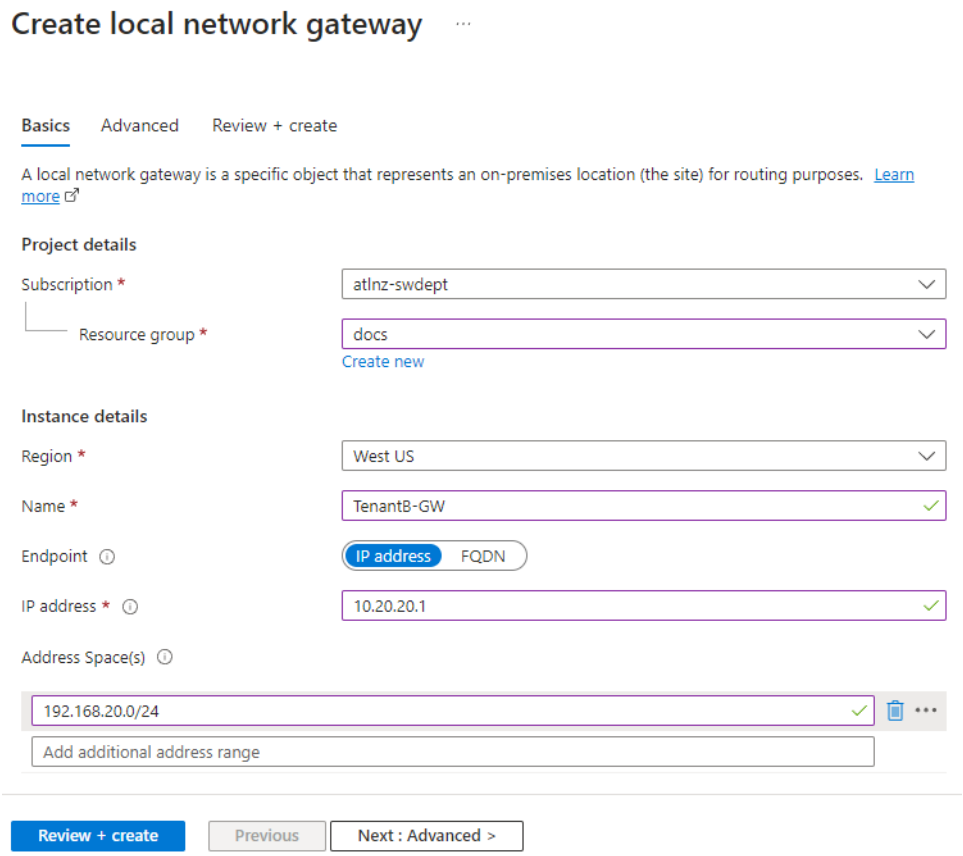
2. On the **Basics** tab in the **Create local network gateway** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Region	Choose the appropriate region for your installation
Name	TenantA-GW
IP address	10.10.10.1
Address Space	192.168.10.0/24

3. Click on **Review + create**, and make sure the settings are correct. Once you have confirmed the settings, click on **Create**.
4. Once the creation is complete, you will see a “Deployment succeeded” notification.
5. Next, create a local gateway for Tenant B. Return to the Azure portal, and select **Create a Resource > Networking > Local network gateway**.

6. On the **Basics** tab in the **Create local network gateway** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Region	Choose the appropriate region for your installation
Name	TenantB-GW
IP address	10.20.20.1
Address Space	192.168.20.0/24

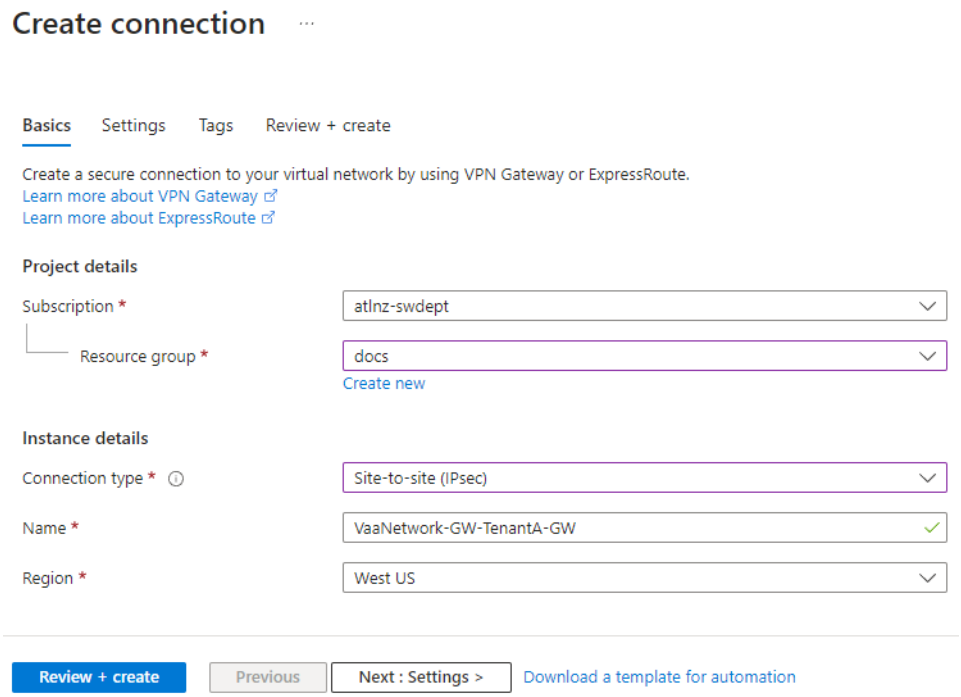
7. Click on **Review + create**, and make sure the settings are correct. Once you have confirmed the settings, click on **Create**.
8. Once the creation is complete, you will see a “Deployment succeeded” notification.

This completes the creation of the local network gateways.

Create site-to-site connections

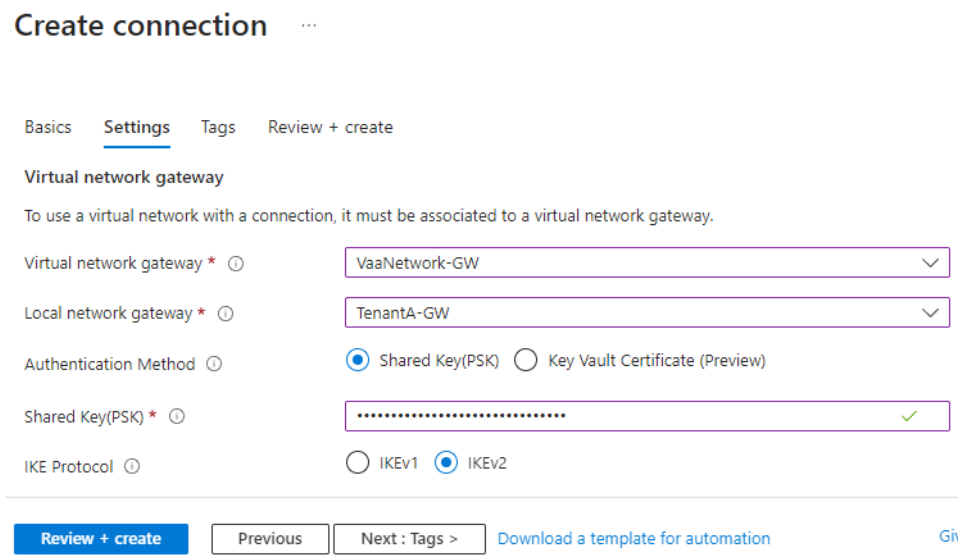
Next, add site-to-site connections between Azure and Tenant A and between Azure and Tenant B using the local network gateway definitions created in the previous section.

1. First, create a connection for Tenant A. From the Azure portal, select **Create a Resource > Networking > Connection**.
2. On the **Basics** tab in the **Create connection** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Connection type	Site-to-site (IPsec)
Name	VaaNetwork-GW-TenantA-GW
Region	Choose the appropriate region for your installation

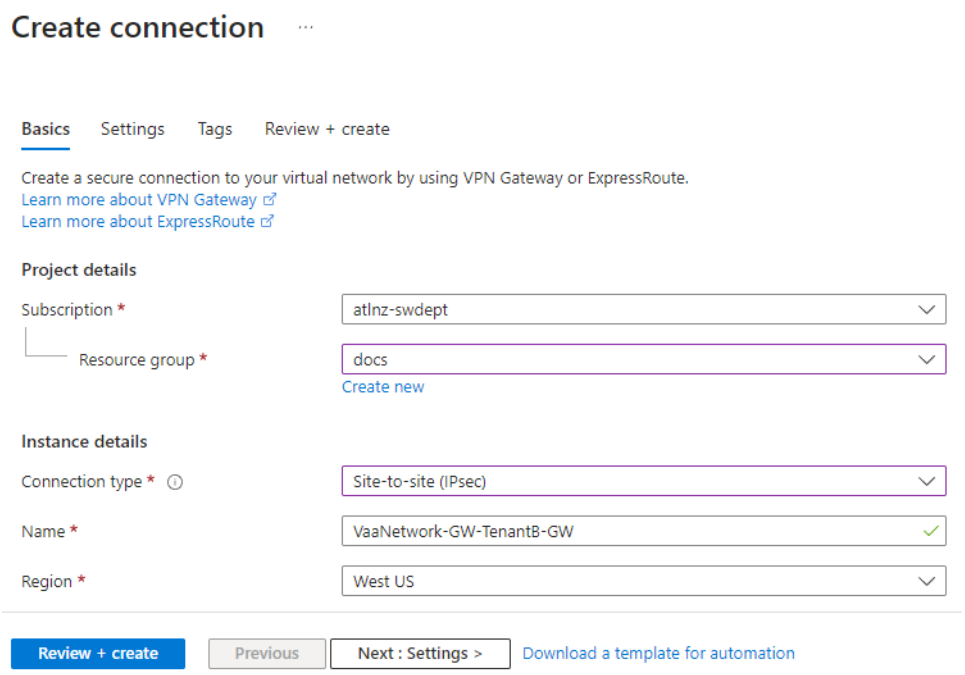
3. On the **Settings** tab in the **Create connection** dialog, enter appropriate values for each item.



Virtual network gateway	VaaNetwork-GW
Local Network Gateway	TenantA-GW
Shared Key	abcdefghijklmnopqrstuvwxyz1234

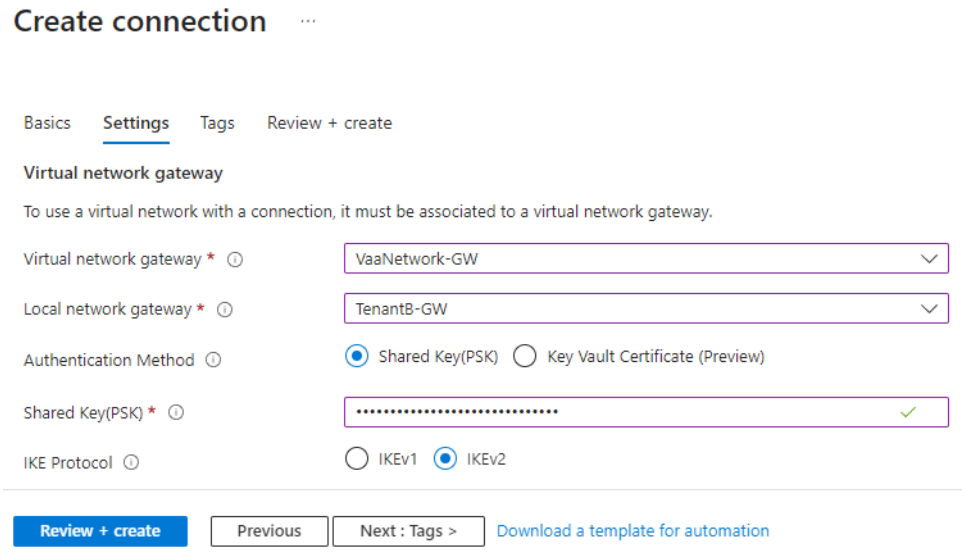
4. Click on **Review + create**, and make sure the settings are correct. Once you have confirmed the settings, click on **Create**.
5. Once the creation is complete, you will see a “Deployment succeeded” notification.
6. Next, create a connection for Tenant B. From the Azure portal, select **Create a Resource > Networking > Connection**.

7. On the **Basics** tab in the **Create connection** dialog, enter appropriate values for each item.



Subscription	Your Azure subscription
Resource group	The resource group you have created
Connection type	Site-to-site (IPsec)
Name	VaaNetwork-GW-TenantB-GW
Region	Choose the appropriate region for your installation

8. On the **Settings** tab in the **Create connection** dialog, enter appropriate values for each item.



Virtual network gateway	VaaNetwork-GW
Local Network Gateway	TenantB-GW
Shared Key	abcdefghijklmnopqrstuvwxyz1234

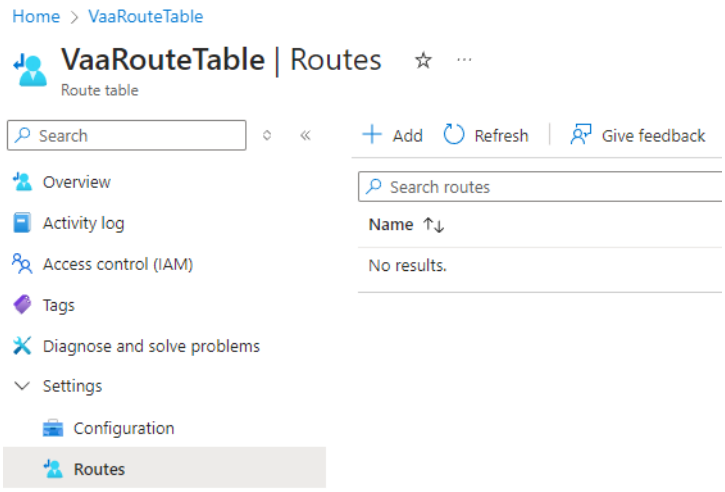
9. Click on **Review + create**, and make sure the settings are correct. Once you have confirmed the settings, click on **Create**.
10. Once the creation is complete, you will see a “Deployment succeeded” notification.

This completes the creation of the site-to-site connection.

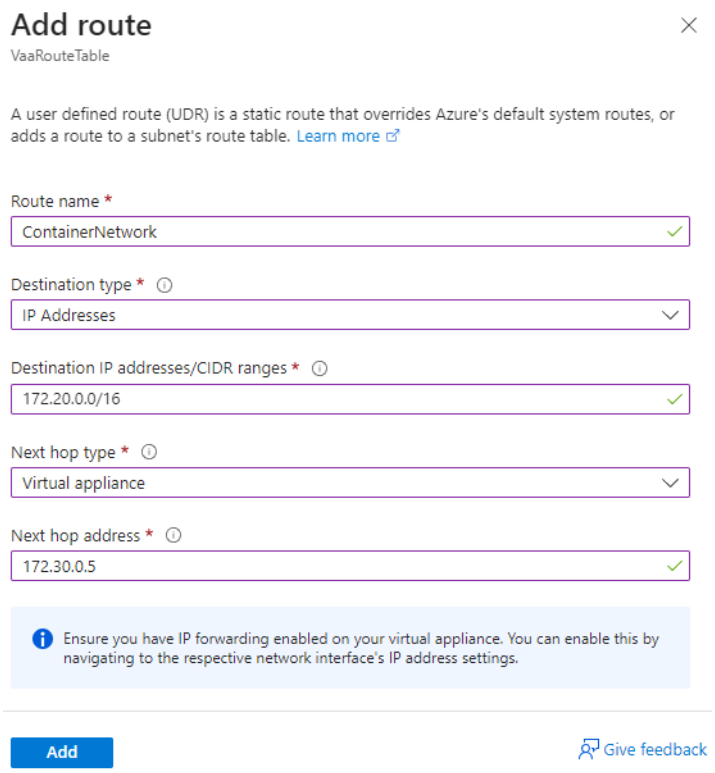
Adding a route

When using the AMF multi-tenant function, you must add routes to the address ranges (prefixes) used by each container and to the networks of Tenant A and Tenant B to the route table.

1. From the Azure portal, enter “VaaRouteTable” in the **Search resources** field, then select the route table you created earlier.
2. From the side menu, select **Settings > Routes**, and click **+Add**.



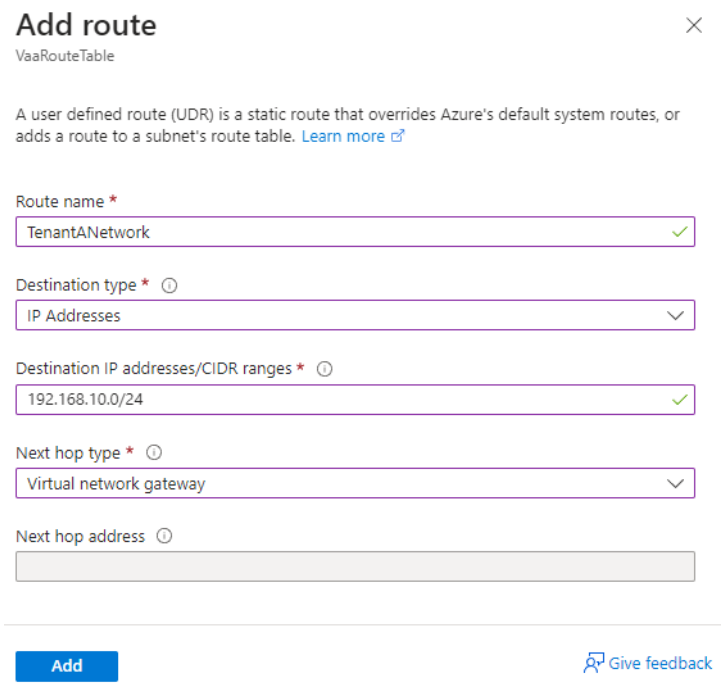
3. Add a static route to the address range used by the container. On the **Add route** dialog, enter appropriate values for each item and click **Add**.



Route name	ContainerNetwork
Destination type	IP Addresses
Destination IP addresses/CIDR ranges	172.20.0.0/16
Next hop type	Virtual appliance
Next hop address	172.30.0.5 (This is the private IP address of the virtual machine)

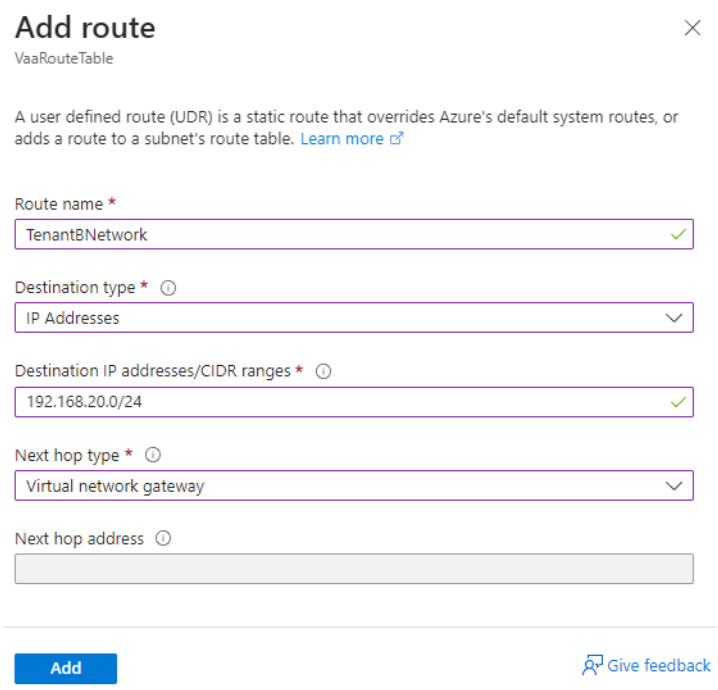
4. After a few moments, the addition will be completed and you will see a notification that says “Route added successfully”.

5. Next, add a static route for TenantA. From the side menu, select **Settings > Routes**, and click **+Add**. On the **Add route** dialog, enter appropriate values for each item and click **Add**.



Route name	TenantANetwork
Destination type	IP Addresses
Destination IP addresses/CIDR ranges	192.168.10.0/24
Next hop type	Virtual network gateway

6. Finally, add a static route for TenantB. From the side menu, select **Settings > Routes**, and click **+Add**. On the **Add route** dialog, enter appropriate values for each item and click **Add**.



Route name	TenantBNetwork
Destination type	IP Addresses
Destination IP addresses/CIDR ranges	192.168.20.0/24
Next hop type	Virtual network gateway

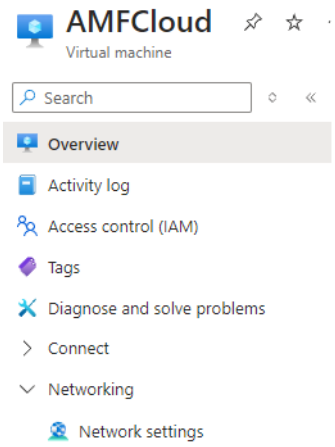
7. After a few moments, the addition will be completed and you will see a notification that says “Route added successfully”.

This completes the process of adding new routes.

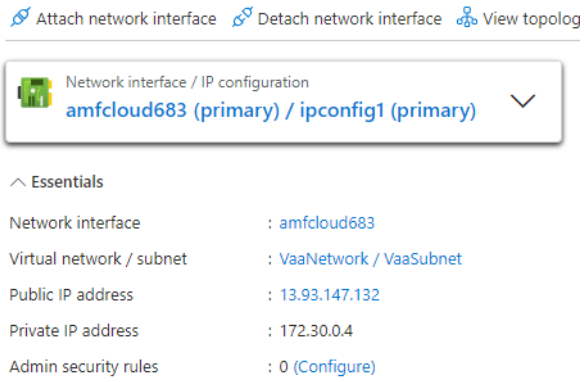
Enable IP forwarding on the virtual machine's network interface

If you use the AMF multi-tenancy function, you must enable IP forwarding on the network interface of the virtual machine. You need to configure it so that packets addressed to the container from outside can be forwarded to the container.

1. From the Azure portal, enter “AMFCloud” in the **Search resources** field, then select the virtual machine you created.
2. From the menu at the left, click on **Networking > Network settings**.

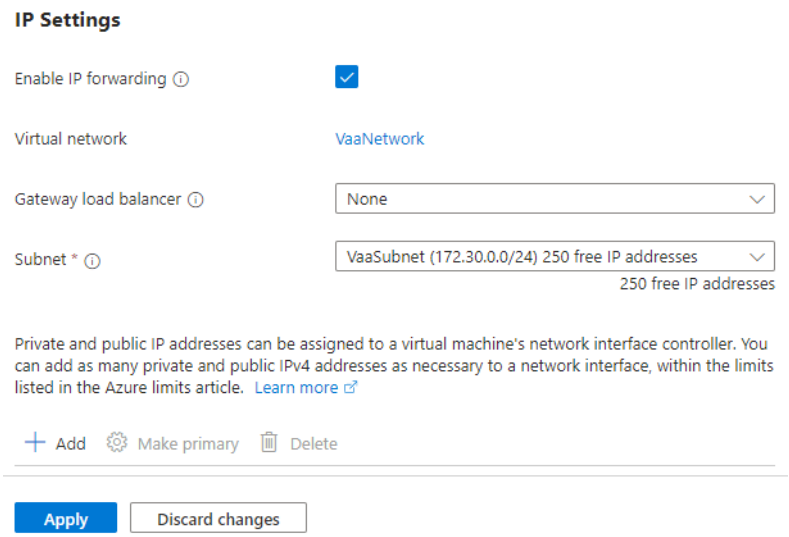


3. Next, under **Network interface**, click on the name displayed.



Note: When you create a virtual machine, a name such as “amfcloud683” is automatically assigned to the network interface. In your installation, the number will probably be different.

4. In the **IP Settings** tab, check the check-box labelled **Enable IP forwarding**. Click **Apply**.



5. After a few moments, the configuration changes are complete and you'll see a notification that says “Network interface saved.”

This completes the process of enabling IP forwarding on the network interface of the virtual machine, and also completes the additional settings for the multi-tenant mode configuration.

AR router settings

Next, we will explain the IPsec-related settings of the AR router, which is the VPN router on the tenant network side. For information on the network configuration, refer to Network Configuration in Multitenant Mode.

Here, we assume that the AR router is connected to the Internet via the ppp0 interface. We also assume that the settings on the Azure side have been completed.

Note: The following is a reference example, so please adjust the settings as appropriate in your actual environment.

The following parameters are used for the VPN connection with Azure:

Table 16: ISAKMP settings

IKE PHASE 1 (ISAKMP) SETTINGS	
Authentication Method	Pre-shared key
IKE version and exchange mode	IKEv2
Diffie-Hellman Groups	Group2 (1024-bit MODP)
Encryption algorithm	AES256
Authentication Algorithm	SHA-1
SA validity period	28800 seconds (8 hours)

Table 17: IPSEC settings

IKE PHASE 2 (IPSEC) SETTINGS	
SA mode	Tunnel Mode
Security Protocol	ESP (Encryption + Authentication)
Encryption algorithm	AES256
Authentication Algorithm	SHA-1
SA validity period	3600 seconds (1 hour)

Table 18: Other settings

UNIQUE SETTINGS IN THIS EXAMPLE	
Pre-shared key	abcdefghijklmnopqrstuvwxyz1234

ISAKMP Settings

ISAKMP Profile

```
awplus(config)# crypto isakmp profile Azure-Phase-1
awplus(config-isakmp-profile)# version 2
awplus(config-isakmp-profile)# lifetime 28800
awplus(config-isakmp-profile)# transform 1 integrity sha1
encryption aes256 group 2
awplus(config-isakmp-profile)# exit
awplus(config)#
```

Pre-shared key

```
awplus(config)# crypto isakmp key abcdefghijklmnopqrstuvwxyz1234
address 10.0.0.1
```

ISAKMP Peer (Specify the ISAKMP profile to use for connecting to the Azure Virtual Network Gateway)

```
awplus(config)# crypto isakmp peer address 10.0.0.1 profile
Azure-Phase-1
```

IPsec settings

IPsec Profile

```
awplus(config)# crypto ipsec profile Azure-Phase-2
awplus(config-ipsec-profile)# lifetime seconds 3600
awplus(config-ipsec-profile)# transform 1 protocol esp integrity
sha1 encryption aes256
awplus(config-ipsec-profile)# exit
```

Tunnel interface settings

Tunnel0 interface

```
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source ppp0
awplus(config-if)# tunnel destination 10.0.0.1
awplus(config-if)# tunnel protection ipsec profile Azure-Phase-2
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# ip address 169.254.0.1/32
awplus(config-if)# ip tcp adjust-mss 1260
awplus(config-if)# exit
```

Routing Settings

Static Routes

```
awplus(config)# ip route 0.0.0.0/0 ppp0
awplus(config)# ip route 172.20.0.0/16 tunnel0
awplus(config)# ip route 172.20.0.0/16 null 254
```

At this point, IP communication is possible between Container A and Tenant A network, and between Container B and Tenant B network.

Note: This installation guide does not cover AMF configuration. For information on setting up virtual links between this product and the AMF network, see the AMF Feature Overview and Configuration Guide.

Firmware Updates

To update the firmware of this product, use the **software-upgrade** command.

Prerequisites

You must download the maintenance firmware (ISO image file) for this product from our website and upload it to the product on Azure.

The firmware for this product is distributed in the following two formats, each of which has different uses as follows:

- The VHD image file is for uploading to Azure to create a custom image for this product. For more information, see “Create an Azure image”.
- The ISO image file is used to update the firmware. The ISO image files provided on our website are for updating the firmware of this product that is already running on Azure.

Update Procedure

To update the firmware of the product, log in to the product's CLI and follow the steps below.

1. Verify that the ISO image file is present on the file system.

```
awplus#  you
4096 drwx Mar 14 2016 03:00:00 atmf/
2401 -rw- Mar 13 2016 23:10:34 V60153A591FFD2F0.bin
143 -rw- Mar 13 2016 09:58:49 reboot.log
551 -rw- Mar 13 2016 09:57:48 default.cfg
25499648 -rw- Feb 16 2016 20:45:45 vaa-5.5.4-2.2.iso • New firmware
```

The last line in this example output shows the ISO file that has been uploaded, and is ready for you to use for upgrading.

2. Specify the ISO image file with the software-upgrade command. A confirmation message will be displayed, so enter “y”.

```
awplus# software-upgrade vaa-5.5.4-2.2.iso
Install this release to disk? (y/n): y
Upgrade succeeded, the changes will take effect after rebooting the device.
```

3. Reboot with the new firmware.

```
awplus# reboot
```

C613-04179-00 REV A

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com