

# Local and virtual network gateways

Local and virtual network gateways are **virtual private network (VPN)** gateways that are used to connect to on-premises networks and encrypt all traffic going between an **Azure Virtual Network (VNet)** and a local network. Each virtual network can have only one virtual network gateway, but one virtual network gateway can be used to configure multiple VPN connections.

We will cover the following recipes in this chapter:

- Creating a local network gateway in the Azure portal
- Creating a local network gateway with PowerShell
- Creating a virtual network gateway in the Azure portal
- Creating a virtual network gateway with PowerShell
- Modifying the local network gateway settings

## Technical requirements

For this chapter, the following is required:

- An Azure subscription
- Azure PowerShell

The code samples can be found in <https://github.com/PacktPublishing/Azure-Networking-Cookbook-Second-Edition/tree/master/Chapter05>.

## Creating a local network gateway in the Azure portal

When a Site-to-Site connection is created, we have to provide configuration for both sides of the connection—that is, both Azure and on-premises. Although a local network gateway is created in Azure, it represents your local (on-premises) network and holds configuration information on your local network settings. It's an essential component for creating the VPN connection that is needed to create a Site-to-Site connection between the virtual network and the local network.

### Getting ready

Before you start, open a web browser and go to the Azure portal at <https://portal.azure.com>.

### How to do it...

In order to create a new local network gateway, the following steps are required:

1. In the Azure portal, select **Create a resource** and choose **Local network gateway** under the **Networking** services (or search for **local network gateway** in the search bar).
2. The parameters that we need to provide are **Name**, **IP address** (that is, the public IP address of the local firewall), **Address space** (the local address space that you want to connect to), **Subscription**, **Resource group**, and **Location**. Optionally, we can configure the **Border Gateway Protocol (BGP)** settings:

## Create local network gateway

**Name \***

packt-lng-portal ✓

**IP address \*** ⓘ

195.222.10.20 ✓

**Address space** ⓘ

192.168.1.0/24 ...

Add additional address range ...

☐ **Configure BGP settings**

**Subscription \***

Microsoft Azure Sponsorship ▾

**Resource group \*** ⓘ

Packt-Networking-Portal ▾

[Create new](#)

**Location \***

(Europe) West Europe ▾

Figure 5.1: Creating a new local network gateway

### How it works...

The local network gateway is used to connect a virtual network gateway to an on-premises network. The virtual network gateway is directly connected to the virtual network and has all the relevant Azure VNet information needed to create a VPN connection. On the other hand, a local network gateway holds all the local network information needed to create a VPN connection.

In this recipe, we created a local network gateway in the Azure portal. In the next recipe, we will learn how to do the same using PowerShell.

## Creating a local network gateway with PowerShell

As mentioned in the previous recipe, the local network gateway holds information on the local network that we want to connect to an Azure VNet. In addition to creating a local network gateway through the Azure portal, we can create it with Azure PowerShell.

### Getting ready

Open the PowerShell console and make sure you are connected to your Azure subscription.

### How to do it...

To create a new local network gateway, execute the following command:

```
New-AzLocalNetworkGateway -Name packt-Ing-script -ResourceGroupName 'Packt-  
Networking-Script' -Location 'westeurope' -GatewayIpAddress '195.222.10.20'  
-AddressPrefix '192.168.1.0/24'
```

### How it works...

In order to deploy a new local network gateway, we need to provide parameters for the name, resource group, location, gateway IP address, and address prefix that we want. The gateway IP address is the public IP address of the local firewall that you are trying to connect to. The address prefix is the subnet prefix of the local network that you are trying to connect to. This address must be associated with a firewall address that is provided as a gateway IP address.

In this recipe, we created a local network gateway with Azure PowerShell. Let's move on to the next recipe and learn how to create a virtual network gateway in the Azure portal.

## Creating a virtual network gateway in the Azure portal

After a local network gateway is created, we need to create a virtual network gateway in order to create a VPN connection between the local and Azure networks. As a local network gateway holds information on the local network, the virtual network gateway holds information for the Azure VNet that we are trying to connect to.

### Getting ready

Before you start, open a web browser and go to the Azure portal at <https://portal.azure.com>.

## How to do it...

In order to create a new virtual network gateway, the following steps are required:

1. In the Azure portal, select **Create a resource** and choose **Virtual network gateway** under the **Networking** services (or search for **virtual network gateway** in the search bar).
2. Everything is done in a single pane, but for the purpose of better visibility, I'm going to break it down into two sections. In the first section, we need to provide **Subscription**, **Name**, **Region**, **Gateway type**, **VPN type**, **SKU**, and **Generation**, (the **Generation** option depends on the SKU; not all SKUs support **Generation 2**), and we need to select **Virtual network** that will be used in the connection. Note that the gateway subnet must be created prior to this, and only virtual networks with a gateway subnet will be available for selection. An example is shown in Figure 5.2:

### Create virtual network gateway

#### Project details

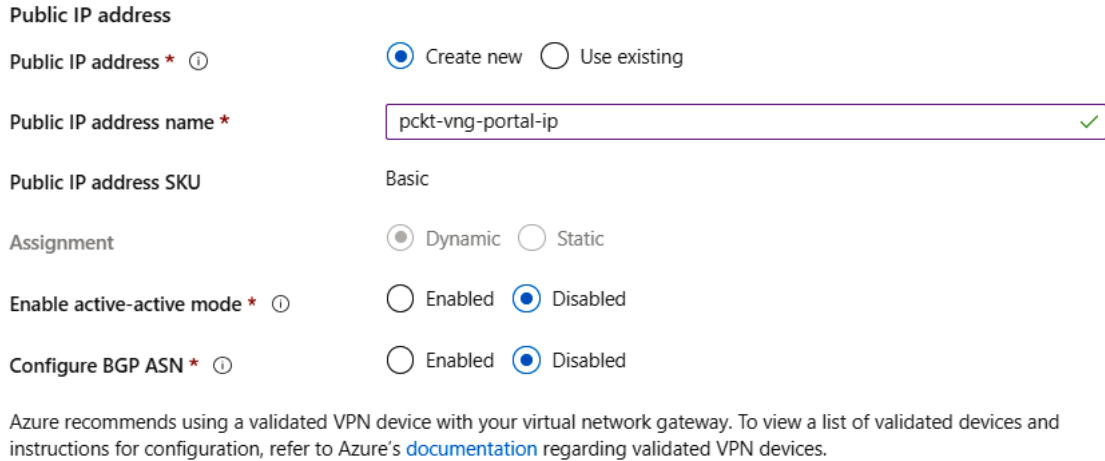
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Microsoft Azure Sponsorship
Resource group ⓘ	Packt-Networking-Portal (derived from virtual network's resource group)
<b>Instance details</b>	
Name *	packt-vng-portal ✓
Region *	(Europe) West Europe
Gateway type * ⓘ	<input checked="" type="radio"/> VPN <input type="radio"/> ExpressRoute
VPN type * ⓘ	<input checked="" type="radio"/> Route-based <input type="radio"/> Policy-based
SKU * ⓘ	VpnGw1
Generation ⓘ	Generation1
Virtual network * ⓘ	Packt-Portal <a href="#">Create virtual network</a>
Subnet ⓘ	GatewaySubnet (10.10.2.0/24)

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Figure 5.2: Creating a new virtual network gateway

3. In the second section, we need to set the **Public IP address** options (select an existing IP address or create a new one), and optionally, we can set **Enable active-active mode** and **Border Gateway Protocol Autonomous System Number (BGP ASN)**:



Public IP address

Public IP address \* ⓘ ☒ Create new ☐ Use existing

Public IP address name \*  ✓

Public IP address SKU Basic

Assignment ☒ Dynamic ☐ Static

Enable active-active mode \* ⓘ ☐ Enabled ☒ Disabled

Configure BGP ASN \* ⓘ ☐ Enabled ☒ Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

Figure 5.3: Setting the public IP address options

4. After validation, we can click on **Create** and start the deployment. Note that creating the virtual network gateway takes longer than for most other Azure resources; deployment can take from 45 to 90 minutes.

## How it works...

The virtual network gateway is the second part needed to establish the connection to the Azure VNet. It is directly connected to the virtual network and is needed to create both Site-to-Site and Point-to-Site connections. We need to set the VPN type, which needs to match the type of the local VPN device when a Site-to-Site connection is created.

Active-active mode provides high availability by associating two IP addresses with separate gateway configurations to ensure uptime.

The border gateway protocol is a standard protocol for the exchange of routing and reachability information between different **autonomous systems (ASes)**. Each system is assigned an **autonomous systems number (ASN)**.

In this recipe, we created a virtual network gateway in the Azure portal. Let's move on to the next recipe.

## Creating a virtual network gateway with PowerShell

Creating a virtual network gateway is possible with PowerShell. Again, this helps automate processes. For example, if we start creating a virtual network gateway using a portal and notice that our virtual network isn't listed, it's probably because it's missing a gateway subnet. So, we must abandon the process, go back, create the gateway subnet, and start creating the virtual network gateway. Using PowerShell, we can ensure that all the requisite resources are present before starting, and then continue with the creation of the virtual network gateway.

### Getting ready

Open the PowerShell console and make sure that you are connected to your Azure subscription.

### How to do it...

To create a new virtual network gateway, execute the following script:

```
$vnet = Get-AzVirtualNetwork -ResourceGroupName 'Packt-Networking-Script'
-Name 'Packt-Script'

Add-AzVirtualNetworkSubnetConfig -Name 'GatewaySubnet' -AddressPrefix
10.11.2.0/27 -VirtualNetwork $vnet

$vnet | Set-AzVirtualNetwork

$gwpip = New-AzPublicIpAddress -Name VNet1GWIP -ResourceGroupName 'Packt-
Networking-Script' -Location 'westeurope' -AllocationMethod Dynamic

$vnet = Get-AzVirtualNetwork -ResourceGroupName 'Packt-Networking-Script'
-Name 'Packt-Script'

$subnet = Get-AzVirtualNetworkSubnetConfig -Name 'GatewaySubnet'
-VirtualNetwork $vnet

$gwipconfig = New-AzVirtualNetworkGatewayIpConfig -Name gwipconfig1 -SubnetId
$subnet.Id -PublicIpAddressId $gwpip.Id

New-AzVirtualNetworkGateway -Name VNet1GW -ResourceGroupName 'Packt-
Networking-Script' -Location 'westeurope' -IpConfigurations $gwipconfig
-GatewayType Vpn -VpnType RouteBased -GatewaySku VpnGw1
```

## How it works...

The script performs a few different operations to make sure that all requirements are met so that we can create a virtual network gateway. The first step is to collect information on the virtual network that we are going to use. Next, we add the gateway subnet to Azure VNet and create a public IP address that will be used by the virtual network gateway. We collect all the information and ensure that all the required resources are present, and then finally we create a new virtual network gateway.

In this recipe, we learned how to create a virtual network gateway with Azure PowerShell. In the next recipe, we will learn how to modify the settings of the local network gateway.

## Modifying the local network gateway settings

Network configurations may change over time, and we may need to address these changes in Azure as well—for example, the public IP address of a local firewall may change, and we'd then need to reconfigure the local network gateway, or a local network might be reconfigured and the address space or subnet has changed, so we would need to reconfigure the local network gateway once again.

## Getting ready

Before you start, open a web browser and go to the Azure portal at <https://portal.azure.com>.

## How to do it...

In order to modify local network gateway settings, we must do the following:

1. Locate the local network gateway in the Azure portal and go to **Configuration**.
2. In **Configuration**, we can edit **IP address** or **Address space**. We can also add additional address spaces if we want to connect multiple local subnets to Azure VNet:



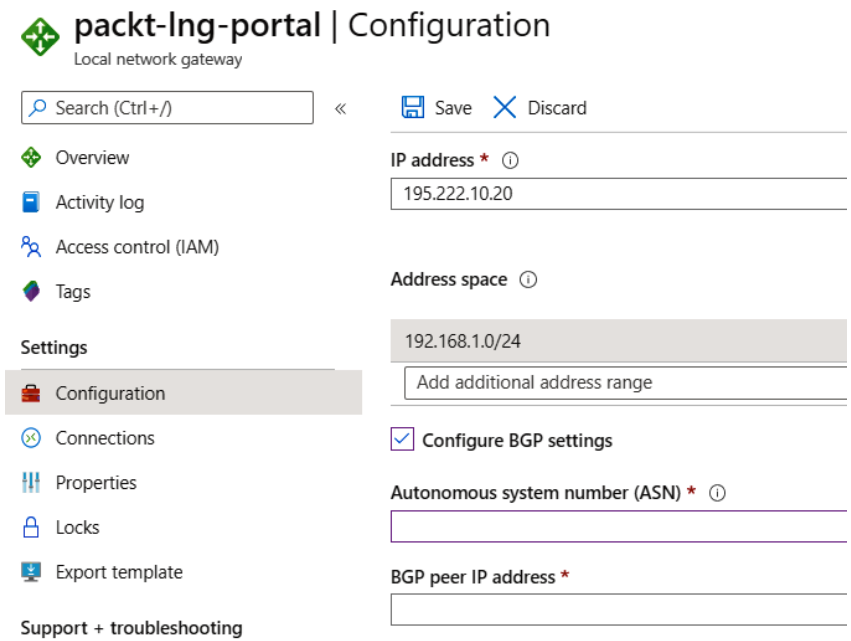


Figure 5.4: Modifying the local network gateway settings

How it works...

The local network gateway holds the local network information needed to create a Site-to-Site connection between the local and Azure networks. If this information changes, we can edit it in the **Configuration** settings. The changes that can be made are the IP address (that is, the public IP address of the local firewall) and the address space we are connecting to. Additionally, we can add or remove address spaces if we want to add or remove subnets that are able to connect to Azure VNet. If the configuration in the local network gateway is no longer valid, we can still use it to create a completely new connection to a new local network if needed.

