**NETWORK**

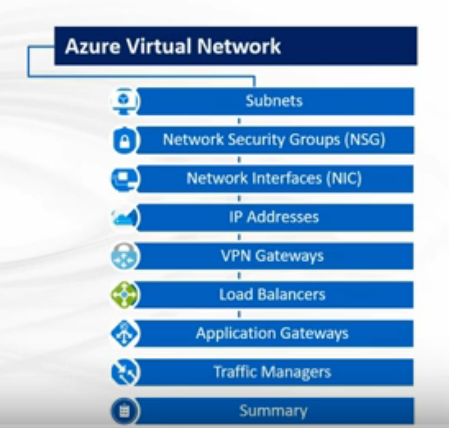
* A network is a collection of computers, servers or other devices connected to one another to allow the sharing of data
* An excellent example of a network is the **Internet**, which connects millions of people all over the world
* Network Devices: Laptop, Desktop Computers

**Types of Network**

LAN, WAN

* **LAN (Local Area Network):** A Local Area Network (LAN) is a network that is limited to a relatively small area
* It is generally limited to a geographic area such as a writing lab, school, or building
* Computers connected to a network are broadly categorized as servers or workstations
* Humans do generally not use servers directly, but rather run continuously to provide "services" to the other computers (and their human users) on the network. Services provided can include printing and faxing, software hosting, file storage and sharing, messaging, data storage and retrieval, complete access control (security) for the network's resources, and many others
* On a single LAN, computers and servers may be connected by cables or wirelessly
* **A WAN (wide area network)** is a communications network that spans a large geographic area such as across cities, states, or countries
* A WAN connects different smaller networks, including local area networks (LANs) and metro area networks (MANs)
* This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.
* WANs are similar to a banking system, where hundreds of branches in different cities are connected with each other in order to share their official data
* Since WANs, by definition, cover a larger distance than LANs, it makes sense to connect the various parts of the WAN using a [**virtual private network**](https://www.lifewire.com/what-is-a-vpn-2377977) **(VPN).** This provides protected communications between sites, which is necessary given that the data transfers are happening over the internet

**VNET**



<https://www.edureka.co/blog/azure-virtual-network-tutorial/>

* Azure Virtual Network (VNet) is a representation of your own network in the cloud.
* You have the total control over the IP address blocks, DNS settings, security policies within this network
* You also have the power to divide the VNet into further partitions called subnets and launch your Azure Virtual Machines along with your Cloud Services
* You can connect the VNet to your on-premises network using one of the connectivity options available in Azure
* **Public IP addresses** allow Azure resources to communicate with the Internet and other Azure public facing services like Azure Redis Cache.
* A dynamic IP is assigned to the VM, by default. At the point the VM is started /stopped the IP is released/renewed
* **Private IP addresses** allow communication between resources in the virtual network, along with those connected through a Virtual Private Network without using an Internet-routable IP address

**SUBNETS**

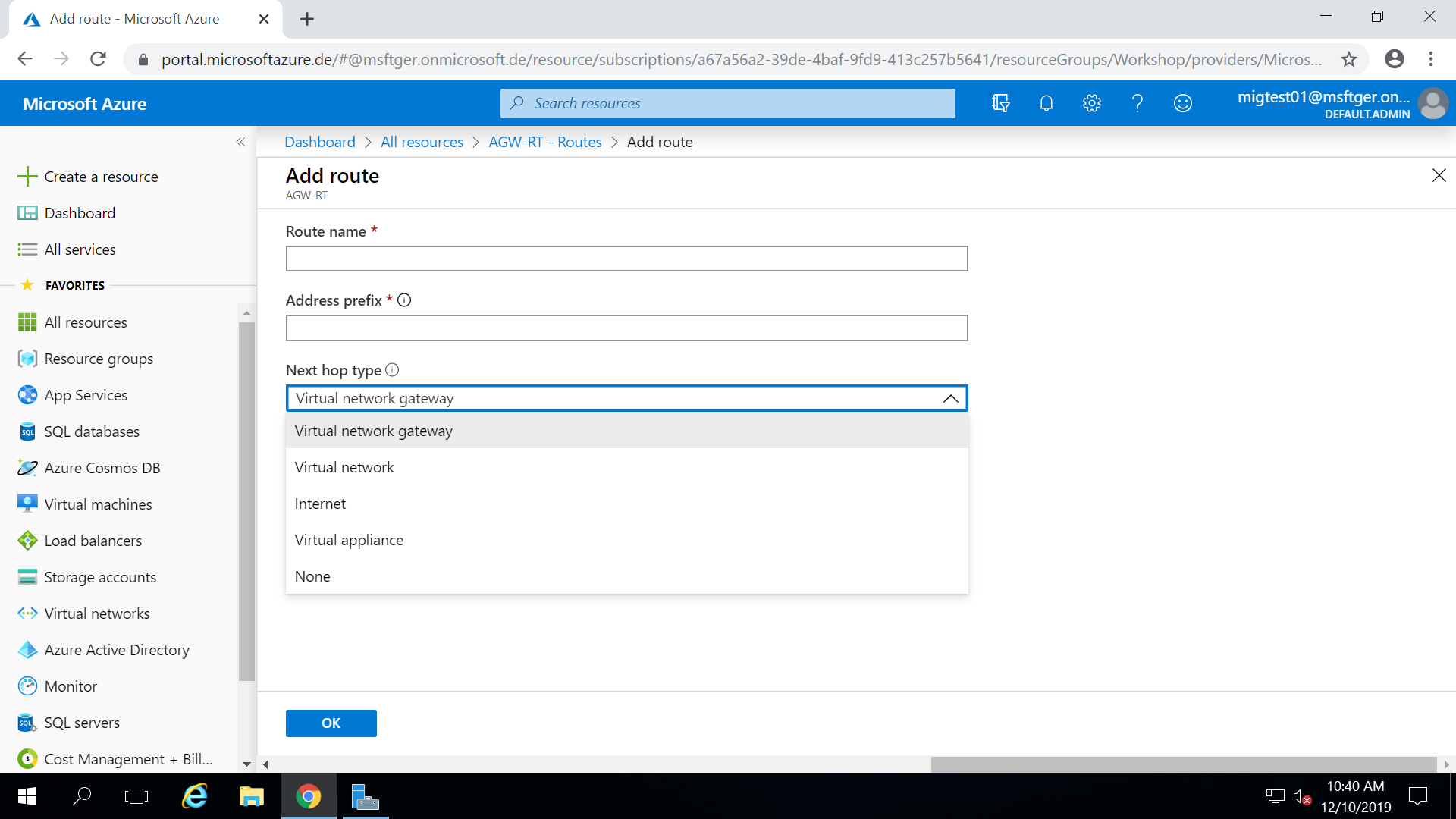
* A subnet is a range of IP addresses in the VNet
* We can divide a VNet into multiple subnets for organization and security
* All the VMs and PaaS role instances that are deployed to subnets, whether same or different, within a VNet can easily communicate with each other without any extra configuration.
* Additionally, you can configure route tables and Network Security Groups that handle the inbound and outbound traffic to a subnet.

**Peering**

* A virtual network is mapped to a single region
* Suppose, Multiple virtual networks from different regions can be connected together using Virtual Network Peering

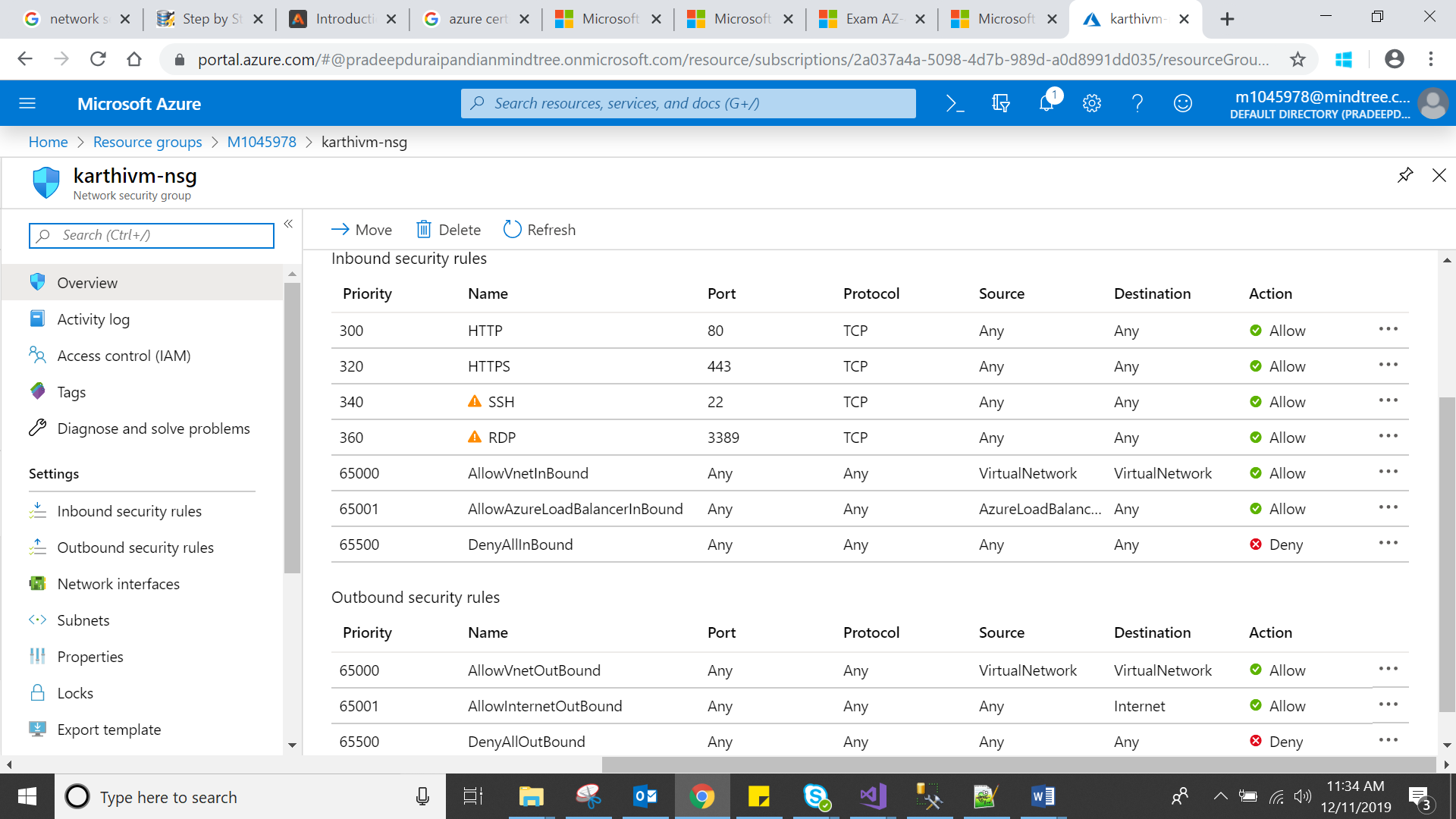
**Route Table**

* Azure automatically routes traffic between Azure subnets, virtual networks, and on-premises networks. If you want to change any of Azure's default routing, you do so by creating a route table.
* Azure automatically creates a route table for each subnet within an Azure virtual network and adds system default routes to the table
* You can override some of Azure's system routes with [custom routes](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#custom-routes), and add additional custom routes to route tables
* Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create system routes, nor can you remove system routes, but you can override some system routes with [custom routes](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#custom-routes)
* When different route types are present in a UDR route table, user defined routes are preferred over the default system routes



**Network security group**

* A network security group (NSG) is a networking filter (firewall) containing a list of security rules allowing or denying network traffic to resources connected to Azure VNets
* NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager)
* When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet
* A network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#security-rules) that allow or deny **inbound network traffic to**, or **outbound network traffic from**, several types of Azure resources
* NSG Rules are enforced based on their Priority. Priority values start from 100 and go to 4096. Rules will be read and enforced starting with 100 then 101, 102 etc.
* Ex: A protocol is a set of formalized rules that explains how data is communicated over a network. **HTTP** (Hypertext Transfer Protocol) is the set of rules for transferring files, such as text, graphic images, sound, video, and other multimedia files, on the [World Wide Web](https://whatis.techtarget.com/definition/World-Wide-Web)
* HTTP provides a pathway for you to communicate with a web [server](https://www.lifewire.com/servers-in-computer-networking-817380). When you open a web page that uses HTTP, your web browser uses the Hypertext Transfer Protocol (over port 80) to request the page from the webserver. When the webserver receives and accepts the request, it uses the same protocol to send the page back to you



* Remote Desktop Protocol (RDP) is a [proprietary protocol](https://en.wikipedia.org/wiki/Proprietary_protocol) developed by [Microsoft](https://en.wikipedia.org/wiki/Microsoft), which provides a user with a [graphical interface](https://en.wikipedia.org/wiki/Graphical_user_interface) to connect to another computer over a network connection

**Vnet to Vnet VPN gateway**

Multiple virtual networks from different regions & different subscriptions can be connected together

**VPN**

* Virtual Private Network, allows you to create a secure connection to another network over the Internet.
* Therefore, if that server is in a different country, it will appear as if you are coming from that country, and you can potentially access things that you could not normally.
* Virtual Private Networks are most often used by corporations to protect sensitive data

## Why do I need a VPN?

* [**Hide your IP address**](https://www.whatismyip.com/should-i-hide-my-ip-address/)

Connecting to a Virtual Private Network often conceals your real IP address.

* [**Change your IP address**](https://www.whatismyip.com/how-to-change-your-ip-address/)

Using a VPN will almost certainly result in getting a different IP address.

* **Encrypt data transfers**

A Virtual Private Network will protect the data you transfer over public WiFi.

* [**Mask your location**](https://www.whatismyip.com/ip-address-lookup/)

With a Virtual Private Network, users can choose the country of origin for their Internet connection.

* **Access blocked websites**

Get around website blocked by governments with a VPN

**Network service endpoints**

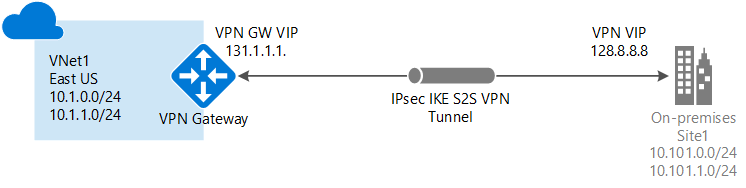
* Today most of the Azure services including **Azure storage** and **Azure SQL** have public IPs
* Anyone would be able to connect to these services over a public IP address and secure access using either a firewall or a security token
* Many customers are not happy using a public facing service as this can be a huge compliance and security issue as well as the attack vectors these services have
* Since the IPs are public and accessible from everywhere
* There is not a way to pull the Azure storage into your VNet, Microsoft introduced a concept called **Virtual Network Service Endpoints**
* **It** allows you to connect your VNet address space to Azure services
* You can also restrict access to the services to be from your VNet only. This allows you to secure access to Azure resources from your VNet only

**VPN GATEWAY**

* A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.
* You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.
* Each virtual network can have only one VPN gateway.
* However, you can create multiple connections to the same VPN gateway. When you create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth
* Two types of VPN Gateway **Site to Site** and **Point to site**

**Site - to – Site**

* It shows you how to use the Azure portal to create a Site-to-Site VPN gateway connection from your on-premises network to the VNet
* A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.
* This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it

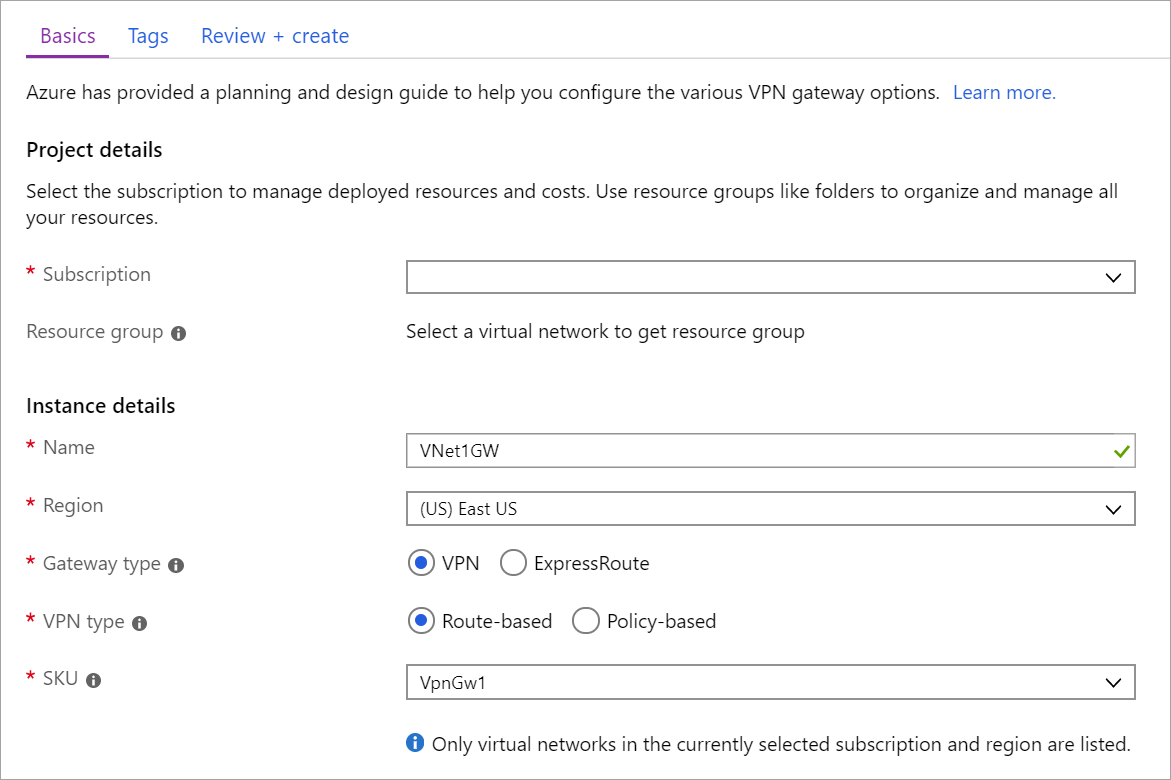


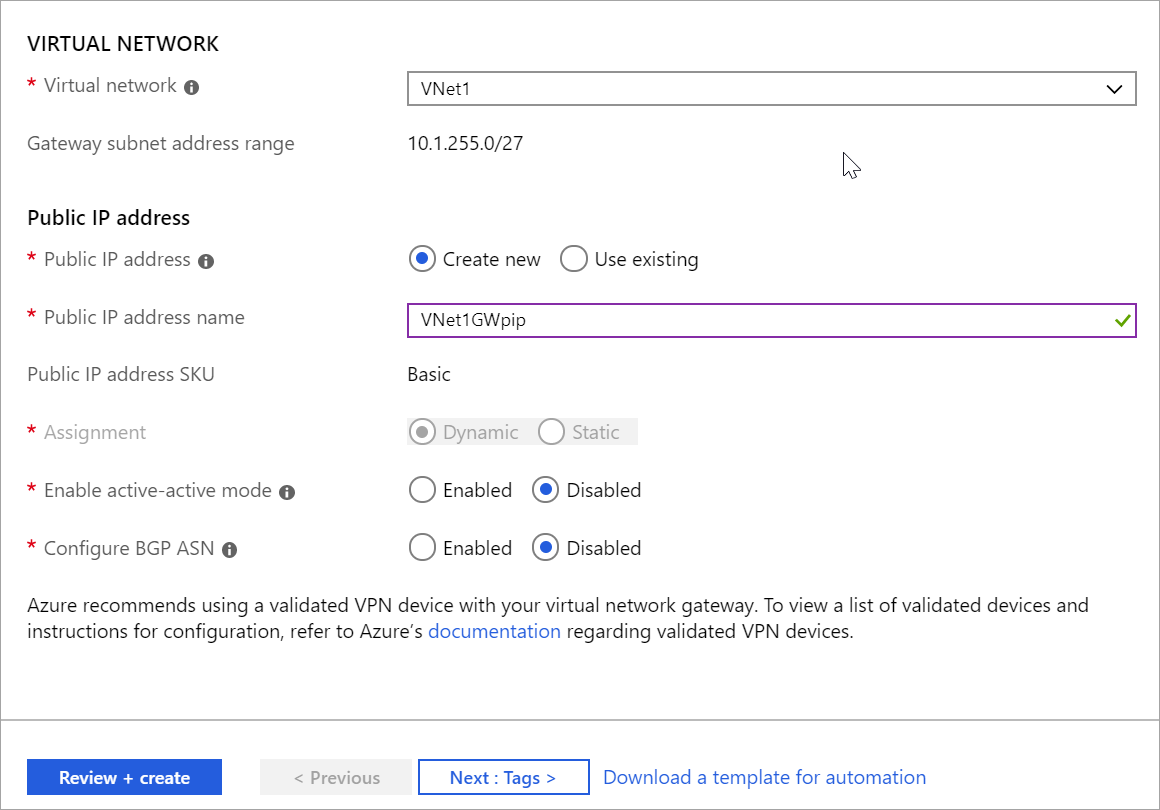
* Steps to be follow,

1. Create a virtual network
2. Create VPN Gateway

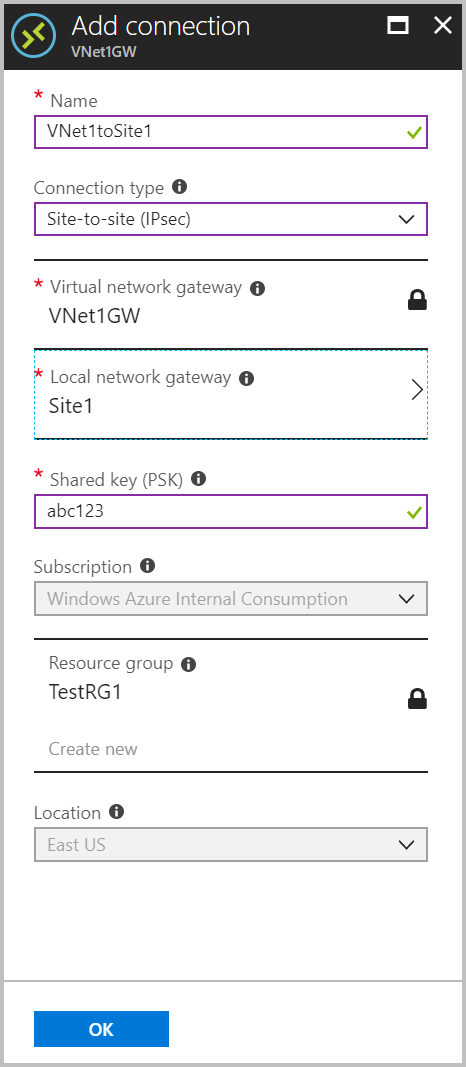
Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU

In the **Search the marketplace** field, type 'Virtual Network Gateway'.





1. Create local network gateway
2. Configure VPN devices
3. Create VPN connections

****

1. Verify the VPN connections