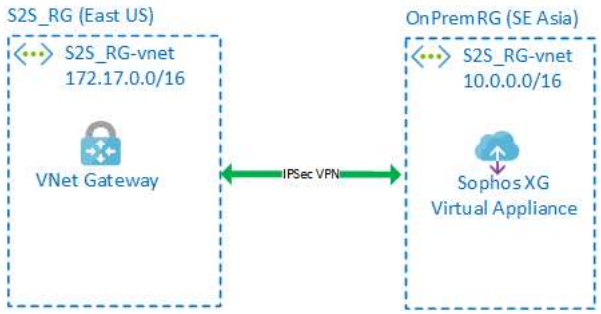
Module 3 - Lab 2: On-Prem to Azure Connections (Optional) - Site-to-Site VPN Connections

Task 1: Review the deployment.

- [ ] 1. In this task review the resources that are being deployed for you. You will see a Sophos XG Virtual Appliance being created which will emulate an on-premises device. The layout of this is depicted in the digaram below



Task 2: Create a VNet.

> In this task you will create a Virtual Machine and a Virtual Network inside a new Resource group which will be use to connect to your emulated On-Prem environment.

- [ ] 1. Open a web browser and navigate to the Azure Portal https://portal.azure.com.
- [ ] 2. Log in with the username sheikhnasirVE7MK@gdcs2.com and password yixbqlD09Z60KFf9.
- [ ] 3. In the search box, search for and select **Virtual Networks**.
- [ ] 4. In the **Virtual Networks** page, click **+ Create**.
- [ ] 5. On the **Basics** blade enter the following and then click **Next : IP Addresses >**:
    - Resource group: **S2S_RG-XDSTSGT1RP**
    - Name: S2S_RG-vnet
    - Region: **East US**
- [ ] 6. On the **IP Addresses** blade, update the the following:
    - IPv4 address space: 172.17.0.0/16
    - Subnet Name: Default
    - Subnet address range: 172.17.0.0/24
- [ ] 7. Click **Review + Create** then click **Create**.

> **Note:** You can continue to the next task without having to wait for the deployment to complete.

Task 3: Create a Gateway Subnet and a Virtual network Gateway.

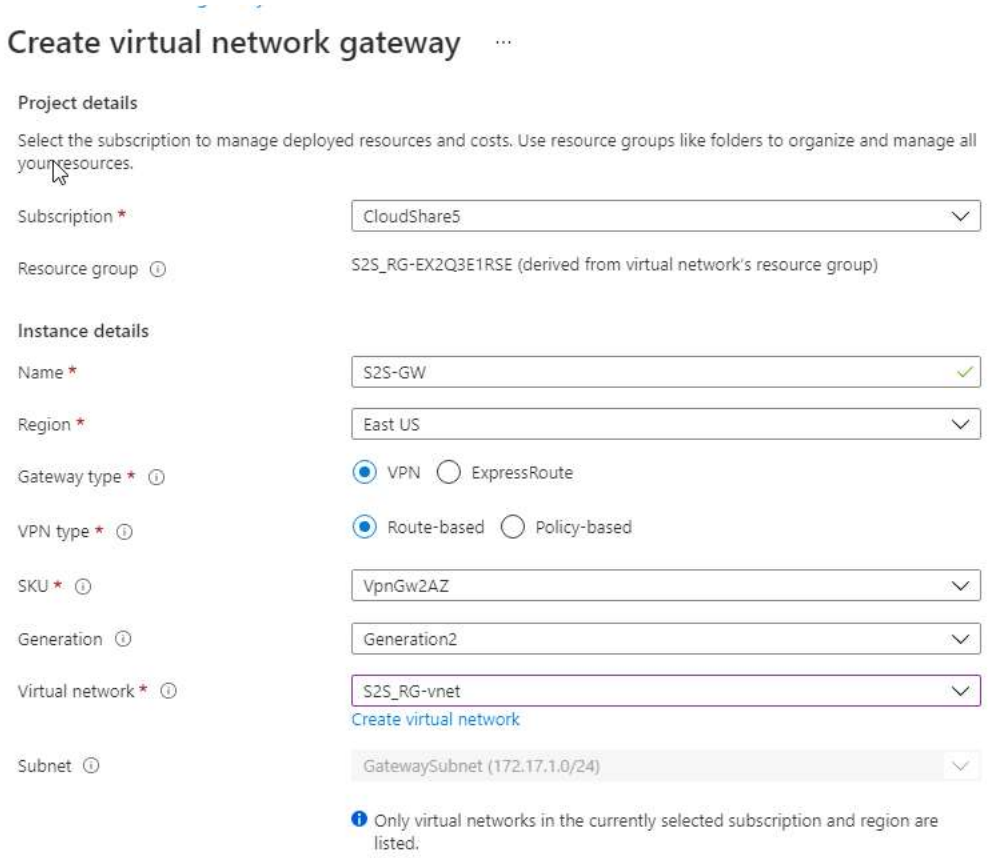
> In this task you will Create a Gateway Subnet and a Virtual network Gateway which will enable you to create a connection between On-Prem and your Azure VNet.

- [ ] 1. In the Azure Portal click **Resource Groups** on the Hub Menu.
- [ ] 2. Click the **S2S_RG-XDSTSGT1RP** resource group that has been created for you.
- [ ] 3. In the **S2S_RG-XDSTSGT1RP** Resource Group blade click the **S2S_RG-vnet**.
- [ ] 4. On the **S2S_RG-vnet** menu click **Subnets**.
- [ ] 5. Click **+ Gateway subnet**.

> **Note:** You need to create a Gateway subnet in order for the Gateway machines to reside in. All the routing is done by the Azure Software Defined Networking.

- [ ] 6. Leave the default options on the **Add subnet** blade and click **Save**.

- [ ] 7. Click **+ Create a resource**.
- [ ] 8. Search for Virtual Network Gateway and select **Virtual network gateway**.
- [ ] 9. Click **Create**.
- [ ] 10. On the **Create virtual network gateway** blade enter the following information:
    - **Name**: S2S-GW
    - **Region**: (US) East US
    - **Gateway type**: VPN
    - **VPN Type**: Route-based
    - **SKU**: Basic
    - **Virtual network**: Select the S2S_RG-vnet (this was created earlier when you deployed the VM)
    - **Public IP address**: (Create New)
    - **Name**: S2S-GW-PIP
    - **Availability Zone**: Zone-reduntant
    - **Enable active-active mode**: Disabled
    - **Configure BGP**: Disabled

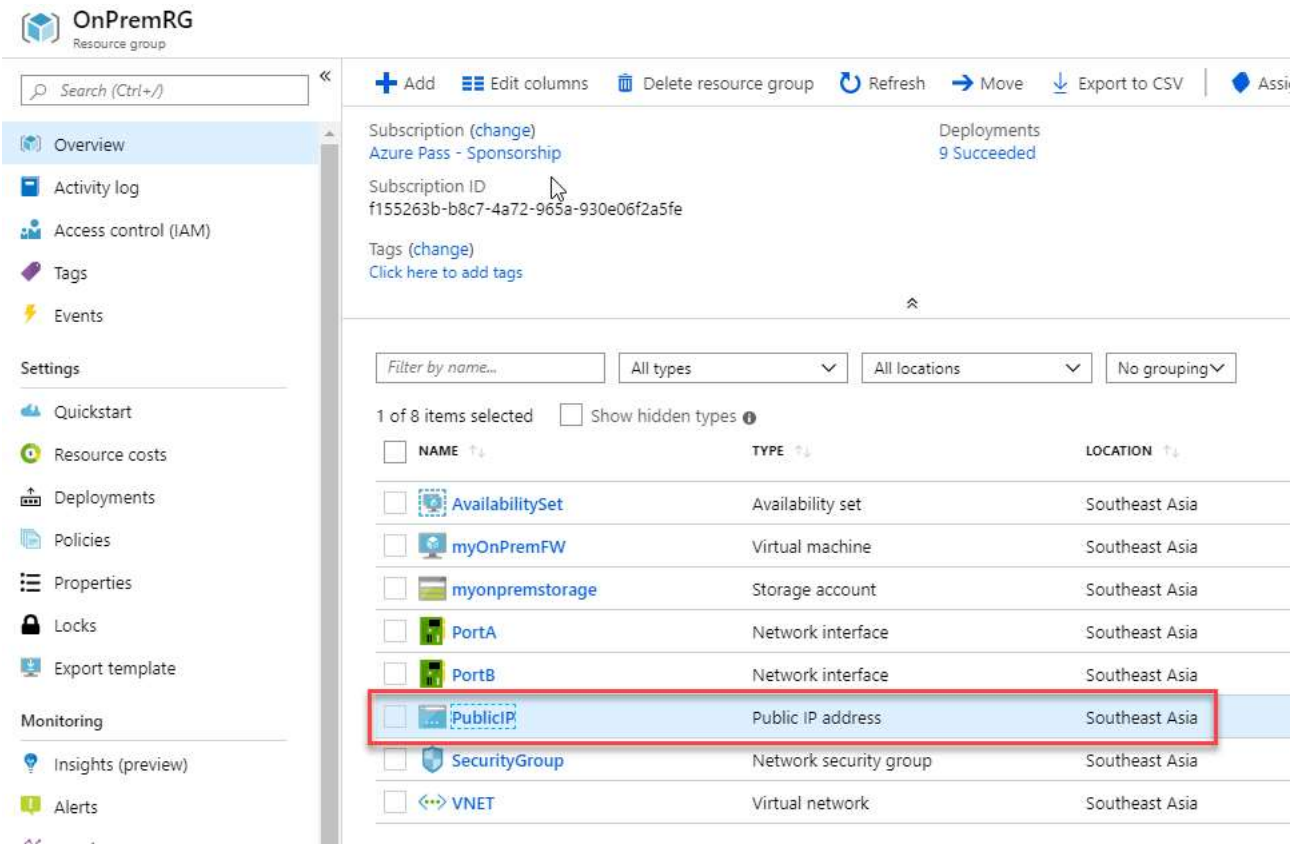


- [ ] 11. Click **Review + create** then on the summary screen click **Create**

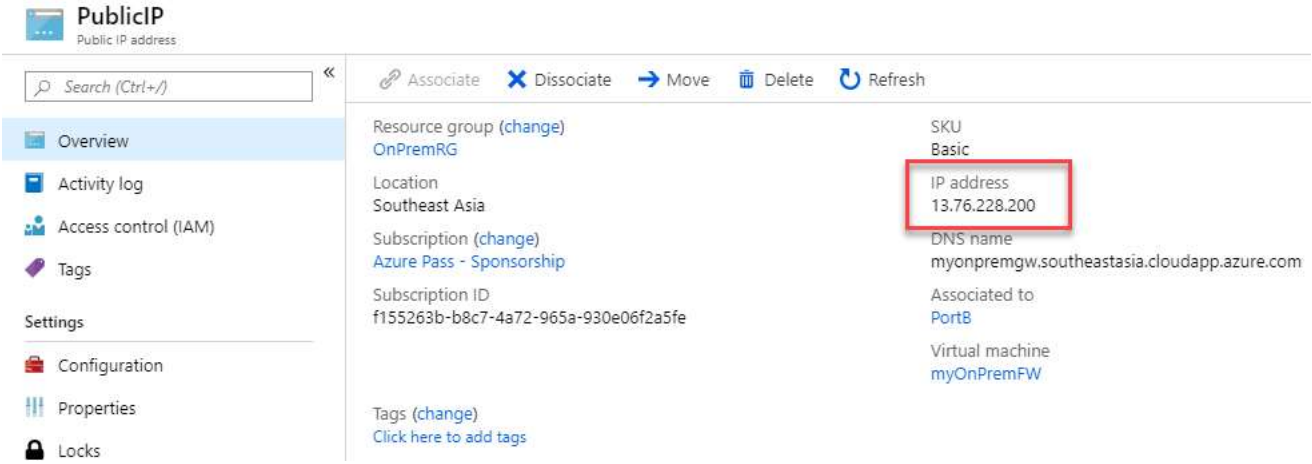
> ⚠ **Note:** The gateway may take upto 45 minutes to deploy, although. in most cases it is much quicker. Monitor this by clicking on the Bell Icon. You can continue to the next task whilst the Gateway is deploying.

Task 4: Configure the Sophos virtual appliance.

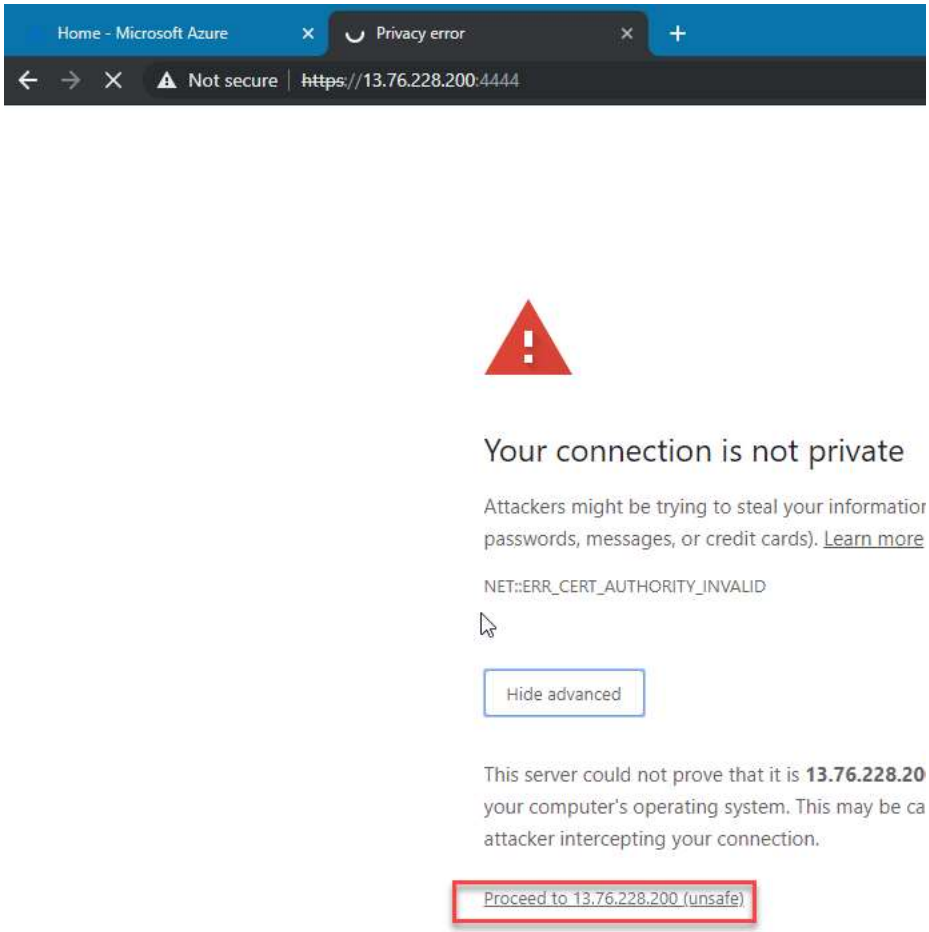
- [ ] 1. On the Azure Portal Hub menu click **Resource Groups**.
- [ ] 2. Select the **OnPremRG-XDSTSGT1RP** Resource Group.
- [ ] 3. Select the **PublicIP** Resource.



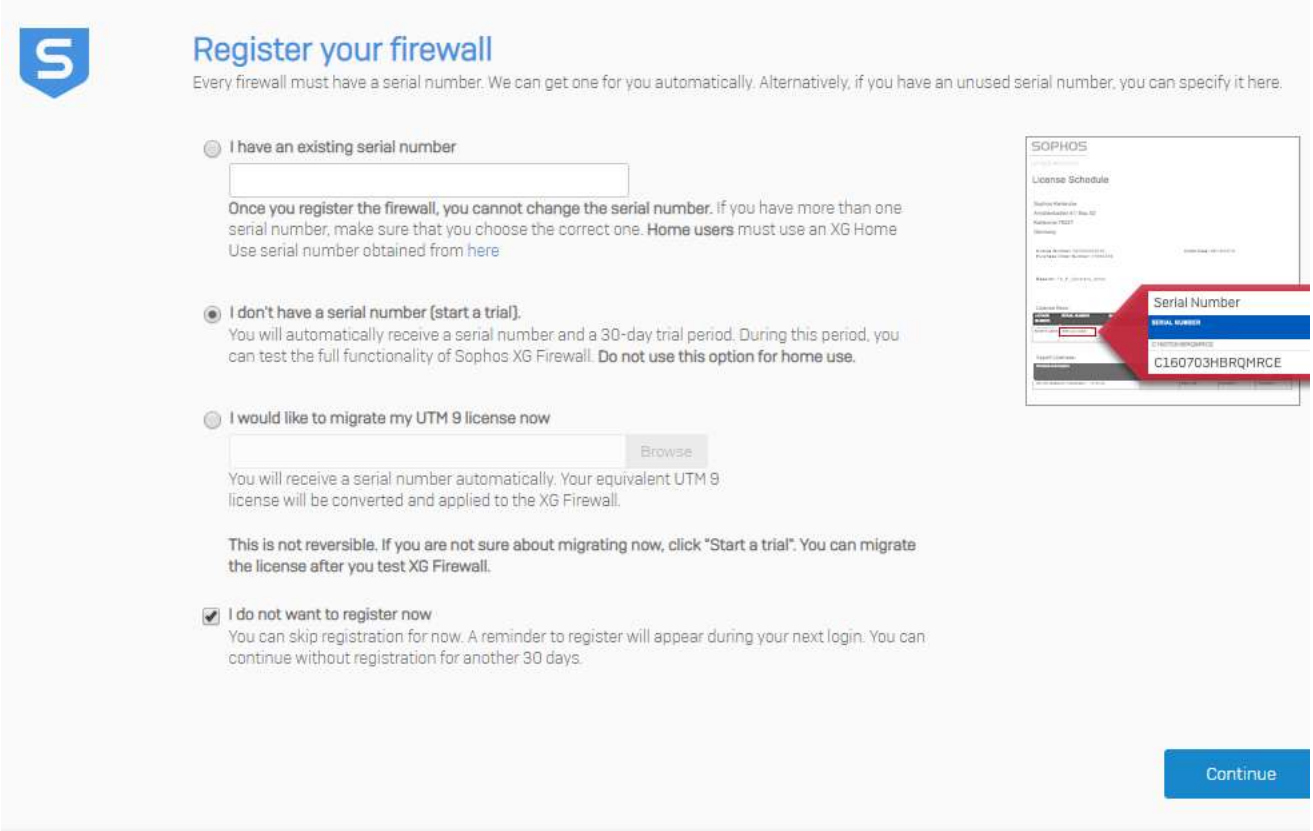
- [ ] 4. Make a note of the assigned Public IP address.



- [ ] 5. Open a new browser session and navigate to https://x.x.x.x:4444 (where x.x.x.x is the public IP address you noted above).
- [ ] 6. Depending on your browser there may be different options to proceed with the connection.

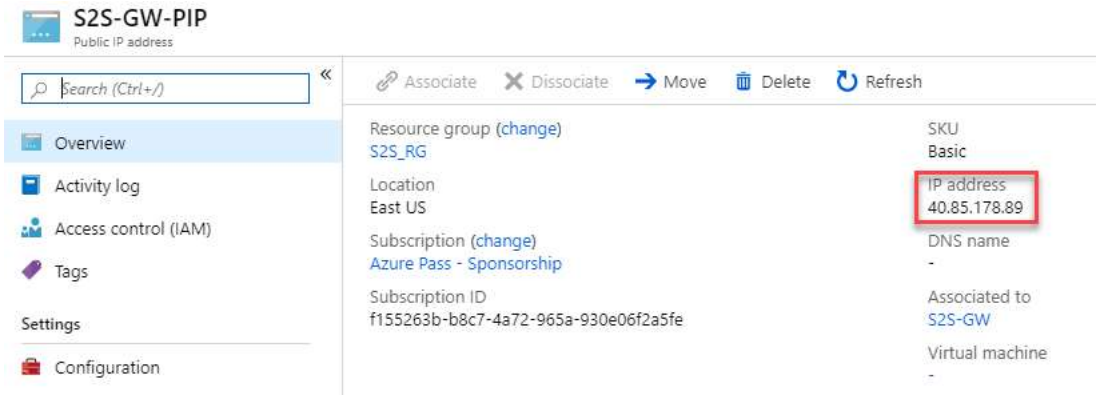


- [ ] 7. Log into the Firewall with the following credentials:
    - Admin
    - 28fCfmb8kFURSdKj
- [ ] 8. Accept the licence agreement.
- [ ] 9. On the Register your firewall page click **I don't have a a serial number (start a trial)** and select **I do not want to register now** then click **Continue**.



- [ ] 10. On the Warning pop up click **Continue**.
- [ ] 11. Return back to the Azure Portal. Open the **S2S_RG-XDSTSGT1RP** Resource Group and select the **S2S-GW-PIP** Public IP and make a note of it.

> ⚠ **Note**: This is your Public IP you will connect your Sophos virtual applicabce to via IPSec VPN.



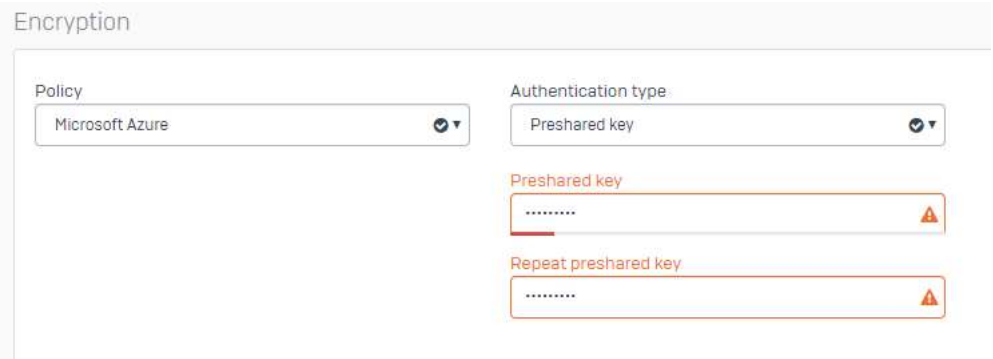
- [ ] 12. Return back to the Sophos Portal.
- [ ] 13. Go to **VPN** > **IPsec Connections**, select **Add** and configure the following settings:

General Settings Section:

- **Name**: On_Prem_to_Azure
- **IP Version**: IPv4.
- **Activate on Save:** Selected.
- **Create firewall rule:** Selected.
- **Description**: Site to Site connection from On Prem to Azure VNet.
- **Connection Type**: Site-to-Site.
- **Gateway Type**: Respond Only.

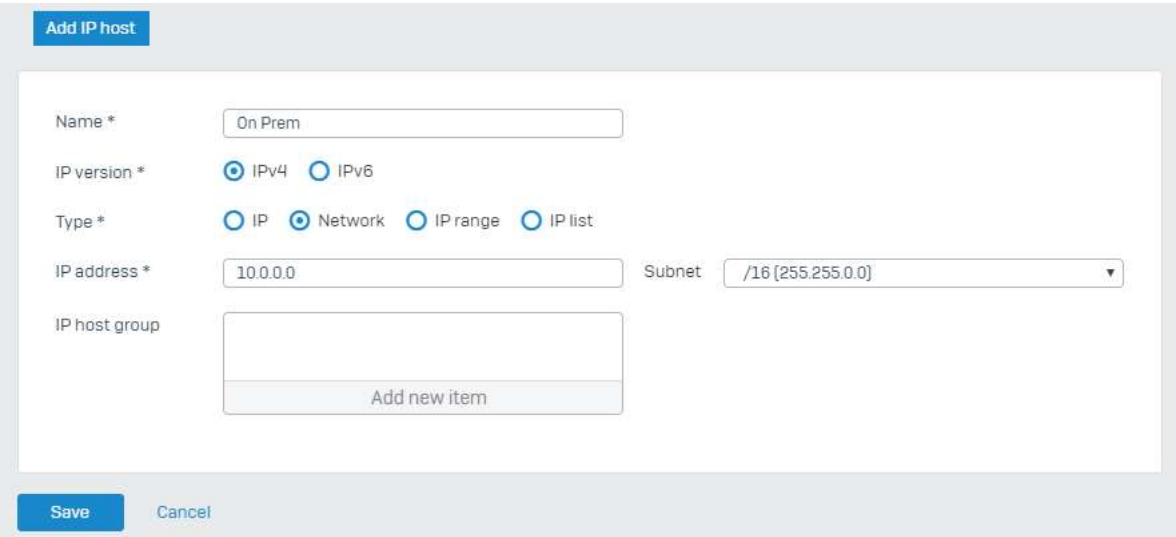
Encryption Section:

- **Policy**: Microsoft Azure.
- **Authentication Type**: Preshared Key.
- **Preshared Key**: 123456789
- **Repeat Preshared Key**: 123456789

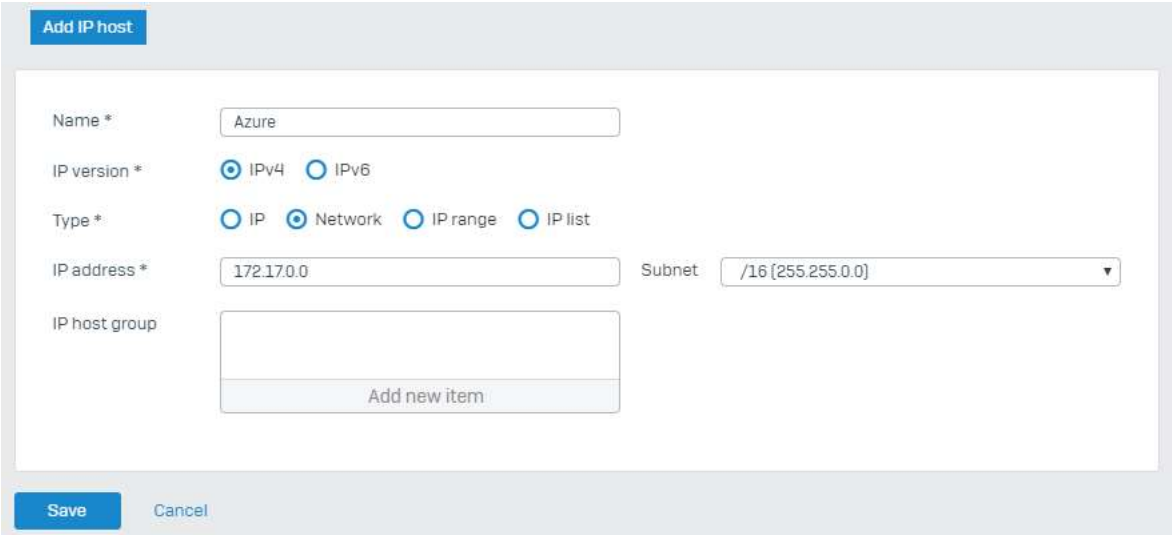


Gateway Settings Section:

- **Listening Interface**: Leave the default.
- **Gateway Address**: Input the public IP of the Azure VPN gateway noted earlier.
- **Local ID**: IP Address.
- **Remote ID**: IP Address.
- **Local ID**: Enter the public IP of the on-premises Sophos XG Firewall.
- **Remote ID**: Input the public IP of the Azure VPN gateway that you noted earlier.
- **Local Subnet**: Enter the local subnet of 10.0.0.0 /16 (255.255.0.0)



- **Remote Subnet**: Enter the remote subnet 172.17.0.0 /16 (255.255.0.0)



- [ ] 14. **Advanced**: leave the default settings.
- [ ] 15. Upon clicking **Save**, the IPsec connection is activated.

Task 5: Creating Azure connection.

> In this task you will create a connection on your Azure Gateway to the On-Prem firewall and establish the connection.

- [ ] 1. Click on **Resource Groups** on the **Hub Menu**.
- [ ] 2. Select the **S2S_RG-XDSTSGT1RP** Resource Group.
- [ ] 3. Select your **S2S-GW** Gateway.
- [ ] 4. Click **Connections** from the S2S-GW menu.
- [ ] 5. Click **Add**.
- [ ] 6. Enter the following information in the **Add connection** blade.
    - **Name:** GWConnection
    - **Connection type:** Site-to-site (IPSec)
    - **Virtual Network Gateway:** S2S-GW
- [ ] 7. Click the **Local network gateway**
- [ ] 8. Click **Create new**.
- [ ] 9. Enter the following information in the **Create local network gateway** blade:
    - **Name:** OnPremGW
    - **IP address:** *Enter your IP address of your Sophos on prem firewall you recorded earlier*
    - **Address space:** 10.0.0.0/16

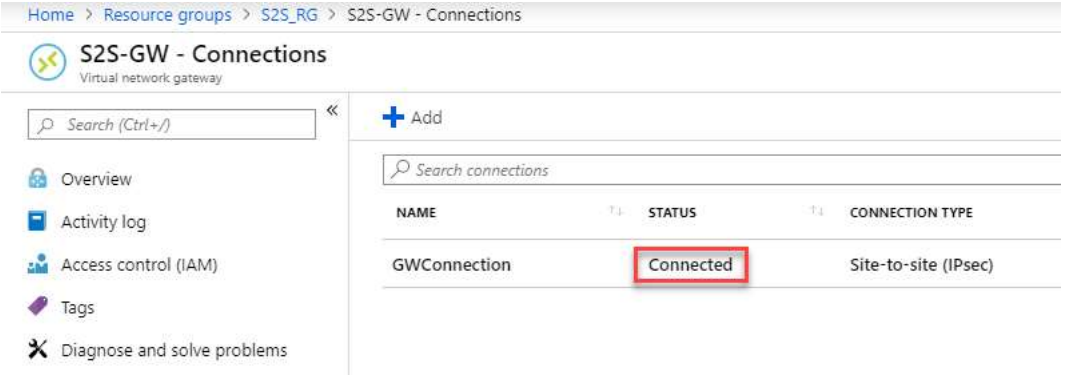
    > **Note**: This is the IP range of your On-Prem servers

- [ ] 10. Click **OK**.
- [ ] 11. In the **Shared key (PSK)** box enter 123456789 then click **OK**.

    > **Note:** This key is just for this lab. In the real world you would use something with greater complexity.

- [ ] 12. Refresh the page and the connection should be established.

    > **Note:** It may take 30 seconds to establish the connection.



✓ **Congratulations**! You have now completed this lab. You can safely end your lab.