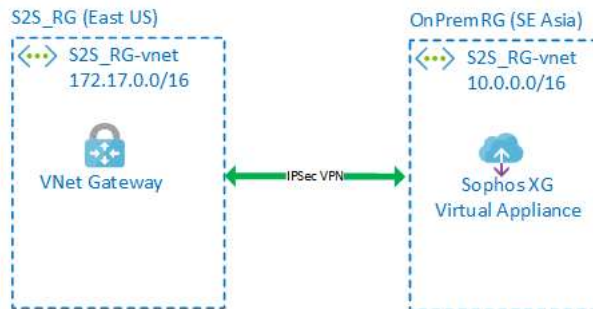


## Module 3 - Lab 2: On-Prem to Azure Connections (Optional) - Site-to-Site VPN Connections

### 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 diagram 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](mailto: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-redundant
  - **Enable active-active mode:** Disabled
  - **Configure BGP:** Disabled

## 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 \*

Resource group ⓘ

### Instance details

Name \*  ✓

Region \*

Gateway type \* ⓘ ☒ VPN ☐ ExpressRoute

VPN type \* ⓘ ☒ Route-based ☐ Policy-based

SKU \* ⓘ

Generation ⓘ

Virtual network \* ⓘ  [Create virtual network](#)

Subnet ⓘ

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

- ☐ 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.

**OnPremRG**  
Resource group

Search (Ctrl+/)

Overview  
Activity log  
Access control (IAM)  
Tags  
Events

Settings  
Quickstart  
Resource costs  
Deployments  
Policies  
Properties  
Locks  
Export template

Monitoring  
Insights (preview)  
Alerts

Subscription (change)  
Azure Pass - Sponsorship  
Subscription ID  
f155263b-b8c7-4a72-965a-930e06f2a5fe  
Tags (change)  
Click here to add tags

Deployments  
9 Succeeded

Filter by name... All types All locations No grouping

1 of 8 items selected Show hidden types

NAME	TYPE	LOCATION
AvailabilitySet	Availability set	Southeast Asia
myOnPremFW	Virtual machine	Southeast Asia
myonpremstorage	Storage account	Southeast Asia
PortA	Network interface	Southeast Asia
PortB	Network interface	Southeast Asia
PublicIP	Public IP address	Southeast Asia
SecurityGroup	Network security group	Southeast Asia
VNET	Virtual network	Southeast Asia

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

**PublicIP**  
Public IP address

Search (Ctrl+/)

Overview  
Activity log  
Access control (IAM)  
Tags

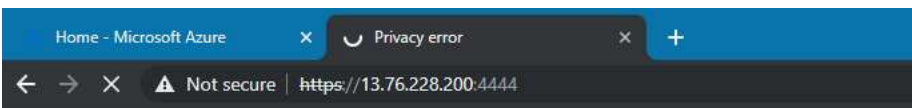
Settings  
Configuration  
Properties  
Locks

Associate Dissociate Move Delete Refresh

Resource group (change)  
OnPremRG  
Location  
Southeast Asia  
Subscription (change)  
Azure Pass - Sponsorship  
Subscription ID  
f155263b-b8c7-4a72-965a-930e06f2a5fe  
Tags (change)  
Click here to add tags

SKU  
Basic  
IP address  
13.76.228.200  
DNS name  
myonpremgw.southeastasia.cloudapp.azure.com  
Associated to  
PortB  
Virtual machine  
myOnPremFW

- ☐ 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.



## Your connection is not private

Attackers might be trying to steal your information (passwords, messages, or credit cards). [Learn more](#)



NET::ERR\_CERT\_AUTHORITY\_INVALID



Hide advanced

This server could not prove that it is **13.76.228.20** your computer's operating system. This may be caused by an attacker intercepting your connection.

[Proceed to 13.76.228.200 \(unsafe\)](#)

- ☐ 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 serial number (start a trial)** and select **I do not want to register now** then click **Continue**.



## Register your firewall

Every firewall must have a serial number. We can get one for you automatically. Alternatively, if you have an unused serial number, you can specify it here.

☐ I have an existing serial number

Once you register the firewall, you cannot change the serial number. If you have more than one serial number, make sure that you choose the correct one. **Home users** must use an XG Home. Use serial number obtained from [here](#)

☐ I don't have a serial number (start a trial).

You will automatically receive a serial number and a 30-day trial period. During this period, you can test the full functionality of Sophos XG Firewall. **Do not use this option for home use.**

☐ I would like to migrate my UTM 9 license now

You will receive a serial number automatically. Your equivalent UTM 9 license will be converted and applied to the XG Firewall.

This is not reversible. If you are not sure about migrating now, click "Start a trial". You can migrate the license after you test XG Firewall.

☒ I do not want to register now

You can skip registration for now. A reminder to register will appear during your next login. You can continue without registration for another 30 days.

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 appliance to via IPsec VPN.

**S2S-GW-PIP**  
Public IP address

Overview

Activity log

Access control (IAM)

Tags

Settings

Configuration

Associate Dissociate Move Delete Refresh

Resource group (change)  
S2S\_RG

Location  
East US

Subscription (change)  
Azure Pass - Sponsorship

Subscription ID  
f155263b-b8c7-4a72-965a-930e06f2a5fe

SKU  
Basic

IP address  
40.85.178.89

DNS name  
-

Associated to  
S2S-GW

Virtual machine  
-

- ☐ 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.

## General settings

Name <input type="text" value="On_Prem_to_Azure"/>	IP version <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	<input checked="" type="checkbox"/> Activate on save
Description <input type="text" value="Site to Site connection from On Prem to Azure VNet"/>	Connection type <input type="text" value="Site-to-site"/>	<input checked="" type="checkbox"/> Create firewall rule
	Gateway type <input type="text" value="Respond only"/>	

### Encryption Section:

- **Policy:** Microsoft Azure.
- **Authentication Type:** Preshared Key.
- **Preshared Key:** [123456789](#)
- **Repeat Preshared Key:** [123456789](#)

## Encryption

Policy <input type="text" value="Microsoft Azure"/>	Authentication type <input type="text" value="Preshared key"/>
	Preshared key <input type="text" value="....."/>
	Repeat preshared key <input type="text" value="....."/>

### 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](#)

**Add IP host**

Name *	<input type="text" value="On Prem"/>		
IP version *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6		
Type *	<input type="radio"/> IP <input checked="" type="radio"/> Network <input type="radio"/> IP range <input type="radio"/> IP list		
IP address *	<input type="text" value="10.0.0.0"/>	Subnet	<input type="text" value="/16 [255.255.0.0]"/>
IP host group	<div><input type="text"/></div> <div>Add new item</div>		

**Save** **Cancel**

- **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.

## S2S-GW - Connections

Virtual network gateway

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

+ Add

Search connections

NAME	STATUS	CONNECTION TYPE
GWConnection	Connected	Site-to-site (IPsec)

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