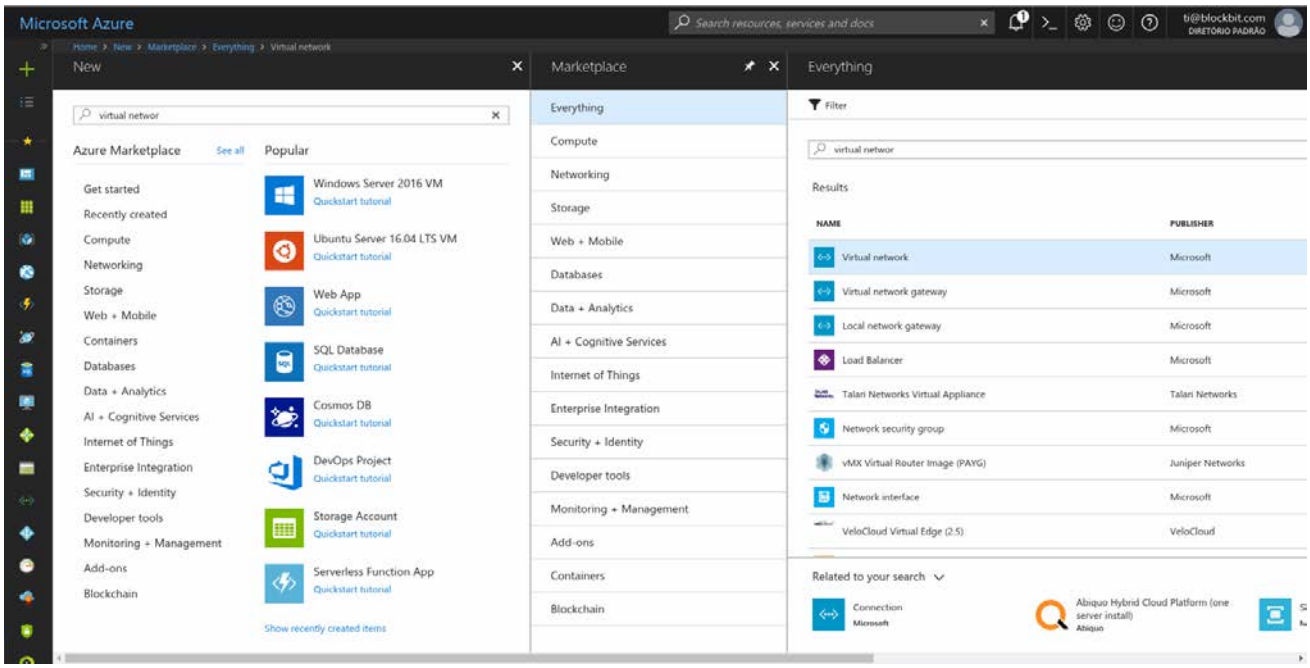
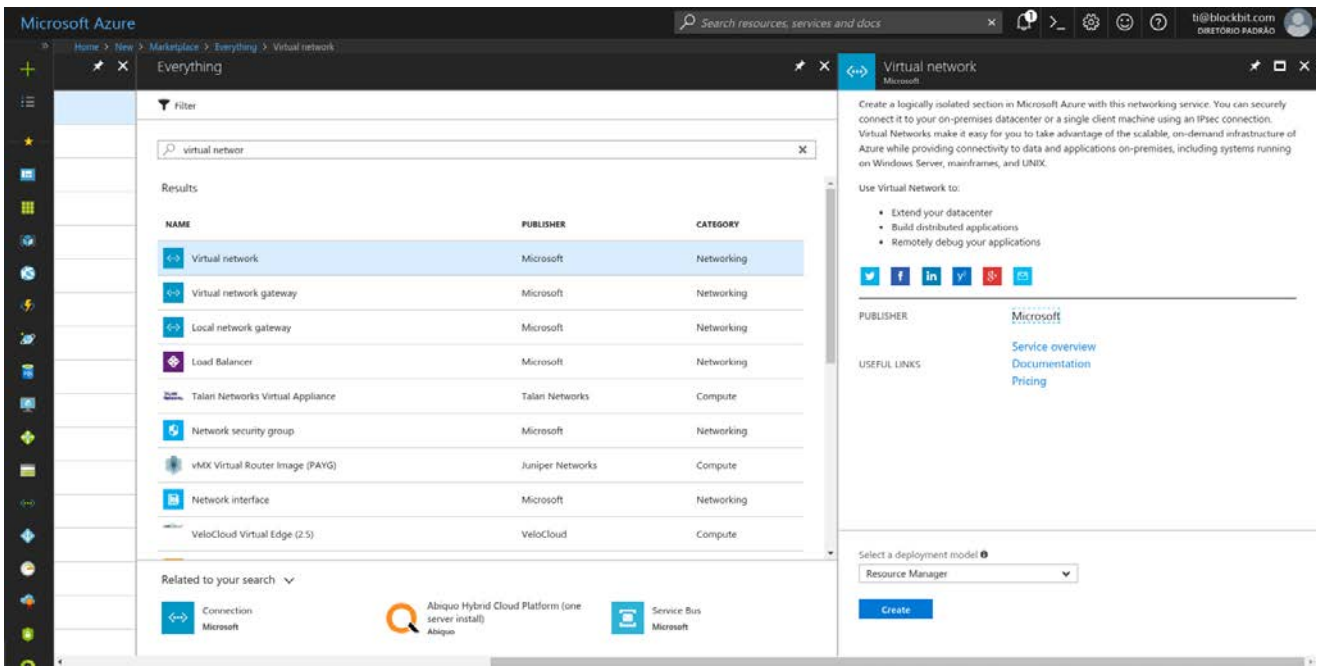
1 Setting Up Microsoft Azure virtual network

Log in to Azure Portal and click on "New (+)".

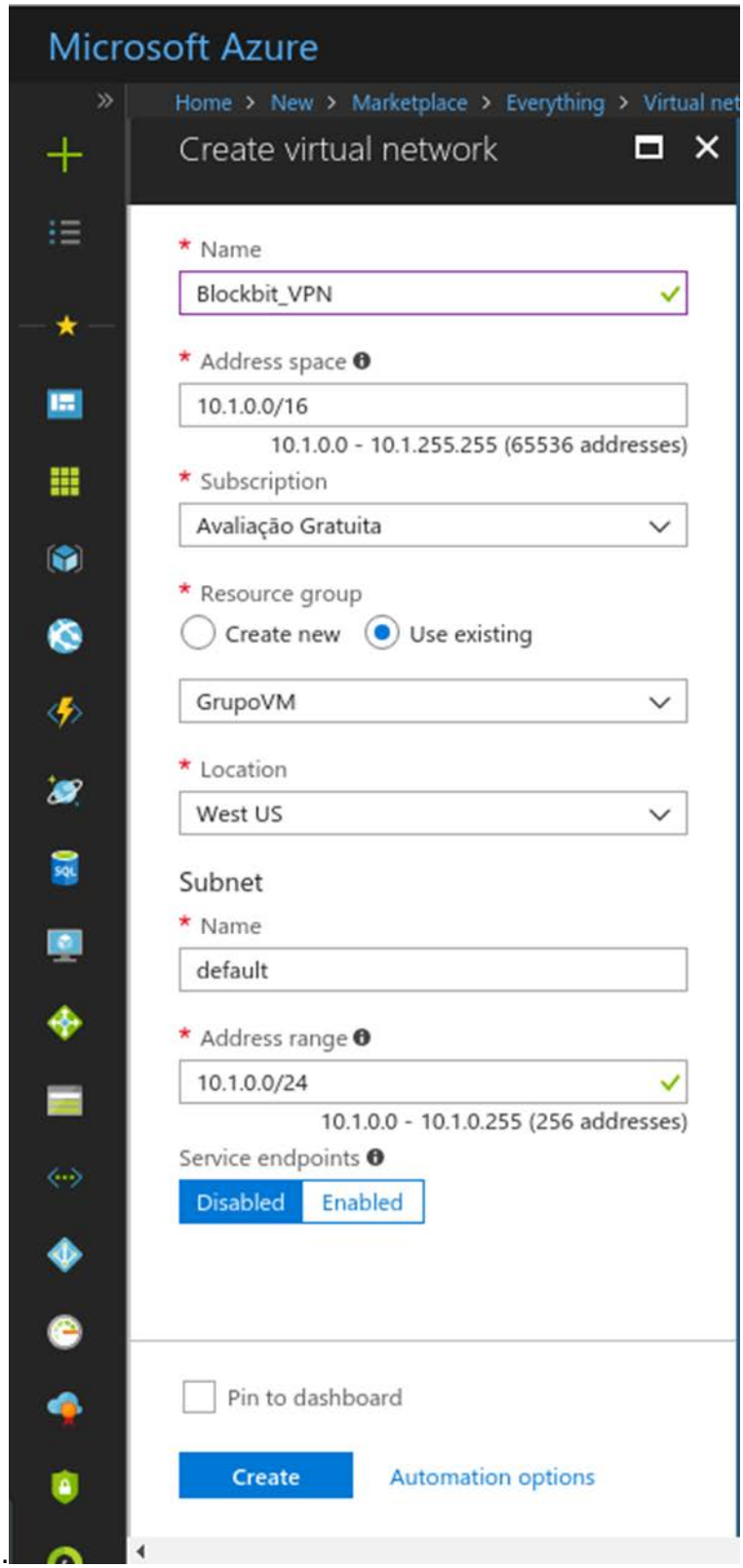
Then, in the Marketplace search field, type and select **“Virtual Network”.**



Click in the button **“Virtual Network”**. Select the option "Resource Manager", available on the list *"Select a deployment model list"*.

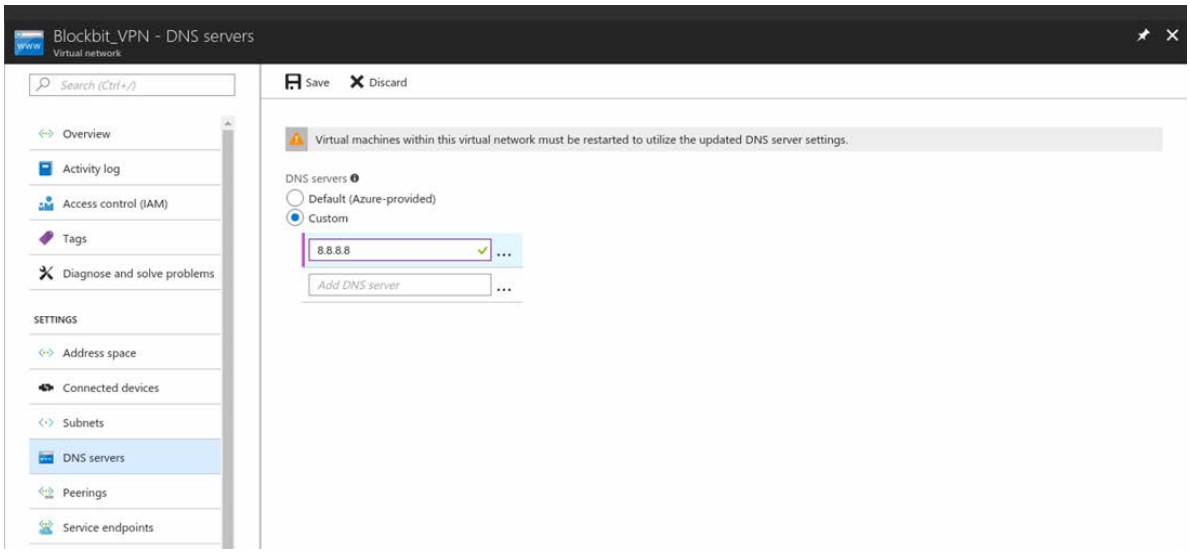


On the page "Create virtual network", set the requested values, as shown in the image below.



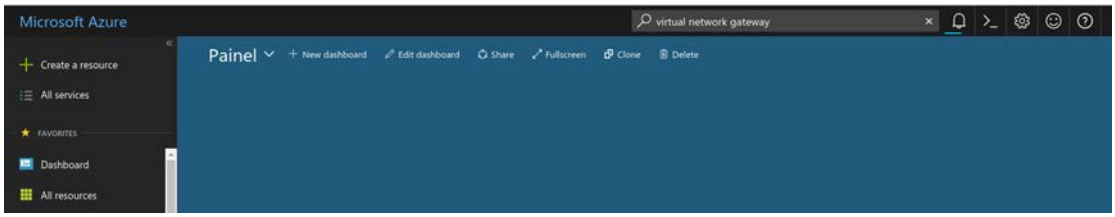
1.1 Specify a DNS server

Open the *virtual network* you've created and click on "**DNS".** Select the option *Custom* and then click the "save" button.



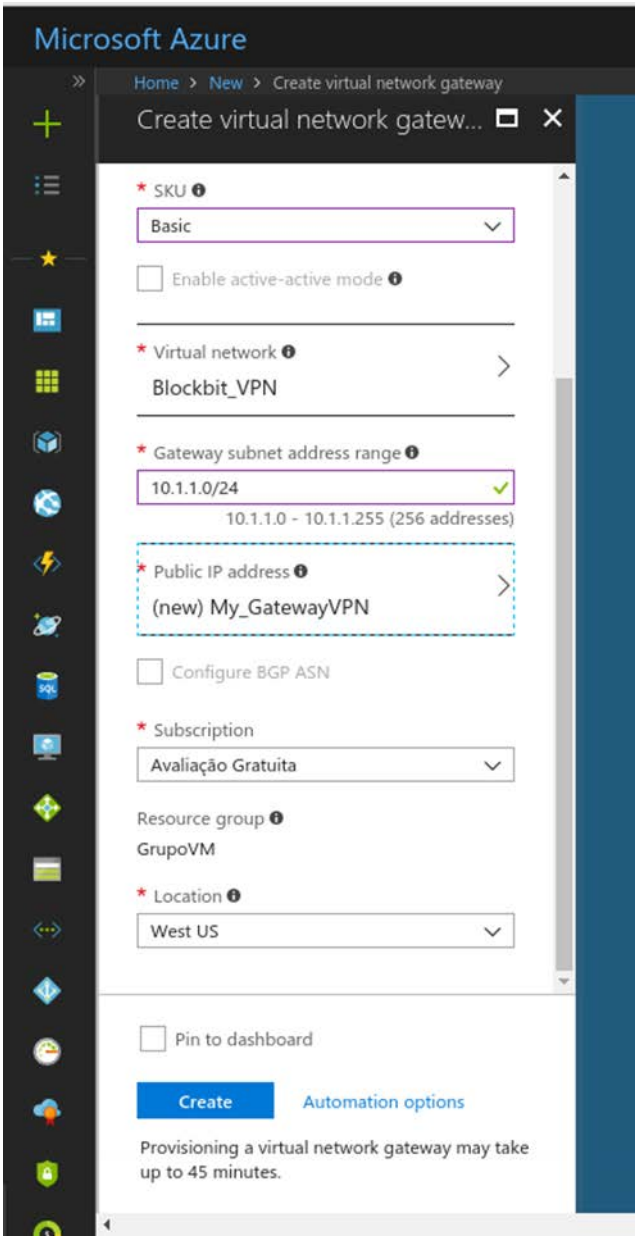
1.2 Creating the Virtual Network Gateway on Microsoft Azure

On the dashboard, click on New.

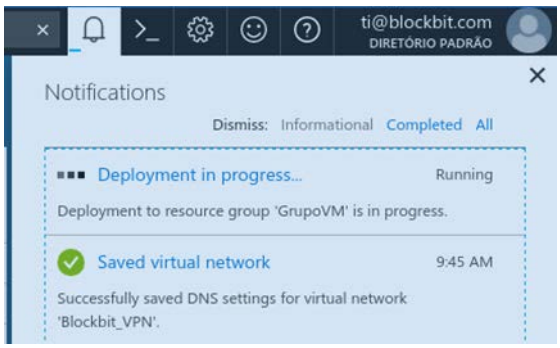


In the search box, search for Network Virtual Gateway. Then, select Create virtual network gateway.

If necessary, create a "Public IP address" by clicking on the button "Create".

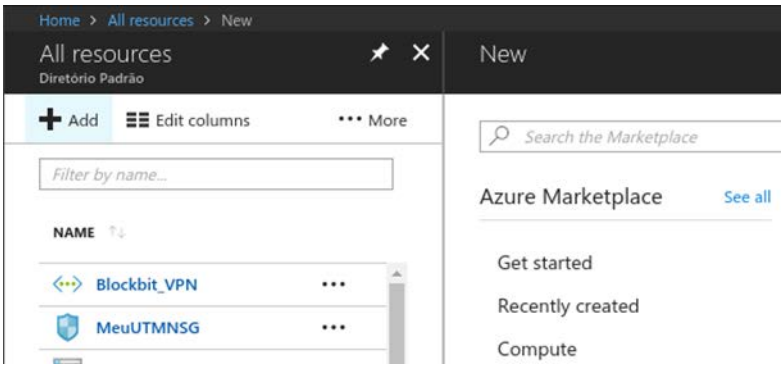


You can track any activity by using the notification button:

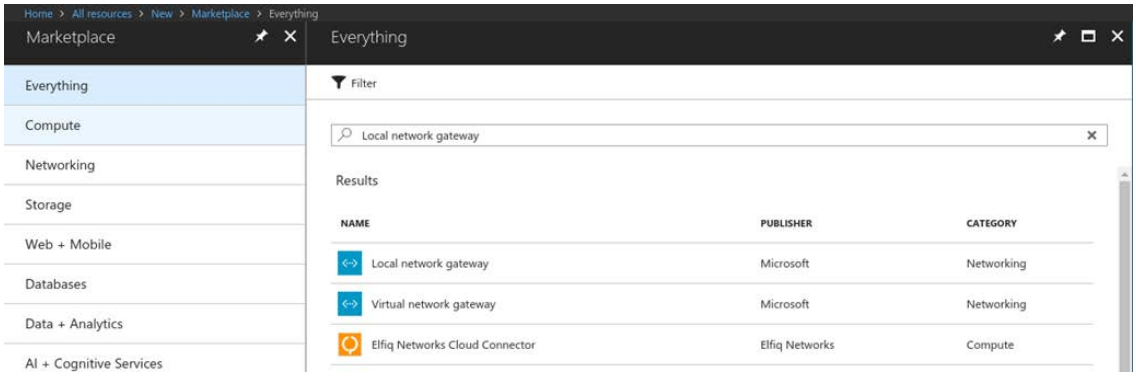


1.3 Creating a gateway for Microsoft Azure's local network

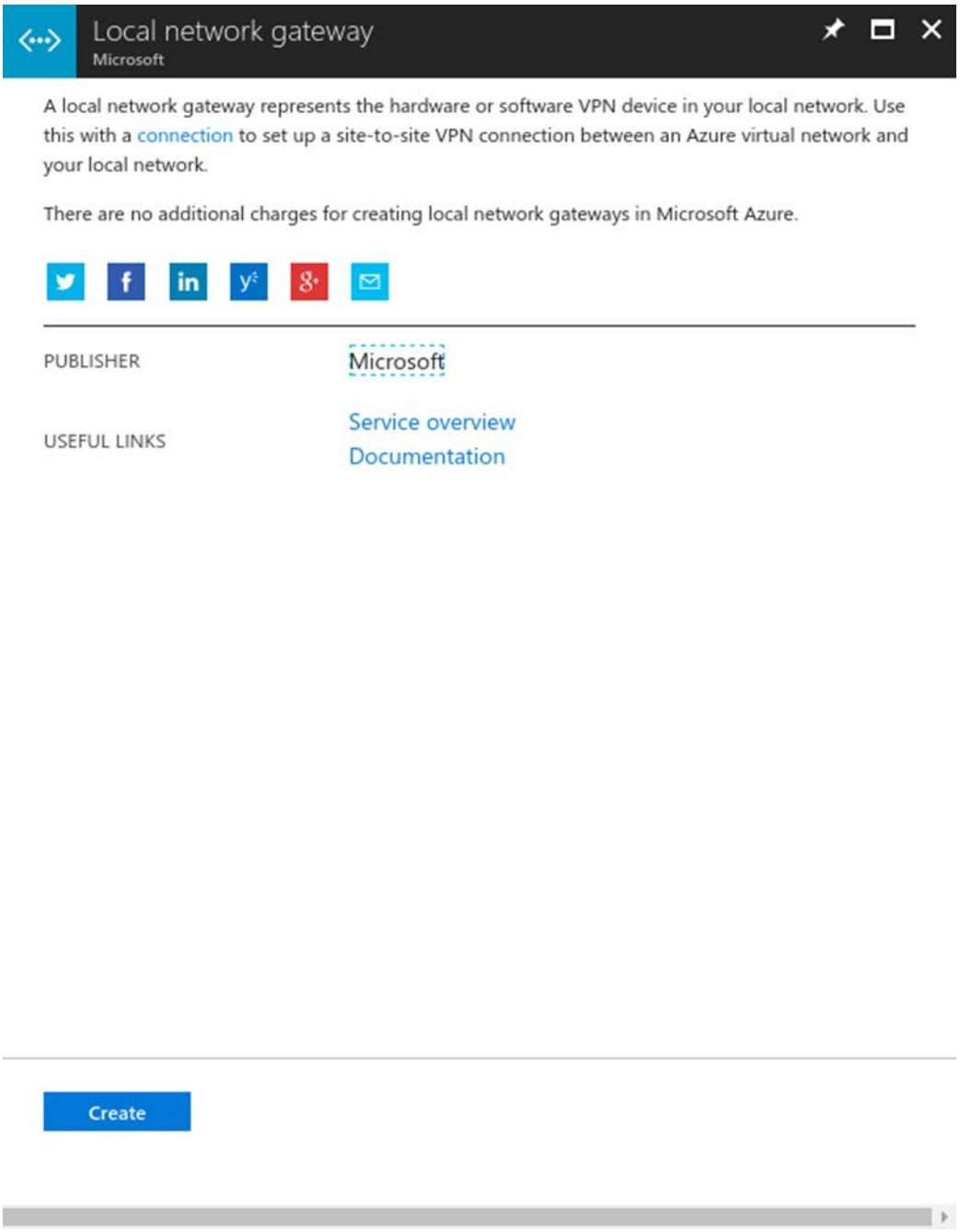
On the dashboard, select **"All resources"**. ***Click*** **"+Add"** and select **"see all".**



On the tab ***"Everything"****, search for and click on* ***"Local Network gateway"****.*



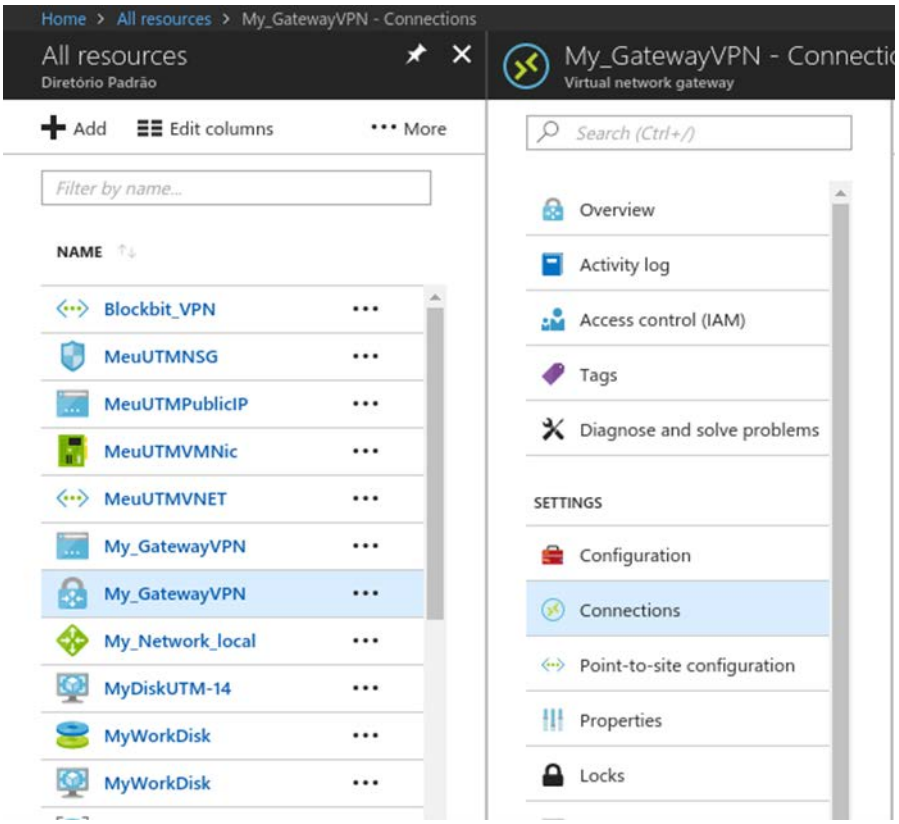
Click **"Create"**



1.4 Creating Site-to-Site VPN Connection on Microsoft Azure

In the Azure portal, find your *virtual network gateway.*

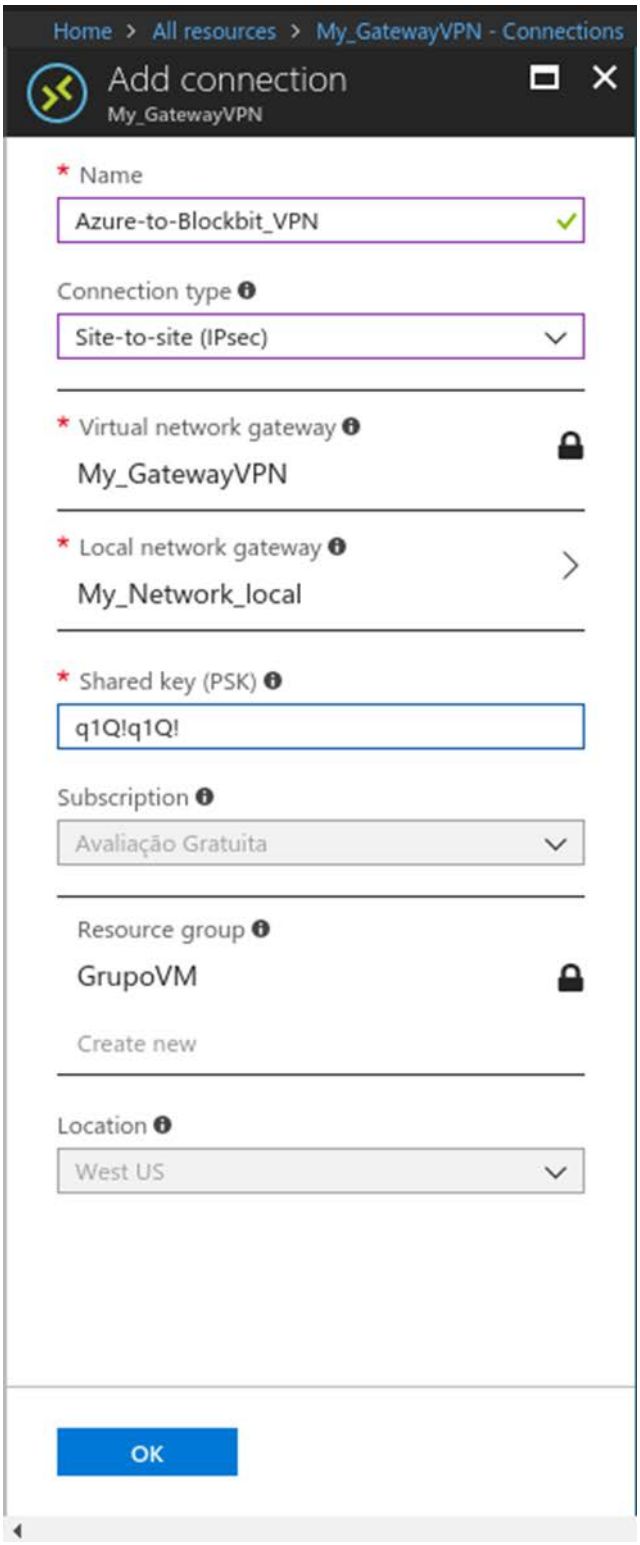
On the settings tab, click "Connections", then "Add" to add a new connection.



Set the values of your connection.

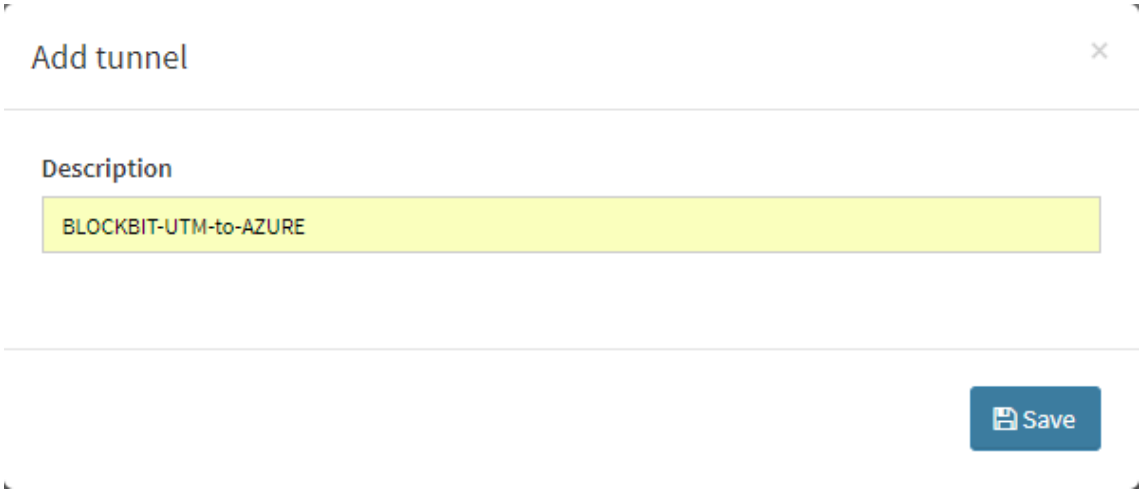
Check the Shared Key (PSK), the same used on BLOCKBIT UTM

Click OK.



1.5 Configuring Site-to-Site tunnel in BOCKBIT UTM

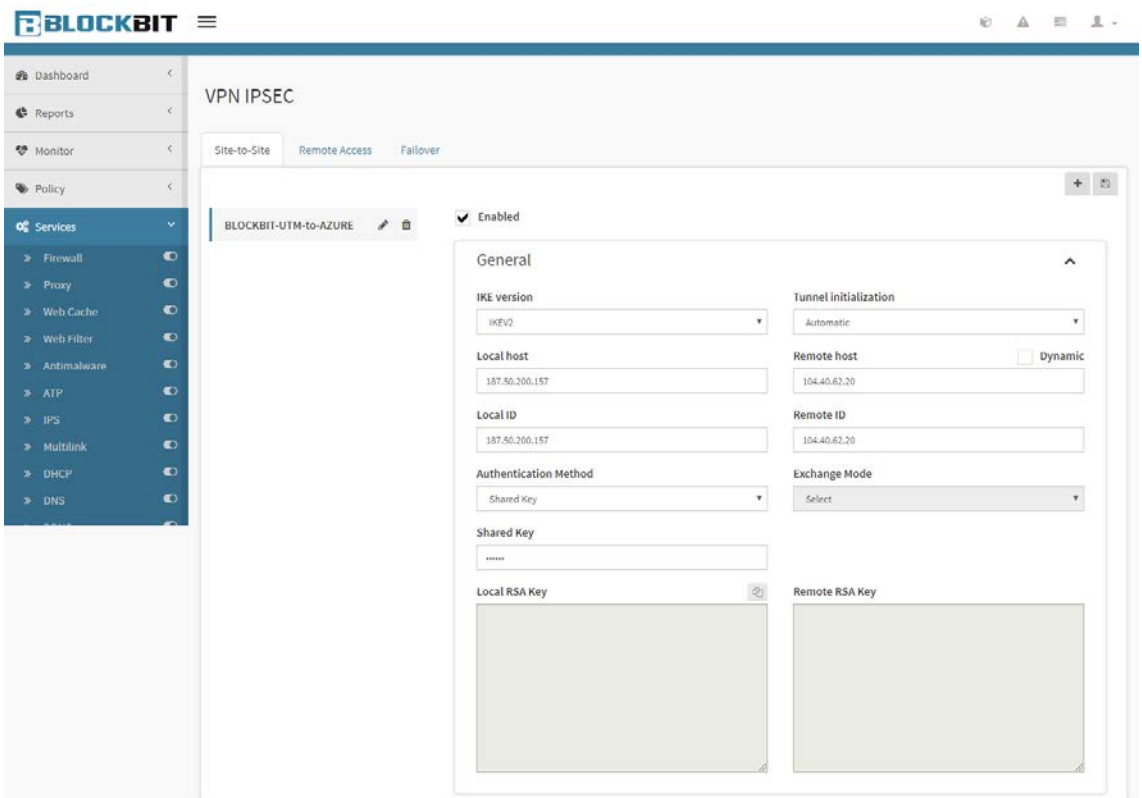
Go to **[Services] >> [VPN IPSEC]**. In the tab *Site-to-Site*, click on the button [**+**] para add a new tunnel.



Enter the **"***Host Local***"** (*Public IP address* UTM) and *Host Remote (Azure Remote).*

Set the fields as shown below:

General



IKE version: Ex.: ikev2

Local host: Ex.: 187.50.200.157

Local ID: Ex.: 187.50.200.157

Authentication Method: Ex.: Shared Key

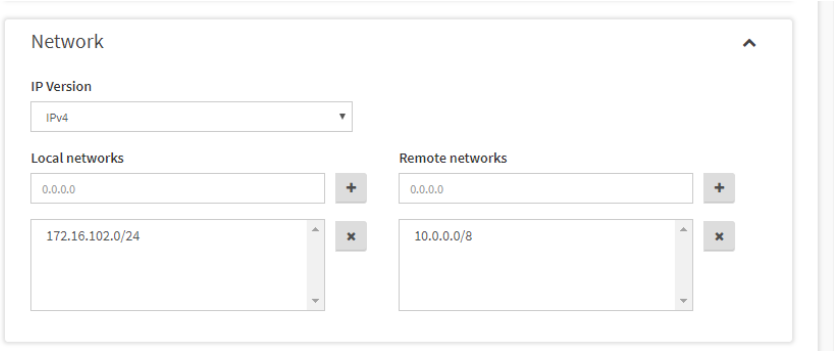
Shared Key: Ex.: 123456

Tunnel initialization: Ex.: Automatic

Remote host: Ex.: 104.40.62.20

Remote ID: Ex.: 104.40.62.20

Network

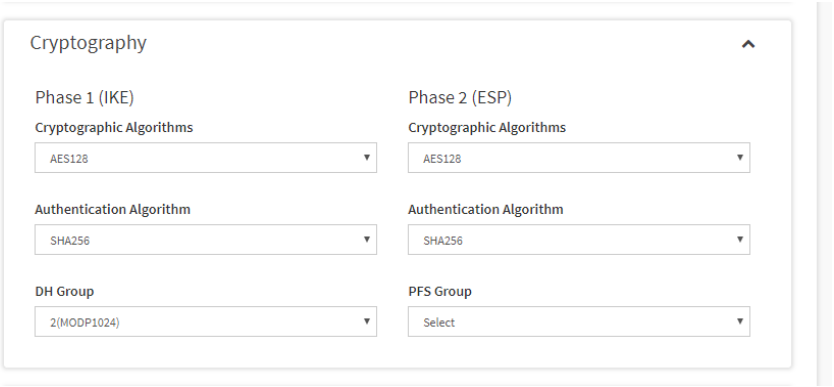


IP Version: Ex.: IPv4

Local network: Ex.: 172.16.102.0/24

Remote networks: Ex.: 10.0.0.0/16

Cryptography



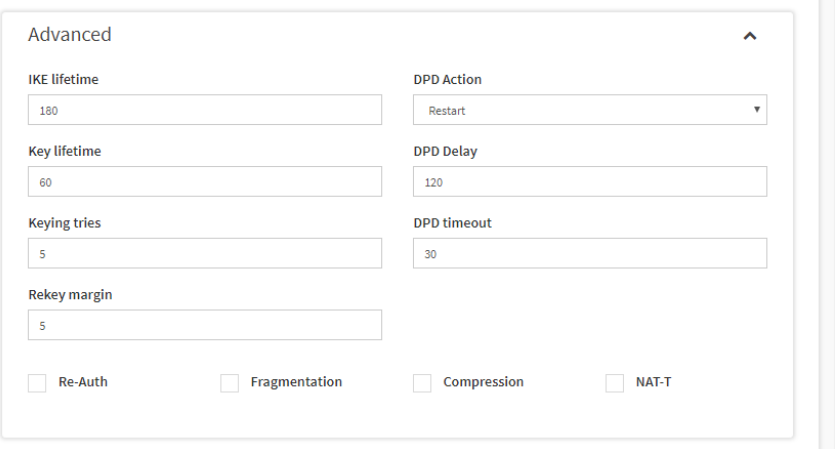
Phase1 (IKE)

- **Criptographic Algoriyhms:** Ex.: AES256
- **Authentication Algorithm:** Ex.: SH256
- **DH Group:** Ex.: 2(MODP1024)

Phase2 (ESP)

- **Criptographic Algoriyhms:** Ex.: AES256
- **Authentication Algorithm:** Ex.: SH256

Advanced



IKE lifetime: Ex.: 86600

Key lifetime: Ex.: 28800

Keying tries: Ex.: 5

Rekey margin: Ex.: 5

DPD Action: Ex.: Restart

DPD Delay: Ex.: 120

DPD timeout: Ex.: 30

Go to BLOCKBIT UTM. On **[Monitor] >> [IPsec Connections]** you can confirm the established VPN tunnel connection.

View connection status: