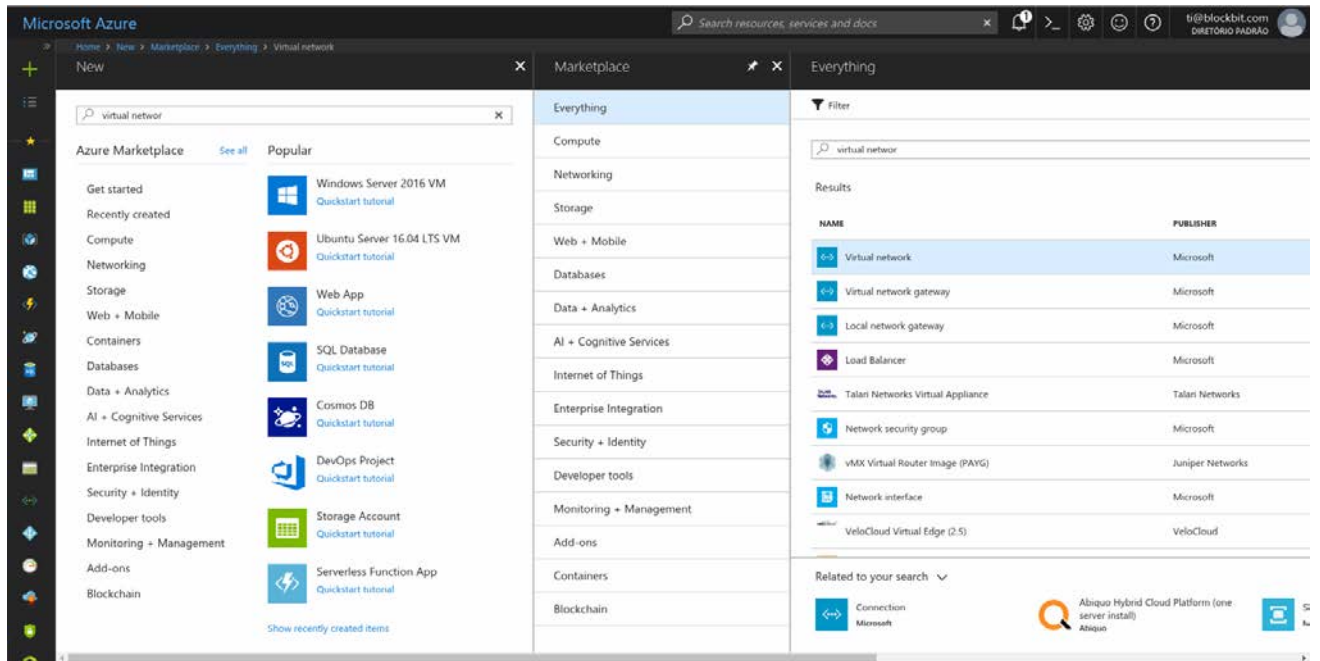


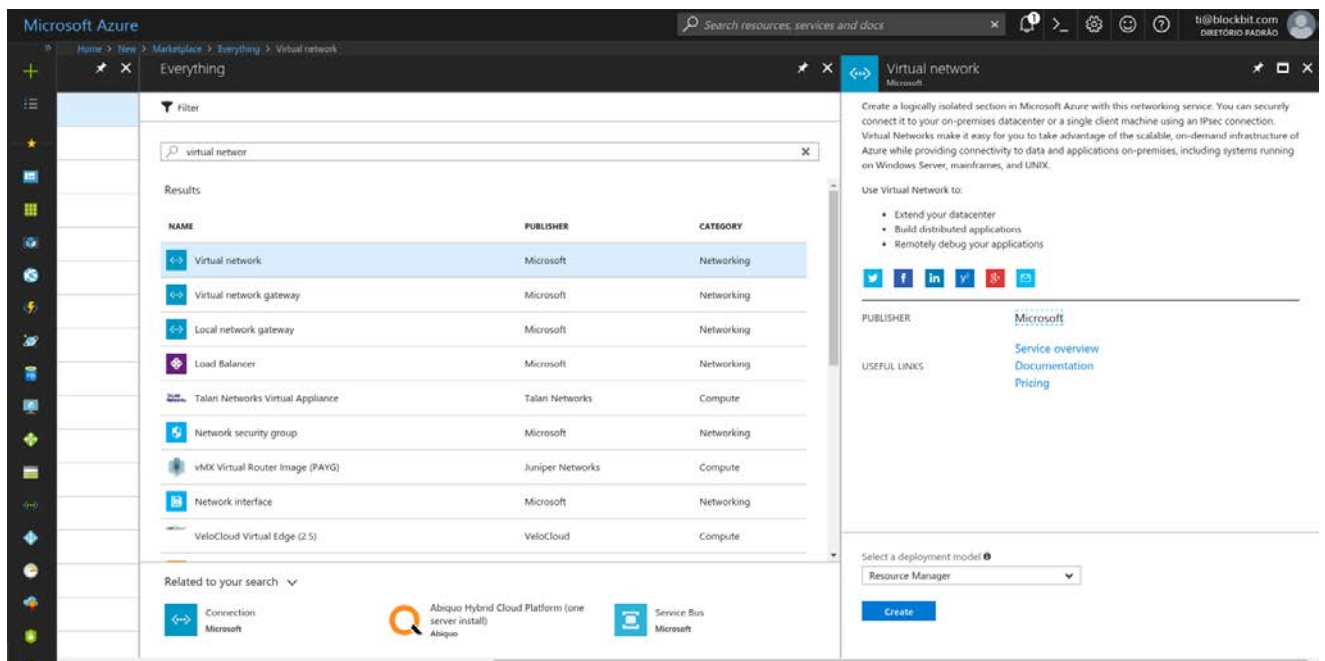
1 Setting Up Microsoft Azure virtual network

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.

Microsoft Azure

Home > New > Marketplace > Everything > Virtual network

Create virtual network

* Name
Blockbit_VPN ✓

* Address space ⓘ
10.1.0.0/16
10.1.0.0 - 10.1.255.255 (65536 addresses)

* Subscription
Avaliação Gratuita ▾

* Resource group
 Create new Use existing

GrupoVM ▾

* Location
West US ▾

Subnet

* Name
default

* Address range ⓘ
10.1.0.0/24 ✓
10.1.0.0 - 10.1.0.255 (256 addresses)

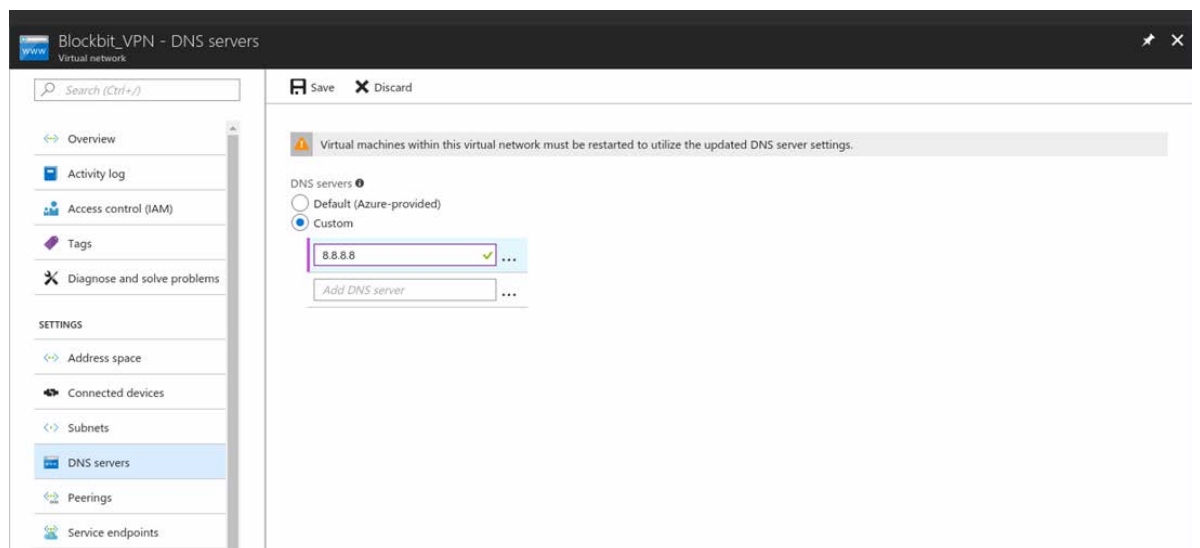
Service endpoints ⓘ
 Disabled Enabled

Pin to dashboard

[Create](#) [Automation options](#)

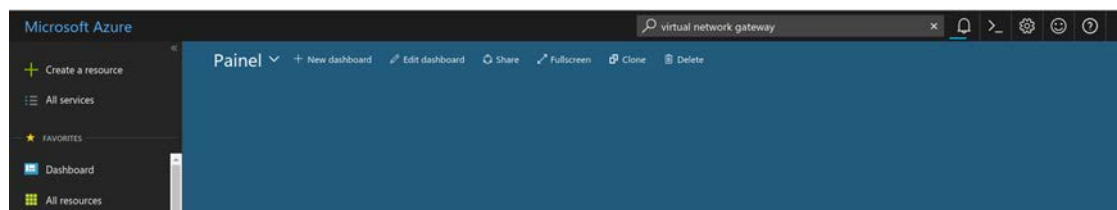
1.1 Specify a DNS server

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



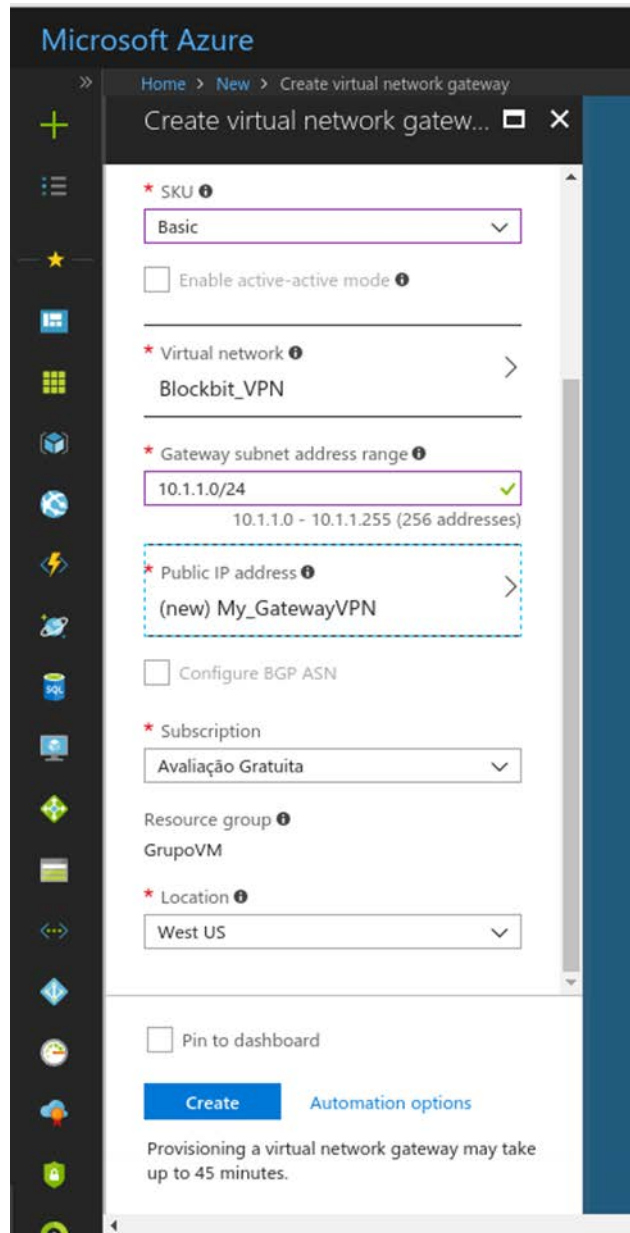
1.2 Creating the Virtual Network Gateway on Microsoft Azure

On the dashboard, click on New.

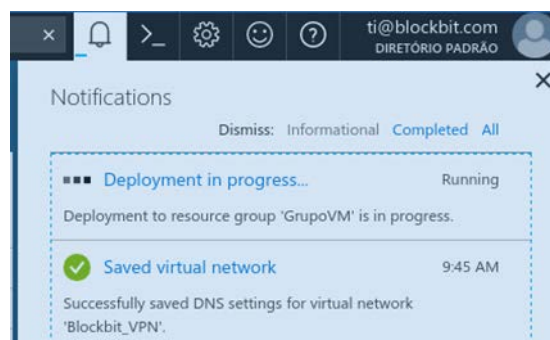


In the search box, search for Network Virtual Gateway. Then, select Create virtual network gateway.

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

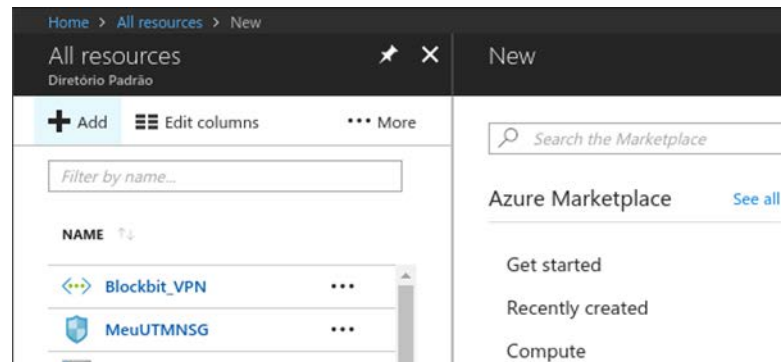


You can track any activity by using the notification button:

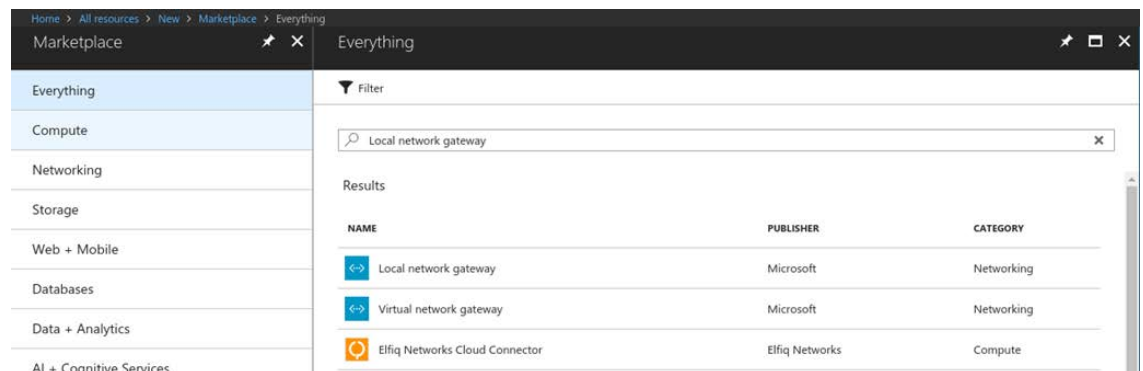


1.3 Creating a gateway for Microsoft Azure's local network

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”

Local network gateway
Microsoft

A local network gateway represents the hardware or software VPN device in your local network. Use this with a [connection](#) to set up a site-to-site VPN connection between an Azure virtual network and your local network.

There are no additional charges for creating local network gateways in Microsoft Azure.

[Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#) [Google+](#) [Email](#)

PUBLISHER [Microsoft](#)

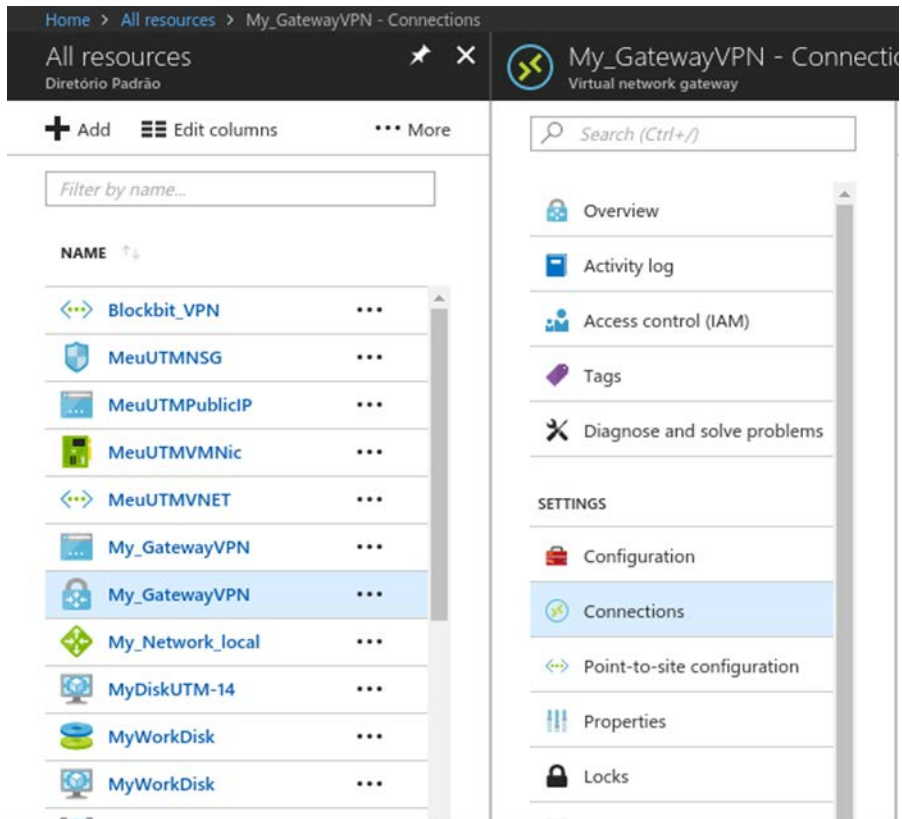
USEFUL LINKS [Service overview](#)
[Documentation](#)

[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.

Home > All resources > My_GatewayVPN - Connections

 Add connection My_GatewayVPN

* Name
Azure-to-Blockbit_VPN ✓


Connection type ⓘ
Site-to-site (IPsec) ▾

* Virtual network gateway ⓘ 
My_GatewayVPN

* Local network gateway ⓘ >
My_Network_local

* Shared key (PSK) ⓘ
q1Q!q1Q!

Subscription ⓘ
Avaliação Gratuita ▾

Resource group ⓘ 
GrupoVM
Create new

Location ⓘ
West US ▾

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.

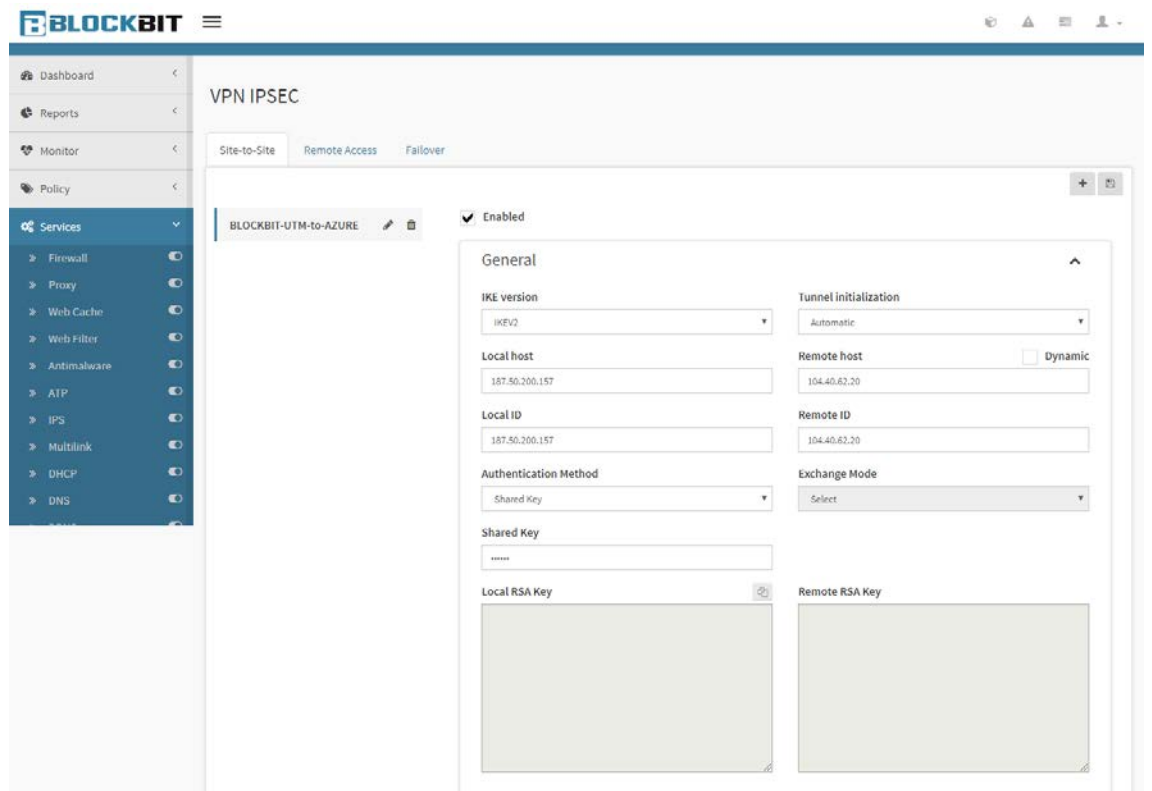


The screenshot shows a dialog box titled "Add tunnel" with a close button (X) in the top right corner. Below the title is a section labeled "Description" containing a yellow text box with the text "BLOCKBIT-UTM-to-AZURE". At the bottom right of the dialog is a blue button with a floppy disk icon and the text "Save".

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

Set the fields as shown below:

General



The screenshot displays the VPN IPSEC configuration interface. The left sidebar shows the "Services" menu with various options like Firewall, Proxy, Web Cache, etc. The main area is titled "VPN IPSEC" and has tabs for "Site-to-Site", "Remote Access", and "Failover". The "Site-to-Site" tab is active, showing a tunnel named "BLOCKBIT-UTM-to-AZURE" which is "Enabled". The "General" configuration section is expanded, showing the following fields:

- IKE version:** IKEv2
- Tunnel initialization:** Automatic
- Local host:** 187.50.200.157
- Remote host:** 104.40.62.20 (with a "Dynamic" checkbox)
- Local ID:** 187.50.200.157
- Remote ID:** 104.40.62.20
- Authentication Method:** Shared Key
- Exchange Mode:** Select
- Shared Key:** (empty field)
- Local RSA Key:** (empty text area)
- Remote RSA Key:** (empty text area)

IKE version: Ex.: ikev2

Local host: Ex.: 187.50.200.157

Local ID: Ex.: 187.50.200.157

Authentication Method: Ex.: Shared Key

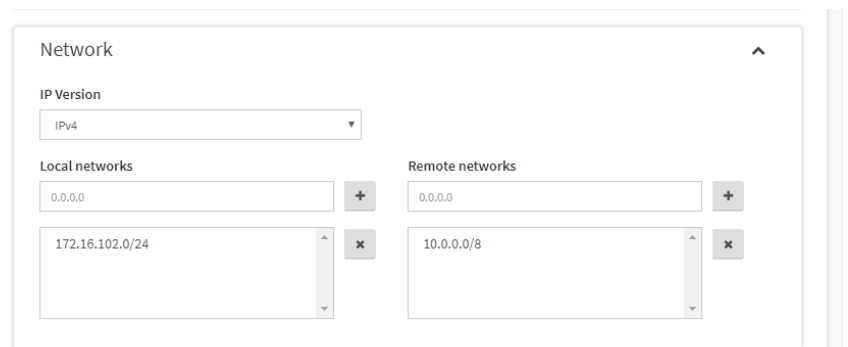
Shared Key: Ex.: 123456

Tunnel initialization: Ex.: Automatic

Remote host: Ex.: 104.40.62.20

Remote ID: Ex.: 104.40.62.20

Network



The screenshot shows a 'Network' configuration window. At the top, there is a title bar with the text 'Network' and a small upward-pointing arrow on the right. Below the title bar, there is a section for 'IP Version' with a dropdown menu currently set to 'IPv4'. Underneath, there are two columns: 'Local networks' and 'Remote networks'. Each column has a text input field at the top with a '+' button to its right. Below each input field is a list box containing one or more entries, with an 'x' button to its right. In the 'Local networks' list, the entry '172.16.102.0/24' is visible. In the 'Remote networks' list, the entry '10.0.0.0/8' is visible. The '0.0.0.0' text is also present in the input fields of both columns.

IP Version: Ex.: IPv4

Local network: Ex.: 172.16.102.0/24

Remote networks: Ex.: 10.0.0.0/16

Cryptography

Cryptography

Phase 1 (IKE)	Phase 2 (ESP)
Cryptographic Algorithms AES128	Cryptographic Algorithms AES128
Authentication Algorithm SHA256	Authentication Algorithm SHA256
DH Group 2(MODP1024)	PFS Group Select

Phase1 (IKE)

- **Cryptographic Algorithms:** Ex.: AES256
- **Authentication Algorithm:** Ex.: SH256
- **DH Group:** Ex.: 2(MODP1024)

Phase2 (ESP)

- **Cryptographic Algorithms:** Ex.: AES256
- **Authentication Algorithm:** Ex.: SH256

Advanced

Advanced

IKE lifetime 180	DPD Action Restart
Key lifetime 60	DPD Delay 120
Keying tries 5	DPD timeout 30
Rekey margin 5	

Re-Auth Fragmentation Compression NAT-T

IKE lifetime: Ex.: 86600

Key lifetime: Ex.: 28800

Keying tries: Ex.: 5

Rekey margin: Ex.: 5

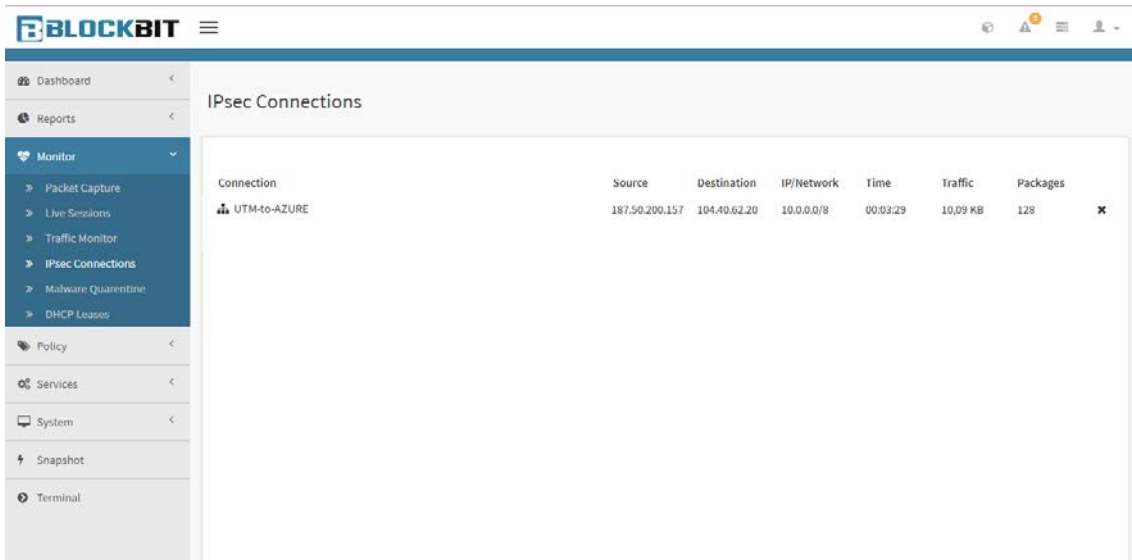
DPD Action: Ex.: Restart

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:



The screenshot shows the BLOCKBIT UTM web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Reports, Monitor (expanded), Policy, Services, System, Snapshot, and Terminal. The 'Monitor' section is expanded, showing sub-items: Packet Capture, Live Sessions, Traffic Monitor, IPsec Connections (selected), Malware Quarantine, and DHCP Leases. The main content area is titled 'IPsec Connections' and displays a table with the following data:

Connection	Source	Destination	IP/Network	Time	Traffic	Packages	
UTM-to-AZURE	187.50.200.157	104.40.62.20	10.0.0.0/8	00:03:29	10,09 KB	128	✕