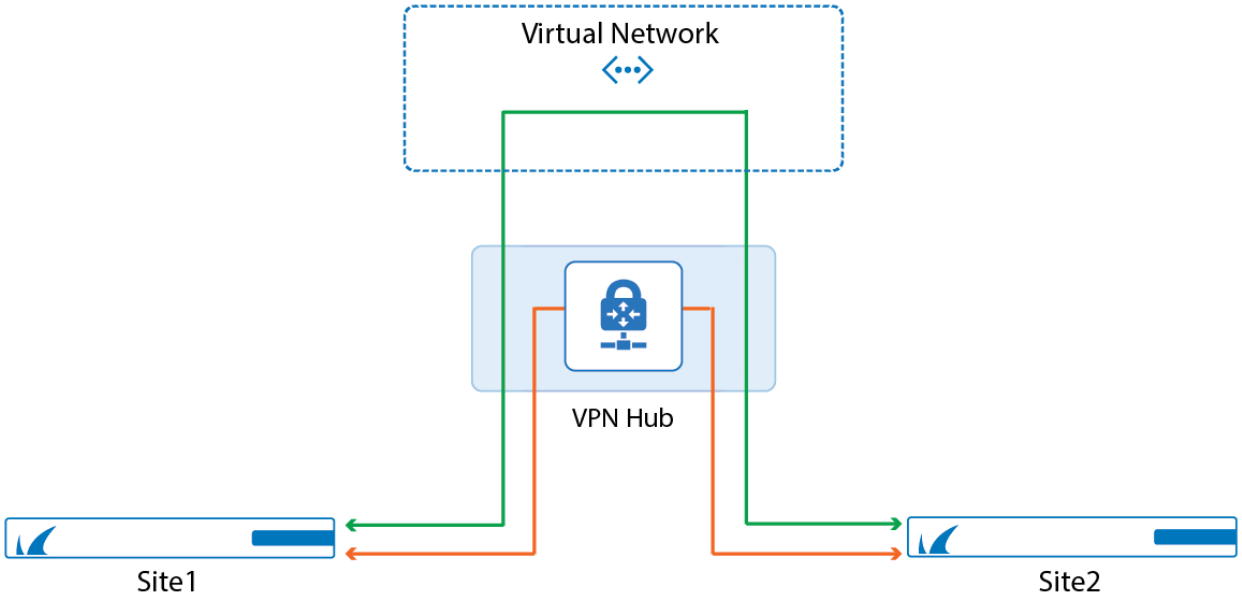
How to Configure Automatic Connectivity to Azure Virtual WAN

https://campus.barracuda.com/doc/78808340/

VPN connections from a CloudGen Firewall to the Azure Virtual WAN hub can be provisioned automatically. The automatic configuration provides a robust and redundant connection by introducing two active-active IPsec IKEv2 VPN tunnels with the corresponding BGP setup and fully automated Azure Virtual WAN site creation on Microsoft Azure. The finished deployment allows for both branch-to-branch and branch-to-cloud connections.



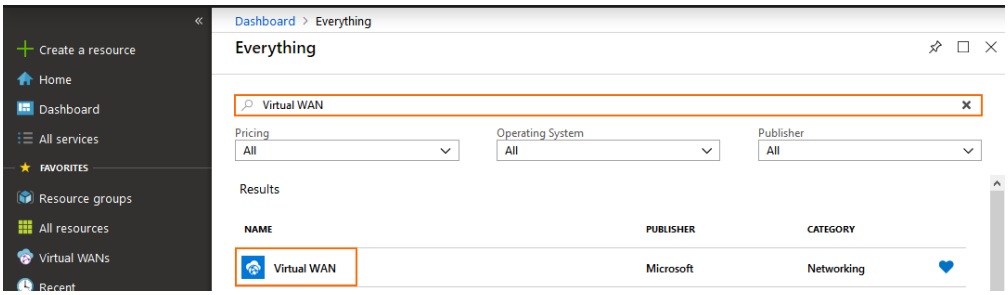
Before You Begin

- Create an Azure service principal to allow the firewall to authenticate to the Azure Virtual WAN APIs. For more information, see How to Create a Service Principal for Azure Virtual WAN.
- Configure direct attached routes to announce the local networks that should have access to cloud resources. For more information, see the **Advertise Route** setting in How to Configure Direct Attached Routes.

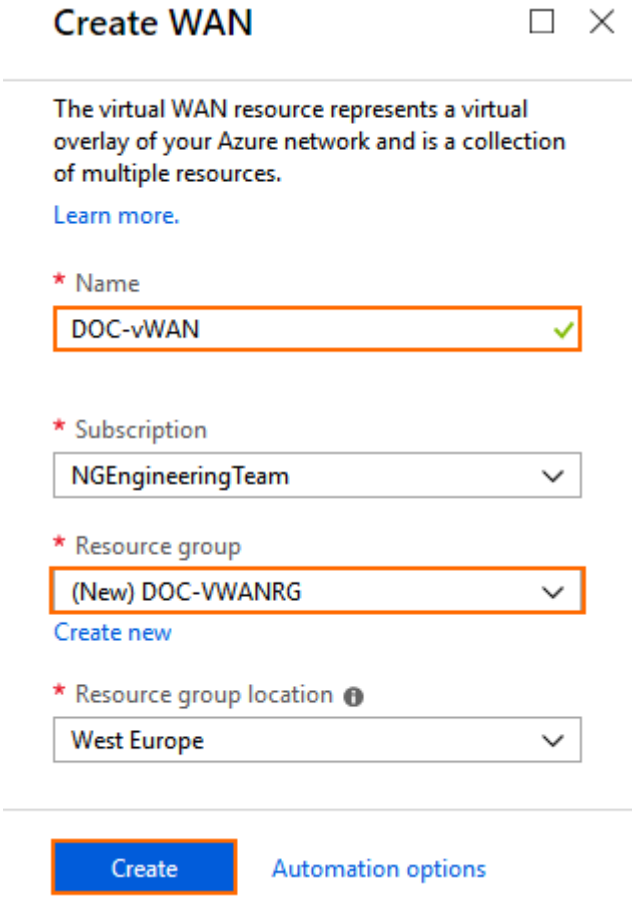
Step 1. Configure Microsoft Azure Virtual WAN Service

1. Log into the Azure portal: https://portal.azure.com
2. In the left menu, click **Create a resource** and search for **Virtual WAN**.

3. Click **Virtual WAN**.



4. In the next blade, click **Create**.
5. In the **Create WAN** blade, enter the Virtual WAN **Name** and select an existing **Resource Group** or create a new one.



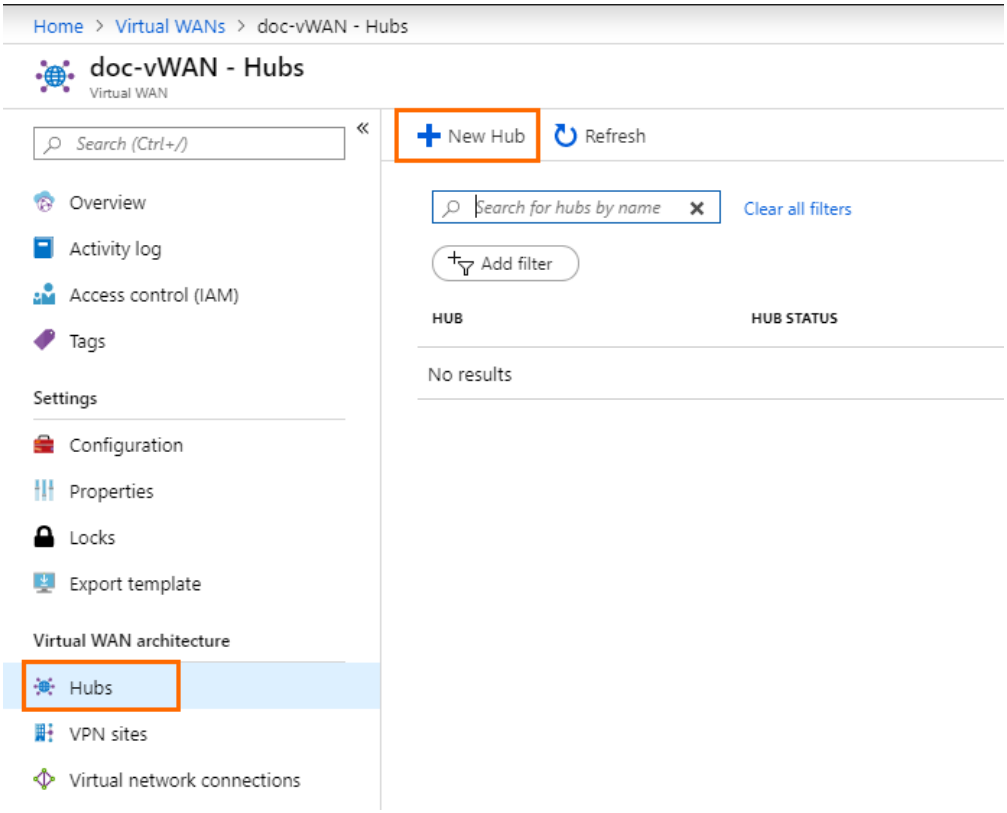
6. Click **Create** to finish Virtual WAN creation.

The CloudGen Firewall can now trigger the connection process to the Azure Virtual WAN.

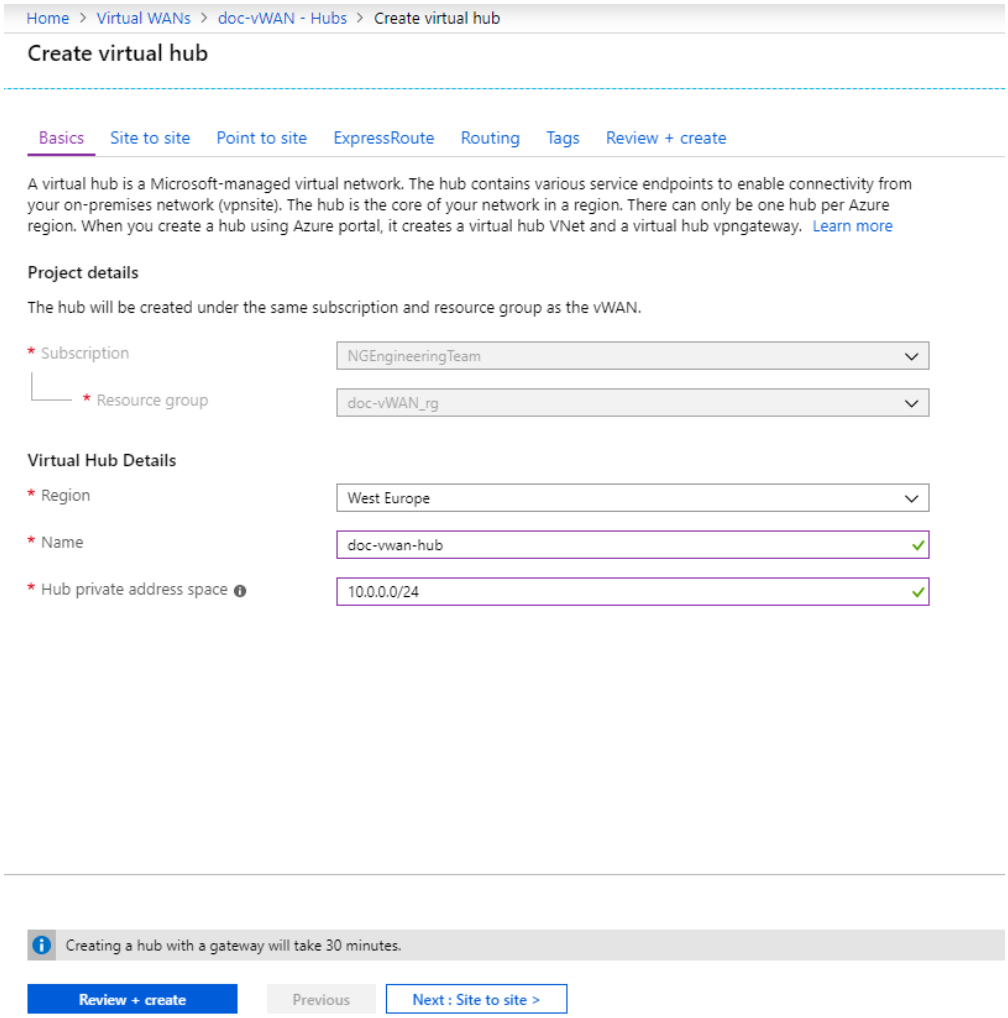
Step 2. Create a Hub in Your vWAN

Creating a hub takes up to 30 minutes.

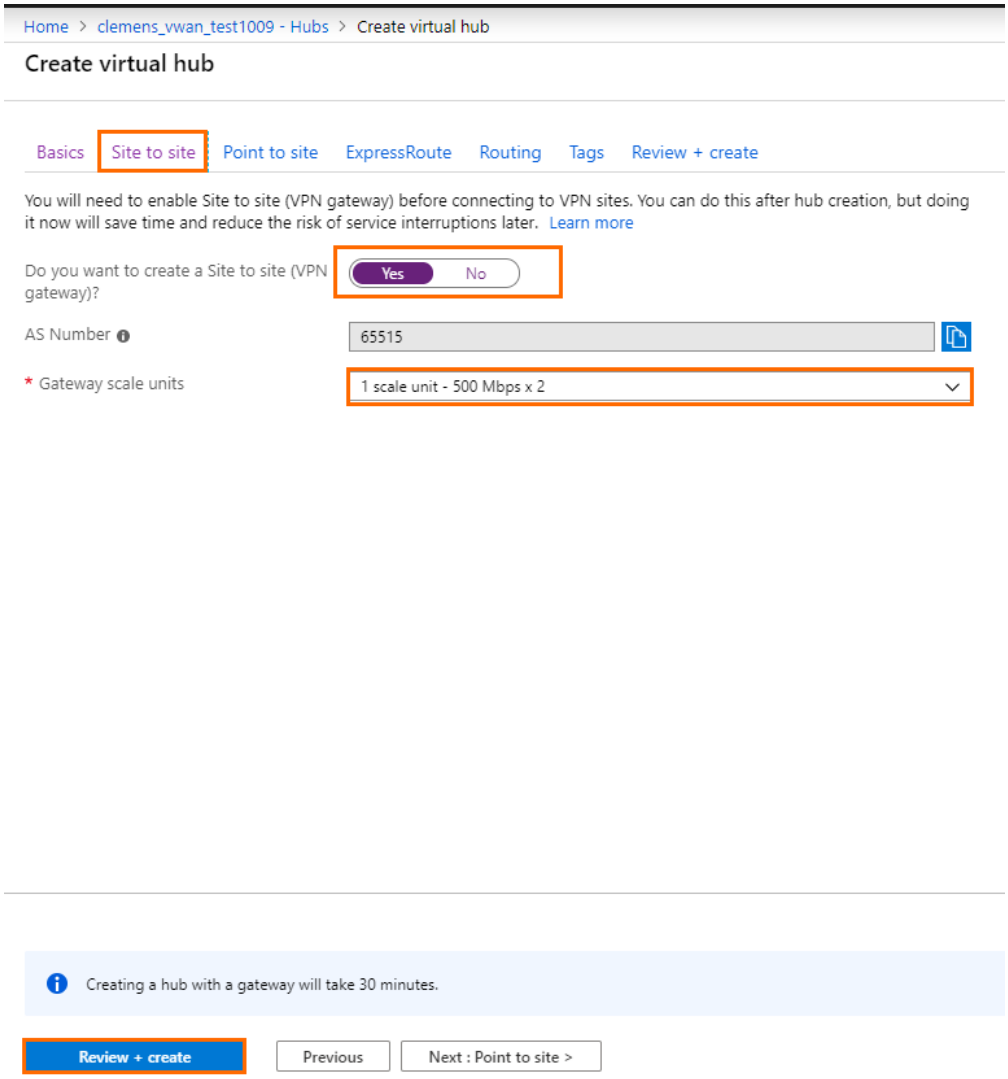
1. Log into the Azure portal: https://portal.azure.com
2. In the left menu, click **All services** and search for **Resource groups**.
3. Click on the resource group your vWAN is attached to. It was created in Step 1.
4. Click on your vWAN created in Step 1.
5. On the left side, click **Hubs**.
6. In the next blade, click **New Hub**.



7. The **Create virtual hub** blade opens.
   1. **Region** – Select a region from the drop-down list, e.g., `West Europe`.
   2. **Name** – Enter a name for the hub, e.g., `doc-vwan-hub`.
   3. **Hub private address space** – Enter the hub's address range in CIDR, e.g., `10.0.0.0/24` .



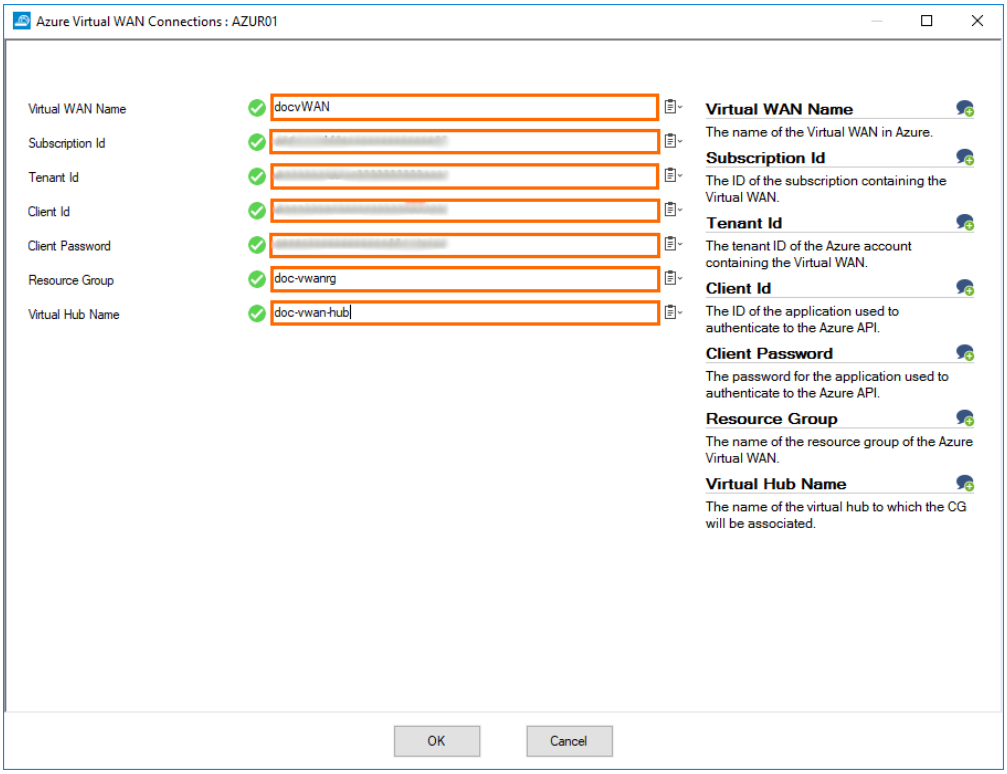
8. Click **Next: Site to site >**.
9. The **Site to site** blade opens.
    1. **Do you want to create a Site to site (VPN gateway)** – Select **Yes**.
    2. **Gateway scale units** – Select a scale unit from the drop-down menu according to your requirements.



10. Click **Review + create**.
11. Review your settings and click **Create** to start the creation of the hub. This can take up to 30 minutes.

Step 3. Trigger Virtual WAN connection

1. Log into the CloudGen Firewall with CloudGen Admin.
2. Go to **CONTROL > Box**.
3. Click **Microsoft Azure Virtual WAN** and select **Connect to Virtual WAN**.
4. Enter the required information in the dialog to start automatic creation of the site. The site will be created and is then available in the Azure Virtual WAN **Settings**.



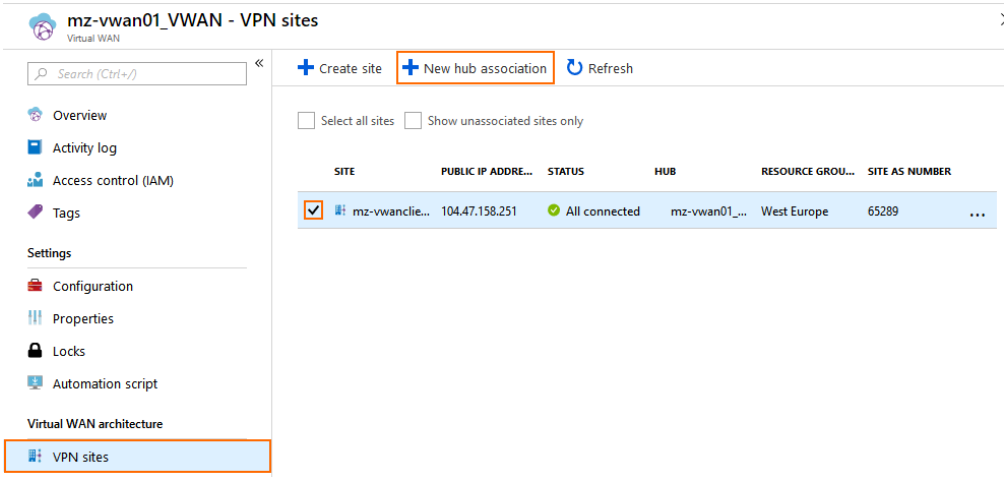
5. Click **Connect** to start the automatic site configuration process on Microsoft Azure.

A VPN site entry is automatically created, and the firewall starts to check for an available configuration every 30 seconds. To view the connection log, click **Check Connection Status**. Repeat as needed to update the status log messages.

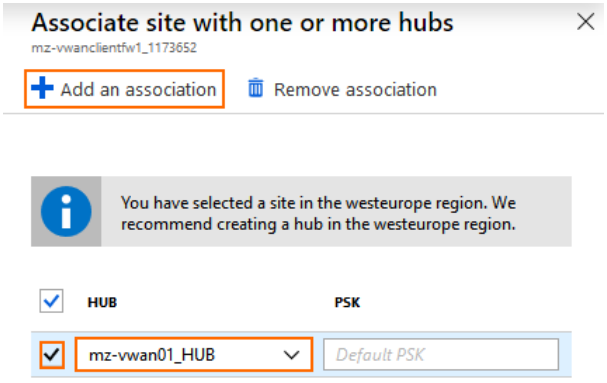
Step 4. Associate Site to the Hub

The Virtual WAN VPN site must be associated to the geographically nearest Virtual WAN hub by the admin.

1. Log into the Azure portal: https://portal.azure.com
2. In your Azure Resource group, open your **Azure Virtual WAN**.
3. In the left menu of the Virtual WAN blade, click **VPN Sites**.
4. Select the check box of the Virtual WAN VPN site created by the firewall in Step 2 and click **New hub association**. The **Associate site with one or more hubs** blade opens.



5. Select the **Hub** from the list.
6. Select the check box for the hub and click **Add an association**.

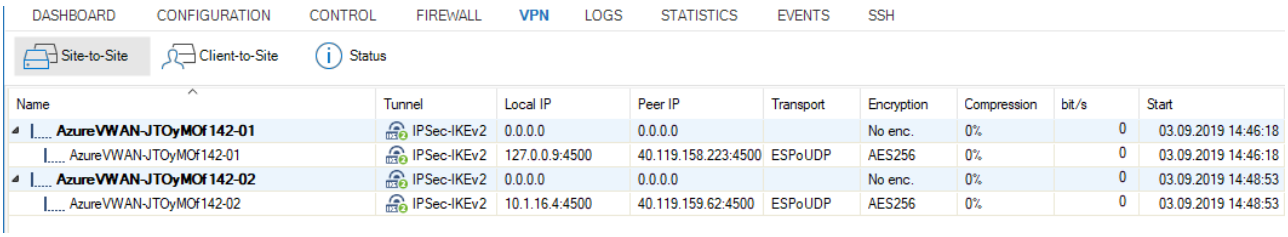


Wait for the new hub association to complete. The firewall automatically picks up the new configuration and connects to the Virtual WAN.

Step 5. Verify Connectivity and Routing

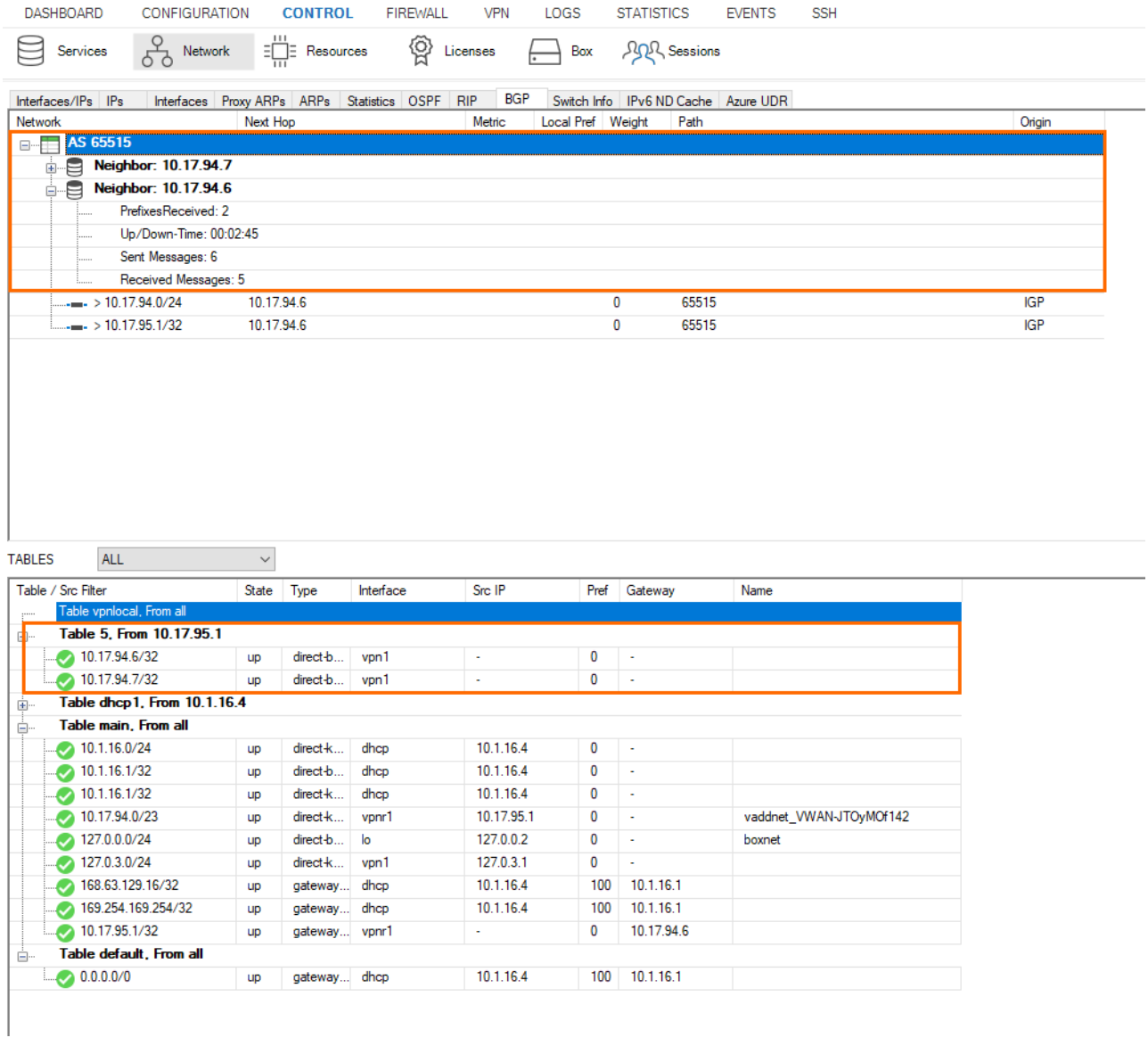
For redundancy reasons, the CloudGen Firewall automatically creates two IPSec-IKEv2 VPN tunnels and the required BGP routes to the Microsoft Azure virtual hub. Both tunnels are in active-active mode. In case one tunnel fails, the routing is changed to automatically use the other tunnel.

1. Log into the CloudGen Firewall.
2. Go to **VPN > Site-to-Site**.
3. Verify if two IPSec-IKEv2 tunnels are up and running.



Name	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Start
AzureVWAN-JTOyMOf142-01	IPSec-IKEv2	0.0.0.0	0.0.0.0		No enc.	0%	0	03.09.2019 14:46:18
AzureVWAN-JTOyMOf142-01	IPSec-IKEv2	127.0.0.9:4500	40.119.158.223:4500	ESPoUDP	AES256	0%	0	03.09.2019 14:46:18
AzureVWAN-JTOyMOf142-02	IPSec-IKEv2	0.0.0.0	0.0.0.0		No enc.	0%	0	03.09.2019 14:48:53
AzureVWAN-JTOyMOf142-02	IPSec-IKEv2	10.1.16.4:4500	40.119.159.62:4500	ESPoUDP	AES256	0%	0	03.09.2019 14:48:53

4. Go to **CONTROL > Network** and open the **BGP** tab.
5. Verify that, along with the VPN tunnels, all associated BGP autonomous systems and neighbors are present.



Step 6. Configure the Forwarding Firewall Rule Set

To manage and restrict network traffic from and to the Azure Virtual hub, the forwarding firewall rule

set needs to be adapted to allow traffic as required.

For more information, see How to Create a Pass Access Rule.

Next Steps

Attach an Azure Virtual Network to the Virtual WAN hub to use the VPN connection for branch-to-cloud connectivity.

Figures

1. vpn_hub.png
2. vwan2_01.png
3. vwan2_02.png
4. create_hub.png
5. create_hub2.png
6. site to site vpn_gateway.png
7. vwan_config_cgf.png
8. vwan2_03.png
9. vwan2_04.png
10. vpn.png
11. cgf_network.png