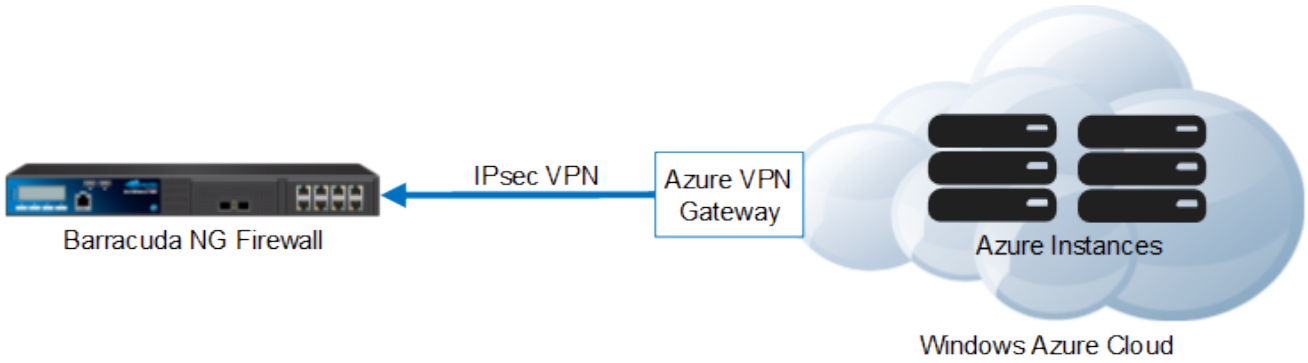
How to Configure an IPsec Site-to-Site VPN to a Microsoft Azure VPN Gateway

https://campus.barracuda.com/doc/41116398/

You can configure your local Barracuda NG Firewall to connect to the IPsec VPN gateway service in the Windows Azure cloud.



In this article

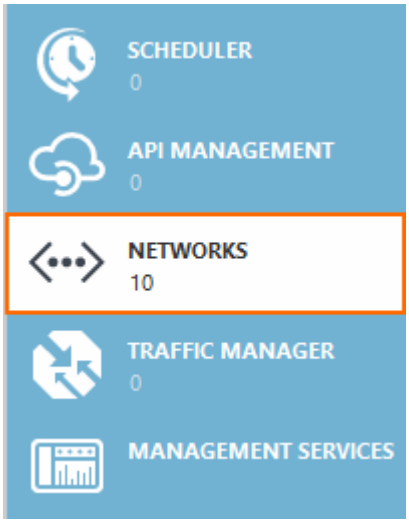
Before you Begin

- Create and configure a Windows Azure static VPN Gateway for your virtual network.
- You will need the following information:
  - VPN Gateway
  - External IP address for the Barracuda NG Firewall
  - Remote and local networks.

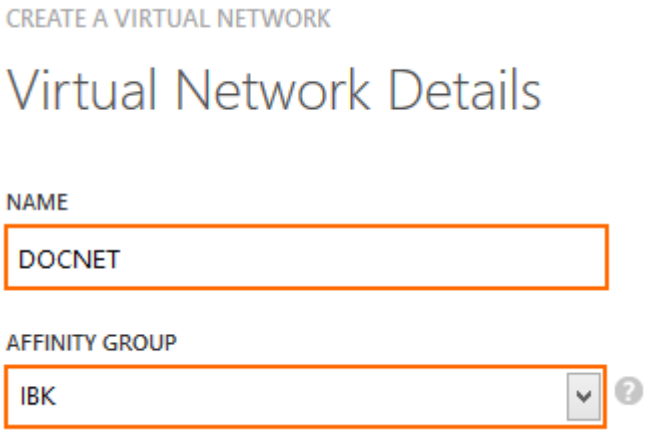
Step 1. Create a Network in the Windows Azure Cloud

Create a virtual Network in the Windows Azure cloud. Choose subnets which are not present in your local networks to avoid IP address conflicts.

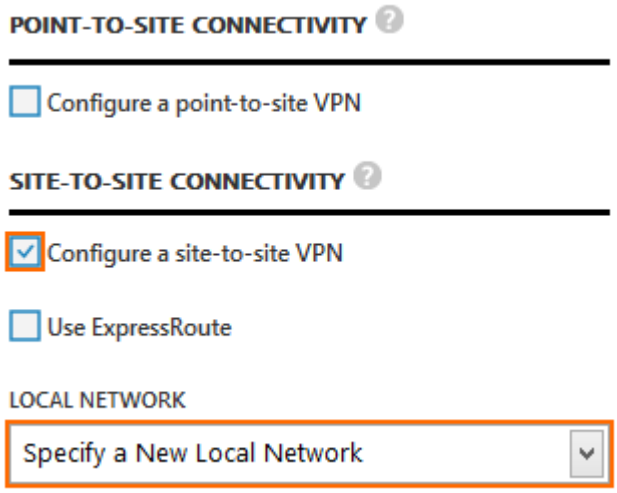
1. Log into your Windows Azure Management Portal (https://manage.windowsazure.com)
2. In the left pane click **NETWORKS**.



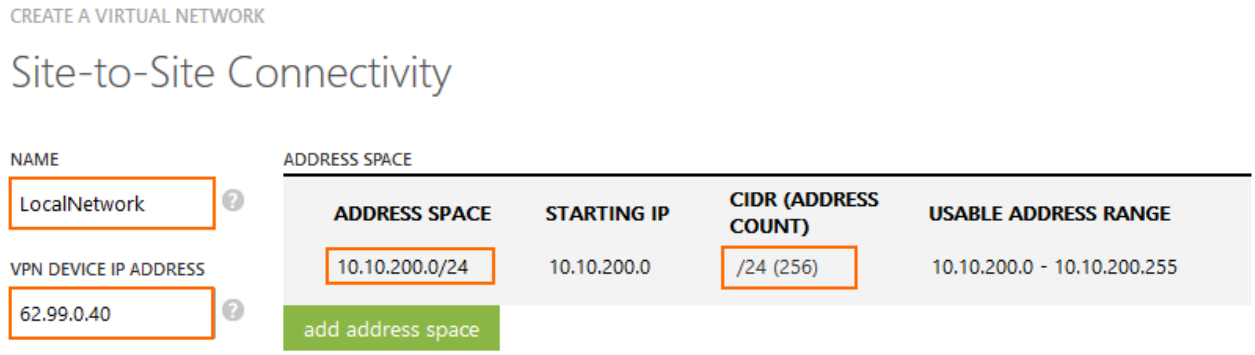
3. In the bottom left corner click **+ NEW**.
4. Click **CUSTOM CREATE**. The **create a virtual network** windows opens.
5. Enter the **Name** for the network.
6. Select an affinity group or create a new affinity group.
7. Click **NEXT** .



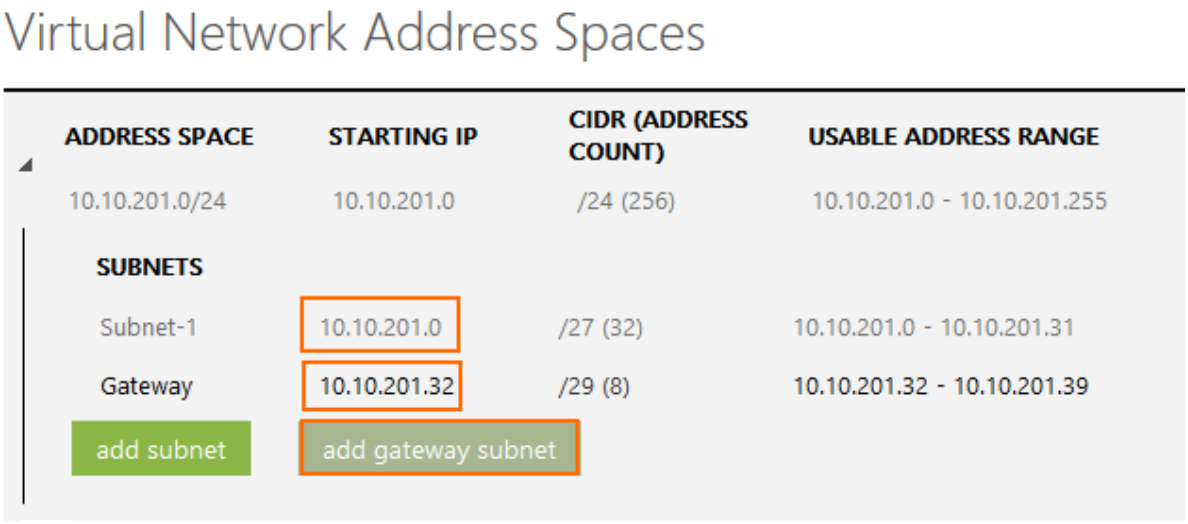
8. (optional) Enter or select a DNS server.
9. In the right panel enable **Configure site-to-site VPN**.
10. Select **Specify a New Local Network** from the **LOCAL NETWORK** drop down.



11. Click **Next** .
12. Enter a **NAME** for your local on-premises network.
13. Enter the **VPN DEVICE IP ADDRESS**. This is the external IP address of the Barracuda NG Firewall running the VPN service.
14. In the **ADDRESS SPACE** section enter the on-premise network(s). E.g., `10.10.200.0/24`
15. Click **Next** .



16. In the **Virtual Network Address Spaces** section click **add subnet**:
    - **Subnet** – Enter a name for the subnet.
    - **Starting IP** – Enter the first IP of the IP Range for the subnet. E.g., `10.10.201.0`
    - **CIDR(ADDRESS COUNT)** – Select the subnet mask from the list. E.g., **/24** for 256 IP addresses.
17. Click **add gateway subnet**:
    - **Starting IP** – Enter the first IP for the gateway subnet. E.g., `10.10.201.0`
    - **CIDR (ADDRESS COUNT)** – Select the subnet mask from the list. E.g., /29 for 8 IP addresses.



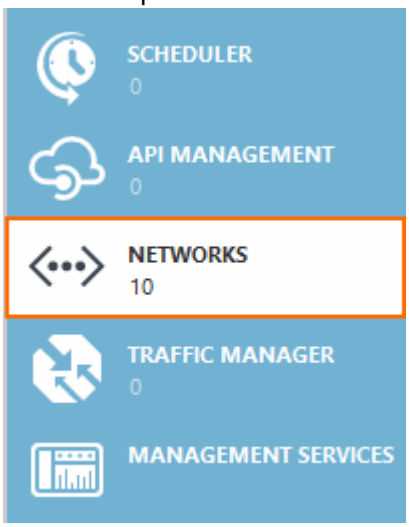
18. Click OK .

The Azure Virtual Network you have just created is now listed in the **NETWORK** menu in the Azure management interface.

Step 2. Create a VPN Gateway for the Windows Azure Network

Create the Azure VPN Gateway.

1. Log into your Windows Azure Management Portal (https://manage.windowsazure.com).
2. In the left pane click **NETWORKS**.

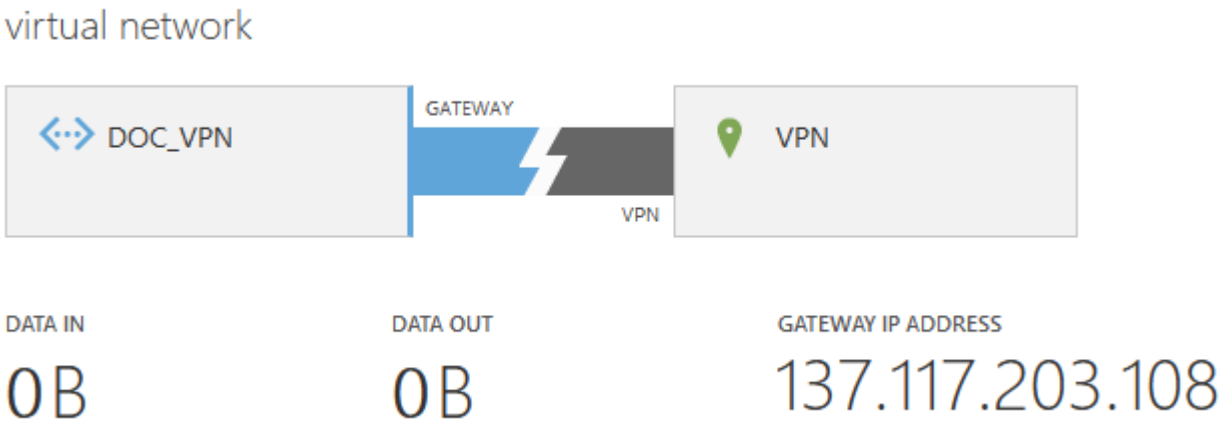


3. Click on the Network previously created in **Step 1**.

4. in the top menu click on **DASHBOARD**.
5. In the bottom pane, click **CREATE GATEWAY**.

6. Select **Static Routing** from the list. Creating the gateway will take a couple of minutes.

When the color of the gateway turns blue, the gateway has been successfully created. The Gateway IP is now displayed below the VPN Gateway image.

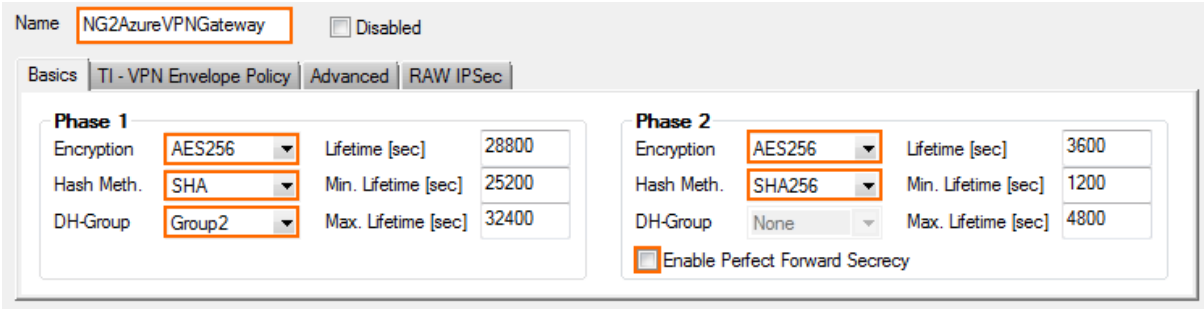


Step 3. Configure IPsec Site-to-Site VPN on the Barracuda NG Firewall

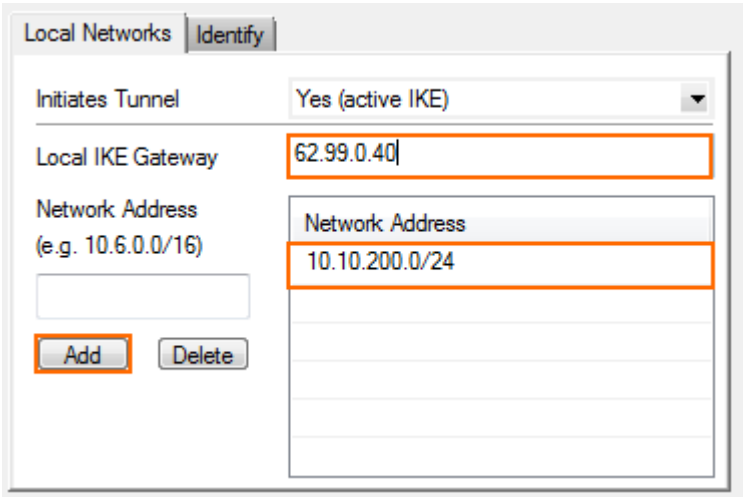
Create a passive IPsec VPN connection on the local Barracuda NG Firewall.

1. Open the **Site to Site** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **VPN-Service**).
2. Click the **IPSEC Tunnels** tab.
3. Click **Lock**.
4. Right-click the table and select **New IPSec tunnel**. The **IPsec Tunnel** window opens.
5. In the **Name** field, enter your tunnel name. E.g., `NG2AzureVPNGateway`
6. In the **Basics** tab enter the Phase1 and Phase2 encryption settings:
    - **Phase 1**
        - **Encryption** – Select **AES-256**.
        - **Hash Meth**. – Select **SHA**.
        - **DH Group** – Select **Group 2**.

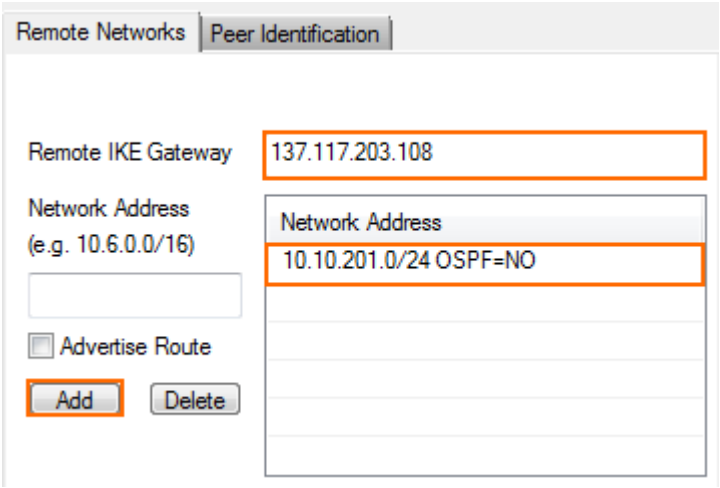
        - **Lifetime** – Enter 28800.
    - **Phase 2**
        - **Encryption** – Select **AES-256**.
        - **Hash Meth.** – Select **SHA256**.
        - **Perfect Forward Secrecy** – Disable.
        - **Lifetime** – Enter 3600.



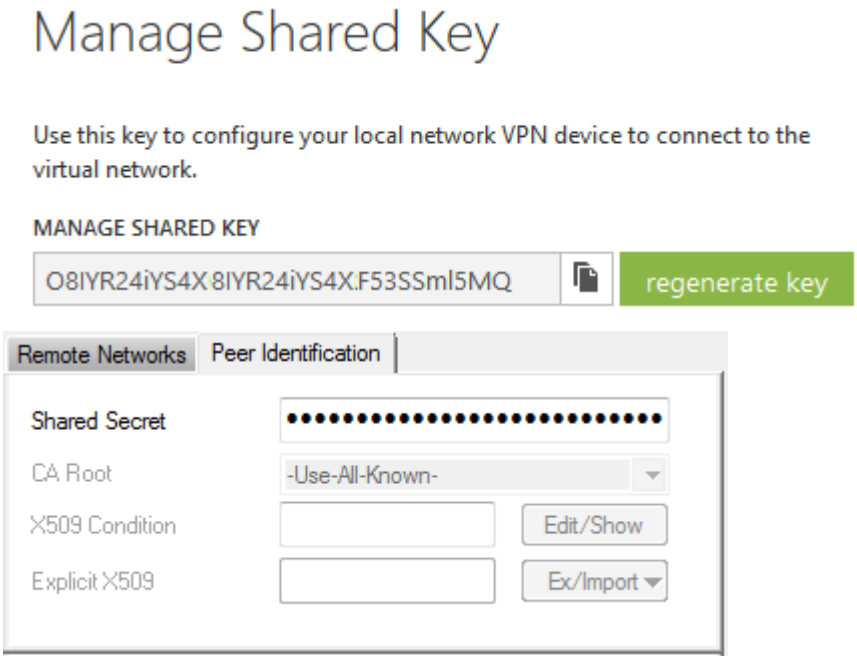
7. Configure the local network settings. Click the **Local Networks** tab and specify the following settings:
    - **Local IKE Gateway –** Enter the external IP address of the Barracuda NG Firewall. E.g., 62.99.0.40
    - **Network Address –** Enter your local on-premise network and click **Add**. E.g., 10.10.200.0/24



8. Configure the remote network settings. Click the **Remote Networks** tab and specify the following settings:
    - **Remote IKE Gateway –** Enter the Gateway IP Address of the Azure VPN Gateway created in Step 2. E.g., 137.117.205.83
    - **Network Address –** Enter the Azure subnet(s) configured in the Azure Virtual Network and click **Add**. E.g., 10.10.201.0/24.



Click on the **Peer Identification** tab and enter the Azure **MANAGE KEY** passphrase.



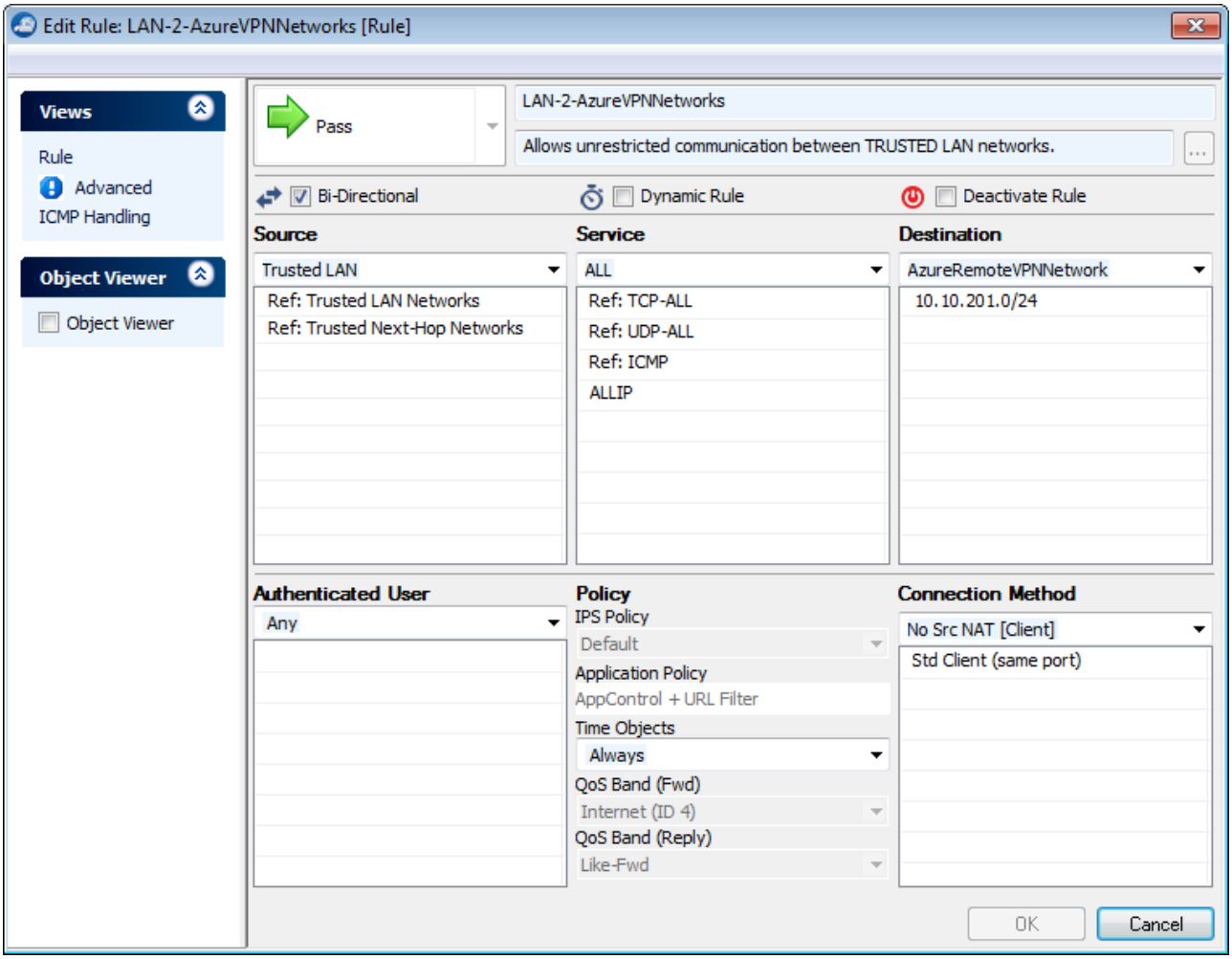
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Step 4. Create a Access Rule

Create a pass firewall rule to allow traffic from the local network to the remote network.

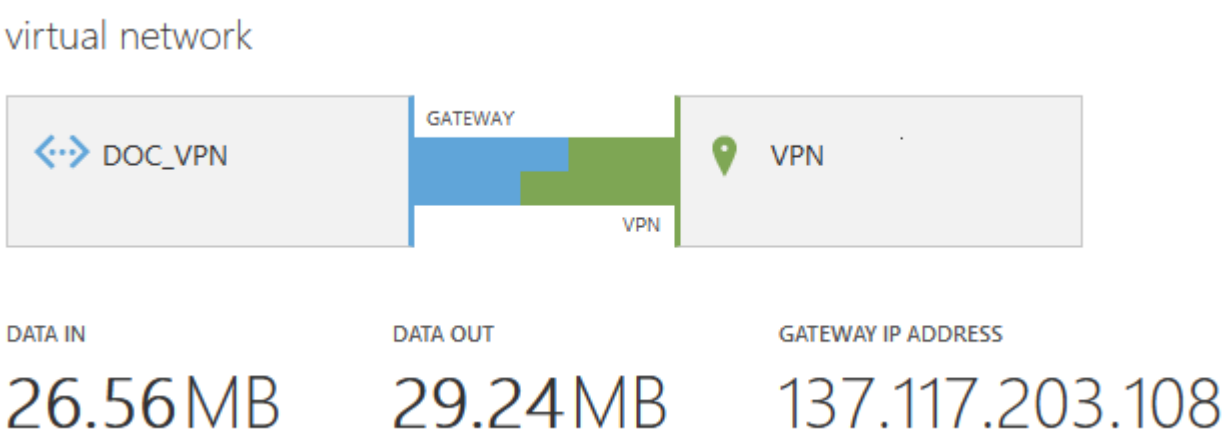
1. Create a Network Object containing the remote Azure subnets.
2. Create a Pass access rule:
   - **Bi-Directional** – Enable.
   - **Source** – Select the local on-premise network(s).
   - **Service** – Select the service you want to have access to the remote network or **ALL** for complete access.

- **Destination** – Select the network object containing the remote Azure Virtual Network subnet(s).
- **Connection Method** – Select **No Src NAT**.



3. Click **OK**.
4. Move the firewall rule up in the rule list, so that it is the first rule to match the firewall traffic.
5. Click **Send Changes** and **Activate**.

Your Barracuda NG Firewall will now automatically connect to the Azure VPN Gateway.


virtual network
DOC_VPN
GATEWAY
VPN
VPN
DATA IN
26.56 MB
DATA OUT
29.24 MB
GATEWAY IP ADDRESS
137.117.203.108

Figures

1. Azure_VPN_Gateway.png
2. azVPN01.png
3. AzureNextArrow.png
4. azVPN02.png
5. azVPN03.png
6. AzureNextArrow.png
7. AzureNextArrow.png
8. azVPN04.png
9. azVPN05.png
10. AzureOK.png
11. azVPN01.png
12. azVPN07.png
13. azVPN08.png
14. azVPN09.png
15. Azure_ipsec01.png
16. Azure_ipsec02.png
17. Azure_ipsec03.png
18. azVPN06.png
19. Azure_ipsec04.png
20. access_rule01.png
21. azVPN10.png