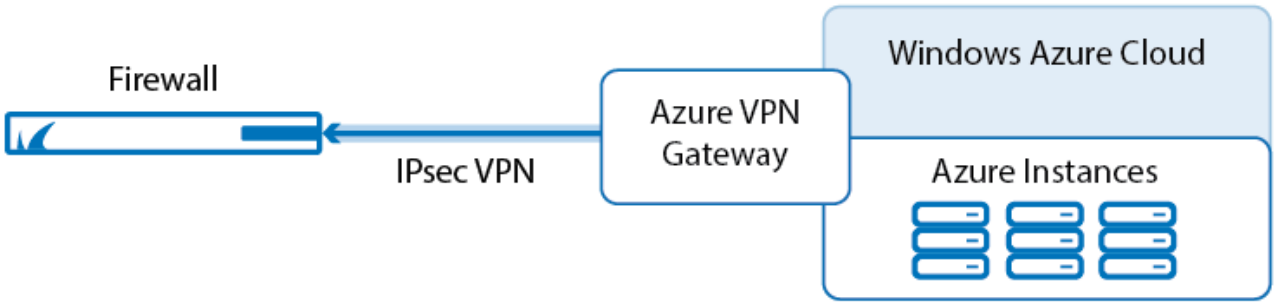
# How to Configure an IKEv1 IPsec Site-to-Site VPN to the Static Microsoft Azure VPN Gateway

https://campus.barracuda.com/doc/72516428/

You can configure your local firewall to connect to the static IPsec VPN gateway service in the Windows Azure cloud using an IKEv1 IPsec VPN tunnel.



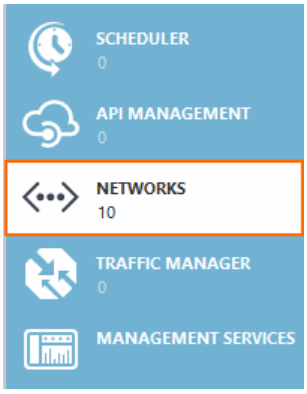

## Before You Begin

- 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 firewall
  - Remote and local networks

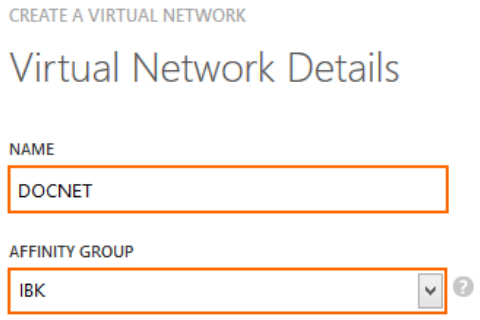
## Step 1. Create a Network in the Windows Azure Cloud

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

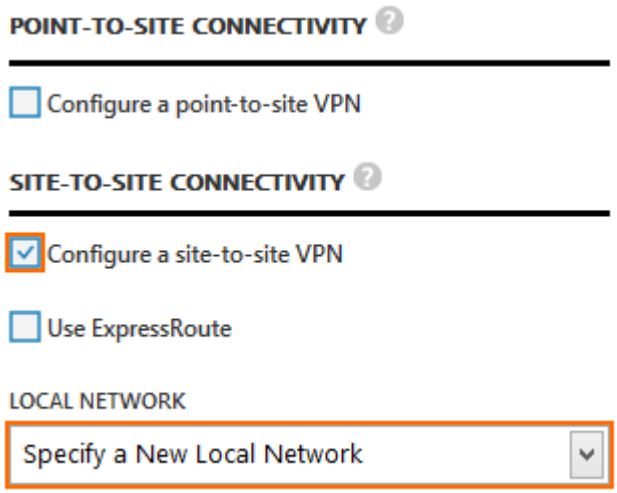
1. Log into your Windows Azure Management Portal (https://manage.windowsazure.com).
2. In the left pane, click **NETWORKS**.




3. In the bottom left, 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** .

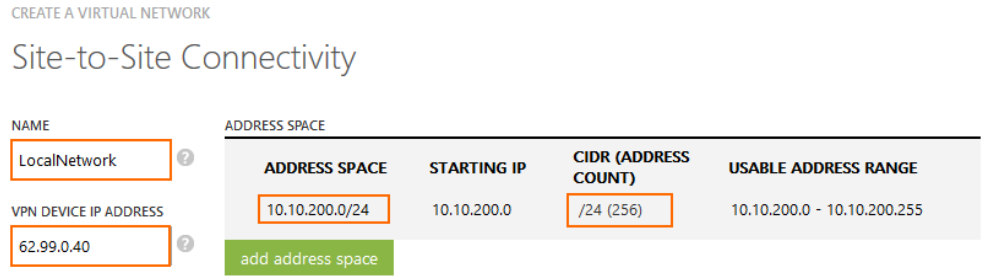



8. (optional) Enter or select a DNS server.
9. In the right panel, enable **Configure site-to-site VPN**.
10. Select **Specify a New Local Network** from the **LOCAL NETWORK** drop-down list.

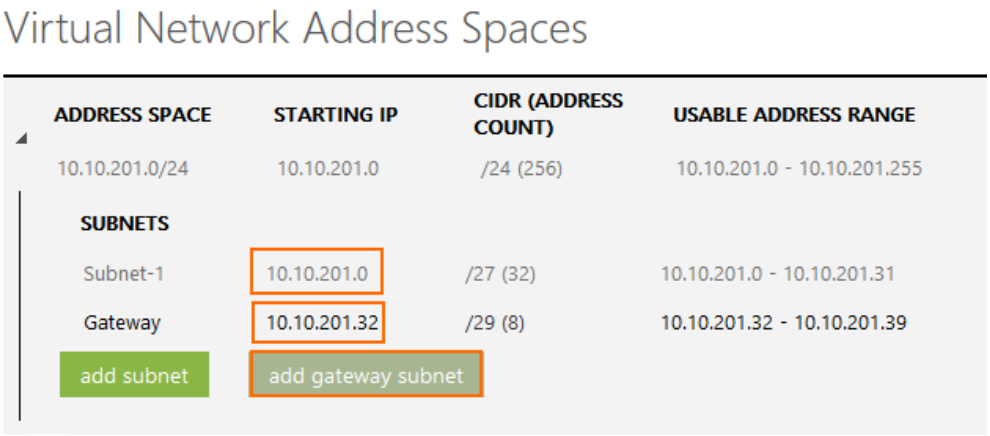



11. Click **Next** .
12. Enter a **NAME** for your local on-premises network.
13. Enter the **VPN DEVICE IP ADDRESS**. This is the external IP address of the firewall running the VPN service.
14. In the **ADDRESS SPACE** section, enter the on-premises network(s). E.g., `10.10.200.0/24`

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.



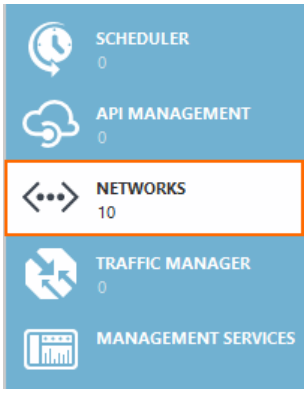

18. Click **OK** .

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**.

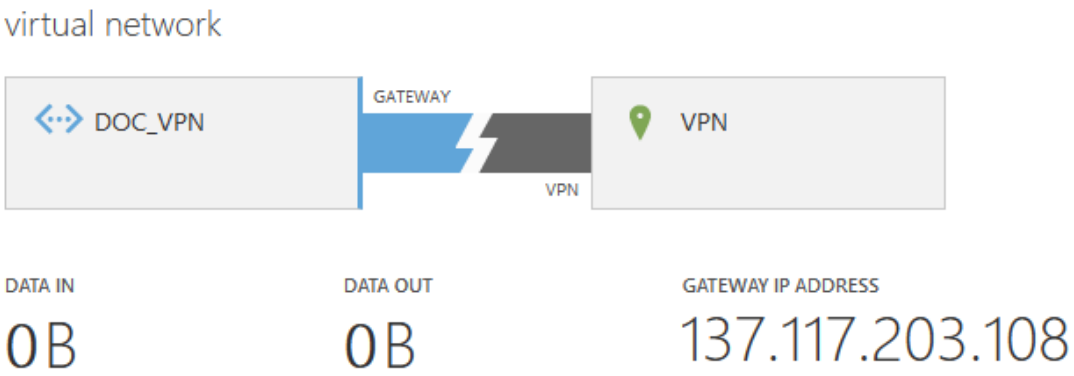



4. In the top menu, click **DASHBOARD**.
5. In the bottom pane, click **CREATE GATEWAY**.




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.



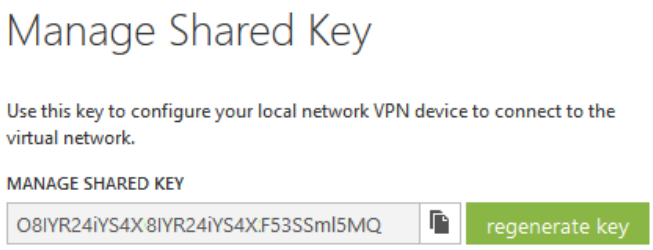

## Step 3. Configure IPsec Site-to-Site VPN on the Firewall

Create an active IPsec VPN connection on the firewall.

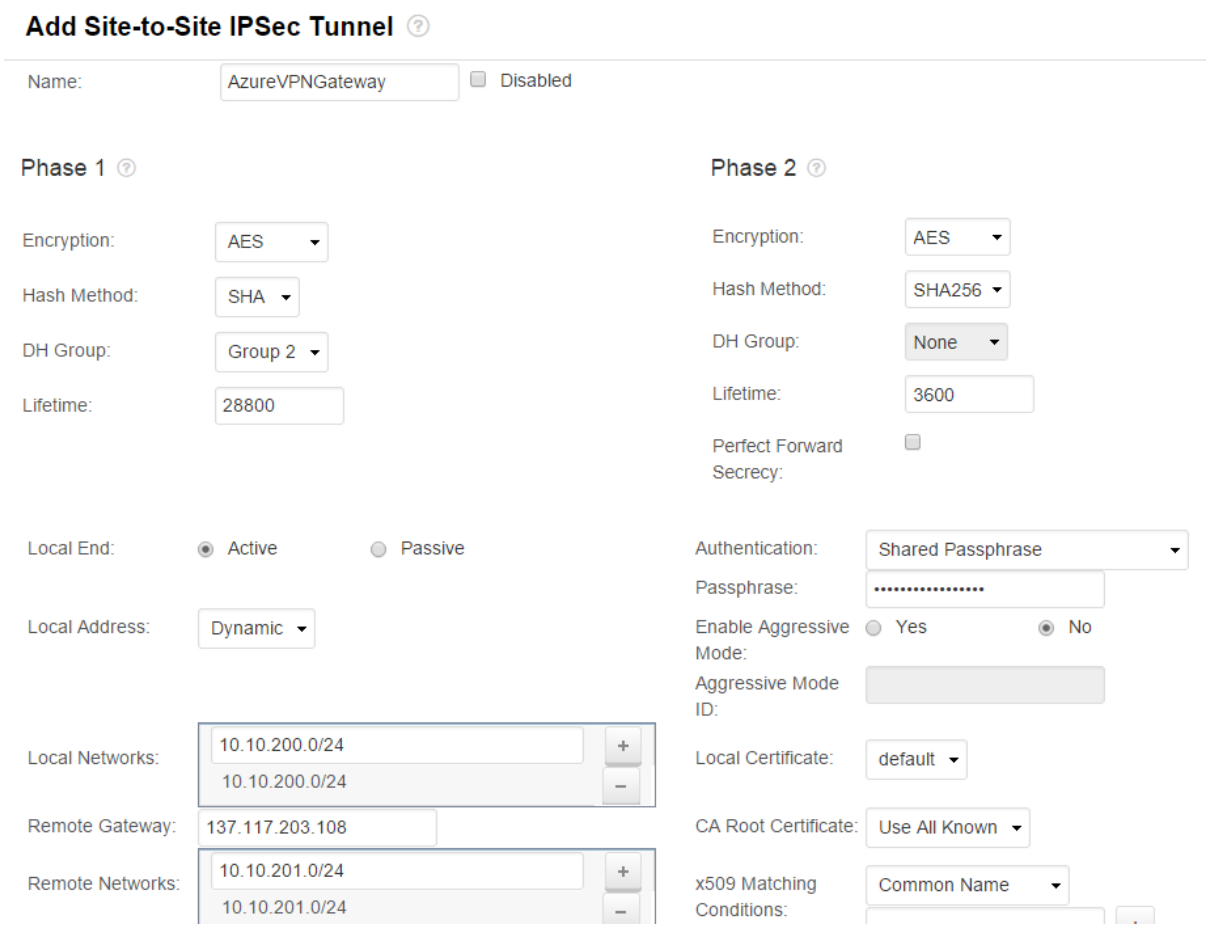
1. Go to **VPN > Site-to-Site**.
2. If you are using a dynamic address (DHCP, xDSL, 3G) to connect to the Internet, or if you are

behind a NAT, enable **Use Dynamic IPs** in the **GLOBAL SERVER SETTINGS** section, and click **Save**. The VPN service restarts.

3. In the **Site-to-Site IPsec Tunnels** section, click **Add**.
4. Enter the **Name** for the IPsec VPN. E.g., `AzureVPNGateway`
5. Configure the **Phase 1** and **Phase 2** encryption settings:
   - **Phase 1:**
     - **Encryption** – AES
     - **Hash Method** – SHA
     - **DH Group** – Group 2
     - **Lifetime** – 28800
   - **Phase 2:**
     - **Encryption** – AES
     - **Hash Method** – SHA256
     - **Lifetime** – 3600
     - **Perfect Forward Secrecy** – No
   - **Local End** – Active
   - **Local Address** – Dynamic or static if you are using a static WAN connection.
   - **Local Networks** – Enter your on-premises subnet(s). E.g., `10.10.200.0/24`
   - **Remote Gateway** – Enter the IP for the **GATEWAY IP ADDRESS** listed on the **DASHBOARD** of your Azure network. E.g., `137.117.203.108`
   - **Remote Networks** – Enter the remote VPC subnet. E.g., `10.10.201.0/24`
   - **Authentication** – Select **Shared Passphrase**.
   - **Passphrase** – Enter the **Shared Key** generated by your Azure VPN gateway. To view the shared key, go to the **DASHBOARD** of your Azure network, and click on the **Manage Key** icon in the bottom pane.




   - **Enable Aggressive** – No.



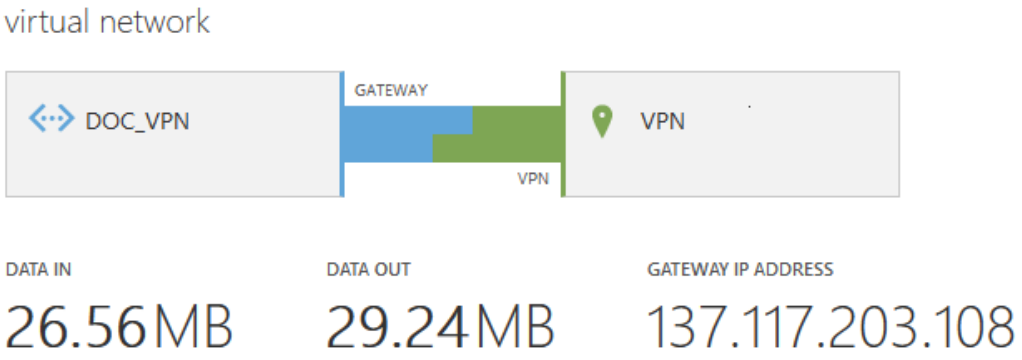

6. Click **Save.**

## Step 4. Create an Access Rule

If you do not have the VPN-SITE-2-SITE access rule, you must create an access rule to allow traffic from your local network to the Azure subnet.

1. Go to **FIREWALL > Access Rules**.
2. Add an access rule:
   - **Type** – Select **ALLOW**.
   - **Source** – Enter your local network(s), or select a network object containing only your local network(s). E.g., `10.10.200.0/24`
   - **Destination** – Enter the remote subnet in the Azure network. E.g., `10.10.201.0/24`
   - **Network Services** – Select **Any**.
   - **Connection** – Select **Original Source IP.**
3. Click **Save**.
4. Place the firewall rule so no rule matches the VPN traffic above it.
5. Click **Save**.

Your firewall will now automatically connect to the Azure VPN gateway.



## 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. azVPN06.png
16. ng_azure_vpn.png
17. azVPN10.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.