**Supported Platforms**

Microsoft Azure is supported with the following Dell SonicWALL appliances:

|  |  |  |
| --- | --- | --- |
| • | | SuperMassive E10000 Series |
| • | SuperMassive 9200 / 9400 / 9600 | | |

|  |  |  |
| --- | --- | --- |
| • | | E-Class NSA E5500 / E6500 / E7500 / E8500 / E8510 |
| • | NSA 2600 / 3600 / 4600 / 5600 / 6600 | | |

|  |  |  |
| --- | --- | --- |
| • | | NSA 220 / 220W / 240 / 250M / 250MW / 2400 / 2400MX / 3500 / 4500 / 5000 |
| • | TZ 100 / 100W / 105 / 105W / 200 / 200W / 205 / 205W / 210 / 210W / 215 / 215W | | |

|  |  |  |
| --- | --- | --- |
| • | | TZ 300 / 300W / 400 / 400W / 500 / 500W / 600 |
| • | SOHO / SOHO W | | |

**Supported firmware**

For the SuperMassive E10000 series, all approved versions of SonicOS support Microsoft Azure.

For platforms other than the SuperMassive E10000 Series, the following SonicOS firmware or hotfixes support the latest version of Microsoft Azure:

**Supported firmware and associated platforms**

|  |  |
| --- | --- |
| **Firmware or hotfix** | **Platforms supported** |
| 6.2.4.3 (December 2015) | TZ300/300W, TZ400/400W, TZ500/500W, TZ600, SOHO W |
| 6.2.3.1-19n--HF163571-1n |
| 6.2.2.3-20n support build | NSA 2600/3600/4600/5600/6600, SuperMassive 9200/9400/9600 |
| 5.9.1.1\_39o--HF157568\_2o | E-Class NSA E5500 / E6500 / E7500 / E8500 / E8510  NSA 220/220W, 240, 250M/250MW, 2400, 2400MX, 3500, 4500, 5000  TZ 100/100W, 105/105W, 200/200W, 205/205W, 210/210W, 215/215W  SOHO |
| 5.9.1-39o--HF160565\_3o |
| 5.8.1.15 |

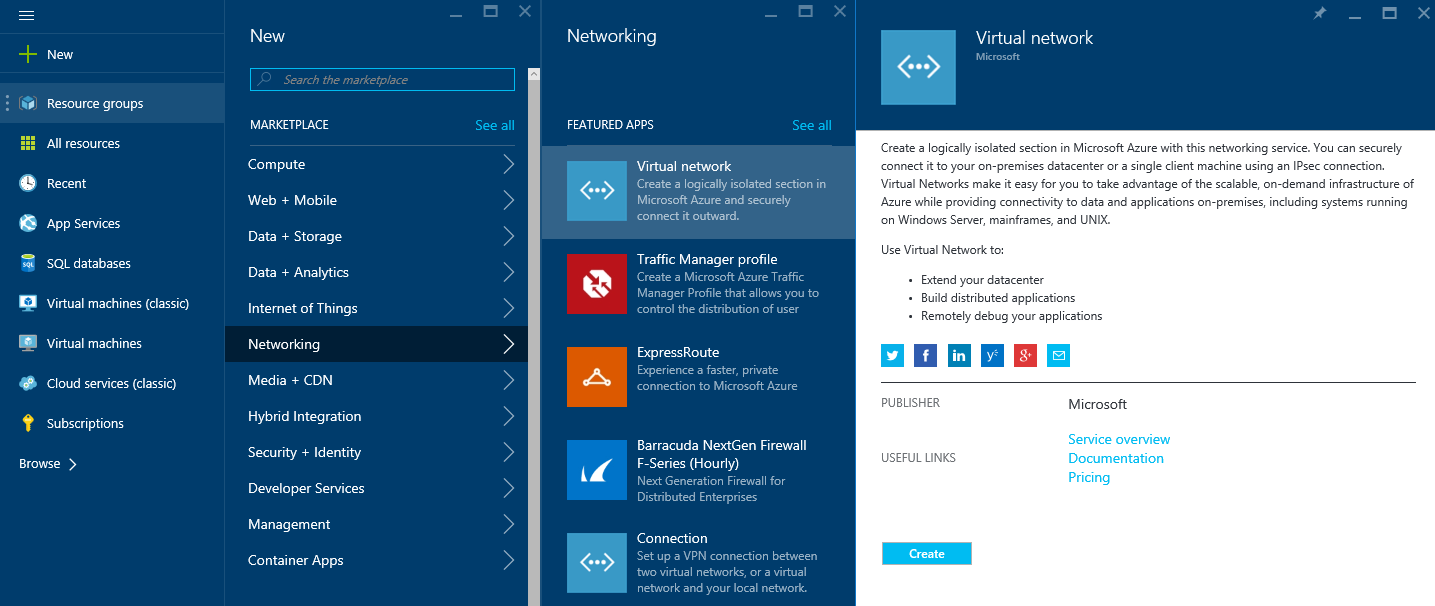
Contact Support at [https://support.software.dell.com/manage-service-request](https://support.software.dell.com/manage-service-request" \t "external_window) to obtain a hotfix or support build for your Dell SonicWALL firewall. Non-hotfix or support build firmware is available on MySonicWALL for your platform.

**Creating the Azure Virtual Network**

In this section, we’ll be creating a virtual network in the Azure portal.

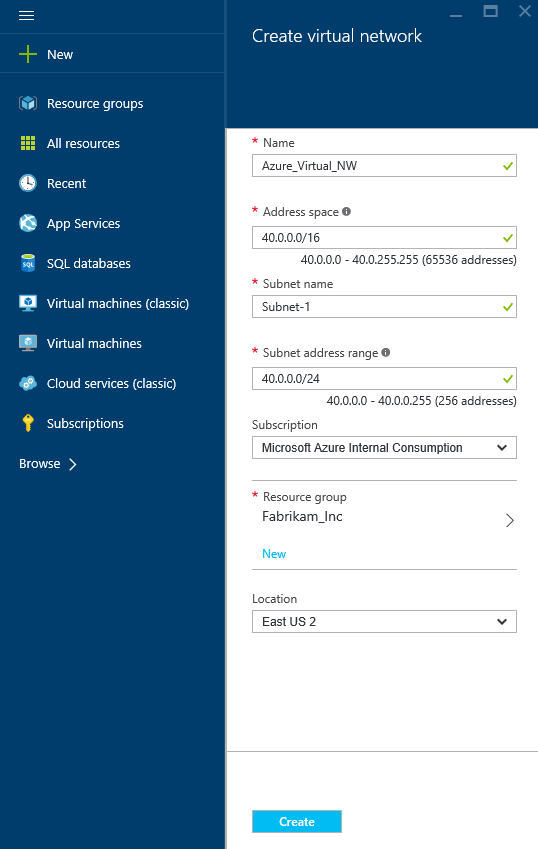
**Step 1:** Create the virtual network:

After login to Azure portal, click New -> Networking -> Virtual Network, Create

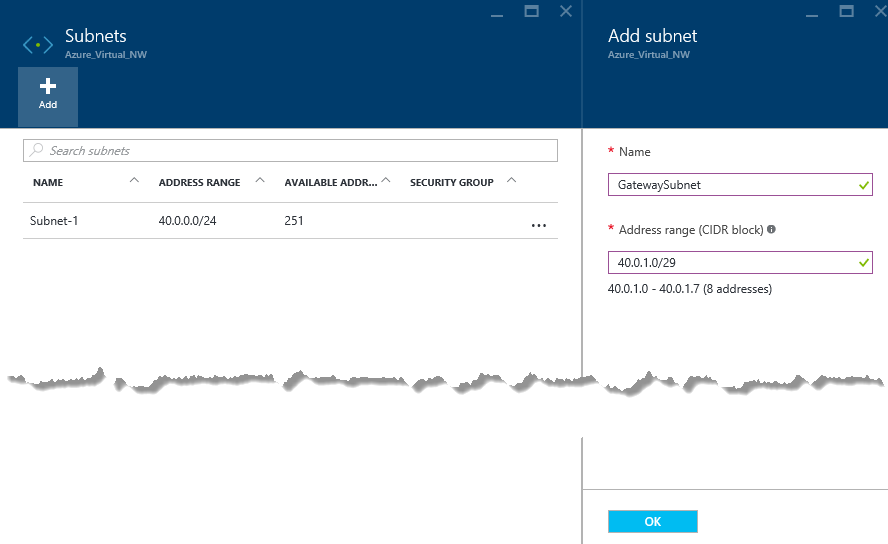


**Step 2:** Create new virtual network

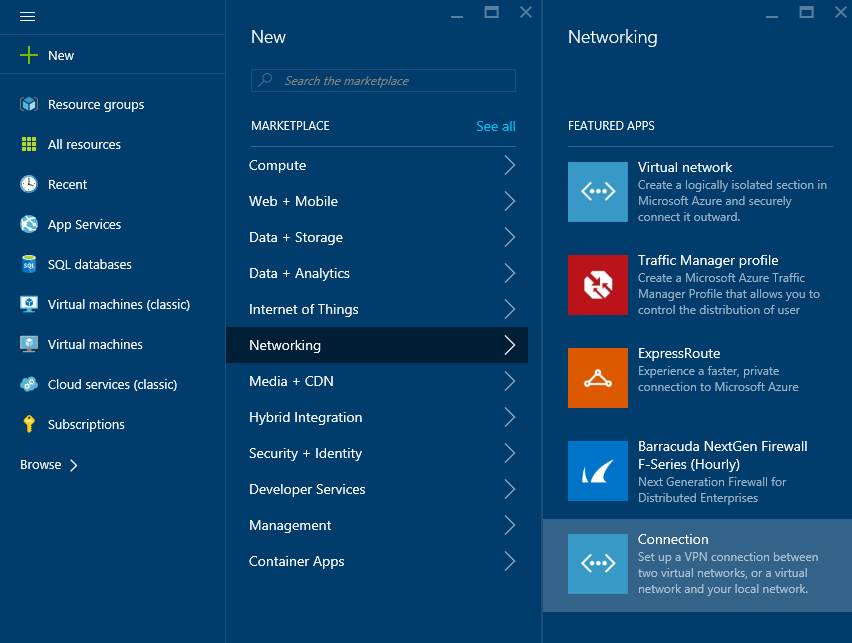
Fill in the name of Virtual Network, the Address range you wish to use in Azure, and the location.



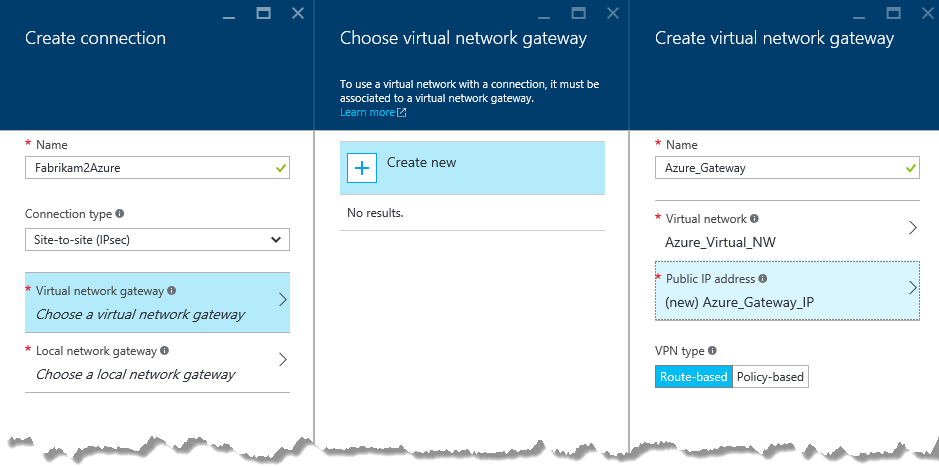
**Step 3:** After creation of a virtual network add a gateway subnet named GatewaySubnet



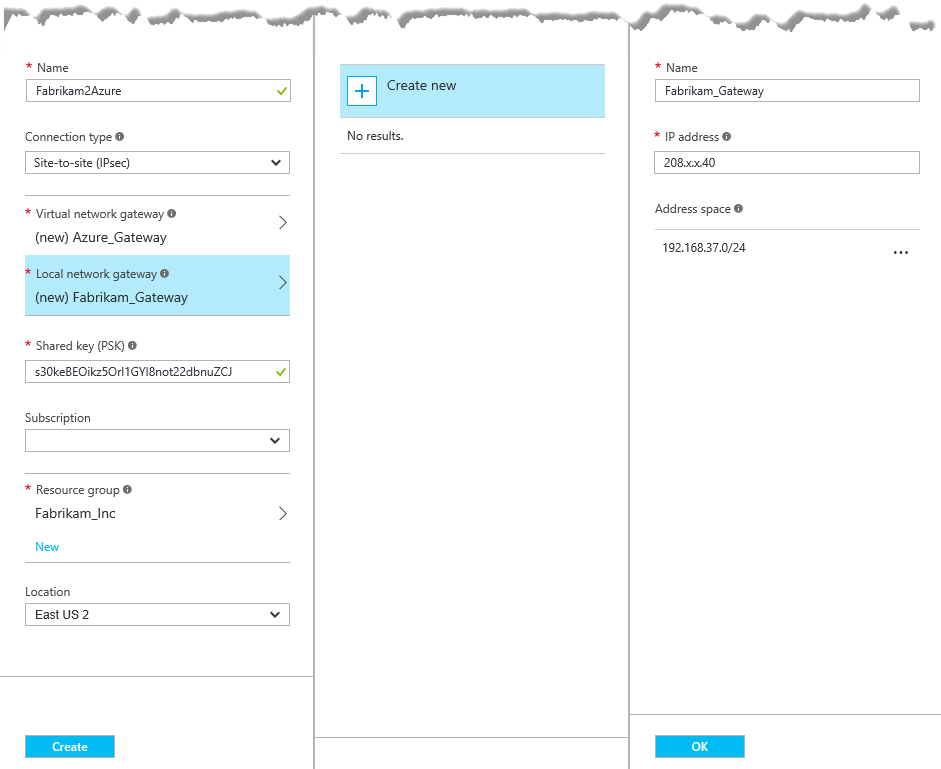
**Step 4:** Create a VPN Connection



**Step 5**: Setup Azure Route-based gateway



**Step 6:** Setup Local Gateway



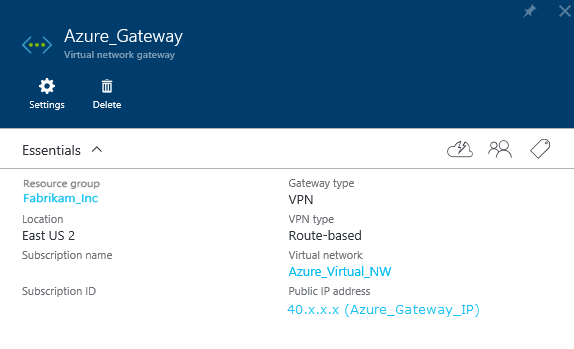
In our example:

**Local virtual network gateway:** 208.X.X.40 *(Sonicwall external interface IP (Public IP address)*

**Local Network Address:** 192.168.37.0/24 *(Your on-premises local network. Specify starting IP address of your network.)*

**Shared Key:** s30keBEOikz5Orl1GYI8not22dbnuZCJ

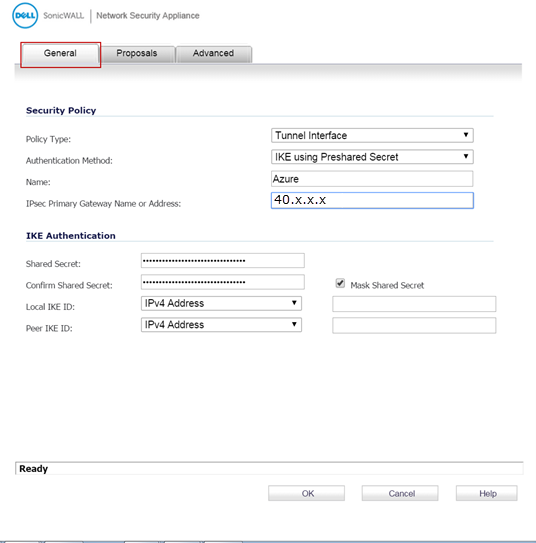
It takes couple of minutes to create Gateway Connection. Once created review the Virtual Network Gateway IP Address



**Creating a Tunnel Interface VPN**

|  |  |
| --- | --- |
| 1 | Log into the SonicOS management interface as an administrator. |
| 2 | Navigate to the VPN > Settings dialog. | |
| 3 | Click Add. | |

The VPN Policy dialog displays.

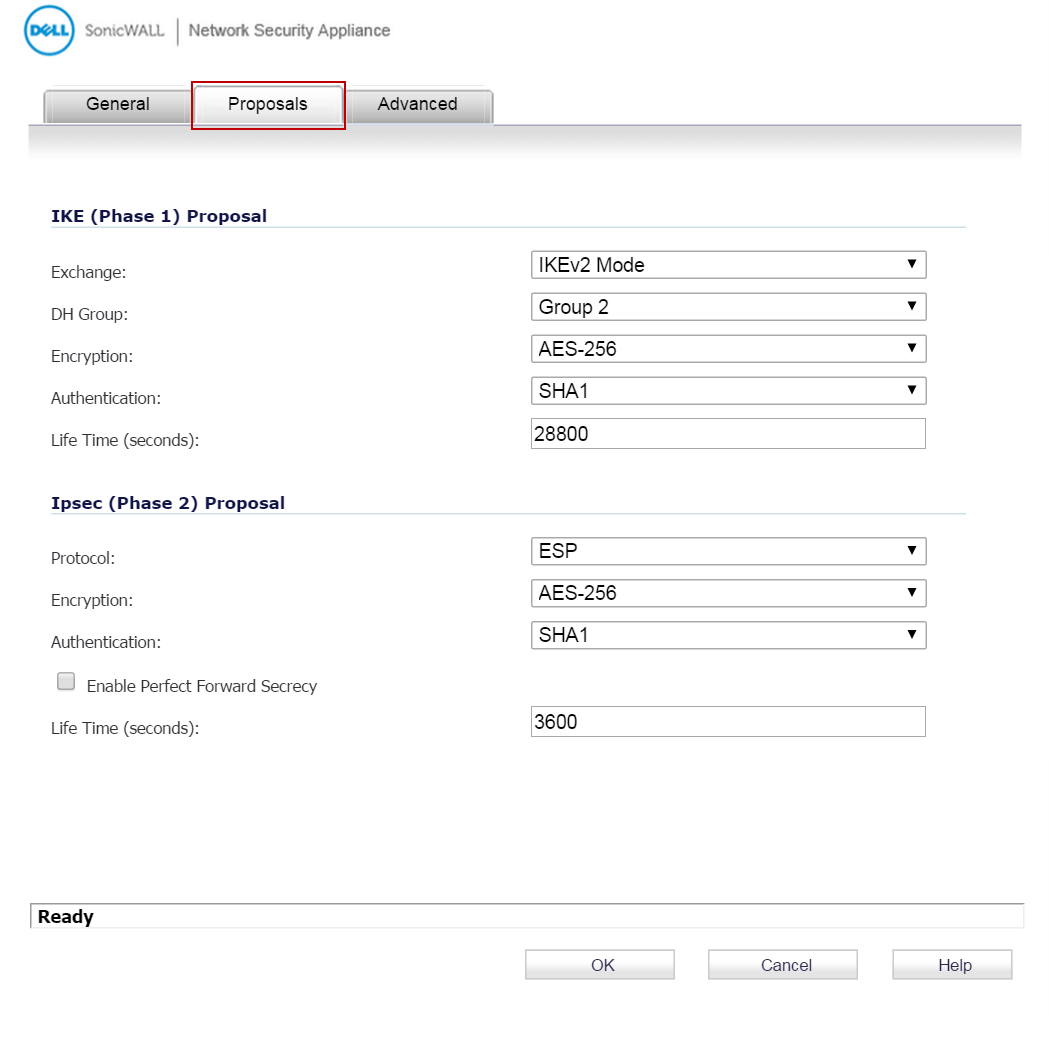


4 Enter the following information:

|  |  |
| --- | --- |
|  | * Authentication Method – select IKE using Preshared Secret. |
|  | * Name – Enter a name for the policy (Azure is used in this example). | |
|  | * IPsec Primary Gateway Name or Address – Enter the GATEWAY IP ADDRESS displayed on the Virtual Network TestVPN Dashboard dialog of the Azure Management Portal. For more information, see the [DynRouteVPN](http://documents.software.dell.com/sonicos/6.2/microsoft-azure-configuration-guide/configuring-a-route-based-vpn/azure-configuration-tasks/creating-a-virtual-network-gateway?ParentProduct=646#pid0e0nd0ha) Quick Start dialog. |
|  | * Shared Secret – This is auto-generated by Azure. Copy it from the Azure Virtual Network dashboard, under Manage Key, and then enter it into this field. For more information, see [Managing Shared Keys](http://documents.software.dell.com/sonicos/6.2/microsoft-azure-configuration-guide/configuring-a-route-based-vpn/azure-configuration-tasks/managing-shared-keys?ParentProduct=646). | |

|  |  |
| --- | --- |
| 5 | Click the Proposals tab. |
| 6 | Click the Exchange drop-down menu, and then select IKEv2 Mode. | |

Azure supports only IKEv2 Mode for route-based site-to-site VPN. For more information about the settings on this dialog, refer to this MSN article titled [About VPN Devices for Virtual Network](https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-about-vpn-devices/" \t "external_window).



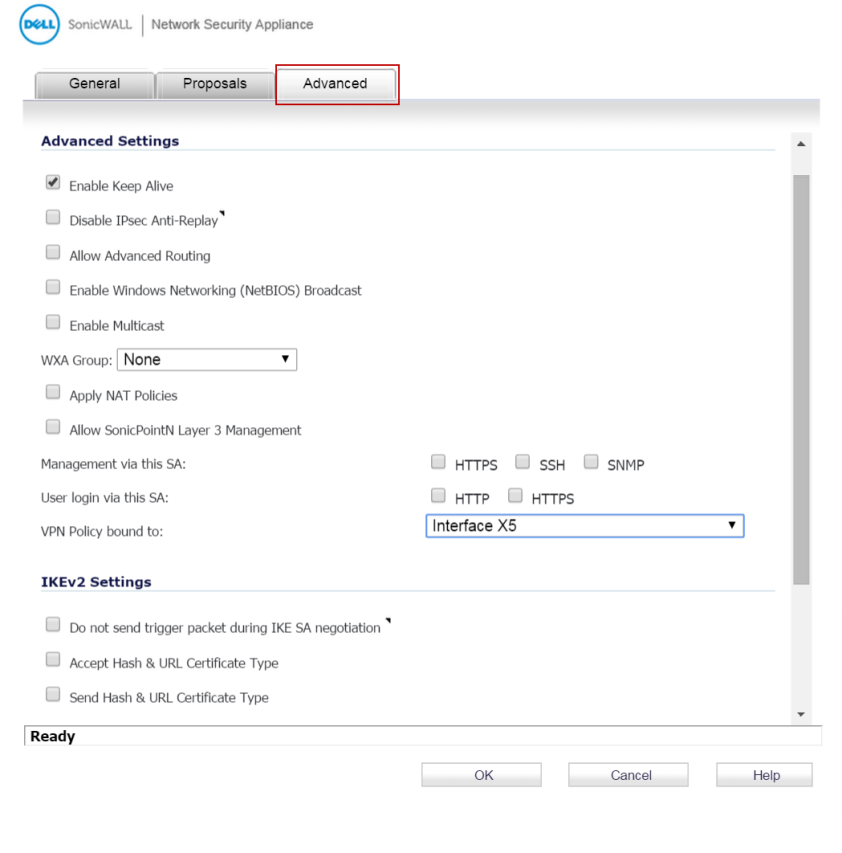
|  |  |
| --- | --- |
|  |  |

7 Click the Advanced tab.

8 Enable Keep Alive by checking Enable Keep Alive.

9 Click the VPN Policy bound to drop-down menu, and then select a WAN interface. For example, Interface X5.

10 Click OK.

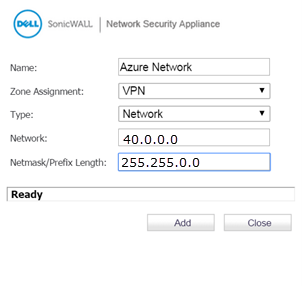


|  |  |
| --- | --- |
| 11 | Select Enable Keep Alive to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives allows for the automatic renegotiation of the tunnel without having to wait for the proposed Life Time to expire. |
| 12 | Click the VPN Policy bound to drop-down menu, and then select the appropriate interface (the WAN interface on the Dell SonicWALL firewall). For example: Interface X1. | |
| 13 | Click OK. | |

**Creating an Address Object for the Virtual Network**

|  |  |
| --- | --- |
| 14 | Navigate to the Network > Address Objects dialog. |
| 15 | Click Add to create a new Address Object. | |

The **Add Address Object** dialog displays:



|  |  |
| --- | --- |
|  | NOTE: The information displayed in this dialog is for example only, and can vary depending on your network. |

16 Enter the following information:

* Name – Enter a name for the Address Object (Azure Network is used in this example)
* Zone Assignment – Click the drop-down, and then select VPN.
* Type – Click the drop-down, and then select Network.
* Network – Enter the network IP address as shown in the Configuring a Virtual Network Address section.
* Netmask/Prefix Length – Enter the netmask.

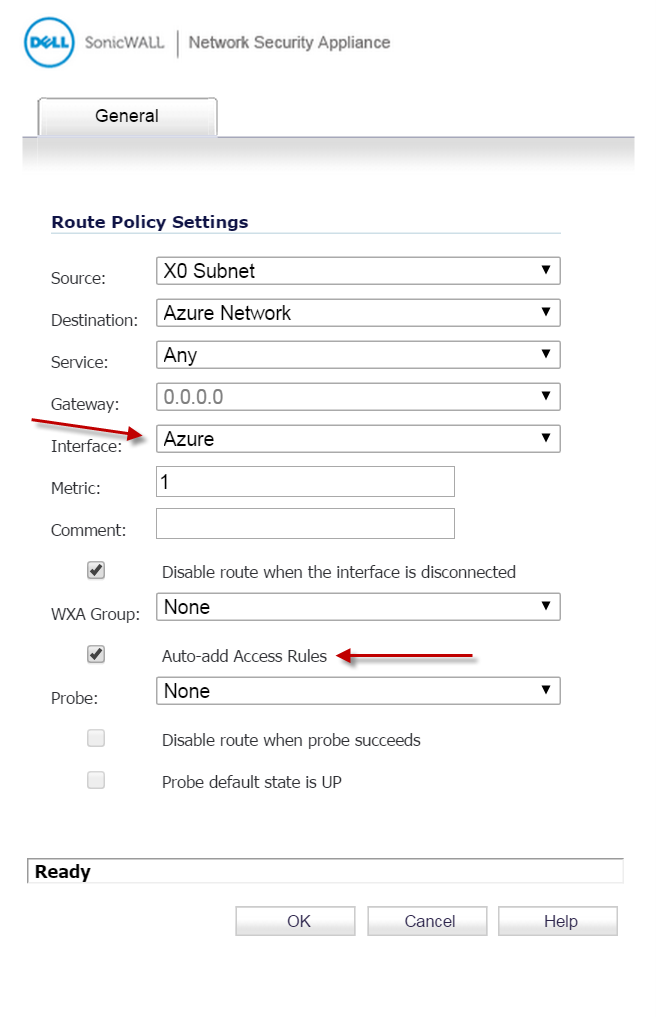
|  |  |
| --- | --- |
| 17 | Click Add. |

**Creating a Static Route Policy**

To create a static route policy, complete the following steps:

|  |  |
| --- | --- |
| 18 | Navigate to the Network > Routing dialog. |
| 19 | Click Add to create a new Route Policy. | |

The Add Route Policy dialog displays.



20 Configure Source to the same on-premise network you configured in the Site-to-Site Connectivity dialog.

NOTE: The information displayed in this screenshot is for example only, and could vary depending on your network.

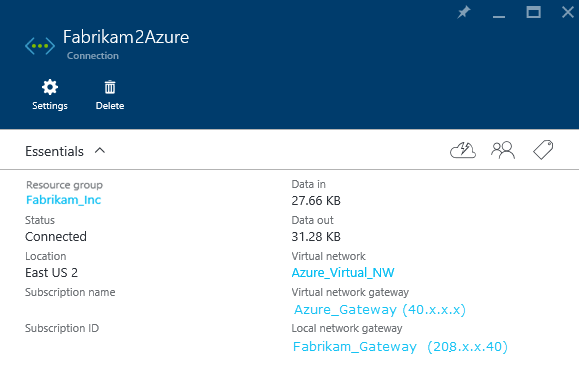
21 Select Disable route when the interface is disconnected.

22 Select Auto-add Access Rules.

23 Click OK.

**Testing the Connectivity**

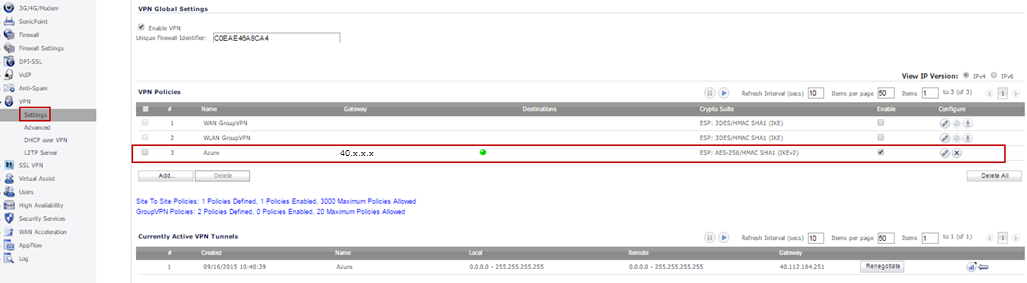
To test the connectivity from Azure portal view connection resource



To test the connectivity from SonicOS:

|  |  |
| --- | --- |
| 1 | Log in to the SonicOS management interface, and navigate to the VPN > Settings dialog. |

In the VPN Policies table, the VPN shows as connected.



It might take a while for the VPN tunnel to show as connected in the Azure Management Portal. After the tunnel is established, the portal appears as shown in the image below.

2 To test traffic flow from the SonicOS side to the Azure cloud, complete either of the following:

* Try to establish an RDP connection to a Virtual Machine (VM) in the cloud on port 3389 from a host behind the Dell SonicWALL firewall.
* Try to ping a VM in the cloud from a host behind the Dell SonicWALL firewall.

NOTE: By default, a VM in the Azure cloud has the inbound ICMP blocked by Windows Firewall and needs to be enabled in Windows using this command: netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any dir=in action=allow