Overview

This TechNote details how to configure a policy-based or route-based VPN between Windows Azure and a Dell SonicWALL Firewall running SonicOS. Windows Azure is a cloud computing platform and infrastructure created by Microsoft. It is used for building, deploying, and managing applications and services through a global network of Microsoft managed datacenters. For SonicOS platforms, Windows Azure provides site-to-site Virtual Private Network (VPN) connectivity between a Dell SonicWALL Next-Generation (NG) Firewall and virtual networks hosted in the Windows Azure cloud.
Deployment Considerations

Please consider the following before deploying Windows Azure:

- The Windows Azure Management Portal uses different terminology for VPNs than the SonicOS Management Interface, see the following for comparison:

<table>
<thead>
<tr>
<th>Windows Azure</th>
<th>SonicOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Routing</td>
<td>Route-Based</td>
</tr>
<tr>
<td>Static Routing</td>
<td>Policy-Based</td>
</tr>
</tbody>
</table>

- Windows Azure supports Dynamic Routing (route-based) and Static Routing (policy-based) site-to-site VPNs.
- For authentication, only Pre-Shared Key (PSK) is currently supported, certificate based site-to-site VPNs are not yet supported.

Supported Platforms

Windows Azure is supported with the following Dell SonicWALL appliances:

- SuperMassive E10000 Series
- SuperMassive 9000 Series
- E-Class NSA Series
- NSA 2600 / 3600 / 4600 / 5600 / 6600
- NSA 220 / 220W / 240 / 250M / 250MW / 2400 / 2400MX / 3500 / 4500 / 5000

Configuring a Policy-Based VPN

To configure a policy-based VPN between the Dell SonicWALL Firewall and Windows Azure, perform the following tasks on each side of the deployment (Windows Azure and SonicOS), then test the connectivity between them:

- Windows Azure Configuration Tasks
  1. Creating a Virtual Network
  2. Define the SonicWALL Network
  3. Configure a Virtual Network Address
  4. Create a Virtual Network Gateway
- SonicWALL Configuration Tasks
  1. Create an Address Object for the Virtual Network
  2. Create a Policy-Based VPN
- Test the Connectivity
**Windows Azure Configuration Tasks**
Perform the following tasks in the Windows Azure Management Portal.

**Creating a Virtual Network**
2. In the left-hand navigation menu, click Networks.
3. In the bottom left-hand corner of the screen, click New.

   ![NEW menu display](image)

   The “NEW” menu displays:

   ![NEW menu](image)

4. Click Networks > Virtual Network > Custom Create.
5. On the Virtual Network Details page, enter the following information:
   - **Name** – Name your virtual network.
   - **Affinity Group** – Select an affinity group from the dropdown if you already created one, or create a new one.
   - **Region** – Select a region. This option only appears if you create a new affinity group.
   - **Affinity Group Name** – Name the new affinity group. This option only appears if you create a new affinity group.

6. Click the **Right Arrow** button to continue to the next page.
Define the SonicWALL Network

The “DNS Servers and VPN Connectivity” page displays:

7. Click the **Configure site-to-site VPN** checkbox.
   For the purpose of this TechNote we skip entering the DNS server name or the IP address. For more information about the settings on this page, refer to this MSN article on **DNS Servers and VPN Connectivity**.

8. Click the **LOCAL NETWORK** drop-down menu and either select a network (if it has been created already) or select **Specify a New Local Network**. The Local network here would be the network behind the Dell SonicWALL Firewall.

9. Click on the **Right Arrow** button to proceed to the next page.
The “Site-to-Site Connectivity” page displays:

10. Enter the following information:
   - **Name** – The name you want to call your local network site. This is the network behind the Dell SonicWALL Firewall.
   - **VPN Device IP Address** – This is the WAN IPv4 address of the Dell SonicWALL Firewall. **Note**: The firewall cannot be located behind a NAT device.

   The **Address Space** (including **Starting IP** and **CIDR**) is the internal network behind the Dell SonicWALL Firewall. You can add additional networks behind the Dell SonicWALL Firewall by clicking the **add address space** button. For more information about the settings on this page, see Site-To-Site Connectivity.

11. Click on the **Right Arrow** button to proceed to the next page.
### Configure a Virtual Network Address

The "Virtual Network Address Spaces" page displays:

<table>
<thead>
<tr>
<th>ADDRESS SPACE</th>
<th>STARTING IP</th>
<th>CIDR (ADDRESS COUNT)</th>
<th>USABLE ADDRESS RANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.0.0/24</td>
<td>172.16.0.0</td>
<td>/24 (256)</td>
<td>172.16.0.0 - 172.16.0.255</td>
</tr>
</tbody>
</table>

**Note:** Address space must be a private address range, specified in CIDR notation. For Example, 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 (as specified by RFC 1918). For more information about the settings on this page, see Virtual Network Address Spaces page in About Configuring a Virtual Network using the Management Portal.

12. Enter the virtual network name in the cloud.

13. Click the **STARTING IP** drop-down menu, and then enter the network ID (private address range).

14. Click the **CIDR** drop-down menu, and then select the desired subnet bit.

The "add gateway subnet" will be automatically populated based on the address space entered above. Microsoft runs a gateway service to enable cross-premises connectivity. To this end, they require 2 IP addresses from the virtual network to enable routing between the physical premises and the cloud. At least a /29 subnet must be specified from which they can pick IP addresses for setting up routes.

15. Click the **Checkmark** button to create your network.
After your virtual network is created, the Management Portal > Networks page displays the Status as “Created”:

At this point in the configuration, a virtual network is created in the cloud and a remote network is specified (the Dell SonicWALL network). To view the configuration details, click on the name of the virtual network (in this case MyCloud) in the NAME column. A dashboard displays, click CONFIGURE to view the details:
Create a Virtual Network Gateway

16. Click DASHBOARD.

17. Click the CREATE GATEWAY button, and then select Static Routing.

18. When prompted to confirm the gateway creation, click YES. Depending on your connection, it may take about 15 minutes for the gateway to be created.
The updated DASHBOARD page displays:

![DASHBOARD Page Screenshot]

The public facing IPv4 address will not be generated until the gateway has been created. Once the gateway is created, you will be able to see the public facing IPv4 address of your virtual network under GATEWAY IP ADDRESS. This IP address must be entered under IPsec Primary Gateway Name or Address in the SonicWALL.

**Note:** The gateway IP address may change if the gateway is deleted and recreated.
**SonicOS Configuration Tasks**

Perform the following in the SonicOS Management Interface of your Dell SonicWALL appliance:

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

1. Navigate to the **Network > Address Objects** page.
2. Click the **Add…** button to create a new Address Object.

The "Add Address Object" window displays:

![Add Address Object Window](image)

**Note**: The information displayed in this screenshot is for example only, and may vary depending on your network.

3. Enter the address object information in the text-fields. This needs to be the same information that was previously entered/configured in the Windows Azure Management Portal.
4. Click the **OK** button.
Create a Policy-Based VPN

5. Login to the SonicOS Management Interface as an administrator.
6. Navigate to the VPN > Settings page.
7. Click the Add… button.

The “VPN Policy” pop-up window displays:

8. Enter the following information:
   - Policy Type – Select Site to Site from the drop-down menu.
   - Authentication Method – select the desired method.
   - Name – Enter a name for the policy (we are using Azure in this example).
   - IPSec Primary Gateway Name or Address – Enter the GATEWAY IP ADDRESS displayed on the “Virtual Network” page of the Windows Azure Management Portal.
   - Shared Secret – This is auto-generated by Windows Azure. Copy it from the Windows Azure Virtual Network dashboard, under Manage Key, and then enter it into this text-field.
9. Click the **Network** tab.

10. Click the **Choose local network from list** radio button, and then select the desired local network (this may vary depending on your network, we are using the **X0 Subnet** in this as an example).

    **Note**: This needs to be the same local network that was previously entered in the Azure Management Portal under the **Starting IP** text-field. Please refer to step 13 in the "Windows Azure Configuration Tasks" section to obtain this IP address.

11. Click the **Choose destination network from list** radio button, and then select **Azure Network** from the drop-down menu.

![Network Settings](image)

12. Click the **Proposals** tab.
13. Click the **Exchange** drop-down menu, and then select **Main Mode**.

Windows Azure supports only Main Mode for static-routing site to site VPN. For more information about the Proposals supported in Windows Azure, see About VPN Devices for Virtual Network.

14. Click the **Advanced** tab.

15. Click the **VPN Policy bound to** drop-down menu, and then select the appropriate interface (the WAN interface on the SonicWALL Security Appliance). For example: Interface X1.

16. Click the **OK** button.
**Test the Connectivity**

Now that we have completed the configuration on both sides, it is time to initiate the VPN connection.

1. In the Windows Azure Management Portal, navigate to **Networks**, and then click on your virtual network to go to its Dashboard page.

2. At the bottom of this page, click on **CONNECT**.

3. Log into the SonicOS management interface, and navigate to the **VPN > Settings** Page.

In the VPN Policies table, the VPN will show as connected:
TechNote

It may take a while for the VPN tunnel to show as connected in the Windows Azure Management Portal. Once the tunnel is established, the portal will look like this:

4. To test traffic flow from the Dell SonicWALL side to the Azure cloud, perform either of the following:
   - Try to establish an RDP connection to a 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 Virtual Machine (VM) in the Azure cloud will have inbound ICMP blocked by Windows Firewall and needs to be enabled using this command: `netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any dir=in action=allow`
Configuring a Route-Based VPN

To configure a route-based VPN between the Dell SonicWALL Firewall and Windows Azure, perform the following tasks on each side of the deployment (Windows Azure and SonicWALL), then test the connectivity between them.

- **Windows Azure Configuration Tasks**
  1. Creating a Virtual Network
  2. Define the SonicWALL Network
  3. Configure a Virtual Network Address
  4. Create a Virtual Network Gateway

- **SonicWALL Configuration Tasks**
  1. Create a Route-Based VPN
  2. Create an Address Object for the Virtual Network
  3. Create a Static Route Policy

  Note: While SonicOS supports dynamic routing protocols over VPN tunnels, Windows Azure dynamic routing VPN is currently in preview mode and does not support dynamic routing protocols. Until this is supported, routing must be configured manually using static routes.

- **Test the Connectivity**

**Windows Azure Configuration Tasks**

Perform the following tasks in the Windows Azure Management Portal.

**Creating a Virtual Network**

2. In the left-hand navigation menu, click Networks.
3. In the bottom left-hand corner of the screen, click New.
The “NEW” menu displays:

4. Click Networks > Virtual Network > Custom Create.

The “Create A Virtual Network” wizard displays:

5. On the Virtual Network Details page, enter the following information:
   - Name – Name your virtual network.
   - Affinity Group – Select an affinity group from the dropdown if you already created one, or create a new one.
   - Region – Select a region. This option only appears if you create a new affinity group.
   - Affinity Group Name – Name the new affinity group. This option only appears if you create a new affinity group.

6. Click the Right Arrow button to continue to the next page.
Define the SonicWALL Network
The “DNS Servers and VPN Connectivity” page displays:

7. Click the **Configure site-to-site VPN** checkbox.
   For the purpose of this article we skip entering the DNS server name or the IP address. For more information about the settings on this page, refer to this MSN article on DNS Servers and VPN Connectivity.

8. Click the **LOCAL NETWORK** drop-down menu and either select a network (if it has been created already) or select **Specify a New Local Network**. The Local network here would be the network behind the Dell SonicWALL Firewall.

9. Click on the **Right Arrow** button to proceed to the next page.
The “Site-to-Site Connectivity” page displays:

10. Enter the following information:

- **Name** – The name you want to call your local network site. This is the network behind the Dell SonicWALL Firewall.

- **VPN Device IP Address** – This is the WAN IPv4 address of the Dell SonicWALL Firewall. **Note**: The firewall cannot be located behind a NAT device.

  The **Address Space** (including **Starting IP** and **CIDR**) is the internal network behind the Dell SonicWALL Firewall. You can add additional networks behind the Dell SonicWALL Firewall by clicking the **add address space** button. For more information about the settings on this page, see Site-To-Site Connectivity.

11. Click on the **Right Arrow** button to proceed to the next page.
Configure a Virtual Network Address

The “Virtual Network Address Spaces” page displays:

12. Enter the virtual network name in the cloud.  
   **Note:** Address space must be a private address range, specified in CIDR notation 10.0.0.0/8,  
   172.16.0.0/12, or 192.168.0.0/16 (as specified by RFC 1918). For more information about the settings on  
   this page, see Virtual Network Address Spaces page in About Configuring a Virtual Network using the  
   Management Portal.

13. Click the **STARTING IP** drop-down menu, and then enter the network ID (private address range).

14. Click the **CIDR** drop-down menu, and then select the desired subnet bit.

   The “add gateway subnet” will be automatically populated based on the address space entered above.  
   Microsoft runs a gateway service to enable cross-premises connectivity. To this end, they require 2 IP  
   addresses from the virtual network to enable routing between the physical premises and the cloud. At least  
   a /29 subnet must be specified from which they can pick IP addresses for setting up routes.

15. Click the **Checkmark** button to create your network.
After your virtual network is created, the Management Portal > Networks page displays the Status as “Created”:

At this point in the configuration, a virtual network is created in the cloud and a remote network is specified (the Dell SonicWALL network). To view the configuration details, click on the name of the virtual network (in this case MyCloud) in the NAME column. A dashboard displays, click CONFIGURE to view the details:
Create a Virtual Network Gateway

16. Click DASHBOARD.

17. Click the CREATE GATEWAY button, and then select Dynamic Routing.

18. When prompted to confirm the gateway creation, click YES. Depending on your connection, it may take about 15 minutes for the gateway to be created.
The updated DASHBOARD page displays:

Once the gateway has been created, you will be able to see the public facing IPv4 address of your virtual network under GATEWAY IP ADDRESS. This IP address must be entered under IPsec Primary Gateway Name or Address in the SonicOS management interface.
**SonicOS Configuration Tasks**

Perform the following in the SonicOS management interface of the Dell SonicWALL appliance:

**Create a Tunnel Interface VPN**

1. Login to the SonicOS management interface as an administrator.
2. Navigate to the **VPN > Settings** page.
3. Click the **Add...** button.

The “VPN Policy” pop-up window displays:

4. Enter the following information:
   - **Policy Type** – Select **Tunnel Interface** from the drop-down menu.
   - **Authentication Method** – select the desired method.
   - **Name** – Enter a name for the policy (we are using **Azure** in this example).
   - **IPsec Primary Gateway Name or Address** – Enter the GATEWAY IP ADDRESS displayed on the “Virtual Network” page of the Windows Azure Management Portal.
   - **Shared Secret** – This is auto-generated by Windows Azure. Copy it from the Windows Azure Virtual Network dashboard, and then enter it in this text-field.
5. Click the **Proposals** tab.

6. Click the **Exchange** drop-down menu, and then select **IKEv2 Mode**.

   Windows Azure supports only IKEv2 Mode for route-based site to site VPN. For more information about the Proposals supported in Windows Azure, see About VPN Devices for Virtual Network.

7. Click the **Advanced** tab.

8. Click the **VPN Policy bound to:** drop-down menu, and then select **Interface X1**.

9. Click the **OK** button.
Create an Address Object for the Virtual Network

10. Navigate to the **Network > Address Objects** page.
11. Click the **Add...** button to create a new Address Object.

The “Add Address Object” window displays:

12. Enter the following information:
   - **Name** – Enter a name for the Address Object (we are using *Azure Network* 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.
   - **Netmask/Prefix Length** – Enter the netmask.

13. Click the **OK** button.
Create a Static Route Policy

14. Navigate to the **Network > Routing** page.
15. Click the **Add...** button to create a new Route Policy.

The “Add Route Policy” pop-up window displays:

![Add Route Policy](image)

**Note**: The information displayed in this screenshot is for example only, and may vary depending on your network.

16. Enter the route policy information in the text-fields. This needs to be the same information that was previously entered/configured in the Windows Azure Management Portal.
17. Click the **Disable route when the interface is disconnected** checkbox.
18. Click the **Auto-add Access Rules** checkbox.
19. Click the **OK** button.
**Test the Connectivity**

Now that we have completed the configuration on both sides, it is time to initiate the VPN connection.

1. In the Windows Azure Management Portal, navigate to **Networks**, and then click on your virtual network to go to its Dashboard page.
2. At the bottom of this page, click on **CONNECT**.

3. Log into the SonicOS Management Interface, and navigate to the **VPN > Settings** Page.

In the VPN Policies table, the VPN will show as connected:
TechNote

It may take a while for the VPN tunnel to show as connected in the Windows Azure Management Portal. Once the tunnel is established, the portal will look like this:

4. To test traffic flow from the SonicOS side to the Azure cloud, perform 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 will have 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
   ```

Last updated: 10/4/2013