STEP 1. Configuring NU-850C Network Settings

1. NU series support creating **Site-to-Site Route Based VPN tunnels** with Microsoft Azure. The following steps show how to create the tunnel. And now we use NU-850C as a demonstration.


3. If the firmware version of NU-850C is lower than **9.0.1.3**, try to upgrade NU-850C to 9.0.1.3 or higher.

4. Set an external IP of NU-850C and configure on-premise network.

5. The above figure shows network topology in this article.
STEP 2. Configuring the Microsoft Azure Virtual Network

1. Log into Microsoft Azure, and create a Resource group.

2. Create a Virtual Network and Gateway Subnet
   2.1 Type the Name of this Virtual Network and Address space, for example, vnet-1 and 10.10.0.0/16.
   2.2 Create a Subnet in this virtual network. This subnet address (10.10.0.0/24) will be added to our VPN setting of NU-850C.

2.3 After creating Virtual Network, open vnet-1 blade in All Resources. Click Subnets and then add a Gateway Subnet.
STEP 2. Configuring the Microsoft Azure Virtual Network

1. Log into Microsoft Azure, and create a Resource group.

2. Create a Virtual Network and Gateway Subnet
   2.1 Type the Name of this Virtual Network and Address space, for example, vnet-1 and 10.10.0.0/16.
   2.2 Create a Subnet in this virtual network. This subnet address (10.10.0.0/24) will be added to our VPN setting of NU-850C.
   2.3 After creating Virtual Network, open vnet-1 blade in All Resources. Click Subnets and then add a Gateway Subnet.

3. Virtual Network Gateway setup
   3.1 Type the name, for example, vnet-1-gw.
   3.2 Gateway type : VPN
   3.3 VPN type : Route-based
   3.4 SKU : VpnGw1
   3.5 Virtual network : vnet-1

3.6 On the Create virtual network gateway blade, click First IP configuration to create Public IP.

3.7 After deploying, we can get the following result. The Public IP address will be added to our VPN setting of NU-850C.
4. **Local Network Gateway** setup

4.1 Type the name of **Local Network Gateway**, for example, OnpremNetwork1.

4.2 Set the external IP of NU-850C in the **IP address** field.

4.3 Fill the on-premise network in **Address space**.

5. Create the **VPN Connections**.

5.1 Navigate to and open the OnpremNetwork1 blade in **All Resources**. Click **Connections** and add a new one. On the **Add connection** blade, fill in the values we have just set.

5.2 Type **Shared Key (PSK)**, and remember this value which will be added to our VPN setting of NU-850C.
6. Through this step, we get some values which will be used in next step.
   - Remote Network : 10.10.0.0/24
   - Remote Gateway : 13.94.24.101
   - Shared Key (PSK) : 123456abc

**STEP 3. Configuring the NU-850C IPSec Tunnel**

1. Start to create a tunnel. Go to **VPN > IPSec Tunnel**, click **IPSec Tunnel** tab, and Add a new one.

2. Configure the connection
   2.1 Check Enable.
   2.2 Enter a name for this tunnel in **Tunnel Name**, for example, Azure_RouteBased_VPN.
   2.3 Fill the external IP address of NU-850C in **local IP**, and this IP should match the **Local Network Gateway** setting in Azure. You could select the IP you have set in **Network > Interface** from the drop-down list.
   2.4 Fill **Remote Gateway** of Azure in **Remote IP**.
   2.5 In **Local Subnet** section, type on-premise network, and the address space should match the **Local Network Gateway** setting in Azure.
   2.6 In **Remote Subnet** section, type **Remote Network** of Azure.

2.7 In **IKE** section, check **v2**.
   2.8 In **Connection Type** section, check **Main**.
   2.9 In **Preshare Key** text box, type the **Shared Key (PSK)** we have set in Azure.
   2.10 In **ISAKMP** section, there are three drop-down lists. The first one, select **aes128**; the second one, select **sha1**; the third one, select **DH Group 2**. Don’t check **Auto Matching**.
   2.11 In **Local ID** and **Remote ID** section, check **IP Address**.
   2.12 From **IKE SA Lifetime** drop-down list, select **8 Hours**.

4. **Local Network Gateway** setup
   4.1 Type the name of **Local Network Gateway**, for example, OnpremNetwork1.
   4.2 Set the external IP of NU-850C in the **IP address** field.
   4.3 Fill the on-premise network in **Address space**.

5. Create the VPN Connections.
   5.1 Navigate to and open the OnpremNetwork1 blade in **All Resources**. Click **Connections** and add a new one. On the **Add connection** blade, fill in the values we have just set.
   5.2 Type **Shared Key (PSK)**, and remember this value which will be added to our VPN setting of NU-850C.
2.13 In **IPSec** section, there are two drop-down lists. Select **aes128** from the first one, and select **sha1** from the other. **Don't** check **Auto Matching**.

2.14 From **IPSec SA Lifetime** drop-down list, select **1 Hour**.

2.15 Check **Dead Peer Detection**. Select **hold** from the drop-down list. Enter **10** in **Delay** text box and **60** in **Time out** text box.

2.16 Click **Add**.

3. If the connection is established, there is a connected icon in Status field.

**STEP 4. Configuring IPSec Policies**

1. Go to **Policy > Security Policy**, click **IPSec Policy** tab, and **Add** a new one.
2. Create the first policy which allows the outgoing connections from local network to the hosts in Azure network.

2.1 Enter a name for this policy.

2.2 Select the Protocol from the drop-down list. For example, select ALL.

2.3 Select To IPSec from Path drop-down list.

2.4 Select Source from the drop-down list, or click Change To Define to type any address you want to manage. For example, select Any from drop-down list.

2.5 Select Destination from the drop-down list, or click Change To Define to type any address you want to manage. For example, select the name of Azure VPN connection created in the last step from drop-down list.

2.6 Select Service Port or Group from drop-down list, or type other port in the text box. For example, only select User Defined that is to allow any port.

2.7 Select Permit from Action drop-down list.

2.8 Configure Schedule and QoS sections if needed.

2.9 Click Add.
3. Create the second policy which allows the incoming connections from hosts in Azure network to local network.

3.1 Enter a name for this policy.

3.2 Select the Protocol from the drop-down list. For example, select **ALL**.

3.3 Select **IPSec To** from Path drop-down list.

3.4 Select **Source** from the drop-down list, or click **Change To Define** to type any address you want to manage. For example, select the name of Azure VPN connection created in the last step from drop-down list.

3.5 Select **Destination** from the drop-down list, or click **Change To Define** to type any address you want to manage. For example, select **Any** from drop-down list.

3.6 Select **Service Port or Group** from drop-down list, or type other port in the text box. For example, only select **User Defined** that is to allow any port.

3.7 Select **Permit** from Action drop-down list.

3.8 Configure **Schedule** and **QoS** sections if needed.

3.9 **Don’t** check **NAT**.

3.10 Click **Add**.

4. After creating the two policies, they will show in the **IPSec Policy** list.
STEP 5. Testing

1. Create a Virtual Machine in the cloud, and its IP is 10.10.0.4. On the other hand, there is a host 192.168.14.169 in on-premise network. The two hosts ping each other.

1.1 Go to Policy > Security Policy, click Statistics field of first policy, and then pop out a window. In the window, the list shows the ICMP packets sent from 192.168.14.169 to 10.10.0.4.

1.2 Click Statistics field of second policy, and pop out a window. In the window, the list shows the ICMP packets sent from 10.10.0.4 to 192.168.14.169.

2. Return to Microsoft Azure Portal, click All Resources and navigate to the Connection named vnet-1-onprem-Conn. On the vnet-1-onprem-Conn blade, click Overview and open Essentials. And it shows the information about this connection, such as Status, Data in and Data out.