Configure Cisco Catalyst 8000V on Microsoft Azure

The following chapter tells you how to configure your Cisco Catalyst 8000V instance for Microsoft Azure.

Update Route Tables

In Microsoft Azure, all VMs send packets to a hypervisor router, and the hypervisor forwards the packets based on the routing table associated with that subnet.

When a Cisco Catalyst 8000V VM is created, a route table is created for each subnet. For a 2 vNIC Cisco Catalyst 8000V VM, a default route is created for a second (internally facing) subnet that points to the Cisco Catalyst 8000V. All the VMs created on this subnet use the Cisco Catalyst 8000V as the default gateway. For Cisco Catalyst 8000V VMs that have more than two vNICs, you need to define the default routes and apply them to the subnets.

Step 1 Click **Route Tables**.

Expands the Settings pane.

Step 2 Navigate to the Route Tables pane and select the target route table.

Step 3 Click **All Settings**.

Step 4 In the **Settings** pane, click **Routes**.

Add or modify routes.

Update Security Group

A Security Group controls which ports/destinations the hypervisor allows/denies for certain interfaces. When creating a Cisco Catalyst 8000V, a new Security Group is created for the first subnet inbound interface by default. For Cisco Catalyst 8000V virtual machines deployed through this deployment, the following ports are added for inbound internet traffic: TCP 22, UDP 500 and UDP 4500. Use of other ports is denied.

Step 1 Click Network security groups on the left hand side panel.

The Network security groups pane appears, and shows a list of security groups.

Step 2 Click the target network security group.

The system displays the pane that shows the details of the security group.

Step 3 Click **All Settings**.

Step 4 From the **Settings** pane, click **Inbound Security Rules**.

Step 5 From **Network Security Rules**, click **Add** to add additional rules.

Configuring IPsec VPN

The following example shows an IPsec VPN configured for a Cisco Catalyst 8000V instance running on Microsoft Azure.

```
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 0.0.0.0
crypto ipsec transform-set T1 esp-3des esp-md5-hmac
 mode transport
crypto ipsec profile P1
 set transform-set T1
interface Tunnel0
 ip address 3.3.3.1 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 104.45.154.184
 tunnel protection ipsec profile P1
end
!!!! To test, create loop back interface and static route!!!!!
interface Loopback1
 ip address 5.5.5.5 255.255.255.255
end
ip route 6.6.6.6 255.255.255.255 Tunnel0
```

Best Practices and Caveats

1. Cisco recommends that you keep resources in a Resource Group. To clean up all the resources in a group, you can remove the relevant Resource Group.
2. When a Cisco Catalyst 8000V VM is deleted, not all the resources for the VM are deleted (route table, security group, public IP, network interfaces). Subsequently, if you create a new Cisco Catalyst 8000V with the same name as before, the previous resources may be re-used. If you do not want to re-use these resources, choose one of the following actions:
   - Manually remove each resource.
   - Remove the Resource Group containing the individual resources.
   - Create a new Cisco Catalyst 8000V VM with a different name.
3. If you use the deployment template to create a Cisco Catalyst 8000V instance, make sure that the public IP address is configured as static on Microsoft Azure. To do this, in Microsoft Azure, navigate to the public IP address. In the configuration settings, see if the address is shown as Dynamic or Static. Select the **Static** option. Note that the default option is Dynamic.

SSH Connectivity Issues

You may fail to establish an SSH connection to a Cisco Catalyst 8000V on Microsoft Azure after you initially deploy the Cisco Catalyst 8000V, or after you reload or restart the Cisco Catalyst 8000V. In the Azure portal, the Cisco Catalyst 8000V instance is in the running state. The following three scenarios suggest workarounds for when you fail to connect using SSH.

Scenario 1. Attempted SSH access soon after booting up Cisco Catalyst 8000V

You may fail to establish an SSH connection if you tried to gain access to the Cisco Catalyst 8000V soon after boot up. After starting the deployment of the instance, it takes about 5 minutes for SSH connectivity to become available.

Scenario 2. Binding problem in the Microsoft Azure Infrastructure

Microsoft Azure support recommends that you perform the following steps:

1. On the Cisco Catalyst 8000V interface that has a public IP address, reassign the private IP address to a new static IP address within the subnet.
2. Open the PowerShell in the Azure portal.
3. Update the ARM VM.

   Refer to this Azure documentation: https://docs.microsoft.com/en-us/powershell/module/azurerm.compute/update-azurermvm?view=azurermps-5.6.0.
4. In the powershell, enter the following commands:

   $vm = Get-AzureRmVM -Name "reload-lnx" **-ResourceGroupName** "reload-rg"

   Update-AzureRmVM -VM $vm -ResourceGroupName "reload-rg"
5. Reset the network interface to which the public IP address is attached.

For further information on resetting the network interface, see: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/reset-network-interface.

6. Select **VM** > **Networking** and select the Network Interface.
7. Go to **IP configurations** and select the IP name.
8. If the private IP address that is assigned to the interface is statically configured, write down the address for use in step **13**.
9. Under **Assignment**, click **Static**.
10. In the IP address field, use an available IP address. Choose an available IP address within the subnet to which the network interface is connected.
11. Click **Save** and wait for the save to complete.
12. Retry connecting to the router using SSH.
13. After you add (or change) a static IP address and gain access to the VM, if the IP address that you originally assigned to this interface (see step **8.**) is statically configured, you can either change the IP address from static to dynamic, or you can reconfigure the IP address to the original address (the address you noted in step **8**).

Scenario 3. Misconfiguration of idle terminal timeouts

When you start an SSH session to the Cisco Catalyst 8000V, ensure that you do not configure the terminal VTY timeout as infinite - do not configure: `exec-timeout 0 0`. Use a non-zero value for the timeout; for example, `exec-timeout 4 0`. This command specifies a timeout of four minutes and zero seconds.

The reason why the `exec-timeout 0 0` command causes an issue is as follows:

Azure enforces a timeout for the console idle period of between 4 and 30 minutes. When the idle timer expires, Azure disconnects the SSH session. However, the session is not cleared from the point of view of the Cisco Catalyst 8000V as the timeout was set to infinite by the `exec-timeout 0 0` configuration command. The disconnection causes a terminal session to be orphaned. The session in the Cisco Catalyst 8000V remains open indefinitely. If you try to establish a new SSH session, a new virtual terminal session is used. If this pattern continues to occur, the number of allowed simultaneous terminal sessions is reached and no new sessions can be established.

In addition to configuring the `exec-timeout` command correctly, it is also a good practice to delete idle virtual terminal sessions using the commands that are shown in the following example:

```
Router# show users
Line User Host(s) Idle Location
2 vty 0 cisco idle 00:07:40 128.107.241.177
* 3 vty 1 cisco idle 00:00:00 128.107.241.177

Router# clear line 2
```

If the workarounds in the preceding scenarios are ineffective, as a last resort, you can restart the Cisco Catalyst 8000V instance from the Azure portal.