Configuring CSR1000v on Microsoft Azure

The following chapter tells you how to configure your CSR1000v instance for Microsoft Azure.

Note The Microsoft Azure serial console is supported only for Cisco CSR 1000v routers running on 16.9.1s release and later. If you want to use the serial console, upgrade the CSR 1000v to a 16.19.1s release or later

To configure your CSR1000v instance, see the following sections:

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 CSR 1000v VM is created, a route table is created for each subnet. For a 2 vNIC Cisco CSR 1000v VM, a default route is created for a second (internally facing) subnet that points to the CSR. All the VMs created on this subnet use the Cisco CSR 1000v as the default gateway. For Cisco CSR 1000v VMs that have more than two vNICs, you need to define the default routes and apply them to the subnets.

SUMMARY STEPS

1. Click **Route tables**
2. Navigate to the "Route tables" pane and select the target route table.
3. Click **All Settings**
4. In the Settings pane, click **Routes**

DETAILED STEPS

	Command or Action	Purpose
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 CSR 1000v, a new Security Group is created for the first subnet inbound interface by default. For Cisco CSR1000v 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.

SUMMARY STEPS

1. Click Network security groups on the left hand side panel.
2. Click the target network security group.
3. Click **All Settings**.
4. Click Inbound security rules.
5. Click **Add** (under "Network security groups") to add additional rules.

DETAILED STEPS

	Command or Action	Purpose
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.	A pane appears that shows the details of the security group.
Step 3	Click **All Settings**.	The Settings pane appears.
Step 4	Click Inbound security rules.	
Step 5	Click **Add** (under "Network security groups") to add additional rules.	

Configuring IPsec VPN for a Cisco CSR 1000v on Microsoft Azure

This example shows an IPsec VPN configured for Cisco CSR 1000v 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
```

Upgrading a Cisco IOS XE Image on Microsoft Azure

This procedure shows how to upgrade the image on a running CSR 1000v (Cisco IOS XE Fuji 16.7.1 and later).

Before you begin

To upgrade a Cisco CSR 1000v image for a Cisco CSR 1000v running in Microsoft Azure, the current version of Cisco IOS XE running on the Cisco CSR 1000v must be Cisco IOS XE Fuji 16.7.1 or later.

Note (Cisco IOS XE Everest 16.6 and earlier) On Microsoft Azure, you cannot use the Cisco CSR 1000v .bin file to upgrade a Cisco CSR1000v instance. You must re-deploy a new instance from the Microsoft Azure Portal and migrate your configuration and licenses.

Note You cannot downgrade a Cisco CSR 1000v image on Microsoft Azure to Cisco IOS XE Everest 16.6.2 or earlier. For example, if you are running Cisco IOS XE Fuji 16.7.1 or later you must not downgrade to Cisco IOS XE Everest 16.6.2 or earlier.

Note To upgrade or downgrade a Cisco CSR 1000v image on Microsoft Azure, you need to expand the `.bin` file and use `packages.conf` to upgrade to the new version.

Note The only currently available downgrade for a Cisco IOS XE Gibralter 16.10.1 image is to Cisco IOS XE Fuji 16.9.2. You cannot downgrade a Cisco CSR 1000v image on Microsoft Azure from Cisco IOS XE Gibralter 16.10 to Cisco IOS XE Fuji 16.9.1 or earlier.

Note If you are upgrading from an earlier release to 16.10.1 to achieve Accelerated Networking performance, ensure that you select the AZN variant of the 16.10.1 .bin image. The AZN variant contains the string "azn" in the filename. For example, `csr1000v-universalk9azn.2018-12-03_23.12_abcd4.SSA.bin`.

Check the version of Cisco IOS XE that is running on the Cisco CSR 1000v by using the `show version` command. Example:

```
Router# show version
Cisco IOS XE Software, Version 2017-11-08_14.44_user4
Cisco IOS Software [Fuji], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental
 Version 16.8.2017110
```

Procedure

	Command or Action	Purpose
Step 1	**scp** *upgrade-image azure-username@csr-public-ip-address:copied-upgrade-image* **Example:** The public IP address of the Cisco CSR 1000v used in the following example is 207.46.130.0. `scp UpgradeImage.bin azureusr1@207.46.130.0:upgrade.bin`	Copy the new image to the CSR 1000v (boot flash memory). You can choose any name for the copy of the image in bootflash; for example, `upgrade.bin`. **Note** If you are upgrading to Cisco IOS XE 16.10.1 or later, use a Microsoft Azure Accelerated Networking (AN) .bin image from www.cisco.com. For example: csr1000v-universalk9azn.16.10.x.SSA.bin

Step 2	**request platform software package expand file bootflash:upgrade.bin to bootflash:upgrade/**
	Example:
	`Router# request platform software package expand file bootflash:upgrade.bin to bootflash:upgrade/`
	`Nov 8 03:25:34.412`
	`%INSTALL-5-OPERATION_START_INFO: R0/0: packtool: Started expand package bootflash:upgrade.bin`
	`Verifying parameters`
	`Expanding superpackage bootflash:upgrade.bin`
	`Validating package type`
	`Copying package files`
	`SUCCESS: Finished expanding all-in-one software package.`
		Expand the image that is in boot flash memory.
		Note If you have already performed an upgrade on this CSR instance before, use a different directory name when you perform the upgrade the second time. For example, if you used the `request platform software package expand file bootflash:upgrade.bin to bootflash:upgrade/` command when you performed the upgrade the first time, this command expands the bin file in the 'upgrade' directory of the blootflash and places the packages.conf file in the upgrade directory.
		When you perform an upgrade anytime after, ensure that you use a different directory name. For example, your upgrade command would read `request platform software package expand file bootflash:upgrade2.bin to bootflash:upgrade2/`. Note that the directory name is `upgrade2` in this instance.

Step 3	**configure terminal**	Enter global configuration mode.

	Command or Action	Purpose
Step 4	**boot system bootflash:upgrade/packages.conf** **Example:** The following example shows how to correctly enter a boot system entry: `Router(config)# boot system bootflash:upgrade/packages.conf`	Add a boot system entry to the `packages.conf` file that was generated in step 2. For example, add the boot system entry to the `/bootflash/upgrade/packages.conf` file as shown in the example on the left. **Note** Do **not** add the boot system entry like this: `boot system bootflash:upgrade.bin`. This command tells the Cisco CSR 1000v to boot from `upgrade.bin`. However, the CSR 1000v boot fails if the file size of `upgrade.bin` is greater than the low memory size that is allowed by GRUB in Microsoft Azure. **Note** Ensure that you point the boot system command entry to the `packages.conf` file expanded in the upgrade directory as mentioned in step 2. You must use the same directory name that you have specified in step 2.

Step 5	**end**
	Example:
	`Router(config)# end`
	`Router#`
		Exit global configuration mode and return to privileged EXEC mode.

Step 6	**show run | sec boot**
	Example:
	`Router# show run | sec boot`
	`boot-start-marker`
	`boot system bootflash:upgrade/packages.conf`
	`boot-end-marker`
	`diagnostic bootup level minimal`
		Verify the boot system entry.

Step 7	**copy running-configuration startup-configuration**
	Example:
	`Router# copy running-configuration startup-configuration`
	`Building configuration`
	`...`
	`[OK]`
		Save the configuration.

Step 8	Reload the router.	

Deploying CSR 1000v on Microsoft Azure vs Amazon Web Services

The differences between deploying Cisco CSR 1000v on Microsoft Azure and Amazon Web Services (AWS) are shown in the following table:

Table 1: Comparing Cisco CSR 1000v on Microsoft Azure and Amazon Web Services

Function	Cisco CSR 1000v on Microsoft Azure	Cisco CSR1000v on AWS
Number of Interfaces	1, 2, 4, or 8 Interfaces	3 or more Interfaces
Multiple IP addresses	Multiple IP addresses per vNIC	Multiple IP addresses per vNIC
GRE tunnel	GRE tunnel is unsupported	GRE tunnel is supported
Redundancy	Routing Redundancy is supported through 2 CSR instances	Routing Redundancy is supported through 2 CSR instances
Attachment/Detachment of interface on the running Cisco CSR 1000v	Not supported	Supported
Overlapping IP subnet	Supports overlapping IP subnets in different virtual networks.	Support overlapping IP subnet in different VPC

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 CSR 1000v VM is deleted, not all the resources for the VM are deleted (route table, security group, public IP, network interfaces). Then, if you create a new Cisco CSR 1000v 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 individual resource.
   - Remove the Resource Group containing the individual resources.
   - Create a new Cisco CSR 1000v with a different name.
3. If you use the deployment template to create a Cisco CSR 1000v, make sure that the public IP address is configured as static on Microsoft Azure. (In Microsoft Azure, navigate to the public IP address and in the configuration settings, see if the address is shown as Dynamic or Static. Ensure that Static is selected (the default is Dynamic).

SSH Connectivity Issues

You may fail to establish an SSH connection to a Cisco CSR 1000v on Microsoft Azure after you initially deploy the Cisco CSR 1000v, or after you reload or restart the Cisco CSR 1000v. In the Azure portal, the Cisco CSR 1000v 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 CSR 1000v.

You may fail to establish an SSH connection if you tried to gain access to the Cisco CSR 1000v soon after boot up. After starting the deployment of a CSR 1000v, 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 CSR 1000v 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 was originally assigned to this interface (see step **8.**) was 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 CSR 1000v, 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 CSR 1000v, 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 CSR 1000v 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:

```
CSRA# 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

CSRA# clear line 2
```

If the workarounds in the preceding scenarios are ineffective, as a last resort, you can restart the Cisco CSR 1000v in the Azure portal.

Other Related Resources

DMVPN is supported on Microsoft Azure and AWS. The configuration for Microsoft Azure is similar to AWS. For further information, see the following white paper:

Extending Your IT Infrastructure Into Amazon Web Services Using Cisco DMVPN and the Cisco Cloud Services Router 1000V Series (PDF)