Configure L2 Extension for Public Cloud

This chapter describes how to enable enterprise and cloud providers to configure an L2 extension for public clouds with CSR 1000V instances using LISP. Use the command-line interface to extend a layer 2 domain between your public cloud network and the enterprise network.

The following are some of the terminologies and concepts that you should be aware before you configure the LISP Layer 2 Extension:

- **Locator/ID Separation Protocol (LISP)**: LISP is a network architecture and protocol that implements the use of two namespaces instead of a single IP address:
  - Endpoint identifiers (EIDs) - assigned to end hosts.
  - Routing locators (RLOCs) - assigned to devices (primarily routers) that make up the global routing system.
- **LISP-enabled virtualized router**: A virtual machine or appliance that supports routing and LISP functions, including host mobility.
- **Endpoint ID (EID)**: An EID is an IPv4 or IPv6 address used in the source and destination address fields of the first (most inner) LISP header of a packet.
- **Routing locator (RLOC)**: The IPv4 or IPv6 addresses that are used to encapsulate and transport the flow between the LISP nodes. An RLOC is the output of an EID-to-RLOC mapping lookup.
- **Egress Tunnel Router (ETR)**: An ETR is a device that is the tunnel endpoint and connects a site to the LISP-capable part of a core network (such as the Internet), publishes EID-to-RLOC mappings for the site, responds to Map-Request messages, and decapsulates and delivers LISP-encapsulated user data to the end systems at the site. During operation, an ETR sends periodic Map-Register messages to all its configured map servers. These Map-Register messages contain all the EID-to-RLOC entries for the EID-numbered networks that are connected to the ETR’s site.
- **Ingress Tunnel Router (ITR)**: An ITR is a device that is the tunnel start point. An ITR is responsible for finding EID-to-RLOC mappings for all traffic destined for LISP-capable sites. When the ITR receives a packet destined for an EID, it first looks for the EID in its mapping cache. If the ITR finds a match, it encapsulates the packet inside a LISP header with one of its RLOCs as the IP source address and one of the RLOCs from the mapping cache entry as the IP destination. The ITR then routes the packet normally.
- **xTR**: A generic name for a device performing both Ingress Tunnel Router (ITR) and Egress Tunnel Router (ETR) functions.

- **PxTR**: The point of interconnection between an IP network and a LISP network, playing the role of ITR and ETR at this peering point.
- **Map-Server (MS)**: An MS is a LISP Infrastructure device that LISP site ETRs register to with their EID prefixes. An MS implements part of the distributed LISP mapping database by accepting registration requests from its client egress tunnel routers (ETRs), aggregating the successfully registered EID prefixes of those ETRs, and advertising the aggregated prefixes into the alternative logical topology (ALT) with border gateway protocol (BGP).

  In a small private mapping system deployment, an MS may be configured to stand alone (or there may be several MSs) with all ETRs configured to register to each MS. If more than one, all MSs have full knowledge of the mapping system in a private deployment.

  In a larger or public mapping system deployment, an MS is configured with a partial mesh of generic routing encapsulation (GRE) tunnels and BGP sessions to other map server systems
- **Map-Resolver (MR)**: An MR is a LISP Infrastructure device to which the ITRs send LISP Map-Request queries when resolving EID-to-RLOC mappings. MRs receive the request and select the appropriate map server

For detailed overview information on LISP and the terminologies, see Locator ID Separation Protocol Overview.

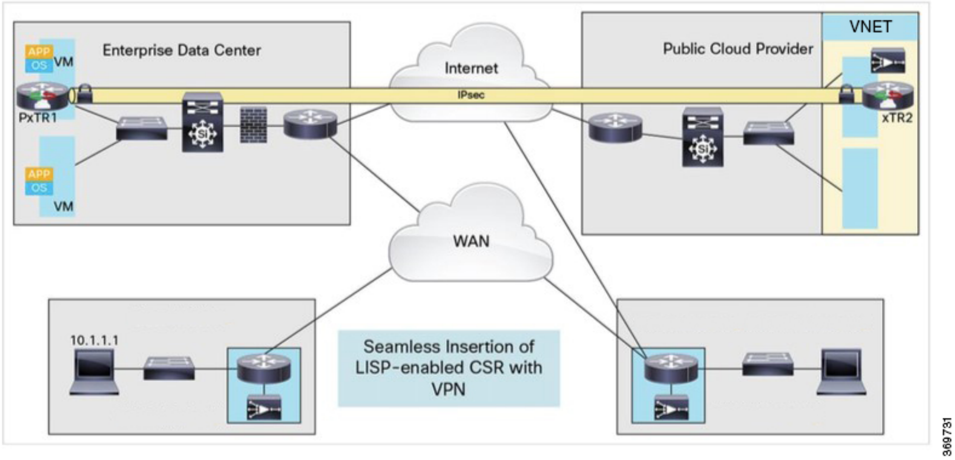
Information about Configuring LISP Layer 2 Extension

You can deploy Cisco CSR 1000v instances on public, private, and hybrid clouds. When enterprises move to a hybrid cloud, they need to migrate the servers to the cloud without making any changes to the servers. Enterprises may want to use the same server IP address, subnet mask, default gateway configurations, and their own IP addressing scheme in the cloud, and not be limited by the addressing scheme of the cloud provider infrastructure.

To fulfill this requirement, you can use LISP, which is an architecture that allows you to separate the location (enterprise data center or public cloud) and the identity (server IP address) so that you can create new servers on the cloud with the same IP address. In the LISP architecture, the endpoint ID-to-router locator (EID-to-RLOC) mapping of the server is updated to reflect the new location that is moved to the cloud. Further, no changes are required to the end systems, users, or servers because LISP handles the mapping between the identity and the location.

LISP operates as an overlay, encapsulating the original packet from the server into a User Datagram Protocol (UDP) packet along with an additional outer IPv4 or IPv6 header. This encapsulation holds the source and destination router locators and allows the server administrators to address the server in the cloud according to their own IP addressing scheme, independent of the cloud provider's addressing structure.

From the 16.12.1 release, you can configure Layer 2 Extension on CSR 1000v instances running on Microsoft Azure, where the CSR 1000v instance acts as the bridge between the enterprise data center and the public cloud. By configuring the Layer 2 Extension, you can extend your Layer 2 networks in the private data center to a public cloud to achieve host reachability between your site and the public cloud. You can also enable the migration of your application workload between the data center and the public cloud.



Benefits

- Move the Public IP addresses between different geographic locations or split them between different public clouds. In either case, the LISP IP-Mobility solution provides optimal routing between clients on the Internet and the public IP address that has moved, regardless of the location. To know more about achieving IP mobility for the Azure cloud, see Achieving IP Mobility.
- Carry out data migration with ease and optimize the workload IP address in your network. Usually, IP address changes cause complexity and additional delays in a solution. By using L2 extension for cloud, you can migrate workloads while retaining the original IP address without any network constraints. To learn more about this use case, see Data Migration Use Case.
- Virtually add a VM that is on the provider site to facilitate cloud bursting to virtually insert a VM in the Enterprise server while the VM runs on the provider site.
- Provide backup services for partial disaster recovery and disaster avoidance.

Prerequisites for configuring LISP Layer 2 Extension

- Ensure that the underlay for your solution is ready before you configure the L2 Extension.
- Since clouds do not support Address Resolution Protocol (ARP), and the cloud infrastructure is not aware of the hosts in the remote site, you must add a virtual IP to help the cloud route the packets appropriately to the edge router. To add a virtual or alias IP, see Add an IP address for an Azure interface.
- Each CSR 1000V router must be configured with one external IP address. In this case, an IPsec tunnel is built either between the IP addresses of the two CSR 1000v instances, or between the CSR 1000v instance and the ASR1k device. Ensure that the IPsec tunnel has a private address.
- Ensure that the IPsec tunnel is working between the IP address of the two CSR 1000v instances or between the CSR 1000v instance and the ASR1k device.
- Depending on your solution, ensure that a ping is successful between: the two CSR 1000v instances, between a CSR 1000v and an ASR1k, and between the VMs and the hosts.

Restrictions for configuring LISP Layer 2 Extension

- If you move a host from the data center to the cloud or vice-versa, you must first add or remove the secondary address from the virtual IP table in the cloud.
- If you move a VM to the cloud, you must initiate packets to the CSR 1000v instance so that the CSR 1000v device realizes that the VM is now added from the data center to the cloud.
- For the 16.12 release, High Availability does not work with the L2 Extension functionality.
- Azure supports a maximum of 256 IPs. The maximum number of hosts on the remote site or the data center is thus 256.

How to configure LISP Layer 2 Extension

To configure the L2 extension functionality, you must first deploy the CSR 1000v instance on Microsoft Azure and configure the instance as an xTR. You must then configure the mapping system to complete the deployment.

The LISP site uses the CSR 1000v instance configured as both an ITR and an ETR (also known as an xTR) with two connections to upstream providers. The LISP site then registers to the standalone device that you have configured as the map resolver/map server (MR/MS) in the network core. The mapping system performs LISP encapsulation and de-encapsulation of the packets that are going to the migrated public IPs within Azure. Optionally, for traffic that is leaving Azure, whenever a route to the destination is not found on the CSR routing table, the CSR 1000v instance routes that traffic through the PxTR at the enterprise data center.

Perform the following steps to enable and configure the LISP xTR functionality when using a LISP map server and map resolver for mapping services:

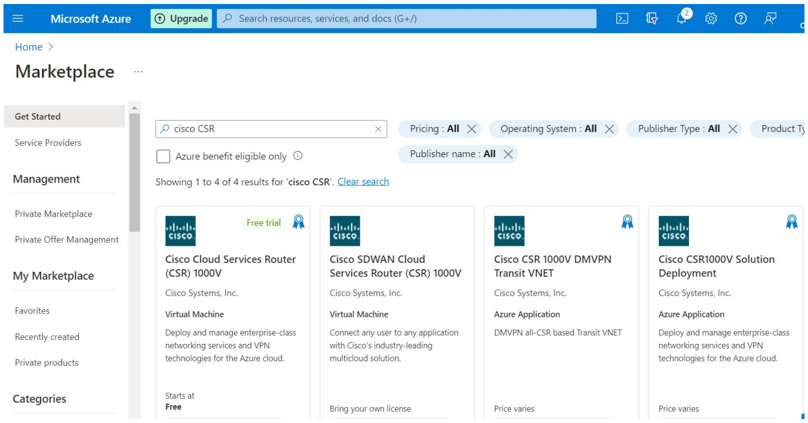
Deploy a CSR 1000v with Multiple Interfaces on Microsoft Azure

Perform the following steps to deploy a Cisco CSR1000V instance with multiple interfaces on Microsoft Azure.

Step 1 Log in to the Microsoft Azure Marketplace.

Step 2 On the Search bar, search for `Cisco CSR`.

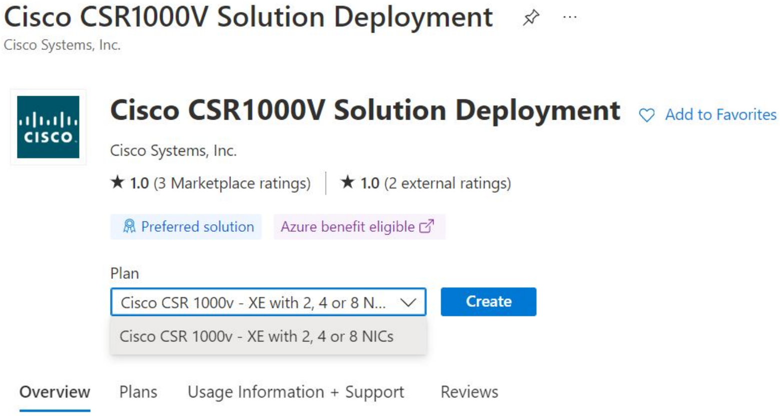
Step 3 The system displays the various offerings under Cisco CSR1000V. Select **Cisco CSR1000V Solution Deployment**, and click **Create**.



Showing 1 to 4 of 4 results for 'cisco CSR'. Clear search

Free trial			
Cisco Cloud Services Router (CSR) 1000V	Cisco SDWAN Cloud Services Router (CSR) 1000V	Cisco CSR 1000V DMVPN Transit VNET	Cisco CSR1000V Solution Deployment
Cisco Systems, Inc.	Cisco Systems, Inc.	Cisco Systems, Inc.	Cisco Systems, Inc.
Virtual Machine	Virtual Machine	Azure Application	Azure Application
Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.	Connect any user to any application with Cisco's industry-leading multicloud solution.	DMVPN all-CSR based Transit VNET	Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.
Starts at Free	Bring your own license	Price varies	Price varies

Step 4 In the Cisco CSR1000V Solution Deployment page, the **Cisco CSR 1000v - XE with 2, 4 or 8 NICs** solution is available in the **Plan** drop-down field. Click **Create**.


Cisco CSR1000V Solution Deployment
Cisco Systems, Inc.
Cisco CSR1000V Solution Deployment
Add to Favorites
Cisco Systems, Inc.
★ 1.0 (3 Marketplace ratings)
★ 1.0 (2 external ratings)
Preferred solution
Azure benefit eligible
Plan
Cisco CSR 1000v - XE with 2, 4 or 8 N...
Create
Cisco CSR 1000v - XE with 2, 4 or 8 NICs
Overview
Plans
Usage Information + Support
Reviews

Step 5 In the Basics page, enter the following details:

a) **Subscription Name**: The name of your subscription. A default subscription name is available. You can modify the subscription name, if required.

b) **Resource Group**: A container that holds the resources for your solution. From this drop-down field, choose either **Create New** or **Select Existing**. You can create a Cisco CSR 1000V instance only in a new Resource Group or in a completely empty existing resource group. To remove a Resource Group, first delete the Cisco CSR 1000V VM and then delete the Resource Group.

c) **Region**: The region or location where you are performing this deployment. From this drop-down field choose your region.

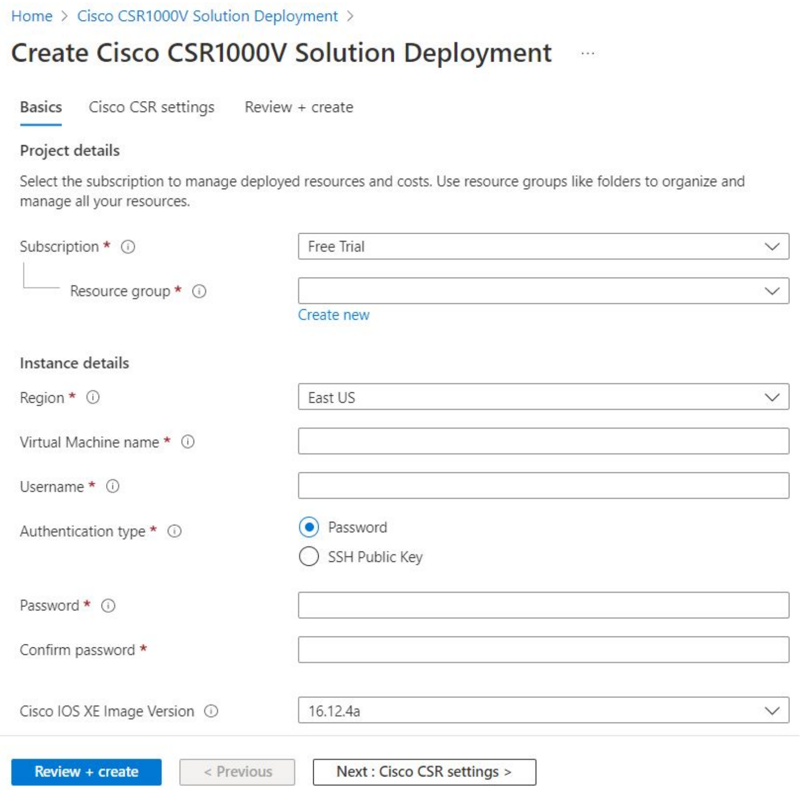
d) **Virtual Machine Name**: The name of the cloud-based network used by Microsoft Azure to represent a private network. Enter a name for the virtual machine.

e) **Username**: The username for your VM using which you can log in to the Cisco CSR 1000V instance. Enter a user name for your VM.

Note For Cisco IOS XE versions 3.16 and 16.4, if you're planning to choose SSH Key as an authentication type, enter the **Username** as `azureuser`.

f) **Authentication type**: The authentication type for the administrator account. You can use a username and password or an SSH key for authentication. If you select the **SSH Key** option, select the **SSH Public Key Source** and provide the **Key Pair Name**. If you select the **Password** opition, enter a password for authentication.

g) **Cisco IOS XE Image Version**: The version of the Cisco IOS XE software. From this drop-down field, choose your Cisco IOS XE version.



Create Cisco CSR1000V Solution Deployment ...

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Free Trial

Resource group * :

Instance details

Region * : East US

Virtual Machine name * :

Username * :

Authentication type * : ● Password ○ SSH Public Key

Password * :

Confirm password * :

Cisco IOS XE Image Version : 16.12.4a

Step 6 Click **Next** and proceed to the Cisco CSR Settings page.

Step 7 In the **Cisco CSR Settings** page, enter the following details:

a) **Number of Network Interfaces in CSR**: The number of network interfaces you want to attach to the VM. From the drop-down list, choose the number of interfaces: 2, 4, or 8.

b) **License Type**: The license type. From this drop-down field, choose either **BYOL** or **PAYG** as the license type.

c) **Managed Disk**: The option that allows you to specify whether you want Azure to manage the disk for you. Select **Enabled**.

d) **Virtual machine size**: The size of the VM to provision. Select the appropriate virtual machine size. Based on the number of interfaces that you are using, select the appropriate virtual machine size. Microsoft Azure supports different image types with different performance expectations.

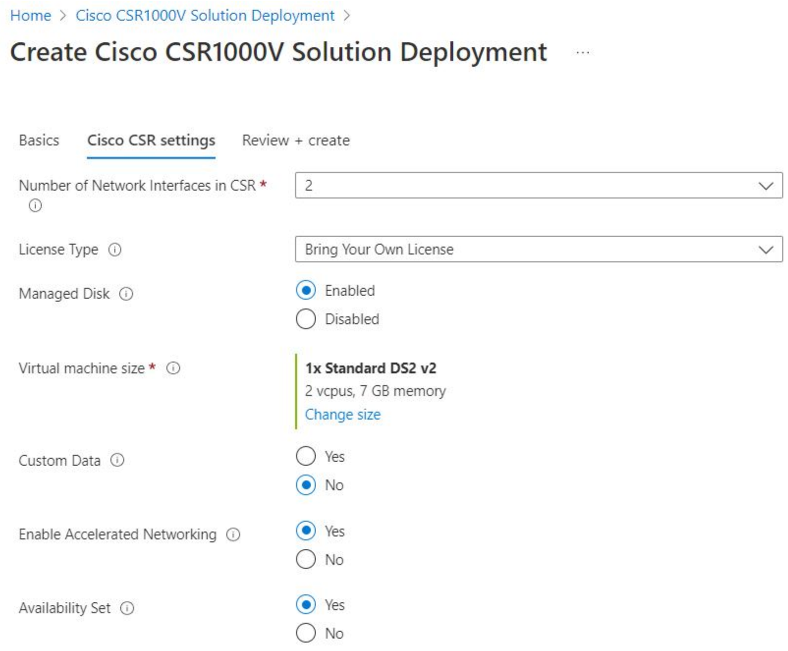
To view the supported instance types and the virtual machine sizes, see the following links:

- Dv2 and DSv2 series
- Fsv2 series

e) **Custom Data**: The provisioning configuration information for your VM. Select **Yes** if you want to provide a bootstrap configuration file for your Cisco CSR 1000V instance. For further information about providing a bootstrap configuration file for the Cisco CSR 1000V instance, see: Deploying a Cisco CSR 1000v VM on Microsoft Azure using a Day 0 Bootstrap File and customdata-examples.

f) **Enable Accelerated Networking**: The option to enable single root I/O virtualization (SR-IOV) to your VM. Select **Yes** to enable the accelerated networking feature.

g) **Availability Set**: The logical grouping of resources to create an availability set. Select **Yes** to create a new availability set.



Home > Cisco CSR1000V Solution Deployment >

Create Cisco CSR1000V Solution Deployment ···

Basics | Cisco CSR settings | Review + create

Number of Network Interfaces in CSR * ⓘ: 2

License Type ⓘ: Bring Your Own License

Managed Disk ⓘ: ● Enabled ○ Disabled

Virtual machine size * ⓘ: 1x Standard DS2 v2, 2 vcpus, 7 GB memory, Change size

Custom Data ⓘ: ○ Yes ● No

Enable Accelerated Networking ⓘ: ● Yes ○ No

Availability Set ⓘ: ● Yes ○ No

h) **Availability Set name**: The name of your availability set. Enter a name for your availability set.

i) **Availability Set Fault Domain Count**: The group of VMs that share a common power source and network switch. Availability sets arrange virtual machines across fault domains. In the field, enter the availability set fault domain count.

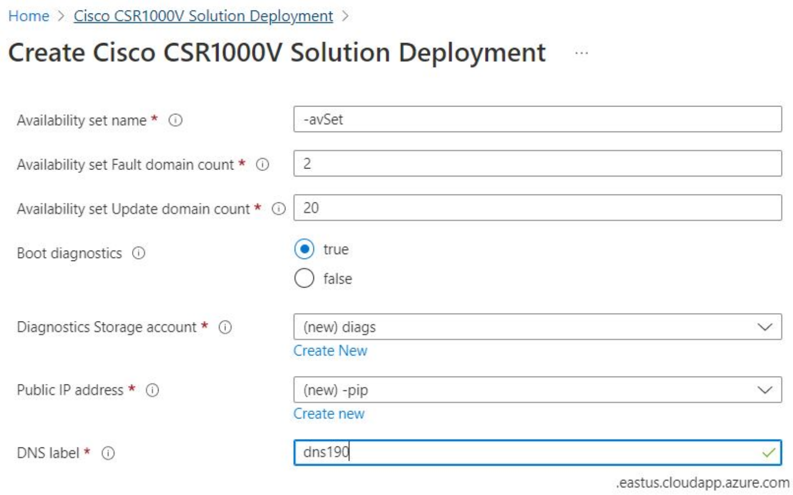
j) **Availability Set Update Domain Count**: A group of VMs and underlying physical hardware that can be rebooted at the same time. Enter the availability set update domain count.

k) **Boot diagnostics**: The option that enables you to capture the boot logs and screenshots of the virtual machine. Select **True** to enable boot diagnostics. For more information on boot diagnostics, see Microsoft Azure Resources.

l) **Diagnostics Storage account**: The storage account for the boot diagnostics. Enter the storage account name. For more information on storage accounts, see Microsoft Azure Resources.

m) **Public IP Address**: The public IP address name. For more information on the public IP address, see Microsoft Azure Resources.

n) **DNS label**: The name of the public IP address to be assigned to the Cisco CSR 1000V instance. A default value for the DNS label is shown in the text box which is the VM name followed by "`-dns`". Change the name of the DNS label, if required.



Home > Cisco CSR1000V Solution Deployment >

Create Cisco CSR1000V Solution Deployment ...

Availability set name * ⓘ -avSet

Availability set Fault domain count * ⓘ 2

Availability set Update domain count * ⓘ 20

Boot diagnostics ⓘ ● true ○ false

Diagnostics Storage account * ⓘ (new) diags
Create New

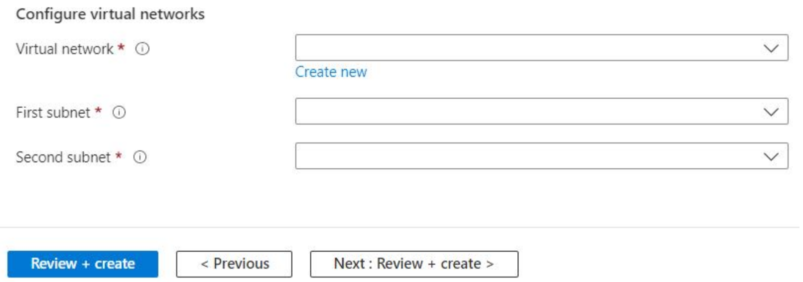
Public IP address * ⓘ (new) -pip
Create new

DNS label * ⓘ dns190 ✓
.eastus.cloudapp.azure.com

Step 8 In the Configure Virtual Networks section, specify the following details:

a) **Virtual network**: From the drop-down field, choose either **Create New** or **Use existing**. For a new virtual network, enter the name and IP address.

b) **First Subnet**/**Second Subnet**: The name and the IP address for your subnets. For more information on subnets, see "Interfaces" in Microsoft Azure Resources.



Configure virtual networks

Virtual network * ⓘ
Create new

First subnet * ⓘ

Second subnet * ⓘ

Step 9 Click **Next: Review + Create**.

Step 10 The system displays the summary of all your settings. Review your settings and then click **Next**.

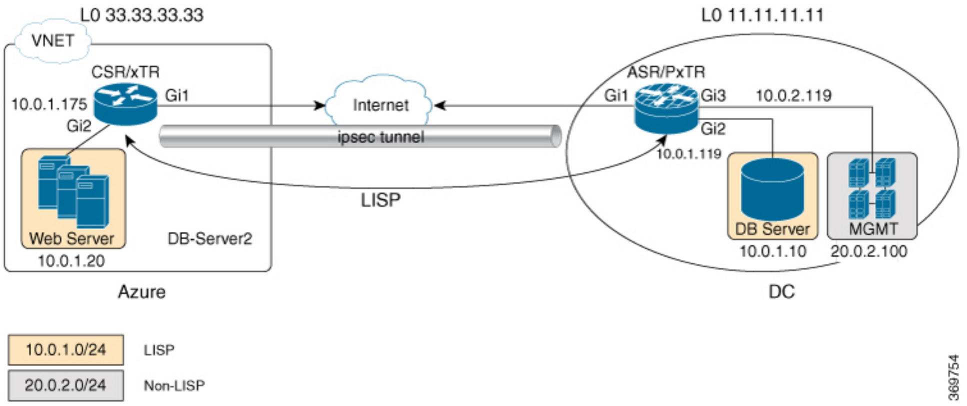
Step 11 Click **Create**

The VM is created and the purchase is confirmed.

Step 12 To verify the successful creation of your VM, click **Virtual machines** in the left hand panel. After a few minutes, the status of the recently created VM changes from “Creating” to “Running”. Make a note of the Public IP address name.

Configure a tunnel between CSR 1000v on Azure and CSR 1000v on the enterprise system

The communication between the CSR 1000v instance deployed within the enterprise data center and the CSR 1000v instance deployed within the public cloud is secured by an IP Security (IPsec) tunnel established between them. The LISP-encapsulated traffic is protected with the IPsec tunnel that provides data origin authentication, integrity protection, anti-reply protection, and confidentiality between the public cloud and the enterprise.



Step 1 Configure a CSR 1000v instance on Microsoft Azure.

Run the **interface Loopback** command. Loopback is used as the LISP RLOC, which identifies where the migrated customer IP space is located.

Run the **interface Tunnel** command to connect to the CSR 1000v instance on the cloud.

```
interface Loopback1
 ip address 33.33.33.33 255.255.255.255
!
interface Tunnel2
 ip address 30.0.0.2 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 173.39.145.79
 tunnel protection ipsec profile p2p_pf1
!
interface GigabitEthernet2
 ip address 10.10.10.140 255.255.255.0
 negotiation auto
 lisp mobility subnet1 nbr-proxy-reply requests 3
 no mop enabled
 no mop sysid
!
```

Step 2 Configure a second CSR 1000v instance on the enterprise site.

```
interface Loopback1
 ip address 11.11.11.11 255.255.255.255

interface Tunnel2
 ip address 30.0.0.1 255.255.255.0
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 52.14.116.161
 tunnel protection ipsec profile p2p_pf1
!
!
interface GigabitEthernet3
 ip address 10.10.10.2 255.255.255.0
 negotiation auto
 lisp mobility subnet1 nbr-proxy-reply requests 3
 no mop enabled
 no mop sysid
!
```

Configure LISP xTR on the CSR1000v instance running on Azure

To configure LISP xTR on the CSR instance running on the service provider, follow the configuration steps in the Configuring LISP (Location ID Separation Protocol) section.

The CSR 1000v instance on Azure uses the enterprise LISP router as the proxy ETR. Whenever the routing table points to the default route, it sends the traffic to the PETR.

Run the router **lisp command** to enable LISP. Execute the **itr map resolver** and the **itr map server** commands, to configure the CSR 1000v instance on the enterprise as the map server/map resolver.

Example:

```
router lisp
 locator-set azure
  33.33.33.33 priority 1 weight 100
  exit-locator-set
 !
 service ipv4
  itr map-resolver 11.11.11.11
  itr
  etr map-server 11.11.11.11 key cisco
  etr
  use-petr 11.11.11.11
  exit-service-ipv4
 !
 instance-id 0
  dynamic-eid subnet1
   database-mapping 10.10.10.0/24 locator-set azure
   map-notify-group 239.0.0.1
   exit-dynamic-eid
  !
  service ipv4
   eid-table default
   exit-service-ipv4
  !
  exit-instance-id
 !
 exit-router-lisp
!
router ospf 11
 network 30.0.0.2 0.0.0.0 area 11
 network 33.33.33.33 0.0.0.0 area 11
!

router lisp
 locator-set dmz
  11.11.11.11 priority 1 weight 100
  exit-locator-set
 !
 service ipv4
  itr map-resolver 11.11.11.11
  etr map-server 11.11.11.11 key cisco
  etr
  proxy-etr
  proxy-itr 11.11.11.11
  map-server
  map-resolver
  exit-service-ipv4
 !
 instance-id 0
  dynamic-eid subnet1
   database-mapping 10.10.10.0/24 locator-set dmz
   map-notify-group 239.0.0.1
   exit-dynamic-eid
  !
  service ipv4
   eid-table default
   exit-service-ipv4
  !
  exit-instance-id
 !
 site DATA_CENTER
  authentication-key cisco
  eid-record 10.10.10.0/24 accept-more-specifics
  exit-site
 !
 exit-router-lisp
!
router ospf 11
 network 11.11.11.11 0.0.0.0 area 11
 network 30.0.0.1 0.0.0.0 area 11
!

!
!
```

Verify the LISP Layer 2 Traffic between CSR 1000v on Azure and CSR 1000v on the enterprise system

Run the following show lisp commands to verify the LISP Layer 2 traffic:

Example:

```
csr-azure#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 2, no-route 0, inactive 0

10.0.1.1/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
33.33.33.33    1/100  cfg-addr   site-self, reachable
10.0.1.20/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
33.33.33.33    1/100  cfg-addr   site-self, reachable
csr-azure#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 4 entries

0.0.0.0/0, uptime: 00:09:49, expires: never, via static-send-map-request
  Negative cache entry, action: send-map-request
10.0.1.0/24, uptime: 00:09:49, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
10.0.1.4/30, uptime: 00:00:55, expires: 00:00:57, via map-reply, forward-native
```

```
  Encapsulating to proxy ETR
10.0.1.100/32, uptime: 00:01:34, expires: 23:58:26, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
11.11.11.11  00:01:34  up           1/100       -
csr-azure#show lisp dynamic-eid detail
% Command accepted but obsolete, unreleased or unsupported; see documentation.

LISP Dynamic EID Information for VRF "default"

Dynamic-EID name: subnet1
  Database-mapping EID-prefix: 10.0.1.0/24, locator-set dc
  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: 239.0.0.1
  Number of roaming dynamic-EIDs discovered: 2
  Last dynamic-EID discovered: 10.0.1.20, 00:01:37 ago
    10.0.1.1, GigabitEthernet2, uptime: 00:09:23
      last activity: 00:00:42, discovered by: Packet Reception
    10.0.1.20, GigabitEthernet2, uptime: 00:01:37
      last activity: 00:00:40, discovered by: Packet Reception

CSR-DC#show ip lisp
CSR-DC#show ip lisp data
CSR-DC#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 1, no-route 0, inactive 0

10.0.1.100/32, dynamic-eid subnet1, inherited from default locator-set dc
  Locator  Pri/Wgt  Source     State
11.11.11.11    1/100  cfg-addr   site-self, reachable
CSR-DC#show ip lisp
CSR-DC#show ip lisp map
CSR-DC#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 2 entries

10.0.1.0/24, uptime: 1d08h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
10.0.1.20/32, uptime: 00:00:35, expires: 23:59:24, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
33.33.33.33  00:00:35  up           1/100

CSR-DC#show lisp dynamic-eid detail
% Command accepted but obsolete, unreleased or unsupported; see documentation.

LISP Dynamic EID Information for VRF "default"

Dynamic-EID name: subnet1
  Database-mapping EID-prefix: 10.0.1.0/24, locator-set dc
  Registering more-specific dynamic-EIDs
  Map-Server(s): none configured, use global Map-Server
  Site-based multicast Map-Notify group: 239.0.0.1
  Number of roaming dynamic-EIDs discovered: 1
  Last dynamic-EID discovered: 10.0.1.100, 1d08h ago
    10.0.1.100, GigabitEthernet2, uptime: 1d08h
      last activity: 00:00:47, discovered by: Packet Reception

CSR-DC#show lisp site
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
dc             never     no     --                            10.0.1.0/24
               00:08:41  yes#   33.33.33.33                   10.0.1.1/32
               00:01:00  yes#   33.33.33.33                   10.0.1.20/32
               1d08h     yes#   11.11.11.11                   10.0.1.100/32
CSR-DC#show ip cef 10.0.1.20
10.0.1.20/32
  nexthop 33.33.33.33 LISP0
CSR-DC#
```

```
newlispcsr#show lisp instance-id 0 ipv4 database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1
Entries total 7, no-route 0, inactive 4

10.20.20.1/32, locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.5/32, dynamic-eid subnet1, inherited from default locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.6/32, Inactive, expires: 01:20:16
10.230.1.7/32, Inactive, expires: 01:20:16
10.230.1.8/32, dynamic-eid subnet1, inherited from default locator-set dc
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
10.230.1.31/32, Inactive, expires: 01:21:52
10.230.1.32/32, Inactive, expires: 01:20:16
newlispcsronprem#show lisp instance-id 0 ipv4 map
newlispcsr#show lisp instance-id 0 ipv4 map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 6 entries

10.20.0.0/16, uptime: 22:39:53, expires: never, via static-send-map-request
Negative cache entry, action: send-map-request
10.230.1.0/24, uptime: 22:39:53, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request
10.230.1.6/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
10.230.1.7/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
10.230.1.31/32, uptime: 22:38:14, expires: 01:21:45, via map-reply, complete
Locator Uptime State Pri/Wgt Encap-IID
11.11.11.11 22:38:14 up 1/100 -
10.230.1.32/32, uptime: 22:37:05, expires: never, via away, send-map-request
Negative cache entry, action: send-map-request
```