VPN

VPN

A VPN template in Cisco Catalyst SD-WAN is a configuration template that

- enables the creation of separate feature templates for each VPN, and
- supports configuration of VPN 0 and VPN 512 on all device types, with additional VPN templates for segmenting service-side user networks on Cisco IOS XE Catalyst SD-WAN devices.

Types of VPNs

The types of VPNs in Cisco Catalyst SD-WAN include:

- **VPN 0—Transport VPN**, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.
- **VPN 512—Management VPN**, which carries out-of-band network management traffic among the Cisco IOS XE Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco IOS XE Catalyst SD-WAN devices. For controller devices, by default, VPN 512 is not configured.
- **VPNs 1–511, 513–65530—Service VPNs**, for service-side data traffic on Cisco IOS XE Catalyst SD-WAN devices.

You create a separate VPN feature template for each VPN. For example, create one feature template for VPN 0, a second for VPN 1, and a third for VPN 512.

Interfaces in the WAN Transport VPN

A VPN 0 is a WAN transport VPN that

- handles all control plane traffic carried over OMP sessions in the overlay network,

- requires at least one interface configured in VPN 0 for a Cisco IOS XE Catalyst SD-WAN device to participate in the overlay network, and
- mandates that at least one interface connects to a WAN transport network, such as the Internet or an MPLS or a metro Ethernet network.

Tunnel interface configurations

The WAN transport interface, known as a tunnel interface, is configured in VPN 0.

To configure a tunnel interface on a Cisco SD-WAN Controller or a Cisco SD-WAN Manager, you must create an interface in VPN 0, assign an IP address (static or via DHCP), enable the interface with the **no shutdown** command, and mark it as a tunnel interface.

The IP address can be either IPv4 or IPv6. To enable dual stack, configure both address types. Optionally, you can associate a color with the tunnel.

Note You can configure IPv6 addresses only on transport interfaces in VPN 0. Configuring IPv6 addresses is not supported in VPN 512.

On Cisco IOS XE Catalyst SD-WAN devices, tunnel interfaces must have an IP address, a color, and an encapsulation type. For releases before Cisco IOS XE Catalyst SD-WAN Release 17.3.2, dual stack is enabled by configuring both IPv4 and IPv6 addresses. Starting from Release 17.3.2, only one address type is supported per TLOC or interface. Using a second address type requires a second TLOC or interface on which it can be provisioned.

On Cisco Catalyst SD-WAN Controllers and Controller NMSs, interface names can be either ethnumber or loopbacknumber, and only VPN 0 and VPN 512 are supported for interface configuration.

On Cisco SD-WAN Controller and Cisco SD-WAN Manager, *interface-name* can be either **eth** *number* or **loopback** *number*, and only VPN 0 and VPN 512 are supported for interface configuration. Hence, all interfaces are present only on these VPNs.

Dual stack configuration

To use dual stack with Cisco IOS XE Catalyst SD-WAN devices from Cisco IOS XE Catalyst SD-WAN Release 17.3.2, configure all controllers with both IPv4 and IPv6 addresses. In addition, configure DNS for the Cisco SD-WAN Validator interface to resolve IPv4 and IPv6 address types so that controllers can reach the Cisco SD-WAN Validator through either IP address type.

Starting from Cisco vManage Release 20.6.1, in case of a dual-stack configuration, if an IPv4 address or the fully qualified domain name (FQDN) is not available, but an IPv6 address is available, then the IPv6 address is used to connect to the Cisco SD-WAN Validator.

Interfaces in the Management

VPN 512 is a default out-of-band management VPN that

- is included as part of the factory-default configuration for out-of-band management, and
- is converted to VRF Mgmt-Intf on Cisco IOS XE Catalyst SD-WAN devices, which use VRFs in place of VPNs.

VPN 512 is local to the device and not advertised in the overlay. If you need a management VPN that is reachable through the overlay, create a VPN with a number other than 512.

Configure VPN

Use one of these methods to configure VPN parameters:

- Configuration group
- Feature template
- CLI commands

Configure VPN using configuration groups

Configure transport VPN using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Transport VPN feature in Transport and Management profile.

a) Enter the basic configuration information.

Table 1: Basic Configuration

Field	Description
VPN	Enter the numeric identifier of the VPN.
Enhance ECMP Keying	Enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source IP address, destination IP address, protocol, and DSCP field, as the ECMP hash key. Default: Disabled

b) Enter DNS information.

Table 2: DNS

Field	Description
Add DNS	
Primary DNS Address (IPv4)	Enter the IP address of the primary IPv4 DNS server in this VPN.
Secondary DNS Address (IPv4)	Enter the IP address of a secondary IPv4 DNS server in this VPN.

Field	Description
Add DNS IPv6	
Primary DNS Address (IPv6)	Enter the IP address of the primary IPv6 DNS server in this VPN.
Secondary DNS Address (IPv6)	Enter the IP address of a secondary IPv6 DNS server in this VPN.

c) Enter host happing information.

Table 3: Host Mapping

Field	Description
Add New Host Mapping	
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.
List of IP*	Enter up to 14 IP addresses to associate with the hostname. Separate the entries with commas.

Step 3 Configure the following parameters based on the features you choose to configure on your network.

a) Enter the route details.

Table 4: Route

Field	Description
Add IPv4 Static Route	
Network address*	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
Subnet Mask*	Enter the subnet mask.
Gateway*	Choose one of the following options to configure the next hop to reach the static route: • **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative distance***: Enter the administrative distance for the route. • **dhcp** • **null0**: When you choose this option, the following field appears: • **Administrative distance**: Enter the administrative distance for the route.
Add IPv6 Static Route	

Field	Description
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **NAT**: When you choose this option, the following field appears: • **IPv6 NAT***: Choose NAT64 or NAT66.
Add BGP Routing	Choose a BGP route.

b) Enter the NAT details

Table 5: NAT

Field	Description
Add NAT64 v4 Pool	
NAT64 v4 Pool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
NAT64 Pool Range Start*	Enter a starting IP address for the NAT pool.
NAT64 Pool Range End*	Enter a closing IP address for the NAT pool.
NAT64 Overload	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Disabled

c) Enter the service information.

Table 6: Service

Field	Description
Add Service	
Service Type	Choose the service available in the VPN. Value: **TE**

What to do next

Also see Deploy a Configuration Group.

Configure management VPN using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Management VPN feature in Transport and Management profile.

a) Enter the basic configuration information.

Table 7: Basic Configuration

Field	Description
VPN	Management VPN carries out-of-band network management traffic among the Cisco IOS XE Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco IOS XE Catalyst SD-WAN devices.
Name	Enter a name for the interface.

b) Enter DNS information.

Table 8: DNS

Field	Description
Add DNS	
Primary DNS Address (IPv4)	Enter the IPv4 address of the primary DNS server in this VPN.
Secondary DNS Address (IPv4)	Enter the IPv4 address of a secondary DNS server in this VPN.
Add DNS IPv6	

Field	Description
Primary DNS Address (IPv6)	Enter the IPv6 address of the primary DNS server in this VPN.
Secondary DNS Address (IPv6)	Enter the IPv6 address of a secondary DNS server in this VPN.

c) Enter host happing information.

Table 9: Host Mapping

Field	Description
Add New Host Mapping	
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.
List of IP Address*	Enter IP addresses to associate with the hostname. Separate the entries with commas.

d) Enter the IPv4/IPv6 static route information.

Table 10: IPv4/IPv6 Static Route

Field	Description
Add IPv4 Static Route	
IP Address*	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
Subnet Mask*	Enter the subnet mask.
Gateway*	Choose one of the following options to configure the next hop to reach the static route: • **nextHop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative distance***: Enter the administrative distance for the route. • **dhcp** • **null0**: When you choose this option, the following field appears: • **Administrative distance**: Enter the administrative distance for the route.
Add IPv6 Static Route	
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.

Field	Description
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv6 address. **Administrative distance***: Enter the administrative distance for the route. • **Null 0**: When you choose this option, the following field appears: • **NULL0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **NAT**: When you choose this option, the following field appears: • **IPv6 NAT**: Choose NAT64 or NAT66.

What to do next

Also see Deploy a Configuration Group.

Configure service VPN using a configuration group

This section helps you configure a service VPN (range 1 – 65527, except 512) or the LAN VPN.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure Service VPN in a Service profile.

a) Enter the basic configuration information.

Table 11: Basic Configuration

Field	Description
VPN*	Enter the numeric identifier of the VPN.
Name*	Enter a name for the VPN.

Field	Description
OMP Admin Distance IPv4	Administrative distance for OMP routes. The Cisco SD-WAN Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255.
OMP Admin Distance IPv6	Administrative distance for OMP routes. The Cisco SD-WAN Controllers learn the topology of the overlay network and the services available in the network using OMP routes. The distance can be a value between 1–255.

b) Enter DNS information.

Table 12: DNS

Field	Description
Add DNS IPv4	
Primary DNS Address (IPv4)	Enter the IP address of the primary IPv4 DNS server in this VPN.
Secondary DNS Address (IPv4)	Enter the IP address of a secondary IPv4 DNS server in this VPN.
Add DNS IPv6	
Primary DNS Address (IPv6)	Enter the IP address of the primary IPv6 DNS server in this VPN.
Secondary DNS Address (IPv6)	Enter the IP address of a secondary IPv6 DNS server in this VPN.

c) Enter host happing information.

Table 13: Host Mapping

Field	Description
Add New Host Mapping	
Hostname*	Enter the hostname of the DNS server. The name can be up to 128 characters.
List of IP*	Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas.

Step 3 Configure the following parameters based on the features you choose to configure on your network.

a) Enter advertise OMP information.

Table 14: Advertise OMP

Field	Description
Add OMP Advertise IPv4	

Field	Description
Protocol	Choose a protocol to configure route advertisements to OMP, for this VPN: • **bgp** • **ospf** • **ospfv3** • **connected** • **static** • **network** • **aggregate** **Applied to Region**: (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. Choose **core**, **access**, or **core-and-access**, to apply route aggregation only to access regions, the core region, or both. This option is applicable only to a Multi-Region Fabric border router, not an edge router or a transport gateway. • **eigrp** • **lisp** • **isis**
Select Route Policy	Enter the name of the route policy. Route policy is not supported in Cisco vManage Release 20.9.1.
Add OMP Advertise IPv6	

Field	Description
Protocol	**Note** Advertising IPv6 OMP routes as network statements is not supported. This applies when using the Service VPN feature in a configuration group, and applies also when using a Cisco VPN feature template. You can configure to advertise: • IPv6 routes by BGP and OSPF protocols • Connected routes, static routes, and aggregate routes The reason for the lack of support is that the Service VPN feature and the Cisco VPN feature template both use the **advertise network** *prefix* command, which does not fully support IPv6 addresses. Choose a protocol to configure route advertisements to OMP, for this VPN: • **BGP** • **OSPF** • **Connected** • **Static** • **Network** • **Aggregate** **Applied to Region**: (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, route aggregation is a method for reducing the number of entries that routers in a network must maintain in routing tables, for better scaling. Choose **core**, **access**, or **core-and-access**, to apply route aggregation only to access regions, the core region, or both. This option is applicable only to a Multi-Region Fabric border router, not an edge router or a transport gateway.
Select Route Policy	Enter the name of the route policy. Route policy is not supported in Cisco vManage Release 20.9.1.
Protocol Sub Type	When you choose the OSPF protocol, specify the sub type as external.

b) Enter route information.

Table 15: Route

Field	Description
Add IPv4 Static Route	
Network Address*	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.

Field	Description
Subnet Mask*	Enter the subnet mask.
Next Hop/Null 0/VPN/DHCP	Choose one of the following options to configure the next hop to reach the static route: • **Next Hop**: When you choose this option, the **IPv4 Route Gateway Next Hop** field appears. Enable this option to add the next hop. You can add a hop with and without a tracker. When you click **Add Next Hop**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative Distance***: Enter the administrative distance for the route. When you click **Add Next Hop with Tracker**, the following fields appear: • **Address***: Enter the next-hop IPv4 address. • **Administrative Distance***: Enter the administrative distance for the route. • **Tracker***: Enter the name of the gateway tracker to determine whether the next hop is reachable before adding that route to the route table of the device. • **Null 0**: When you choose this option, the following field appears: • **IPv4 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. • **VPN**: When you choose this option, the following field appears: • **IPv4 Route VPN***: Selects VPN as the gateway to direct packets to the transport VPN. • **DHCP**: When you choose this option, the following field appears: • **IPv4 Route Gateway DHCP***: Assigns a static route for the default next-hop router when the DHCP server is accessed for an IP address.
Add BGP Routing	Choose a BGP route.
Add OSPF Routing	Choose an OSPF route.
Add IPv6 Static Route	
Prefix*	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.

Field	Description
Next Hop/Null 0/NAT	Choose one of the following options to configure the next hop to reach the static route: - **Next Hop**: When you choose this option and click **Add Next Hop**, the following fields appear: - **Address***: Enter the next-hop IPv6 address. - **Administrative distance***: Enter the administrative distance for the route. - **Null 0**: When you choose this option, the following field appears: - **IPv6 Route Null 0***: Enable this option to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages. - **NAT**: When you choose this option, the following field appears: - **IPv6 NAT***: Choose NAT64 or NAT66. - **Interface**: When you choose this option, the following fields appear: - **Interface Name**: Choose IPv6 interface name for the IPsec tunnel. - **Next Hop**: Enter the IPv6 address and the administrative distance for the next hop.

c) Enter service information.

Table 16: Service

Field	Description
Add Service	
Service Type	Choose a service available at the local site and in the VPN. Values: **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4**, **TE**, **SIG**
IPv4 Addresses (Maximum: 4)*	Enter up to four IP address, separated by commas. The service is advertised to the Cisco SD-WAN Controller only if one of the addresses can be resolved locally, at the local site, not via routes learned through OMP. You can configure up to four IP addresses.
Tracking*	Cisco Catalyst SD-WAN tests each service device periodically to check whether it is operational. Tracking saves the results of the periodic tests in a service log. Tracking is enabled by default.

d) Enter service route information.

Table 17: Service Route

Field	Description
Add Service Route	
Prefix*	Enter the IP address or prefix. For Umbrella SIG, use any RFC 1918 subnet for Service IP addresses.
Service*	Configure routes pointing to any service. Values: **FW**, **IDS**, **IDP**, **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4**.
VPN*	Destination VPN to resolve the prefix.

e) Enter GRE route information.

Table 18: GRE Route

Field	Description
Add GRE Route	
Prefix*	Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route.
Interface*	Enter the name of one or two GRE tunnels to use to reach the service.
VPN*	Enter the number of the VPN to reach the service. This must be VPN 0.

f) Enter IPSEC route information.

Table 19: IPSEC Route

Field	Description
Add ipSec Route	
Prefix*	Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route.
Interface*	Enter the name of one or two IPsec tunnel interfaces. If you configure two interfaces, the first is the primary IPsec tunnel, and the second is the backup. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel.

g) Enter NAT information.

Table 20: NAT

Field	Description
Nat Pool	

Field	Description
NatPool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
Prefix Length*	Enter the NAT pool prefix length.
Range Start*	Enter a starting IP address for the NAT pool.
Range End*	Enter a closing IP address for the NAT pool.
Overload*	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Enabled
Direction*	Choose the NAT direction.
Nat64 V4 Pool	
Nat64 V4 Pool Name*	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–32) NAT pools per router.
Nat 64 V4 Pool Range Start*	Enter a starting IP address for the NAT pool.
Nat 64 V4 Pool Range End*	Enter a closing IP address for the NAT pool.
Overload*	Enable this option to configure per-port translation. If this option is disabled, only dynamic NAT is configured on the end device. Per-port NAT is not configured. Default: Disabled

h) Enter route leak information.

Table 21: Route leak from Global VPN

Field	Description
Route Protocol*	Choose a protocol to configure leak routes from global VPN to the service VPN that you are configuring: • **static** • **connected** • **bgp** • **ospf**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in service VPN)	

Field	Description
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.

Table 22: Route leak to Global VPN

Field	Description
Route Protocol*	Choose a protocol to leak routes from the service VPN that you are configuring to the global VPN: • **static** • **connected** • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in global VPN)	
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf**
Select Route Policy	Enter the name of the route policy.
Select Route Policy	Choose a route policy from the drop-down list.

Table 23: Route leak between services

Field	Description
Source VPN	Enter a value of the source VPN.

Field	Description
Route Protocol*	Choose a protocol from the available options to leak routes from the source service VPN to the service VPN that you are configuring: • **static** • **connected** • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.
Redistribution (in Service VPN)	
Protocol*	Choose a protocol from the available options to redistribute the leaked routes: • **bgp** • **ospf** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1) **eigrp**
Select Route Policy	Choose a route policy from the drop-down list.

i) Enter route target information.

Table 24: Route Target

Field	Description
IPv4 Settings	
Import Route Target List: Route Target*	Configure a route target for IPv4 interfaces. It imports routing information from the target VPN extended community.
Export Route Target List: Route Target*	Configure a route target for IPv4 interfaces. It exports routing information to the target VPN extended community.
IPv6 Settings	
Import Route Target List: Route Target*	Configure a route target for IPv6 interfaces. It imports routing information from the target VPN extended community.

Field	Description
Export Route Target List: Route Target*	Configure a route target for IPv6 interfaces. It exports routing information to the target VPN extended community.

What to do next

Also see Deploy a Configuration Group.

Configure VPN using templates

Cisco IOS XE Catalyst SD-WAN devices use VRFs for segmentation and network isolation. However, the following steps still apply if you are configuring segmentation for Cisco IOS XE Catalyst SD-WAN devices through Cisco SD-WAN Manager. When you complete the configuration, the system automatically converts the VPNs to VRFs for Cisco IOS XE Catalyst SD-WAN devices.

You can configure a static route through the VPN template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

Step 2 Click **Device Templates**, and click **Create Template**.

In Cisco vManage Release 20.7.x and earlier releases **Device Templates** is called **Device**.

Step 3 From the **Create Template** drop-down list, choose **From Feature Template**.

Step 4 From the **Device Model** drop-down list, choose the type of device for which you wish to create the template.

Step 5 To create a template for VPN 0 or VPN 512:

a) Click **Transport & Management VPN**, or scroll to the **Transport & Management VPN** section.
b) From the VPN 0 or VPN 512 drop-down list, click **Create Template**. The VPN template form appears.

The form contains fields for naming the template, and fields for defining VPN parameters.

Step 6 To create a template for VPNs 1 through 511, and 513 through 65527:

a) Click **Service VPN**, or scroll to the **Service VPN** section.
b) Click the **Service VPN** drop-down list.
c) From the **VPN** drop-down list, click **Create Template**. The VPN template form displays.

The form contains fields for naming the template, and fields for defining VPN parameters.

Step 7 In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8 In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Step 9 Configure the VPN template parameters.

a) Configure basic VPN parameters.

Parameter Name	Description
VPN	Enter the numeric identifier of the VPN. Range for Cisco IOS XE Catalyst SD-WAN devices: 0 through 65527 Values for Cisco SD-WAN Controller and Cisco SD-WAN Manager devices: 0, 512
Name	Enter a name for the VPN. **Note** For Cisco IOS XE Catalyst SD-WAN devices, you can't enter a device-specific name for the VPN.
Enhance ECMP keying	Click **On** to enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source, and destination IP addresses, as the ECMP hash key. ECMP keying is **Off** by default.
OMP Admin Distance (IPv4)	To configure a site to prefer the OMP route over the leaked route path, configure the IPv4 address with a lower administrative distance than the leaked route. You can apply the configuration at the global level or at the specific VRF level by choosing **Global** or **Device Specific** respectively. Range: 1-251
OMP Admin Distance (IPv6)	To configure a site to prefer the OMP route over the leaked route path, configure the IPv6 address with a lower administrative distance than the leaked route. You can apply the configuration at the global level or at the specific VRF level by choosing **Global** or **Device Specific** respectively. Range: 1-251

Note
To complete the configuration of the transport VPN on a router, you must configure at least one interface in VPN 0.

b) Configure DNS addresses and static hostname mapping.

Parameter Name	Options	Description
Primary DNS Address	Click either **IPv4** or **IPv6**, and enter the IP address of the primary DNS server in this VPN.	

Parameter Name	Options	Description
New DNS Address	Click **New DNS Address** and enter the IP address of a secondary DNS server in this VPN. This field appears only if you have specified a primary DNS address.	
	Mark as Optional Row	Check the **Mark as Optional Row** check box to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.
	Hostname	Enter the hostname of the DNS server. The name can be up to 128 characters.
	List of IP Addresses	Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas.
To save the DNS server configuration, click **Add**.		

Configure VPN parameters using CLI commands

Configure load-balancing algorithm using CLI commands

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, you need CLI template to configure the **src-only** load-sharing algorithm for IPv4 and IPv6 Cisco Catalyst SD-WAN and non Cisco Catalyst SD-WAN traffic. For complete details on the load-sharing algorithm CLI, see IP Commands list.

Follow these steps to configure load-balancing algorithm using CLI commands:

Procedure

Step 1 Select a Cisco Express Forwarding load-balancing algorithm for non Cisco Catalyst SD-WAN IPv4 and IPv6 traffic.

Example:

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm {universal [id] | include-ports [ source [id] |
destination [id]] |
src-only [id]}
```

```
Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm {universal [id] | include-ports [ source [id] |
destination [id]] |
src-only [id]}
```

Step 2 Enable load balancing algorithm on an interface for Cisco Catalyst SD-WAN IPv4 and IPv6 traffic.

Example:

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

Map host names to IP addresses using CLI commands

Perform this task to associate host names with IP addresses.

A name server is used to keep track of information associated with domain names. A name server can maintain a database of host name-to-address mappings. Each name can map to one or more IP addresses. In order to use this service to map domain names to IP addresses, you must specify a name server.

Procedure

Step 1 Define a static host name-to-address mapping in the host name cache.

Example:

```
Device(config)# ip host cisco-rtp 192.168.0.148
```

Step 2 Define a default domain name that Cisco Catalyst SD-WAN can use to complete unqualified host names.

Example:

```
Device(config)# ip domain name cisco.com
```

Step 3 Specify one or more hosts that supply name information.

Example:

```
Device(config)# ip name-server 172.16.1.111 172.16.1.2
```

Step 4 Enable DNS-based address translation.

DNS is enabled by default. Use this command if DNS has been disabled.

Example:

```
Device(config)# ip domain lookup
```

The following example configures the host-name-to-address mapping process. IP DNS-based translation is specified, the addresses of the name servers are specified, and the default domain name is given.

```
! IP DNS-based host name-to-address translation is enabled
  ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
  ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the device uses to complete
! Set the name for unqualified host names
  ip domain name cisco.com
```

Verify the VPN configuration

This section provides examples for VPN configurations.

Use the **show sdwan running-config | sec vrf definition Mgmt-intf** command to verify the management interface configurations.

```
Device# show sdwan running-config | sec vrf definition Mgmt-intf

vrf definition Mgmt-intf
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
============
interface GigabitEthernet0
 no shutdown
 vrf forwarding Mgmt-intf
 negotiation auto
exit
============
config-t
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0

vrf definition Mgmt-intf
 rd 1:512
 !
 address-family ipv4
  route-target export 1:512
  route-target import 1:512
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
interface GigabitEthernet1
 vrf forwarding Mgmt-intf
 ip address 192.168.20.11 255.255.255.0
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0
!
```

To display information about the configured management interfaces, use the **show interface** command.

```
Device# show interface gigabitEthernet0
GigabitEthernet0 is up, line protocol is up
  Hardware is RP management port, address is d478.9bfe.9f7f (bia d478.9bfe.9f7f)
  Internet address is 10.34.9.177/16
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
```

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 8000 bits/sec, 12 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
   4839793 packets input, 415574814 bytes, 0 no buffer
   Received 3060073 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 0 multicast, 0 pause input
   82246 packets output, 41970224 bytes, 0 underruns
   Output 0 broadcasts (0 IP multicasts)
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```