Configure Basic Parameters to Form Control Connections on Cisco Edge Router

Contents

Introduction

This document describes the basic configuration and commit order to onboard a Cisco Edge Router to a Software-Defined Wide Area Network overlay.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Basic Cisco IOS® XE Command Line Interface (CLI)

Components Used

This document is based on these software and hardware versions:

- Cisco Edge Router version 17.6.3
- vManage version 20.6.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Note: This guide assumes that for physical routers the Cisco Edge Router Serial Number is already in Cisco Network Plug & Play (PnP) portal and synced with vManage devices list; and for virtual Edge

> Routers, that a virtual instance is added to PnP portal and synced to vManage.

Mode Verification

Step 1. Verify the router is on Controller-Managed mode.

<#root>

```
show platform software device-mode


show version | in mode
```

Example:

<#root>

```
Router#

show platform software device-mode


Device Operating-mode:

Controller-Managed


Device-mode bootup status:
 8/03 00:44:16 System is green
 Bootup Success
```

<#root>

```
Router#

show version | in mode


Router operating mode:

Controller-Managed
```

> **Note**: If the operating mode results in Autonomous, move the router to Controller-Managed with **controller-mode enable** command.

Step 2. Perform a software reset.

For a new onboard it is recommended to clean the device up with a software reset, this ensures all previous configurations in the Configuration Data Base (CBD) are removed.

<#root>

```
Router#

request platform software sdwan software reset
```

The device reloads and boots up with blank configuration.

Step 3. Stop PNP discovery process.

If no Zero Touch Provisioning (ZTP) is required, stop PNP discovery process.

<#root>

```
Router#

pnpa service discovery stop
```

Note: PNP process stops within 5-10 minutes.

Configuration

There are two scenarios covered:

- Physical interfaces
- Sub interfaces

Both scenarios need a Cisco IOS XE tunnel and an SD-WAN tunnel associated with an interface to work and basic SD-WAN system configuration.

Physical Interface Configuration

The interface and tunnel configuration for VPN 0 or Global VRF requires a specific order, otherwise, there are errors in the tunnel interface associations.

Configuration order:

1. Physical Interface
2. Default route
3. Commit changes
4. XE tunnel with a physical interface as source
5. SD-WAN XE tunnel
6. Commit changes

Example:

<#root>

```
!IOS-XE Portion


!
config-transaction
interface GigabitEthernet0/0/0
ip address 192.168.10.2 255.255.255.0
negotiation auto
no shutdown
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!

commit    <<<<<<<<<< Commit changes here


!
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
exit
!

! SD-WAN portion


!
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation ipsec
color default
allow-service all
!

commit    <<<<<<<<<< Commit changes here


!
end
```

If the changes are committed in a different order, it can lead to an error because the Cisco IOS XE Tunnel interface is not associated with the SD-WAN Tunnel Interface.

<#root>

```
cEdge(config-if)#

commit


Aborted: 'interface Tunnel 0 ios-tun:tunnel': Tunnel interface doesn't have corresponding sdwan Gigabit
```

In the opposite direction, if an SD-WAN tunnel is attempted to be removed without the Cisco IOS XE tunnel simultaneously, it can lead to a reference error.

<#root>

```
cEdge(config)#

commit


Aborted: 'sdwan interface GigabitEthernet0/0/0 tunnel-interface' : No Tunnel interface found with tunne
```

Subinterface Configuration

The physical interface, sub interface, and tunnel configuration for VPN 0 or Global VRF require a specific order, otherwise, there are errors in the tunnel interface associations.

Configuration order:

1. Physical Interface
2. Subinterface
3. Default route
4. Commit changes
5. XE tunnel with a sub interface as source
6. SD-WAN XE tunnel
7. Commit changes

Example:

<#root>

```
!IOS-XE Portion


!
config-transaction
interface GigabitEthernet0/0/0
no shutdown
no ip address
ip mtu 1500
mtu 1500
!
interface GigabitEthernet0/0/0.100
no shutdown
encapsulation dot1Q 100
ip address 192.168.10.2 255.255.255.0
ip mtu 1496
mtu 1496
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!

commit      <<<<<<<<<< Commit changes here


!
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0.100
tunnel source GigabitEthernet0/0/0.100
tunnel mode sdwan
```

```
exit
!

! SD-WAN portion


!
sdwan
interface GigabitEthernet0/0/0.100
tunnel-interface
encapsulation ipsec
color default
allow-service all
!

commit      <<<<<<<<<< Commit changes here


!
end
```

Note: To accommodate the 32-bit field added to packets by the 802.1Q protocol, the MTU for subinterfaces must be at least 4 bytes smaller than the MTU of the physical interface. This is configured with the **mtu<value>** command. The default MTU on a physical interface is 1500 bytes, hence the MTU of the subinterface must not be larger than 1496 bytes. Also, if the subinterface requires an MTU of 1500 bytes, the physical interface MTU can be adjusted to 1504 bytes.

If the changes are committed in a different order, it can lead to an error because the Cisco IOS XE Tunnel interface is not associated with the SD-WAN Tunnel Interface.

<#root>

```
cEdge(config)#

commit


Aborted: 'sdwan interface GigabitEthernet0/0/0.100 tunnel-interface' : No Tunnel interface found with t
```

System Configuration

In order to join the SD-WAN fabric, the Cisco Edge Router needs basic overlay information under system so that it can start the authentication with vBond.

1. System IP**:** Unique identifier for the Edge Router, it comes in octal dotted format. It is not a routable IP.
2. Site ID: Unique identifier of the site.
3. Organization Name: Unique identifier of the SD-WAN overlay.
4. vBond IP and port: vBond IP and port. It can be obtained from the vBond itself with **show sdwan running-config system** command.

Example:

<#root>

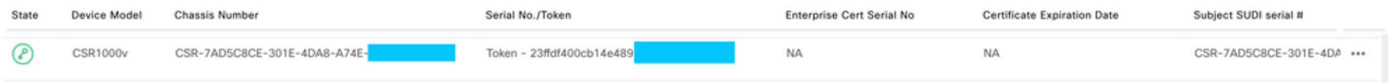
```
config-transaction
system
system-ip 10.10.10.1
site-id 10
organization-name SDWAN-OVERLAY
vbond 172.16.120.20 port 12346
!

commit
```

Right after the system configuration is committed, the Cisco Edge Router contacts the vBond for authentication and starts to build control connections to vManage and vSmarts.

CSR1000V and C8000V Activation

Cisco Edge virtual routers require an extra step to associate a chassis and a token since they are not real hardware and the Universal Unique Device Identifier (UUDI) is virtual.

In vManage GUI navigate to: **Configuration** > **Devices** and locate an available CSR1000v or C8000v entry:



State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Certificate Expiration Date	Subject SUDI serial #
✓	CSR1000v	CSR-7AD5C8CE-301E-4DA8-A74E-[redacted]	Token - 23ffdf400cb14e489[redacted]	NA	NA	CSR-7AD5C8CE-301E-4DA •••

Run the activation and substitute the chassis and serial numbers in the command.

<#root>

```
request platform software sdwan vedge_cloud activate chassis-number CHASSIS_NUMBER token TOKEN_ID
```

Example:

<#root>

```
Router#

request platform software sdwan vedge_cloud activate chassis-number 7AD5C8CE-301E-4DA8-A74E-90A316XXXXXX
```

Control Connections Verification

Verify the state of the control connections with the verification commands.

<#root>

```
show sdwan control connections
```

```
show sdwan control connection-history
```

Related Information

- Technical Support & Documentation - Cisco Systems
- Troubleshoot SD-WAN Control Connections