

Configure Active/Standby Hub and Spoke Topology on SD-WAN

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the steps to configure and validate an Active Standby Hub and Spoke Topology on Cisco SD-WAN.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Cisco SD-WAN
- Basic Cisco IOS-XE® Command Line Interface (CLI)

Components Used

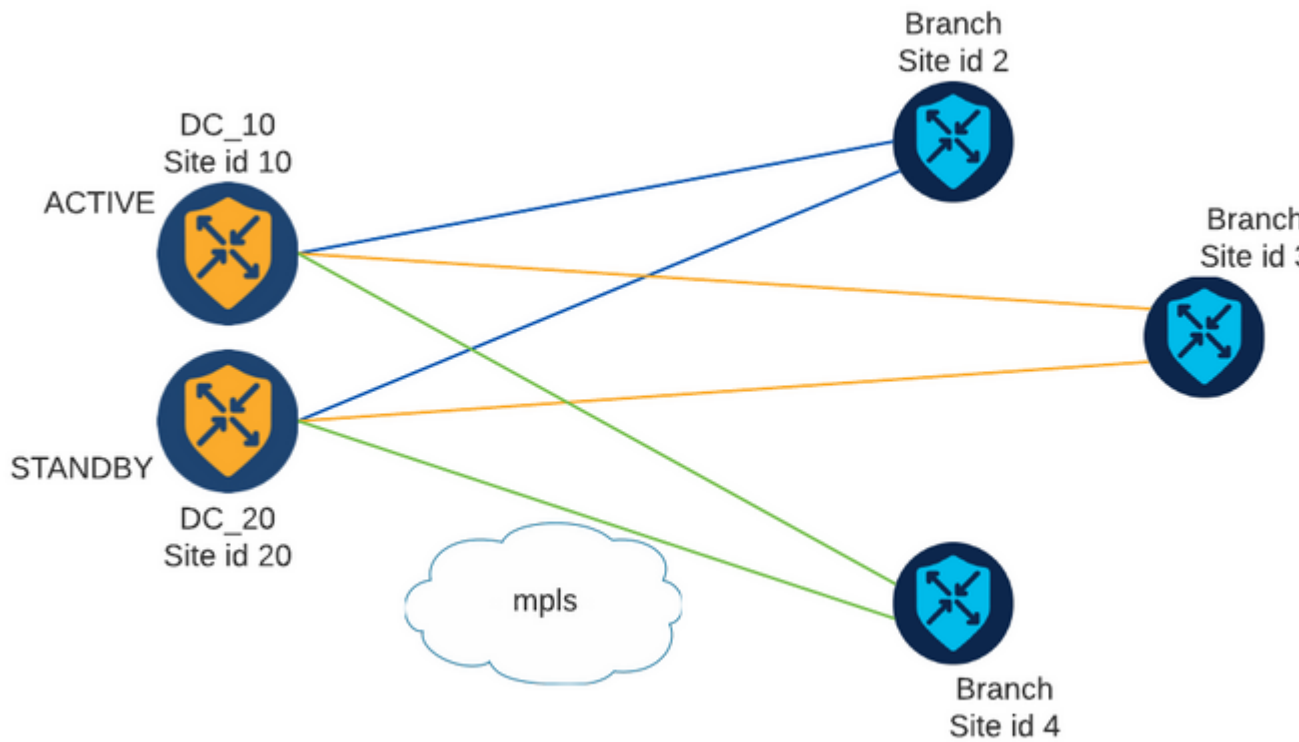
This document is based on these software and hardware versions:

- C8000V version 17.6.3a
- vManage version 20.6.3.1
- vSmart 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.

Configure

Network Diagram



There are two Hubs with Site ID 10 and 20. Site ID 10 acts as Active Hub and Site ID 20 as the Standby Hub. The Branches can communicate with each other, but all communication must go through the Hub. No tunnels must be created between Branch Sites.

Configurations

1. Log into vManage and navigate to **Configuration > Policies** and click **Add Policy**.
2. In the Create Groups of Interest section click **TLOC > New TLOC List** and add an one entry for the Active Hub and one for the Standby Hub on the same list:

TLOC List



List Name

PREFER_DC10_DC20

TLOC IP

Color

Encap

Preference

10.10.10.1

mpls

ipsec

1000



10.10.10.2

mpls

ipsec

500



+ Add TLOC

Cancel

Save

Make sure to set a higher preference for the active Hub and a lower preference for the Standby Hub.

3. Navigate to **Site > New Site List** and create a list for the Branch Sites and a list for the Hub Sites:

Site List



Site List Name

BRANCHES

Site

2-4

Save

Cancel

Site List



Site List Name

DCs_10_20

Site

10,20

Save

Cancel

4. Click **Next**. In the Configure Topology and VPN Membership section, navigate to **Add Topology > Custom Control**.

5. Add a Name and Description for the Policy.

6. Click **Sequence Type > TLOC**, add a **Sequence Rule**.

7. Choose **Match > Site** and add the Site list for the Branches, then choose **Actions > Reject** and click **Save Match And Actions**:



TLOC

+ Sequence Rule Drag and drop to re-arrange rules

1

Match

Actions

Accept Reject

Match Conditions

Site List

BRANCHES x

Site ID

0-4294967295

Actions

Reject

Enabled

Cancel

8. Click **Sequence Rule**, and add an entry to match the Hub Sites and Accept:

TLOC

Sequence Rule Drag and drop to re-arrange rules

Match **Actions**

Accept Reject

OMP Tag Preference

Match Conditions

Site List

Site ID

Actions

Accept Enabled

Cancel Save M

9. Navigate to **Sequence Type > Route**, add **Sequence Rule**.

10. Leave the match section in blank, set the Action as **Accept**, choose **TLOC**, add the TLOC list created earlier and click **Save Match And Actions**:

Route

Sequence Rule Drag and drop to re-arrange rules

Match **Actions**

Protocol Accept Reject

Community Export To OMP Tag Preference Service **TLOC Action** T

Match Conditions

Actions

Accept Enabled

TLOC List

TLOC IP

Color

Encapsulation

Cancel

11. Click **Save Control Policy**.

12. Click **Next** until the Apply Policies to Sites and VPNs section.

13. In the Topology section, your Control Policy shows up, click **New Site List**, choose the Branches list for the Outbound Site List and click **Add**:

Add policies to sites and VPNs

Policy Name

Centralized_Active_Standby_HnS

Policy Description

Centralized_Active_Standby_HnS

Topology

Application-Aware Routing

Traffic Data

Cflowd

Active_Standby_HnS

+ New Site List

Inbound Site List

Select one or more site lists

Outbound Site List

BRANCHES x

14. Click **Preview** and review the Policy.

```

viptela-policy:policy
control-policy Active_Standby_HnS
sequence 1
  match tloc
    site-list BRANCHES
  !
  action reject
  !
!
sequence 11
  match tloc
    site-list DCs_10_20
  !
  action accept
  !
!
sequence 21
  match route
    prefix-list _AnyIpv4PrefixList
  !
  action accept
  set
    tloc-list PREFER_DC10_DC20
  !
  !
!
default-action reject
!
lists
site-list BRANCHES
  site-id 2-4
!

```

```

site-list DCs_10_20
  site-id 10
  site-id 20
!
tloc-list PREFER_DC10_DC20
  tloc 10.10.10.1 color mpls encap ipsec preference 1000
  tloc 10.10.10.2 color mpls encap ipsec preference 500
!
prefix-list _AnyIpv4PrefixList
  ip-prefix 0.0.0.0/0 le 32
!
!
!
apply-policy
  site-list BRANCHES
  control-policy Active_Standby_HnS out
!
!

```

15. Click **Save Policy**.

16. In the Centralized Policy menu, click the 3 dots at the right of the new created Policy and select **Activate**.

The screenshot shows a web interface for policy management. At the top, there are two tabs: "Centralized Policy" (selected) and "Localized Policy". Below the tabs is a search bar with a magnifying glass icon and the text "Search". Underneath the search bar is a link labeled "Add Policy". The main part of the interface is a table with the following columns: Name, Description, Type, Activated, Updated By, Policy Version, and Last. The table contains one visible row with the following data:

Name	Description	Type	Activated	Updated By	Policy Version	Last
Centralized_Active_Stand...	Centralized_Active_Stand...	UI Policy Builder	false	admin	03302023T184504926	30 M

17. Once task is completed, a Success status shows.

Status	Message	Hostname
Success	Done - Push vSmart Policy	vsmart

Verify

Verify the policy is created on vSmart with these commands:

```
<#root>
```

```
vsmart#
```

```
show running-config policy
```

```
policy
lists
tloc-list PREFER_DC10_DC20
tloc 10.10.10.1 color mpls encap ipsec preference 1000
tloc 10.10.10.2 color mpls encap ipsec preference 500
!
site-list BRANCHES
site-id 2-4
!
site-list DCs_10_20
site-id 10
site-id 20
!
prefix-list _AnyIpv4PrefixList
ip-prefix 0.0.0.0/0 le 32
!
!
control-policy Active_Standby_HnS
sequence 1
match tloc
site-list BRANCHES
!
action reject
!
!
sequence 11
match tloc
site-list DCs_10_20
!
action accept
!
!
sequence 21
match route
prefix-list _AnyIpv4PrefixList
!
action accept
set
tloc-list PREFER_DC10_DC20
!
!
!
default-action reject
!
!
vsmart#
```

```
show running-config apply-policy
```

```
apply-policy
site-list BRANCHES
control-policy Active_Standby_HnS out
```



```
!  
!  
vsmart#
```

Note: This is a Control Policy. It is applied and executed on the vSmart and it is not pushed into the edge devices. "**show sdwan policy from-vsmart**" command does not show the policy on the Edge Devices.

Troubleshoot

Useful commands to troubleshoot.

On vSmart:

```
show running-config policy  
show running-config apply-policy  
show omp routes vpn <vpn> advertised <detail>  
show omp routes vpn <vpn> received <detail>  
show omp tlocs advertised <detail>  
show omp tlocs received <detail>
```

On cEdge:

```
show sdwan bfd sessions  
show ip route vrf <service vpn>  
show sdwan omp routes vpn <vpn> <detail>  
show sdwan omp tlocs
```

Example:

Confirm only the BFD session is formed from Branch to the Hubs:

```
<#root>
```

```
Branch_02#
```

```
show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP	DST PUBLIC PORT	ENCAP	DETECT MULTIPLIER
10.10.10.1	10	up	mpls	mpls	192.168.1.36	192.168.1.30	12386	ipsec	7
10.10.10.2	20	up	mpls	mpls	192.168.1.36	192.168.1.33	12366	ipsec	7

Verify routes from other branches are preferred via Active Hub with preference 1000:

<#root>

Branch_02#

show sdwan omp route vpn 10 172.16.1.0/24 detail

Generating output, this might take time, please wait ...

omp route entries for vpn 10 route 172.16.1.0/24

RECEIVED FROM:

peer 10.1.1.3

path-id 8

label 1002

status C,I,R <-- Chosen, Installed, Received

loss-reason not set

lost-to-peer not set

lost-to-path-id not set

Attributes:

originator 10.3.3.3

type installed

tloc 10.10.10.1, mpls, ipsec <-- Active Hub

ultimate-tloc not set

domain-id not set

overlay-id 1

site-id 3

preference 1000

tag not set

origin-proto connected

origin-metric 0

as-path not set

community not set

unknown-attr-len not set

RECEIVED FROM:

peer 10.1.1.3

path-id 9

label 1003

status R <-- Received

loss-reason preference

lost-to-peer 10.1.1.3

lost-to-path-id 8

Attributes:

originator 10.3.3.3

type installed

tloc 10.10.10.2, mpls, ipsec <-- Backup Hub

ultimate-tloc not set
domain-id not set
overlay-id 1
site-id 3

preference 500

tag not set
origin-proto connected
origin-metric 0
as-path not set
community not set
unknown-attr-len not set

Related Information

[Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x](#)