

SD-WAN에서 액티브/스탠바이 허브 및 스포크 토폴로지 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco SD-WAN에서 액티브 스탠바이 허브 및 스포크 토폴로지를 구성하고 검증하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco SD-WAN
- 기본 Cisco IOS-XE® CLI(명령줄 인터페이스)

사용되는 구성 요소

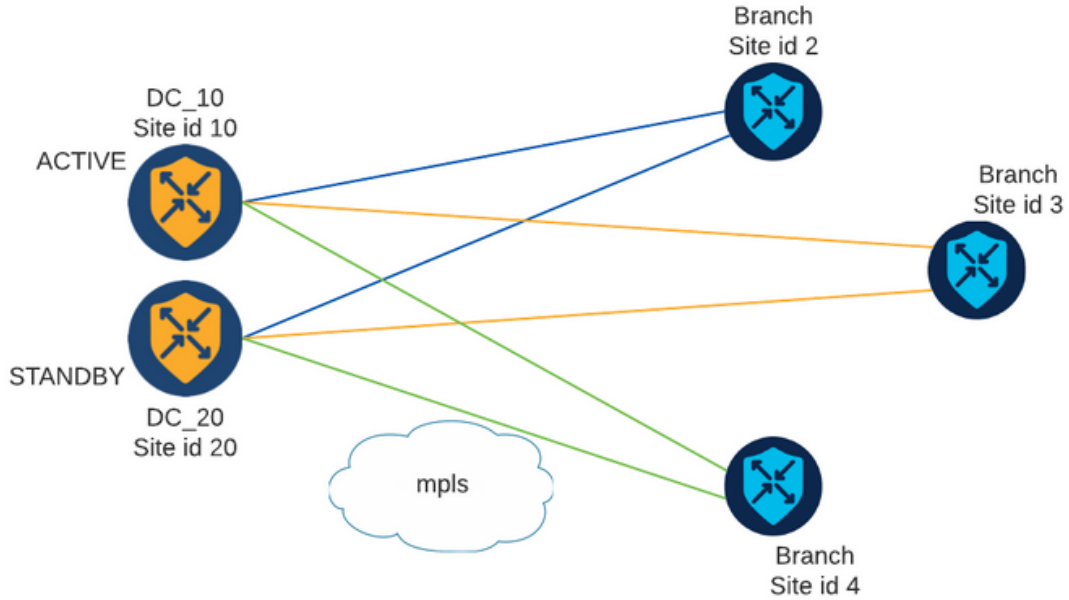
이 문서는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C8000V 버전 17.6.3a
- vManage 버전 20.6.3.1
- vSmart 버전 20.6.3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



사이트 ID가 10 및 20인 허브가 2개 있습니다. 사이트 ID 10은 액티브 허브 역할을 하고 사이트 ID 20은 스탠바이 허브 역할을 합니다. 브랜치는 서로 통신할 수 있지만 모든 통신은 허브를 거쳐야 합니다. 브랜치 사이트 간에는 터널이 생성되지 않아야 합니다.

설정

1. vManage에 로그인하고 Configuration(컨피그레이션) > Policies(정책)로 이동한 후 Add Policy(정책 추가)를 클릭합니다.
2. [관심 그룹 생성] 섹션에서 [TLOC] > [새 TLOC 목록]을 클릭하고 활성 허브에 대한 항목 하나와 대기 허브에 대한 항목 하나를 동일한 목록에 추가합니다.

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

액티브 허브에 대한 기본 설정을 높이고 스탠바이 허브에 대한 기본 설정을 낮추십시오.

3. 지점 > 신규 지점 목록으로 이동하여 지점 지점에 대한 목록과 허브 지점에 대한 목록을 생성합니다.

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. 다음을 클릭합니다. Configure Topology and VPN Membership(토폴로지 및 VPN 멤버십 구성) 섹션에서 Add Topology(토폴로지 추가) > Custom Control(사용자 지정 제어)으로 이동합니다.
- 5. 정책의 이름 및 설명을 추가합니다.
- 6. Sequence Type(시퀀스 유형) > TLOC를 클릭하고 시퀀스 규칙을 추가합니다.
- 7. 대응 > 지점을 선택하고 지점에 대한 지점 목록을 추가한 다음 조치 > 거부를 선택하고 대응 및 조치 저장을 클릭합니다.

TLOC TLOC

Sequence Rule Drag and drop to re-arrange rules

Match **Actions**

Accept Reject

Match Conditions	Actions
<p>Site List ×</p> <p>BRANCHES ×</p> <hr/> <p>Site ID 0-4294967295</p>	<p>Reject Enabled</p>

Cancel Save Match And Actions

- 8. Sequence Rule을 클릭하고 허브 사이트와 일치하는 항목을 추가하고 수락합니다.

TLOC TLOC

Sequence Rule Drag and drop to re-arrange rules

Match **Actions**

Accept Reject

OMP Tag Preference

Match Conditions

Site List ×

DCs_10_20 ×

Site ID: 0-4294967295

Actions

Accept: Enabled

Cancel **Save Match And Actions**

9. 순번 유형 > 경로, 순번 규칙으로 이동합니다.
10. 일치 섹션을 비워 두고, 작업을 수락으로 설정하고, TLOC를 선택하고, 이전에 생성한 TLOC 목록을 추가하고, Save Match And Actions를 클릭합니다.

Route Route

Sequence Rule Drag and drop to re-arrange rules

Match **Actions**

Protocol: IPv4 | Accept Reject

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

Match Conditions

Actions

Accept: Enabled

TLOC List ×

PREFER_DC10_DC20 ×

TLOC IP: Example: 10.0.0.1

Color: Select a color list

Encapsulation: Select an encap

Cancel **Save Match And Actions**

11. 제어 정책 저장을 클릭합니다.
12. [사이트 및 VPN에 정책 적용] 섹션이 시작될 때까지 [다음]을 클릭합니다.
13. Topology(토폴로지) 섹션에서 Control Policy(제어 정책)가 표시되고 New Site List(새 사이트 목록)를 클릭하고 Outbound Site List(아웃바운드 사이트 목록)에 대한 Branches(브랜치) 목록을 선택한 후 Add(추가)를 클릭합니다.

Centralized Policy > Add Policy

✔ Create Groups of Interest
✔ Configure Topology and VPN Membership
✔ Configure Traffic Rules
● Apply Policies to Sites and VPNs

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 CUSTOM CONTROL

+ New Site List

Inbound Site List
Select one or more site lists

Outbound Site List
BRANCHES x

Add Cancel

14. 미리보기를 누르고 정책을 검토합니다.

```
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 mp1s encap ipsec preference 1000
tloc 10.10.10.2 color mp1s 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. 정책 저장을 클릭합니다.

16. Centralized Policy(중앙 집중식 정책) 메뉴에서 새로 생성한 Policy(정책) 오른쪽에 있는 3개의 점을 클릭하고 Activate(활성화)를 선택합니다.

Centralized Policy | Localized Policy

Search

Add Policy

Total Rows: 9

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
Centralized_Active_Stand...	Centralized_Active_Stand...	UI Policy Builder	false	admin	03302023T184504926	30 Mar 2023 6:45:04 PM

- View
- Preview
- Copy
- Edit
- Delete
- Activate

17. 작업이 완료되면 성공 상태가 표시됩니다.

Status	Message	Hostname
Success	Done - Push vSmart Policy	vsmart

다음을 확인합니다.

다음 명령을 사용하여 vSmart에서 정책이 생성되었는지 확인합니다.

```

<#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#

```


 니다. "show sdwan policy from-vsmart" 명령은 에지 디바이스의 정책을 표시하지 않습니다.

문제 해결

문제 해결에 유용한 명령입니다.

vSmart의 경우:

```
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>
```

cEdge의 경우:

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

예:

BFD 세션만 브랜치에서 허브로 구성되었는지 확인합니다.

<#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	mp1s	mp1s	192.168.1.36	192.168.1.30	12386	ipsec	7
10.10.10.2	20	up	mp1s	mp1s	192.168.1.36	192.168.1.33	12366	ipsec	7

다른 브랜치의 경로가 기본 설정 1000인 Active Hub를 통해 기본 설정되었는지 확인합니다.

<#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

관련 정보

[Cisco SD-WAN 정책 컨피그레이션 가이드, Cisco IOS XE 릴리스 17.x](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.