SD-WANオンデマンドトンネルの設定と確認

闪谷		
<u>はじめに</u>		
<u>前提条件</u>		
<u>使用するコンポーネント</u>		
<u>背景</u>		
<u>長所</u>		
<u>設定</u>		
<u>コンフィギュレーション</u>		
<u>確認</u>		
<u>トラブルシュート</u>		
<u>関連情報</u>		

はじめに

このドキュメントでは、SD-WANオンデマンドトンネルを作成するための設定および検証手順に ついて説明します。

前提条件

使用するコンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- vManageバージョン20.9.3
- ・ Ciscoエッジルータバージョン17.9.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景

Cisco SD-WANは、任意の2つのCisco SD-WANスポークデバイス間のダイナミックオンデマンド トンネルをサポートします。これらのトンネルは、2つのデバイス間にトラフィックが存在すると きにのみ設定されるようにトリガーされ、帯域幅の使用率とデバイスのパフォーマンスが最適化 されます。

長所

オンデマンドトンネルには、次の利点があります。

- パフォーマンスの向上。特に、フルメッシュネットワークで動作する処理能力の低いプラットフォームのパフォーマンスが向上します。
- スポーク間でオンデマンドトンネルを使用する際のハブアンドスポーク導入における遅延の 改善。
- 非アクティブ状態のトンネルは双方向フォワーディング検出(BFD)プローブを必要としない ため、ネットワークで生成されるBFDトラフィックが少なくなり、ネットワークの帯域幅使 用量が削減されます。
- CPUとメモリの使用率を最適化しながら、スポーク間の直接トンネル。

設定

コンフィギュレーション

オンデマンドトンネルを設定する手順を次に示します。

手順1:VPN 0機能テンプレートの下のハブサイトルータでのみ、トラフィックエンジニアリング を有効にします。ハブサイトとスポークサイト用に個別のVPN 0機能テンプレートを用意するこ とを推奨します。

Configuration > Templates > Feature Templateの順に移動します。ハブルータに割り当てられた 正しいVPN 0機能テンプレートを検索するには、3つのドットをクリックしてEditを選択します。

1. サービスセクションの下

2. New Serviceをクリックします。

3. サービスタイプからTEを選択します。

Add、Updateの順にクリックします。

\sim	SERVICE	1			
	New Service 2				
	Service Type			\oplus	Choose 🔻
	IPv4 address			•	Choose FW IDS IDP
	Tracking			⊘•	netsvc1 netsvc2 netsvc3 netsvc4
					TE 3

TEの有効化

手順2:CiscoエッジルータでOMPパス制限を推奨値の16に増やす。

Configuration> Template> Feature Templateの順に移動し、OMP機能テンプレートを検索し、3つのドットをクリックしてEditを選択します。

Basic Configurationで、Number of Paths Advertised per Prefix、ECMP Limitの順に探し、値を 16に変更します。

\vee BASIC CONFIGURATION

Graceful Restart for OMP	⊙ ▼ On Off
Overlay AS Number	\odot -
Graceful Restart Timer (seconds)	⊘ - 43200
Number of Paths Advertised per Prefix	● - 16
Number of Paths Advertised per Prefix ECMP Limit	● < 16● < 16
Number of Paths Advertised per Prefix ECMP Limit	 ● ▼ 16 ● ▼ 16 ○ ▼ 16

OMP:ECMP制限



注: vSmarts OMPのsend-path-limitを4より大きい値、推奨値の16に変更する方法の詳細 については、Cisco SD-WAN<u>構成</u>ガイドのルーティング構成ガイドを参照してください。

ステップ3:システム機能テンプレートを作成またはクローニングして、オンデマンドトンネルを 有効にし、必要に応じてオンデマンドトンネルアイドルタイムアウトタイマーを変更します(デ フォルト値は10分)。このシステムテンプレートをオンデマンドスポークサイト専用に適用しま す。

Configuration > Templates > Feature Templates の順に移動し、System機能テンプレートを検索 します。次に、3つのドットをクリックして、Editを選択します。

On Advanced セクション: On-demand Tunnelを有効にします。 サイト間でトラフィックの受け 渡しがない場合に、デフォルトの10分よりも早くトンネルをダウンさせるには、オプションでオ ンデマンドのトンネルのアイドルタイムアウトを調整します。

Gateway Tracking	⊙ ▼ O On Off
Collect Admin Tech on Reboot	⊙ ▼ O On Off
Idle Timeout	⊘ -
On-demand Tunnel	● • On Off
On-demand Tunnel Idle Timeout(min)	⊕ - 2

オンデマンドトンネルの有効化

ステップ4:matchタブセットサイトリスト(一致するオンデマンドスポークサイト)でルートシー ケンスを使用してカスタムトポロジポリシーを作成し、actionタブでTLOCリスト(一致する Hubのtlocs)をbackupに設定する必要があります。

オンデマンドのスポークリストとHUBバックアップTLOCリストを作成します。

ドロップダウンメニューからConfiguration > Policies > Custom Optionsの順に移動し、 Centralized Policy > Listsの順に選択して、対象のグループを作成します。

- Siteをクリックして、すべてのオンデマンドサイトのすべてのサイトIDを含む新しいサイト リストを作成します。
- TLOCで、バックアップとして使用されるすべてのHUB tlocを含むTLOCリストを作成します。

対象のグループのリストを作成したら、ドロップダウンメニューからCustom Optionsに移動し、 Centralized Policy > Topology > Topology > Add Topology > Custom Control (Route & TLOC)の順 に選択します。

- ・ トポロジの名前と説明を入力します。
- 鉛筆のアイコンをクリックし、Save Match And Actionをクリックして、デフォルトアクションをAcceptに変更します。
- Sequence Typeをクリックして、Routeを選択します。新しいシーケンスを追加するには、 Sequence Ruleをクリックします。
- MatchタブでSiteをクリックし、正しいサイトリストを選択します。

	Route Sequence Rule Drag and drop to re-arrange rules			
0	Protocol IPv4 -	Color List Community List	Expanded Community List OMP Tag Ori	gin Originator Preference Site Regi
	Match Conditions			Actions
	Site List 🚺		×	Reject Enabled
	Branches-ON-Demand ×		*	
	Site ID	0-4294967295		

シーケンスの作成

 ActionタブでAcceptをクリックし、TLOC ActionでBackupを選択し、TLOC で正しい TLOCリストを選択します。完了したら、Save Match and Actionsをクリックします。

• Accept • Reject	Community Export To	Actions OMP Tag	Preference Service	TLOC Action TLOC
			Actions	
		×	Accept	Enabled
		*	TLOC Action	
0-4294967295			Backup ×	
			TLOC List	
			DC ×	

Configuration > Policies > Centralized Policyの順に移動して、制御トポロジポリシーをメインポリシーに割り当てます。

アクティブなポリシーを検索し、3つのドットをクリックしてEditを選択します。

クリック

1.トポロジ

- 2.トポロジ
- 3. トポロジの追加

4.既存のインポート

5.カスタムコントロール(ルートおよびTLOC)

アクションポリシーセット

6. ドロップダウンメニューからポリシーを検索し、[インポート]をクリックします。

		Policy Application Topology Oraffic Rules	
Specify your network topology Topology VPN Membership	Import Existing Topo	logy 🕢	_
Q Search Add Topology 3	Policy Type	Hub And Spoke O Mesh O Custom Control (Route and TLOC) 5	
	Policy	Select a policy to import	
Name		Search	
on-demond		Branch-Region2-Outbound-Policy on-demond 6	- pc

既存のポリシーのインポート

Policy Application > Topology > New Site/Region Listの順にクリックします。

アウトバウンドのサイトリストで、正しいサイトリスト名を選択します。

Add policies to sites an	d VPNs				
Policy Name*	main_policy				
Policy Description*	main_policy				
Topology Applicat	ion-Aware Routing	Traffic Data	Cflowd	Role Mapping for Regions	
New Site/Region	List 3				
🔵 Site List 🔵 Regi	on 🚺				
Inbound Site List					
Select one or more site lists					
Outhound Site List					
Outbound Site List					

ポリシーアウトバンドの適用

Addをクリックし、Save Policy Changesをクリックします。これはアクティブなポリシーである ため、変更はvSmartsにプッシュされます。



注:Cisco vSmart Controller集中制御ポリシーの設定については、『<u>Cisco SD-WAN設定ガ</u> <u>イド</u>』を参照してください。

確認

確認するには、show sdwan system on-demand remote-systemコマンドを実行します。 出力から 、On-demand: yesを見つけることができます。 ステータスがinactiveの場合は、サイト間のトン ネルがダウンしていることを示しています。

<#root>

Spoke#sho	ow sdwan system	on-demand rem	ote-system	
SITE-ID	SYSTEM-IP	ON-DEMAND	STATUS	<pre>IDLE-TIMEOUT-EXPIRY(sec)</pre>
100	192.168.0.70	no	-	-
100	192.168.0.71	no	-	-

1000	192.168.0.72	yes	inactive	-
1000	192.168.0.73	yes	inactive	-
200	192.168.0.80	no	-	-

オンデマンドサイト間でトラフィックを生成した後、同じ出力を確認できます。この場合、ステ ータスはActiveを示し、トンネルがダウンするまでの残り秒数を示します。

<#root>

Spoke#sh	ow sdwan system	on-demand rem	ote-system	
SITE-ID	SYSTEM-IP	ON-DEMAND	STATUS	IDLE-TIMEOUT-EXPIRY(sec)
100	192.168.0.70	no	-	-
100	192.168.0.71	no	-	-
1000	192.168.0.72	yes	active	105
1000	192.168.0.73	yes	active	105
200	192.168.0.80	no	-	-

この例では、トンネルのダウン時にサイト192.168.0.72と192.168.0.73のBFDが消失していることが確認できます。

Spoke#show sdwan bfd sessions

SYSTEM IP	SITE ID	STATE	SOURCE TLOC R COLOR	EMOTE TLOC COLOR	SOURCE IP
192.168.0.70	100	 up	public-internet	public-internet	<pre><removed></removed></pre>
192.168.0.71	100	up	public-internet	public-internet	<removed></removed>
192.168.0.80	200	up	public-internet	public-internet	<removed></removed>
192.168.0.70	100	up	mpls	mpls	<removed></removed>
192.168.0.71	100	up	mpls	mpls	<removed></removed>
192.168.0.80	200	up	mpls	mpls	<removed></removed>

サイト間のトンネルがアップしているときに、サイト192.168.0.72と192.168.0.73のBFDがアッ プしていることに気付きます。

<#root>

Spoke#show sdwan bfd sessions

			SOURCE TLOC	REMOTE TLOC	
SYSTEM IP	SITE ID	STATE	COLOR	COLOR	SOURCE IP

192.168.0.70 10	0 up	public-internet	public-internet	<removed></removed>	
192.168.0.71 10	0 up	public-internet	public-internet	<removed></removed>	<re< td=""></re<>
192.168.0.80 20	0 up	public-internet	public-internet	<removed></removed>	<re< td=""></re<>
192.168.0.73 10	00 up	public-internet	public-internet	<removed></removed>	<rer< td=""></rer<>
192.168.0.72 10	00 up	public-internet	public-internet	<removed></removed>	<rei< td=""></rei<>
0.00.00.	03 2				
102 168 0 70 10	0.5 2	mple	mnlc	(nomo) (od)	(19.0)
192.168.0.70 10	up up	mpis	mpis	<removed></removed>	<re< td=""></re<>
192.168.0.71 10	0 up	mpls	mpls	<removed></removed>	<rei< td=""></rei<>
192.168.0.80 20	0 up	mpls	mpls	<removed></removed>	<re< td=""></re<>
192.168.0.73 10	00 up	mpls	mpls	<removed></removed>	<rei< td=""></rei<>
192.168.0.72 10	00 up	mpls	mpls	<removed></removed>	<re< td=""></re<>

vMange GUIでMonitor > DeviceまたはMonitor > Network(コード20.6以前)に移動し、デバイス を見つけてWAN > Tunnelに移動し、Down番号に注目することで、同じ結果を得ることができま す。

SSL Proxy	
AppQoE TCP Optimization	Chart Options 🗸
AppQoE DRE Optimization	C C Los
Connection Events	E E
WAN Throughput	Jan 31, 20:00 Jan 31, 22:00 Feb 01, 00:00 Feb 01, 02:00 Feb 01, 04:00 Feb 01, 06:00 Feb 01, 08:00 Feb 01, 10:00 Feb 01, 12:00 Feb 01, 14:00
Flows	
Top Talkers	Q. Search
WAN	6 Rows Selected (Interface Endpoints, Local Interface Description and Remote Interface Description are hidden by default. Please click on the Columns dropdown on the right to en
TLOC	
Tunnel	↓ Down (4) 🔇 Init (0) ↑ Up (6)
	Y Tunnel Endpoints Interface Endpoints Local Interface Description Remote Interface Description Protocol State
Eirewall	✓ public-internet

オンデマンドトンネルの監視

同じメニューで、下にスクロールしてReal Timeをクリックします。 デバイスオプションで、オ ンデマンドでリモートを検索します。

次の例は、オンデマンドトンネルがダウンした場合の出力を示します。

Device Options: Q On Demand Remote				
Q Search				
System IP	Site ID	On Demand	Status	Idle Timeout Expiry
192.168.0.70	100	no		-
192.168.0.71	100	no	-	-
192.168.0.72	1000	yes	inactive	-
192.168.0.73	1000	yes	inactive	-
192.168.0.80	200	no		

オンデマンドのトンネルダウン

次の例は、オンデマンドトンネルが稼働しているときの出力を示します。

Device Options: Q On Demand	Remote			
Q Search				
System IP	Site ID	On Demand	Status	Idle Timeout Expiry
192.168.0.70	100	no	-	-
192.168.0.71	100	no	-	
192.168.0.72	1000	yes	active	111
192.168.0.73	1000	yes	active	111
192.168.0.80	200	no		

オンデマンドのトンネルアップ

トラブルシュート

詳細な手順については、『<u>SD-WANダイナミックオンデマンドトンネルのトラブルシューティン</u> <u>グ</u>』を参照してください。

関連情報

• シスコのテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。