Cisco IOS® XE SD-WAN cEdgeルータでのTCP最適化機能の設定

内容

概要

このドキュメントでは、2019年8月の16.12リリースで導入されたCisco IOS® XE SD-WANルータのTransmission Control Protocol(TCP)最適化機能について説明します。取り上げるトピックは、前提条件、問題の説明、ソリューション、Viptela OS(vEdge)とXE SD-WAN(cEdge)のTCP最適化アルゴリズムの違い、設定、検証、および関連ドキュメントのリストです。

前提条件

要件

このドキュメントに特有の要件はありません。

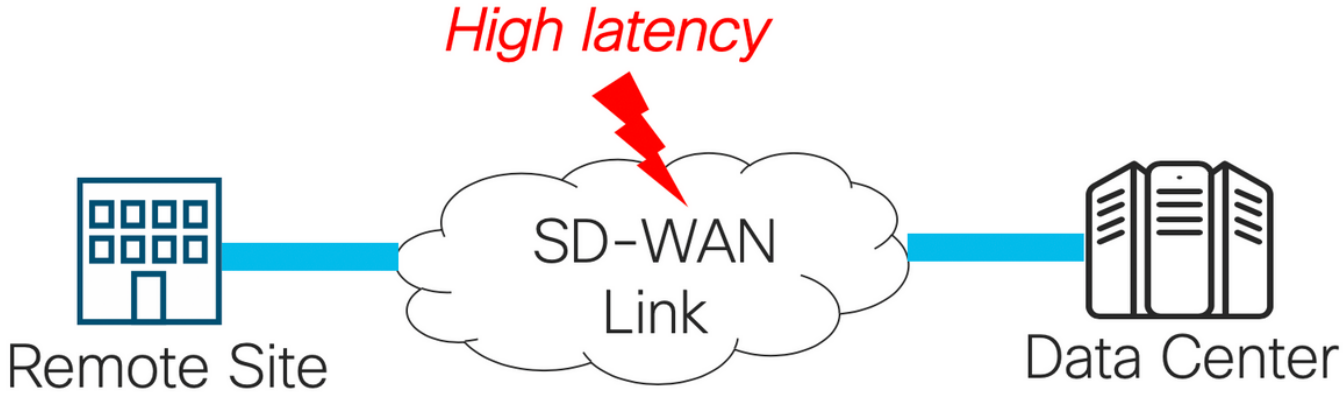
使用するコンポーネント

このドキュメントの情報は、Cisco IOS® XE SD-WANに基づくものです。

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、初期（デフォルト）設定の状態から起動しています。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。

問題

2つのSD-WAN側の間のWANリンクで高い遅延が発生すると、アプリケーションパフォーマンスが低下します。重要なTCPトラフィックがあるため、最適化する必要があります。



解決方法

TCP最適化機能を使用すると、2つのSD-WANサイト間の重要なTCPフローの平均TCPスループットが向上します。

cEdge Bottleneck Bandwidth and Round-trip(BBR)とvEdge(CUBIC)でのTCP最適化の概要と相違点について説明します。

XE SD-WAN実装(cEdge)では、高速BBR伝搬時間アルゴリズムが使用されます。

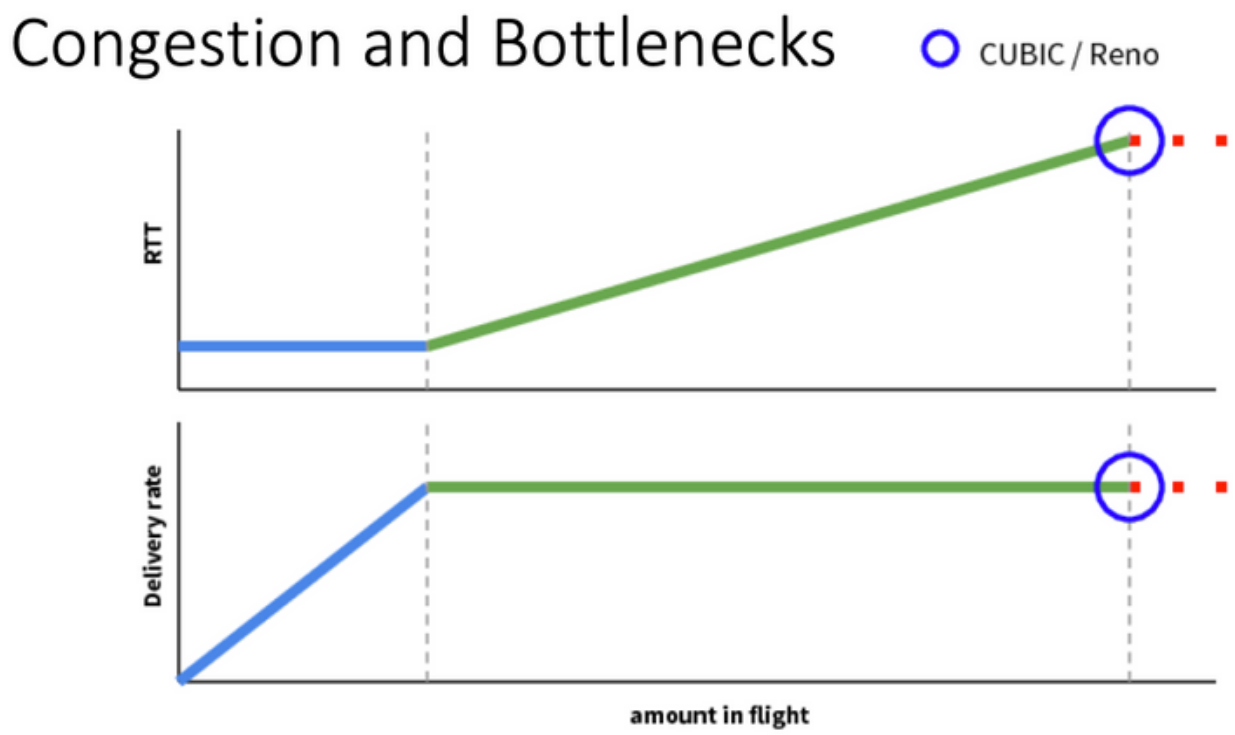
Viptela OS(vEdge)には、CUBICと呼ばれる異なる古いアルゴリズムがあります。

CUBICは主にパケット損失を考慮し、さまざまなクライアントオペレーティングシステムで広く実装されています。Windows、Linux、MacOS、AndroidにはすでにCUBICが組み込まれています。CUBICを使用せずにTCPスタックを実行している古いクライアントがある場合、vEdgeでTCP最適化を有効にすると改善が得られます。vEdge TCP CUBICの最適化が役立つ例の1つは、古いクライアントホストとWANリンクを使用する潜水艦で、大幅な遅延/ドロップが発生することです。TCP CUBICをサポートしているのはvEdge 1000とvEdge 2000だけです。

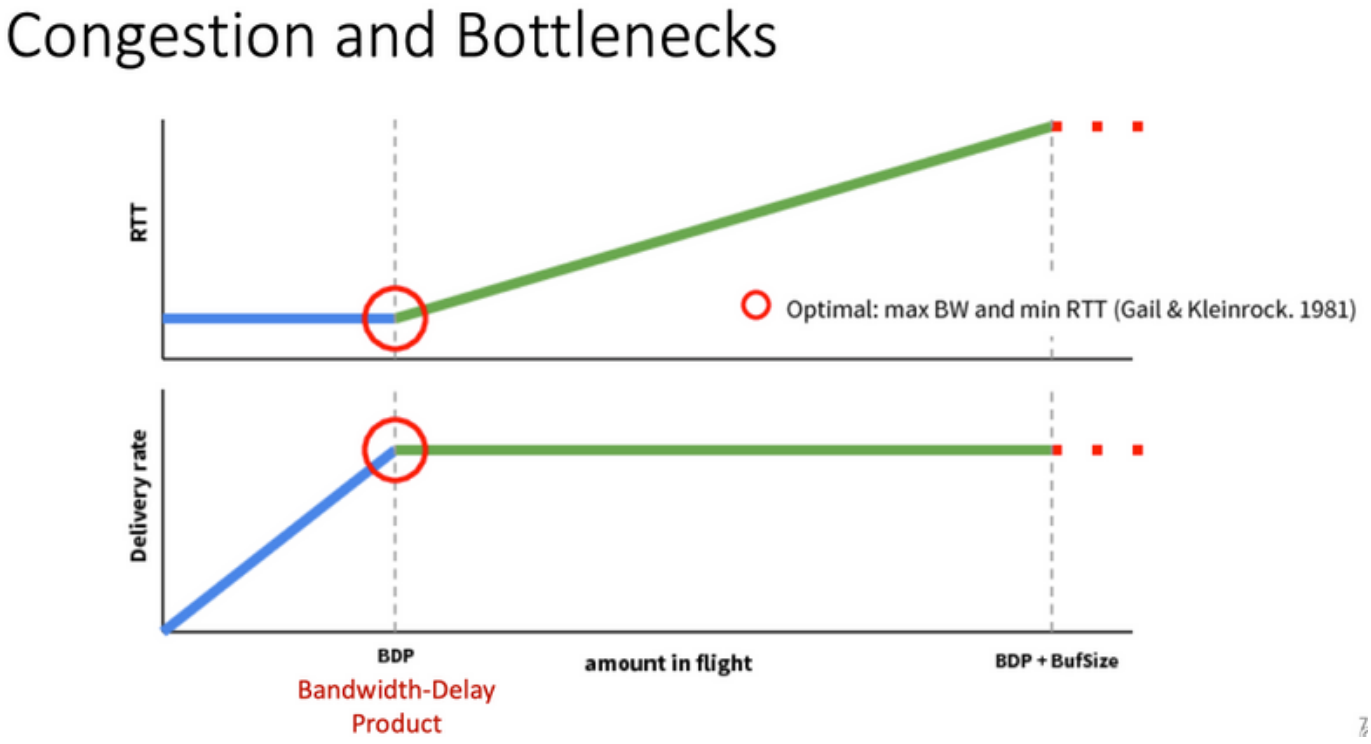
BBRは、主にラウンドトリップ時間と遅延に重点を置いています。パケット損失ではない。米国西部から東海岸、さらにはヨーロッパまでパブリックインターネットを介してパケットを送信する場合、ほとんどの場合、パケット損失は発生しません。パブリックインターネットは、パケット損失の点で非常に優れている場合があります。しかし、遅延/遅延が発生します。そして、この問題は、2016年にGoogleによって開発されたBBRによって対処されています。

つまり、BBRはネットワークをモデル化し、各確認応答(ACK)を確認し、最大帯域幅(BW)と最小ラウンドトリップ時間(RTT)を更新します。 次に、制御送信はモデルに基づきます。最大BWと最小RTTをプローブし、推定BWに近いペースで進み、Bandwidth-Delay-Product(BDP)に近い状態を維持します。 主な目標は、ボトルネックの少ないキューで高スループットを確保することです。

Mark Claypoolのこのスライドは、CUBICが動作するエリアを示しています。



BBRは、Mark Claypoolからも提供されている、より適切な場所で動作します。



BBRのアルゴリズムの詳細については、bbr-devメーリングリストのホームページHereの上部に、BBRに関するいくつかの出版物がリンクされています。

ここまでの内容をまとめます。

プラットフォームとアルゴリズム	キー入力パラメーター	使用例
cEdge(XE SD-WAN):BBR	RTT/遅延	2つのSD-WANサイト間の重要なTラフィック
vEdge(Viptela OS):キュービップ	パケット損失	TCP最適化のない古いクライアン

サポートされるXE SD-WANプラットフォーム

XE SD-WAN SWリリース16.12.1dでは、次のcEdgeプラットフォームがTCP最適化BBRをサポートしています。

- ISR4331
- ISR4351
- CSR1000v（8 vCPUおよび最小）メモリ 8 GB

警告

- DRAMが8 GB未満のプラットフォームは、現在サポートされていません。
- 4コア以下のプラットフォームは現在サポートされていません。
- TCP最適化はMTU 2000をサポートしていません。
- 現在、IPv6トラフィックはサポートされていません。
- サードパーティBBRサーバへのDIAトラフィックの最適化はサポートされていません。両側にcEdge SD-WANルータが必要です。
- 現在のデータセンターのシナリオでは、1つの制御ノード(CN)につき1つのサービスノード(SN)だけがサポートされます。
- 現在、同じデバイス上でセキュリティ（UTDコンテナ）とTCP最適化を組み合わせたユースケースはサポートされていません。

注：ASR1kは現在、TCP最適化をサポートしていません。ただし、ASR1kにはASR1kがAppNavトンネル（GREカプセル化）を介してTCPトラフィックを外部CSR1kvに送信して最適化するソリューションがあります。現在（2020年2月）、外部サービスノードとしてサポートされているCSR1kは1つだけです。これについては、「設定」セクションで後述します。

次の表に、リリースごとの注意事項をまとめ、サポートされるハードウェアプラットフォームを示します。

シナリオ	使用例	16.12.1	17.2.1	17.3.1	17.4.1	注
ブランチからインターネット	直径	No	Yes	**Yes**	**Yes**	16.12.1では、AppQFIAがインターネッンターフェイスで有なっていません
	SAAS	No	Yes	**Yes**	**Yes**	16.12.1では、AppQFIAがインターネッンターフェイスで有なっていません
ブランチからDC	シングルエッジルータ	No	No	**EFT**	**Yes**	複数のSNをサポート必要がある
	複数のエッジルータ	No	No	**EFT**	**Yes**	フローの対称性またAppnavフロー同期がです。16.12.1でテスれていない
	複数のSN	No	No	**EFT**	**Yes**	複数のSN IPを受けるvManageの拡張
ブランチ間	フルメッシュネットワーク（スポーク間）	**Yes**	**Yes**	**Yes**	**Yes**	

	ハブアンドスポーク（スポーク – ハブスポーク）	No	Yes	Yes	Yes
BBRサポート	BBRによるTCP最適化	部分的	部分的	Full	Full
プラットフォーム	サポート対象プラットフォーム	4300とCSRのみ	ISR1100以外	すべて	すべて

設定

TCP最適化には、SNとCNの概念が使用されます。

- SNはデーモンであり、TCPフローの実際の最適化を行います。
- CNはAppNavコントローラと呼ばれ、トラフィックの選択とSNとの間の転送を行います。

SNとCNは、同じルータ上で実行することも、異なるノードとして分離することもできます。

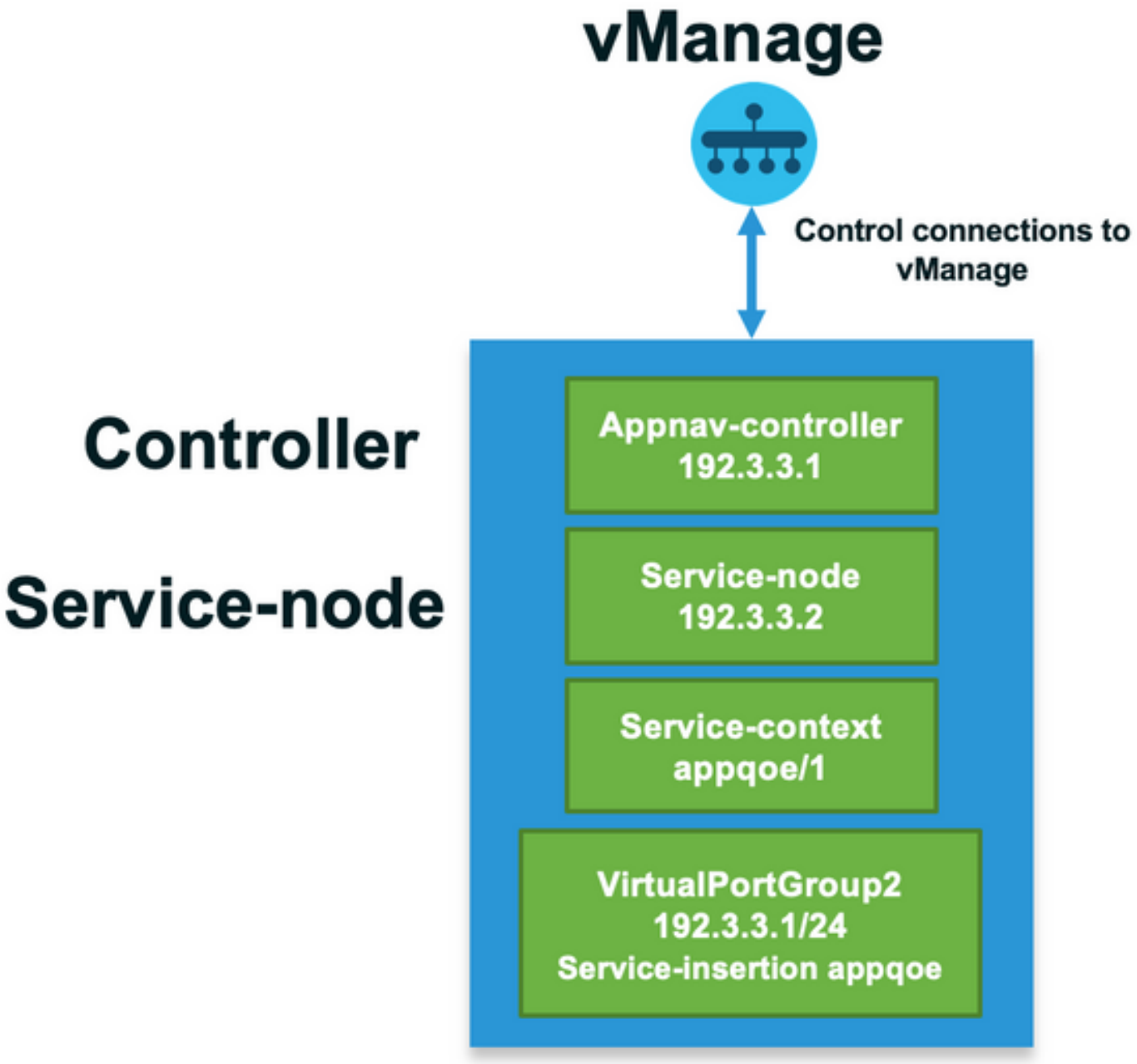
主な使用例は2つあります。

1. 同じISR4kルータ上でSNとCNが実行されているブランチの使用例。
2. データセンターのユースケース。CNはASR1kで実行され、SNは別のCSR1000v仮想ルータで実行されます。

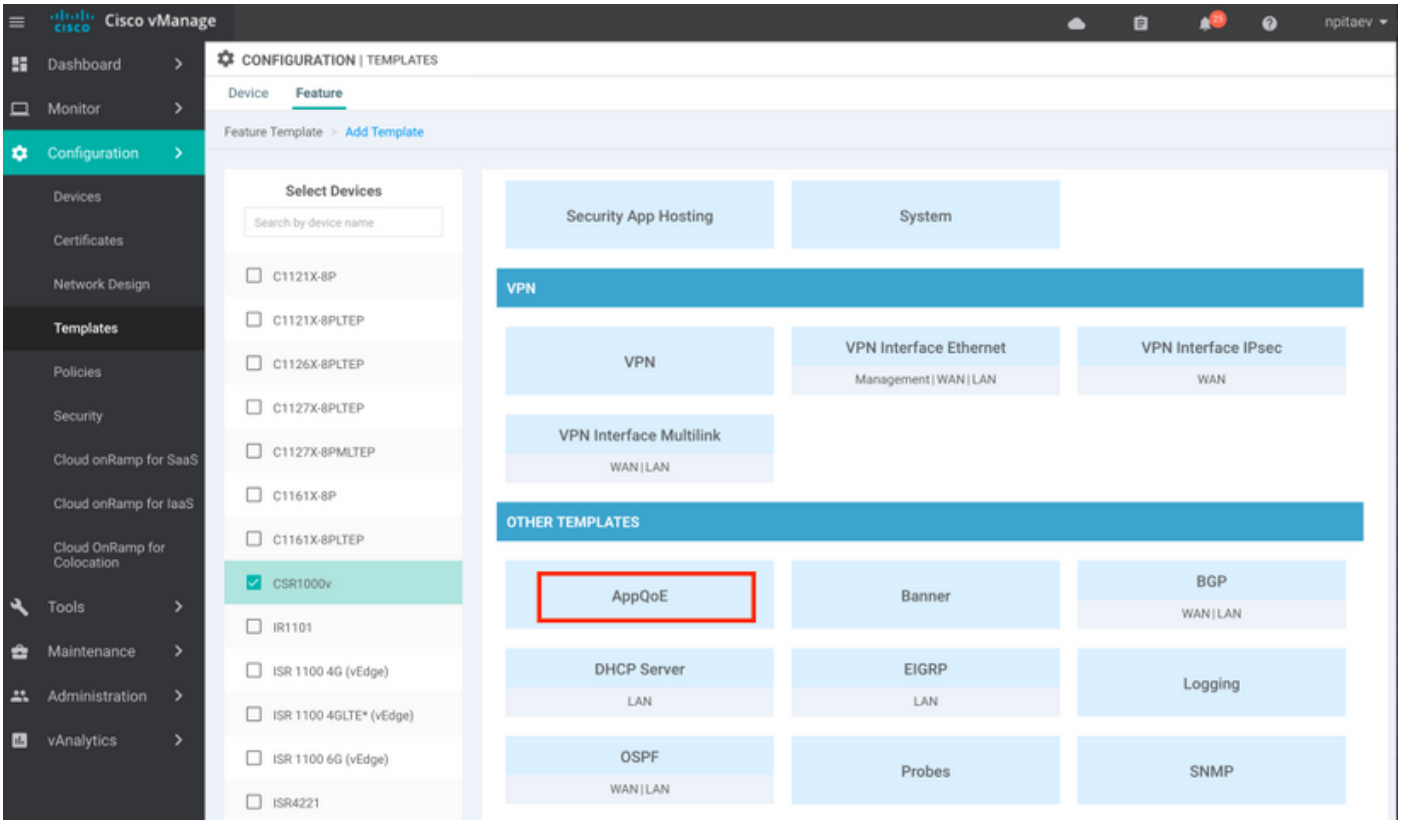
このセクションでは、両方の使用例について説明します。

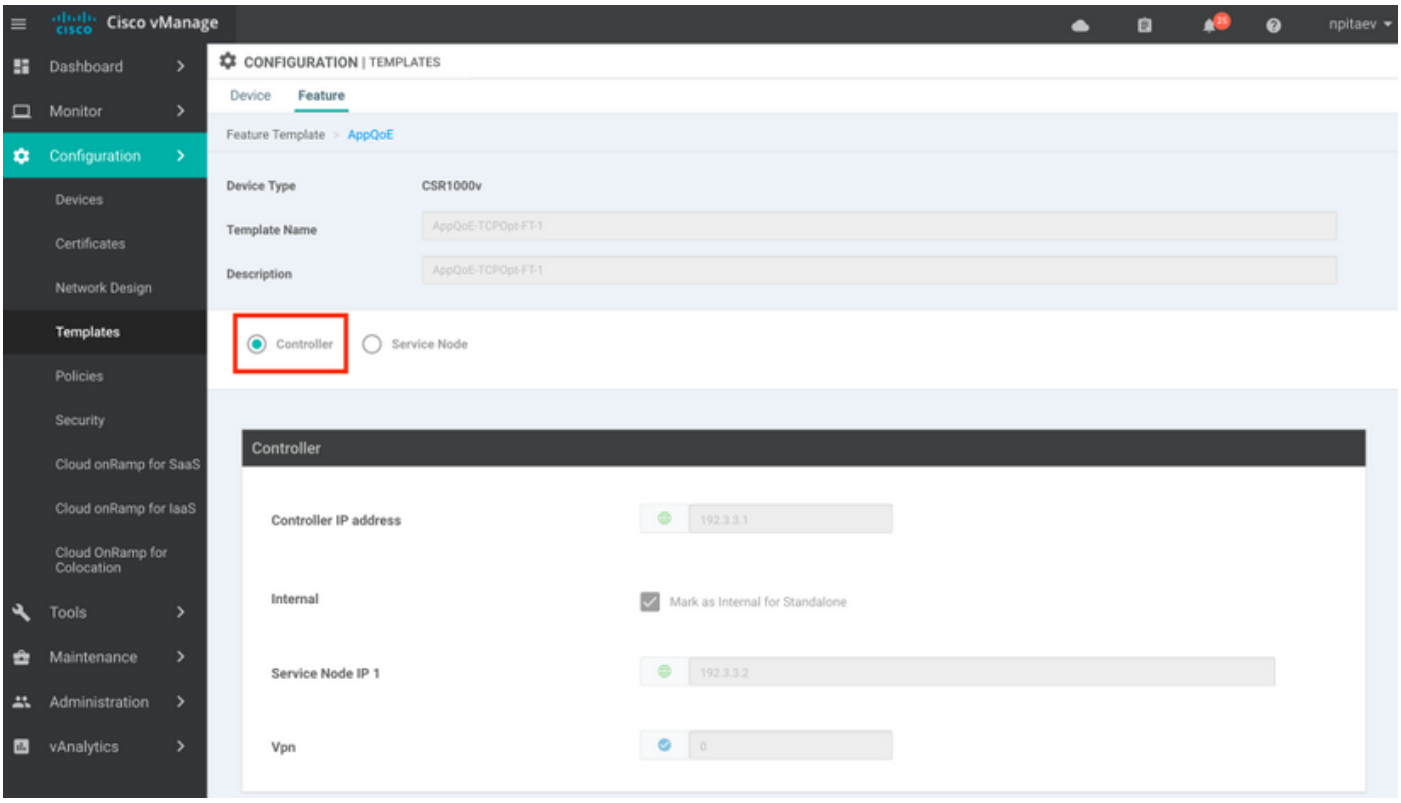
使用例1：ブランチでのTCP最適化の設定（すべて1つのcEdge内）

次の図は、ブランチの単一スタンドアロンオプションの全体的な内部アーキテクチャを示しています。

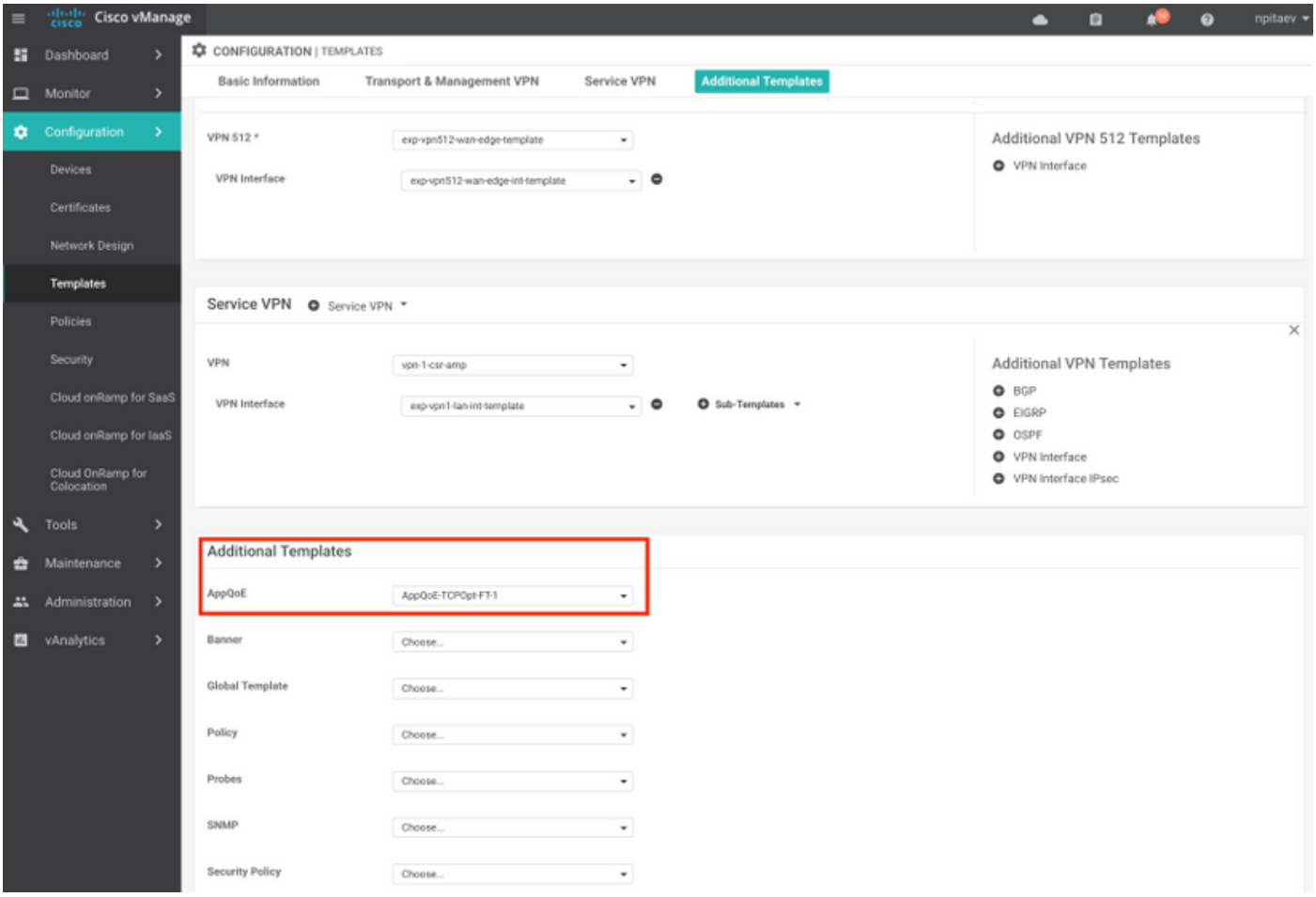


ステップ1:TCP最適化を設定するには、vManageでTCP最適化用の機能テンプレートを作成する必要があります。図に示すように、[Configuration] > [Templates] > [Feature Templates] > [Other Templates] > [AppQoE] に移動します。





ステップ2:[Additional Templates] で、AppQoE機能テンプレートを適切なデバイステンプレートに追加します。

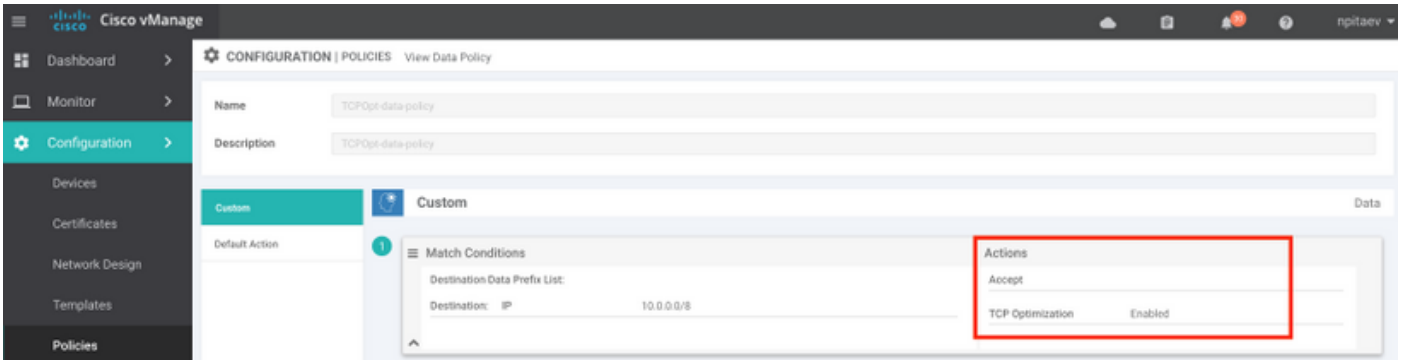


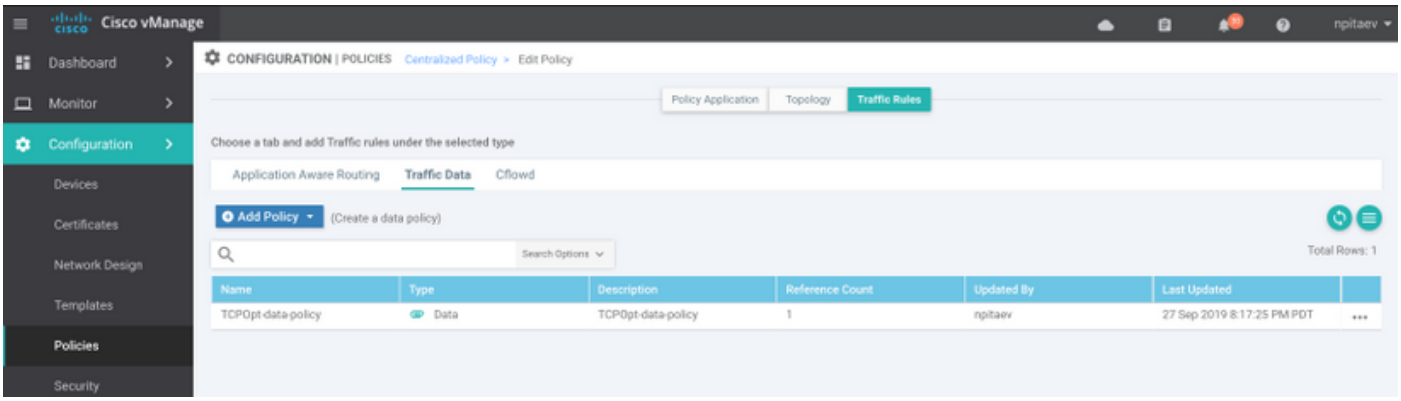
テンプレート設定のCLIプレビューを次に示します。

```
service-insertion service-node-group appqoe SNG-APPQOE
service-node 192.3.3.2
!
service-insertion appnav-controller-group appqoe ACG-APPQOE
appnav-controller 192.3.3.1
!
service-insertion service-context appqoe/1
appnav-controller-group ACG-APPQOE
service-node-group SNG-APPQOE
vrf global
enable
! !
interface VirtualPortGroup2
ip address 192.3.3.1 255.255.255.0
no mop enabled
no mop sysid
service-insertion appqoe
!
```

ステップ3：最適化のための対象TCPトラフィックの定義を使用して、中央集中型データポリシーを作成します。

以下に例を示します。このデータポリシーは、送信元アドレスと宛先アドレスを含むIPプレフィックス10.0.0.0/8に一致し、TCP最適化を有効にします。





vSmartポリシーのCLIプレビューを次に示します。

```
policy
 data-policy _vpn-list-vpn1_TCPOpt_1758410684
  vpn-list vpn-list-vpn1
    sequence 1
     match
      destination-ip 10.0.0.0/8
     !
     action accept
      tcp-optimization
     !
    !
  default-action accept
 !
 lists
  site-list TCPOpt-sites
   site-id 211
   site-id 212
  !
  vpn-list vpn-list-vpn1
   vpn 1
  !
 !
!
apply-policy
 site-list TCPOpt-sites
  data-policy _vpn-list-vpn1_TCPOpt_1758410684 all
 !
!
```

使用例2：外部SNを使用したデータセンターでのTCP最適化の設定

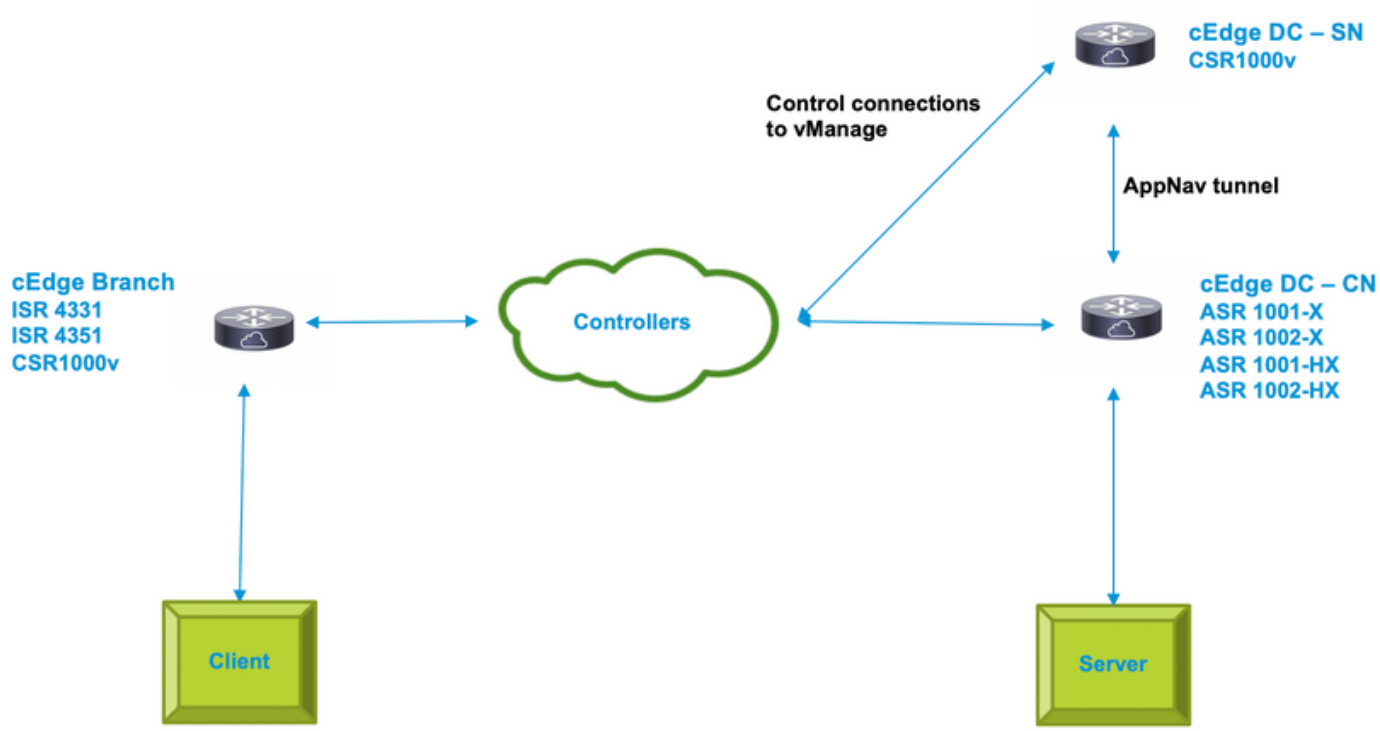
ブランチユースケースの主な違いは、SNとCNの物理的な分離です。オールインワンブランチの使用例では、仮想ポートグループインターフェイスを使用して、同じルータ内で接続が行われま

す。データセンターの使用例では、CNとして動作するASR1kとSNとして動作する外部CSR1kの間にAppNav GREカプセル化トンネルがあります。CNと外部SNの間に専用リンクやクロスコネクトは必要なく、シンプルなIP到達可能性で十分です。

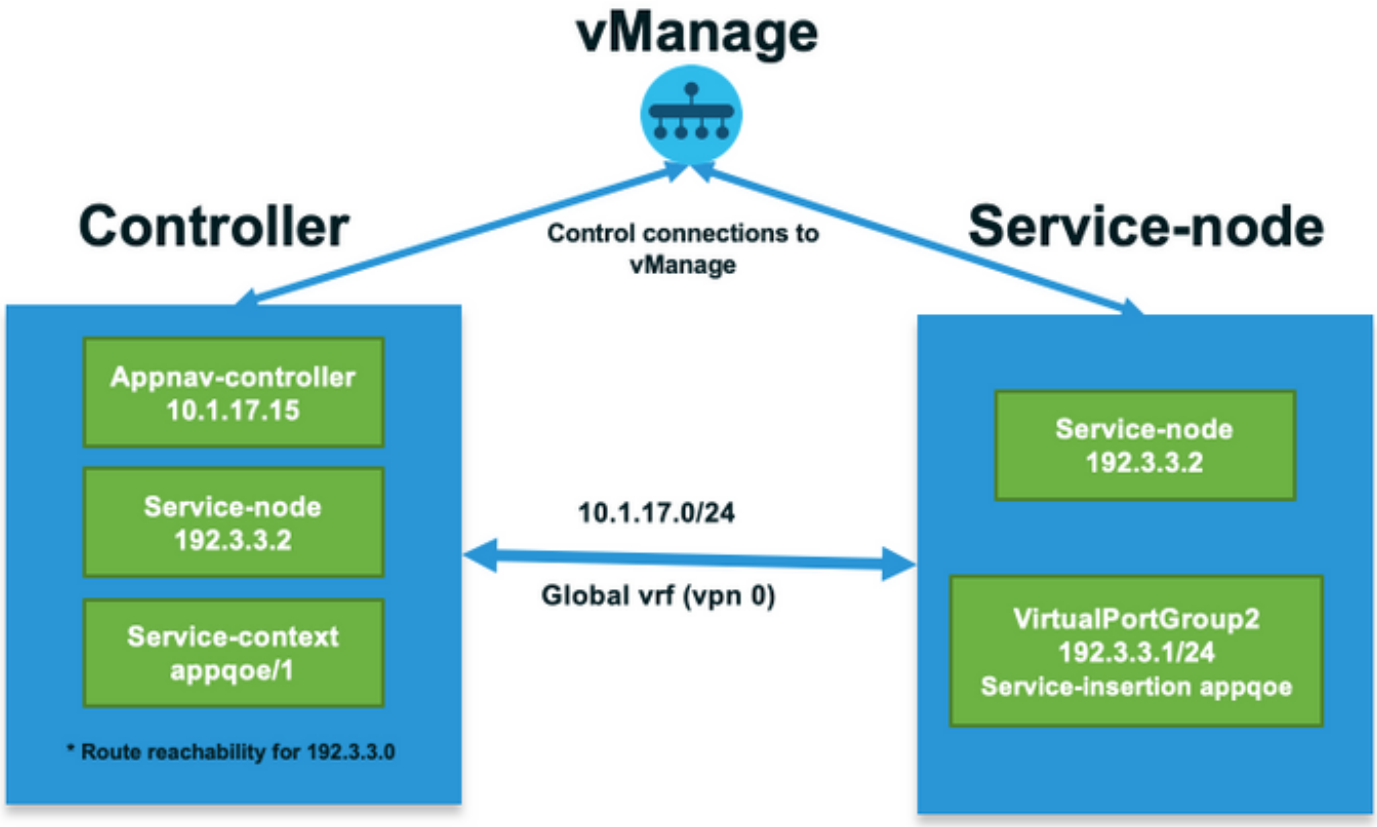
SNごとに1つのAppNav(GRE)トンネルがあります。複数のSNがサポートされている将来の使用のために、CNとSN間のネットワークに/28サブネットを使用することをお勧めします。

SNとして機能するCSR1kには2つのNICが推奨されます。SNをvManageで設定/管理する必要がある場合は、SD-WANコントローラ用の2つ目のNICが必要です。SNを手動で設定/管理する場合、2番目のNICはオプションです。

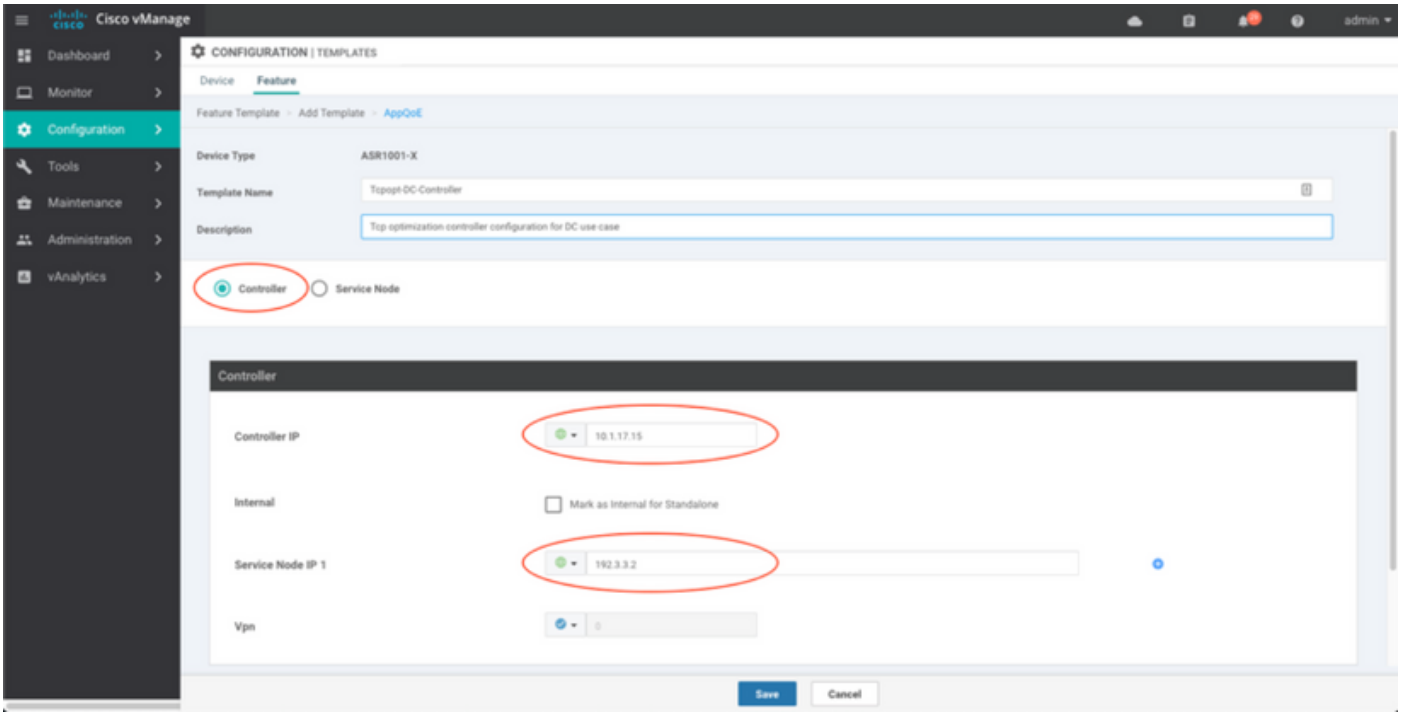
次の図は、CNとして動作するデータセンターASR1kと、サービスノードSNとして動作するCSR1kvを示しています。



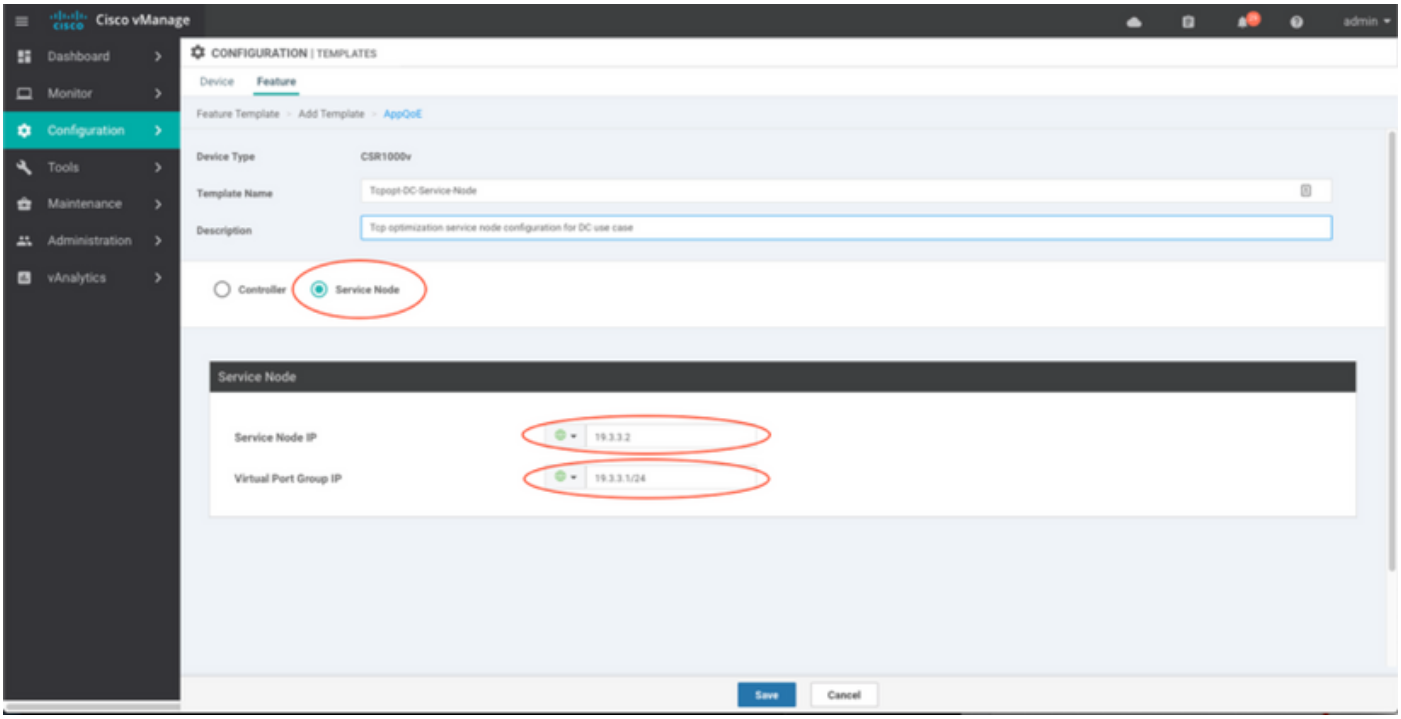
ASR1kおよび外部CSR1kを使用するデータセンターの使用例のトポロジを次に示します。



次のAppQoE機能テンプレートは、コントローラとして設定されたASR1kを示しています。



外部サービスノードとして設定されたCSR1kを次に示します。



フェールオーバーケース

外部CSR1kに障害が発生した場合の、CSR1kがSNとして機能するデータセンターの使用例でのフェールオーバー：

- SN上のTCPセッションが終了するため、既存のTCPセッションは失われます。
- 新しいTCPセッションは最終宛先に送信されますが、TCPトラフィックは最適化されません（バイパス）。
- SN障害の場合、対象トラフィックに対するブラックホールは発生しません。

フェールオーバー検出はAppNavハートビートに基づいており、1秒あたり1ビートです。3つまたは4つのエラーの後、トンネルはダウンとして宣言されます。

ブランチでのフェールオーバーも同様です。SN障害の場合、トラフィックは最適化されずに直接宛先に送信されます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

次のCLIコマンドを使用してCLIでTCP最適化を確認し、最適化されたフローの要約を確認します。

```
BR11-CSR1k#show plat hardware qfp active feature sdwan datapath appqoe summary
TCPOPT summary
----------------
  optimized flows     : 2
  expired flows       : 6033
  matched flows       : 0
  divert pkts         : 0
  bypass pkts         : 0
  drop pkts           : 0
  inject pkts         : 20959382
```

```
  error pkts         : 88
BR11-CSR1k#
```

次の出力は、最適化されたフローに関する詳細情報を示します。

```
BR11-CSR1k#show platform hardware qfp active flow fos-to-print all
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
     GLOBAL CFT  ~  Max Flows:2000000   Buckets Num:4000000
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Filtering parameters:
    IP1 : ANY
    Port1 : ANY
    IP2 : ANY
    Port2 : ANY
    Vrf id : ANY
    Application: ANY
    TC id: ANY
    DST    Interface id: ANY
    L3 protocol : IPV4/IPV6
    L4 protocol : TCP/UDP/ICMP/ICMPV6
    Flow type : ANY
Output parameters:
    Print CFT internal data ? No
    Only print summary ? No
    Asymmetric : ANY
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
keyID: SrcIP SrcPort DstIP DstPort L3-Protocol L4-Protocol vrfID
==================================================================
   key #0: 192.168.25.254 26113 192.168.25.11 22 IPv4 TCP 3
   key #1: 192.168.25.11 22 192.168.25.254 26113 IPv4 TCP 3
==================================================================
   key #0: 192.168.25.254 26173 192.168.25.11 22 IPv4 TCP 3
   key #1: 192.168.25.11 22 192.168.25.254 26173 IPv4 TCP 3
==================================================================
   key #0: 10.212.1.10 52255 10.211.1.10 8089 IPv4 TCP 2
   key #1: 10.211.1.10 8089 10.212.1.10 52255 IPv4 TCP 2

Data for FO with id: 2
-------------------------
appqoe: flow action DIVERT, svc_idx 0, divert pkt_cnt 1, bypass pkt_cnt 0, drop pkt_cnt 0,
inject pkt_cnt 1, error pkt_cnt 0, ingress_intf Tunnel2, egress_intf GigabitEthernet3
==================================================================
   key #0: 10.212.1.10 52254 10.211.1.10 8089 IPv4 TCP 2
   key #1: 10.211.1.10 8089 10.212.1.10 52254 IPv4 TCP 2

Data for FO with id: 2
-------------------------
appqoe: flow action DIVERT, svc_idx 0, divert pkt_cnt 158, bypass pkt_cnt 0, drop pkt_cnt 0,
inject pkt_cnt 243, error pkt_cnt 0, ingress_intf Tunnel2, egress_intf GigabitEthernet3
==================================================================
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
           Number of flows that passed filter: 4
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
                       FLOWS DUMP DONE.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

BR11-CSR1k#
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco IOS XE SD-WANリリース16.12.xのリリースノート
- Cisco SD-WANリリース19.1、19.2:TCP最適化ガイドの設定
- Cisco SD-WAN vEdge向けTCP最適化の設定
- **テクニカル サポートとドキュメント – Cisco Systems**

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。