Configurar o recurso de otimização TCP nos roteadores Cisco IOS® XE SD-WAN cEdge

Contents

Introduction

Este documento descreve o recurso de otimização do Transmission Control Protocol (TCP) nos roteadores SD-WAN Cisco IOS® XE, que foi introduzido na versão 16.12 em agosto de 2019. Os tópicos abordados são pré-requisitos, descrição do problema, solução, as diferenças nos algoritmos de otimização TCP entre Viptela OS (vEdge) e XE SD-WAN (cEdge), configuração, verificação e lista de documentos relacionados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

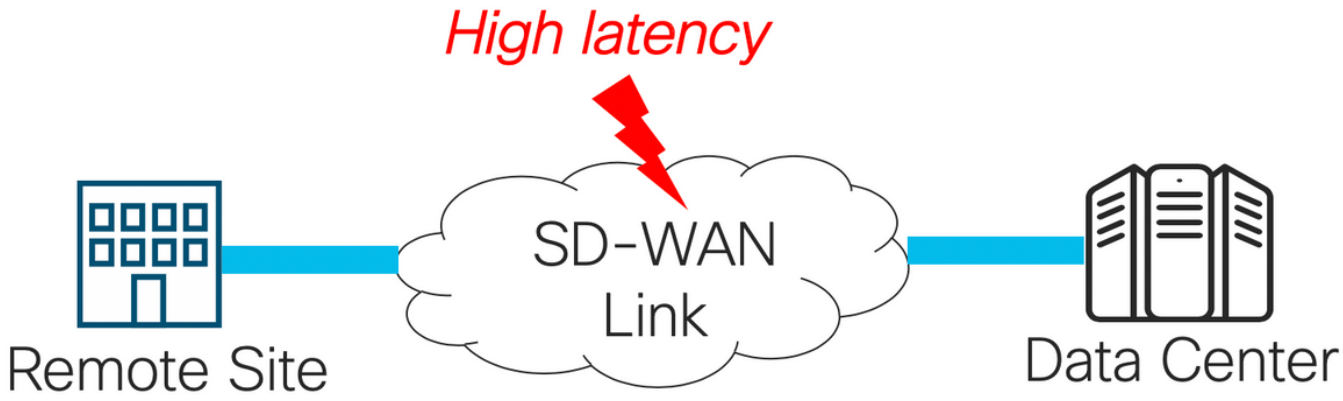
Componentes Utilizados

As informações neste documento são baseadas no Cisco IOS® XE SD-WAN.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

A alta latência em um link de WAN entre dois lados de SD-WAN causa mau desempenho do aplicativo. Você tem tráfego TCP crítico, que deve ser otimizado.



Solução

Ao usar o recurso Otimização de TCP, você melhora a taxa de transferência média de TCP para fluxos TCP críticos entre dois sites SD-WAN.

Observe a visão geral e as diferenças entre a otimização de TCP em cEdge Bottleneck Bandwidth and Round-trip (BBR) e vEdge (CUBIC)

O algoritmo de tempo de propagação BBR rápido é usado na implementação XE SD-WAN (no cEdge).

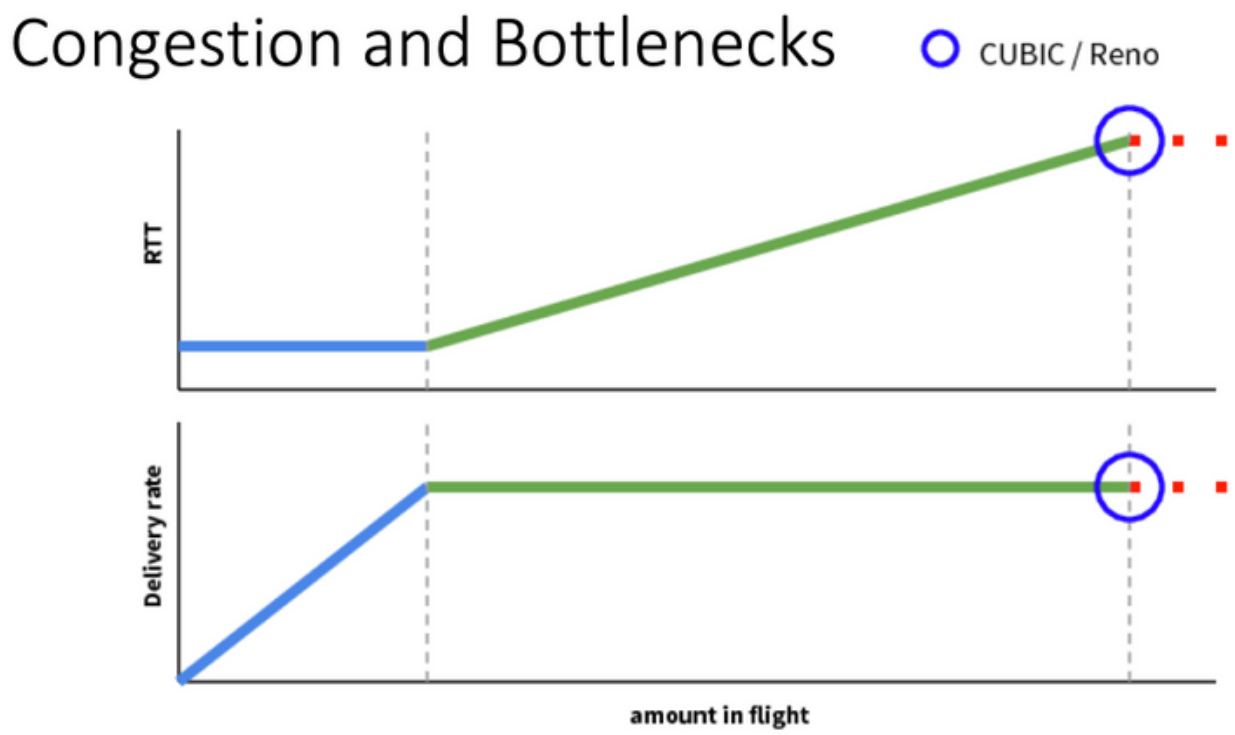
O Viptela OS (vEdge) tem um algoritmo diferente e mais antigo, chamado CUBIC.

O CUBIC leva em consideração principalmente a perda de pacotes e é amplamente implementado em diferentes sistemas operacionais clientes. Windows, Linux, MacOS, Android já têm CUBIC integrado. Em alguns casos, quando você tem clientes antigos executando a pilha TCP sem CUBIC, a ativação da otimização TCP no vEdge traz melhorias. Um dos exemplos, em que a otimização CUBIC de TCP do vEdge se beneficiou, está em submarinos que usam hosts clientes antigos e links de WAN que sofrem atrasos/quedas significativas. Observe que somente o vEdge 1000 e o vEdge 2000 suportam TCP CUBIC.

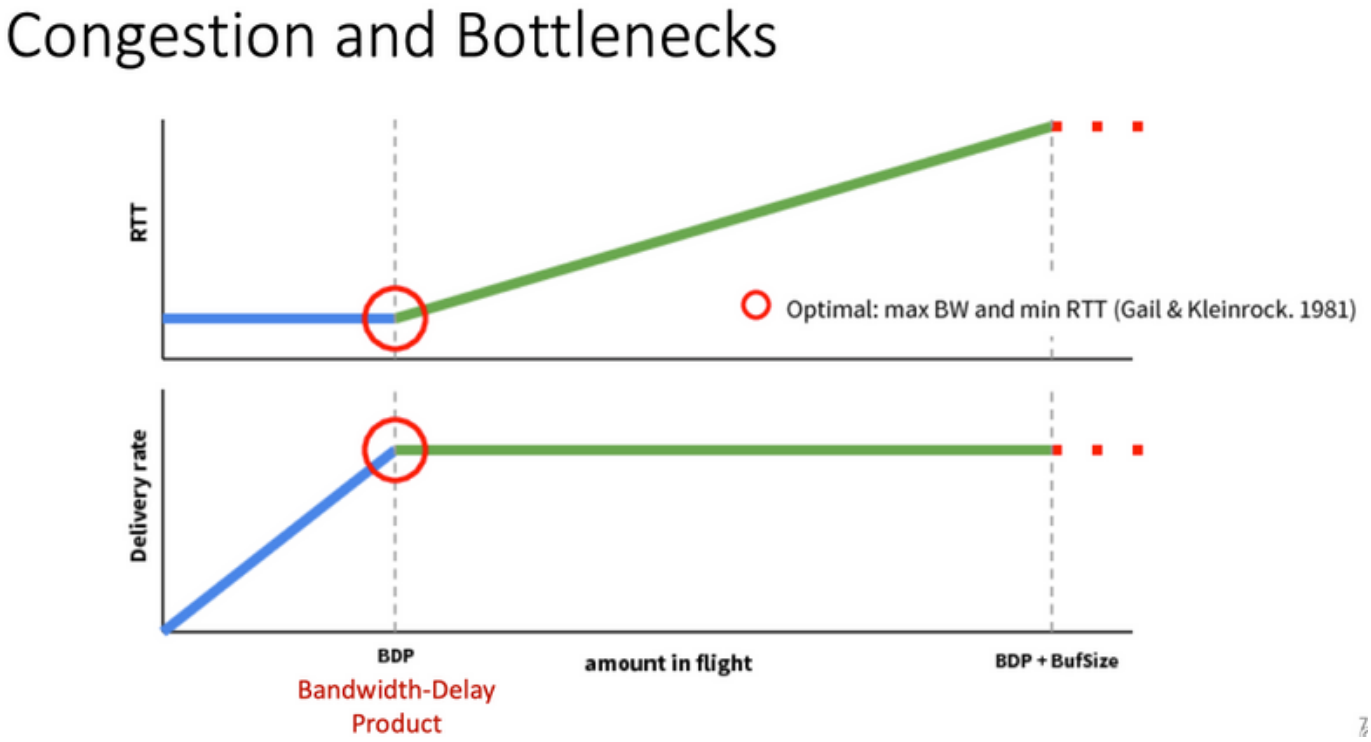
O BBR se concentra principalmente no tempo de ida e volta e na latência. Não em perda de pacotes. Se você enviar pacotes do oeste dos EUA para a costa leste ou até mesmo para a Europa através da internet pública, na maioria dos casos você não vê nenhuma perda de pacotes. Às vezes, a Internet pública é boa demais em termos de perda de pacotes. Mas o que você vê é atraso/latência. E esse problema é abordado pela BBR, que foi desenvolvida pela Google em 2016.

Em poucas palavras, a BBR modela a rede e observa cada confirmação (ACK) e atualiza a largura de banda máxima (BW) e o tempo mínimo de ida e volta (RTT). Em seguida, o envio de controle é baseado no modelo: sonda para largura de banda máxima e RTT mínimo, ritmo próximo à estimativa de largura de banda e mantenha a operação perto do produto de atraso de largura de banda (BDP). O objetivo principal é garantir alto throughput com uma fila de gargalo pequena.

Este slide de Mark Claypool mostra a área onde o CUBIC opera:



A BBR opera em um lugar melhor, que é mostrado neste slide também de Mark Claypool:



Se você quiser ler mais sobre o algoritmo BBR, você pode encontrar várias publicações sobre BBR vinculadas na parte superior da página inicial da lista de discussão bbr-dev Aqui.

Em resumo:

Plataforma e algoritmo	Parâmetro de entrada de chave	Caso de uso
Borda (XE SD-WAN): BBR	RTT/Latência	Tráfego TCP crítico entre dois site WAN
vEdge (Viptela OS): CUBICP	Perda de pacote	Clientes antigos sem otimização T

Plataformas XE SD-WAN suportadas

No XE SD-WAN SW versão 16.12.1d, essas plataformas cEdge suportam TCP Otimization BBR:

- ISR4331
- ISR4351
- CSR1000v com 8 vCPU e mín. 8 GB de RAM

Caveats

- Atualmente, não há suporte para todas as plataformas com menos de 8 GB de RAM.
- Atualmente, não há suporte para todas as plataformas com 4 ou menos núcleos de dados.
- A otimização de TCP não suporta MTU 2000.
- No momento, não há suporte para tráfego IPv6.
- Não há suporte para a otimização do tráfego DIA para um servidor BBR de terceiros. Você precisa ter roteadores cEdge SD-WAN em ambos os lados.
- No cenário do data center, somente um nó de serviço (SN) é suportado por um nó de controle (CN).
- Atualmente, não há suporte para um caso de uso combinado com segurança (contêiner UTD) e otimização TCP no mesmo dispositivo.

> **Note**: O ASR1k não suporta atualmente a otimização TCP. No entanto, há uma solução para o ASR1k, onde o ASR1k envia tráfego TCP através do túnel AppNav (GRE encapsulado) para um CSR1kv externo para otimização. Atualmente (fevereiro de 2020), apenas um CSR1k como nó de serviço externo é suportado. Isso é descrito mais adiante na seção de configuração.

Esta tabela resume advertências por versão e sublinha plataformas de hardware suportadas:

Cenários	Casos de uso	16.12.1	17.2.1	17.3.1	17.4.1	Comentários
Filial para Internet	DIA	No	Yes	**Yes**	**Yes**	Em 16.12.1, o AppC FIA não está habilita na interface de Inter
	SAAS	No	Yes	**Yes**	**Yes**	Em 16.12.1, o AppC FIA não está habilita na interface de Inter
Filial para DC	Roteador de borda única	No	No	**TEF**	**Yes**	Necessidade de ofe suporte a vários SN
	Vários roteadores de borda	No	No	**TEF**	**Yes**	Precisa de simetria fluxo ou sincronizaç fluxo Appnav. 16.12 não ensaiado com
	Vários SNs	No	No	**TEF**	**Yes**	Aprimoramento do vManage para aceit vários IPs SN
De filial para filial	Rede de malha completa (spoke-to-spoke)	**Yes**	**Yes**	**Yes**	**Yes**	
	Hub-and-Spoke (Spoke-Hub-Spoke)	**No**	**Yes**	**Yes**	**Yes**	

Suporte a BBR	TCP Opt com BBR	**Parcial**	**Parcial**	**Completo**	**Completo**
Plataformas	Plataformas com suporte	**Somente 4300 e CSR**	**Todos, exceto ISR1100**	**Todos**	**Todos**

Configurar

Um conceito de SN e CN é usado para otimização de TCP:

- SN é um daemon, que é responsável pela otimização real dos fluxos TCP.
- O CN é conhecido como AppNav Controller e é responsável pela seleção de tráfego e pelo transporte de/para o SN.

SN e CN podem ser executados no mesmo roteador ou separados como nós diferentes.

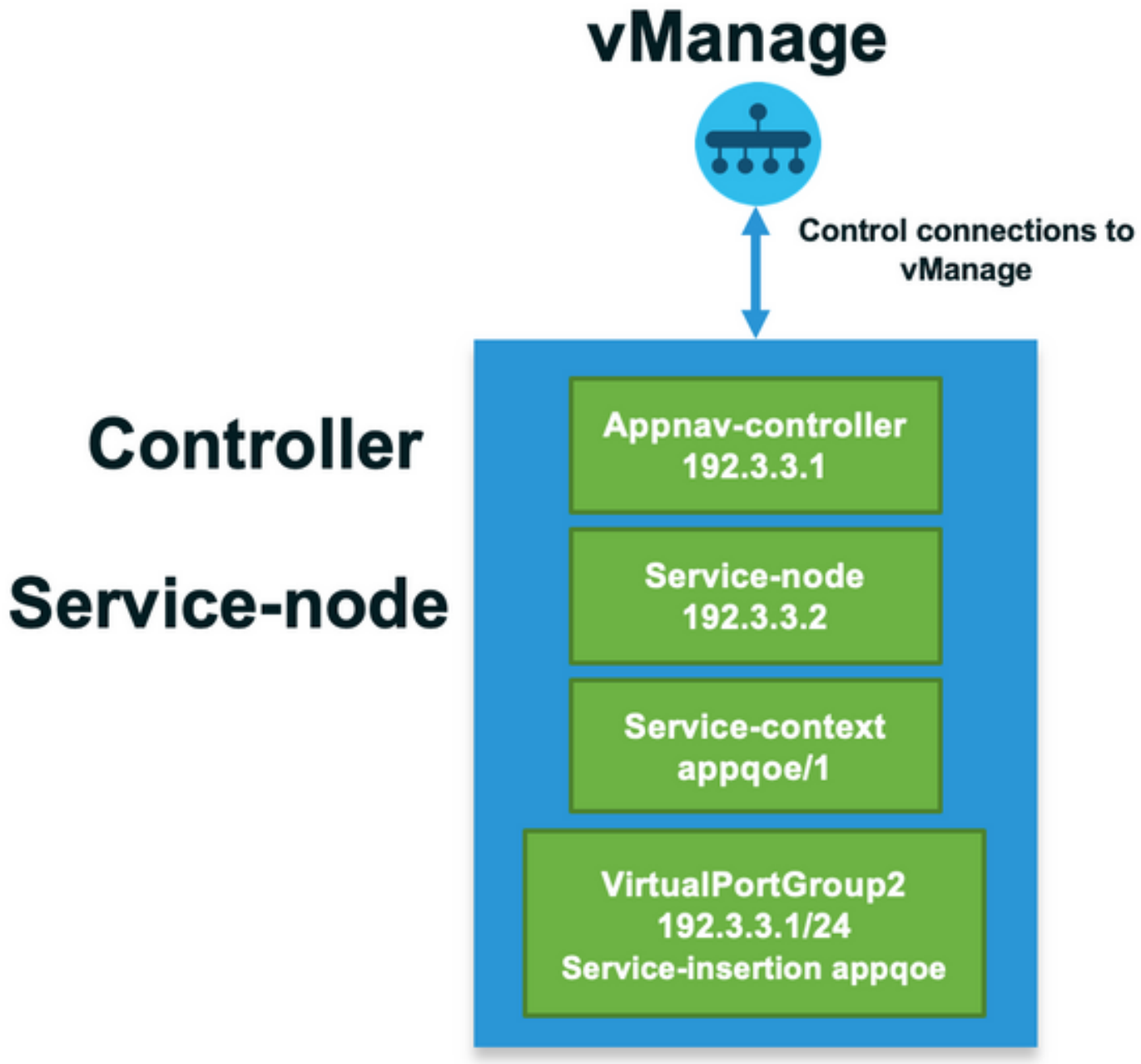
Há dois casos de uso principais:

1. Caso de uso de filial com SN e CN sendo executados no mesmo roteador ISR4k.
2. Caso de uso do data center, em que o CN é executado no ASR1k e o SN é executado em um roteador virtual CSR1000v separado.

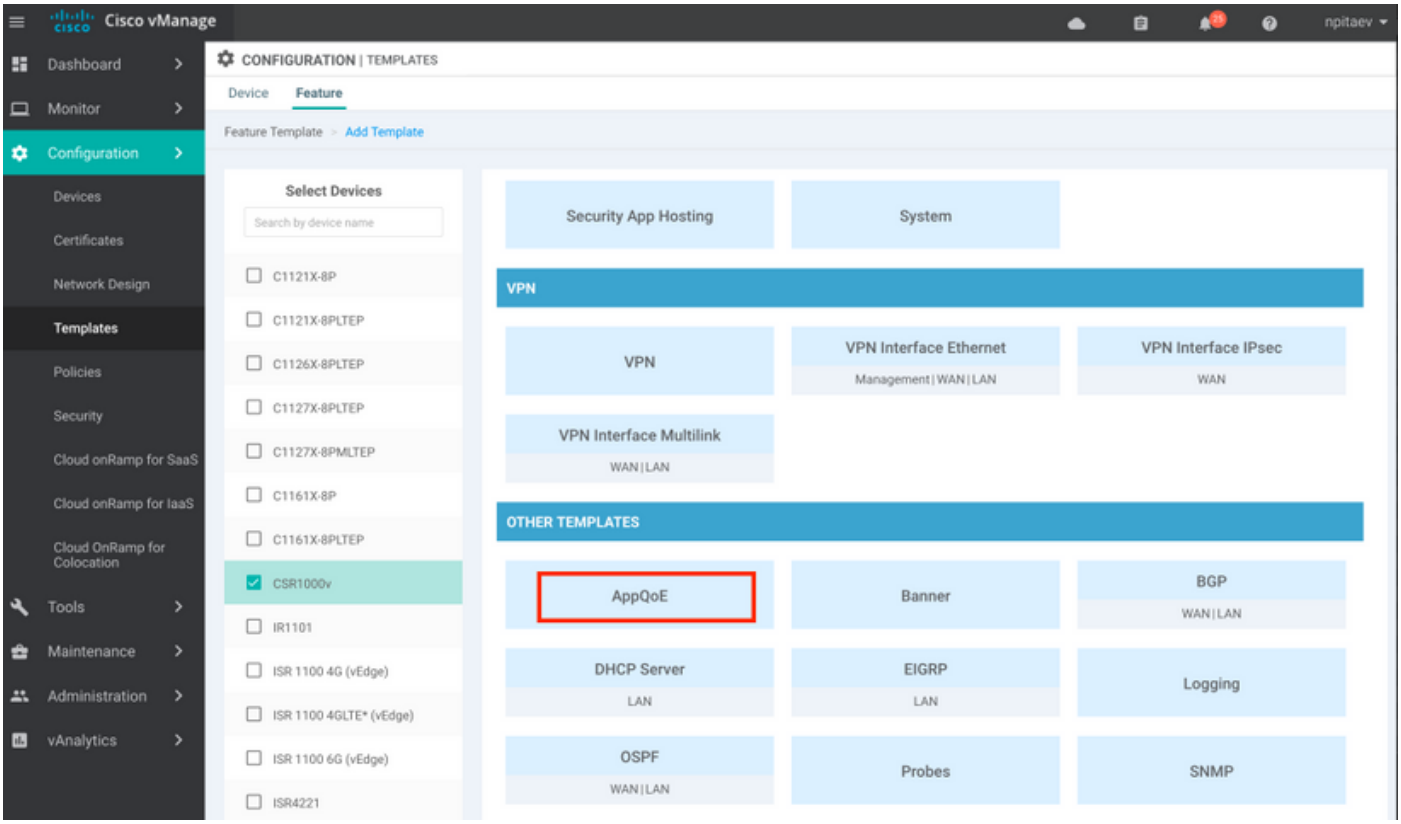
Os dois casos de uso são descritos nesta seção.

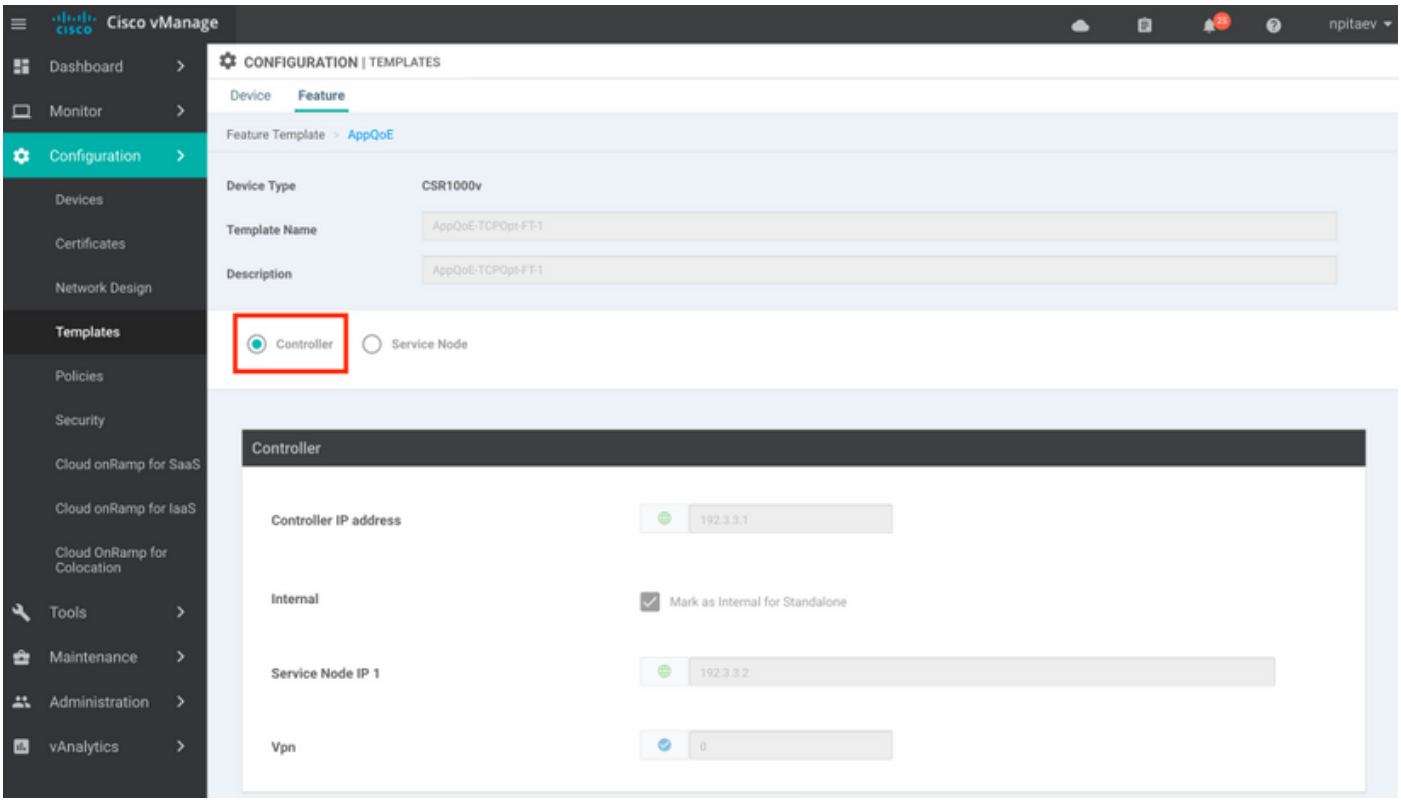
Caso de uso 1. Configurar a otimização TCP em uma filial (tudo em um cEdge)

Esta imagem mostra a arquitetura interna geral para uma única opção independente em uma filial:

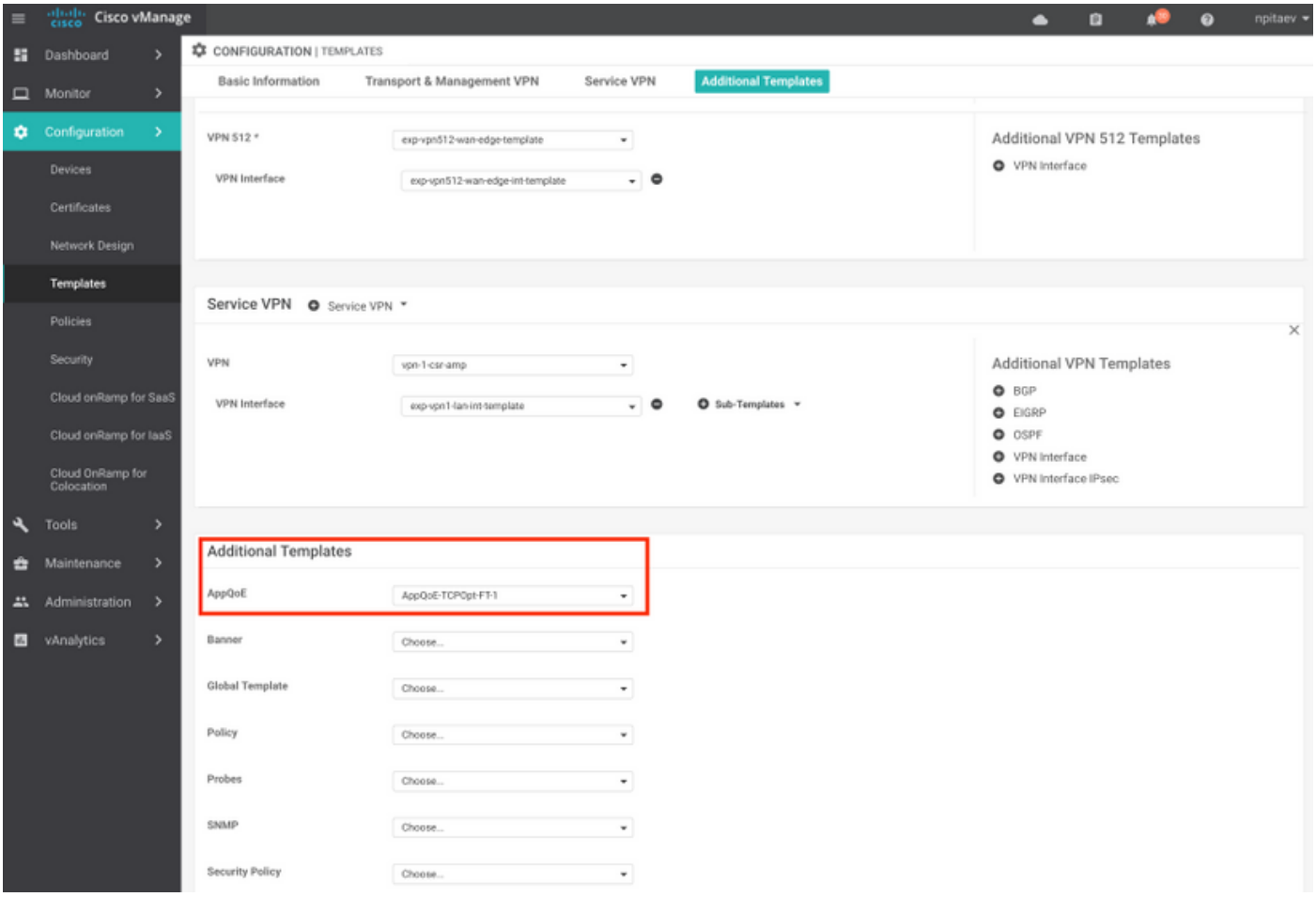


Etapa 1. Para configurar a otimização TCP, você precisa criar um modelo de recurso para a otimização TCP no vManage. Navegue até **Configuration > Templates > Feature Templates > Other Templates > AppQoE** como mostrado na imagem.





Etapa 2. Adicione o modelo de recurso AppQoE ao modelo de dispositivo apropriado em **Modelos Adicionais**:

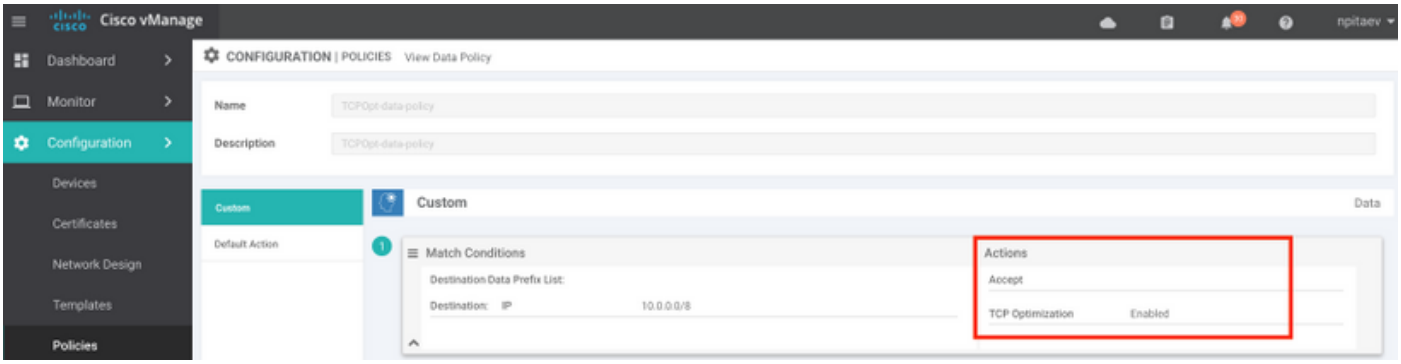


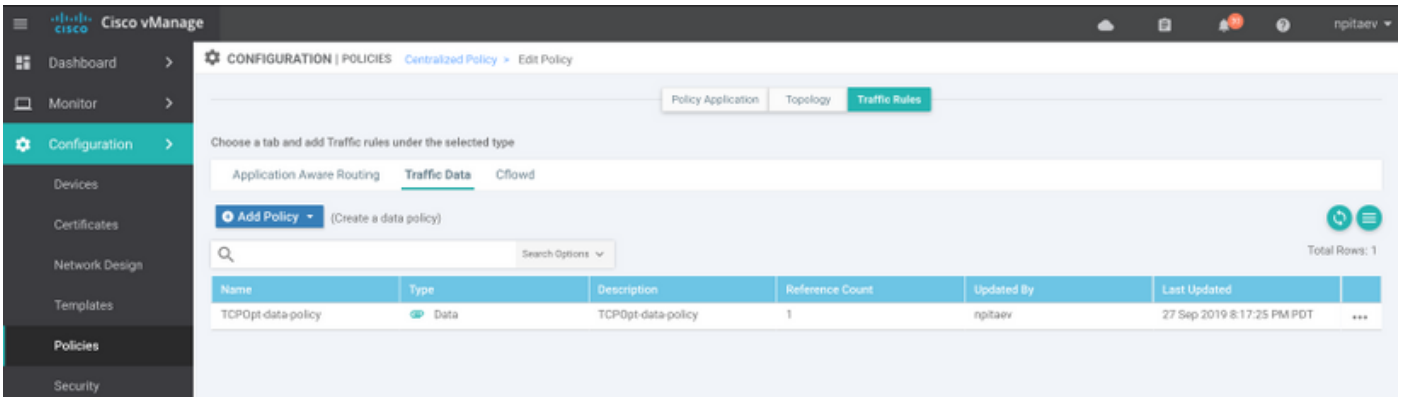
Esta é a visualização CLI da configuração do modelo:

```
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
!
```

Etapa 3. Criar uma política de dados centralizada com a definição do tráfego TCP interessante para otimização.

Como um exemplo; essa política de dados corresponde ao prefixo IP 10.0.0.0/8, que inclui endereços de origem e destino e permite a otimização TCP para ele:





Esta é a visualização CLI da Política vSmart:

```
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
 !
!
```

Caso de uso 2. Configurar a otimização TCP no data center com um SN externo

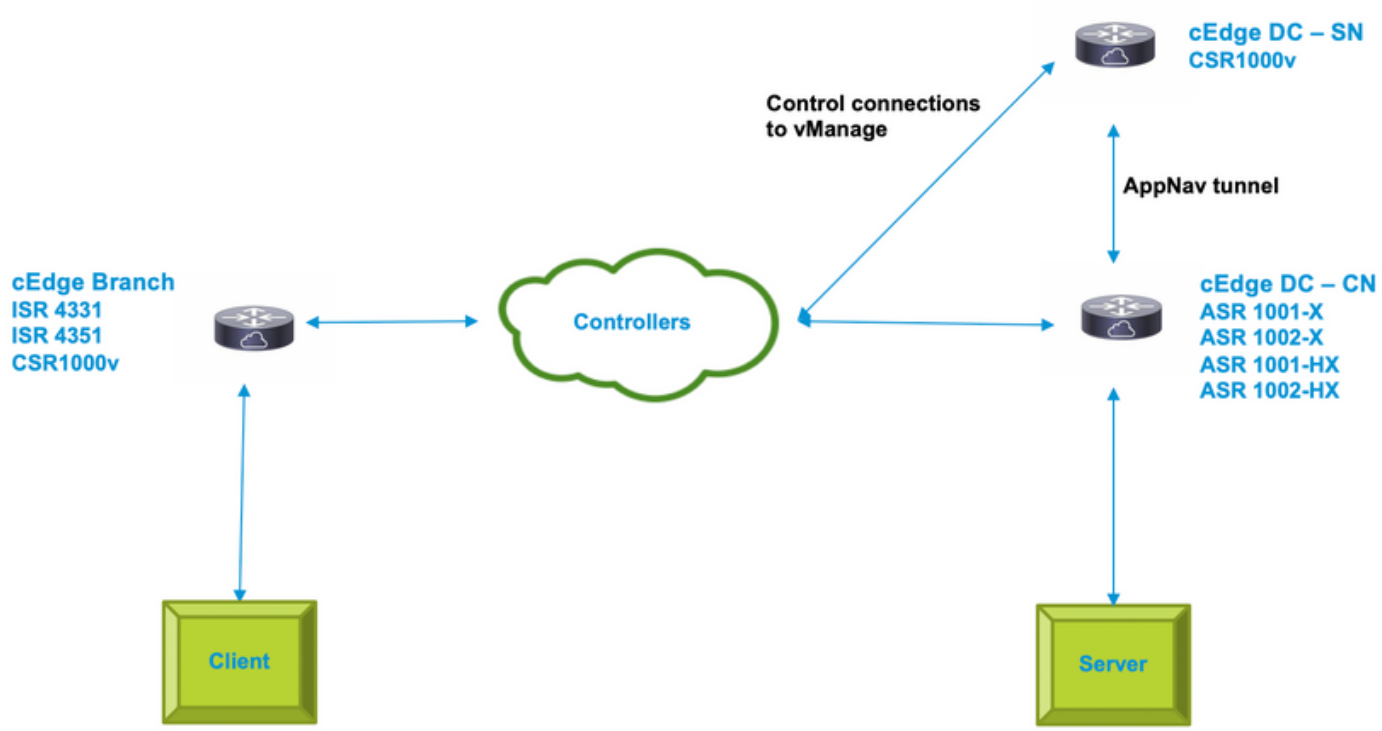
A principal diferença para o caso de uso de filial é a separação física de SN e CN. No caso de uso de filial all-in-one, a conectividade é feita dentro do mesmo roteador usando a Virtual Port Group

Interface. No caso de uso do data center, há um túnel encapsulado de GRE do AppNav entre o ASR1k atuando como CN e o CSR1k externo sendo executado como SN. Não há necessidade de um link dedicado ou conexão cruzada entre CN e SN externo, o alcance IP simples é suficiente.

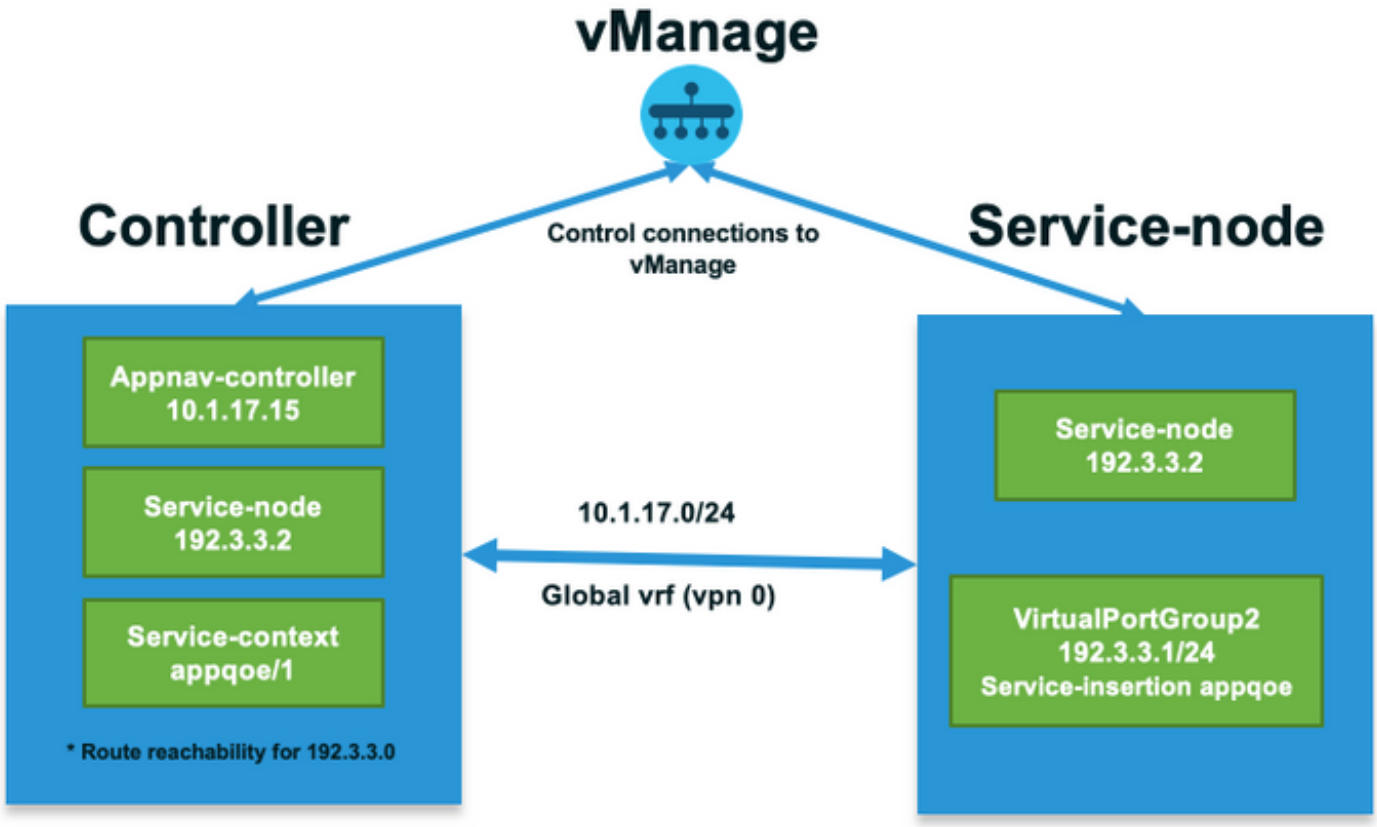
Há um túnel AppNav (GRE) por SN. Para uso futuro, onde vários SNs são suportados, recomenda-se usar a sub-rede /28 para a rede entre CN e SN.

Duas NICs são recomendadas em um CSR1k atuando como SN. A segunda NIC para o controlador SD-WAN é necessária se o SN tiver que ser configurado/gerenciado pelo vManage. Se o SN for configurado/gerenciado manualmente, a 2ª NIC será opcional.

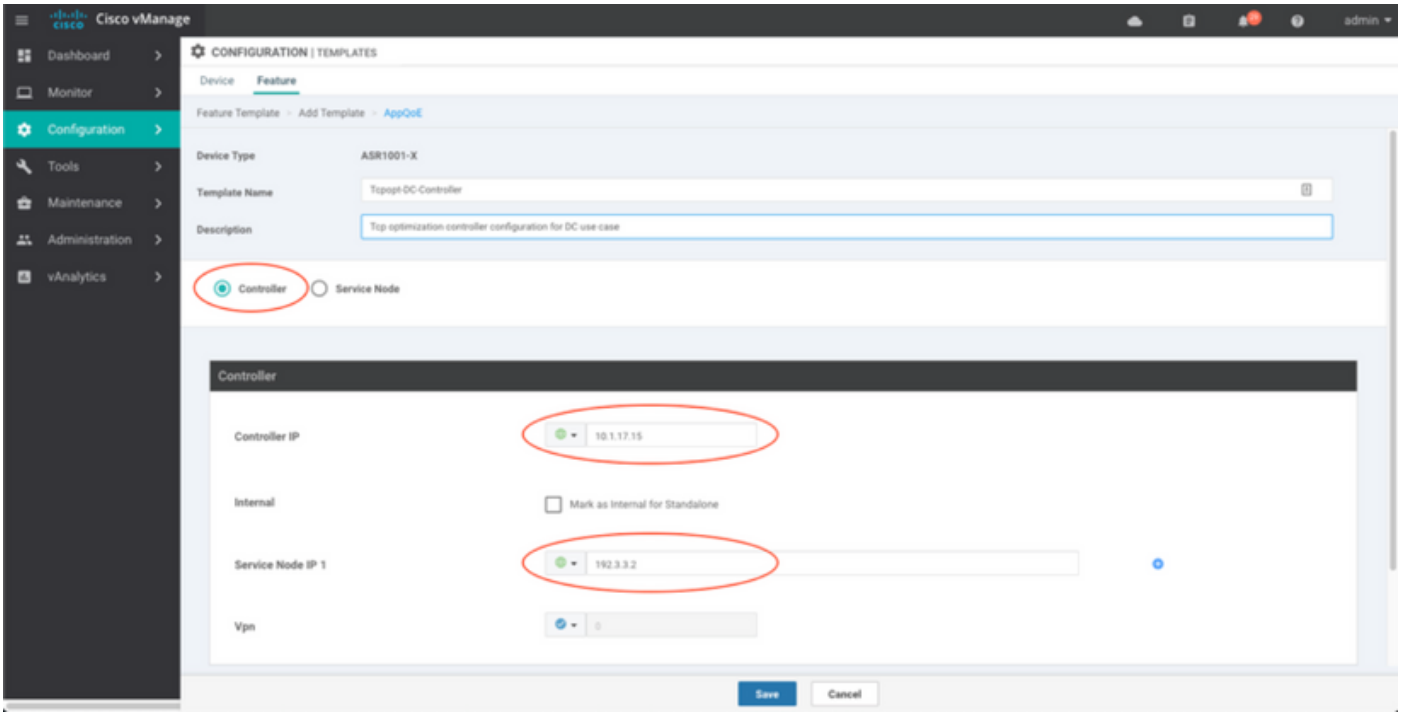
Esta imagem mostra o Data Center ASR1k sendo executado como CN e CSR1kv como Nó de Serviço SN :



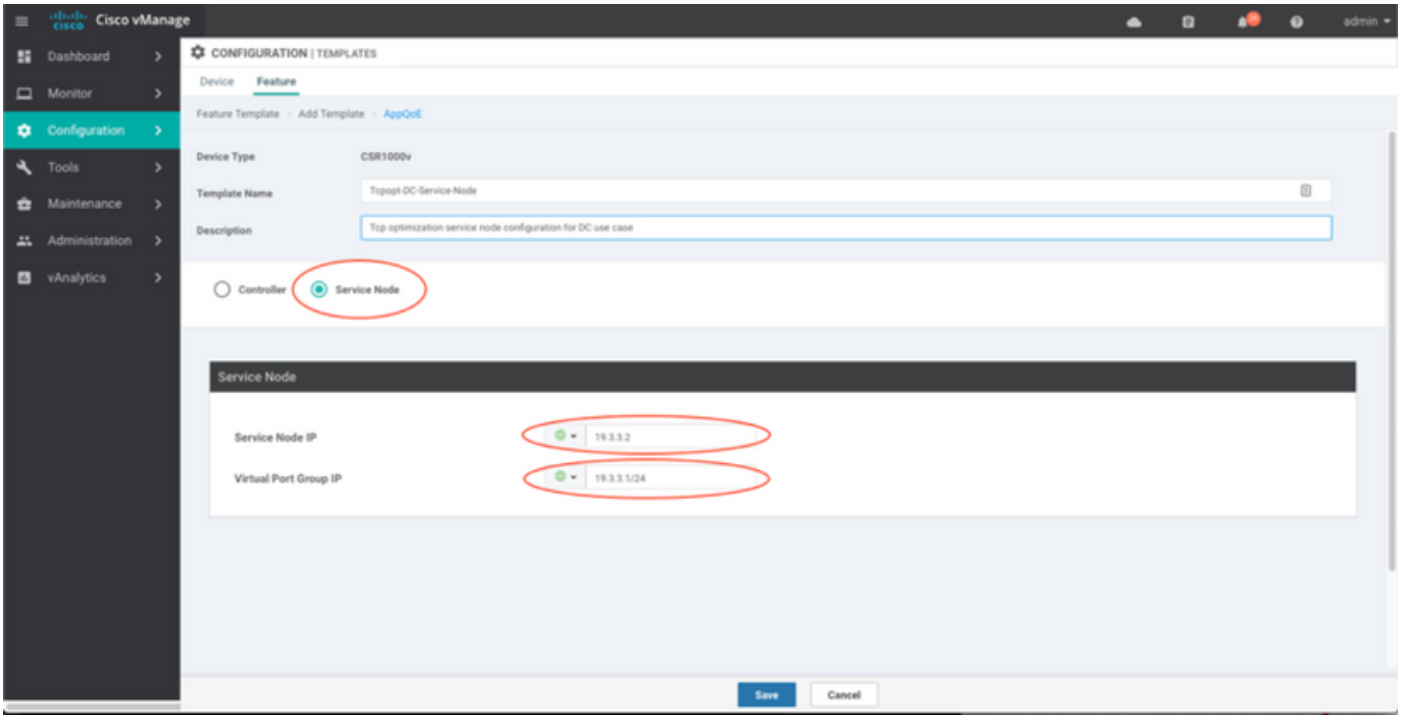
A topologia do caso de uso do data center com ASR1k e CSR1k externo é mostrada aqui:



Este modelo de recurso AppQoE mostra o ASR1k configurado como Controlador:



CSR1k configurado como nó de serviço externo é mostrado aqui:



Caso de failover

Failover no caso de uso do data center com CSR1k agindo como SN, em caso de falha CSR1k externa:

- As sessões TCP que já existem são perdidas porque a sessão TCP no SN é encerrada.
- Novas sessões TCP são enviadas ao destino final, mas o tráfego TCP não é otimizado (desvio).
- Sem blackholing para tráfego interessante em caso de falha de SN.

A detecção de failover é baseada na pulsação do AppNav, que é de 1 pulsação por segundo. Após 3 ou 4 erros, o túnel é declarado inativo.

O failover no caso de uso da filial é semelhante - em caso de falha de SN, o tráfego é enviado diretamente ao destino sem ser otimizado.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique a otimização TCP na CLI com o uso deste comando CLI e veja o resumo dos fluxos otimizados:

```
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#
```

Esta saída fornece informações detalhadas sobre fluxos otimizados:

```
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#
```

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Notas de versão do Cisco IOS XE SD-WAN versão 16.12.x
- Cisco SD-WAN versões 19.1, 19.2 - Guia de otimização de configuração de TCP
- Cisco SD-WAN Configurar otimização TCP para vEdge
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.