Configurazione della funzionalità di ottimizzazione TCP sui router Cisco IOS® XE SD-WAN cEdge

Sommario

Introduzione

Questo documento descrive la funzione di ottimizzazione TCP (Transmission Control Protocol) sui router Cisco IOS® XE SD-WAN, introdotta nella versione 16.12 ad agosto 2019. Gli argomenti trattati sono: prerequisiti, descrizione del problema, soluzione, differenze negli algoritmi di ottimizzazione TCP tra Viptela OS (vEdge) e XE SD-WAN (cEdge), configurazione, verifica ed elenco dei documenti correlati.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

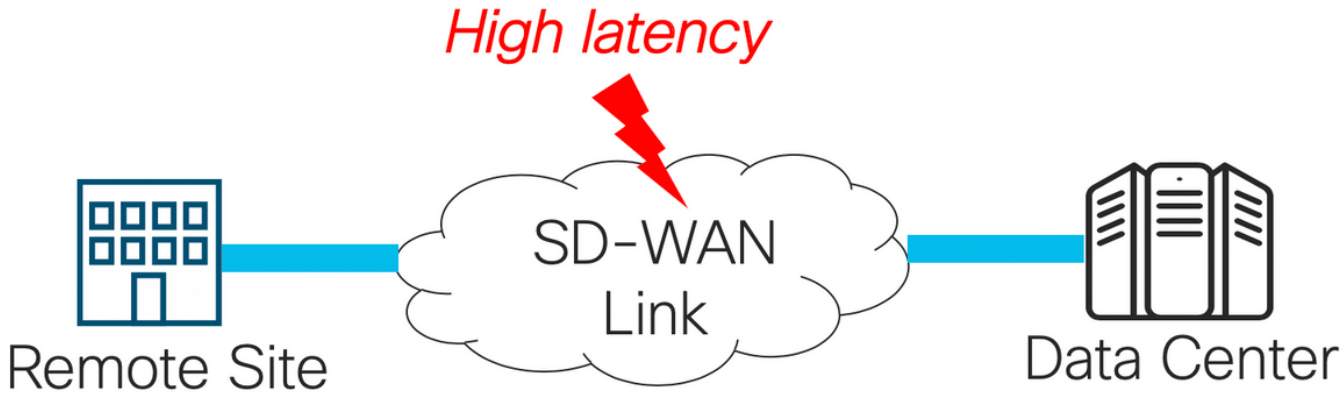
Il riferimento delle informazioni contenute in questo documento è Cisco IOS® XE SD-WAN.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Problema

L'alta latenza su un collegamento WAN tra due lati SD-WAN causa prestazioni errate delle applicazioni. È necessario ottimizzare il traffico TCP critico.



Soluzione

Quando si utilizza la funzione di ottimizzazione TCP, si migliora il throughput TCP medio per i flussi TCP critici tra due siti SD-WAN.

Panoramica e differenze tra l'ottimizzazione TCP su cEdge Bottleneck Bandwidth e Round-trip (BBR) e vEdge (CUBIC)

L'algoritmo per il tempo di propagazione Fast BBR viene utilizzato nell'implementazione XE SD-WAN (su cEdge).

Viptela OS (vEdge) ha un algoritmo diverso, più vecchio, chiamato CUBIC.

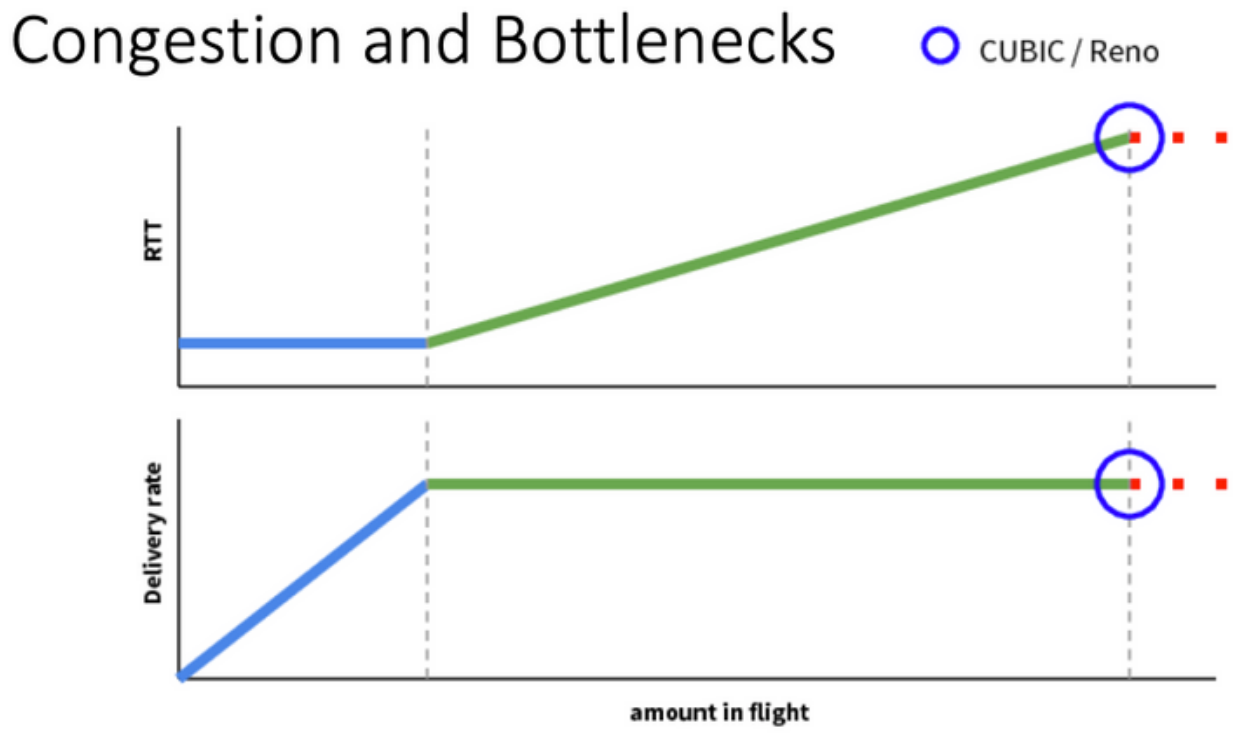
CUBIC prende in considerazione principalmente la perdita di pacchetti ed è ampiamente implementato nei diversi sistemi operativi client. Windows, Linux, MacOS, Android hanno già CUBIC incorporato. In alcuni casi, se sui vecchi client viene eseguito lo stack TCP senza CUBIC, l'abilitazione dell'ottimizzazione TCP su vEdge comporta miglioramenti. Uno degli esempi, in cui l'ottimizzazione TCP CUBIC di vEdge ha tratto vantaggio, è quello dei sottomarini che utilizzano host client e collegamenti WAN obsoleti che subiscono ritardi/perdite significativi. Si noti che solo vEdge 1000 e vEdge 2000 supportano TCP CUBIC.

La BBR è incentrata principalmente sul tempo di andata e ritorno e sulla latenza. Non sulla perdita di pacchetti. Se si inviano pacchetti dagli Stati Uniti occidentali verso la costa orientale o persino verso l'Europa attraverso il web pubblico, nella maggior parte dei casi non si vedono perdite di pacchetti. Internet pubblico a volte è troppo buono in termini di perdita di pacchetti. Ma ciò che vedete è ritardo/latenza. E questo problema è affrontato da BBR, che è stato sviluppato da Google nel 2016.

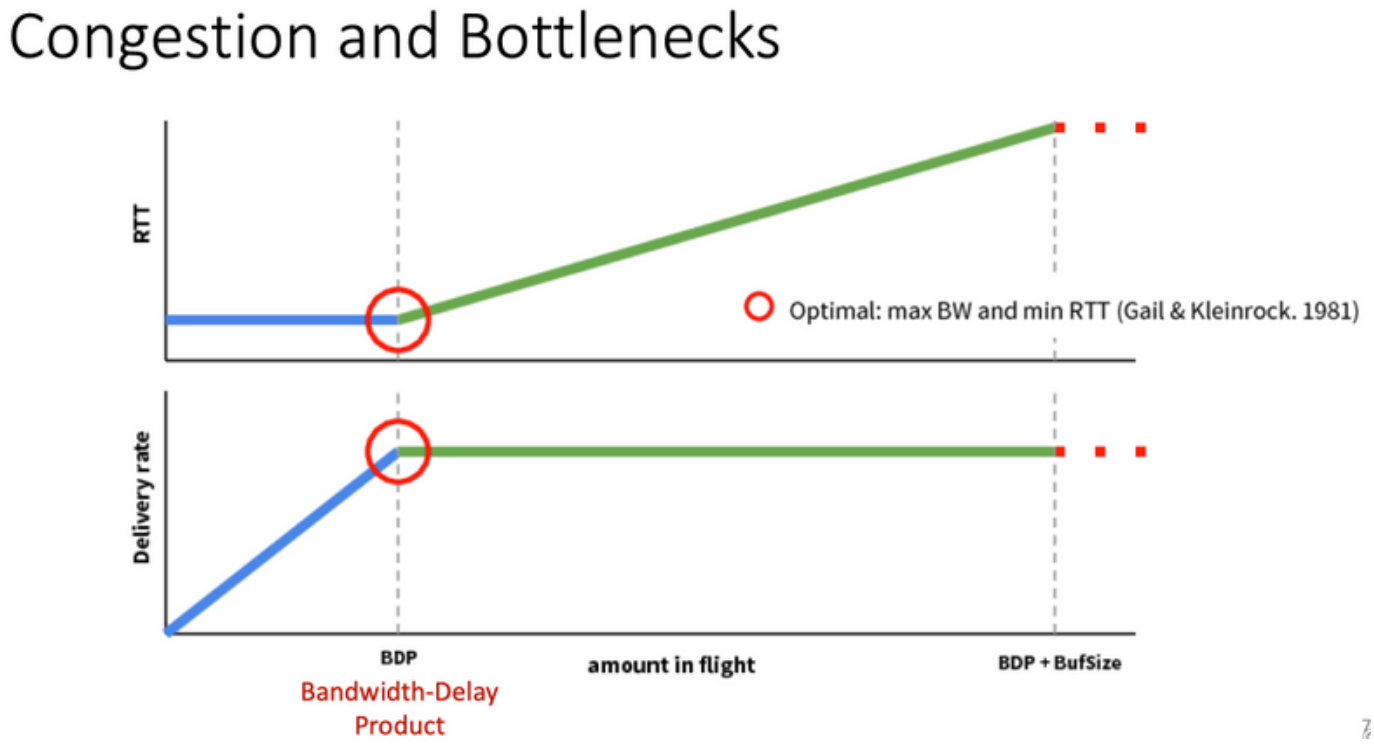
In poche parole, BBR modella la rete e analizza ogni conferma (ACK) e aggiorna la larghezza di banda massima (BW) e il tempo di andata e ritorno minimo (RTT). L'invio del controllo è basato sul modello: sonda per max BW e min RTT, passo vicino a stima BW e mantenere l'inflight vicino Bandwidth-Delay-Product (BDP). L'obiettivo principale è quello di garantire un throughput elevato

con una coda di colli di bottiglia di piccole dimensioni.

Questa diapositiva di Mark Claypool mostra l'area in cui opera CUBIC:



BBR opera in una posizione migliore, come illustrato in questa diapositiva anche da Mark Claypool:



Per ulteriori informazioni sull'algoritmo BBR, fare clic qui nella parte superiore della home page della mailing list bbr-dev, sono disponibili diverse pubblicazioni su BBR.

In sintesi:

Piattaforma e algoritmo	Parametro di input chiave	Scenario d'uso

cEdge (XE SD-WAN): BBR	RTT/Latenza	Traffico TCP critico tra due siti SD
vEdge (Viptela OS): POSTAZIONE UFFICIO	Perdita di pacchetti	Vecchi client senza ottimizzazione

Piattaforme XE SD-WAN supportate

Nel software XE SD-WAN versione 16.12.1d, queste piattaforme cEdge supportano l'ottimizzazione TCP BBR:

- ISR 4331
- ISR 4351
- CSR1000v con 8 vCPU e minimo 8 GB di RAM

Avvertenze

- Al momento non sono supportate tutte le piattaforme con memoria DRAM inferiore a 8 GB di RAM.
- Al momento non sono supportate tutte le piattaforme con 4 o meno core di dati.
- L'ottimizzazione TCP non supporta MTU 2000.
- Attualmente non è supportato il traffico IPv6.
- Ottimizzazione per il traffico DIA verso un server BBR di terze parti non supportata. È necessario avere un router cEdge SD-WAN su entrambi i lati.
- Nello scenario attuale del centro dati, è supportato un solo nodo di servizio (SN) per ogni nodo di controllo (CN).
- Attualmente non è supportato uno Use Case combinato con protezione (contenitore UTD) e ottimizzazione TCP sullo stesso dispositivo.

> **Nota:** ASR1k non supporta attualmente l'ottimizzazione TCP. Tuttavia, esiste una soluzione per ASR1k, in cui ASR1k invia il traffico TCP tramite il tunnel AppNav (incapsulato da GRE) a un CSR1k esterno per l'ottimizzazione. Attualmente (febbraio 2020) è supportato un solo CSR1k come nodo di servizio esterno. Questa condizione viene descritta più avanti nella sezione di configurazione.

La tabella seguente riepiloga le avvertenze per ogni release e sottolinea le piattaforme hardware supportate:

Scenari	Scenari d'uso	16.12.1	17.2.1	17.3.1	17.4.1	Commenti
Filiale verso Internet	DIA	No	Sì	**Sì**	**Sì**	In 16.12.1 AppQoE non è abilitato sull'interfaccia Interr
	SAAS	No	Sì	**Sì**	**Sì**	In 16.12.1 AppQoE non è abilitato sull'interfaccia Interr
Branch-to-DC	Single Edge Router	No	No	**EFT**	**Sì**	Necessità di suppor più SN
	Router per più edge	No	No	**EFT**	**Sì**	Ènecessaria la simn di flusso o la sincronizzazione di t di Appnav. 16.12.1 r testato con

	Più SN	No	No	**EFT**	**Sì**	Miglioramento di vManage per accett più IP SN
Filiale a filiale	Rete Mesh Completa (Spoke-to-Spoke)	**Sì**	**Sì**	**Sì**	**Sì**	
	Hub-and-Spoke (Spoke-Hub-Spoke)	**No**	**Sì**	**Sì**	**Sì**	
Supporto BBR	TCP Opt con BBR	**Parziale**	**Parziale**	**Full**	**Full**	
Piattaforme	Piattaforme supportate	**Solo 4300 e CSR**	**Tutti tranne ISR1100**	**Tutto**	**Tutto**	

Configurazione

Per l'ottimizzazione TCP vengono utilizzati i concetti di SN e CN:

- SN è un daemon che è responsabile dell'ottimizzazione effettiva dei flussi TCP.
- CN è noto come AppNav Controller ed è responsabile della selezione del traffico e del trasporto da/verso SN.

SN e CN possono essere eseguiti sullo stesso router o separati come nodi diversi.

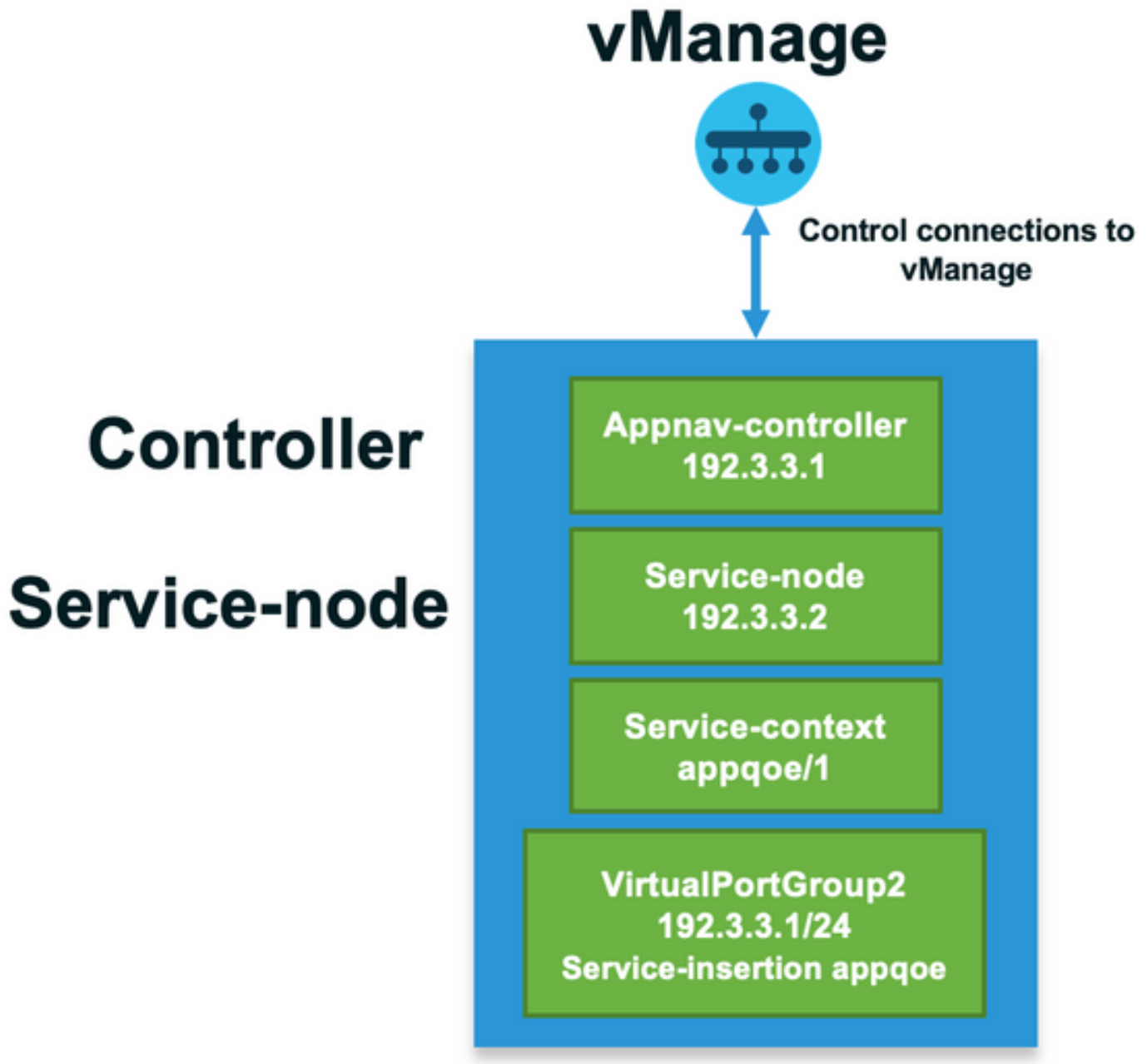
Esistono due casi di utilizzo principali:

1. Caso di utilizzo per filiali con SN e CN in esecuzione sullo stesso router ISR4k.
2. Scenario di utilizzo del data center, in cui CN viene eseguito su ASR1k e SN su un router virtuale CSR1000v separato.

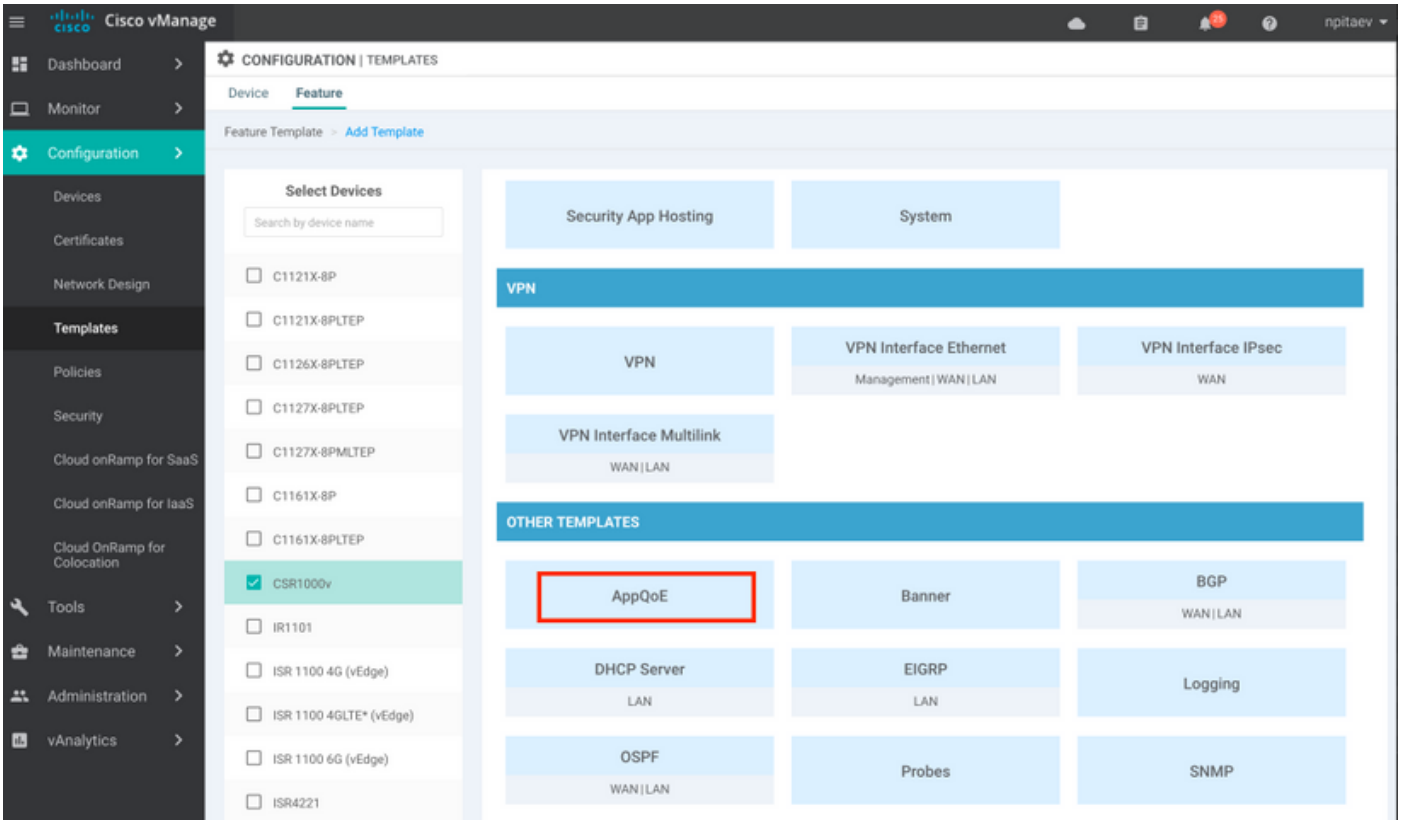
In questa sezione vengono descritti entrambi i casi di utilizzo.

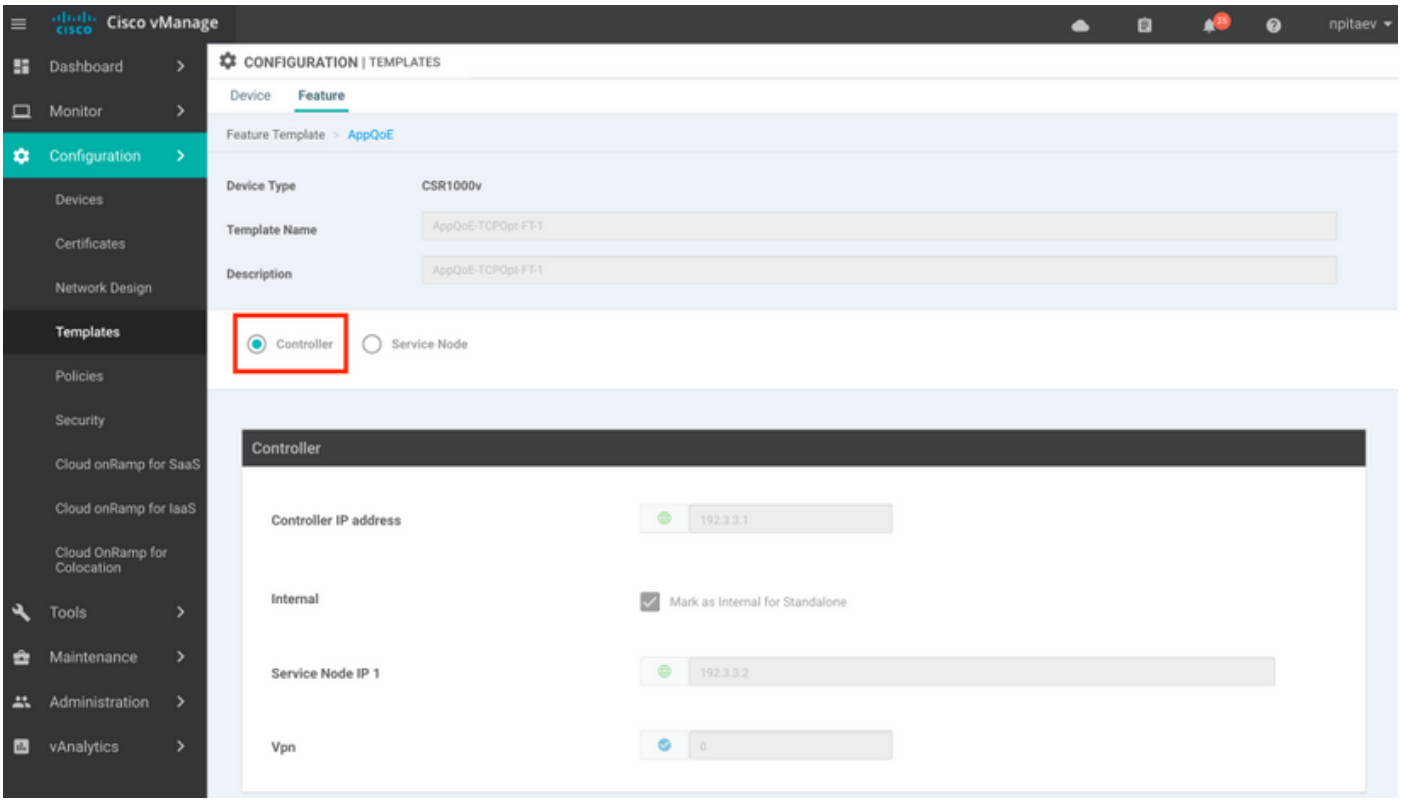
Caso di utilizzo 1. Configurazione dell'ottimizzazione TCP su un branch (tutto in un unico cEdge)

L'immagine mostra l'architettura interna complessiva per una singola opzione standalone in una filiale:

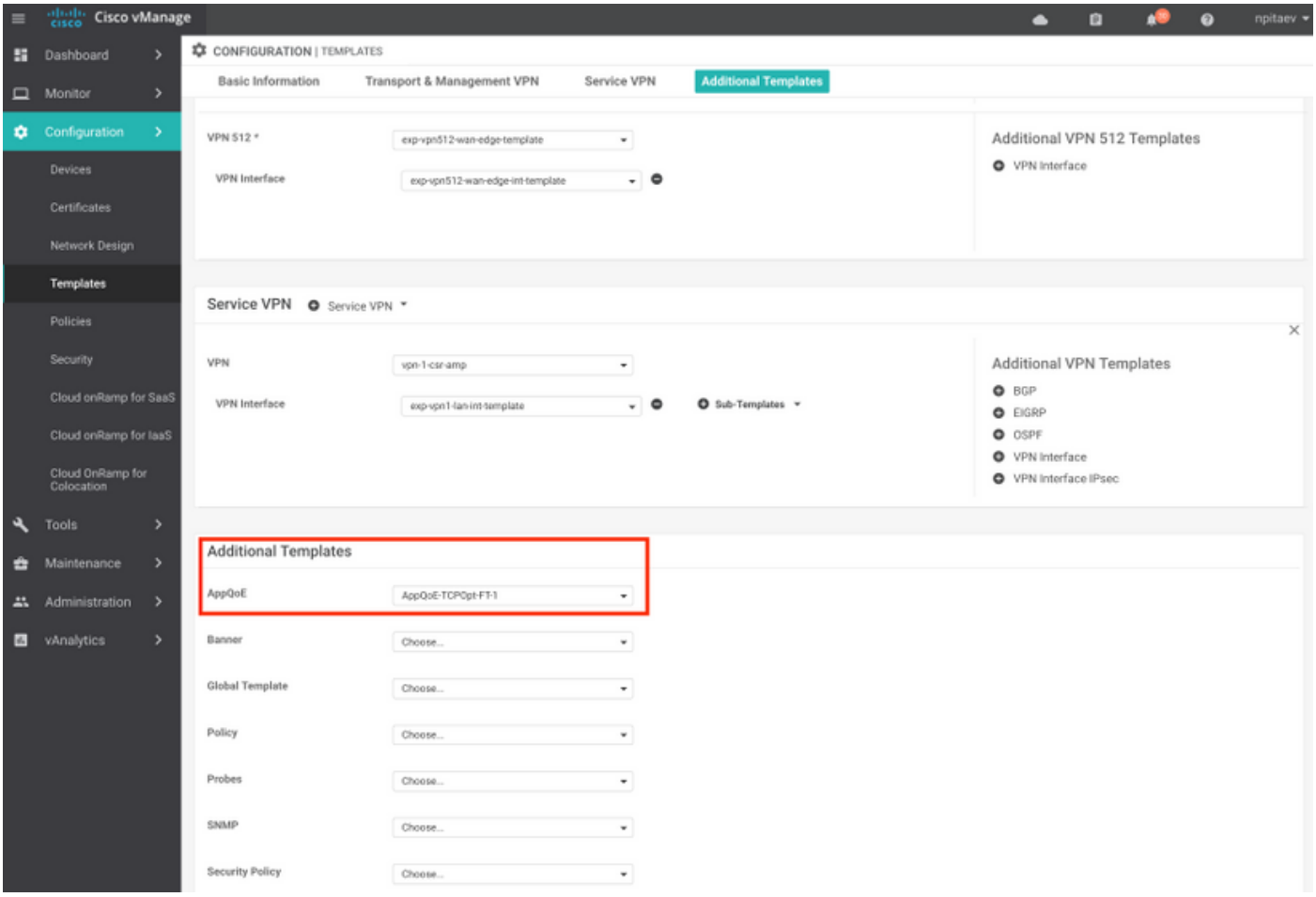


Passaggio 1. Per configurare l'ottimizzazione TCP, è necessario creare un modello di funzionalità per l'ottimizzazione TCP in vManage. Passare a **Configurazione > Modelli > Modelli funzionalità > Altri modelli > AppQoE** come mostrato nell'immagine.





Passaggio 2. Aggiungere il modello della funzionalità AppQoE al modello di dispositivo appropriato in **Modelli aggiuntivi**:

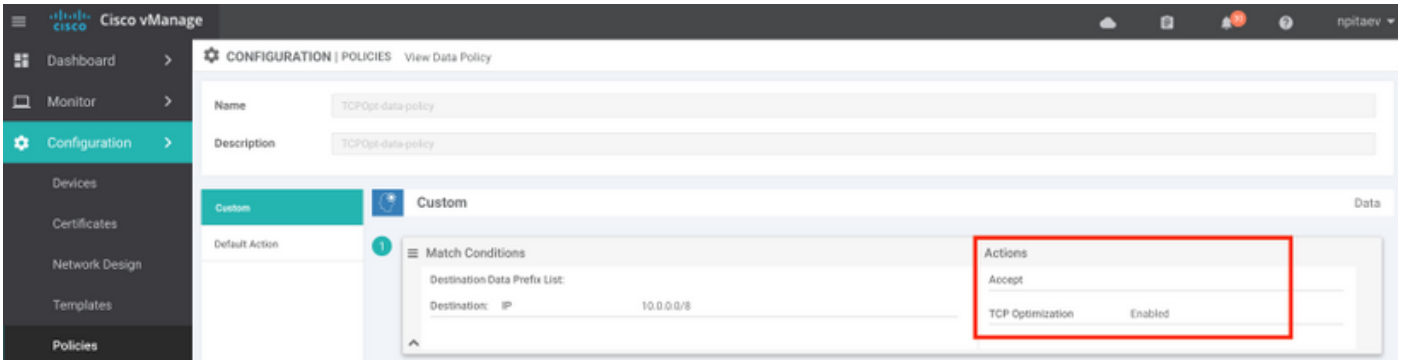


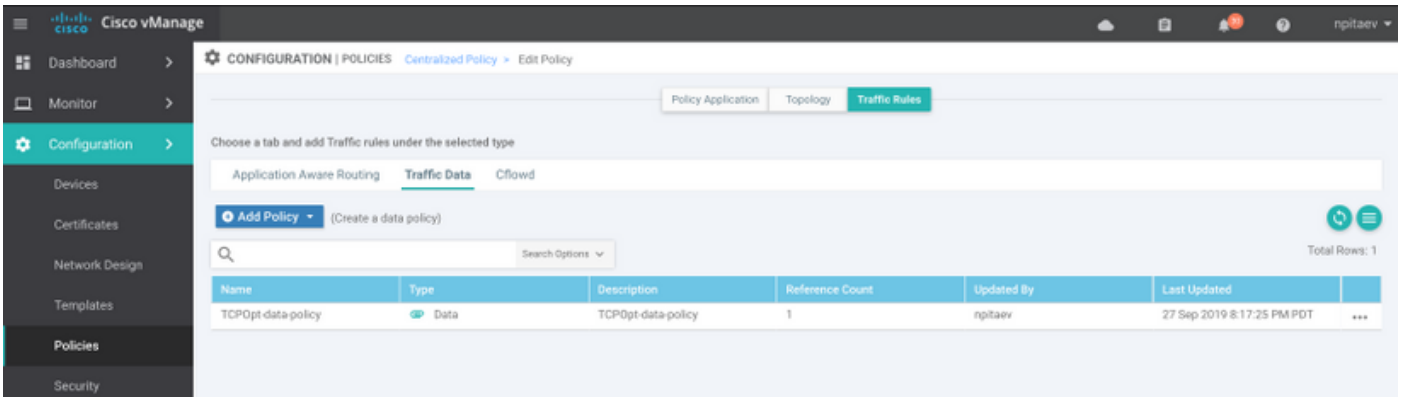
Di seguito è riportata l'anteprima CLI della configurazione del modello:

```
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
!
```

Passaggio 3. Creare una policy dei dati centralizzata con la definizione del traffico TCP interessante per l'ottimizzazione.

Ad esempio: questo criterio dei dati corrisponde al prefisso IP 10.0.0.0/8, che include gli indirizzi di origine e di destinazione, e abilita l'ottimizzazione TCP:





Di seguito è riportata l'anteprima CLI di vSmart Policy:

```
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 di utilizzo 2. Configurazione dell'ottimizzazione TCP nel data center con un numero di serie esterno

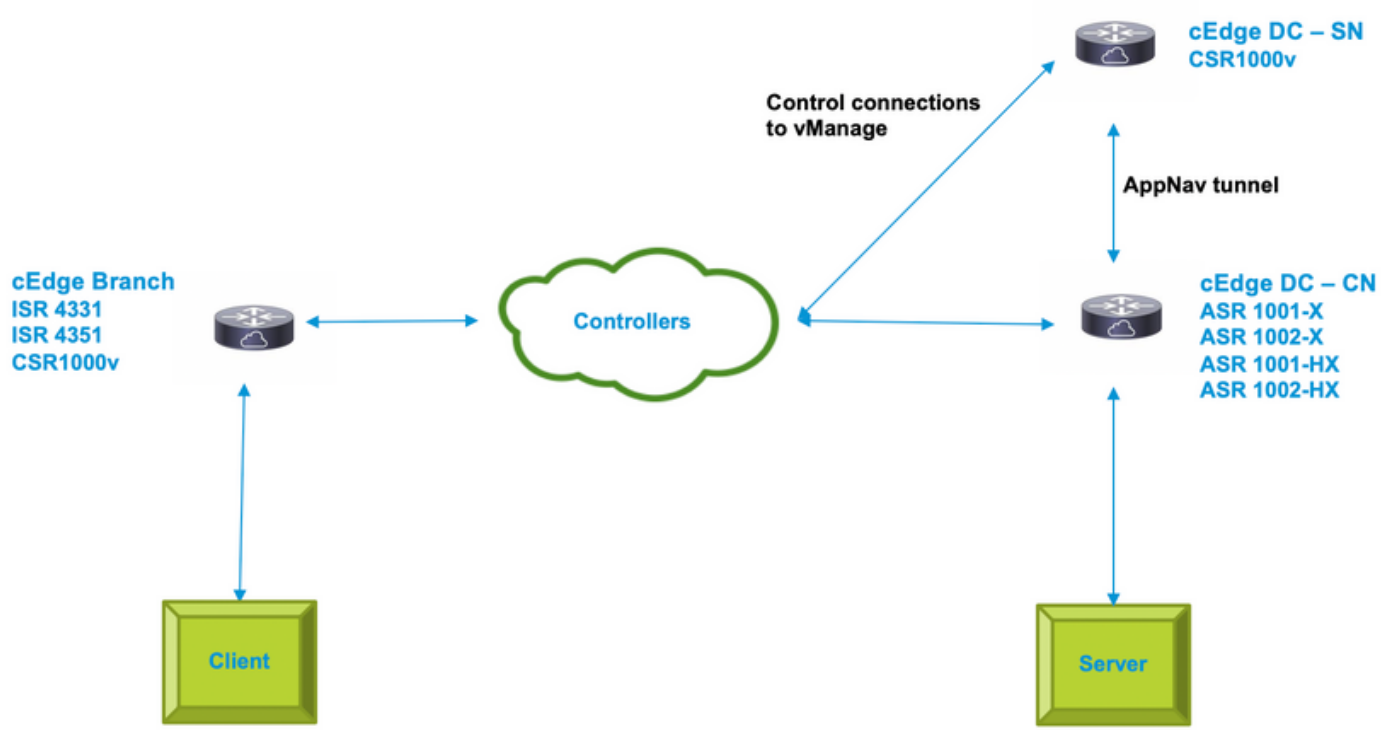
La principale differenza rispetto al caso di utilizzo delle filiali è la separazione fisica tra SN e CN.

Nel caso di utilizzo di un ramo all-in-one, la connettività viene effettuata all'interno dello stesso router utilizzando l'interfaccia Virtual Port Group. Nel caso di utilizzo del centro dati, è presente un tunnel incapsulato GRE di AppNav tra ASR1k che funge da CN e CSR1k esterno che funziona come SN. Non è necessario un collegamento dedicato o una connessione incrociata tra CN e SN esterno, è sufficiente una semplice raggiungibilità IP.

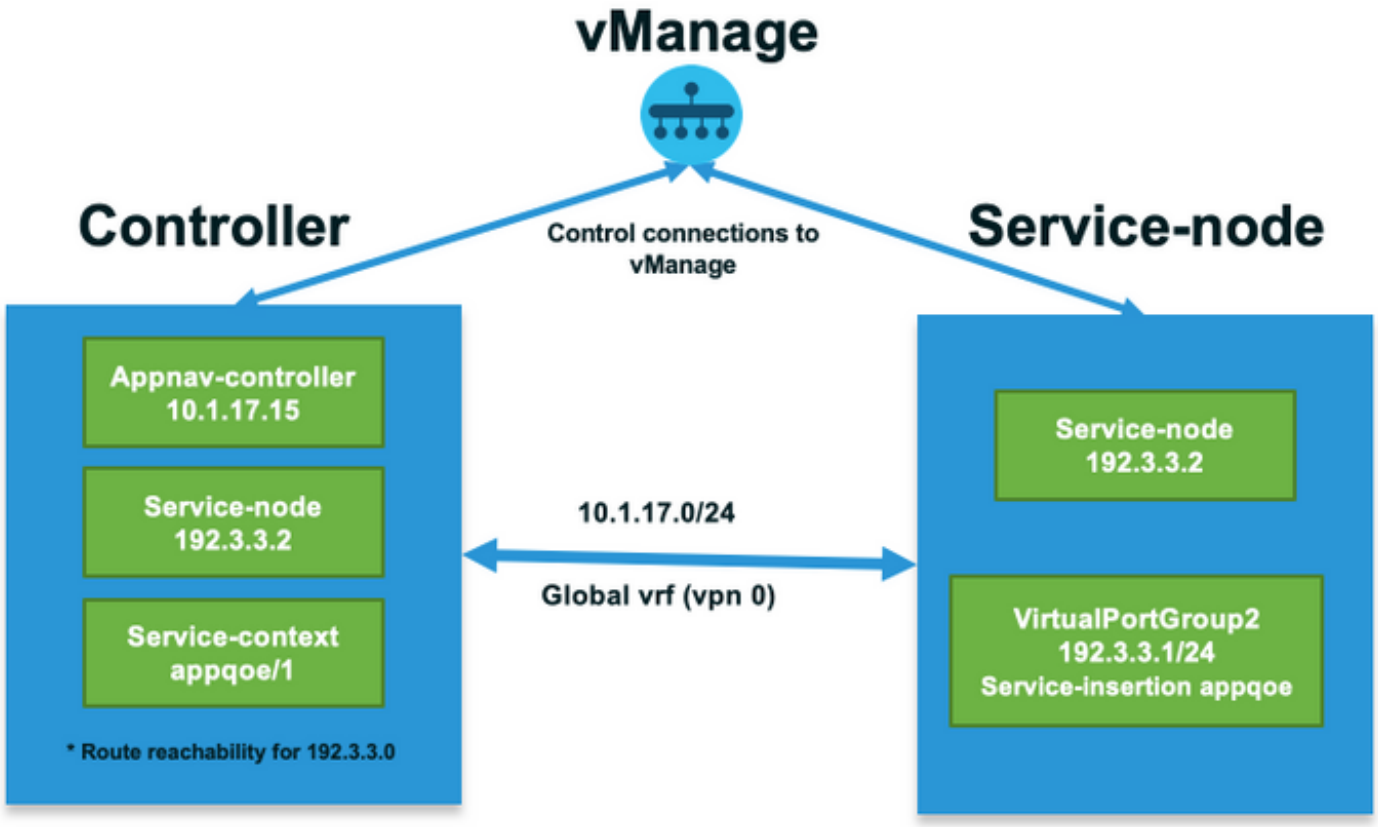
Esiste un tunnel AppNav (GRE) per SN. Per un utilizzo futuro, quando sono supportati più SN, si consiglia di utilizzare la subnet /28 per la rete tra CN ed SN.

Si consigliano due schede NIC su un CSR1k che funge da SN. Se il SN deve essere configurato/gestito da vManage, è necessaria una seconda scheda NIC per il controller SD-WAN. Se il numero di serie deve essere configurato/gestito manualmente, la seconda NIC è opzionale.

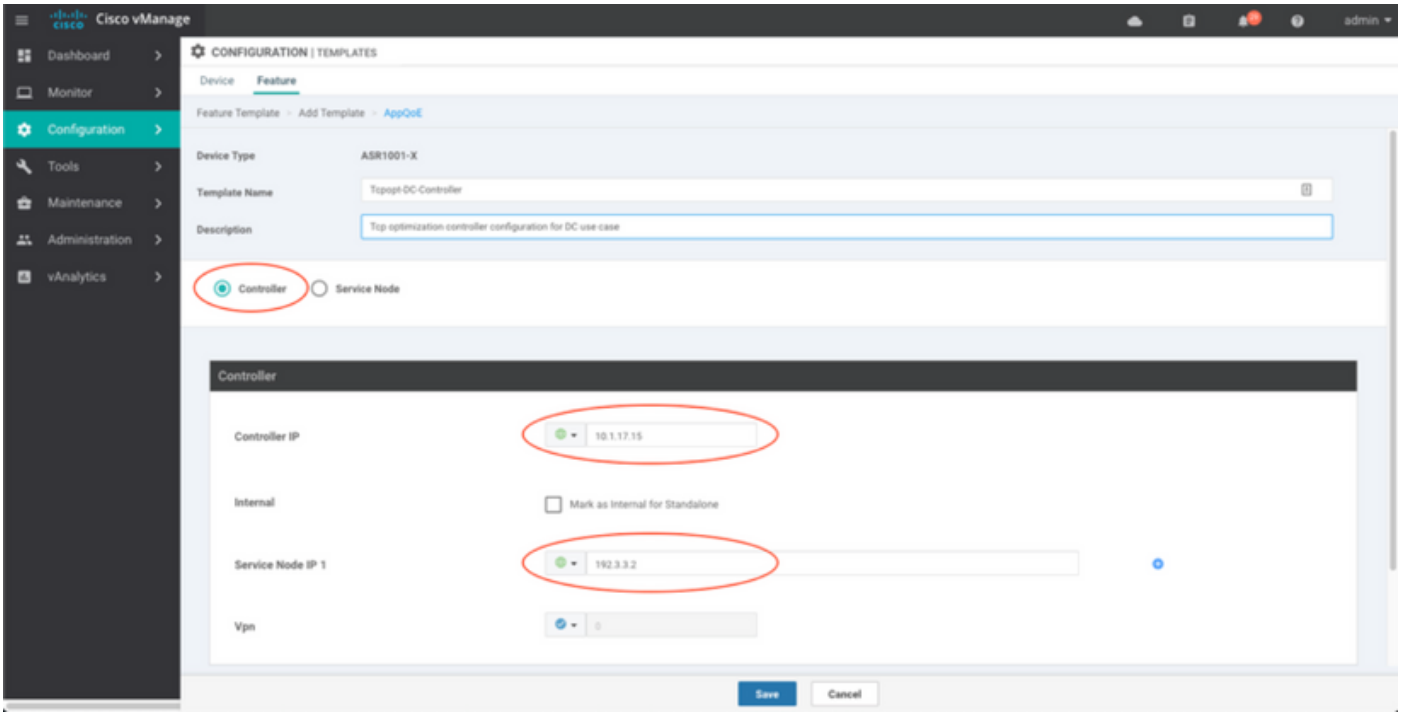
In questa immagine viene mostrato il Data Center ASR1k in esecuzione come CN e CSR1kv come numero di serie del nodo di servizio:



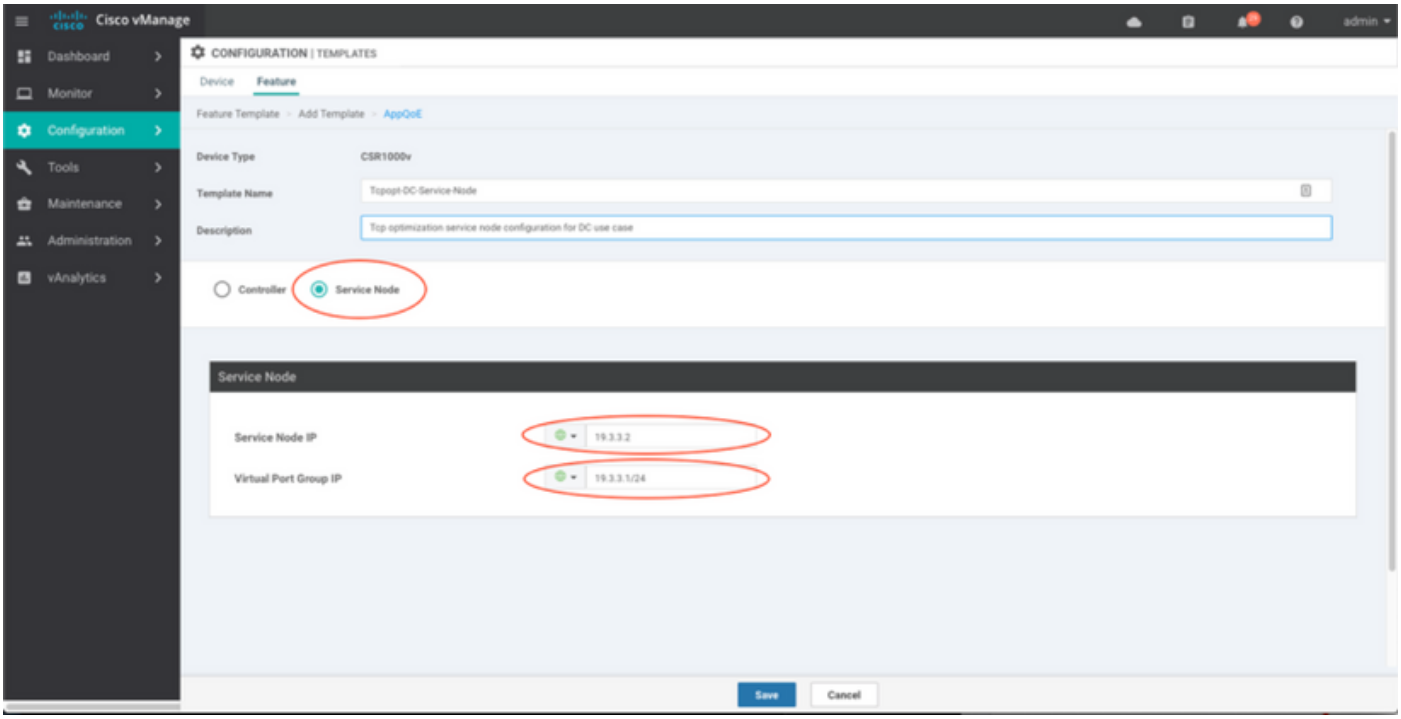
Di seguito è riportata la topologia dello scenario di utilizzo del centro dati con ASR1k e CSR1k esterno:



In questo modello di funzionalità AppQoE viene visualizzato ASR1k configurato come controller:



Di seguito è illustrato CSR1k configurato come Service Node esterno:



Caso di failover

Failover nello scenario di utilizzo del centro dati con CSR1k che funge da SN, in caso di guasto CSR1k esterno:

- Le sessioni TCP già esistenti vengono perse perché la sessione TCP su SN viene terminata.
- Le nuove sessioni TCP vengono inviate alla destinazione finale, ma il traffico TCP non è ottimizzato (bypass).
- Nessuna blackholing per il traffico interessante in caso di guasto della rete SAN.

Il rilevamento del failover si basa sull'heartbeat AppNav, che è di 1 beat al secondo. Dopo 3 o 4 errori, il tunnel viene dichiarato inattivo.

Il failover nello scenario di utilizzo della filiale è simile: in caso di guasto del server di rete, il traffico viene inviato non ottimizzato direttamente alla destinazione.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Verificare l'ottimizzazione TCP sulla CLI con questo comando CLI e vedere il riepilogo dei flussi ottimizzati:

```
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#
```

Questo output fornisce informazioni dettagliate sui flussi ottimizzati:

```
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#
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Note sulla versione di Cisco IOS XE SD-WAN release 16.12.x
- Cisco SD-WAN release 19.1, 19.2 - Guida alla configurazione dell'ottimizzazione TCP
- Cisco SD-WAN - Configurazione dell'ottimizzazione TCP per vEdge
- **Documentazione e supporto tecnico – Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).