

Konfigurieren der TCP-Optimierungsfunktion auf Cisco IOS® XE SD-WAN cEdge-Routern

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

[Unterstützte XE SD-WAN-Plattformen](#)

[Hinweise](#)

[Konfigurieren](#)

[Anwendungsfall 1. Konfigurieren der TCP-Optimierung in einer Außenstelle \(alles in einem cEdge\)](#)

[Anwendungsfall 2. Konfigurieren der TCP-Optimierung im Rechenzentrum mit einem externen SN](#)

[Failover-Fall](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die TCP-Optimierungsfunktion (Transmission Control Protocol) auf Cisco IOS® XE SD-WAN-Routern beschrieben, die im August 2019 mit der Version 16.12 eingeführt wurde. Zu den behandelten Themen gehören Voraussetzungen, Problembeschreibung, Lösung, Unterschiede bei TCP-Optimierungsalgorithmen zwischen Viptela OS (vEdge) und XE SD-WAN (cEdge), Konfiguration, Verifizierung und Liste verwandter Dokumente.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

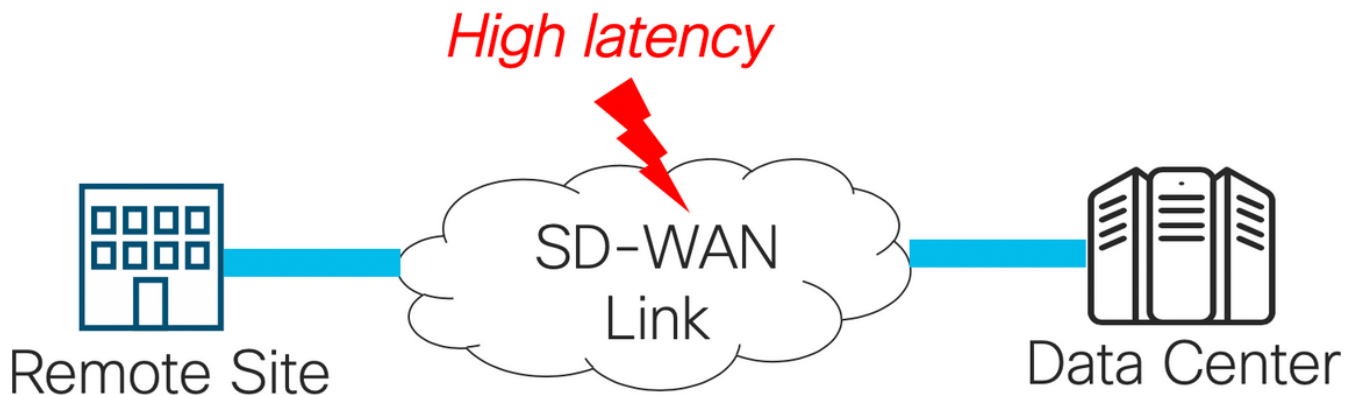
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS®XE SD-WAN.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Problem

Eine hohe Latenz bei einer WAN-Verbindung zwischen zwei SD-WAN-Seiten führt zu einer schlechten Anwendungsleistung. Sie haben kritischen TCP-Datenverkehr, der optimiert werden muss.



Lösung

Wenn Sie die TCP-Optimierungsfunktion verwenden, verbessern Sie den durchschnittlichen TCP-Durchsatz für kritische TCP-Datenflüsse zwischen zwei SD-WAN-Standorten.

Überblick und Unterschiede zwischen TCP-Optimierung auf cEdge Bottleneck-Bandbreite und Round-Trip (BBR) und vEdge (CUBIC)

Bei der XE SD-WAN-Implementierung (auf cEdge) wird ein schneller BBR-Laufzeitalgorithmus verwendet.

Viptela OS (vEdge) verfügt über einen anderen, älteren Algorithmus, den so genannten CUBIC.

CUBIC berücksichtigt hauptsächlich den Paketverlust und wird häufig in verschiedenen Client-Betriebssystemen implementiert. Für Windows, Linux, MacOS und Android ist CUBIC bereits integriert. In einigen Fällen führen ältere Clients den TCP-Stack ohne CUBIC aus, wodurch die TCP-Optimierung auf vEdge verbessert wird. Eines der Beispiele, bei denen die vEdge TCP CUBIC-Optimierung von Nutzen war, ist das Vorhandensein von U-Booten, die alte Client-Hosts und WAN-Verbindungen nutzen, bei denen es zu erheblichen Verzögerungen/Verlusten kam. Beachten Sie, dass TCP CUBIC nur von vEdge 1000 und vEdge 2000 unterstützt wird.

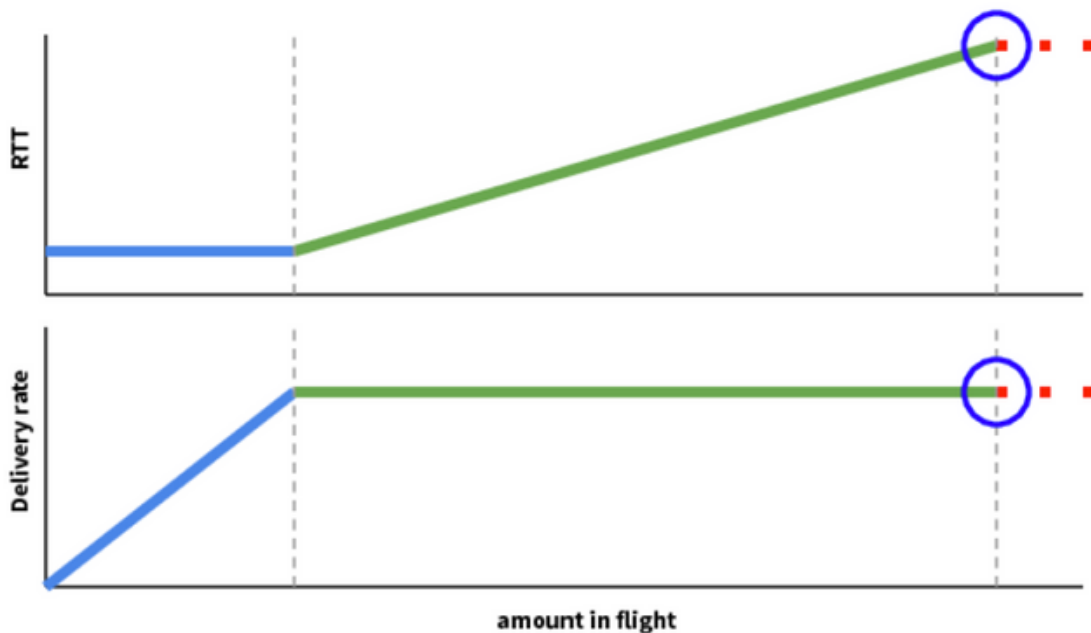
Der Schwerpunkt von BBR liegt auf Round-Trip-Zeit und Latenz. Kein Paketverlust. Wenn Sie Pakete von der West- zur Ostküste der USA oder sogar nach Europa über das öffentliche Internet senden, sehen Sie in den meisten Fällen keinen Paketverlust. Das öffentliche Internet ist manchmal zu gut, was den Paketverlust angeht. Aber was Sie sehen, ist Verzögerung/Latenz. Und dieses Problem wird durch BBR angegangen, das 2016 von Google entwickelt wurde.

Kurz gesagt modelliert BBR das Netzwerk und betrachtet jede Bestätigung (ACK) und aktualisiert die maximale Bandbreite (BW) und die minimale Round-Trip-Zeit (RTT). Die Steuerung des Sendens basiert dann auf dem Modell: Überprüfung auf max. Bandbreite und min. RTT, Annäherung an den Schätzwert und Aufrechterhaltung des Flugverkehrs in der Nähe des Bandwidth-Delay-Product (BDP). Das Hauptziel besteht darin, einen hohen Durchsatz mit einem kleinen Engpass in der Warteschlange sicherzustellen.

Diese Folie von [Mark Claypool](#) zeigt den Einsatzbereich von CUBIC:

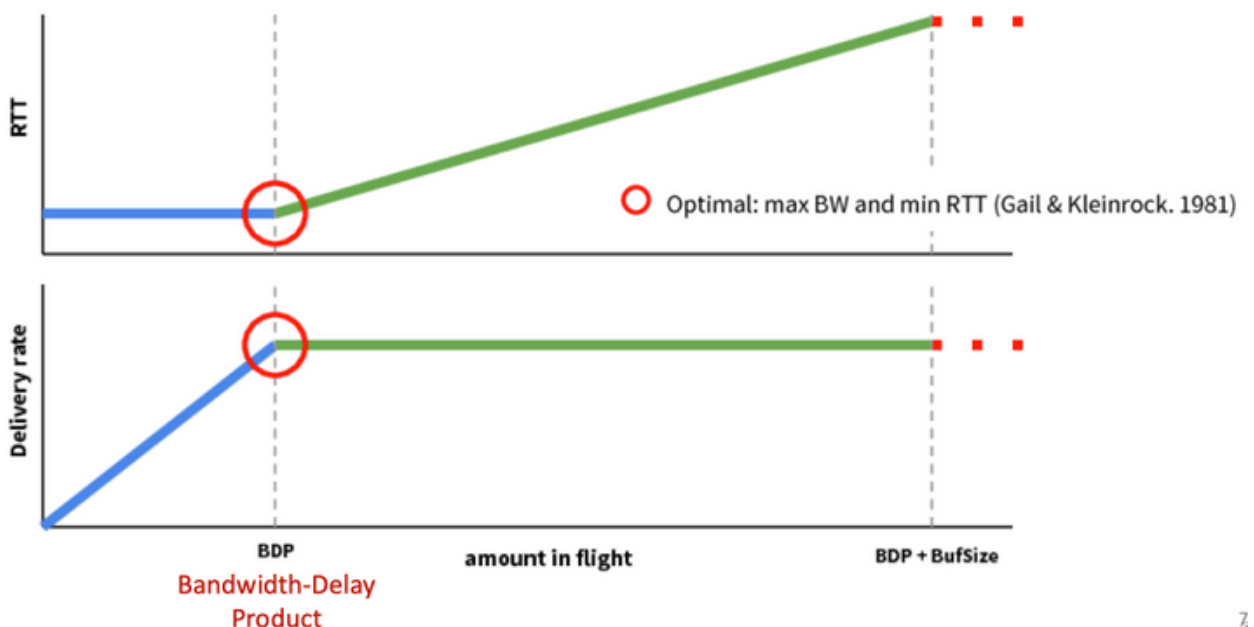
Congestion and Bottlenecks

○ CUBIC / Reno



BBR arbeitet an einem besseren Ort, was in dieser Folie auch von Mark Claypool gezeigt wird:

Congestion and Bottlenecks



Wenn Sie mehr über den BBR-Algorithmus lesen möchten, finden Sie mehrere Publikationen über BBR, die oben auf der [bbr-dev Mailinglisten-Homepage](#) verlinkt sind. [Hier](#) finden Sie die [wichtigsten](#) Informationen.

Zusammenfassung:

Plattform und Algorithmus
 cEdge (XE SD-WAN): BR

Eingabeparameter
 RTT/Latenz

Anwendungsfall
 Kritischer TCP-Datenverkehr zwis

vEdge (Viptela OS): CUBICP

Paketverlust

zwei SD-WAN-Standorten

Alte Clients ohne TCP-Optimierung

Unterstützte XE SD-WAN-Plattformen

In der XE SD-WAN SW-Version 16.12.1d unterstützen diese cEdge-Plattformen TCP-Optimierung BBR:

- ISR 4331
- ISR 4351
- CSR1000v mit 8 vCPU und mind. 8 GB RAM

Hinweise

- Alle Plattformen mit DRAM unter 8 GB RAM werden derzeit nicht unterstützt.
- Alle Plattformen mit 4 oder weniger Datenkernen werden derzeit nicht unterstützt.
- Die TCP-Optimierung unterstützt MTU 2000 nicht.
- Derzeit keine Unterstützung für IPv6-Datenverkehr.
- Optimierung für DIA-Datenverkehr zu einem BBR-Server eines Drittanbieters wird nicht unterstützt. Sie benötigen auf beiden Seiten cEdge SD-WAN-Router.
- Im Rechenzentrumsszenario wird derzeit nur ein Service Node (SN) pro Control Node (CN) unterstützt.
- Derzeit wird kein kombinierter Anwendungsfall mit Sicherheit (UTD-Container) und TCP-Optimierung auf demselben Gerät unterstützt.

Anmerkung: ASR1k unterstützt derzeit keine TCP-Optimierung. Es gibt jedoch eine Lösung für ASR1k, bei der der ASR1k TCP-Datenverkehr über den AppNav-Tunnel (GRE-gekapselt) an einen externen CSR1kv zur Optimierung sendet. Derzeit (Februar 2020) wird nur ein CSR1k als externer Serviceknoten unterstützt. Dies wird später im Konfigurationsabschnitt beschrieben.

In dieser Tabelle werden die Probleme pro Version zusammengefasst und die unterstützten Hardwareplattformen hervorgehoben:

Szenarien	Anwendungsbeispiele	16.12.1	17.2.1	17.3.1	17.4.1	Kommentare
Zweigstelle-zu-Internet	DIA	Nein	Ja	Ja	Ja	In 16.12.1 ist AppNav-Flow-Synchronisierung auf der Internetschnittstelle aktiviert.
	SAAS	Nein	Ja	Ja	Ja	In 16.12.1 ist AppNav-Flow-Synchronisierung auf der Internetschnittstelle aktiviert.
Von Zweigstelle zu Rechenzentrum	Single-Edge-Router	Nein	Nein	EFT	Ja	Unterstützung mehrerer SN erforderlich
	Router mit mehreren Edges	Nein	Nein	EFT	Ja	Flow-Symmetrie oder AppNav-Flow-Synchronisierung erforderlich. 16.12.1

	Mehrere SNs	Nein	Nein	EFT	Ja	getestet mit vManage-Erweiterung Annahme mehrerer IPs
Von Zweigstelle zu Zweigstelle	Vollständiges Mesh-Netzwerk (Spoke-to-Spoke) Hub-and-Spoke (Spoke-Hub-Spoke)	Ja	Ja	Ja	Ja	
BBR-Unterstützung	TCP-Auswahl mit BBR	Nein	Ja	Ja	Ja	
Plattformen	Unterstützte Plattformen	Teilweise	Teilweise	Full-Commit	Full-Commit	
		Nur 4300 und CSR	Alle außer ISR1100	Alle	Alle	

Konfigurieren

Für die TCP-Optimierung wird ein Konzept aus SN und CN verwendet:

- SN ist ein Daemon, der für die eigentliche Optimierung von TCP-Flows verantwortlich ist.
- CN ist als AppNav Controller bekannt und für die Auswahl des Datenverkehrs und den Transport von/zu SN verantwortlich.

SN und CN können auf demselben Router oder getrennt als verschiedene Knoten ausgeführt werden.

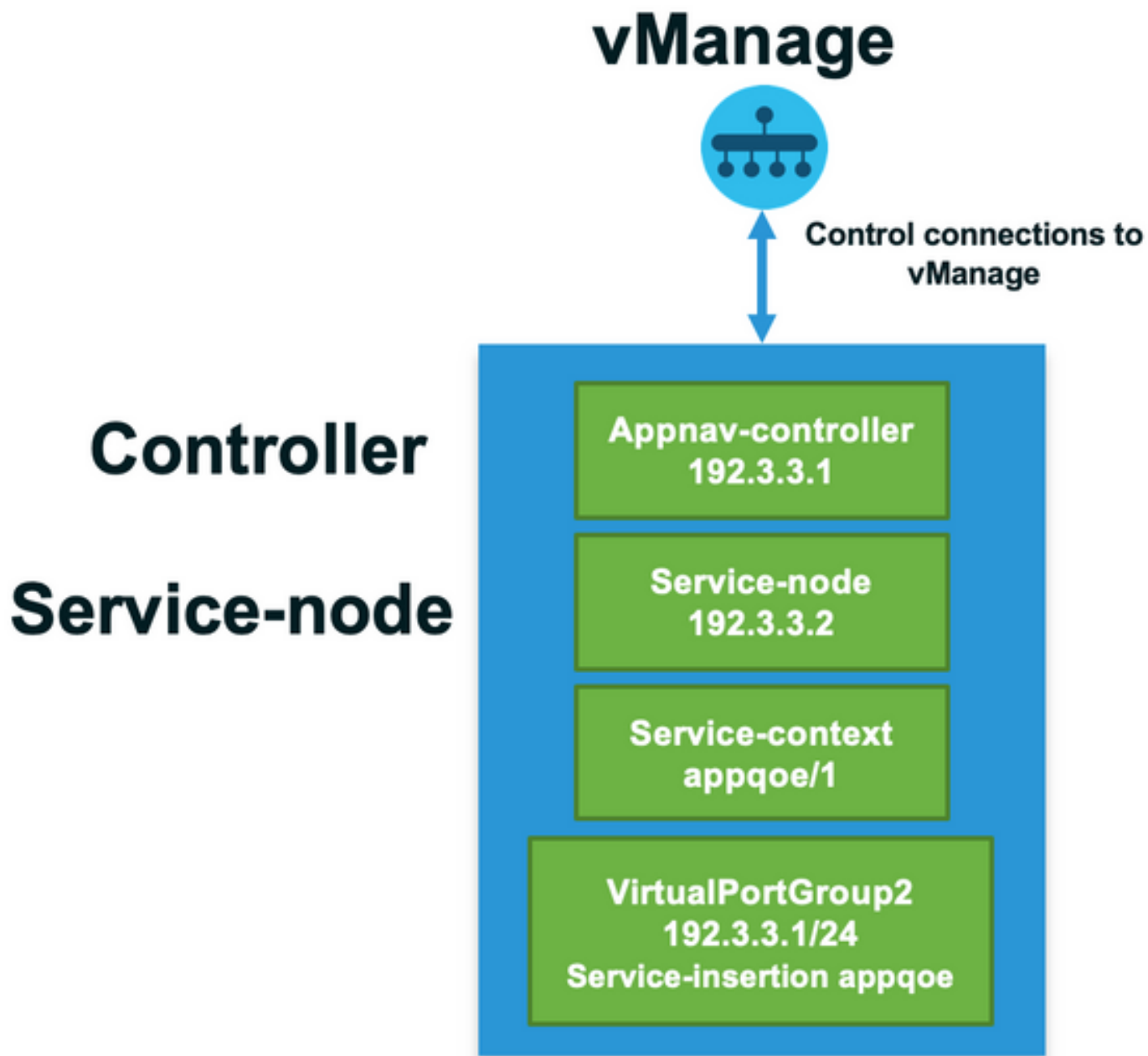
Es gibt zwei Hauptanwendungsfälle:

1. Anwendungsfall in Zweigstellen mit SN und CN auf demselben ISR4k-Router
2. Anwendungsfall für Rechenzentren: CN wird auf ASR1k und SN auf einem separaten virtuellen CSR1000v-Router ausgeführt.

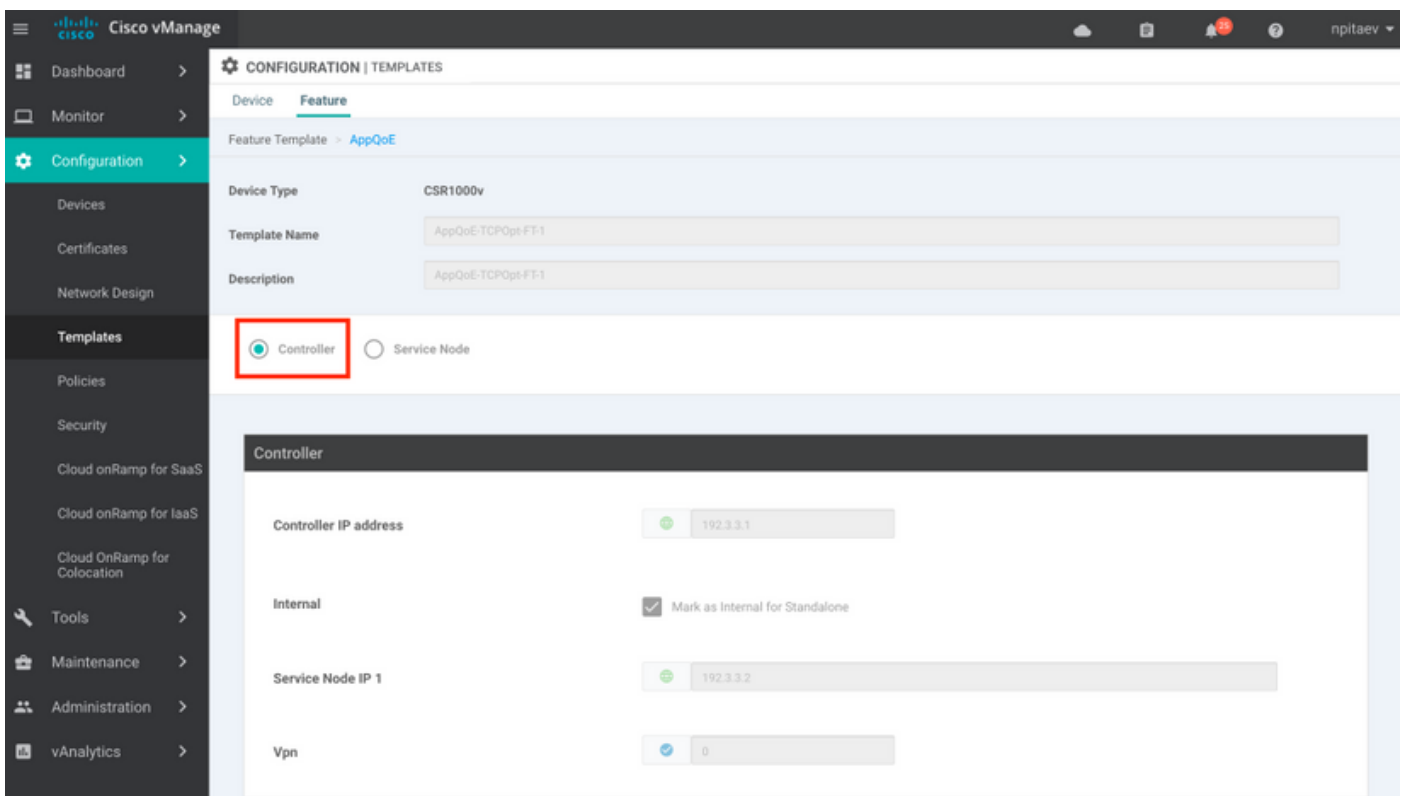
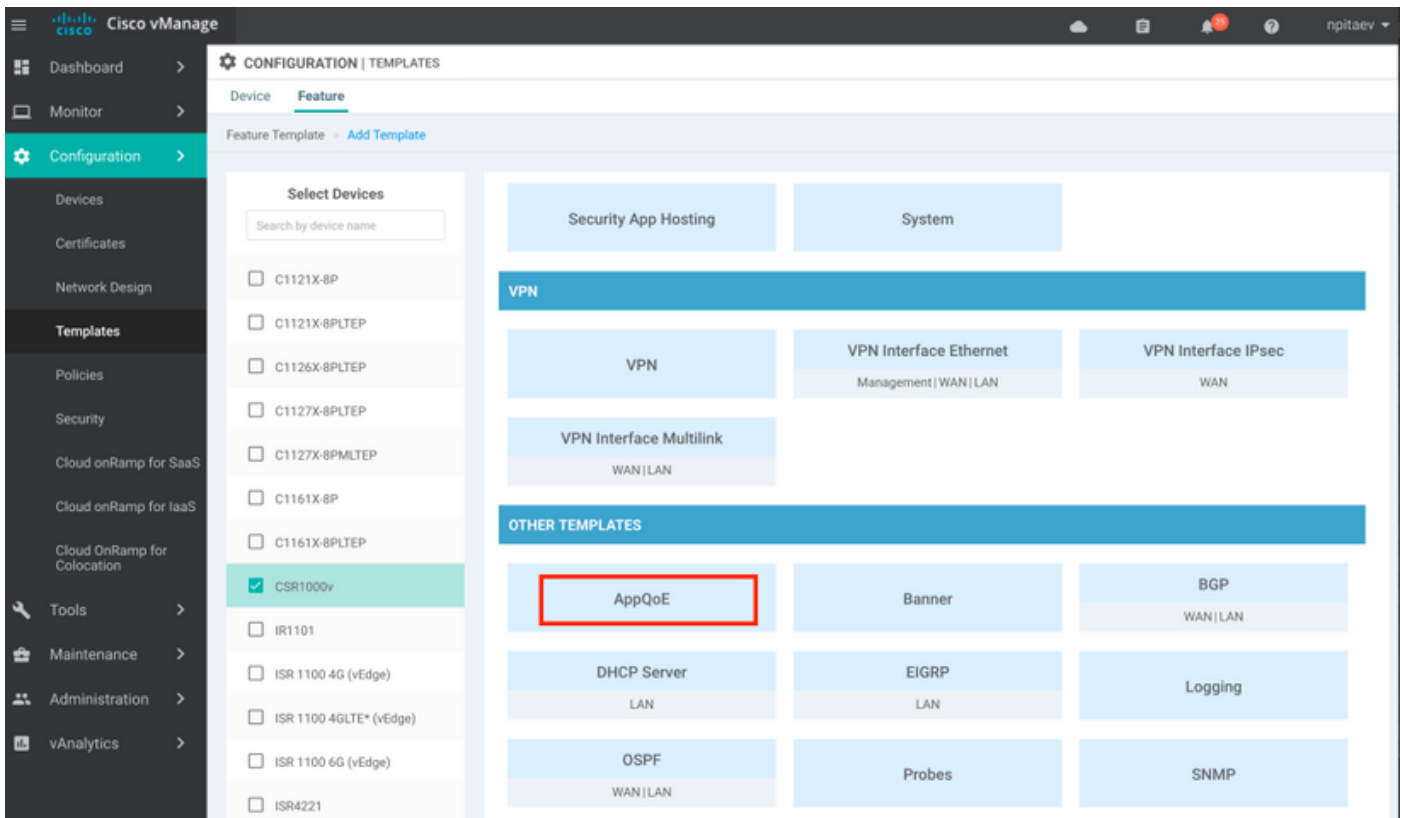
Beide Anwendungsfälle werden in diesem Abschnitt beschrieben.

Anwendungsfall 1. Konfigurieren der TCP-Optimierung in einer Außenstelle (alles in einem cEdge)

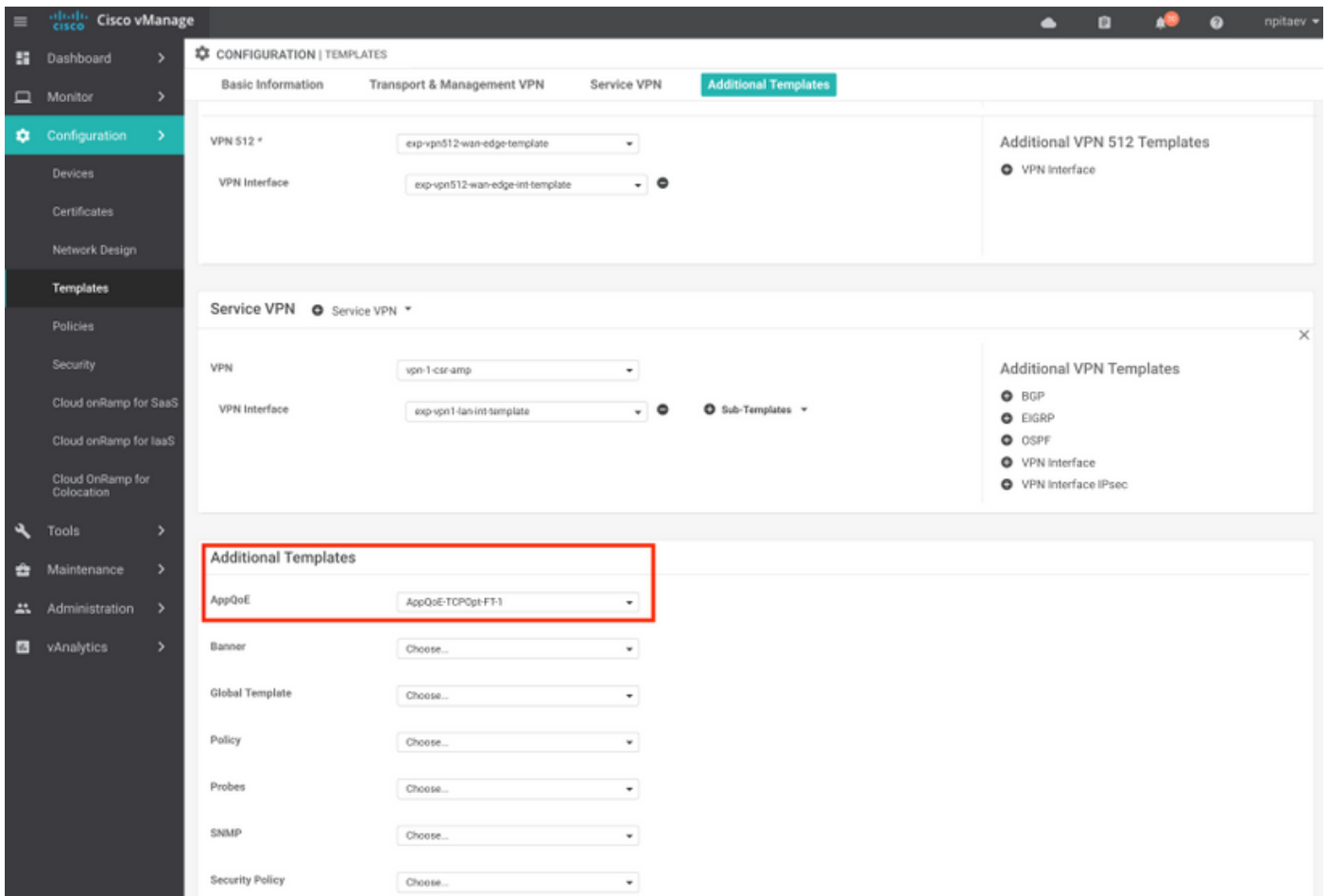
Dieses Bild zeigt die interne Gesamtarchitektur für eine einzelne Standalone-Option in einer Außenstelle:



Schritt 1: Um die TCP-Optimierung zu konfigurieren, müssen Sie in vManage eine Funktionsvorlage für die TCP-Optimierung erstellen. Navigieren Sie zu **Konfiguration > Vorlagen > Funktionsvorlagen > Andere Vorlagen > AppQoE**, wie im Bild dargestellt.



Schritt 2: Fügen Sie die AppQoE-Funktionsvorlage der entsprechenden Gerätevorlage unter "Zusätzliche Vorlagen" hinzu:



Dies ist die CLI-Vorschau der Vorlagenkonfiguration:

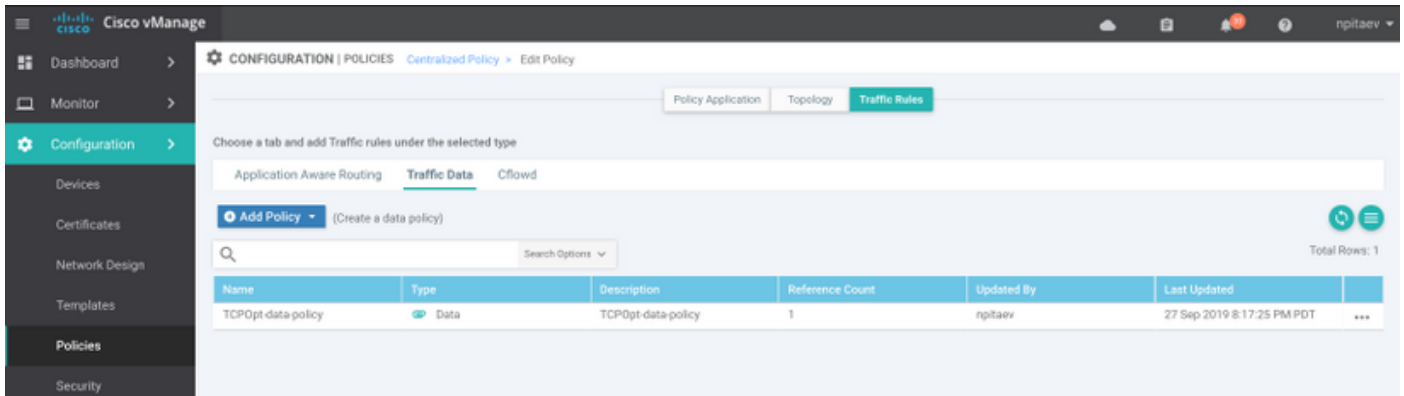
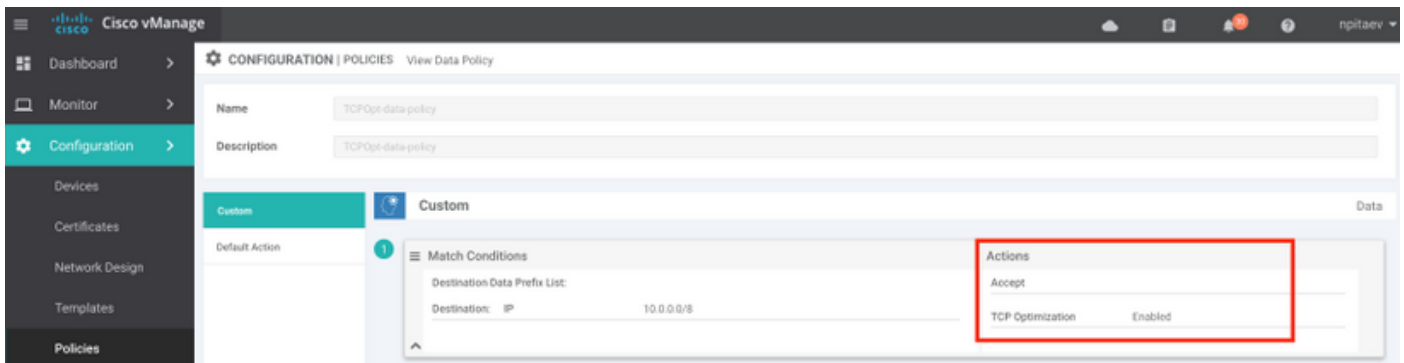
```

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
!

```

Schritt 3: Erstellen Sie eine zentrale Datenrichtlinie mit der Definition des interessanten TCP-Verkehrs für die Optimierung.

Als Beispiel: Diese Datenrichtlinie stimmt mit dem IP-Präfix 10.0.0.0/8 überein, das Quell- und Zieladressen enthält, und aktiviert die TCP-Optimierung:



Dies ist die CLI-Vorschau der vSmart-Richtlinie:

```

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
!
!

```

Anwendungsfall 2. Konfigurieren der TCP-Optimierung im Rechenzentrum mit einem externen SN

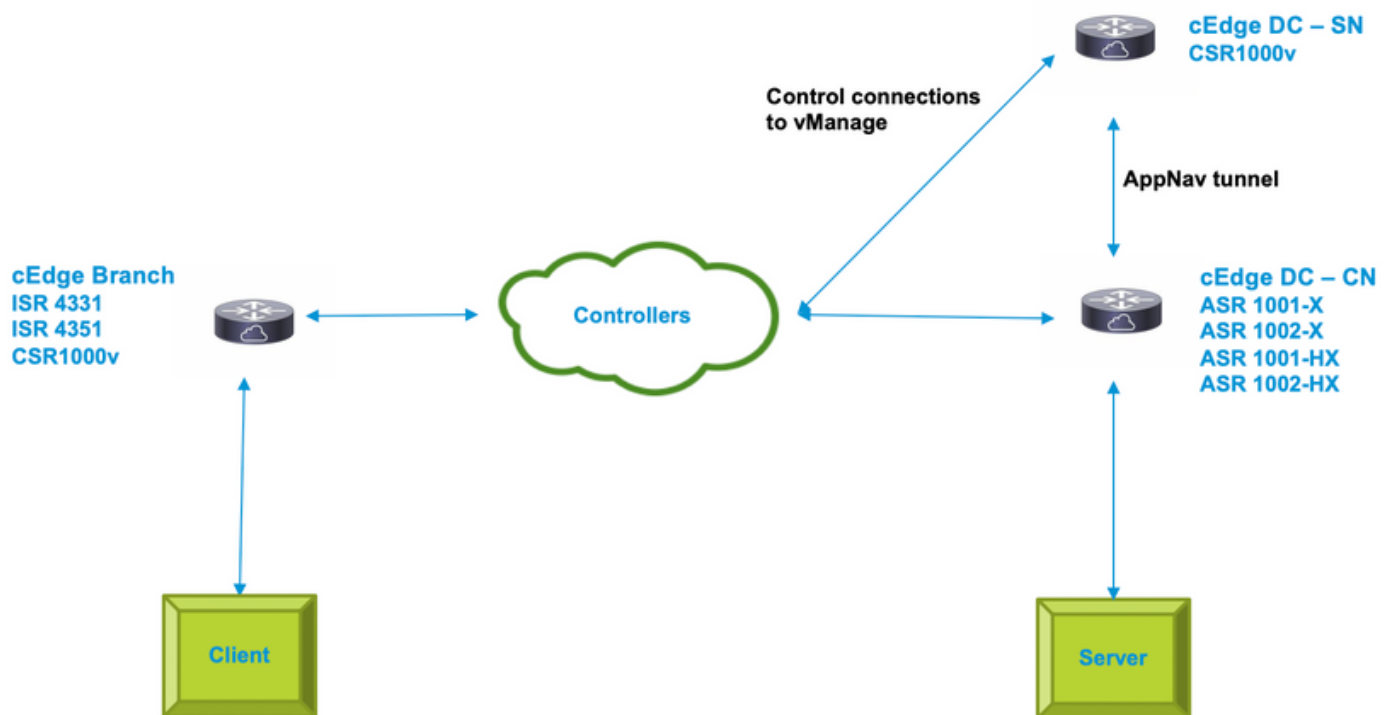
Der Hauptunterschied zwischen SN und CN zum Anwendungsfall für Zweigstellen. Im

Anwendungsfall einer Zweigstelle erfolgt die Anbindung mittels Virtual Port Group Interface innerhalb desselben Routers. Im Anwendungsfall für Rechenzentren gibt es einen AppNav GRE-gekapselten Tunnel zwischen ASR1k als CN und einem externen CSR1k als SN. Es ist keine dedizierte Verbindung oder Cross-Connect-Verbindung zwischen CN und externem SN erforderlich, einfache IP-Erreichbarkeit ist ausreichend.

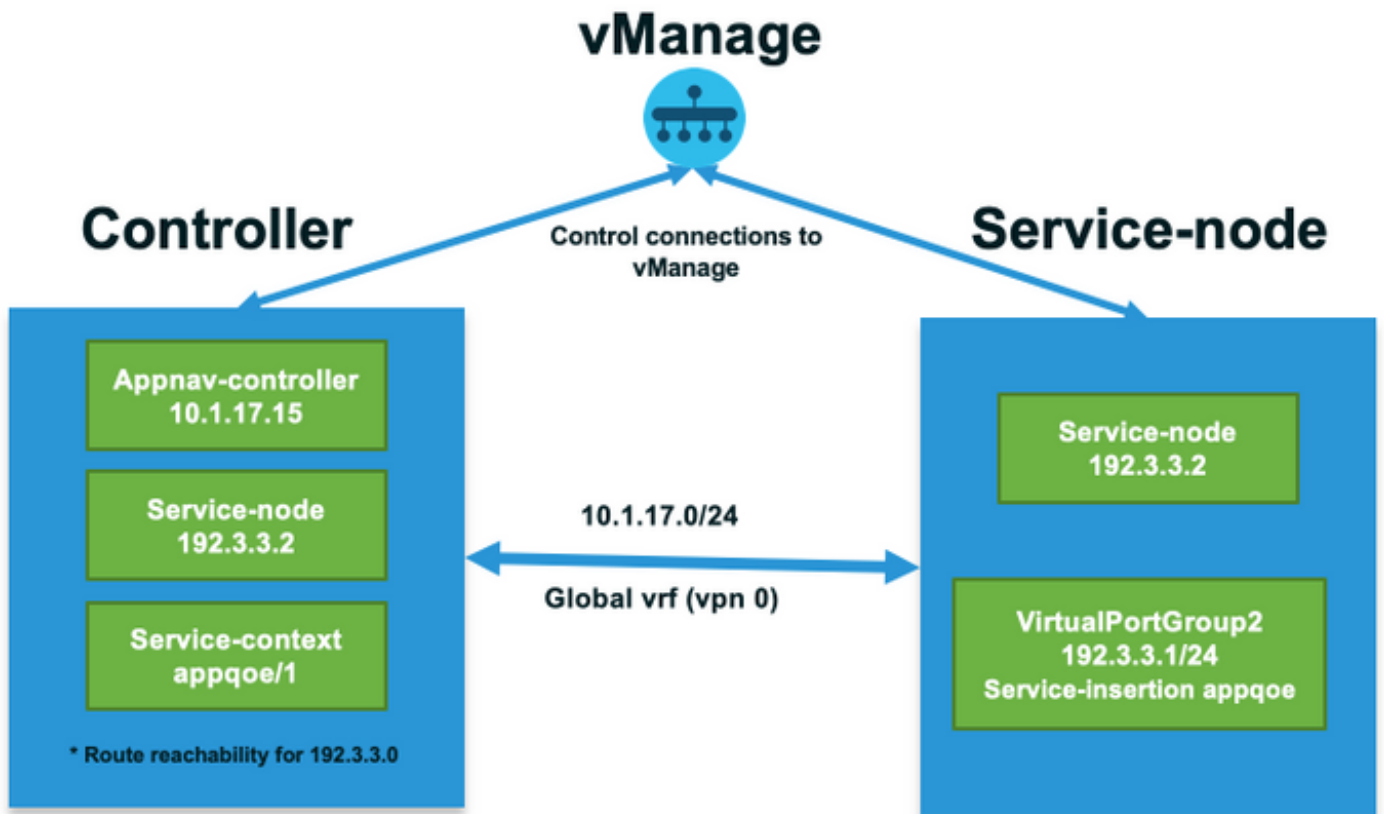
Pro SN ist ein AppNav-Tunnel (GRE) vorhanden. Für die zukünftige Verwendung, bei der mehrere SNs unterstützt werden, wird empfohlen, das Subnetz /28 für das Netzwerk zwischen CN und SN zu verwenden.

Auf einem CSR1k werden zwei NICs empfohlen, die als SN fungieren. Eine zweite NIC für den SD-WAN-Controller ist erforderlich, wenn SN von vManage konfiguriert/verwaltet werden muss. Wenn SN manuell konfiguriert/verwaltet wird, ist die zweite Netzwerkkarte optional.

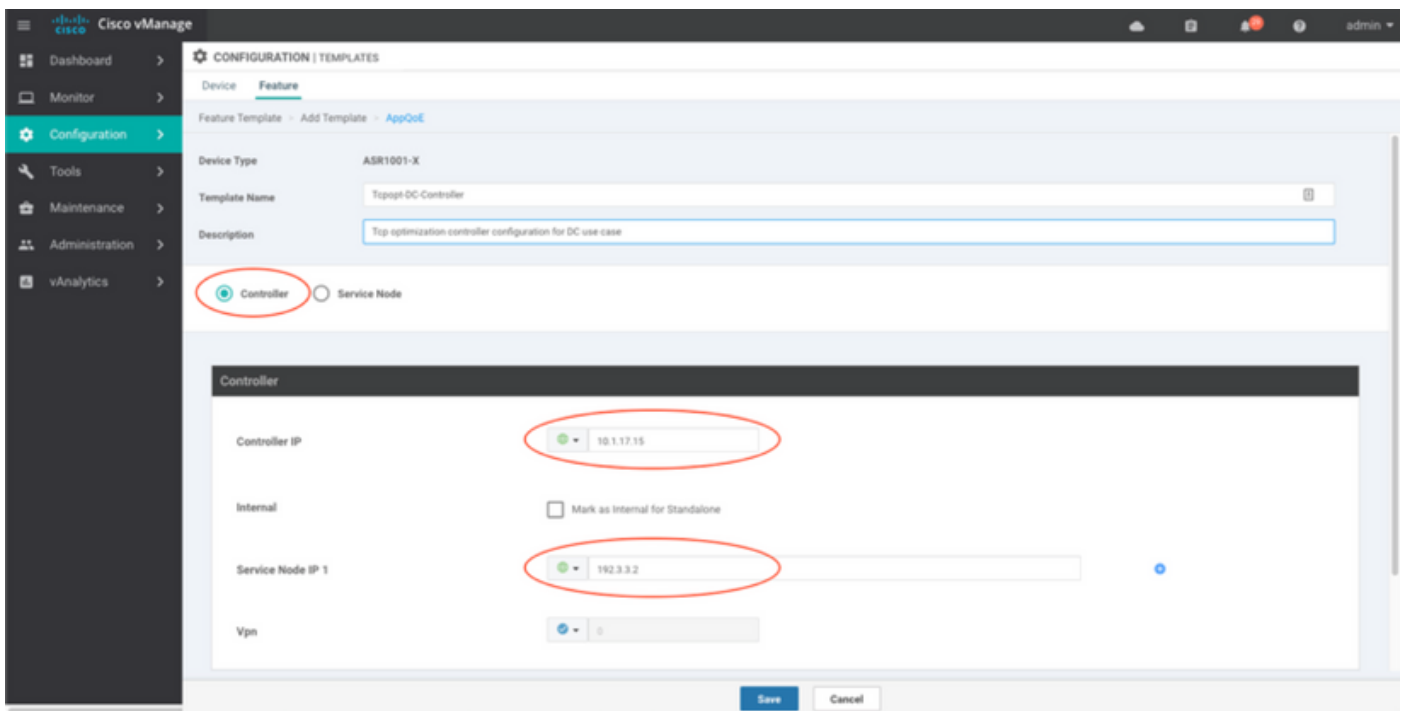
Dieses Bild zeigt das Rechenzentrum ASR1k als CN und CSR1kv als Service Node SN:



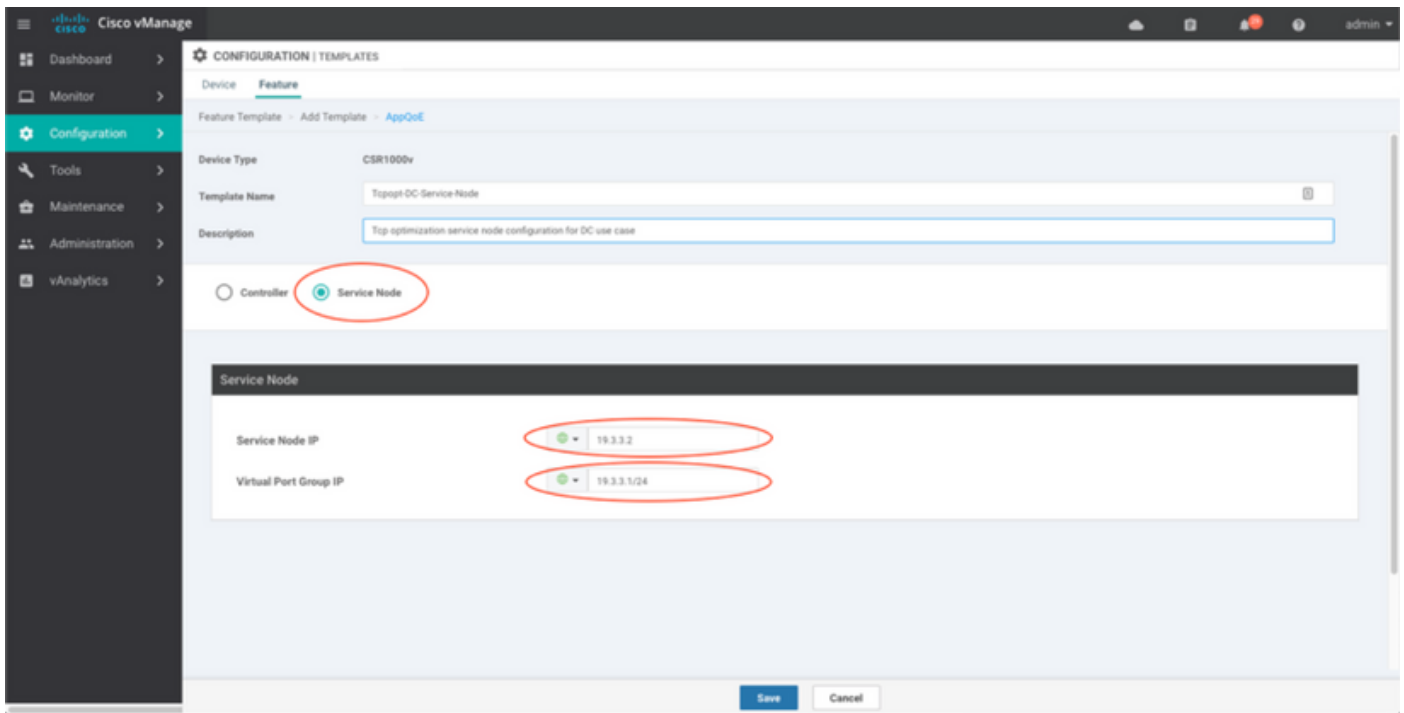
Die Topologie für den Anwendungsfall des Rechenzentrums mit ASR1k und externem CSR1k ist hier dargestellt:



Diese AppQoE-Funktionsvorlage zeigt den als Controller konfigurierten ASR1k:



Der als externer Serviceknoten konfigurierte CSR1k wird hier angezeigt:



Failover-Fall

Failover im Rechenzentrums-Anwendungsfall mit CSR1k als SN, bei einem externen CSR1k-Ausfall:

- Bereits vorhandene TCP-Sitzungen gehen verloren, da die TCP-Sitzung auf SN beendet wird.
- Neue TCP-Sitzungen werden an das endgültige Ziel gesendet, der TCP-Datenverkehr wird jedoch nicht optimiert (umgangen).
- Kein Blackholing von interessantem Datenverkehr bei einem SN-Ausfall.

Die Failover-Erkennung basiert auf AppNav-Heartbeat, d. h. 1 Beat pro Sekunde. Nach 3 oder 4 Fehlern wird der Tunnel als ausgefallen deklariert.

Das Failover in der Außenstelle ist ähnlich: Bei einem SN-Ausfall wird der Datenverkehr nicht optimiert direkt an das Ziel gesendet.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen Sie mithilfe dieses CLI-Befehls die TCP-Optimierung für CLI, und sehen Sie sich die Zusammenfassung der optimierten Datenflüsse an:

```
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#

Diese Ausgabe liefert detaillierte Informationen zu optimierten Flows:

```
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

```
-----
appgoe: 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

```
-----
appgoe: 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#

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung

verfügbar.

Zugehörige Informationen

- [Versionshinweise für Cisco IOS XE SD-WAN Version 16.12.x](#)
- [Cisco SD-WAN-Versionen 19.1, 19.2 - Konfigurieren des TCP-Optimierungsleitfadens](#)
- [Cisco SD-WAN Konfigurieren der TCP-Optimierung für vEdge](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.