Implementierung von QoS in Cisco SD-WAN

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Problem](#)
[Lösung](#)
[Konfigurieren und Implementieren der Cisco SD-WAN QoS](#)
[Konfigurieren der QoS-Richtlinie](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird der Cisco Viptela-Ansatz zur Implementierung von Quality of Service (QoS) mit Software Defined WAN (SD-WAN) beschrieben. SD-WAN ist die neueste Innovation für die Integration in Unternehmen, Unternehmen und Unternehmen weltweit. Mit der neuen SD-WAN-Technologie können Regierungen und Unternehmen wichtige Anwendungen ohne zusätzlichen Aufwand unterstützen. Obwohl die Cloud den Kapazitäts-Provisioning-Prozess erheblich vereinfacht hat, stellt sie im Bereich des QoS-Managements eine Reihe neuer Herausforderungen dar. Das neue SD-WAN muss mit der Leistung, Zuverlässigkeit und Verfügbarkeit einer Anwendung und der Plattform oder Infrastruktur, die bzw. die sie hostet, übereinstimmen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- SD-WAN-Lösung
- Traditionelle QoS und Richtlinienstruktur

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco vEdge-Hardwaregeräte
- Cisco vEdge-Software (VM)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

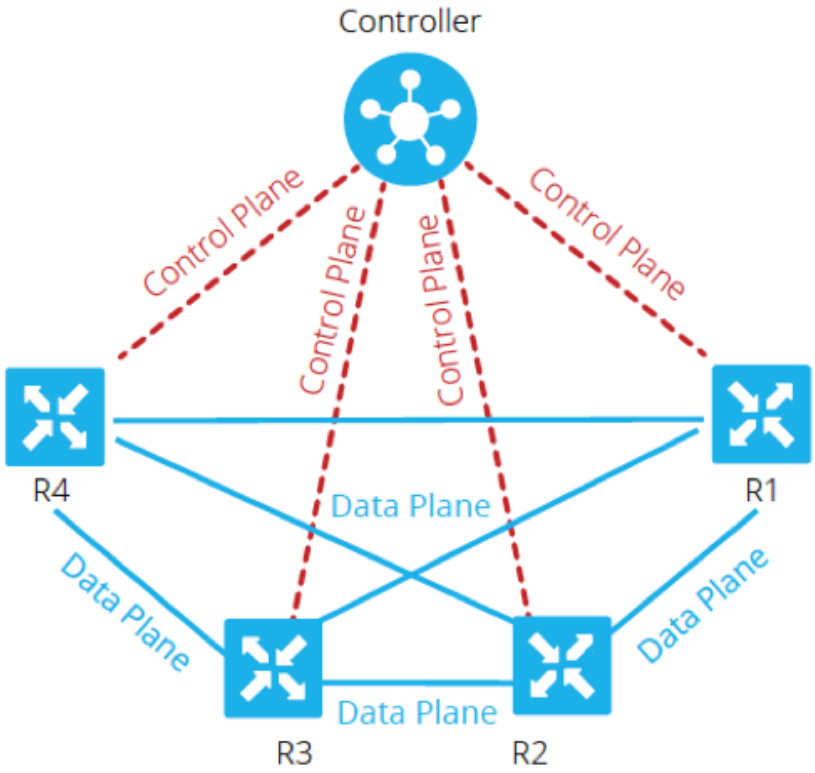
Bis vor kurzem basierten die Netzwerke streng auf den zugrunde liegenden Übertragungsnetzwerken. Einige Lösungen, z. B. Multiprotocol Label Switching (MPLS) Traffic Engineering, beeinflussten die Pfadauswahl zwischen Knoten. Jedes Gerät von der Quelle bis zum Ziel musste jedoch programmiert werden, um Datenverkehr zwischen zwei Endpunkten zuzulassen oder zu verweigern und völlig autonome Entscheidungen zu treffen.

Traditionelle Carrier-Services wie ein IP-VPN oder MPLS werden von vielen als die einzige Möglichkeit angesehen, die QoS-Services für ein Unternehmen zuverlässig bereitzustellen. Der größte Nachteil von MPLS sind die Bandbreitenkosten. Die Verbraucher von heute sind zunehmend an bandbreitenintensiven Multimedia-Inhalten wie Videos und Augmented Reality (AR)/Virtual Reality (VR) interessiert. Gleichzeitig steigen die Kosten pro Megabit, die MPLS-Anforderungen verursachen. Schließlich bietet ein MPLS-Netzwerk keinen integrierten Datenschutz. Wenn es falsch implementiert ist, kann es Schwachstellen im Netzwerk verursachen.

Aus Sicherheitssicht wird auch der MPLS-Datenverkehr nicht standardmäßig verschlüsselt. MPLS-Netzwerke bieten viele Sicherheitsfunktionen, ihre traditionellen VPN-Lösungen sind jedoch nicht ohne Herausforderungen. Ein vorinstallierter Schlüssel dient zur Authentifizierung von VPN IPSec-Geräten. Um jedoch eine große Anzahl von vorinstallierten Schlüsseln auf mehreren Geräten zu verwalten, ist die Skalierung und Sicherheit nicht ausreichend.

Lösung

Im SD-WAN-Ansatz werden hingegen zentralisierte WAN-Controller zum Hosten und Verwalten aller Adjacencies mit Knoten im Netzwerk verwendet. Sie bietet Flexibilität bei der Erstellung und Durchsetzung von Richtlinien. Da jedes Gerät nur über Controller Peers für die Anbindung und Kontrollebenenrichtlinien verfügt, um Datenverkehr zwischen Service-Knoten zu übertragen, können diese dynamisch angepasst werden, basierend auf der allgemeinen Transparenz der Netzwerkbedingungen. Wie hier gezeigt, gibt jeder Router seine lokalen Informationen an den Controller weiter. So kann der Datenfluss durch den zentralen Controller einfach mithilfe von Richtlinien gesteuert werden, die an jedem lokalen Router durchgesetzt werden.



In diesem Beispiel haben R1 und R4 keine paarweise Adjacency nur den Datenebenenpfad. Der zentrale Controller steuert und ändert daher problemlos den Datenverkehrsfluss. So kann sie beispielsweise alle Präfixe von R1 steuern, die R4 über R3 angekündigt werden, oder bestimmte Präfixe werden R4 über R3 angekündigt, während bestimmte Präfixe direkt von R1 angekündigt werden, wobei R3 ein Anwendungspunkt für eine Firewall-Richtlinie sein könnte. Durch diesen Ansatz wird die Anzahl der Datenebenenrichtlinien, die auf jedem Router implementiert werden müssen, durch die Verwendung herkömmlicher Netzwerktopologien drastisch reduziert. SD-WAN ist ein Overlay-Netzwerk, das Administratoren bei der Identifizierung von geschäftskritischem Datenverkehr und der Bereitstellung einer speziellen Behandlung im gesamten Netzwerk unterstützt.

Konfigurieren und Implementieren der Cisco SD-WAN QoS

Im SD-WAN-Overlay-Netzwerk funktioniert die QoS, wenn die Pakete untersucht werden, die am Netzwerk-Edge eingehen. Jeder vEdge-Router im Netzwerk muss für die Bereitstellung von QoS konfiguriert werden. Sobald das SD-WAN-Overlay-Netzwerk und die Steuerungsebenenverbindungen eingerichtet und ausgeführt sind, fließt der Datenverkehr automatisch über die IPsec-Verbindungen zwischen den vEdge-Routern. Der standardmäßige Datenpaketweiterleitungsfluss kann geändert werden, wenn eine zentrale Datenrichtlinie oder eine lokalisierte Datenrichtlinie erstellt und angewendet werden.

Die zentralisierte Datenrichtlinie gibt die Kontrolle über das Management des Datenverkehrspfads, der über das Netzwerk geroutet wird. Der Datenverkehr kann anhand der Felder für Adresse, Port und Differentiated Services Code Point (DSCP) im IP-Header des Pakets gesteuert werden (zulassen oder blockieren).

Die lokalisierte Datenrichtlinie kann den Datenverkehrsfluss an den Schnittstellen eines vEdge-Routers steuern und Funktionen wie QoS aktivieren. Die Richtlinien können aktiviert werden, wenn Sie die Zugriffslisten entweder in die ausgehende Richtung oder in die eingehende Richtung anwenden.

Jede Schnittstelle verfügt über acht Warteschlangen auf Hardware-vEdge-Routern, die von 0 bis 7 nummeriert sind. Warteschlange 0 ist reserviert und wird sowohl für Steuerungs- als auch LLQ-Datenverkehr (Low Latency Queuing) verwendet. Für LLQ muss jede Klasse, die Warteschlange 0 zugeordnet ist, auch für die Verwendung von LLQ konfiguriert werden. Der gesamte Steuerungsdatenverkehr wird übertragen. Für den Datenverkehr sind die Warteschlangen 1 bis 7 verfügbar.

Wie in Abbildung 2 gezeigt, werden die QoS-Richtlinien auf ein Datenpaket angewendet, das von einer Außenstelle zur anderen übertragen wird:

1. Eingangsklassifizierung - Der eingehende Datenverkehr kann klassifiziert werden, indem jedes Paket einer Weiterleitungsklasse zugeordnet wird. Die Weiterleitungsklassen gruppieren Datenpakete und weisen Pakete für Ausgabewarteschlangen zur Übertragung an ihr Ziel zu, basierend auf der Weiterleitungsklasse.

2. Eingabe von ACLs und Definition von Policer: Die maximale Datenverkehrsrate von gesendeten oder empfangenen Daten auf einer Schnittstelle kann durch die Konfiguration von Policers und die Aufteilung eines Netzwerks in mehrere Prioritätsebenen gesteuert werden. Policers für den eingehenden Schnittstellendatenverkehr ermöglichen Ihnen die Einsparung von Ressourcen, indem Sie Datenverkehr verwerfen, der nicht über das Netzwerk geroutet werden muss.

3. Route Lookup - Der vEdge-Router überprüft die lokale Routing-Tabelle, um festzustellen, welche Schnittstelle das Paket verwenden soll, um sein Ziel zu erreichen.

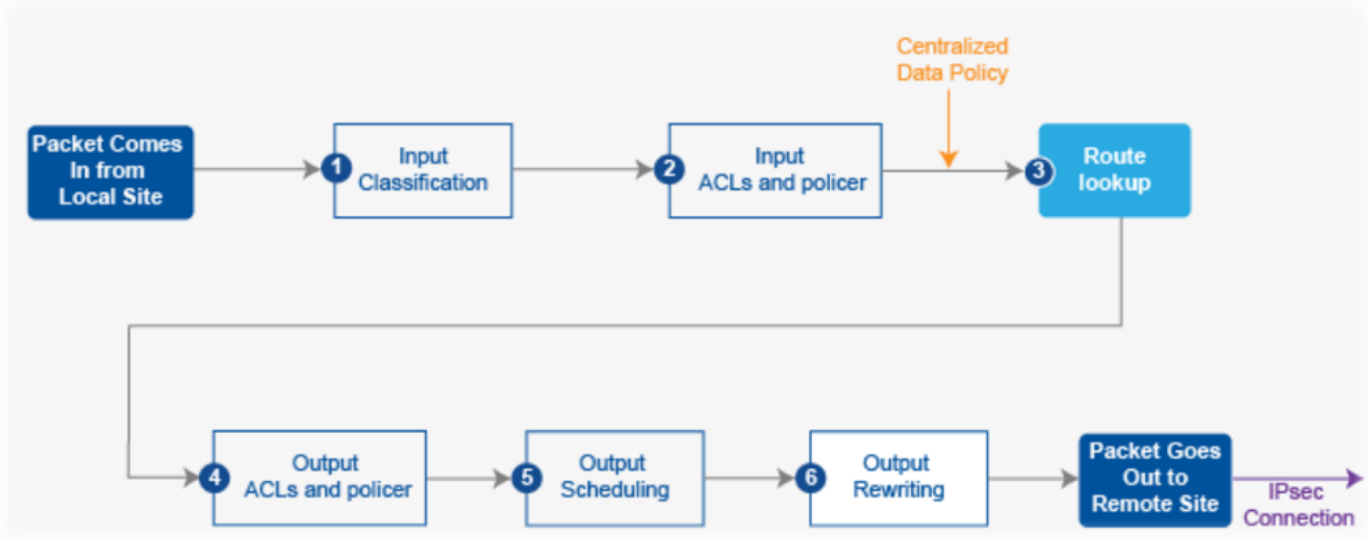
4. Ausgabe-ACLs und Policer - Datenverkehr, der der Policer-Rate entspricht, wird übertragen, und Datenverkehr, der die Policer-Rate überschreitet, wird mit einer verminderten Priorität gesendet oder verworfen. Die auf den ausgehenden Schnittstellendatenverkehr angewendeten Policers steuern die genutzte Bandbreite.

5. Ausgabeplanung - Die Pakete können priorisiert werden, indem für jede Ausgabewarteschlange eine QoS-Zuordnung konfiguriert wird, um die Bandbreite, die Verzögerungspuffergröße und die Paketverlustpriorität (Packet Loss Priority, PLP) der Ausgabewarteschlangen anzugeben. Dies hängt von der Priorität des Datenverkehrs ab, der die Zuweisung von Paketen mit höherer oder niedrigerer Bandbreite, Pufferebenen und Drop-Profilen ermöglicht.

6. Ausgabe umschreiben: Wenn Sie Regeln umschreiben, können Sie Datenverkehr zuordnen, um Punkte zu codieren, wenn der Datenverkehr aus dem System ausläuft. Definieren Sie eine Umschreibregel, um das DSCP-Feld des äußeren IP-Headers zu überschreiben. Wenden Sie die Umschreibregel auf die Ausgangsschnittstelle an.

Konfigurieren der QoS-Richtlinie

In diesen Schritten wird die Konfiguration der lokalisierten Datenrichtlinie (QoS) beschrieben:



Schritt 1: Konfigurieren Sie die Weiterleitungsklassen und die Zuordnung zu Ausgabewarteschlangen. Definieren Sie **Klassenzuordnung**, um Pakete nach Wichtigkeit in entsprechende Weiterleitungsklassen zu klassifizieren. Weitere Informationen finden Sie in der **Klassenzuordnung** in einer Zugriffsliste.

```
policy

 class-map

 class best-effort queue 3

 class bulk-data queue 2

 class critical-data queue 1

 class voice queue 0
```

Schritt 2: Konfigurieren Sie die Weiterleitungsklassen des QoS-Planers. Definieren Sie **qos Scheduler** und geben Sie die Geschwindigkeit an, mit der Datenverkehr an die Schnittstelle gesendet wird. Siehe Richtlinie in einer Zugriffsliste.

```
policy

 qos-scheduler be-scheduler

 class                          best-effort

 bandwidth-percent     20

 buffer-percent             20

 scheduling                  wrr

 drops                          red-drop

 !

 qos-scheduler bulk-scheduler

 class                          bulk-data

 bandwidth-percent     20
```

```
 buffer-percent            20
 scheduling                 wrr
 drops                         red-drop
 !
 qos-scheduler critical-scheduler
 class                          critical-data
 bandwidth-percent     40
 buffer-percent            40
 scheduling                 wrr
 drops                         red-drop
 !
 qos-scheduler voice-scheduler
 class                          voice
 bandwidth-percent     20
 buffer-percent            20
 scheduling                 llq
 drops                         tail-drop
```

Schritt 3: Gruppen-QoS-Scheduler und definieren QoS-Zuordnung:

```
policy
 qos-map MyQoSMap
 qos-scheduler be-scheduler
 qos-scheduler bulk-scheduler
 qos-scheduler critical-scheduler
 qos-scheduler voice-scheduler
```

Schritt 4: Wenden Sie die QoS-Zuordnung auf die Ausgangsschnittstelle an:

```
interface ge0/1
 qos-map  MyQoSMap
```

Schritt 5: Definieren Sie eine Zugriffsliste, um Datenpakete in geeignete Weiterleitungsklassen zu klassifizieren:

```
policy
 access-list MyACL
```

```
sequence 10
 match
  dscp 46
 !
 action accept
  class voice
 !
!
sequence 20
 match
  source-ip          10.1.1.0/24
  destination-ip   192.168.10.0/24
 !
 action accept
  class bulk-data
  set
   dscp 32
  !
 !
!
sequence 30
 match
  destination-ip  192.168.20.0/24
 !
 action accept
  class critical-data
  set
   dscp 22
  !
 !
!
sequence 40
```

```
  action accept
   class best-effort
   set
    dscp 0
   !
  !
 !
 default-action drop
```

Schritt 6: Anwenden der Zugriffsliste auf eine Schnittstelle:

```
vpn 10
 interface ge0/0
 access-list MyACL in
 !
```

Zugehörige Informationen

Ideale Anforderungen für garantierte QoS mit SD-WAN:

Es ist leicht verständlich, warum dies als Lösung die herkömmlichen MPLS-WANs dort draußen bedroht, da die Cisco SD-WAN QoS-Lösung die QoS-Level bereitstellen kann, die über das Internet mit dynamischen Methoden übereinstimmen. Cisco SD-WAN wählt dynamisch das kosteneffizienteste Sortiment an privaten Links und öffentlichen Internetverbindungen aus. Bei einem SD-WAN werden Anwendungen nicht der Standardbandbreite ausgeliefert, sondern die Verbindung, die für jede Anwendung am besten geeignet ist, wird ausgewählt.

Unabhängig davon, ob MPLS oder SD-WAN die beste Lösung ist, ist zu beachten, dass die QoS mit SD-WAN ohne MPLS mit einem symmetrischen Internet ohne Paketverlust mit VPN erreicht werden kann. Wenn Datenverkehr über mehrere Hops über mehrere ISPs übertragen wird, kann ein Unternehmen nicht garantieren, wie geschäftskritische und verzögerungsempfindliche Services funktionieren. Tatsächlich benötigen die SD-WAN-Produkte Aktiv-Aktiv-Konfigurationen, um die Zuverlässigkeit und QoS des WAN zu verbessern.

Kurz gesagt: SD-WAN ist eine fantastische Technologie, die die Abhängigkeit von MPLS-Netzwerken in Zukunft verringert. Sie können einen Teil des nicht interaktiven Datenverkehrs auf eine Breitband-Internetverbindung auslagern. So kann beispielsweise das SD-WAN latenzempfindlichen Datenverkehr wie Sprache über eine MPLS-Verbindung weiterleiten, die QoS garantiert, und alles andere über eine Breitband-Internetverbindung, oder es können zwei Breitband-Verbindungen zu einem ungefähren MPLS kombiniert werden.