QoS implementeren in Cisco SD-WAN

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Probleem](#)
[Oplossing](#)
[Cisco SD-WAN QoS configureren en implementeren](#)
[QoS-beleid configureren](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de Cisco-Videobenadering om Quality of Service (QoS) te implementeren met softwaregedefinieerde WAN (SD-WAN). SD-WAN is de meest recente innovatie om te kunnen integreren met bedrijven, bedrijven en organisaties in de hele wereld. De nieuwe golf van SD-WAN technologieën stelt overheden en bedrijven in staat om kritische toepassingsondersteuning te bieden zonder extra problemen. Hoewel de wolk het capaciteitsvoorzieningsproces enorm heeft vereenvoudigd, kent het verschillende nieuwe uitdagingen op het gebied van het QoS-beheer. Het nieuwe SD-WAN moet voldoen aan de prestatieniveaus, betrouwbaarheid en beschikbaarheid die worden geboden door een toepassing en door het platform of de infrastructuur die er de gastheer van is.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SD-WAN oplossing
- Traditionele QoS- en beleidsstructuur

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco vEdge-hardwareapparaten
- Cisco vEdge-software (VM)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

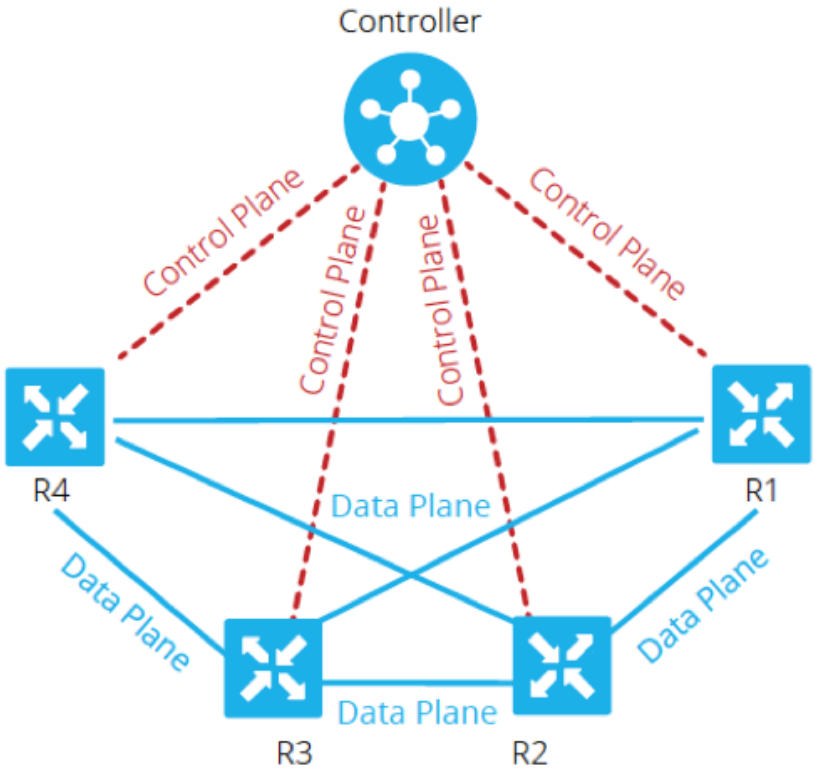
Tot voor kort waren de netwerken strikt gebaseerd op de manier waarop de onderliggende transmissienetwerken zijn. Sommige oplossingen, zoals Multiprotocol Label Switching (MPLS) Traffic Engineering beïnvloedden de selectie van snijpunten tussen knooppunten, maar elk apparaat van bron naar bestemming moet worden geprogrammeerd om verkeer dat tussen twee endpoints stroomt toe te staan of te ontkennen en volledig autonome beslissingen te nemen.

De traditionele transportservices zoals een IP VPN of MPLS zijn door velen verondersteld de enige manier te zijn om de QoS-services voor een organisatie betrouwbaar af te leveren. De grootste negatieve kant van MPLS is bandbreedtekosten. Vandaag de dag zijn consumenten steeds meer geïnteresseerd in het bewaren van bandbreedte-gerelateerde multimedia-inhoud zoals video's en Augmented Reality (AR)/ Virtual Reality (VR), en de hoge kosten per megabit die de MPLS-eisen kunnen mislopen. Ten slotte biedt een MPLS-netwerk geen ingebouwde gegevensbeveiliging aan en kan het netwerk, als het niet correct wordt geïmplementeerd, worden geopend op kwetsbaarheden.

Vanuit veiligheidsoogpunt wordt het MPLS-verkeer niet standaard versleuteld. MPLS-netwerken bieden veel beveiligingsfuncties aan, maar hun traditionele VPN-oplossingen zijn niet zonder problemen. Een vooraf gedeelde sleutel wordt gebruikt om VPN IPSec-apparaten voor authentiek te verklaren, maar om een groot aantal pre-gedeelde sleutels over meerdere apparaten te beheren geen schaal en is minder veilig.

Oplossing

Aan de andere kant gebruikt de SD-WAN benadering gecentraliseerde WAN controllers om alle nabijheid met knooppunten in het netwerk te ontvangen en te beheren. Het zorgt voor flexibiliteit bij het opzetten en uitvoeren van beleid. Aangezien elk apparaat alleen peers heeft met controllers voor connectiviteit en controle vliegtuigbeleid om gegevensverkeer tussen de dienstknooppunten door te geven, kunnen deze dynamisch worden aangepast op basis van algehele zichtbaarheid in netwerkomstandigheden. Zoals hier wordt getoond, adverteert elke router zijn lokale informatie aan de controller. Dit maakt het mogelijk dat gegevensstroom eenvoudig wordt gemanipuleerd door de centrale controller met het gebruik van beleid dat op elke lokale router wordt afgedwongen.



In dit voorbeeld, hebben R1 en R4 geen paarsgewijze nabijheid enkel het gegevenspadpad. Daarom regelt en wijzigt de centrale controller de verkeersstroom gemakkelijk. Zo kan zij alle prefixes van R1 die via R3 aan R4 worden geadverteerd, controleren of bepaalde prefixes via R3 aan R4 worden geadverteerd, terwijl bepaalde prefixes rechtstreeks worden geadverteerd via R1, waar R3 een punt van toepassing kan zijn op een firewallbeleid. Deze benadering reduceert dramatisch het volume van gegevensbeleid dat op elke router moet worden geïmplementeerd, met het gebruik van traditionele netwerktopologieën. SD-WAN is een overlay netwerk dat beheerders kan helpen om kritisch verkeer te identificeren en er een speciale behandeling door het netwerk op te zetten.

Cisco SD-WAN QoS configureren en implementeren

In het SD-WAN overlay netwerk, werkt QoS wanneer het de pakketten onderzoekt die aan de rand van het netwerk binnendringen. Elk van de vEdge-routers in het netwerk moet worden geconfigureerd om QoS te leveren. Zodra het SD-WAN overlay netwerk en de besturingsplannen actief zijn, stroomt het gegevensverkeer automatisch via de IPsec-verbindingen tussen vEdge-routers. De standaard gegevenspakketdoorvoerstroom kan worden gewijzigd wanneer het gecentraliseerde gegevensbeleid of het gelokaliseerde gegevensbeleid worden gecreëerd en toegepast.

Het gecentraliseerde gegevensbeleid geeft de controle om het verkeer-pad te beheren dat door het netwerk wordt routeerd en het verkeer kan worden gecontroleerd (licentie of blok) op basis van het adres, de poort en de velden Gedifferentieerd servicescodepunt (DSCP) in de IP-header van het pakket.

Het gelokaliseerde gegevensbeleid kan de stroom van gegevensverkeer in en uit de interfaces van een vEdge-router controleren en functies zoals QoS toestaan. Het beleid kan worden geactiveerd als u de toegangslijsten toepast, in de uitgaande richting of in de inkomende richting.

Elke interface heeft acht wachtrijen op hardware vEdge-routers, genummerd van 0 tot 7. Wachtrij 0 is gereserveerd en wordt gebruikt voor zowel controle-verkeer als LLQ-verkeer (Low-Latency Wachting). Voor LLQ moet elke klasse die in kaart is gebracht om 0 ook worden geconfigureerd voor gebruik van LLQ. Al het controleverkeer wordt overgedragen. Er zijn wachtrijen 1 tot 7 beschikbaar voor gegevensverkeer.

Zoals geïllustreerd in Afbeelding 2., wordt het QoS-beleid toegepast op een gegevenspakket aangezien het van de ene tak naar de andere wordt verzonden:

1. Classifier Input - Het inkomende verkeer kan geclassificeerd worden door elk pakje te koppelen aan een verzendklasse. Het doorsturen van klassen groepgegevens pakketten en toewijzen pakketten aan uitvoerrijen voor transmissie naar hun bestemming, gebaseerd op de het door:sturen klasse.

2. Voer ACL’s in en definieer Policer - het maximale verkeerspercentage van verzonden of ontvangen gegevens op een interface kan worden bepaald door politiemensen te configureren en een netwerk op meerdere prioriteitsniveaus te verdelen. Toewijzers op inkomende interfaceverkeer staan u toe om middelen te besparen door verkeer te laten vallen dat niet door het netwerk hoeft te worden geleid.

3. Routeanalyse - vEdge-router controleert de lokale routeswitchtabel om te bepalen welke interface het pakket moet gebruiken om de bestemming te bereiken.

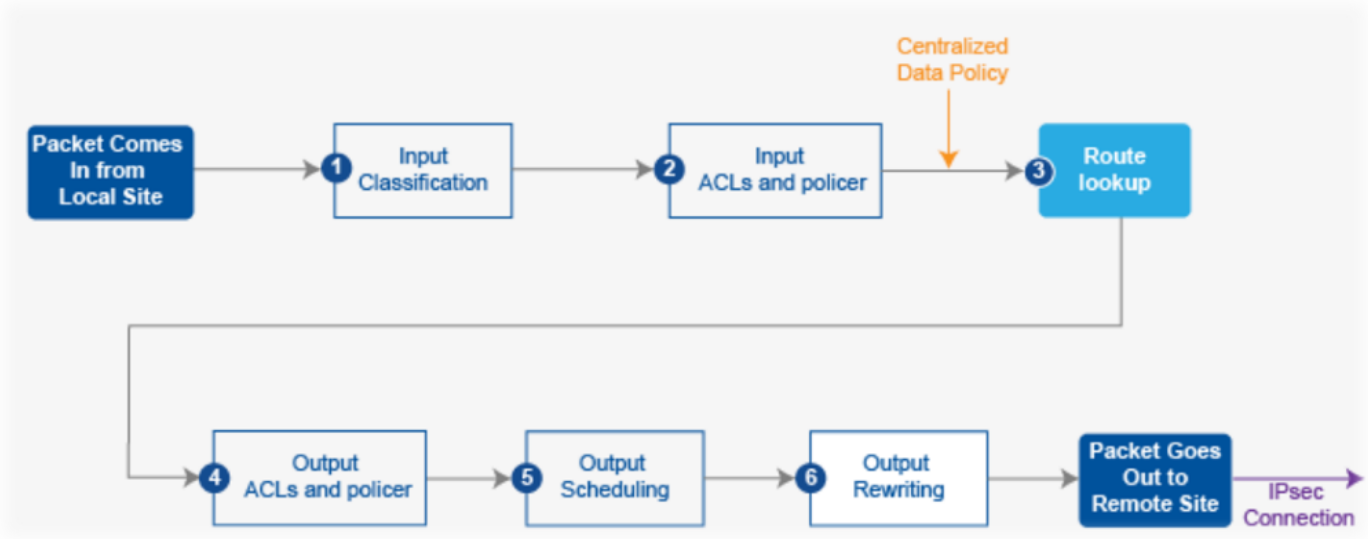
4. Uitvoer ACL's en Policer - verkeer dat conformeert aan de politieresnelheid, wordt verzonden en verkeer dat hoger is dan de politieresnelheid wordt verzonden met een lagere prioriteit of wordt gedropt. De Policers toegepast op uitgaande interface traffic control de hoeveelheid gebruikte bandbreedte.

5. Uitvoerplanning - Er kunnen prioriteiten aan de pakketten worden gesteld door een QoS-kaart te configureren voor elke uitvoerwachtrij om de bandbreedte, de grootte van de vertragingsbuffer en de prioriteit van het Packet Loss (PLP) van uitvoerwachtrijen te specificeren. Het hangt van de prioriteit van het verkeer af dat u pakketten hoger of lager bandbreedte, bufferniveaus, en dalprofielen kunt toewijzen.

6. Uitvoer herschrijven - Als u regels herschrijft, kunt u het verkeer in kaart brengen om punten te coderen wanneer het verkeer in het systeem is afgelopen. Defineer herschrijfregel om het DSCP-veld van de buitenste IP-kop te overschrijven. Pas de herschrijfregel op de uitgaande (spanning)interface toe.

QoS-beleid configureren

In deze stappen wordt de configuratie van het gelokaliseerde gegevensbeleid (QoS) beschreven:



Stap 1. Configuratie van de expediteurenklassen en de omzetting in uitvoerrijen. Defineer **class map** om pakketten, door belangrijkheid, in aangewezen expediteurenklassen te classificeren. Raadpleeg de **class map** in een toegangslijst.

```
policy

 class-map

 class best-effort queue 3

 class bulk-data queue 2

 class critical-data queue 1

 class voice queue 0
```

Stap 2. Configureer de QoS planner-klassen. Defineer **qos planner** en specificeer de snelheid waarmee verkeer op de interface wordt verzonden. Raadpleeg de politie in een toegangslijst.

```
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
```

Stap 3. QoS-planners van groepen en definiëren QoS-kaart:

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

Stap 4. Pas de QoS-kaart op de spanning-interface toe:

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

Stap 5. Defineer een toegangslijst om gegevenspakketten in de juiste categorieën te classificeren:

```
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
```

Stap 6. Pas de toegangslijst op een interface toe:

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

Gerelateerde informatie

Ideale vereisten voor een gegarandeerde QoS met SD-WAN:

Het is makkelijk te begrijpen waarom deze oplossing als een oplossing de traditionele MPLS WAN's daarbuiten bedreigt aangezien Cisco SD-WAN QoS-oplossing de QoS-niveaus kan leveren die via het internet overeenkomen met het gebruik van dynamische methoden. Cisco SD-WAN selecteert dynamisch de meest kosteneffectieve assortiment van particuliere verbindingen en openbare internetverbindingen. Met SD-WAN zijn de toepassingen niet gelijk aan de standaardbandbreedte, maar in plaats daarvan wordt de verbinding die het meest van toepassing is op elke app geselecteerd.

Ongeacht of MPLS of SD-WAN de beste oplossing is, is het belangrijk om op te merken dat QoS met SD-WAN zonder MPLS met een symmetrisch internet zonder pakketverlies met VPN kan worden bereikt. Als het verkeer via meerdere sprongen via meerdere ISP's overstapt, kan een bedrijf niet garanderen hoe missie-kritieke en vertragingsgevoelige services zullen uitvoeren. De SD-WAN producten hebben actieve configuraties nodig om de betrouwbaarheid en QoS van WAN te verbeteren.

In het kort: SD-WAN is een fantastische technologie die in de toekomst de afhankelijkheid van MPLS-netwerken vermindert. U kunt een deel van het niet-interactieve verkeer offload naar een breedbandinternetverbinding. SD-WAN kan bijvoorbeeld letselgevoelig verkeer zoals spraak via een MPLS-link, die QoS garandeert, en al het andere via een breedbandinternetverbinding routeren of twee breedbandverbindingen combineren om MPLS aan te passen.