Implémenter la QoS dans Cisco SD-WAN

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Problème](#)

[Solution](#)

[Configuration et implémentation de la qualité de service Cisco SD-WAN](#)

[Configurer la stratégie QoS](#)

[Informations connexes](#)

Introduction

Ce document décrit l'approche de Cisco-Viptela afin de mettre en oeuvre la qualité de service (QoS) avec le WAN défini par logiciel (SD-WAN). SD-WAN est l'innovation la plus récente afin de s'intégrer avec les entreprises, les entreprises et les organisations à travers le monde. La nouvelle vague de technologies SD-WAN permet aux gouvernements et aux entreprises de fournir une prise en charge des applications critiques sans contraintes supplémentaires. Bien que le cloud ait considérablement simplifié le processus de provisionnement des capacités, il présente de nouveaux défis en matière de gestion de la qualité de service. Le nouveau SD-WAN doit correspondre aux niveaux de performances, de fiabilité et de disponibilité offerts par une application et par la plate-forme ou l'infrastructure qui l'héberge.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solution SD-WAN
- Structure de la QoS et des politiques traditionnelles

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Périphériques matériels Cisco vEdge

- Logiciel Cisco vEdge (VM)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

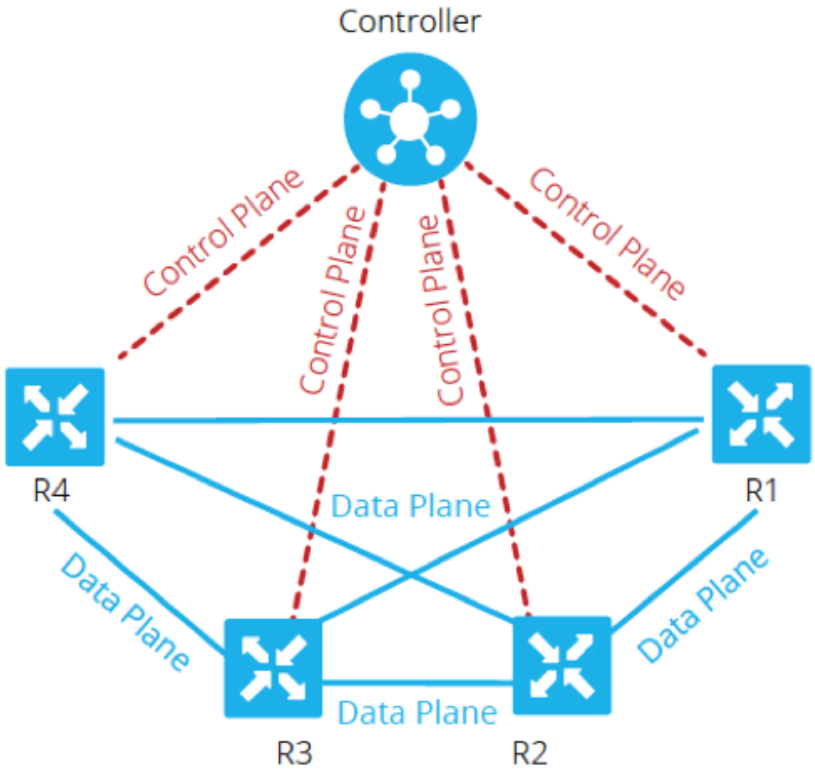
Jusqu’à récemment, les réseaux étaient strictement construits sur la base de la configuration des réseaux de transmission sous-jacents. Certaines solutions, telles que l'ingénierie de trafic MPLS (Multiprotocol Label Switching), ont influencé la sélection du chemin entre les noeuds, mais chaque périphérique, de la source à la destination, devait être programmé afin d'autoriser ou de refuser le trafic qui circule entre deux points d'extrémité et de prendre des décisions complètement autonomes.

Les services d’opérateur traditionnels comme un VPN IP ou un MPLS ont été considérés par beaucoup comme la seule manière de fournir de manière fiable les services QoS pour une organisation. Le principal inconvénient du MPLS est le coût de la bande passante. Les consommateurs d'aujourd'hui sont de plus en plus intéressés par les contenus multimédias monopolisant la bande passante, tels que les vidéos et la réalité augmentée (RA)/réalité virtuelle (VR), et par le coût élevé par mégabit que les demandes MPLS peuvent être hors de portée. Enfin, un réseau MPLS n'offre pas de protection des données intégrée et, s'il est mal implémenté, il peut ouvrir le réseau à des vulnérabilités.

En outre, du point de vue de la sécurité, le trafic MPLS n'est pas chiffré par défaut. Les réseaux MPLS offrent de nombreuses fonctionnalités de sécurité, mais leurs solutions VPN traditionnelles ne sont pas sans difficultés. Une clé pré-partagée est utilisée pour authentifier les périphériques VPN IPSec, mais afin de gérer un grand nombre de clés pré-partagées sur plusieurs périphériques ne s'adapte pas et est moins sécurisé.

Solution

D'autre part, l'approche SD-WAN utilise des contrôleurs WAN centralisés afin d'héberger et de gérer toutes les contiguïtés avec les noeuds du réseau. Elle offre une certaine souplesse dans la création et l'application des politiques. Étant donné que chaque périphérique n'est associé qu'à des contrôleurs pour les politiques de connectivité et de plan de contrôle afin de transmettre le trafic de données entre les noeuds de service, ces derniers peuvent être ajustés de manière dynamique en fonction de la visibilité globale sur les conditions du réseau. Comme illustré ici, chaque routeur annonce ses informations locales au contrôleur. Cela permet au flux de données d'être facilement manipulé par le contrôleur central avec l'utilisation de politiques appliquées à chaque routeur local.



Dans cet exemple, R1 et R4 n'ont pas de contiguïté par paires, juste le chemin du plan de données. Par conséquent, le contrôleur central contrôle et modifie facilement le flux de trafic. Par exemple, il peut contrôler tous les préfixes de R1 qui sont annoncés à R4 via R3, ou que certains préfixes sont annoncés à R4 via R3, tandis que certains sont annoncés directement à partir de R1, où R3 pourrait être un point d'application pour une stratégie de pare-feu. Cette approche réduit considérablement le volume des politiques de plan de données qui devraient être mises en oeuvre sur chaque routeur, à l'aide de topologies de réseau traditionnelles. Le SD-WAN est un réseau superposé qui peut aider les administrateurs à identifier le trafic critique et à lui accorder un traitement spécial sur l'ensemble du réseau.

Configuration et implémentation de la qualité de service Cisco SD-WAN

Dans le réseau de superposition SD-WAN, la qualité de service fonctionne lorsqu'elle examine les paquets qui entrent à la périphérie du réseau. Chaque routeur vEdge du réseau doit être configuré pour fournir la qualité de service. Une fois que le réseau de superposition SD-WAN et les connexions du plan de contrôle sont opérationnels, le trafic de données circule automatiquement sur les connexions IPsec entre les routeurs vEdge. Le flux de transfert de paquets de données par défaut peut être modifié lorsque la stratégie de données centralisée ou la stratégie de données localisée est créée et appliquée.

La politique de données centralisée permet de gérer le chemin de trafic qui est routé à travers le réseau et le trafic peut être contrôlé (autorisé ou bloqué) en fonction des champs d'adresse, de port et de DSCP (Differentiated Services Code Point) dans l'en-tête IP du paquet.

La politique de données localisées peut contrôler le flux du trafic de données entrant et sortant des interfaces d'un routeur vEdge et permet des fonctionnalités telles que la QoS. Les stratégies peuvent être activées si vous appliquez les listes d'accès, soit dans la direction sortante, soit dans la direction entrante.

Chaque interface comporte huit files d'attente sur les routeurs vEdge matériels, numérotées de 0 à 7. La file d'attente 0 est réservée et est utilisée à la fois pour le trafic de contrôle et pour le trafic LLQ (Low-Latency Queuing). Pour LLQ, toute classe mappée à la file d'attente 0 doit également être configurée pour utiliser LLQ. Tout le trafic de contrôle est transmis. Les files d'attente 1 à 7 sont disponibles pour le trafic de données.

Comme l'illustre l'image 2, les stratégies QoS sont appliquées à un paquet de données lorsqu'il est transmis d'une branche à l'autre :

1. Classification des entrées : le trafic entrant peut être classé en associant chaque paquet à une classe de transfert. Les classes de transfert regroupent les paquets de données et les attribuent aux files d'attente de sortie pour les transmettre à leur destination, en fonction de la classe de transfert.

2. Listes de contrôle d'accès d'entrée et définition d'un régulateur : le débit de trafic maximal des données envoyées ou reçues sur une interface peut être contrôlé en configurant des régulateurs et en partitionnant un réseau en plusieurs niveaux de priorité. Les contrôleurs appliqués au trafic d'interface entrant vous permettent d'économiser des ressources en abandonnant le trafic qui n'a pas besoin d'être routé via le réseau.

3. Recherche de route : le routeur vEdge vérifie la table de route locale afin de déterminer l'interface que le paquet doit utiliser pour atteindre sa destination.

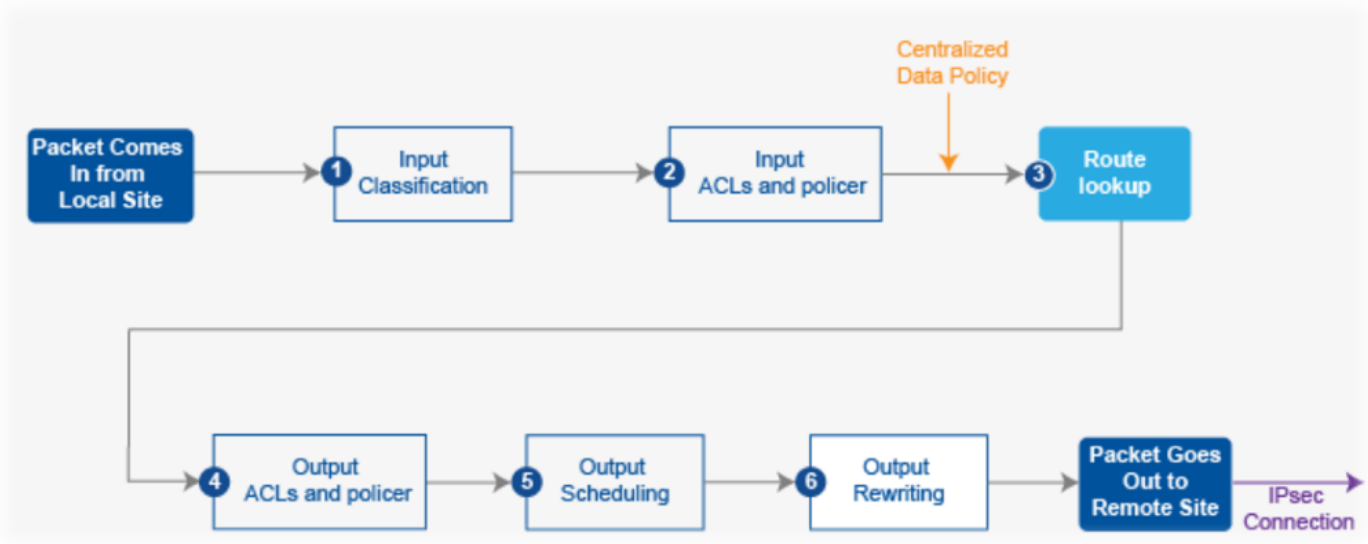
4. Listes de contrôle d'accès et régulateur de sortie : le trafic qui est conforme au débit du régulateur est transmis et le trafic qui dépasse le débit du régulateur est envoyé avec une priorité réduite ou est abandonné. Les régulateurs appliqués au trafic de l'interface sortante contrôlent la quantité de bande passante utilisée.

5. Planification des sorties : les paquets peuvent être classés par ordre de priorité en configurant une carte QoS pour chaque file d'attente de sortie afin de spécifier la bande passante, la taille du tampon de délai et la priorité de perte de paquets (PLP) des files d'attente de sortie. Cela dépend de la priorité du trafic que vous pouvez attribuer aux paquets une bande passante supérieure ou inférieure, des niveaux de mémoire tampon et des profils d'abandon.

6. Sortie de réécriture - Si vous réécrivez des règles, il vous permet de mapper le trafic afin de coder des points quand le trafic sort dans le système. Définissez la règle de réécriture pour remplacer le champ DSCP de l'en-tête IP externe. Appliquez la règle de réécriture à l'interface de sortie.

Configurer la stratégie QoS

Les étapes suivantes décrivent la configuration de la stratégie de données localisées (QoS) :



Étape 1 : configuration des classes de transfert et du mappage aux files d'attente de sortie Définissez la carte de classe afin de classer les paquets, par importance, en classes de transmission appropriées. Référez-vous à la carte de classe dans une liste d'accès.

```
policy
 class-map
  class best-effort queue 3
  class bulk-data queue 2
  class critical-data queue 1
  class voice queue 0
```

Étape 2 : configuration des classes de transfert du planificateur QoS Définissez le planificateur Qos et spécifiez le débit auquel le trafic est envoyé sur l'interface. Reportez-vous au contrôleur d'une liste d'accès.

```
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
```

Étape 3. Regroupez les planificateurs QoS et définissez la correspondance QoS :

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

```
  qos-scheduler voice-scheduler
```

Étape 4. Application de la carte QoS à l'interface de sortie :

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

Étape 5. Définition d'une liste d'accès afin de classer les paquets de données dans les classes de transfert appropriées :

```
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
```

Étape 6. Application de la liste d’accès à une interface :

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

Informations connexes

Exigences idéales pour obtenir une qualité de service garantie avec SD-WAN :

Il est facile de comprendre pourquoi cette solution menace les WAN MPLS traditionnels, car la solution Cisco SD-WAN QoS peut fournir les niveaux de QoS qui correspondent sur Internet grâce à l'utilisation de méthodes dynamiques. Cisco SD-WAN sélectionne de manière dynamique l'assortiment le plus rentable de liaisons privées et de connexions Internet publiques. Avec le SD-WAN, les applications ne sont pas à la merci de la bande passante standard, mais la connexion la plus applicable à chaque application est sélectionnée.

Quelle que soit la meilleure solution, MPLS ou SD-WAN, il est important de noter que la QoS avec SD-WAN peut être obtenue sans MPLS avec un Internet symétrique sans perte de paquets avec VPN. Si le trafic traverse plusieurs sauts via plusieurs FAI, une entreprise ne peut pas garantir le fonctionnement des services critiques et sensibles aux retards. En fait, les produits SD-WAN ont besoin de configurations actives-actives afin d'améliorer la fiabilité et la qualité de service du WAN.

En bref, le SD-WAN est une technologie fantastique qui réduit la dépendance vis-à-vis des réseaux MPLS à l'avenir. Vous pouvez décharger une partie du trafic non interactif vers une connexion Internet haut débit. Par exemple, le SD-WAN peut acheminer le trafic sensible à la latence, tel que la voix sur une liaison MPLS, qui garantit la qualité de service (QoS), et tout le reste sur une connexion Internet haut débit, ou il peut combiner deux liaisons haut débit pour obtenir approximativement le MPLS.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.