Implémenter la QoS dans Cisco SD-WAN

Contenu

Introduction

Ce document décrit l'approche Cisco-Viptela afin de mettre en oeuvre la qualité de service (QoS) avec un WAN défini par logiciel (SD-WAN). SD-WAN est l'innovation la plus récente pour s'intégrer aux entreprises, aux entreprises et aux organisations du monde entier. La nouvelle vague de technologies SD-WAN permet aux gouvernements et aux entreprises de fournir un support d'application essentiel sans plus de tracas. Bien que le cloud ait considérablement simplifié le processus de provisionnement des capacités, il présente plusieurs défis nouveaux dans le domaine de la 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

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solution SD-WAN
- QoS traditionnelle et structure des politiques

Components Used

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

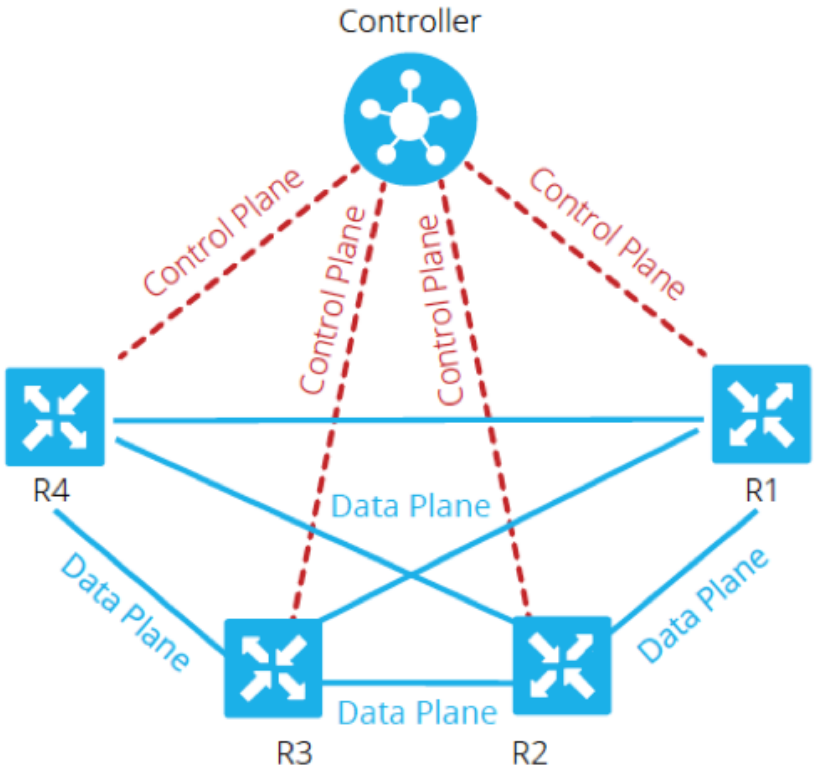
Jusqu'à récemment, les réseaux étaient strictement construits en fonction de la manière dont les réseaux de transmission sous-jacents sont. Certaines solutions, telles que MPLS (Multiprotocol Label Switching) Traffic Engineering ont influencé la sélection du chemin entre les noeuds, mais chaque périphérique 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.

De nombreux opérateurs ont considéré que les services d'opérateur traditionnels tels qu'un VPN IP ou MPLS étaient le seul moyen de fournir les services QoS de manière fiable à une entreprise. Le principal inconvénient de MPLS est le coût de la bande passante. Aujourd'hui, les consommateurs s'intéressent de plus en plus aux contenus multimédias à bande passante encombrante, tels que les vidéos et la réalité augmentée (AR)/réalité virtuelle (VR), et au coût élevé par mégabit que les demandes MPLS peuvent être hors de portée. Enfin, un réseau MPLS n'offre pas de protection intégrée des données et, s'il est mal mis en oeuvre, il peut ouvrir le réseau à des vulnérabilités.

De plus, du point de vue de la sécurité, le trafic MPLS n'est pas chiffré par défaut. Les réseaux MPLS offrent de nombreuses fonctions 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 pour gérer un grand nombre de clés pré-partagées sur plusieurs périphériques, elle n'évolue pas et est moins sécurisée.

Solution

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



Dans cet exemple, R1 et R4 n'ont pas de contiguïté par paire, 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 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 doivent être mises en oeuvre sur chaque routeur, grâce à l'utilisation de topologies de réseau traditionnelles. SD-WAN est un réseau de superposition qui peut aider les administrateurs à identifier le trafic critique et à lui accorder un traitement spécial sur l'ensemble du réseau.

Configuration et mise en oeuvre de la QoS Cisco SD-WAN

Dans le réseau de superposition SD-WAN, la QoS fonctionne lorsqu'elle examine les paquets qui entrent à la périphérie du réseau. Chacun des routeurs vEdge du réseau doit être configuré pour provisionner la qualité de service. Une fois que le réseau de superposition SD-WAN et les connexions du plan de contrôle sont en cours d'exécution, 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 lors de la création et de l'application d'une stratégie de données centralisée ou localisée.

La stratégie de données centralisée permet de gérer le chemin de trafic qui est acheminé via le réseau et le trafic peut être contrôlé (autorisation ou blocage) en fonction des champs d'adresse, de port et de point de code de services différenciés (DSCP) de 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 active 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. Classify Input - Le trafic entrant peut être classifié en associant chaque paquet à une classe de transfert. Les classes de transfert regroupent les paquets de données et attribuent les paquets aux files d'attente de sortie pour transmission vers leur destination, en fonction de la classe de transfert.

2. Input ACLs and Define Policer : le débit de trafic maximal des données envoyées ou reçues sur une interface peut être contrôlé par la configuration de régulateurs et la partition d'un réseau en plusieurs niveaux de priorité. Les régulateurs appliqués au trafic d'interface entrante 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.

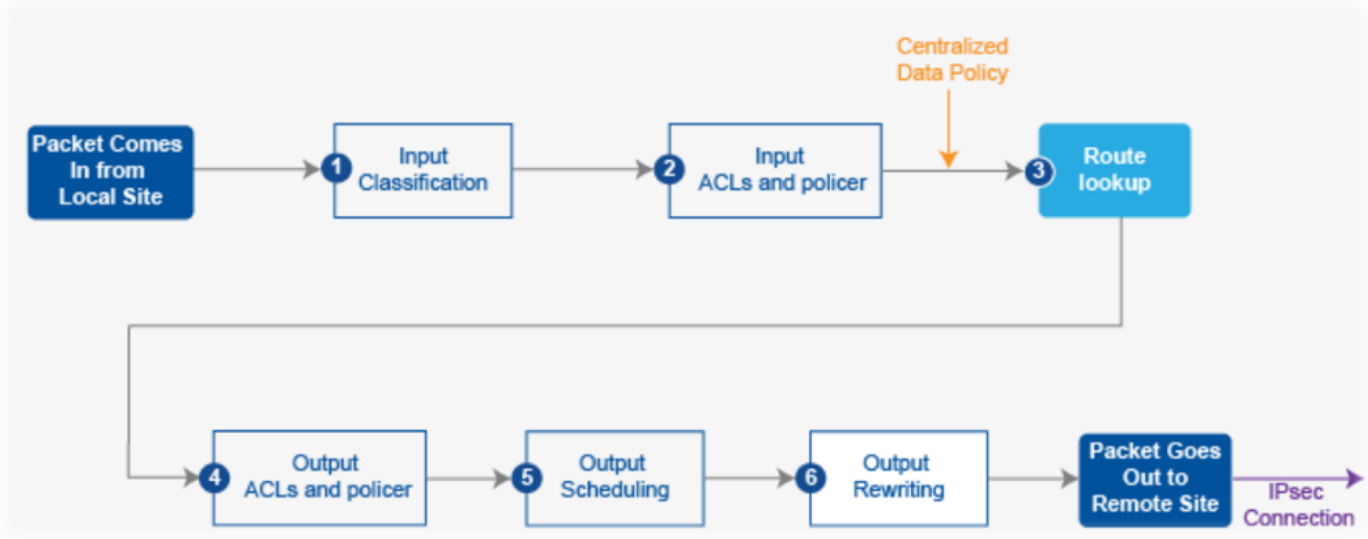
4. Listes de contrôle d'accès et régulateur de sortie : le trafic qui est conforme au débit du régulateur est transmis et le trafic qui dépasse le débit du régulateur est envoyé avec une priorité réduite ou abandonné. Les régulateurs ont appliqué au trafic d'interface sortante le contrôle de la quantité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

5. Planification des sorties : les paquets peuvent être hiérarchisés en configurant une carte QoS pour chaque file d'attente de sortie afin de spécifier la bande passante, la taille de la mémoire 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, cela vous permet de mapper le trafic afin de coder les points lorsque le trafic sort du système. Définissez la règle de réécriture pour remplacer le champ DSCP de l'en-tête IP externe. Appliquez la règle de réécriture sur l'interface sortante (sortie).

Configurer la stratégie QoS

Ces étapes décrivent la configuration de la politique de données localisées (QoS) :



Étape 1. Configurez les classes de transfert et le mappage aux files d'attente de sortie. Définissez **la carte de classe** afin de classer les paquets, par importance, en classes de transfert appropriées. Reportez-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. Configurez les classes de transfert du planificateur QoS. Définissez le **planificateur qos** et spécifiez le taux d'envoi du trafic sur l'interface. Reportez-vous au régulateur 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. Regrouper les planificateurs QoS et définir la carte QoS :

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

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

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

Étape 5. Définissez une liste d’accès afin de classer les paquets de données en 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. Appliquer la liste de contrôle d’accès à une interface :

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

Informations connexes

Exigences idéales pour obtenir une QoS garantie avec SD-WAN :

Il est facile de comprendre pourquoi cette solution constitue une menace pour les WAN MPLS traditionnels, car la solution Cisco SD-WAN QoS peut fournir les niveaux de QoS qui correspondent sur Internet avec l'utilisation de méthodes dynamiques. Cisco SD-WAN sélectionne dynamiquement l'assortiment de liaisons privées et de connexions Internet publiques le plus rentable. Avec 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.

Que MPLS ou SD-WAN soit la meilleure solution, 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 active-active afin d'améliorer la fiabilité et la qualité de service du WAN.

En bref, SD-WAN est une technologie fantastique qui réduit la dépendance future vis-à-vis des réseaux MPLS. 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, et tout le reste via une connexion Internet haut débit, ou il peut combiner deux liaisons haut débit pour approcher MPLS.