Mise en place QoS à Cisco SD-WAN

Contenu

Introduction

Ce document décrit l'approche de Cisco-Viptela afin d'implémenter le Qualité de service (QoS) avec le WAN défini par logiciel (SD-WAN). SD-WAN est l'innovation la plus récente afin d'intégrer avec les entreprises, l'entreprise, et les organismes à travers le monde. La nouvelle onde des Technologies SD-WAN permet à des gouvernements et à des entreprises pour fournir le support d'application stratégique sans tracas supplémentaire. Quoique le nuage ait considérablement simplifié le processus d'approvisionnement de capacité, il possède plusieurs défis nouveaux dans le domaine de la gestion QoS. Le nouveau SD-WAN doit apparier les niveaux de performance, la fiabilité, et la Disponibilité offerte par une application et par la plate-forme ou l'infrastructure qui la héberge.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solution SD-WAN
- Structure traditionnelle de QoS et de stratégie

Composants utilisés

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

- Périphériques matériels de vEdge de Cisco
- Logiciel de vEdge de Cisco (VM)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

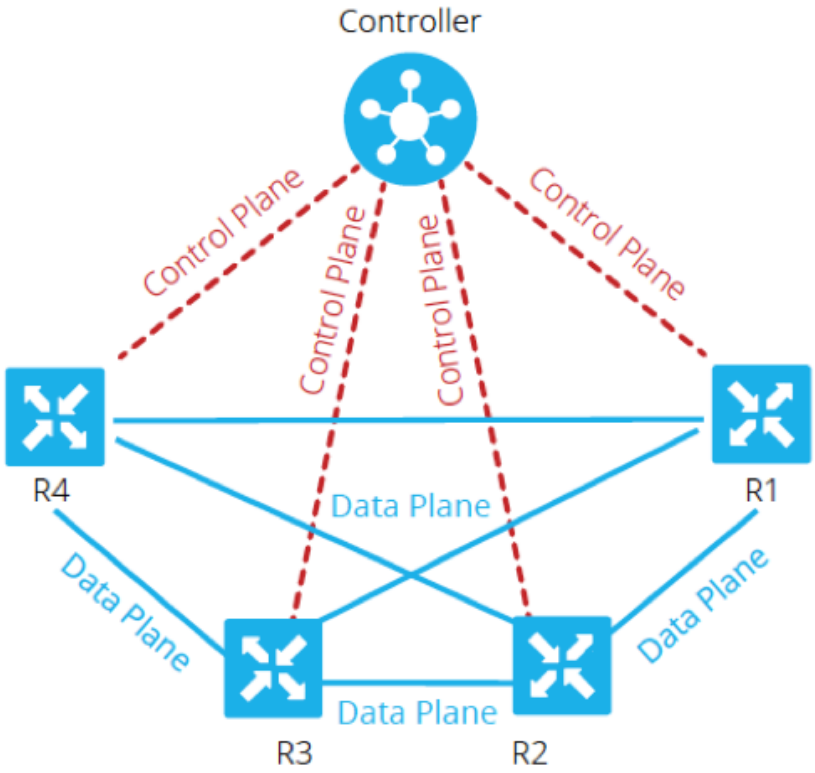
Jusque récemment, des réseaux ont été strictement établis basés sur la façon dont les réseaux sous-jacents de transmission sont. Quelques solutions, telles que l'ingénierie de trafic de Commutation multiprotocole par étiquette (MPLS) ont influencé la sélection de chemin entre les Noeuds, mais chaque périphérique de source à la destination requise pour être programmé afin de permettre ou refuser le trafic qui circule entre deux points finaux et prennent des décisions complètement autonomes.

Les opérateurs traditionnels comme un IP VPN ou MPLS ont été assumés par beaucoup pour être la seule manière de fournir sûrement les services QoS pour une organisation. Le plus grand du côté incliné du MPLS est coût de bande passante. D'aujourd'hui consommateur sont de plus en plus intéressé à bande passante-accaparant contenu multimédia comme vidéo et augmenté réalité) (AR/réalité virtuelle (VR), et le par-mégabit élevé coûté que les exigences MPLS peuvent être hors de portée. En conclusion, un réseau MPLS n'offre pas la protection des données intégrée, et s'inexactement mis en application, il peut ouvrir le réseau aux vulnérabilités.

En outre, du point de vue de la sécurité, le trafic MPLS n'est pas chiffré par défaut. Les réseaux MPLS offrent beaucoup de fonctionnalités de sécurité, cependant, leurs solutions VPN traditionnelles ne sont pas sans des défis. Pré une clé partagée par - est utilisée pour authentifier des périphériques VPN IPSec, mais afin de gérer un grand nombre pré de - a partagé des clés à travers de plusieurs périphériques ne mesure pas et est moins sécurisé.

Solution

D'autre part, l'approche SD-WAN utilise les contrôleurs BLÊMES centralisés afin de héberger et gérer toutes les contiguïtés avec des Noeuds dans le réseau. Il fournit la flexibilité dans la création et l'application des stratégies. Puisque chaque périphérique scrute seulement avec des contrôleurs pour des stratégies plates de Connectivité et de contrôle afin de passer le trafic de données entre les Noeuds de service, ceux-ci peuvent être dynamiquement ajustés basés sur la visibilité globale dans des états de réseau. Comme affiché ici, chaque routeur annonce ses informations locales au contrôleur. Ceci permet le flux de données à manipuler facilement par l'unité centrale de traitement avec l'utilisation des stratégies imposées à chaque routeur local.



Dans cet exemple, R1 et R4 n'ont aucune par paires contiguïté juste le chemin de plan de données. Par conséquent, l'unité centrale de traitement facilement contrôle et modifie la circulation. Par exemple, il peut contrôler tous les préfixes de R1 qui sont annoncés à R4 par l'intermédiaire de R3, ou qui certains préfixes sont annoncé à R4 par l'intermédiaire de R3, tandis que certain sont annoncés directement de R1, où R3 pourrait être un point de demande de stratégie de Pare-feu. Cette approche réduit excessivement le volume de stratégies de plan de données qui devraient être mises en application à chaque routeur, avec l'utilisation des topologies traditionnelles de réseau. SD-WAN est un réseau de substitution qui peut aider des admins pour identifier le trafic critique et pour lui donner le traitement spécial dans tout le réseau.

Configurez et implémentez Cisco SD-WAN QoS

Dans le réseau de substitution SD-WAN, le QoS fonctionne quand il examine les paquets qui entrent à la périphérie du réseau. Chacun des Routeurs de vEdge dans le réseau doit être configuré pour provision QoS. Une fois le réseau de substitution SD-WAN et les connexions d'avion de contrôle sont en service, les écoulements du trafic de données automatiquement au-dessus des connexions d'IPsec entre les Routeurs de vEdge. L'écoulement par défaut d'expédition de paquet de données peut être modifié quand la stratégie centralisée de données ou la stratégie localisée de données sont créées et appliquées.

La stratégie centralisée de données donne le contrôle pour gérer le trafic-chemin qui est conduit par le réseau et le trafic peut être commandé (autorisation ou bloc) basé sur l'adresse, le port, et les gisements de Differentiated Services Code Point (DSCP) dans l'en-tête IP du paquet.

La stratégie localisée de données peut contrôler le sortir du trafic de données dans et des

interfaces d'un routeur de vEdge et active des caractéristiques telles que QoS. Les stratégies peuvent être lancées si vous appliquez les Listes d'accès, dans la direction sortante ou dans la direction d'arrivée.

Chaque interface a huit files d'attente sur des Routeurs de vEdge de matériel, numérotés de 0 7. à la file d'attente 0 est réservé et est utilisé pour le trafic de contrôle et le trafic de Fonction Low Latency Queuing (LLQ). Pour LLQ, n'importe quelle classe qui est tracée pour s'aligner 0 doit également être configurée pour utiliser LLQ. Tout le trafic de contrôle est transmis. Les files d'attente 1 7 sont disponibles pour le trafic de données.

Comme illustré dans l'image 2., les stratégies QoS sont appliquées à un paquet de données pendant qu'il est transmis d'un branchement à des autres :

1. Classifiez l'entrée - Le trafic entrant peut être classifié en associant chaque paquet avec une classe d'expédition. En expédiant des classes groupez les paquets de données et assignez les paquets aux files d'attente de sortie pour la transmission à leur destination, basées sur la classe d'expédition.

2. Entrez ACLs et définissez le régulateur - Le débit de trafic maximum d'envoyer ou des données reçues sur une interface peut être contrôlé en configurant des régulateurs, et partitionner un réseau dans des plusieurs niveaux de priorité. Les régulateurs appliqués au trafic d'arrivée d'interface te permettent pour économiser des ressources par la baisse du trafic qui n'a pas besoin d'être conduit par le réseau.

3. Recherche de route - le routeur de vEdge vérifie la table de route locale afin de déterminer quelle interface le paquet devrait employer pour atteindre sa destination.

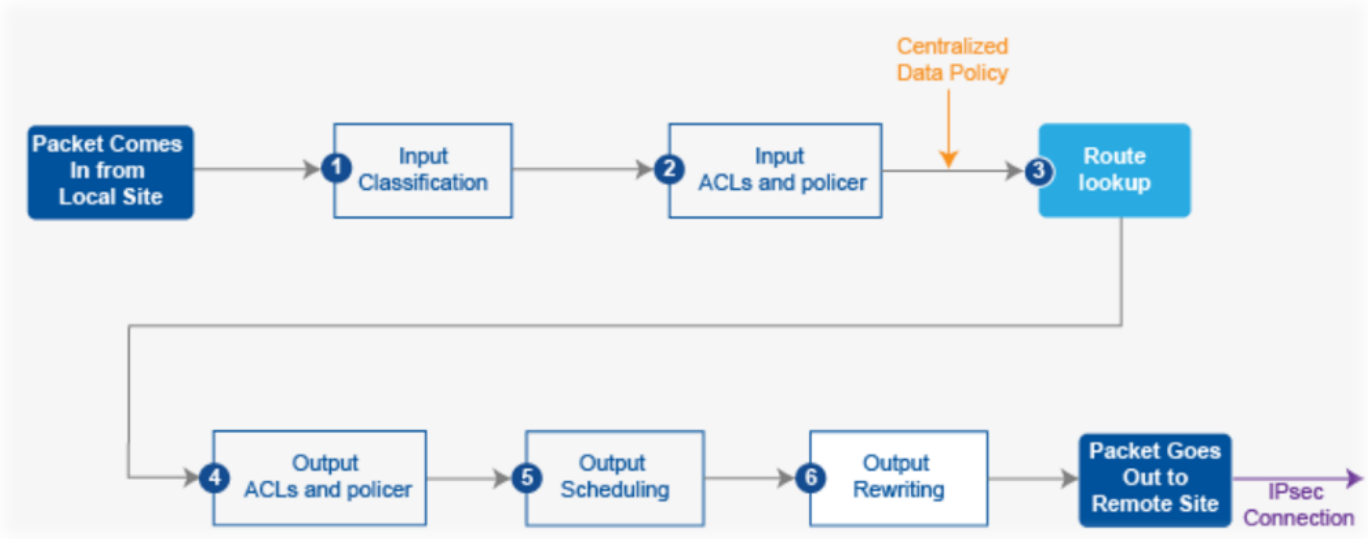
4. Sortie ACLs et régulateur - Trafiquez qui se conforme au débit de régulateur, est transmis, et trafiquez qui dépasse le débit de régulateur est envoyé avec une priorité diminuée ou est relâché. Les régulateurs ont appliqué au contrôle de trafic d'interface sortant que la quantité de bande passante l'a utilisé.

5. Planification de sortie - Les paquets peuvent être donnés la priorité en configurant une carte de QoS pour chaque file d'attente de sortie afin de spécifier la bande passante, la taille de mémoire tampon de retard, et la priorité de perte de paquets (PLP) des files d'attente de sortie. Il dépend de la priorité du trafic que vous pouvez assigner des paquets plus élevés ou la bande passante inférieure, mémoire tampon nivelle, et des profils de baisse.

6. Réécriture sortie - Si vous réécrivez des règles, elle te permet pour tracer des points de code du trafic quand les sorties de trafic dans le système. Définissez la réécriture-règle de remplacer le champ de DSCP de l'en-tête IP externe. Appliquez la réécriture-règle sur l'interface sortante (de sortie).

Configurez la stratégie QoS

Ces étapes décrivent la configuration localisée de stratégie de données (QoS) :



Étape 1. Configurez les classes et le mappage d'expédition aux files d'attente de sortie. Définissez le **class map** afin de classifier des paquets, par l'importance, dans les classes appropriées d'expédition. Référez-vous au **class map** 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 d'expédition de programmateur de QoS. Définissez le **programmateur de qos** et spécifiez le débit auquel le trafic est envoyé sur l'interface. Référez-vous au régulateur dans 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. Groupez les programmateurs de QoS et définissez la carte de 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 de QoS à l'interface de sortie :

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

Étape 5. Définissez une liste d'accès afin de classifier des paquets de données dans les classes appropriées d'expédition :

```
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. Appliquez la liste d'accès à une interface :

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

Informations connexes

Les conditions requises idéales afin de réaliser ont garanti QoS avec SD-WAN :

Il est facile de comprendre quant à pourquoi ceci car une solution menace le MPLS traditionnel WAN là pendant que la solution de Cisco SD-WAN QoS peut fournir les niveaux de QoS qui s'assortissent au-dessus de l'Internet avec l'utilisation des méthodes dynamiques. Cisco SD-WAN sélectionne dynamiquement l'assortiment le plus rentable des liens privés et des connexions Internet publiques. Avec SD-WAN, les applications ne sont pas à la merci de bande passante standard, mais à la place, la connexion qui s'applique à chaque app est sélectionnée.

Indépendamment de si le MPLS ou le SD-WAN est la meilleure solution, il est important de noter que le QoS avec SD-WAN peut être réalisé sans MPLS avec un Internet symétrique sans la perte de paquets avec le VPN. Si le trafic traverse de plusieurs sauts par l'intermédiaire des ISP de multiple, une entreprise ne peut pas garantir comment les services critiques et sensibles au retard exécuteront. Le fait est, les configurations actif-actives du besoin de Produits SD-WAN afin d'améliorer la fiabilité et le QoS du WAN.

En bref, SD-WAN est une technologie fantastique qui réduit la dépendance sur des réseaux MPLS à l'avenir. Vous pouvez débarquer une partie du trafic non-interactif à une connexion internet haut débit. Par exemple, le SD-WAN pourrait conduire le trafic sensible à la latence tel que la Voix au-dessus d'un lien MPLS, qui garantit QoS, et tout autrement au-dessus d'une connexion internet haut débit ou de lui pourrait combiner deux liens larges bandes pour rapprocher le MPLS.