Implementazione di QoS in Cisco SD-WAN

Sommario

Introduzione

Questo documento descrive l'approccio Cisco-Viptela per implementare Quality of Service (QoS) con Software Defined WAN (SD-WAN). SD-WAN è l'innovazione più recente per l'integrazione con aziende, aziende e organizzazioni di tutto il mondo. La nuova ondata di tecnologie SD-WAN consente agli enti pubblici e alle aziende di fornire supporto per applicazioni critiche senza ulteriori inconvenienti. Anche se il cloud ha notevolmente semplificato il processo di provisioning della capacità, presenta diverse nuove sfide nell'area della gestione QoS. La nuova SD-WAN deve soddisfare i livelli di prestazioni, affidabilità e disponibilità offerti da un'applicazione e dalla piattaforma o dall'infrastruttura che la ospita.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Soluzione SD-WAN
- QoS e struttura delle policy tradizionali

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Dispositivi hardware Cisco vEdge
- Software Cisco vEdge (VM)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

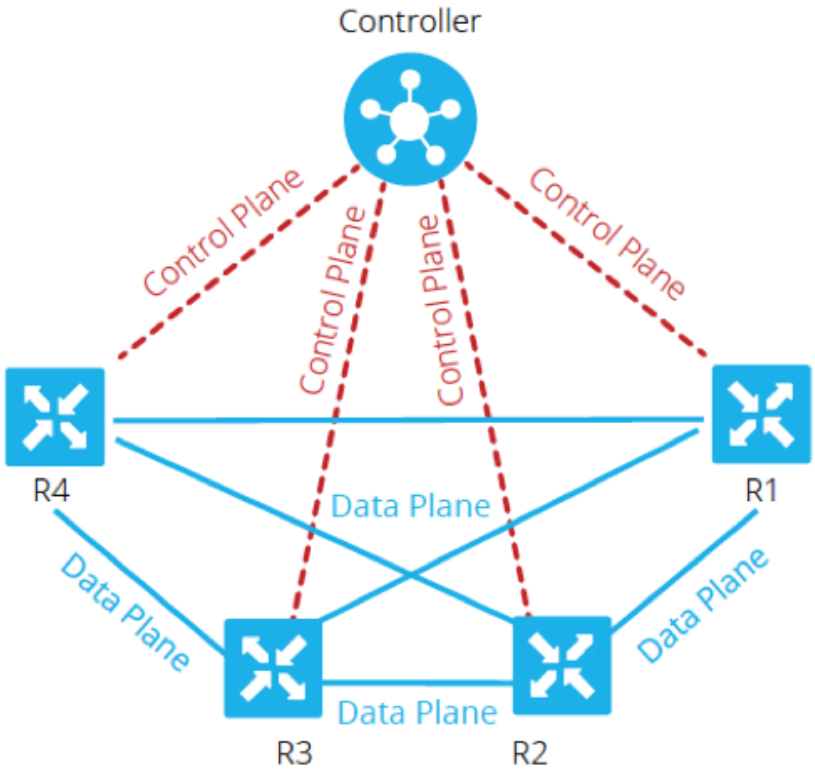
Fino a poco tempo fa, le reti erano costruite esclusivamente sulla base delle reti di trasmissione sottostanti. Alcune soluzioni, come MPLS (Multiprotocol Label Switching) Traffic Engineering, hanno influenzato la selezione dei percorsi tra i nodi, ma era necessario programmare ogni dispositivo dall'origine alla destinazione in modo da consentire o bloccare il traffico che passa tra due endpoint e prendere decisioni completamente autonome.

Molti ritengono che i servizi vettore tradizionali, come una VPN IP o MPLS, siano l'unico modo per fornire in modo affidabile i servizi QoS per un'organizzazione. Il principale svantaggio di MPLS è il costo della larghezza di banda. Gli utenti di oggi sono sempre più interessati ai contenuti multimediali che hogging la larghezza di banda, come i video e la realtà aumentata/realtà virtuale (VR), e all'elevato costo per megabit che i requisiti MPLS possono essere fuori portata. Infine, una rete MPLS non offre protezione dei dati integrata e, se implementata in modo non corretto, può aprire la rete alle vulnerabilità.

Inoltre, dal punto di vista della sicurezza, il traffico MPLS non è crittografato per impostazione predefinita. Le reti MPLS offrono molte funzioni di sicurezza, tuttavia le loro soluzioni VPN tradizionali non sono esenti da problemi. Una chiave precondivisa viene utilizzata per autenticare i dispositivi IPSec VPN, ma per gestire un numero elevato di chiavi precondivise su più dispositivi non è possibile scalare ed è meno sicura.

Soluzione

D'altra parte, l'approccio SD-WAN utilizza controller WAN centralizzati per ospitare e gestire tutte le adiacenze con i nodi della rete. Fornisce flessibilità nella creazione e nell'applicazione delle politiche. Poiché ciascun dispositivo è associato solo a controller per la connettività e policy di control plane al fine di passare il traffico di dati tra i nodi di servizio, è possibile regolarlo in modo dinamico in base alla visibilità complessiva sulle condizioni di rete. Come mostrato di seguito, ciascun router annuncia le proprie informazioni locali al controller. In questo modo il flusso di dati può essere facilmente manipolato dal controller centrale con l'utilizzo di policy applicate a ogni router locale.



In questo esempio, R1 e R4 non hanno alcuna adiacenza parallela solo al percorso del piano dati. Il controller centrale controlla e modifica facilmente il flusso del traffico. Ad esempio, può controllare tutti i prefissi da R1 annunciati a R4 tramite R3 o che alcuni prefissi sono annunciati a R4 tramite R3, mentre alcuni sono annunciati direttamente da R1, dove R3 potrebbe essere un punto di applicazione per un criterio firewall. Questo approccio riduce drasticamente il volume delle policy di pianificazione dei dati da implementare su ciascun router, utilizzando le tradizionali topologie di rete. SD-WAN è una rete overlay che può aiutare gli amministratori a identificare il traffico critico e darle un trattamento speciale in tutta la rete.

Configurazione e implementazione di QoS Cisco SD-WAN

Nella rete di overlay SD-WAN, la funzione QoS esamina i pacchetti che entrano al margine della rete. Ogni router vEdge della rete deve essere configurato per il provisioning QoS. Una volta che la rete overlay SD-WAN e le connessioni del control plane sono attive e in esecuzione, il traffico di dati passa automaticamente attraverso le connessioni IPsec tra i router vEdge. Il flusso di inoltro dei pacchetti di dati predefinito può essere modificato quando vengono creati e applicati criteri dei dati centralizzati o localizzati.

La policy dei dati centralizzati fornisce il controllo per gestire il percorso del traffico che viene instradato attraverso la rete e il traffico può essere controllato (permesso o blocco) in base all'indirizzo, alla porta e ai campi DSCP (Differentiated Services Code Point) nell'intestazione IP del pacchetto.

I criteri dei dati localizzati possono controllare il flusso del traffico di dati in entrata e in uscita dalle interfacce di un router vEdge e abilitare funzionalità quali QoS. I criteri possono essere attivati se

si applicano gli elenchi degli accessi, nella direzione in uscita o in entrata.

Ogni interfaccia dispone di otto code sui router vEdge hardware, numerate da 0 a 7. La coda 0 è riservata ed è utilizzata sia per il controllo del traffico che per il traffico LLQ (Low-Latency Queuing). Per LLQ, qualsiasi classe mappata alla coda 0 deve essere configurata per l'utilizzo di LLQ. Tutto il traffico di controllo viene trasmesso. Le code da 1 a 7 sono disponibili per il traffico di dati.

Come mostrato nell'Immagine 2., le policy QoS vengono applicate a un pacchetto dati quando viene trasmesso da una diramazione all'altra:

1. Input classificazione - Il traffico in ingresso può essere classificato associando ciascun pacchetto a una classe di inoltro. Le classi di inoltro raggruppano i pacchetti di dati e assegnano i pacchetti alle code di output per la trasmissione alla destinazione, in base alla classe di inoltro.

2. Input ACL e definizione del policer - La velocità massima del traffico di dati inviati o ricevuti su un'interfaccia può essere controllata configurando i policy e partizionando una rete in più livelli di priorità. I criteri applicati al traffico di interfaccia in entrata consentono di risparmiare risorse eliminando il traffico che non deve essere instradato attraverso la rete.

3. Ricerca route: il router vEdge controlla la tabella di route locale per determinare l'interfaccia che il pacchetto deve utilizzare per raggiungere la destinazione.

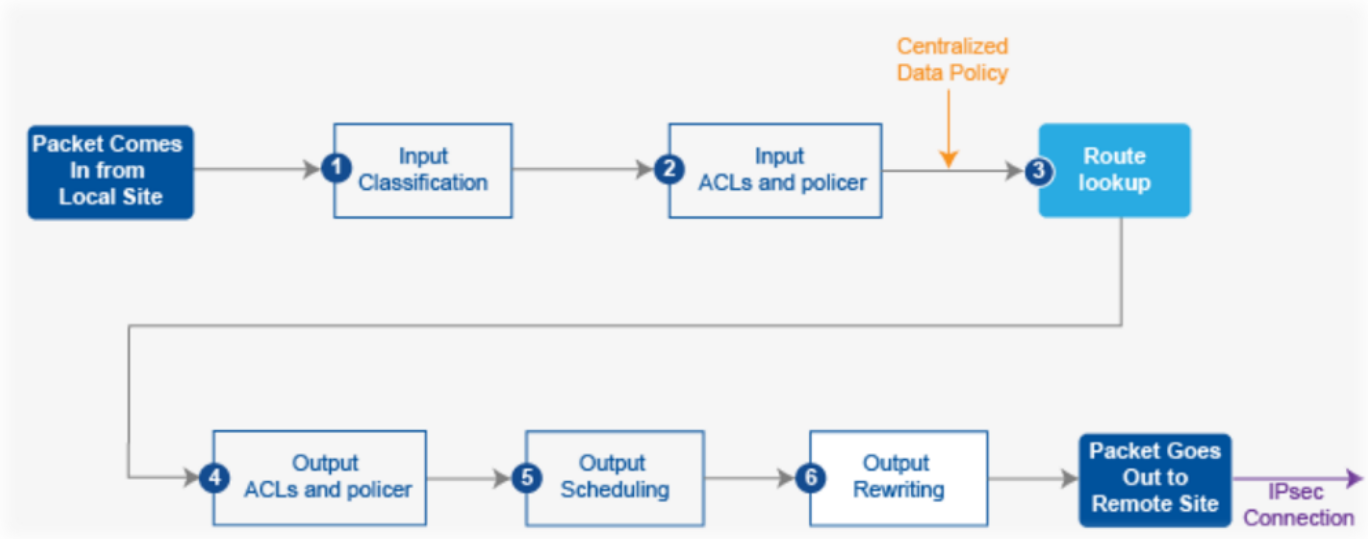
4. ACL di output e Policer: il traffico conforme alla frequenza del policer, viene trasmesso e il traffico che supera la frequenza del policer viene inviato con una priorità ridotta o viene scartato. I Policer applicati al traffico dell'interfaccia in uscita controllano la quantità di larghezza di banda utilizzata.

5. Programmazione dell'output: è possibile assegnare la priorità ai pacchetti configurando una mappa QoS per ciascuna coda di output in modo da specificare la larghezza di banda, le dimensioni del buffer di ritardo e la priorità di perdita dei pacchetti (PLP) delle code di output. Dipende dalla priorità del traffico che è possibile assegnare ai pacchetti una larghezza di banda maggiore o minore, livelli di buffer e profili di rilascio.

6. Output di riscrittura: se si riscrivono le regole, consente di mappare il traffico in modo da raggiungere i punti di codice quando il traffico esce dal sistema. Definire rewrite-rule per sovrascrivere il campo DSCP dell'intestazione IP esterna. Applicare la regola di riscrittura sull'interfaccia in uscita (in uscita).

Configura criterio QoS

La procedura seguente descrive la configurazione di QoS (Localized Data Policy):



Passaggio 1. Configurare le classi di inoltro e il mapping alle code di output. Definire la **mappa delle classi** per classificare i pacchetti, in base alla loro importanza, nelle classi di inoltro appropriate. Fare riferimento alla **mappa** delle **classi** in un elenco degli accessi.

```
policy

 class-map

 class best-effort queue 3

 class bulk-data queue 2

 class critical-data queue 1

 class voice queue 0
```

Passaggio 2. Configurare le classi di inoltro dell'utilità di pianificazione QoS. Definire l'**utilità di pianificazione qos** e specificare la velocità di invio del traffico sull'interfaccia. Fare riferimento al policer in un elenco degli accessi.

```
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
```

Passaggio 3. Raggruppare gli scheduler QoS e definire la mappa QoS:

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

Passaggio 4. Applicare la mappa QoS all'interfaccia in uscita:

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

Passaggio 5. Definire un elenco degli accessi per classificare i pacchetti di dati nelle classi di inoltro appropriate:

```
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
```

Passaggio 6. Applicare l'elenco degli accessi a un'interfaccia:

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

Informazioni correlate

Requisiti ideali per ottenere una QoS garantita con SD-WAN:

Èfacile capire perché questa soluzione rappresenti una minaccia per le tradizionali WAN MPLS là fuori, in quanto la soluzione QoS Cisco SD-WAN può fornire i livelli QoS che corrispondono su Internet con l'uso di metodi dinamici. Cisco SD-WAN seleziona in modo dinamico l'assortimento più conveniente di collegamenti privati e connessioni Internet pubbliche. Con SD-WAN, le applicazioni non sono alla mercé della larghezza di banda standard, ma viene invece selezionata la connessione più applicabile a ciascuna applicazione.

Indipendentemente dal fatto che MPLS o SD-WAN sia la soluzione migliore, è importante notare che la QoS con SD-WAN può essere ottenuta senza MPLS con una connessione Internet simmetrica, senza perdita di pacchetti con VPN. Se il traffico attraversa più hop tramite più ISP, un'azienda non può garantire le prestazioni dei servizi mission critical e sensibili al ritardo. Infatti, i prodotti SD-WAN hanno bisogno di configurazioni attivo-attivo per migliorare l'affidabilità e la QoS della WAN.

In breve, SD-WAN è una tecnologia fantastica che riduce la dipendenza dalle reti MPLS in futuro. È possibile scaricare parte del traffico non interattivo su una connessione Internet a banda larga. Ad esempio, SD-WAN potrebbe indirizzare il traffico sensibile alla latenza, come la voce su un collegamento MPLS, che garantisce QoS, e tutto il resto su una connessione Internet a banda larga, oppure potrebbe combinare due collegamenti a banda larga per approssimare MPLS.