Cisco SD-WANでのQoSの実装

内容

概要

前提条件

- 要件
- 使用するコンポーネント

問題

解決方法

Cisco SD-WAN QoSの設定と実装

QoSポリシーの設定

関連情報

概要

このドキュメントでは、ソフトウェア定義型WAN(SD-WAN)でQuality of Service(QoS)を実装するためのCisco-Viptelaのアプローチについて説明します。 SD-WANは、世界中の企業、ビジネス、組織との統合を目的とした最新のイノベーションです。SD-WANテクノロジーの新しい波により、政府や企業は追加の手間をかけることなく、重要なアプリケーションサポートを提供できます。クラウドはキャパシティプロビジョニングプロセスを大幅に簡素化しましたが、QoS管理の分野でいくつかの新しい課題を抱えています。新しいSD-WANは、アプリケーションと、それをホストするプラットフォームまたはインフラストラクチャが提供するパフォーマンス、信頼性、および可用性のレベルに適合する必要があります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SD-WANソリューション
- 従来のQoSとポリシー構造

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco vEdgeハードウェアデバイス
- Cisco vEdgeソフトウェア(VM)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

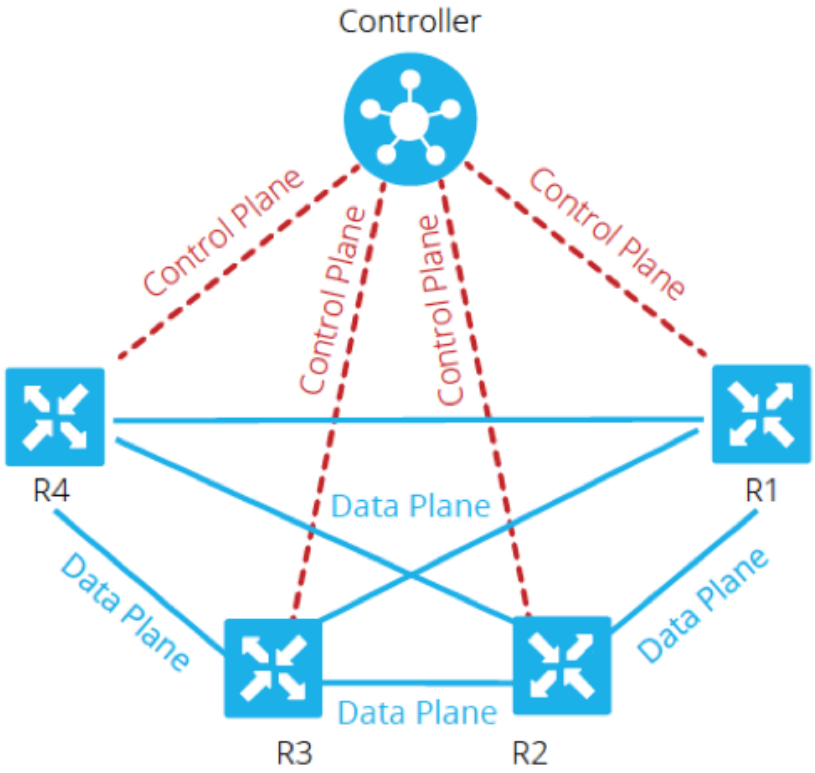
最近まで、ネットワークは基盤となる伝送ネットワークの構造に基づいて厳密に構築されていました。マルチプロトコルラベルスイッチング(MPLS)トラフィックエンジニアリングなどの一部のソリューションは、ノード間のパス選択に影響を与えましたが、送信元から宛先までのすべてのデバイスは、2つのエンドポイント間を流れるトラフィックを許可または拒否し、完全に自律的な決定を行うためにプログラムする必要がありました。

IP VPNやMPLSなどの従来のキャリアサービスは、組織にQoSサービスを確実に提供する唯一の方法であると多くの人が考えています。 MPLSの最大の欠点は帯域幅コストです。今日の消費者は、ビデオや拡張現実(AR)/仮想現実(VR)などの帯域幅を大量に消費するマルチメディアコンテンツに関心を寄せ、MPLSが要求する高いメガビットあたりのコストが手の届かないものになることに関心を寄せています。最後に、MPLSネットワークは組み込みのデータ保護機能を備えていないため、誤って実装すると、ネットワークに脆弱性が生じる可能性があります。

また、セキュリティの観点からは、MPLSトラフィックはデフォルトでは暗号化されません。MPLSネットワークは多くのセキュリティ機能を提供しますが、従来のVPNソリューションには課題があります。事前共有キーはVPN IPSecデバイスの認証に使用されますが、複数のデバイスで大量の事前共有キーを管理するには、拡張性がなく、安全性が低くなります。

解決方法

一方、SD-WANアプローチでは、中央集中型WANコントローラを使用して、ネットワーク内のノードとのすべての隣接関係をホストおよび管理します。ポリシーの作成と適用に柔軟性を提供する各デバイスは、サービスノード間でデータトラフィックを受け渡すために、接続とコントロールプレーンポリシー用のコントローラとだけピアを結ぶので、ネットワーク状態の全体的な可視性に基づいて動的に調整できます。次に示すように、各ルータはコントローラにローカル情報をアドバタイズします。これにより、各ローカルルータで適用されるポリシーを使用して、セントラルコントローラでデータフローを簡単に操作できます。



この例では、R1とR4にはデータプレーンパスのみのペアワイズ隣接関係がありません。そのため、セントラルコントローラではトラフィックフローの制御と変更が簡単に行えます。たとえば、R3を介してR4にアドバタイズされるR1のすべてのプレフィックスや、R3を介してR4にアドバタイズされるプレフィックスと、R3がファイアウォールポリシーのアプリケーションのポイントとなるR1から直接アドバタイズされるプレフィックスを制御できます。このアプローチにより、従来のネットワーキングトポロジを使用して、各ルータに実装する必要があるデータプレーンポリシーの量が大幅に削減されます。SD-WANはオーバーレイネットワークで、管理者が重要なトラフィックを特定し、ネットワーク全体で特別な扱いを行うのに役立ちます。

Cisco SD-WAN QoSの設定と実装

SD-WANオーバーレイネットワークでは、ネットワークのエッジに入ってくるパケットを調べる際にQoSが機能します。ネットワーク内の各vEdgeルータは、QoSをプロビジョニングするように設定する必要があります。 SD-WANオーバーレイネットワークとコントロールプレーン接続が稼働すると、データトラフィックはvEdgeルータ間のIPSec接続を通じて自動的に流れます。 一元化されたデータポリシーまたはローカライズされたデータポリシーを作成して適用するときに、デフォルトのデータパケット転送フローを変更できます。

中央集中型のデータポリシーにより、ネットワークを介してルーティングされるトラフィックパスを管理する制御が可能になり、パケットのIPヘッダーのアドレス、ポート、および Differentiated Services Code Point(DSCP)フィールドに基づいてトラフィックを制御（許可またはブロック）できます。

ローカライズされたデータポリシーにより、vEdgeルータのインターフェイスに出入りするデータトラフィックのフローを制御でき、QoSなどの機能が有効になります。ポリシーは、アクセスリストをアウトバウンド方向またはインバウンド方向に適用するとアクティブ化できます。

各インターフェイスには、ハードウェアvEdgeルータ上に0 ~ 7の番号の8つのキューがあります。キュー0は予約されており、制御トラフィックと低遅延キューイング(LLQ)トラフィックの両方に使用されます。LLQの場合、キュー0にマップされるクラスも、LLQを使用するように設定する必要があります。すべての制御トラフィックが送信されます。キュー1 ~ 7はデータトラフィックに使用できます。

図2.に示すように、QoSポリシーは、あるブランチから別のブランチに送信されるデータパケットに適用されます。

1. 入力の分類 – 着信トラフィックは、各パケットを転送クラスに関連付けることによって分類できます。転送クラスは、データパケットをグループ化し、転送クラスに基づいてパケットを出力キューに割り当て、宛先に送信します。

2. 入力ACLとポリサーの定義 – インターフェイス上で送受信されるデータの最大トラフィックレートは、ポリサーを設定し、ネットワークを複数のプライオリティレベルに分割することによって制御できます。着信インターフェイストラフィックに適用されるポリサーを使用すると、ネットワーク経由でルーティングする必要のないトラフィックをドロップすることで、リソースを節約できます。

3. ルートルックアップ：vEdgeルータは、パケットが宛先に到達するために使用するインターフェイスを決定するためにローカルルートテーブルを確認します。

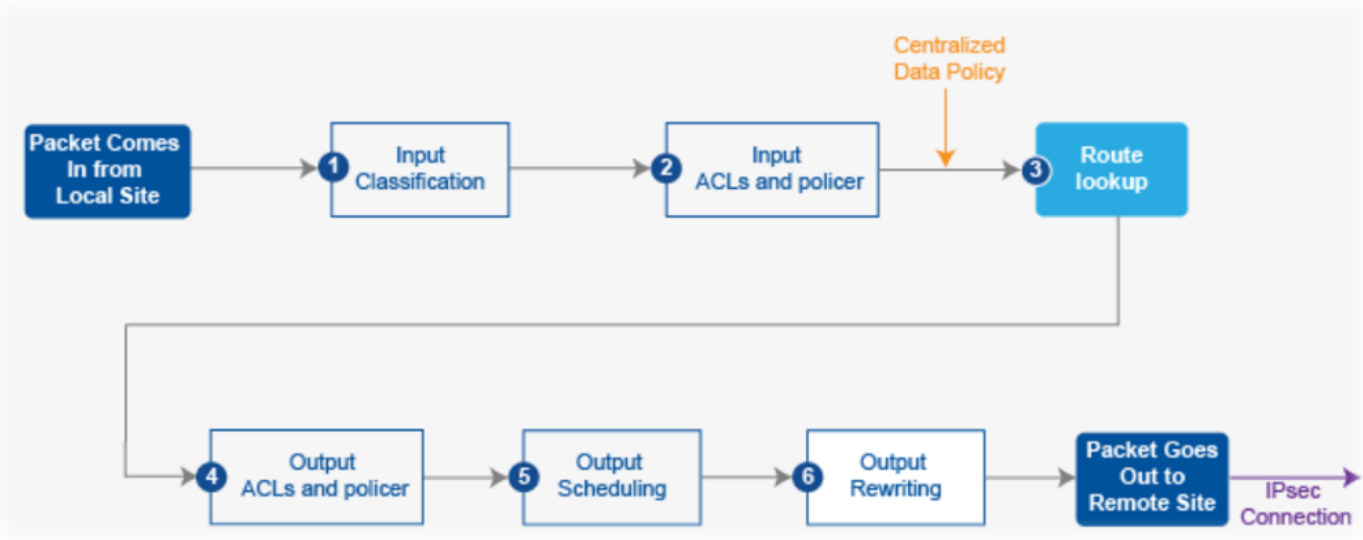
4. 出力ACLとポリサー：ポリサーレートに適合するトラフィックが送信され、ポリサーレートを超えるトラフィックは低い優先順位で送信されるか、廃棄されます。 発信インターフェイスのトラフィックに適用されるポリサーによって、使用される帯域幅の量が制御されます。

5. 出力スケジューリング：出力キューの帯域幅、遅延バッファサイズ、およびパケット損失優先順位(PLP)を指定するために、出力キューごとにQoSマップを設定することによって、パケットに優先順位を付けることができます。これは、パケットに高帯域幅または低帯域幅、バッファレベル、およびドロッププロファイルを割り当てることができるトラフィックの優先順位に依存します。

6. リライト出力：ルールを書き換えると、トラフィックがシステム内に存在するときに、トラフィックをコードポイントにマッピングすることができます。外側のIPヘッダーのDSCPフィールドを上書きするために、rewrite-ruleを定義します。アウトバウンド（出力）インターフェイスにrewrite-ruleを適用します。

QoSポリシーの設定

次の手順では、ローカライズされたデータポリシー(QoS)の設定について説明します。



ステップ 1：転送クラスと出力キューへのマッピングを設定します。パケットを重要度によって適切な転送クラスに分類するために、クラスマップを定義します。アクセスリストのクラスマップを参照してください。

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

ステップ 2：QoSスケジューラの転送クラスを設定します。qos schedulerを定義して、インターフェイスでトラフィックが送信されるレートを指定します。アクセスリストのポリサーを参照してください。

```
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
```

ステップ 3：QoSスケジューラをグループ化し、QoSマップを定義します。

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

ステップ 4：QoSマップを出力インターフェイスに適用します。

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

ステップ 5：データパケットを適切な転送クラスに分類するためのアクセスリストを定義します。

```
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
```

手順 6：アクセスリストをインターフェイスに適用します。

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

関連情報

SD-WANでQoSを保証するための理想的な要件：

Cisco SD-WAN QoSソリューションは、ダイナミックな方法を使用してインターネット上で一致

するQoSレベルを提供できるため、このソリューションが従来のMPLS WANを脅かす原因であることは容易にわかります。 Cisco SD-WANは、プライベートリンクとパブリックインターネット接続から、最もコスト効率の高い組み合わせを動的に選択します。SD-WANでは、アプリケーションは標準の帯域幅に左右されず、各アプリケーションに最も適した接続が選択されます。

MPLSまたはSD-WANのどちらが最適なソリューションかにかかわらず、SD-WANを使用したQoSは、VPNを使用したパケット損失のない対称インターネットを使用したMPLSなしで実現できることに注意することが重要です。トラフィックが複数のISPを経由して複数のホップを通過する場合、ビジネスはミッションクリティカルで遅延の影響を受けやすいサービスの動作を保証できません。実際、SD-WAN製品では、WANの信頼性とQoSを向上させるために、アクティブ – アクティブ設定が必要です。

つまり、SD-WANは、将来的にMPLSネットワークへの依存を軽減する素晴らしいテクノロジーです。一部の非インタラクティブトラフィックは、ブロードバンドインターネット接続にオフロードできます。たとえば、SD-WANは、QoSを保証するMPLSリンク経由の音声など、遅延の影響を受けやすいトラフィックをルーティングし、その他すべてをブロードバンドインターネット接続経由でルーティングする場合や、2つのブロードバンドリンクを組み合わせてMPLSに近似する場合があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。