Implementación de QoS en Cisco SD-WAN

Contenido

Introducción

Este documento describe el enfoque de Cisco-Viptela para implementar Calidad de Servicio (QoS) con WAN definida por software (SD-WAN). SD-WAN es la innovación más reciente para integrarse con empresas, empresas y organizaciones de todo el mundo. La nueva generación de tecnologías SD-WAN permite a los gobiernos y a las empresas ofrecer soporte para aplicaciones críticas sin complicaciones adicionales. Aunque la nube ha simplificado en gran medida el proceso de aprovisionamiento de capacidad, se enfrenta a varios retos novedosos en el ámbito de la gestión de QoS. La nueva SD-WAN debe coincidir con los niveles de rendimiento, fiabilidad y disponibilidad ofrecidos por una aplicación y por la plataforma o infraestructura que la aloja.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Solución SD-WAN
- Estructura de política y QoS tradicional

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivos de hardware Cisco vEdge
- Software 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 tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

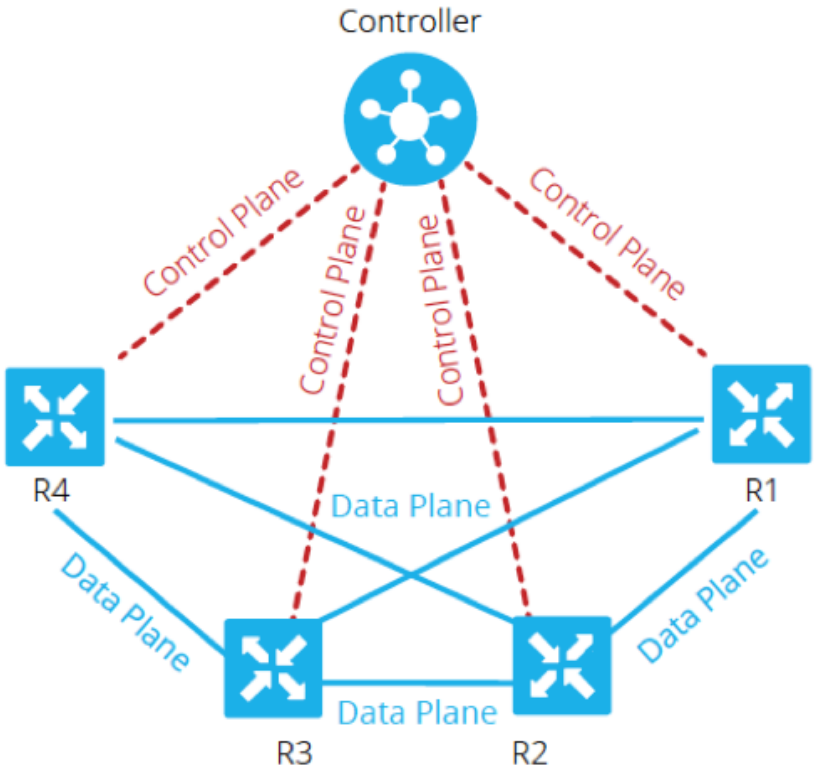
Hasta hace poco, las redes se creaban estrictamente en función de cómo se encuentran las redes de transmisión subyacentes. Algunas soluciones, como la ingeniería de tráfico de switching de etiquetas multiprotocolo (MPLS), influyeron en la selección de rutas entre nodos, pero todos los dispositivos de origen a destino debían programarse para permitir o denegar el tráfico que fluye entre dos terminales y tomar decisiones completamente autónomas.

Muchos han asumido que los servicios de portadora tradicionales, como una VPN IP o MPLS, son la única forma de ofrecer de forma fiable los servicios de QoS para una organización. El mayor inconveniente de MPLS es el coste del ancho de banda. Los consumidores de hoy en día están cada vez más interesados en contenidos multimedia que acaparan el ancho de banda, como vídeos y Realidad Aumentada (AR)/Realidad virtual (VR), y en el elevado coste por megabit que exige MPLS puede estar fuera de alcance. Por último, una red MPLS no ofrece protección de datos integrada y, si se implementa de forma incorrecta, puede abrir la red a vulnerabilidades.

Además, desde el punto de vista de la seguridad, el tráfico MPLS no se cifra de forma predeterminada. Las redes MPLS ofrecen muchas funciones de seguridad, sin embargo, sus soluciones VPN tradicionales no están exentas de retos. Se utiliza una clave previamente compartida para autenticar dispositivos IPSec VPN, pero para administrar un gran número de claves previamente compartidas en varios dispositivos no se amplía y es menos seguro.

Solución

Por otra parte, el enfoque de SD-WAN utiliza controladores WAN centralizados para alojar y administrar todas las adyacencias con nodos en la red. Proporciona flexibilidad en la creación y aplicación de políticas. Dado que cada dispositivo sólo se asocia con controladores para las políticas de conectividad y plano de control con el fin de pasar el tráfico de datos entre los nodos de servicio, estos se pueden ajustar dinámicamente en función de la visibilidad general de las condiciones de red. Como se muestra aquí, cada router anuncia su información local al controlador. Esto permite que el controlador central manipule fácilmente el flujo de datos con el uso de políticas aplicadas en cada router local.



En este ejemplo, R1 y R4 no tienen adyacencia de par solamente la trayectoria del plano de datos. Por lo tanto, el controlador central controla y modifica fácilmente el flujo de tráfico. Por ejemplo, puede controlar todos los prefijos de R1 que se anuncian a R4 a través de R3, o que ciertos prefijos se anuncian a R4 a través de R3, mientras que ciertos se anuncian directamente desde R1, donde R3 podría ser un punto de aplicación para una política de firewall. Este enfoque reduce drásticamente el volumen de políticas de plano de datos que se tendrían que implementar en cada router, con el uso de topologías de red tradicionales. SD-WAN es una red superpuesta que puede ayudar a los administradores a identificar el tráfico crítico y darle un tratamiento especial en toda la red.

Configuración e implementación de Cisco SD-WAN QoS

En la red superpuesta SD-WAN, la QoS funciona cuando examina los paquetes que entran en el borde de la red. Cada uno de los routers vEdge de la red debe configurarse para aprovisionar QoS. Una vez que la red superpuesta SD-WAN y las conexiones del plano de control están en funcionamiento, el tráfico de datos fluye automáticamente a través de las conexiones IPsec entre los routers vEdge. El flujo de reenvío de paquetes de datos predeterminado se puede modificar cuando se crean y aplican políticas de datos centralizadas o políticas de datos localizadas.

La política de datos centralizada proporciona el control para administrar la ruta de tráfico que se enruta a través de la red y el tráfico se puede controlar (permitir o bloquear) en función de los campos de dirección, puerto y punto de código de servicios diferenciados (DSCP) en el encabezado IP del paquete.

La política de datos localizada puede controlar el flujo de tráfico de datos hacia y desde las

interfaces de un router vEdge y habilita funciones como QoS. Las políticas se pueden activar si se aplican las listas de acceso, ya sea en la dirección saliente o en la dirección entrante.

Cada interfaz tiene ocho colas en los routers vEdge de hardware, numerados de 0 a 7. La cola 0 está reservada y se utiliza tanto para el tráfico de control como para el tráfico de cola de baja latencia (LLQ). Para LLQ, cualquier clase asignada a la cola 0 también debe configurarse para utilizar LLQ. Se transmite todo el tráfico de control. Las colas 1 a 7 están disponibles para el tráfico de datos.

Como se muestra en la Imagen 2., las políticas de QoS se aplican a un paquete de datos cuando se transmite de una sucursal a otra:

1. Clasificar entrada: el tráfico entrante se puede clasificar asociando cada paquete con una clase de reenvío. Las clases de reenvío agrupan paquetes de datos y asignan paquetes a colas de salida para su transmisión a su destino, según la clase de reenvío.

2. Entrada de ACL y Definición de Regulador: la velocidad máxima de tráfico de los datos enviados o recibidos en una interfaz se puede controlar mediante la configuración de reguladores y la partición de una red en varios niveles de prioridad. Los reguladores aplicados al tráfico de interfaz entrante le permiten conservar los recursos descartando el tráfico que no necesita enrutarse a través de la red.

3. Búsqueda de ruta: el router vEdge verifica la tabla de ruta local para determinar qué interfaz debe utilizar el paquete para alcanzar su destino.

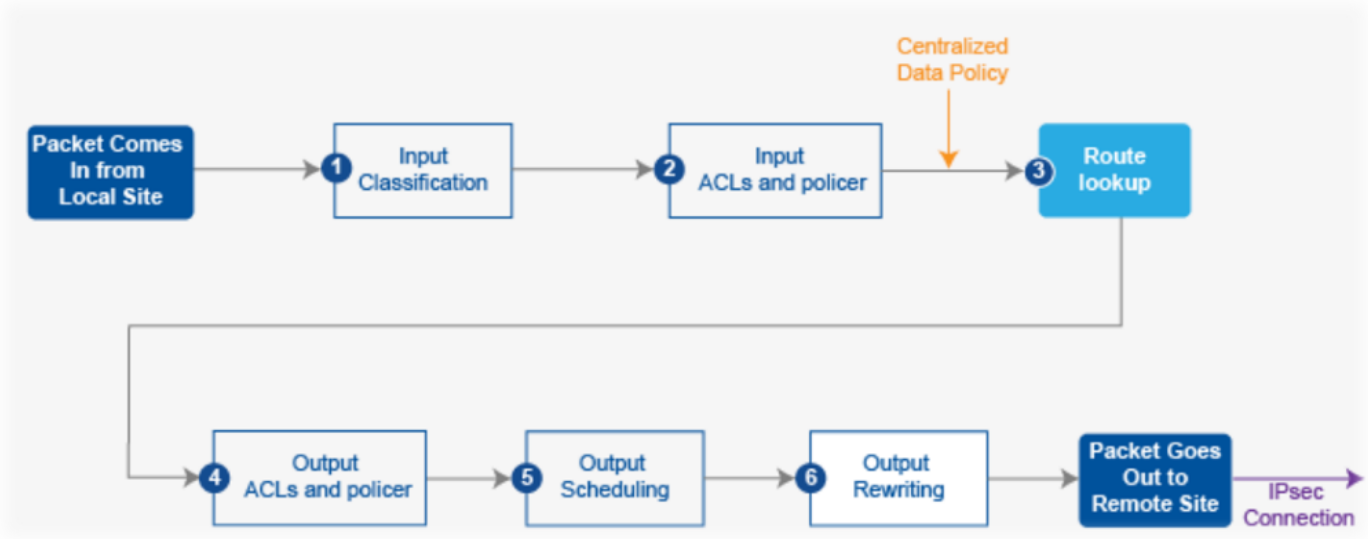
4. ACL de salida y regulador: el tráfico que se ajusta a la velocidad del regulador de tráfico, se transmite y el tráfico que excede la velocidad del regulador se envía con una prioridad reducida o se descarta. Los reguladores aplicados al tráfico de interfaz saliente controlan la cantidad de ancho de banda utilizado.

5. Programación de salida: se puede asignar prioridad a los paquetes mediante la configuración de un mapa de QoS para cada cola de salida a fin de especificar el ancho de banda, el tamaño del búfer de demora y la prioridad de pérdida de paquetes (PLP) de las colas de salida. Depende de la prioridad del tráfico que se puede asignar a los paquetes un ancho de banda mayor o menor, niveles de búfer y perfiles de descarte.

6. Rewrite Output (Reescritura de salida): Si reescribe reglas, le permite asignar tráfico para codificar puntos cuando el tráfico sale del sistema. Defina la regla de reescritura para sobrescribir el campo DSCP del encabezado IP externo. Aplique la regla de reescritura en la interfaz saliente (salida).

Configuración de la política de QoS

Estos pasos describen la configuración de la política de datos localizada (QoS):



Paso 1. Configure las clases de reenvío y la asignación a las colas de salida. Defina **mapa de clase** para clasificar los paquetes, por importancia, en clases de reenvío apropiadas. Consulte el **mapa de clase** en una lista de acceso.

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

Paso 2. Configure las clases de reenvío del planificador de QoS. Defina **qos scheduler** y especifique la velocidad a la que se envía el tráfico en la interfaz. Consulte el regulador en una lista de acceso.

```
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
```

Paso 3. Agrupe programadores de QoS y defina el mapa de QoS:

```
policy

 qos-map MyQoSMap

 qos-scheduler be-scheduler

 qos-scheduler bulk-scheduler

 qos-scheduler critical-scheduler

 qos-scheduler voice-scheduler
```

Paso 4. Aplique el mapa de QoS a la interfaz de salida:

```
interface ge0/1

 qos-map  MyQoSMap
```

Paso 5. Defina una lista de acceso para clasificar los paquetes de datos en las clases de reenvío apropiadas:

```
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
```

Paso 6. Aplique la lista de acceso a una interfaz:

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

Información Relacionada

Requisitos ideales para lograr una QoS garantizada con SD-WAN:

Es fácil entender por qué esto como solución amenaza a las WAN MPLS tradicionales, ya que la solución de QoS SD-WAN de Cisco puede ofrecer los niveles de QoS que coinciden a través de Internet con el uso de métodos dinámicos. La SD-WAN de Cisco selecciona dinámicamente la gama más rentable de enlaces privados y conexiones de Internet públicas. Con la SD-WAN, las aplicaciones no están a merced del ancho de banda estándar, sino que se selecciona la conexión más aplicable a cada aplicación.

Independientemente de si MPLS o SD-WAN son la mejor solución, es importante tener en cuenta que la QoS con SD-WAN se puede lograr sin MPLS con una Internet simétrica sin pérdida de paquetes con VPN. Si el tráfico atraviesa varios saltos a través de varios ISP, una empresa no puede garantizar el rendimiento de los servicios críticos y sensibles a los retrasos. De hecho, los productos SD-WAN necesitan configuraciones activo-activo para mejorar la fiabilidad y QoS de la WAN.

En resumen, la SD-WAN es una tecnología fantástica que reduce la dependencia de las redes MPLS en el futuro. Puede descargar parte del tráfico no interactivo a una conexión a Internet de banda ancha. Por ejemplo, la SD-WAN podría rutear el tráfico sensible a la latencia, como la voz sobre un link MPLS, que garantiza QoS, y todo lo demás a través de una conexión a Internet de banda ancha, o bien podría combinar dos links de banda ancha para MPLS aproximado.