Implementar QoS no Cisco SD-WAN

Contents

Introduction

Este documento descreve a abordagem Cisco-Viptela para implementar a Qualidade de Serviço (QoS) com a WAN definida por software (SD-WAN). A SD-WAN é a inovação mais recente para integrar empresas, empresas e organizações em todo o mundo. A nova onda de tecnologias SD-WAN permite que governos e empresas forneçam suporte essencial a aplicativos sem problemas adicionais. Embora a nuvem tenha simplificado bastante o processo de provisionamento de capacidade, ela possui vários desafios novos na área de gerenciamento de QoS. A nova SD-WAN precisa corresponder aos níveis de desempenho, confiabilidade e disponibilidade oferecidos por um aplicativo e pela plataforma ou infraestrutura que o hospeda.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Solução SD-WAN
- QoS tradicional e estrutura de política

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

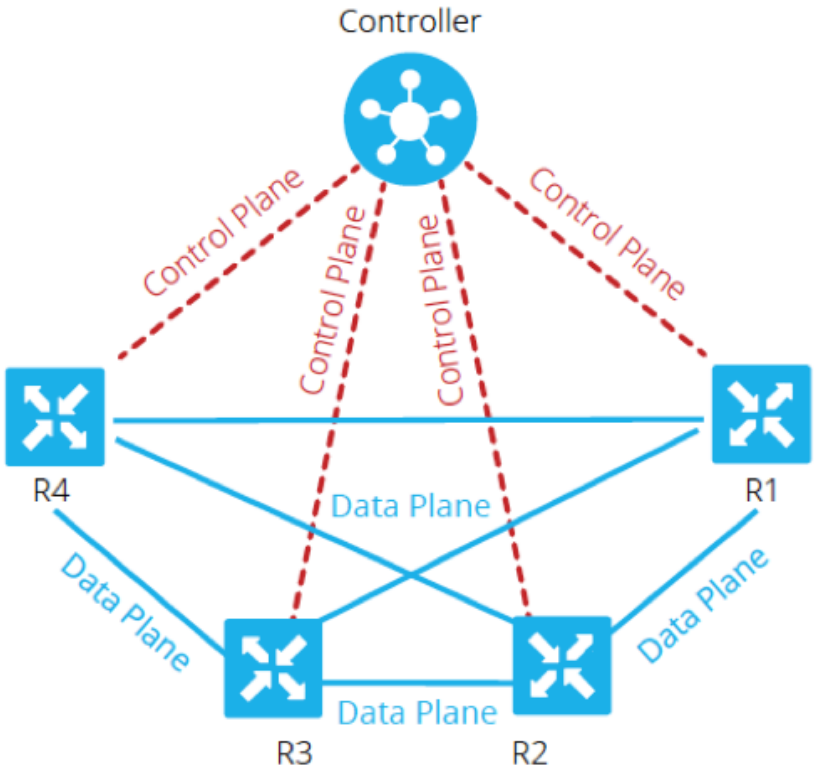
Até recentemente, as redes eram criadas estritamente com base em como as redes de transmissão subjacentes eram. Algumas soluções, como Multiprotocol Label Switching (MPLS) Traffic Engineering influenciaram a seleção de caminhos entre nós, mas cada dispositivo da origem ao destino precisava ser programado para permitir ou negar o tráfego que flui entre dois endpoints e tomar decisões completamente autônomas.

Os serviços de operadora tradicional, como VPN IP ou MPLS, foram considerados por muitos como a única forma de fornecer com segurança os serviços de QoS para uma empresa. A maior desvantagem do MPLS é o custo da largura de banda. Os consumidores de hoje estão cada vez mais interessados em conteúdo multimídia que ocupa muita largura de banda, como vídeos e realidade aumentada (AR)/realidade virtual (VR), e o alto custo por megabit que a MPLS exige pode estar fora de alcance. Finalmente, uma rede MPLS não oferece proteção de dados incorporada e, se implementada incorretamente, pode abrir a rede para vulnerabilidades.

Além disso, do ponto de vista da segurança, o tráfego MPLS não é criptografado por padrão. As redes MPLS oferecem muitos recursos de segurança, no entanto, suas soluções de VPN tradicionais não estão livres de desafios. Uma chave pré-compartilhada é usada para autenticar dispositivos VPN IPSec, mas para gerenciar um grande número de chaves pré-compartilhadas em vários dispositivos não é escalável e é menos seguro.

Solução

Por outro lado, a abordagem SD-WAN usa controladores de WAN centralizados para hospedar e gerenciar todas as adjacências com nós na rede. Proporciona flexibilidade na criação e aplicação de políticas. Como cada dispositivo é conectado somente a controladores para políticas de conectividade e plano de controle para transmitir tráfego de dados entre nós de serviço, eles podem ser ajustados dinamicamente com base na visibilidade geral das condições da rede. Como mostrado aqui, cada roteador anuncia suas informações locais ao controlador. Isso permite que o fluxo de dados seja facilmente manipulado pelo controlador central com o uso de políticas aplicadas em cada roteador local.



Neste exemplo, R1 e R4 não têm adjacência de emparelhamento apenas com o caminho do plano de dados. Portanto, o controlador central controla e modifica facilmente o fluxo de tráfego. Por exemplo, ele pode controlar todos os prefixos de R1 que são anunciados para R4 via R3 ou que certos prefixos são anunciados para R4 via R3, enquanto alguns são anunciados diretamente de R1, onde R3 pode ser um ponto de aplicação para uma política de firewall. Essa abordagem reduz drasticamente o volume de políticas de plano de dados que precisariam ser implementadas em cada roteador, com o uso de topologias de rede tradicionais. A SD-WAN é uma rede de sobreposição que pode ajudar os administradores a identificar o tráfego crítico e dar-lhe um tratamento especial em toda a rede.

Configurar e implementar o Cisco SD-WAN QoS

Na rede de sobreposição SD-WAN, a QoS funciona quando examina os pacotes que entram na borda da rede. Cada um dos roteadores vEdge na rede deve ser configurado para provisionar QoS. Quando a rede de sobreposição SD-WAN e as conexões do plano de controle estiverem ativas e em execução, o tráfego de dados fluirá automaticamente sobre as conexões IPsec entre os roteadores vEdge. O fluxo de encaminhamento de pacotes de dados padrão pode ser modificado quando a política de dados centralizada ou a política de dados localizada são criadas e aplicadas.

A política de dados centralizados fornece o controle para gerenciar o caminho de tráfego que é roteado pela rede e o tráfego pode ser controlado (permitir ou bloquear) com base nos campos endereço, porta e Ponto de Código de Serviços Diferenciados (DSCP) no cabeçalho IP do pacote.

A política de dados localizada pode controlar o fluxo de tráfego de dados para dentro e para fora

das interfaces de um roteador vEdge e habilita recursos como QoS. As políticas podem ser ativadas se você aplicar as listas de acesso, na direção de saída ou na direção de entrada.

Cada interface tem oito filas em roteadores vEdge de hardware, numeradas de 0 a 7. A fila 0 é reservada e é usada para tráfego de controle e para o tráfego de fila de baixa latência (LLQ). Para LLQ, qualquer classe que esteja mapeada para a fila 0 também deve ser configurada para usar LLQ. Todo o tráfego de controle é transmitido. As filas 1 a 7 estão disponíveis para tráfego de dados.

Como ilustrado na Imagem 2., as políticas de QoS são aplicadas a um pacote de dados à medida que ele é transmitido de uma filial para outra:

1. Classificar entrada - O tráfego de entrada pode ser classificado associando cada pacote a uma classe de encaminhamento. As classes de encaminhamento agrupam pacotes de dados e atribuem pacotes a filas de saída para transmissão ao seu destino, com base na classe de encaminhamento.

2. ACLs de entrada e definir policer - A taxa de tráfego máxima de dados enviados ou recebidos em uma interface pode ser controlada pela configuração de policers e pela partição de uma rede em vários níveis de prioridade. Os vigilantes aplicados ao tráfego da interface de entrada permitem que você conserve recursos ao descartar o tráfego que não precisa ser roteado pela rede.

3. Route Lookup - O roteador vEdge verifica a tabela de rotas locais para determinar qual interface o pacote deve usar para alcançar seu destino.

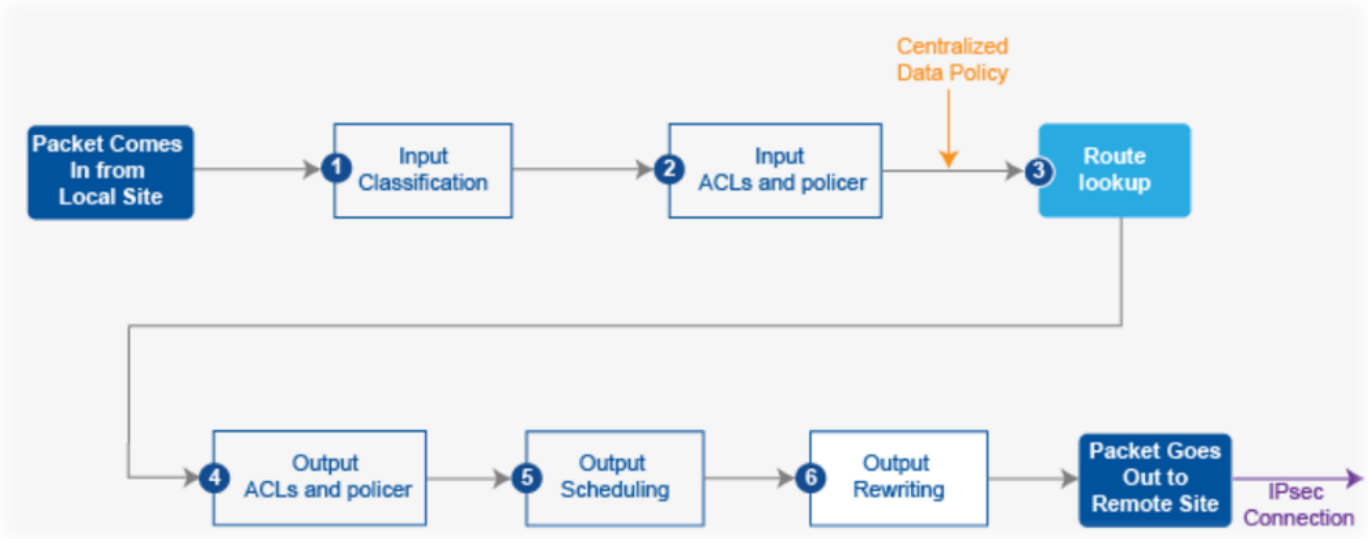
4. ACLs de saída e vigilante - o tráfego que está em conformidade com a taxa do vigilante, é transmitido e o tráfego que excede a taxa do vigilante é enviado com uma prioridade menor ou é descartado. Os vigilantes aplicados ao tráfego da interface de saída controlam a quantidade de largura de banda usada.

5. Programação de saída - Os pacotes podem ser priorizados configurando um mapa de QoS para cada fila de saída para especificar a largura de banda, o tamanho do buffer de atraso e a prioridade de perda de pacotes (PLP) das filas de saída. Depende da prioridade do tráfego que você pode atribuir aos pacotes largura de banda maior ou menor, níveis de buffer e perfis de descarte.

6. Saída de regravação - Se você regravar regras, isso permitirá mapear o tráfego para codificar pontos quando o tráfego existir no sistema. Defina rewrite-rule para substituir o campo DSCP do cabeçalho IP externo. Aplique a regra de regravação na interface de saída (saída).

Configurar política de QoS

Estas etapas descrevem a configuração da política de dados localizados (QoS):



Etapa 1. Configure as classes de encaminhamento e o mapeamento para as filas de saída. Defina o **mapa de classe** para classificar pacotes, por importância, em classes de encaminhamento apropriadas. Consulte o **mapa de classes** em uma lista de acesso.

```
policy

 class-map

 class best-effort queue 3

 class bulk-data queue 2

 class critical-data queue 1

 class voice queue 0
```

Etapa 2. Configure as classes de encaminhamento do agendador de QoS. Defina o **agendador qos** e especifique a taxa na qual o tráfego é enviado na interface. Consulte o vigilante em uma lista de acesso.

```
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
```

Etapa 3. Agendadores de QoS de grupo e mapa de QoS de definição:

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

Etapa 4. Aplique o mapa de QoS à interface de saída:

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

Etapa 5. Defina uma lista de acesso para classificar pacotes de dados em classes de encaminhamento apropriadas:

```
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
```

Etapa 6. Aplique a lista de acesso a uma interface:

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

Informações Relacionadas

Requisitos ideais para alcançar a QoS garantida com SD-WAN:

Éfácil entender por que essa solução ameaça as WANs MPLS tradicionais por aí, já que a solução QoS SD-WAN da Cisco pode fornecer os níveis de QoS que correspondem através da Internet com o uso de métodos dinâmicos. O Cisco SD-WAN seleciona dinamicamente a variedade mais econômica de links privados e conexões de Internet públicas. Com a SD-WAN, os aplicativos não estão à mercê da largura de banda padrão, mas, em vez disso, a conexão mais aplicável a cada aplicativo é selecionada.

Independentemente de o MPLS ou SD-WAN ser a melhor solução, é importante observar que o QoS com SD-WAN pode ser obtido sem o MPLS com uma Internet simétrica sem perda de pacotes com VPN. Se o tráfego atravessa vários saltos através de vários ISPs, uma empresa não pode garantir o desempenho dos serviços de missão crítica e sensíveis a atrasos. Na verdade, os produtos SD-WAN precisam de configurações ativo-ativo para melhorar a confiabilidade e a QoS da WAN.

Em resumo, a SD-WAN é uma tecnologia fantástica que reduz a dependência das redes MPLS no futuro. Você pode descarregar parte do tráfego não interativo para uma conexão de Internet de banda larga. Por exemplo, o SD-WAN pode rotear tráfego sensível à latência, como voz sobre um link MPLS, que garante QoS, e tudo mais sobre uma conexão de Internet de banda larga, ou pode combinar dois links de banda larga para MPLS aproximado.