Comparando a política baseada em classe e a taxa de acesso consolidada

Contents

Introduction

Este documento esclarece as diferenças entre a taxa de acesso comprometida (CAR), que é o recurso de vigilância de tráfego legado da Cisco, e a vigilância baseada em classe, que é o mais novo vigilante de tráfego da Cisco. O policiamento baseado em classe é implementado na interface de linha de comando (CLI - Command Line Interface) modular de Qualidade de Serviço (QoS - Quality of Service) (MQC - Quality of Service) configurando uma política de serviço. A vigilância baseada em classe, também conhecida como vigilância de tráfego, foi introduzida no Cisco IOS® Software 12.1(5)T.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

O que é um vigilante de tráfego?

A vigilância de tráfego controla a taxa máxima de tráfego enviado ou recebido em uma interface. Com base nos resultados da medição do token bucket, uma ação pode ser configurada para marcar pacotes e separar pacotes em várias classes ou níveis de serviço.

Os vigilantes de tráfego fornecem dois benefícios principais:

- **Gerenciamento de largura de banda através de limitação de taxa** - Permite controlar a taxa máxima de tráfego enviado ou recebido em uma interface. O policiamento de tráfego é frequentemente configurado em interfaces na borda de uma rede para limitar o tráfego para dentro ou para fora da rede. O tráfego que está dentro dos parâmetros de taxa é enviado, enquanto o tráfego que excede os parâmetros é descartado ou enviado com uma prioridade diferente.
- **Marcação de pacote por meio de precedência de IP, grupo QoS ou configuração de valor DSCP – A marcação de pacote permite que você particione sua rede em vários níveis de prioridade ou classes de serviço (Cós).**

Use a vigilância de tráfego para definir os valores de precedência de IP ou de DSCP (Differentiated Services Code Point, ponto de código de serviços diferenciados) para os pacotes que entram na rede. Os dispositivos de rede dentro da sua rede podem usar os valores de precedência de IP ajustados para determinar como o tráfego deve ser tratado. Por exemplo, o recurso Detecção Antecipada Aleatória Ponderada Distribuída por VIP, conforme descrito em Visão Geral da Prevenção de Congestionamento, usa os valores de precedência de IP para determinar a probabilidade de um pacote ser descartado.

Comparando CAR e políticas baseadas em classe

A Cisco recomenda o uso dos recursos modulares de QoS CLI quando possível para implementar a qualidade do serviço em sua rede. Use o policiamento baseado em classe por meio do comando police em uma política de serviço para implementar a limitação de taxa sem colocação em buffer ou enfileiramento. Evite usar CAR, para o qual não há planejamento de novos recursos ou funcionalidades. A Cisco continuará a suportar CAR para implementações existentes usando este método.

Esta tabela lista as diferenças funcionais entre a política baseada em classe e o CAR:

Função	Policer baseado em classe	CAR
Método de habilitação	Habilitado em uma política de serviço usando a MQC	Explicitamente habilitado como uma interface

Comando de configuração	**comando de vigia em MQC**	**comando rate-limit em uma interface ou subinterface**
Classificação (nas classes de tráfego)	Necessário	Não exigido. Suporta limitação de taxa por interface para todo o tráfego IP
Ações para tráfego adequado e sem adequação	Três ações: cumprir, exceder e violar	Duas ações: ação de Não violação adequada e em excesso
Método de medição de token	Token buckets separados para burst-normal e burst-max	Um único token bucket para burst-normal e burst-max
Suporte para Solicitação de Comentário (RFC - Request for Comment) 2697	Sim, a partir do software Cisco IOS versão 12.1(5)T	No

Observação: consulte a RFC 2697 e a seção Ação Violada deste documento para obter mais informações.

Critérios de correspondência

O CAR e a vigilância baseada em classe suportam diferentes valores de cabeçalho de pacote nos quais você pode corresponder para classificar seu tráfego. A correspondência de tráfego define o processo de identificação de tráfego para limitação de taxa e/ou marcação de pacote.

Valor do cabeçalho do pacote	**Nível de suporte**	
	Policer baseado em classe	**CAR**
Interface de entrada ou saída	Yes	Yes
Todo o tráfego IP ou pacotes IP que correspondem a um padrão ou a uma lista de acesso estendida	Yes	Yes
valor de precedência de IP	Yes	Yes
DSCP	Yes	—
ID de grupo QoS	Yes	Yes
Endereço MAC	Yes	Yes

Números de porta do Protocolo de Tempo Real (RTP - Real-Time Protocol) IP	Yes	—
Valor de CoS da camada 2	Yes	—
Mapas de classe predefinidos	Yes	—
Valor experimental de MPLS	Yes	—
Protocolos de reconhecimento de aplicativos (NBAR) baseados em rede	Yes	—

Ações de conformação e exceção

Esta tabela lista as ações suportadas para tráfego em conformidade e não em conformidade para cada mecanismo de vigilância de tráfego.

Ação	Nível de suporte	
	Policer baseado em classe	CAR
continuar	—	Yes
queda	Yes	Yes
set-clp-transmit	Yes	Yes
set-dscp-continue	—	Yes
set-dscp-transmit	Yes	Yes
set-frde-transmit	Yes	—
set-mpls-exp-continue	—	Yes
set-mpls-exp-transmit	Yes	Yes
set-prec-continue	—	Yes
set-prec-transmit	Yes	Yes
set-qos-continue	—	Yes
set-qos-transmit	Yes	Yes
transmit	Yes	Yes

Como ilustra a tabela acima, somente o CAR suporta a ação continuar. Essa ação configura o roteador para encaminhar o pacote para a política de taxa seguinte em uma cadeia de comandos rate-limit. O CAR e a vigilância baseada em classe usam algoritmos diferentes. A vigilância baseada em classe usa algoritmos baseados em RFCs 2697 e 2698 e não precisa de uma instrução continue. Consulte a seção a seguir para obter mais informações.

RFC 2697 e ação de violação

Ao contrário de CAR, a vigilância baseada em classe usa os algoritmos especificados nas duas seguintes RFCs:

- RFC 2697 "A Single Rate Three Color Marker" - Cisco IOS versão 12.1(5)T
- RFC 2698 "A Two Rate Three Color Marker" - Cisco IOS versão 12.2(4)T

Além disso, é importante observar que o class-policing usou dois algoritmos dependendo da

versão do Cisco IOS. O Cisco IOS Software Release 12.1(5)T introduziu um novo algoritmo e suporte para um vigilante de dois balde usando a ação de violação. O mecanismo de dois balde representa uma diferença funcional significativa entre CAR e policiamento baseado em classe.

O algoritmo de token bucket oferece aos usuários três ações para cada pacote: uma ação conforme, uma ação superior e uma ação violada. O tráfego que entra na interface com a vigilância de tráfego configurada é colocado em uma dessas categorias. Dessas três categorias, os usuários podem decidir o tratamento dos pacotes. Por exemplo, os pacotes que estão em conformidade podem ser configurados para serem transmitidos; os pacotes que excedem podem ser configurados para serem enviados com uma prioridade menor; e os pacotes que violam podem ser configurados para serem descartados.

Quando a opção de ação violada é especificada, o algoritmo token bucket usa conjuntos de token separados para a reposição e a intermitência de exceder. O exemplo a seguir usa o algoritmo token bucket com dois token buckets.

```
policy-map POLICE
  class twobucket
   police 8000 1000 1000 conform-action transmit exceed-action
   set-dscp-transmit 4 violate-action drop

 interface fastethernet 0/0
  service-policy output POLICE
```

Consulte a seção Visão geral do recurso em Política de tráfego para obter mais informações sobre como configurar a ação violada.

Informações Relacionadas

- Vigilância baseada em classe
- página de suporte de QoS
- Página de suporte aos protocolos de roteamento IP
- Página de Suporte do IP Routing
- Suporte Técnico - Cisco Systems