Vergleichen von Class-Based Policing und Committed Access Rate

Inhalt

Einführung

In diesem Dokument werden die Unterschiede zwischen der Committed Access Rate (CAR), der Funktion für veraltete Datenverkehrsrichtlinien von Cisco, und der klassenbasierten Richtlinienvergabe, der neueren Cisco Traffic Policer, erläutert. Class-Based Policing wird in der Modular Quality of Service (QoS)-Befehlszeilenschnittstelle (CLI) (MQC) implementiert, indem eine Dienstrichtlinie konfiguriert wird. Die klassenbasierte Richtlinienvergabe, auch als Datenverkehrsüberwachung bezeichnet, wurde in der Cisco IOS® Software 12.1(5)T eingeführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

Was ist ein Traffic Policer?

Die Traffic Policing steuert die maximale Übertragungsrate des an einer Schnittstelle gesendeten oder empfangenen Datenverkehrs. Basierend auf den Ergebnissen der Token-Bucket-Messung kann eine Aktion so konfiguriert werden, dass Pakete und Pakete in mehrere Klassen oder Servicelevel unterteilt werden.

Die Überwachung des Datenverkehrs bietet zwei wesentliche Vorteile:

- **Bandbreitenverwaltung durch Ratenbegrenzung** - Ermöglicht Ihnen die Steuerung der maximalen Datenverkehrsrate, die über eine Schnittstelle gesendet oder empfangen wird. Die Datenverkehrsüberwachung wird häufig an Schnittstellen am Netzwerk-Edge konfiguriert, um den ein- oder ausgehenden Datenverkehr des Netzwerks zu beschränken. Datenverkehr, der unter die Übertragungsratenparameter fällt, wird gesendet, während Datenverkehr, der die Parameter überschreitet, verworfen oder mit einer anderen Priorität gesendet wird.
- **Paketkennzeichnung über IP-Rangfolge, QoS-Gruppe oder DSCP-Wertanlage** - Mit der Paketkennzeichnung können Sie Ihr Netzwerk in mehrere Prioritätsstufen oder Serviceklassen (Classes of Service, CoS) unterteilen.

Mithilfe der Datenverkehrsüberwachung können Sie die IP-Rangfolge oder DSCP-Werte (Differentiated Services Code Point) für Pakete festlegen, die in das Netzwerk eingehen. Netzwerkgeräte innerhalb Ihres Netzwerks können dann die angepassten IP-Prioritätswerte verwenden, um zu bestimmen, wie der Datenverkehr behandelt werden soll. So verwendet beispielsweise die VIP-Funktion für die VIP-verteilte weighted Random Early Detection, wie unter Übersicht über die Überlastungsvermeidung beschrieben, die IP-Rangfolgewerte, um die Wahrscheinlichkeit zu bestimmen, dass ein Paket verworfen wird.

Vergleich von CAR und Class-Based Policing

Cisco empfiehlt, die modularen QoS-CLI-Funktionen zu verwenden, wenn dies möglich ist, um Quality of Service in Ihrem Netzwerk zu implementieren. Verwenden Sie klassenbasierte Richtlinien über den Befehl "Police" in einer Dienstrichtlinie, um die Ratenbegrenzung ohne Pufferung oder Warteschlangen zu implementieren. Vermeiden Sie die Verwendung von CAR, für die keine neuen Funktionen oder Funktionen geplant sind. Cisco wird CAR auch weiterhin für bestehende Implementierungen mit dieser Methode unterstützen.

In dieser Tabelle sind die funktionalen Unterschiede zwischen der klassenbasierten Richtlinienvergabe und der CAR aufgeführt:

Funktion	Klassenbasierter Policer	AUTO
Enable-Methode	Aktiviert in einer Service-Richtlinie mithilfe von MQC	explizit auf einer Schnittstelle aktiviert

Konfigurationsbefehl	Polizeibefehl in MQC	**rate-limit-**Befehl auf einer Schnittstelle oder Subschnittstelle
Klassifizierung (in Datenverkehrsklassen)	Erforderlich	Nicht erforderlich. Unterstützt die Durchsatzratenbegrenzung pro Schnittstelle für den gesamten IP-Datenverkehr
Maßnahmen zur Einhaltung und Nichtkonformität des Datenverkehrs	Drei Aktionen: konform, übertreffen und verletzen	Zwei Aktionen: entsprechen und überschreiten *keine verletzenden Maßnahmen*
Token-Messmethode	Separate Token-Buckets für Burst-Normal und Burst-Max	Ein Token-Eimer für Burst-Normal und Burst-Max
Support für Request for Comment (RFC) 2697	Ja, ab der Cisco IOS Software-Version 12.1(5)T	Nein

Hinweis: Weitere Informationen finden Sie im Abschnitt RFC 2697 und im Abschnitt "Aktion gegen die Täuschung" dieses Dokuments.

Anpassungskriterien

CAR und Class-Based Policing unterstützen verschiedene Paket-Header-Werte, mit denen Sie den Datenverkehr klassifizieren können. Die Datenverkehrsabstimmung definiert den Prozess zur Identifizierung des Datenverkehrs zur Ratenbegrenzung und/oder Paketmarkierung.

Paketkopfwert	Support-Stufe	
	Klassenbasierter Policer	AUTO
Eingehende oder ausgehende Schnittstelle	Ja	Ja
Alle IP-Datenverkehr oder IP-Pakete, die einer Standard- oder erweiterten Zugriffsliste entsprechen	Ja	Ja
IP-Rangfolgewert	Ja	Ja
DSCP	Ja	—
QoS-Gruppen-ID	Ja	Ja
MAC-Adresse	Ja	Ja
IP Real-Time Protocol (RTP)-	Ja	—

Portnummern		
Layer-2-CoS-Wert	Ja	—
Vordefinierte Klassenzuordnungen	Ja	—
MPLS-Testwert	Ja	—
Netzwerkbasierte NBAR-Protokolle (Application Recognition)	Ja	—

Ausführen und Übertreffen von Aktionen

In dieser Tabelle sind die unterstützten Aktionen für die Übereinstimmung und Nichtkonformität des Datenverkehrs für jeden Mechanismus zur Datenverkehrsüberwachung aufgeführt.

Aktion	Support-Stufe	
	Klassenbasierter Policer	AUTO
fortfahren	—	Ja
Tropfen	Ja	Ja
Set-clp-Transmit	Ja	Ja
set-dscp-continue	—	Ja
Set-DSCP-Transmit	Ja	Ja
Set-Forde-Transmit	Ja	—
set-mpls-exp-continue	—	Ja
set-mpls-exp-übertragung	Ja	Ja
set-prec-continue	—	Ja
Set-Prec-Transmit	Ja	Ja
set-qos-continue	—	Ja
set-qos-übertragung	Ja	Ja
übertragen	Ja	Ja

Wie die obige Tabelle zeigt, unterstützt nur CAR die Aktion continue (Weiter). Durch diese Aktion wird der Router so konfiguriert, dass das Paket an die nächste Übertragungsratenrichtlinie weitergeleitet wird, die in einer Reihe von Übertragungsratenbegrenzungsbefehlen enthalten ist. CAR und klassenbasierte Richtlinienvergabe verwenden unterschiedliche Algorithmen. Die klassenbasierte Richtlinienvergabe verwendet Algorithmen, die auf den RFCs 2697 und 2698 basieren, ohne dass eine continue-Anweisung erforderlich ist. Weitere Informationen finden Sie im folgenden Abschnitt.

RFC 2697 und die Aktion "Violade"

Im Gegensatz zur CAR verwendet die klassenbasierte Richtlinienvergabe die in den beiden folgenden RFCs angegebenen Algorithmen:

- RFC 2697 "A Single Rate Three Color Marker" - Cisco IOS Release 12.1(5)T
- RFC 2698 "A Two Rate Three Color Marker" (Ein zweistufiges Drei-Farben-Marker) - Cisco IOS Release 12.2(4)T

Darüber hinaus ist zu beachten, dass für die Klassenzuweisung je nach Cisco IOS-Version zwei Algorithmen verwendet wurden. In der Cisco IOS Software, Version 12.1(5)T, wurde ein neuer Algorithmus eingeführt, und die Unterstützung für eine Zwei-Bucket-Policer wurde durch die verletzende Aktion eingeführt. Der Zwei-Bucket-Mechanismus stellt einen signifikanten funktionalen Unterschied zwischen CAR und klassenbasierter Richtlinienvergabe dar.

Der Token-Bucket-Algorithmus bietet Benutzern drei Aktionen für jedes Paket: eine konforme Aktion, eine Überschreitung der Aktion und eine verletzende Aktion. Der Datenverkehr, der in die Schnittstelle eingegeben wird, für den die Datenverkehrsrichtlinien konfiguriert wurden, wird in eine dieser Kategorien eingeordnet. Innerhalb dieser drei Kategorien können Benutzer Paketbehandlungen festlegen. Beispielsweise können konforme Pakete für die Übertragung konfiguriert werden. Größere Pakete können so konfiguriert werden, dass sie mit einer geringeren Priorität gesendet werden. und Pakete, die gegen die Richtlinien verstoßen, können so konfiguriert werden, dass sie verworfen werden.

Wenn die Option für die violate-Action angegeben ist, verwendet der Tokenbucket-Algorithmus separate Token-Buckets für die conform und die Burst für überschreiten. Im folgenden Beispiel wird der Token-Bucket-Algorithmus mit zwei Token-Buckets verwendet.

```
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
```

Weitere Informationen zur Konfiguration der Aktion finden Sie im Abschnitt Funktionsübersicht im Traffic Policing.

Zugehörige Informationen

- Klassenbasiertes Policing
- QoS-Support-Seite
- Support-Seite für IP Routed Protocols
- Support-Seite für IP-Routing
- Technischer Support - Cisco Systems