在思科ASA配置示例的QoS

目录

简介
先决条件
要求
使用的组件
背景信息
流量策略
流量整形
优先级队列
流量的QoS通过VPN通道
与IPSec VPN的QoS
在IPSec隧道的管制
与安全套接字协议层(SSL) VPN的QoS
QoS 注意事项
配置示例
VPN隧道上的VoIP流量的QoS配置示例
网络图
基于 DSCP 的 QoS 配置
基于支持 VPN 的 DSCP 的 QoS 配置
根据ACL的QoS配置
基于支持 VPN 的 ACL 的 QoS 配置
验证
show service策略police
show service策略优先级
show service策略形状
显示priority-queue统计信息
故障排除
其他信息
FAQ
当VPN通道被横断时， QoS标记保留？
相关信息

简介

本文解释服务质量(QoS)如何在思科可适应安全工具(ASA)工作并且提供几示例关于怎样为不同的方案实现它。

您在所选的网络数据流能配置在安全工具的QoS为了提供限制的速率，为各自的流和VPN通道流，为了保证所有流量获得有限带宽其公平份额。

功能集成与Cisco Bug ID CSCsk06260。

先决条件

要求

思科建议您有知识模块化策略Framwork (MPF)。

使用的组件

运行版本9.2的本文档中的信息根据ASA，但是可以使用更早版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

QoS是允许您制定优先级到互联网数据流特定类型的网络功能。互联网用户升级他们的从调制解调器的接入点到高速的宽带连接类似数字用户线路DSL和电缆，在指定时候，单个用户也许能吸收多数的可能性增加，如果不是所有，可用的带宽，因而使其他用户挨饿。为了防止任意一个用户或站点到站点连接占用的带宽超过其公平的带宽份额，QoS 提供了一种管制功能，它规定任一用户可以使用的最大带宽。

QoS 指的是在底层技术所提供的带宽有限的情况下，网络通过使用各种技术为选定的网络流量提供更好的服务以实现最佳整体服务的能力。

安全设备中 QoS 的主要目标是对选定的网络流量（包括单个数据流或 VPN 隧道数据流）提供速率限制，以确保所有流量都获得公平的有限带宽份额。可以使用多种方式定义数据流。在安全设备中，QoS 可以应用于源 IP 地址和目标 IP 地址、源端口号和目标端口号，以及 IP 报头的服务类型 (ToS) 字节的组合。

有您在ASA能实现的三QoS ：管制、Shaping和优先级队列。

流量策略

使用管制，在指定限制的流量丢弃。 管制是方式保证流量不超出该的最大速率(在位/秒)您配置，保证通信流或类不能接收整个资源。当流量超出最大速率时， ASA降低超额流量。也修正设置允许的最大的单个突发数据流。

此图表说明什么流量监管;当流量速率到达配置的最大值最大比率时，超额流量丢弃。结果显示为带有波峰和波谷的锯齿形输出速率。

此示例显示如何节流带宽到一个特定用户的1 Mbps出站方向的：

```
ciscoasa(config)# access-list WEB-LIMIT permit ip host 192.168.10.1 any
ciscoasa(config)# class-map Class-Policy
```

```
ciscoasa(config-cmap)# match access-list WEB-LIMIT
ciscoasa(config-cmap)#exit

ciscoasa(config)# policy-map POLICY-WEB
ciscoasa(config-pmap)# class Class-Policy
ciscoasa(config-pmap-c)# police output 1000000 conform-action transmit exceed-
action drop
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit

ciscoasa(config)# service-policy POLICY-WEB interface outside
```

流量整形

流量整形用于为了匹配设备和连接速度，控制包丢失、可变延迟和链路饱和，能导致抖动和延迟。 在安全工具的流量整形允许设备限制流量流。此机制缓冲在“限速”和尝试的流量发送后的流量。 Shaping不可能为流量特定类型配置。整形的流量包括从设备被发出的流量通过通过设备的，以及流量。

此图表说明什么流量整形;它在队列保留多余数据包然后安排超额于在时间的增量的最新发射。流量整形的结果是一个平滑的数据包输出速率。

> **注意**：ASA版本5505， 5510， 5520， 5540和5550只支持流量整形。多芯的型号(例如5500-X)不支持shaping。

使用流量整形，超出的流量某限制排队(缓冲)在下timeslice期间，并且发送。

如果一个上行设备强加一bottlneck给网络流量，在防火墙的流量整形是最有用的。有100个Mbit接口的好的实例是ASA，与对互联网的一上行连接通过在路由器终止的有线调制解调器或T1。流量整形允许用户配置在接口(例如外部接口的最大出站吞吐量);当链路被饱和时，防火墙传输流量在该接口外面至指定的带宽，然后尝试缓冲后的发射的额外数据流。

Shaping应用对该所有的总流量出口指定的接口;您不能选择只整形某些通信流。

> **注意**：Shaping在加密以后执行，并且不允许根据内部信息包或隧道群基本类型的优先级为VPN。

此示例配置防火墙为了整形在外部接口的所有出站流量到2 Mbps ：

```
ciscoasa(config-pmap)#policy-map qos_outside_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape average 2000000
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit

ciscoasa(config-pmap-c)# service-policy qos_outside_policy interface outside
```

优先级队列

使用优先级队列，您能安置一个特定流量等级在低延时队列(LLQ)，在标准队列前处理。

> **注意**：如果根据整形策略指定优先级流量，您不能使用内部信息包详细信息。防火墙可只执行

LLQ，不同于能提供更加复杂的队列和QoS机制的路由器(加权公平排队(WFQ)，基于类别的加权公平队列(CBWFQ)，等等)。

分层的QoS策略为用户在一个分层的方式提供一机制指定QoS策略。例如，此外，如果用户要整形在一个接口的流量和在整形的接口流量内，为VoIP流量请提供优先级队列，然后用户能在顶部指定流量整形策略和优先级队列策略根据形状策略。分层的QoS策略支持在范围被限制。允许的唯一选择是：

- 在最高级的流量整形
- 在上一层楼的优先级队列

注意：如果根据整形策略指定优先级流量，您不能使用内部信息包详细信息。防火墙可只执行LLQ，不同于能提供更加复杂的队列和QoS机制的路由器(WFQ， CBWFQ，等等)。

此示例使用分层的QoS策略为了整形在外部接口的所有出站流量到2 Mbps类似shaping示例，但是也指定有“E-F”差分服务代码点的值的语音数据包，以及安全壳SSH流量，将接收优先级。

创建在您要启用功能的接口的优先级队列：

```
ciscoasa(config)#priority-queue outsideciscoasa(config-priority-queue)#queue-limit
2048ciscoasa(config-priority-queue)#tx-ring-limit 256
```

匹配DSCP的类E-F ：

```
   ciscoasa(config)# class-map Voice
ciscoasa(config-cmap)# match dscp ef
ciscoasa(config-cmap)# exit
```

匹配端口TCP/22 SSH流量的类：

```
   ciscoasa(config)# class-map SSH
ciscoasa(config-cmap)# match port tcp eq 22
ciscoasa(config-cmap)# exit
```

应用语音和SSH流量的优先级的策略映射：

```
   ciscoasa(config)# policy-map p1_priority
ciscoasa(config-pmap)# class Voice
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# class SSH
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
```

应用shaping对所有流量和附加指定优先级的语音和SSH流量的策略映射：

```
   ciscoasa(config)# policy-map p1_shape
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape average 2000000
ciscoasa(config-pmap-c)# service-policy p1_priority
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
```

最终请附加整形策略对整形和指定优先级出站流量的接口：

```
   ciscoasa(config)# service-policy p1_shape interface outside
```

流量的QoS通过VPN通道

与IPSec VPN的QoS

根据RFC 2401原始IP报头的服务类型(ToS)位复制对加密的信息包的IP报头，以便QoS策略可以在加密以后被强制执行。这允许将用于优先级DSCP/DiffServ位任何地方在QoS策略。

在IPSec隧道的管制

管制可能为特定VPN通道也进行。为了选择修正，您使用**匹配隧道群<tunnel>** in命令您的类映射和**匹配流IP目的地地址**命令的隧道群。

```
 class-map tgroup_out
match tunnel-group ipsec-tun
match flow ip destination-address
policy-map qos
class tgroup_out
police output 1000000
```

当您使用**匹配隧道群**命令时，输入策略不此时工作;欲知更多信息，请参阅Cisco Bug ID CSCth48255。如果设法执行与匹配流IP目的地地址的输入策略，您收到此错误：

```
   police input 10000000
ERROR: Input policing cannot be done on a flow destination basis
```

输入策略不看上去此时工作，当您使用**匹配隧道群时**(Cisco Bug ID CSCth48255)。如果输入策略工作，您会需要使用类映射，不用**匹配流IP目的地地址地址**。

```
  class-map tgroup_in
match tunnel-group ipsec-tun
policy-map qos
class tgroup_in
police input 1000000
```

如果设法修正在没有**匹配IP目的地地址的**类映射的输出，您接收：

```
   police output 10000000
ERROR: tunnel-group can only be policed on a flow basis
```

执行在内在流信息的QoS与使用访问控制列表(ACL)， DSCP，等等也是可能的。由于以前被提及的bug， ACL是方式能现在执行输入策略。

> **注意**：最多64策略映射在所有平台类型可以配置。请使用在策略映射内的不同的类映射为了分段流量。

与安全套接字协议层(SSL) VPN的QoS

直到ASA版本9.2， ASA没有保留Tos位。

SSL VPN隧道不支持与此功能。欲知更多信息，请参阅Cisco Bug ID CSCsl73211。

```
   ciscoasa(config)# tunnel-group a1 type webvpn
ciscoasa(config)# tunnel-group a1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# class-map c1
ciscoasa(config-cmap)# match tunnel-group a1
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# policy-map p1
ciscoasa(config-pmap)# class c1
```

```
ciscoasa(config-pmap-c)# police output 100000
ERROR: tunnel with WEBVPN attributes doesn't support police!

ciscoasa(config-pmap-c)# no tunnel-group a1 webvpn-attributes
ciscoasa(config)# policy-map p1
ciscoasa(config-pmap)# class c1
ciscoasa(config-pmap-c)# police output 100000
ciscoasa(config-pmap-c)#
```

> **注意**：当有电话VPN的用户使用AnyConnect客户端和数据报传输传送层安全(DTL)时加密他们的电话，优先顺序化不工作，因为AnyConnect不保留在DTL封装的DSCP标志。参考的增强请求CSCtq43909关于详细信息。

QoS 注意事项

这是要考虑的一些点关于QoS。

- 它通过模块化政策架构(MPF)应用在严格或分层的方式：管制， Shaping， LLQ。

  能只影响从网络接口卡(NIC)已经通过到DP的流量(数据路径)无用与超出(他们战斗太及早发生)，除非应用在邻接设备

- 在数据包在NIC前后的输出允许和管制在输入应用。

  在您重写在输出的一个Layer2 (L2)之后地址

- 它整形所有流量的出站带宽在接口。

  有用的与有限的上行链路带宽(这样as1Gigabit以太网(GE)与10Mb调制解调器连接)不支持在高性能ASA558x型号

- 优先级队列也许使尽力而为数据流挨饿。

  不支持在10GE在ASA5580或VLAN子接口建立接口接口环大小可以为最佳性能进一步被调整

配置示例

VPN隧道上的VoIP流量的QoS配置示例

网络图

本文档使用以下网络设置：

> **注意**：请确保将 IP 电话和主机置于不同的网段（子网）中。对于良好的网络设计，建议进行这样设置。

本文档使用以下配置：

- 基于 DSCP 的 QoS 配置
- 基于支持 VPN 的 DSCP 的 QoS 配置
- 根据ACL的QoS配置
- 基于支持 VPN 的 ACL 的 QoS 配置

基于 DSCP 的 QoS 配置

```
!--- Create a class map named Voice.

ciscoasa(config)#class-map Voice


!--- Specifies the packet that matches criteria that
!--- identifies voice packets that have a DSCP value of "ef".


ciscoasa(config-cmap)#match dscp ef


!--- Create a class map named Data.


ciscoasa(config)#class-map Data


!--- Specifies the packet that matches data traffic to be passed through
!--- IPsec tunnel.


ciscoasa(config-cmap)#match tunnel-group 10.1.2.1
ciscoasa(config-cmap)#match flow ip destination-address


!--- Create a policy to be applied to a set
!--- of voice traffic.


ciscoasa(config-cmap)#policy-map Voicepolicy


!--- Specify the class name created in order to apply
!--- the action to it.


ciscoasa(config-pmap)#class Voice


!--- Strict scheduling priority for the class Voice.

ciscoasa(config-pmap-c)#priority

PIX(config-pmap-c)#class Data


!--- Apply policing to the data traffic.
```

```
ciscoasa(config-pmap-c)#police output 200000 37500



!--- Apply the policy defined to the outside interface.


ciscoasa(config-pmap-c)#service-policy Voicepolicy interface outside
ciscoasa(config)#priority-queue outside
ciscoasa(config-priority-queue)#queue-limit 2048
ciscoasa(config-priority-queue)#tx-ring-limit 256
```

注意：匹配Voip-rtp流量的DSCP值“E-F”是指加速转发。

基于支持 VPN 的 DSCP 的 QoS 配置

```
ciscoasa#show running-config
: Saved
:
ASA Version 9.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet1
nameif outside
security-level 0
ip address 10.1.4.1 255.255.255.0
!

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- This crypto ACL-permit identifies the
!--- matching traffic flows to be protected via encryption.


access-list 110 extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
access-list 110 extended permit ip 10.1.5.0 255.255.255.0 10.1.6.0 255.255.255.0

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 10.1.4.2 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
```

```
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- Configuration for IPsec policies.

crypto ipsec ikev1 transform-set myset esp-3des esp-sha-hmac
crypto map mymap 10 match address 110

!--- Sets the IP address of the remote end.

crypto map mymap 10 set peer 10.1.2.1

!--- Configures IPsec to use the transform-set
!--- "myset" defined earlier in this configuration.

crypto map mymap 10 set ikev1 transform-set myset
crypto map mymap interface outside

!--- Configuration for IKE policies

crypto ikev1 policy 10

!--- Enables the IKE policy configuration (config-isakmp)
!--- command mode, where you can specify the parameters that
!--- are used during an IKE negotiation.


authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

!--- Use this command in order to create and manage the database of
!--- connection-specific records like group name
!--- as 10.1.2.1, IPsec type as L2L, and password as
!--- pre-shared key for IPsec tunnels.

tunnel-group 10.1.2.1 type ipsec-l2l
tunnel-group 10.1.2.1 ipsec-attributes

!--- Specifies the preshared key "cisco123" which should
!--- be identical at both peers.


ikev1 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
priority-queue outside
queue-limit 2048
tx-ring-limit 256
!
class-map Voice
match dscp ef
class-map Data
match tunnel-group 10.1.2.1
match flow ip destination-address
class-map inspection_default
match default-inspection-traffic
```

```
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
policy-map Voicepolicy
class Voice
priority
class Data
police output 200000 37500
!
service-policy global_policy global
service-policy Voicepolicy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

根据ACL的QoS配置

```
!--- Permits inbound H.323 calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq h323

!--- Permits inbound Session Internet Protocol (SIP) calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq sip

!--- Permits inbound Skinny Call Control Protocol (SCCP) calls.

ciscoasa(config)#access-list 100 extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0
255.255.255.0 eq 2000

!--- Permits outbound H.323 calls.

ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq h323

!--- Permits outbound SIP calls.
```

```
ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq sip

!--- Permits outbound SCCP calls.

ciscoasa(config)#access-list 105 extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0
255.255.255.0 eq 2000

!--- Apply the ACL 100 for the inbound traffic of the outside interface.

ciscoasa(config)#access-group 100 in interface outside


!--- Create a class map named Voice-IN.

ciscoasa(config)#class-map Voice-IN

!--- Specifies the packet matching criteria which
!--- matches the traffic flow as per ACL 100.

ciscoasa(config-cmap)#match access-list 100


!--- Create a class map named Voice-OUT.

ciscoasa(config-cmap)#class-map Voice-OUT

!--- Specifies the packet matching criteria which
!--- matches the traffic flow as per ACL 105.

ciscoasa(config-cmap)#match access-list 105


!--- Create a policy to be applied to a set
!--- of Voice traffic.

ciscoasa(config-cmap)#policy-map Voicepolicy

!--- Specify the class name created in order to apply
!--- the action to it.

ciscoasa(config-pmap)#class Voice-IN
ciscoasa(config-pmap)#class Voice-OUT

!--- Strict scheduling priority for the class Voice.

ciscoasa(config-pmap-c)#priority
ciscoasa(config-pmap-c)#end
ciscoasa#configure terminal
ciscoasa(config)#priority-queue outside


!--- Apply the policy defined to the outside interface.

ciscoasa(config)#service-policy Voicepolicy interface outside
ciscoasa(config)#end
```

基于支持 VPN 的 ACL 的 QoS 配置

```
ciscoasa#show running-config
```

```
: Saved
:
ASA Version 9.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet1
nameif outside
security-level 0
ip address 10.1.4.1 255.255.255.0
!
interface GigabitEthernet2
nameif DMZ1
security-level 95
ip address 10.1.5.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- This crypto ACL-permit identifies the
!--- matching traffic flows to be protected via encryption.


access-list 110 extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
access-list 110 extended permit ip 10.1.5.0 255.255.255.0 10.1.6.0 255.255.255.0


!--- Permits inbound H.323, SIP and SCCP calls.

access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq h323
access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq sip
access-list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq 2000


!--- Permit outbound H.323, SIP and SCCP calls.

access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq h323
access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq sip
access-list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq 2000
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 100 in interface outside

route outside 0.0.0.0 0.0.0.0 10.1.4.2 1
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec ikev1 transform-set myset esp-3des esp-sha-hmac
crypto map mymap 10 match address 110
crypto map mymap 10 set peer 10.1.2.1
crypto map mymap 10 set ikev1 transform-set myset
crypto map mymap interface outside
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
tunnel-group 10.1.2.1 type ipsec-l2l
tunnel-group 10.1.2.1 ipsec-attributes
ikev1 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
priority-queue outside
!
class-map Voice-OUT
match access-list 105
class-map Voice-IN
match access-list 100
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp

!--- Inspection enabled for H.323, H.225 and H.323 RAS protocols.

inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp

!--- Inspection enabled for Skinny protocol.

inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp

!--- Inspection enabled for SIP.

inspect sip
inspect xdmcp
```

```
policy-map Voicepolicy
class Voice-IN
class Voice-OUT
priority
!
service-policy global_policy global
service-policy Voicepolicy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

注意：请使用命令查找工具(仅限注册用户)为了得到命令在此部分使用的更多信息。

验证

使用本部分可确认配置能否正常运行。

show service策略police

为了查看流量监管的QoS统计信息，以police关键字使用policy命令的show service ：

```
ciscoasa(config)# show ser
ciscoasa(config)# show service-policy police
Interface outside:
Service-policy: POLICY-WEB
Class-map: Class-Policy
Output police Interface outside:
cir 1000000 bps, bc 31250 bytes
conformed 0 packets, 0 bytes; actions: transmit
exceeded 0 packets, 0 bytes; actions: drop
conformed 0 bps, exceed 0 bps
```

show service策略优先级

为了查看执行priority命令的服务策略的统计信息，以优先级关键字使用policy命令的show service ：

```
ciscoasa# show service-policy priority
Global policy:
Service-policy: qos_outside_policy
Interface outside:
Service-policy: qos_class_policy
Class-map: voice-traffic
Priority:
Interface outside: aggregate drop 0, aggregate transmit 9383
```

show service策略形状

```
ciscoasa(config)# show service-policy shape
Interface outside:
Service-policy: qos_outside_policy
Class-map: class-default
shape (average) cir 2000000, bc 16000, be 16000
Queueing
```

```
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
```

显示priority-queue统计信息

要显示接口的优先级队列统计信息，请在特权 EXEC 模式下使用 **show priority-queue statistics** 命令。结果显示两个的统计信息尽力而为(BE)队列和LLQ。此示例显示使用**显示priority-queue statistics命令**为从外部名为的接口和命令输出。

```
ciscoasa# show priority-queue statistics outside

Priority-Queue Statistics interface outside

Queue Type = BE
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length = 0

Queue Type = LLQ
Packets Dropped = 0
Packets Transmit = 0
Packets Enqueued = 0
Current Q Length = 0
Max Q Length = 0
ciscoasa#
```

在此统计报告，行项目的含义如下：

- “被丢弃的数据包”表示在此队列丢弃了数据包的整体数量。
- “数据包平湖”表示在此队列传送数据包的整体数量。
- “被排列的数据包”表示在此队列排队了数据包的整体数量。
- “当前问长度”表示此队列的当前深度。
- “最大值问长度”表示在此队列发生的最大深度。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

故障排除

目前没有针对此配置的故障排除信息。

其他信息

这是流量整形功能介绍的一些Bug ：

Cisco Bug ID CSCsq08550	与优先级队列原因流量失败的流量整形ASA的
Cisco Bug ID CSCsx07862	与优先级队列原因信息包延迟和丢包的流量整形
Cisco Bug ID CSCsq07395	如果策略映射编辑，添加shaping服务策略出故障

FAQ

此部分提供一答案到多数常见问题之一关于在本文描述的信息。

当VPN通道被横断时， QoS标记保留？

可以。QoS标记在通道保留，当他们穿程供应商网络，如果供应商在运送中不剥离他们。

> **提示**：*参考CLI书2的*DSCP和DiffServ保存部分*：思科ASA系列防火墙CLI配置指南， 9.2*欲了解更详细的信息。

相关信息

- **思科ASA系列防火墙CLI配置指南，服务质量**
- **应用QoS策略**
- **了解不支持无客户端SSL功能VPN**
- **配置 QoS**
- **技术支持和文档 - Cisco Systems**