Cisco ASA上的QoS配置示例

目录

简介

本文档介绍服务质量(QoS)如何在思科自适应安全设备(ASA)上工作，并提供了如何针对不同场景实施服务质量(QoS)的几个示例。

您可以在安全设备上配置QoS，以便为单个流和VPN隧道流提供对选定网络流量的速率限制，以确保所有流量都获得其有限带宽的公平份额。

该功能已与思科漏洞ID CSCsk06260集成。

先决条件

要求

思科建议您了解模块化策略框架(MPF)。

使用的组件

本文档中的信息基于运行9.2版的ASA，但也可以使用早期版本。

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是一种网络功能，允许您优先处理特定类型的互联网流量。随着互联网用户将接入点从调制解调器升级到高速宽带连接(如数字用户线路(DSL)和电缆)，在任何给定时间，单个用户可能能够吸收大部分（甚至全部）可用带宽，从而导致其他用户挨饿。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。

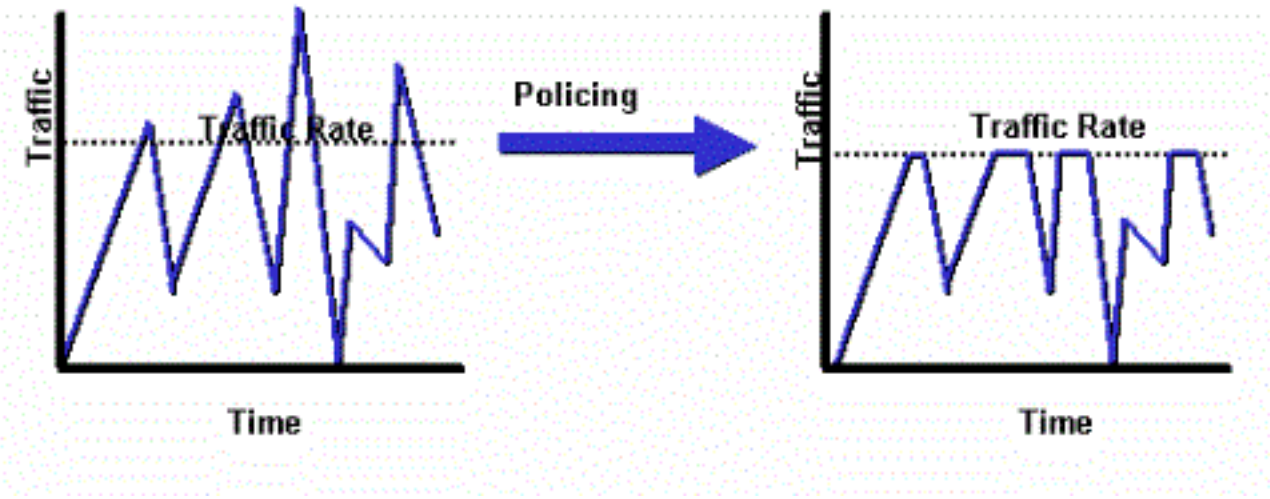
安全设备中 QoS 的主要目标是对选定的网络流量（包括单个数据流或 VPN 隧道数据流）提供速率限制，以确保所有流量都获得公平的有限带宽份额。可以使用多种方式定义数据流。在安全设备中，QoS 可以应用于源 IP 地址和目标 IP 地址、源端口号和目标端口号，以及 IP 报头的服务类型 (ToS) 字节的组合。

在ASA上可以实施三种QoS:策略、整形和优先级队列。

流量策略

使用策略管制时，超过指定限制的流量将被丢弃。策略管制是确保任何流量不超过您配置的最大速率（以位/秒为单位）的一种方法，它可确保没有一个流量或类可以接管整个资源。当流量超过最大速率时，ASA会丢弃超出的流量。策略还设置允许的最大单次突发流量。

此图说明流量管制的作用；当流量速率达到配置的最大速率时，会丢弃超额流量。结果显示为带有波峰和波谷的锯齿形输出速率。



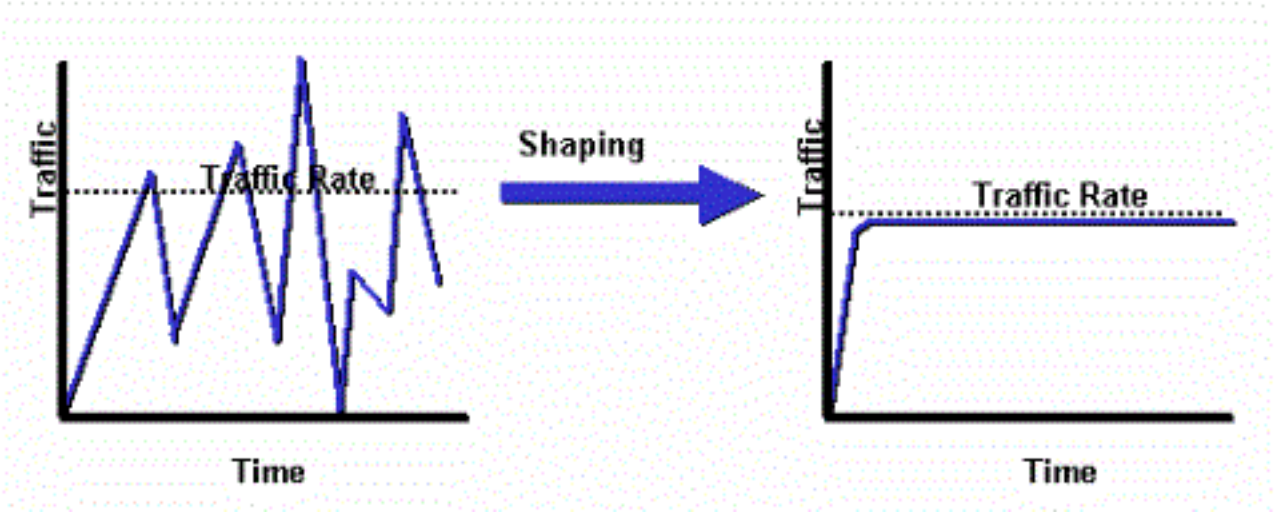
此示例显示如何将特定用户的出站方向带宽限制为1 Mbps:

```
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

流量整形用于匹配设备和链路速度，该速度控制丢包、可变延迟和链路饱和，这可能导致抖动和延迟。安全设备上的流量整形允许设备限制流量流。此机制将流量缓冲到“速度限制”以上，并尝试稍后发送流量。无法为特定类型的流量配置整形。整形流量包括通过设备的流量以及从设备发出的流量。

此图说明流量整形的作用；它会在队列中保留超额数据包，然后安排超额数据包以便随时间递增后传输。流量整形的结果是一个平滑的数据包输出速率。



注意：仅ASA版本5505、5510、5520、5540和5550支持流量整形。多核型号（如5500-X）不支持整形。

在流量整形中，超过特定限制的流量将排队（缓冲）并在下一时间间隔内发送。

如果上游设备对网络流量施加了瓶颈，则防火墙上的流量整形最有用。例如，ASA有100 Mbit接口，通过电缆调制解调器或T1（在路由器上终止）上的上游连接到Internet。流量整形允许用户配置接口（例如外部接口）上的最大出站吞吐量；防火墙将流量从该接口传输到指定的带宽，然后在链路饱和度较低时尝试缓冲过多的流量以便稍后传输。

整形应用于所有汇聚流量，这些流量会流出指定接口；您不能选择仅塑造某些流量。

注意：整形在加密后完成，不允许对VPN的内部数据包或隧道组进行优先排序。

此示例配置防火墙以将外部接口上的所有出站流量整形为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，您可以将特定流量类别放置在低延迟队列(LLQ)中，该队列在标准队列之前进行处理。

注意：如果在整形策略下确定流量的优先级，则不能使用内部数据包详细信息。防火墙只能执行LLQ，而路由器可以提供更复杂的队列和QoS机制(加权公平队列(WFQ)、基于类的加权公平队列(CBWFQ)等)。

分层QoS策略为用户提供了以分层方式指定QoS策略的机制。例如，如果用户希望对接口上的流量

进行整形，并且进一步在整形的接口流量内，为VoIP流量提供优先级排队，则用户可以在顶部指定流量整形策略，并在整形策略下指定优先级排队策略。分层QoS策略支持的范围有限。唯一允许的选项是：

- 流量整形在顶级
- 下一级优先级队列

注意：如果在整形策略下确定流量的优先级，则不能使用内部数据包详细信息。防火墙只能执行LLQ，而路由器可以提供更复杂的队列和QoS机制（WFQ、CBWFQ等）。

此示例使用分层QoS策略，以便将外部接口上的所有出站流量整形为2 Mbps（如整形示例），但它还指定具有差分服务代码点(DSCP)值“ef”以及安全外壳(SSH)流量的语音数据包应获得优先级。

在要启用该功能的接口上创建优先级队列：

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

匹配DSCP ef的类：

```
   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
```

策略映射，用于对所有流量应用整形并附加优先的语音和SSH流量：

```
   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
```

最后，将整形策略附加到要对出站流量进行整形和优先处理的接口：

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

通过VPN隧道的流量的QoS

使用IPsec VPN的QoS

根据RFC 2401 ，原始IP报头中的服务类型(ToS)位将复制到加密数据包的IP报头，以便在加密后实施QoS策略。这允许在QoS策略的任何位置将DSCP/DiffServ位用于优先级。

IPsec隧道上的策略

也可以对特定VPN隧道执行策略管制。要选择要对其进行管制的隧道组，请在类映射中使用**match tunnel-group <tunnel>** 命令和**match flow ip destination address**命令。

```
 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match tunnel-group命令时，输入策略目前**不起作用**;有关详细信息，请参阅Cisco Bug ID CSCth48255。如果尝试使用match flow ip destination-address执行输入管制，您将收到以下错误：

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

当您使用match tunnel-group(Cisco bug ID CSCth48255)时，此时**输入策略似乎**不起作用。 如果输入策略有效，则需要使用类映射，而不使**用match flow ip destination-address地址**。

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

如果尝试在没有匹配ip目标地址的类映射上管制输出，**则会收**到以下信息：

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

还可以使用访问控制列表(ACL)、DSCP等对内部流信息执行QoS。由于前面提到的漏洞，ACL是现在能够执行输入管制的方法。

> **注意**：在所有平台类型上最多可配置64个策略映射。在策略映射中使用不同的类映射以分段流量。

带安全套接字层(SSL)VPN的QoS

在ASA 9.2版之前，ASA不保留ToS位。

此功能不支持SSL VPN隧道。有关详细信息，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：当使用phone-vpn的用户使用AnyConnect客户端和数据报传输层安全(DTLS)加密其电话时，优先级不起作用，因为AnyConnect不会在DTLS封装中保留DSCP标志。有关详细信息，请参阅增强请求CSCtq43909。

QoS 注意事项

以下是关于QoS的一些要点。

- 它通过模块化策略框架(MPF)以严格或分层的方式应用：策略、整形、LLQ。

  仅能影响已从网络接口卡(NIC)传递到DP（数据路径）的流量除非应用于相邻设备，否则无法防止超支（发生得太早）

- 在允许数据包后对输入应用管制，在NIC之前对输出应用管制。

  在输出中重写第2层(L2)地址后

- 它为接口上的所有流量形成出站带宽。

  对于有限的上行链路带宽(例如到10Mb调制解调器的1千兆以太网(GE)链路)非常有用高性能ASA558x型号不支持

- 优先级队列可能会使尽力而为的流量失效。

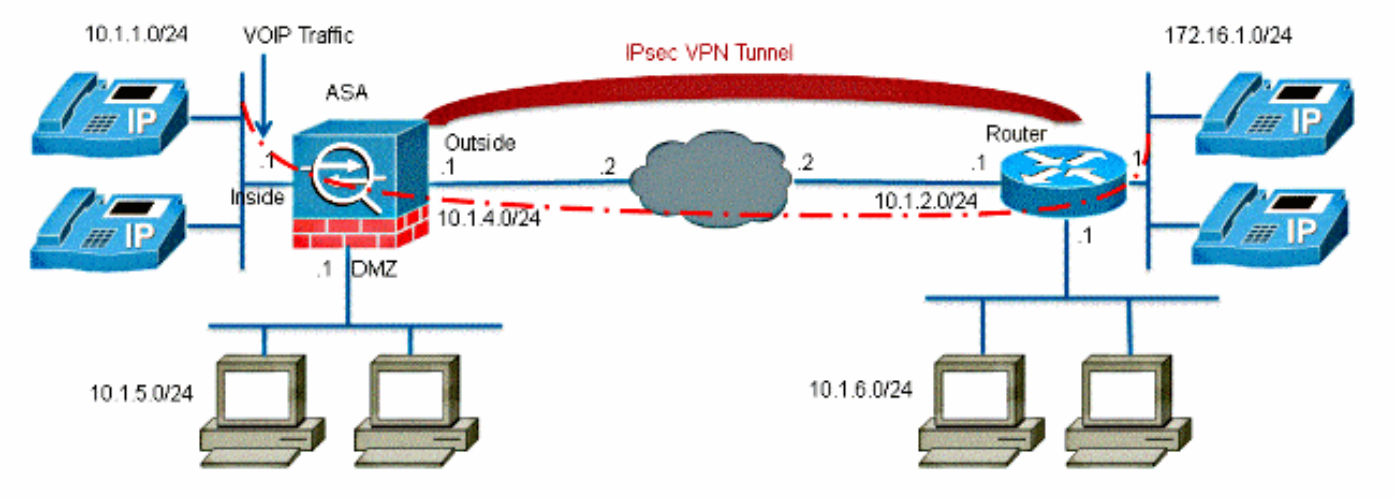
  ASA5580或VLAN子接口上的10GE接口不支持可进一步调整接口环大小以实现最佳性能

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
- 基于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：DSCP值“ef”是指与VoIP-RTP流量匹配的加速转发。

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
```

基于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：使用命令查找工具(仅注册客户)以获取本节中使用的命令的详细信息。

验证

使用本部分可确认配置能否正常运行。

show service-policy police

要查看流量管制的QoS统计信息，请使用带**police关键字的**show service-policy**命令**:

```
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-policy priority

要查看实施priority命令的服务策略的统计信息，请使用**show service-policy**命令和**priority**关键字：

```
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-policy shape

```
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
```

show priority-queue statistics

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。结果显示尽力而为(BE)队列和LLQ的统计信息。本示例显示了对名为outside的接口使用**show priority-queue statistics**命令以及命令输出。

```
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#
```

在本统计报告中，行项目的含义如下：

- “丢弃的数据包”表示此队列中已丢弃的数据包的总数。
- “Packets Transmit”表示此队列中已传输的数据包的总数。
- “已入队的数据包”表示已在此队列中排队的数据包总数。
- “当前Q长度”表示此队列的当前深度。
- “最大Q长度”表示此队列中出现的最大深度。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

故障排除

目前没有针对此配置的故障排除信息。

其他信息

以下是流量整形功能引入的一些错误：

思科漏洞ID CSCsq08550	具有优先级队列的流量整形会导致ASA上的流量失败
思科漏洞ID CSCsx07862	具有优先级队列的流量整形会导致数据包延迟和丢包
思科漏洞ID CSCsq07395	如果策略映射已编辑，则添加整形服务策略失败

常见问题

本节提供对本文档中介绍的有关信息的最常见问题之一的解答。

当穿越VPN隧道时，是否保留QoS标记？

Yes.如果提供商不在传输中删除QoS标记，则当这些标记穿越提供商网络时，这些标记将保留在隧道中。

> **提示**：请参阅CLI手册2的DSCP和DiffServ保*留部分：Cisco ASA系列防火墙CLI配置指南9.2，了*解详细信息。

相关信息

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