Cisco ASA 上 QoS 的組態範例

目錄

簡介

本檔案將說明服務品質(QoS)在思科調適型安全裝置(ASA)上的運作方式，並提供幾個範例說明如何在不同的情況下實作此功能。

您可以在安全裝置上配置QoS，以便為單個流和VPN隧道流對選定網路流量提供速率限制，以確保所有流量均獲得其公平份額的有限頻寬。

此功能已整合到思科錯誤ID CSCsk06260。

必要條件

需求

思科建議您瞭解模組化原則架構(MPF)。

採用元件

本文檔中的資訊基於運行9.2版的ASA，但也可使用更早的版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

QoS是一種網路功能，允許您為特定型別的Internet流量提供優先順序。隨著Internet使用者將其接入點從數據機升級到高速寬頻連線(如數字使用者線路(DSL)和電纜)，出現以下情況的可能性會增加：在任何給定時刻，單個使用者可能吸收大部分（如果不是全部）可用頻寬，從而使其他使用者捱餓。為了防止任何使用者或站點到站點連線消耗的頻寬超過其公平頻寬份額，QoS提供了管制功能，該功能可調整任何使用者可以使用的最大頻寬。

QoS是指網路通過各種技術為所選網路流量提供更好的服務，從而獲得底層技術頻寬有限的最佳總體服務的能力。

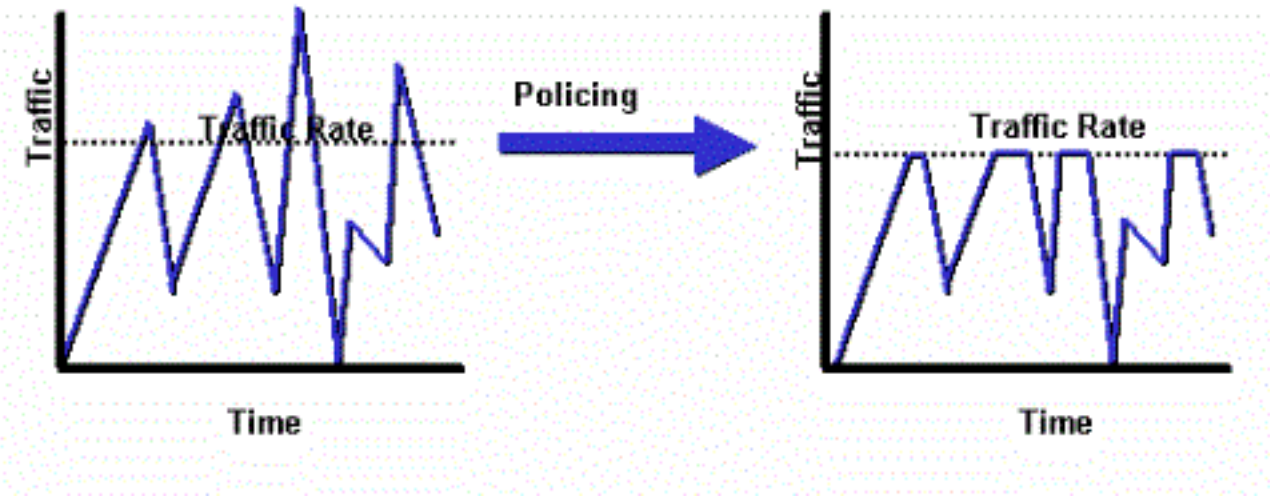
安全裝置中QoS的主要目標是針對單個流量或VPN隧道流量的選定網路流量提供速率限制，以確保所有流量都能獲得其公平份額的有限頻寬。可以通過多種方式定義流。在安全裝置中，QoS可以應用於IP報頭的源和目標IP地址、源和目標埠號以及服務型別(ToS)位元組的組合。

您可以在ASA上實施三種型別的QoS:管制、調節和優先順序佇列。

流量管制

使用策略時，超過指定限制的流量會被丟棄。策略是一種確保沒有流量超過您配置的最大速率（位/秒）的方法，可確保沒有流量或類可以接管整個資源。當流量超過最大速率時，ASA丟棄多餘的流量。策略還設定允許的最大單個突發流量。

此圖說明流量管制的作用；當流量速率達到設定的最大速率時，會捨棄多餘流量。結果輸出速率顯示為具有頂部和槽的鋸齒形。



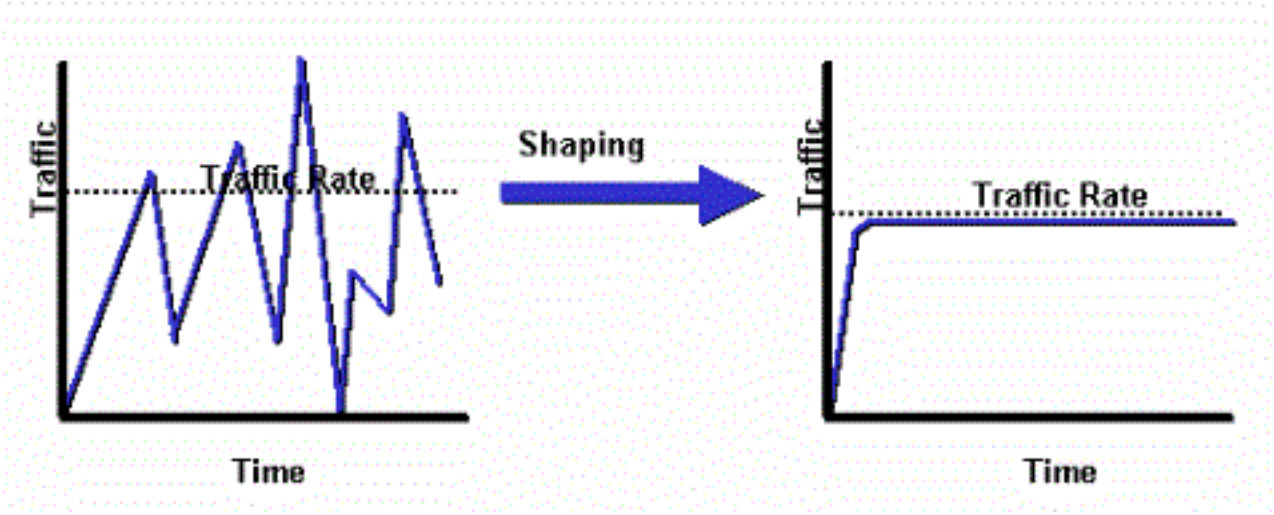
此範例顯示如何在傳出方向將特定使用者的頻寬限製為1 Mbps:

```
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
```

流量調節

流量整形用於匹配裝置和鏈路速度，從而控制資料包丟失、可變延遲和鏈路飽和（可能導致抖動和延遲）。安全裝置上的流量整形允許裝置限制流量。此機制會緩衝超過「速度限制」的流量，並嘗試稍後傳送流量。無法為特定型別的流量配置整形。整形流量包括通過該裝置的流量，以及源自該裝置的流量。

此圖說明流量整形的作用；它在隊列中保留多餘的資料包，然後將多餘的資料包排程到稍後的傳輸過程中。流量整形的結果是平滑資料包輸出速率。



附註：只有ASA 5505、5510、5520、5540和5550版本支援流量調節。多核型號（例如5500-X）不支援整形。

透過流量調節，超過特定限制的流量會排隊（緩衝），並在下一個時間間隔期間傳送。

如果上游裝置對網路流量施加了瓶頸，則防火牆上的流量整形最有用。一個很好的例子是ASA，它有100 Mbit介面，通過電纜數據機或在路由器上終止的T1連線到網際網路。流量整形允許使用者在介面（例如外部介面）上配置最大出站吞吐量；防火牆將流量從該介面傳輸至指定頻寬，然後在鏈路不太飽和時嘗試緩衝過多的流量以便稍後傳輸。

將整形應用於所有從指定介面出發的聚合流量；您不能選擇僅影響特定流量。

附註：整形在加密後完成，不允許在VPN的內部資料包或隧道組基礎上進行優先排序。

此示例配置防火牆以將外部介面上的所有出站流量整形為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
```

優先順序佇列

使用優先順序隊列，您可以將特定類別的流量放在低延遲隊列(LLQ)中，該隊列在標準隊列之前進行處理。

附註：如果在整形策略下優先處理流量，則無法使用內部資料包詳細資訊。防火牆只能執行LLQ，而路由器能夠提供更複雜的排隊和QoS機制(加權公平佇列(WFQ)、類別型加權公平佇列(CBWFQ)等)。

分層QoS策略為使用者提供了一種以分層方式指定QoS策略的機制。例如，如果使用者想要在介面

上整形流量，並在整形後的介面流量內整形流量，為VoIP流量提供優先順序隊列，則使用者可以在頂部指定流量整形策略，在整形策略下指定優先順序隊列策略。分層的QoS策略支援範圍有限。只允許以下選項：

- 頂層流量調節
- 下一級別的優先順序隊列

附註：如果在整形策略下優先處理流量，則無法使用內部資料包詳細資訊。防火牆僅能執行LLQ，而路由器則能提供更完善的排隊和QoS機制（WFQ、CBWFQ等）。

此示例使用分層QoS策略將外部介面上的所有出站流量整形為2 Mbps（與整形示例類似），但它也指定具有區分服務代碼點(DSCP)值「ef」的語音資料包以及安全外殼(SSH)流量應優先接收。

在要啟用功能的介面上建立優先順序隊列：

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

與DSCP ef匹配的類：

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

匹配埠TCP/22 SSH流量的類:

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

應用語音和SSH流量優先順序的策略對映：

```
   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
```

策略對映，將整形應用到所有流量並附加優先順序的語音和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
```

最後，將整形策略附加到要在其上整形和優先處理出站流量的介面：

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

通過VPN隧道的流量的QoS

使用IPsec VPN的QoS

根據RFC 2401，原始IP標頭中的服務型別(ToS)位會複製到加密封包的IP標頭中，以便加密後可以執行QoS原則。這允許DSCP/DiffServ位在QoS策略中的任何位置用作優先順序。

IPsec隧道上的管制

還可以對特定VPN隧道執行管制。若要選擇要強制控制的隧道組，請在類對映中使用**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
```

使用**match tunnel-group**指令時，目前輸入管制無法運作；如需詳細資訊，請參閱Cisco錯誤ID CSCth48255。如果嘗試使用match flow ip destination-address執行輸入管制，則會收到以下錯誤：

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

目前使用**match tunnel-group**(思科錯誤ID CSCth48255)時，輸入管制似乎無法使用。 如果輸入管制有效，則您需要使用沒有**match flow ip destination-address**的類對映。

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

如果嘗試在不具有**match ip destination address**的類對映上管制輸出，您將收到：

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

使用存取控制清單(ACL)、DSCP等也可以對內部流量資訊執行QoS。由於前面提到的錯誤，ACL是現在能夠執行輸入原則管制的方式。

> **附註**：在所有平台型別上最多可以配置64個策略對映。在策略對映中使用不同的類對映來分段流量。

使用安全套接字層(SSL)VPN的QoS

在ASA 9.2版之前，ASA不保留ToS位。

此功能不支援SSL VPN隧道。如需詳細資訊，請參閱Cisco錯誤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)#
```

附註：當使用phone-vpn的使用者使用AnyConnect客戶端和資料包傳輸層安全(DTLS)加密其電話時，優先順序不起作用，因為AnyConnect不保留DTLS封裝中的DSCP標誌。如需詳細資訊，請參閱增強功能要求CSCtq43909。

QoS注意事項

下面是關於QoS的一些注意事項。

- 它通過模組化策略框架(MPF)以嚴格或分層方式應用：管制、整形、LLQ。

  只能影響已經從網路介面卡(NIC)傳遞到DP（資料路徑）的流量如果不在相鄰裝置上應用則無法解決超限問題（它們發生得太早）

- 在允許資料包後對輸入應用管制，在NIC之前對輸出應用管制。

  就在輸出中重寫第2層(L2)地址之後

- 它會對介面上的所有流量形成出站頻寬。

  適用於有限的上行鏈路頻寬(例如到10 Mb數據機的千兆乙太網(GE)鏈路)高效能ASA558x型號不支援

- 優先順序隊列可能會耗盡盡力流量。

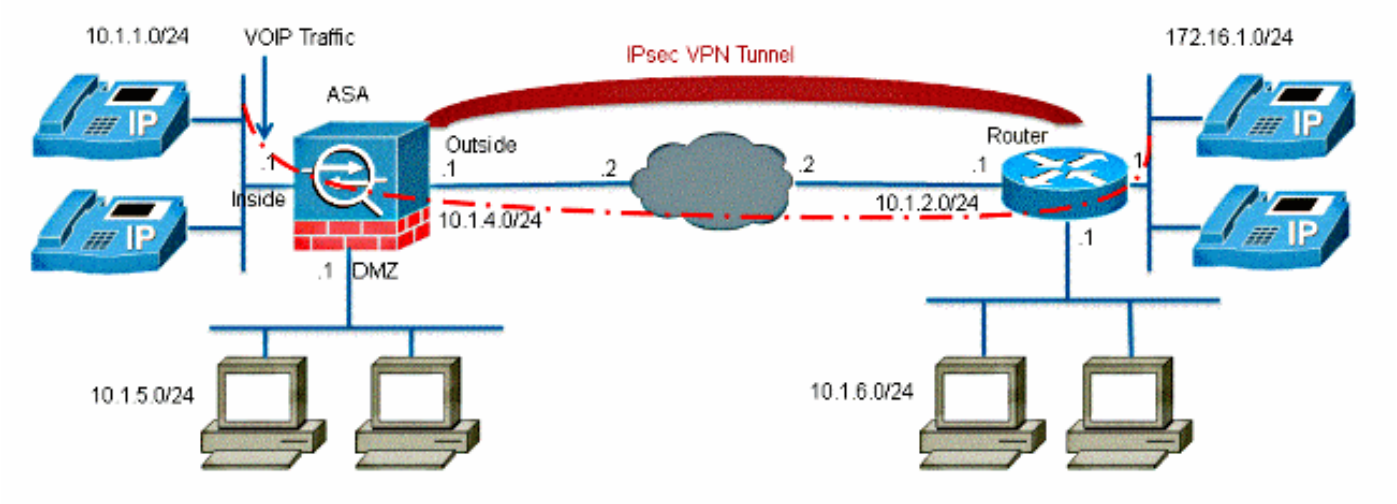
  ASA5580或VLAN子介面上的10GE介面不支援可以進一步調整介面環大小以實現最佳效能

組態範例

VPN隧道上VoIP流量的QoS配置示例

網路圖表

本檔案會使用以下網路設定：



附註：確保IP電話和主機位於不同的網段（子網）中。 這是進行良好網路設計的推薦方法。

本檔案會使用以下設定：

- 基於DSCP的QoS配置
- 基於DSCP的VPN配置QoS
- 基於ACL的QoS配置
- 基於ACL的VPN配置QoS

基於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
```

附註：「ef」的DSCP值是指與VoIP-RTP流量匹配的加速轉發。

基於DSCP的VPN配置QoS

```
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
```

基於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
```

基於ACL的QoS，帶VPN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
```

附註：使用命令查詢工具(僅供註冊客戶使用)可獲取本節中使用的命令的更多資訊。

驗證

使用本節內容，確認您的組態是否正常運作。

show service-policy police

要檢視流量策略的QoS統計資訊，請使用帶有police 關鍵字的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

要檢視實施priority 命令的服務策略的統計資訊，請使用帶有priority 關鍵字的show service-policy命令：

```
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

要顯示介面的優先順序隊列統計資訊，請在特權EXEC模式下使用show priority-queue statistics命令。結果顯示了盡力而為(BE)隊列和LLQ的統計資訊。此示例顯示對名為outside的介面使用show priority-queue statistics命令以及命令輸出。

```
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#
```

在此統計報表中，行專案的含義如下：

- 「Packets Dropped」表示此隊列中已丟棄的資料包總數。
- 「Packets Transmit」表示此隊列中已傳輸的資料包總數。
- 「Packets Enqueued」表示已在此隊列中排隊的資料包總數。
- 「當前Q長度」表示此隊列的當前深度。
- 「Max Q Length」表示此隊列中出現的最大深度。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

其他資訊

以下是流量調節功能引入的一些錯誤：

思科錯誤ID CSCsq08550	帶有優先順序隊列的流量整形導致ASA上的流量故障
思科錯誤ID CSCsx07862	具有優先順序佇列的流量整形會導致封包延遲和捨棄
思科錯誤ID CSCsq07395	如果編輯了策略對映，則新增整形服務策略失敗

常見問題

本節就本文檔中描述的資訊提供了最常見問題之一的解答。

通過VPN隧道時是否保留QoS標籤？

會。如果QoS標籤在傳輸過程中未剝離，則在它們經過提供商網路時，會保留在隧道中。

> **提示：**請參閱*CLI Book 2*的DSCP和DiffServ保留部分：*Cisco ASA系列防火牆CLI配置指南9.2版*，瞭解詳細資訊。

相關資訊

- **Cisco ASA系列防火牆CLI配置指南，服務品質**
- **應用QoS策略**
- **瞭解無客戶端SSL VPN不支援的功能**
- **配置QoS**
- **技術支援與文件 - Cisco Systems**