Esempi di configurazione sulla funzionalità QoS su Cisco ASA

Sommario

Introduzione

Questo documento spiega come Quality of Service (QoS) funziona su Cisco Adaptive Security Appliance (ASA) e fornisce anche diversi esempi su come implementarlo in diversi scenari.

Èpossibile configurare la funzionalità QoS sull'appliance di sicurezza in modo da limitare la velocità del traffico di rete selezionato, sia per i singoli flussi che per i flussi del tunnel VPN, in modo da garantire che tutto il traffico riceva la sua giusta quota di larghezza di banda limitata.

La funzionalità è stata integrata con l'ID bug Cisco CSCsk06260.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Modular Policy Framework (MPF).

Componenti usati

Le informazioni di questo documento si basano su un'appliance ASA con versione 9.2, ma è possibile usare anche le versioni precedenti.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

QoS è una funzione di rete che consente di dare priorità a determinati tipi di traffico Internet. Man mano che gli utenti di Internet aggiornano i propri punti di accesso da modem a connessioni a banda larga ad alta velocità, come DSL (Digital Subscriber Line) e cavo, aumenta la probabilità che in un determinato momento un singolo utente sia in grado di assorbire la maggior parte, se non la totalità, della larghezza di banda disponibile, riducendo così la fame degli altri utenti. Per evitare che un utente o una connessione da sito a sito utilizzi una quantità di larghezza di banda superiore a quella che può utilizzare, QoS offre una funzione di controllo che regola la larghezza di banda massima che ogni utente può utilizzare.

QoS si riferisce alla capacità di una rete di fornire un servizio migliore al traffico di rete selezionato su varie tecnologie per i migliori servizi complessivi con larghezza di banda limitata delle tecnologie sottostanti.

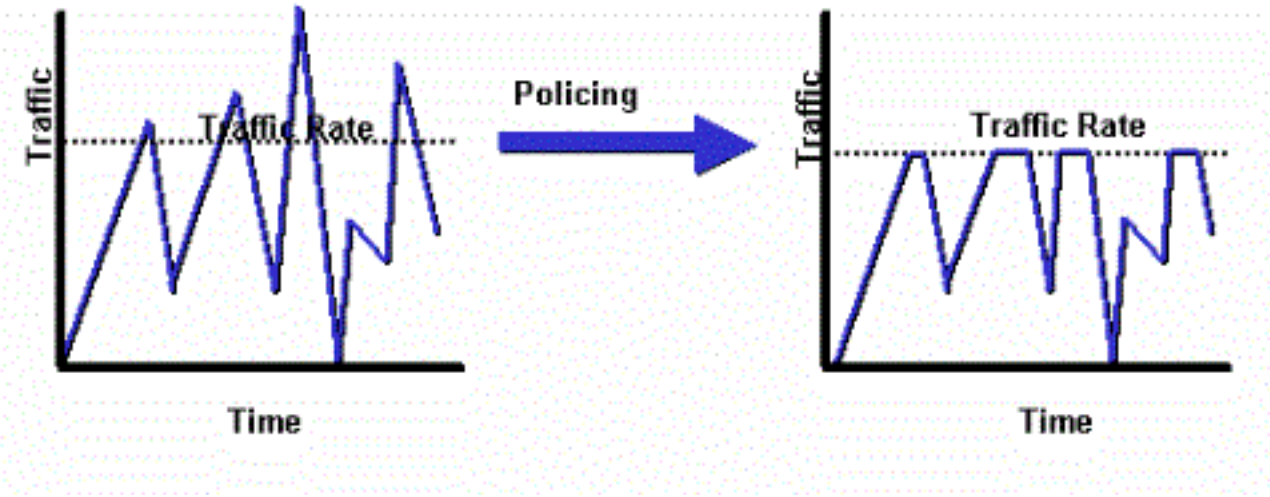
QoS nelle appliance di sicurezza ha come obiettivo principale la limitazione della velocità sul traffico di rete selezionato per il flusso del singolo flusso o del tunnel VPN, in modo che tutto il traffico ottenga la giusta quota di larghezza di banda limitata. Un flusso può essere definito in diversi modi. Nell'appliance di sicurezza, le funzionalità QoS possono essere applicate a una combinazione di indirizzi IP di origine e di destinazione, numeri di porta di origine e di porta di destinazione e byte del tipo di servizio (ToS) dell'intestazione IP.

Esistono tre tipi di QoS che è possibile implementare sull'appliance ASA: Policing, Shaping e Priority Queueing.

Traffic Policing

Con i criteri, il traffico che supera un limite specificato viene scartato. I criteri consentono di garantire che nessun traffico superi la velocità massima (in bit/secondo) configurata, in modo che nessun flusso di traffico o classe possa occupare l'intera risorsa. Quando il traffico supera la velocità massima, l'ASA scarta il traffico in eccesso. Il policing imposta anche la più grande singola frammentazione di traffico consentita.

Il diagramma mostra le attività del traffic policing; quando la velocità del traffico raggiunge la velocità massima configurata, il traffico in eccesso viene interrotto. Il risultato è una velocità di trasmissione che appare come un'onda a dente di sega con picchi ad andamento positivo e negativo.



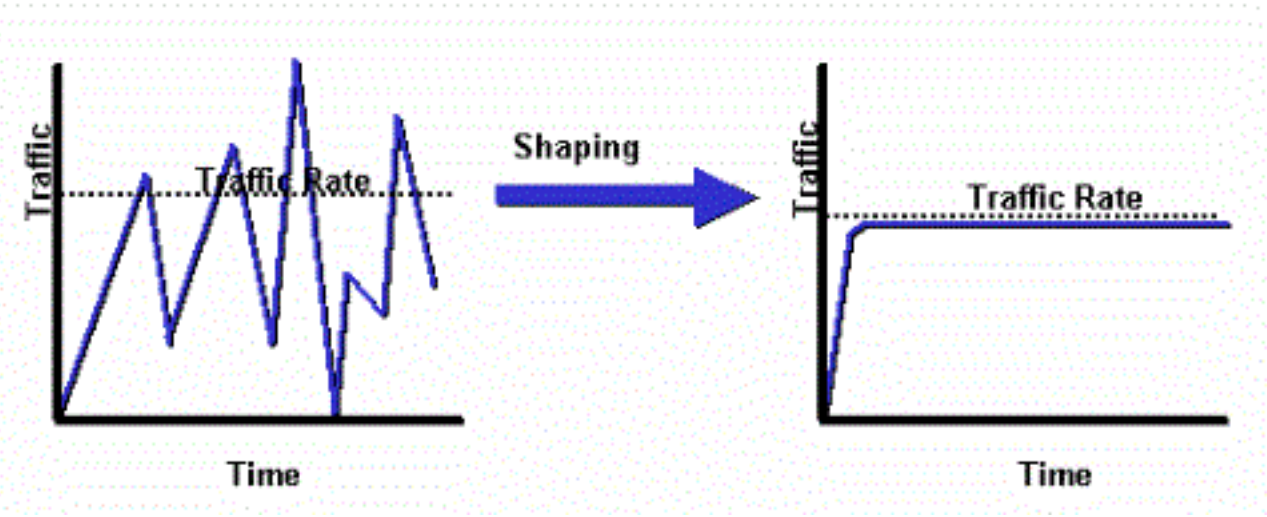
Nell'esempio viene mostrato come limitare la larghezza di banda a 1 Mbps per un utente specifico nella direzione in uscita:

```
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
```

Traffic Shaping

Il Traffic Shaping viene usato per adattarsi alle velocità dei dispositivi e dei collegamenti e controlla la perdita, il ritardo variabile e la saturazione del collegamento che può causare tremolio e ritardo. Il Traffic Shaping sull'appliance di sicurezza permette al dispositivo di limitare il flusso del traffico. Questo meccanismo memorizza il traffico oltre il "limite di velocità" e tenta di inviarlo successivamente. Non è possibile configurare il shaping per determinati tipi di traffico. Il traffico con forma include il traffico che attraversa il dispositivo e il traffico che proviene dal dispositivo.

Il diagramma mostra le funzioni del traffic shaping, conserva i pacchetti in eccesso in una coda e quindi li programma per una successiva trasmissione su incrementi di tempo. Il risultato del traffic shaping è una velocità di trasmissione dei pacchetti fluida e uniforme.



> **Nota:** Il traffic shaping è supportato solo sulle versioni ASA 5505, 5510, 5520, 5540 e 5550. I modelli multicore, ad esempio 5500-X, non supportano la modellazione.

Con il traffic shaping, il traffico che supera un certo limite viene messo in coda (nel buffer) e inviato durante la sessione successiva.

Il traffic shaping sul firewall è particolarmente utile se un dispositivo a monte impone un collo di bottiglia sul traffico di rete. Ad esempio, un'appliance ASA ha interfacce da 100 Mbit e una connessione a monte a Internet tramite modem via cavo o T1 che termina su un router. Il Traffic Shaping consente all'utente di configurare il massimo throughput in uscita su un'interfaccia (ad esempio, l'interfaccia esterna); il firewall trasmette il traffico da quell'interfaccia fino alla larghezza di banda specificata e quindi cerca di buffer del traffico eccessivo per la trasmissione in un secondo momento, quando il collegamento è meno saturo.

Il shaping viene applicato a tutto il traffico aggregato che genera l'interfaccia specificata; non è possibile scegliere di modellare solo determinati flussi di traffico.

> **Nota:** Il shaping viene eseguito dopo la crittografia e non consente la definizione delle priorità per il pacchetto interno o i gruppi di tunnel per la VPN.

Nell'esempio seguente viene configurato il firewall per impostare su 2 Mbps tutto il traffico in uscita sull'interfaccia esterna:

```
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
```

Priority Queueing

L'accodamento delle priorità consente di inserire una classe specifica di traffico nella coda LLQ (Low Latency Queue), che viene elaborata prima della coda standard.

> **Nota:** Se si assegna la priorità al traffico in base a un criterio di shaping, non è possibile utilizzare i dettagli del pacchetto interno. Il firewall può solo eseguire LLQ, a differenza dei router che possono fornire code più sofisticate e meccanismi QoS (WFQ (Weighted Fair Queueing), CBWFQ (Weighted Fair Queueing) basato su classi e così via).

Il criterio QoS gerarchico fornisce un meccanismo che consente agli utenti di specificare il criterio QoS in modo gerarchico. Ad esempio, se gli utenti desiderano configurare il traffico su un'interfaccia e, inoltre, all'interno del traffico dell'interfaccia con forma, fornire una coda di priorità per il traffico VoIP, gli utenti possono specificare un criterio di traffic shaping nella parte superiore e un criterio di coda di priorità nel criterio forma. Il supporto dei criteri QoS gerarchici ha ambito limitato. L'unica opzione consentita è:

- Traffic shaping al livello superiore
- Accodamento priorità al livello successivo

> **Nota:** Se si assegna la priorità al traffico in base a un criterio di shaping, non è possibile utilizzare i dettagli del pacchetto interno. A differenza dei router che possono fornire meccanismi QoS e code più sofisticate (WFQ, CBWFQ e così via), il firewall può solo eseguire LLQ.

In questo esempio viene usato il criterio QoS gerarchico per configurare tutto il traffico in uscita sull'interfaccia esterna su 2 Mbps, come nell'esempio di shaping, ma viene specificato anche che i pacchetti voce con valore "ef" per DSCP (Differentiated Services Code Point) e il traffico SSH (Secure Shell) devono avere la priorità.

Creare la coda di priorità sull'interfaccia per la quale si desidera abilitare la funzionalità:

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

Classe corrispondente a DSCP ef:

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

Classe per la corrispondenza con il traffico TCP/22 SSH della porta:

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

Una mappa policy per assegnare le priorità al traffico voce e SSH:

```
   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
```

Una mappa policy per applicare il shaping a tutto il traffico e associare le priorità al traffico voce e SSH:

```
   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
```

Infine, associare il criterio di shaping all'interfaccia sulla quale definire la forma e la priorità del traffico in uscita:

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

QoS per il traffico attraverso un tunnel VPN

QoS con VPN IPsec

Come stabilito nella RFC 2401, i bit del tipo di servizio (ToS) nell'intestazione IP originale vengono copiati sull'intestazione IP del pacchetto crittografato in modo da poter applicare i criteri QoS dopo la crittografia. In questo modo, i bit DSCP/DiffServ possono essere utilizzati come priorità in qualsiasi punto della policy QoS.

Policy in un tunnel IPsec

Il policing può essere eseguito anche per tunnel VPN specifici. Per selezionare un gruppo di tunnel da controllare, usare il comando **match tunnel-group <tunnel>** nella mappa delle classi e il comando **match flow ip destination**.

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

Il policy di input non funziona quando si usa il comando **match tunnel-group**; per ulteriori informazioni, vedere l'ID bug Cisco CSCth48255. Se si tenta di eseguire il controllo dell'input con l'indirizzo di destinazione IP del flusso di corrispondenza, viene visualizzato questo errore:

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

Il policy di input non sembra funzionare quando si usa **match tunnel-group** (Cisco bug ID CSCth48255). Se il criterio di input funziona, è necessario utilizzare una mappa di classi senza l'**indirizzo di destinazione IP del flusso di corrispondenza**.

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

Se si cerca di controllare l'output su una mappa di classe che non ha l'**indirizzo di destinazione IP corrispondente**, si riceve:

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

Èinoltre possibile eseguire QoS sulle informazioni del flusso interno utilizzando Access Control Lists (ACL), DSCP e così via. A causa del bug menzionato sopra, gli ACL sono il modo per poter eseguire subito il policy di input.

> **Nota:** È possibile configurare un massimo di 64 mappe dei criteri su tutti i tipi di piattaforma. Utilizzare mappe di classi diverse all'interno delle mappe delle policy per segmentare il traffico.

QoS con VPN Secure Sockets Layer (SSL)

Fino alla versione 9.2, l'appliance ASA non conservava i bit del tipo ToS.

Il tunneling VPN SSL non è supportato con questa funzionalità. Per ulteriori informazioni, vedere l'ID bug Cisco 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)#
```

> **Nota:** Quando gli utenti con vpn telefonica usano il client AnyConnect e il protocollo DTLS (Datagram Transport Layer Security) per crittografare il telefono, la definizione delle priorità non funziona perché AnyConnect non mantiene il flag DSCP nell'incapsulamento DTLS. Per ulteriori informazioni, fare riferimento alla richiesta di miglioramento CSCtq43909.

Considerazioni QoS

Ecco alcuni aspetti da considerare riguardo la QoS.

- Èapplicato attraverso il quadro di politica modulare (MPF) in modo rigoroso o gerarchico: Sorveglianza, Shaping, LLQ.

  Può influenzare solo il traffico già passato dalla scheda di interfaccia di rete (NIC, Network Interface Card) al DP (percorso dati)Inutile combattere i sovraccarichi (si verificano troppo presto) a meno che non vengano applicati a un dispositivo adiacente

- La policy viene applicata sull'input dopo che il pacchetto è autorizzato e sull'output prima della scheda NIC.

  Subito dopo aver riscritto un indirizzo di layer 2 (L2) sull'output

- Forma la larghezza di banda in uscita per tutto il traffico su un'interfaccia.

  Utile con larghezza di banda uplink limitata (ad esempio collegamento 1 Gigabit Ethernet (GE) a modem 10 MB)Non supportato sui modelli ASA558x ad alte prestazioni

- L'accodamento delle priorità potrebbe causare la diminuzione del traffico.

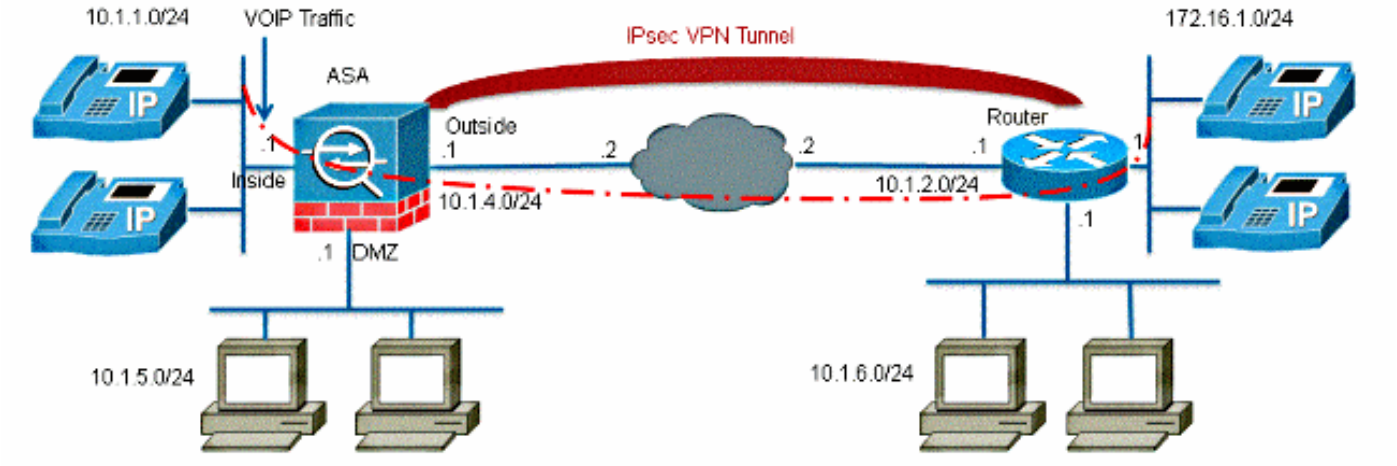
  Non supportato sulle interfacce 10GE sulle sottointerfacce ASA5580 o VLANÈpossibile regolare ulteriormente le dimensioni dell'anello di interfaccia per ottenere prestazioni ottimali

Esempi di configurazione

Esempio di configurazione QoS per il traffico VoIP sui tunnel VPN

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: Accertarsi che i telefoni IP e gli host siano posizionati in segmenti (subnet) diversi. Questa opzione è consigliata per una buona progettazione della rete.

Nel documento vengono usate queste configurazioni:

- Configurazione QoS basata su DSCP
- QoS basato su DSCP con configurazione VPN
- Configurazione QoS basata su ACL
- QoS basato su ACL con configurazione VPN

Configurazione QoS basata su DSCP

```
!--- 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
```

> **Nota:** Il valore DSCP di "ef" si riferisce all'inoltro accelerato che corrisponde al traffico VoIP-RTP.

QoS basato su DSCP con configurazione VPN

```
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
```

Configurazione QoS basata su ACL

```
!--- 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
```

QoS basato su ACL con configurazione VPN

```
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
```

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

show service-policy Police

Per visualizzare le statistiche QoS per il traffic policing, usare il comando **show service-policy** con la parola chiave **Police**:

```
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

Per visualizzare le statistiche relative ai criteri di servizio che implementano il comando **priority**, utilizzare il comando **show service-policy** con la parola chiave **priority**:

```
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
```

mostra forma criteri servizio

```
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
```

mostra statistiche coda di priorità

Per visualizzare le statistiche della coda di priorità per un'interfaccia, usare il comando **show priority-queue statistics** in modalità di esecuzione privilegiata. I risultati mostrano le statistiche sia per la coda del massimo sforzo (BE) che per LLQ. In questo esempio viene mostrato l'utilizzo del comando **show priority-queue statistics** per l'interfaccia esterna e l'output del comando.

```
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#
```

In questo rapporto statistico, il significato delle voci è il seguente:

- "Pacchetti scartati" indica il numero complessivo di pacchetti scartati in questa coda.
- "Trasmissione pacchetti" indica il numero complessivo di pacchetti trasmessi in questa coda.
- "Pacchetti accodati" indica il numero complessivo di pacchetti accodati in questa coda.
- "Lunghezza Q corrente" indica la profondità corrente di questa coda.
- "Lunghezza Q max" indica la profondità massima che si è mai verificata in questa coda.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Ulteriori informazioni

Di seguito sono riportati alcuni bug introdotti dalla funzionalità Traffic Shaping:

ID bug Cisco CSCsq08550	Il traffic shaping con la coda di priorità causa un errore di traffico sull'appliance
ID bug Cisco CSCsx07862	Il traffic shaping con l'accodamento della priorità causa il ritardo e la perdita de pacchetti
ID bug Cisco CSCsq07395	L'aggiunta del criterio del servizio di shaping non riesce se il criterio è stato modificato

Domande frequenti

In questa sezione viene fornita la risposta a una delle domande più frequenti relative alle informazioni descritte in questo documento.

I contrassegni QoS vengono mantenuti quando il tunnel VPN viene attraversato?

Sì. I contrassegni QoS vengono mantenuti nel tunnel mentre attraversano le reti del provider, se quest'ultimo non li rimuove.

> **Suggerimento**: Fare riferimento alla sezione DSCP and DiffServ Preservation del *manuale CLI 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.2* per ulteriori dettagli.

Informazioni correlate

- Guida alla configurazione della CLI del firewall Cisco serie ASA, Quality of Service
- Applicazione dei criteri QoS
- Informazioni sulle funzionalità non supportate nella VPN SSL senza client
- Configurazione di QoS
- Documentazione e supporto tecnico – Cisco Systems