QoS op de Cisco ASA Configuration-voorbeelden

Inhoud

Inleiding

Dit document legt uit hoe Quality of Service (QoS) werkt op Cisco adaptieve security applicatie (ASA) en biedt ook verschillende voorbeelden van hoe deze applicatie te implementeren voor verschillende scenario's.

U kunt QoS op het security apparaat configureren om snelheidsbeperking bij geselecteerd netwerkverkeer te bieden, zowel voor individuele stromen als voor VPN-tunnelstromen, om er zeker van te zijn dat al het verkeer zijn eerlijke deel van de beperkte bandbreedte krijgt.

De functie is geïntegreerd met Cisco bug-ID CSCsk06260.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van modulair beleidskader (MPF).

Gebruikte componenten

De informatie in dit document is gebaseerd op een ASA die versie 9.2 draait. Maar eerdere versies kunnen ook worden gebruikt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

QoS is een netwerkfunctie die u in staat stelt om voorrang te geven aan bepaalde soorten internetverkeer. Aangezien internetgebruikers hun toegangspunten van modems tot snelle breedbandverbindingen zoals Digital Subscriber Line (DSL) en kabel upgraden, wordt de kans groter dat één gebruiker op een bepaald moment de meeste, zo niet alle, beschikbare bandbreedte kan absorberen en zo de andere gebruikers onderuit kan halen. Om te voorkomen dat één gebruiker of site-to-site verbinding meer consumeert dan zijn eerlijke deel van de bandbreedte, biedt QoS een toezichthoudende functie die de maximale bandbreedte reguleert die een gebruiker kan gebruiken.

QoS verwijst naar de mogelijkheid van een netwerk om betere service te bieden aan geselecteerd netwerkverkeer via verschillende technologieën voor de beste algemene services met beperkte bandbreedte van de onderliggende technologieën.

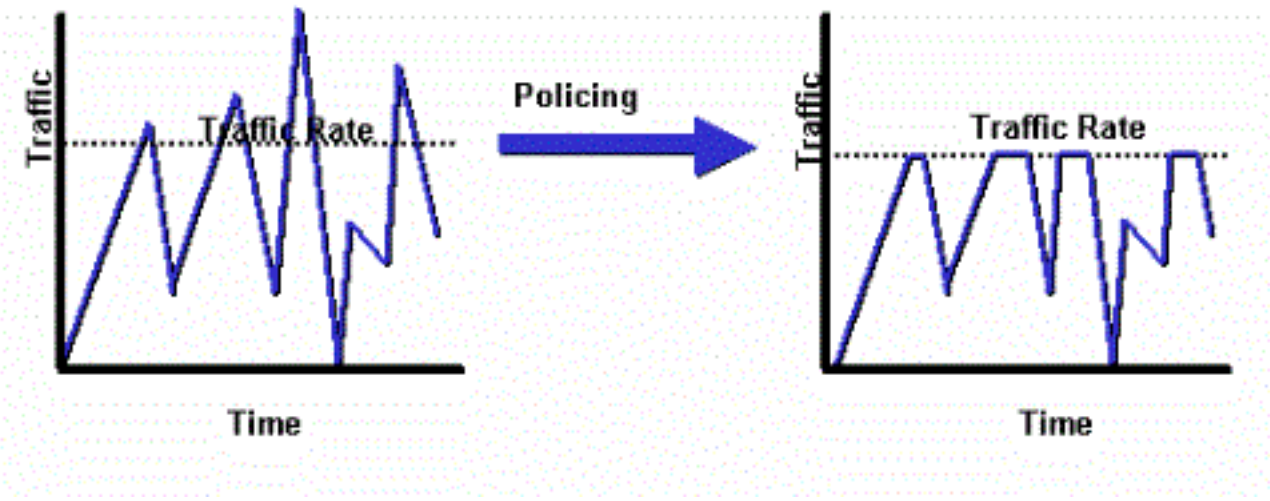
Het primaire doel van QoS in het veiligheidsapparaat is snelheidsbeperking te bieden op geselecteerd netwerkverkeer voor zowel individuele flow als VPN tunnelstromen om ervoor te zorgen dat al het verkeer zijn eerlijke deel van beperkte bandbreedte krijgt. Een stroom kan op een aantal manieren worden gedefinieerd. In het security apparaat kan QoS van toepassing zijn op een combinatie van IP-adressen van bron en bestemming, bron- en doelpoortnummer en het Type of Service (ToS) van de IP-header.

Er zijn drie soorten QoS die je kunt implementeren op de ASA: Toezicht, vormgeving en prioriteitswachtrij.

Toezicht op verkeer

Met toezicht, wordt het verkeer over een gespecificeerde grens gedropt. Toezicht is een manier om te verzekeren dat geen verkeer de maximum snelheid (in bits/seconde) die u vormt overschrijdt, wat ervoor zorgt dat geen één verkeersstroom of klasse de gehele bron kan overnemen. Wanneer het verkeer het maximum tarief overschrijdt, daalt de ASA het overtollige verkeer. Toezicht stelt ook de grootste toegestane uitbarsting van verkeer in.

In dit schema wordt aangegeven wat verkeerstoezicht doet. wanneer het verkeerstarief het geconfigureerde maximumtarief bereikt, wordt het overtollige verkeer verlaagd. Het resultaat is een uitvoersnelheid die als een zaagtand met kreuken en nokken weergegeven wordt.



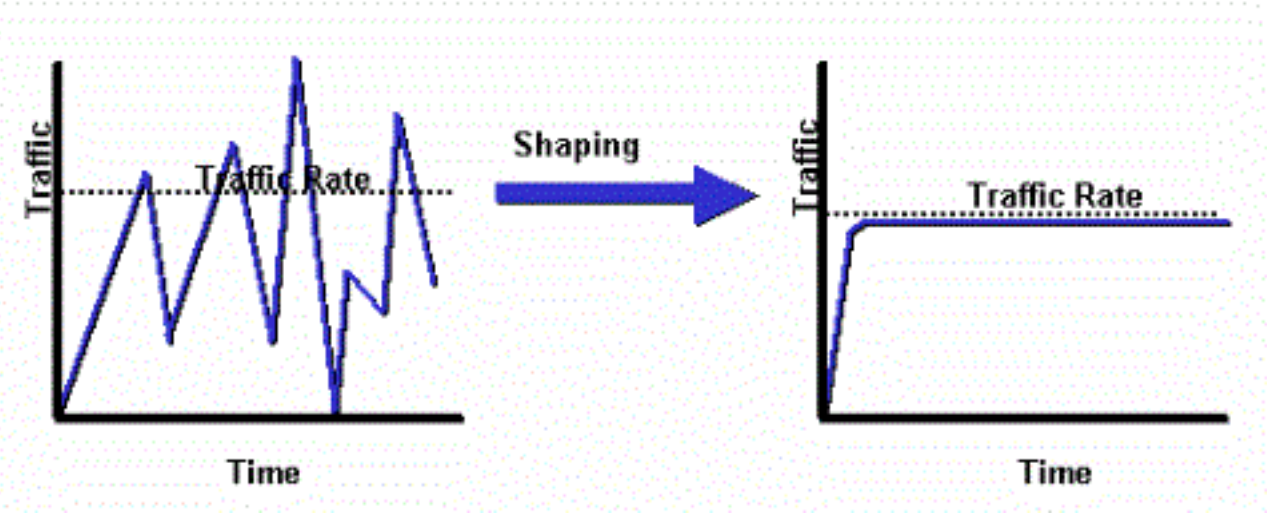
Dit voorbeeld toont hoe de bandbreedte aan 1 Mbps voor een specifieke gebruiker in de uitgaande richting te wissen:

```
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

Traffic Shaping wordt gebruikt om apparaten en verbindingssnelheden aan te passen, die pakketverlies, variabele vertraging en verbindingsverzadiging controleren wat vertraging en vertraging kan veroorzaken. Traffic Shaping op het security apparaat maakt het apparaat mogelijk om de stroom van verkeer te beperken. Dit mechanisme buffert verkeer over de "snelheidsgrens" en probeert het verkeer later te verzenden. Shaping kan niet worden ingesteld voor bepaalde soorten verkeer. Het gevormde verkeer omvat verkeer dat door het apparaat passeert, zowel als verkeer dat van het apparaat afkomstig is.

Dit schema illustreert wat traffic shaping doet; het houdt overtollige pakketten in een rij en plant dan de overmaat voor latere transmissie over stappen van tijd . Het resultaat van traffic shaping is een vloeiend pakketuitvoeringspercentage.



> **Opmerking:** Traffic Shaping wordt alleen ondersteund op ASA versies 5505, 5510, 5520, 5540 en 5550. Multicore modellen (zoals de 5500-X) ondersteunen geen vormgeving.

Met traffic shaping wordt verkeer dat een bepaalde grenswaarde overschrijdt in de wachtrij geplaatst (gebufferd) en tijdens de volgende tijdlijn verstuurd.

Traffic Shaping in de firewall is het meest handig als een upstream-apparaat een flits aan netwerkverkeer oplegt. Een goed voorbeeld zou een ASA zijn die 100 Mbit interfaces heeft, met een upstream verbinding met het internet via een kabelmodem of T1 die op een router eindigt. Traffic Shaping stelt de gebruiker in staat om de maximale uitloop op een interface te configureren (bijvoorbeeld de externe interface); de firewall geeft verkeer vanuit die interface over tot de gespecificeerde bandbreedte, en probeert dan het buitensporige verkeer voor transmissie later te bufferen wanneer de link minder verzadigd is.

Shaping wordt toegepast op al het geaggregeerde verkeer dat zich op de gespecificeerde interface richt; u kunt niet ervoor kiezen alleen bepaalde verkeersstromen vorm te geven.

> **Opmerking:** Shaping wordt uitgevoerd na encryptie en staat geen prioritering op de binnenpakket of tunnelgroepsbasis voor VPN toe.

Dit voorbeeld vormt de firewall om al uitgaande verkeer op de buiteninterface tot 2 Mbps te vormen:

```
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
```

Prioritaire wachtrijen

Met prioriteitswachtrij kunt u een specifieke verkeersklasse in de LLQ-wachtrij plaatsen, die vóór de standaardwachtrij wordt verwerkt.

> **Opmerking:** Als u onder een vormbeleid voorrang geeft aan verkeer, kunt u geen innerlijke pakketdetails gebruiken. De firewall kan alleen LLQ uitvoeren, in tegenstelling tot de routers die geavanceerde wachtrijen en QoS-mechanismen (Weighted Fair Queueing (WFQ), Class-Based Weighted Fair Queueing (CBWFQ) enzovoort.

Het hiërarchische QoS-beleid biedt een mechanisme voor gebruikers om het QoS-beleid in hiërarchische zin te specificeren. Als gebruikers bijvoorbeeld het verkeer op een interface willen vormgeven en bovendien binnen het gevormde interfaceverkeer willen, voorrang geven aan wachtrijen voor VoIP-verkeer, dan kunnen gebruikers aan de top een traffic shaping-beleid en een prioritair wachtend beleid in het vormbeleid specificeren. De hiërarchische QoS-beleidsondersteuning is beperkt in omvang. De enige optie die is toegestaan is:

- Traffic Shaping op bovenniveau
- Prioritaire wachtrij op het volgende niveau

> **Opmerking:** Als u onder een vormbeleid voorrang geeft aan verkeer, kunt u geen innerlijke pakketdetails gebruiken. De firewall kan alleen LLQ uitvoeren, in tegenstelling tot de routers die geavanceerde wachtrijen en QoS-mechanismen (WFQ, CBWFQ, enzovoort) kunnen bieden.

Dit voorbeeld gebruikt het hiërarchische QoS-beleid om al het uitgaande verkeer op de externe interface naar 2 Mbps te vormgeven zoals het vormende voorbeeld, maar het specificeert ook dat spraakpakketten met de DSCP-waarde (Differentiated Services Code Point), evenals het SSH-verkeer (Secure Shell), prioriteit zullen krijgen.

Maak de prioriteitswachtrij op de interface waarop u de functie wilt inschakelen:

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

Een klas die overeenkomt met DSCP ef:

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

Een klasse om port TCP/22 SSH-verkeer aan te passen:

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

Een beleidskaart om prioritering van spraak- en SSH-verkeer toe te passen:

```
   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
```

Een beleidskaart om het vormen op al verkeer toe te passen en prioritair spraak- en SSH-verkeer toe te voegen:

```
   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
```

Sluit tenslotte het vormingsbeleid aan op de interface waarop u uitgaande verkeer wilt vormgeven en prioriteren:

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

QoS voor verkeer via een VPN-tunnelbeheer

QoS met IPsec VPN

Volgens RFC 2401 worden de bits van het Type of Service (ToS) in de oorspronkelijke IP-header gekopieerd naar de IP-kop van het gecodeerde pakket, zodat het QoS-beleid na encryptie kan worden gehandhaafd. Dit laat de bits DSCP/DiffServ toe om voor prioriteit overal in het QoS-beleid te worden gebruikt.

Toezicht op een IPsec-tunnel

U kunt ook toezicht uitoefenen op specifieke VPN-tunnels. Om een tunnelgroep te selecteren waarop de politie moet optreden, gebruikt u de **match tunnel-groep <tunnel>** opdracht in uw class-map en de **match flow-ip** adresopdracht.

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

Invoertoezicht werkt niet op dit moment wanneer u de opdracht **lucifertunnelgroep** gebruikt; zie Cisco bug-ID CSCth48255 voor meer informatie. Als u probeert om invoercontrole met het IP bestemming-adres van de overeenkomende stroom uit te voeren, ontvangt u deze fout:

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

Toezicht ingangssignaal lijkt niet te werken op dit moment wanneer u **tunnelgroep** gebruikt (Cisco bug-ID CSCth48255). Als de input politiing werkt, zou u een class-map moeten gebruiken zonder het **overeenkomende stromen IP bestemming-adres**.

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

Als u probeert om output op een class-map te controleren die niet het **overeenkomende IP bestemmingsadres** heeft, ontvangt u:

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

Het is ook mogelijk om QoS op de binnenstroominformatie uit te voeren met het gebruik van Toegangscontrolelijsten (ACL's), DSCP, etc. Vanwege de eerder genoemde bug zijn ACL's nu de manier om invoercontrole te doen.

> **Opmerking:** Een maximum van 64 beleidskaarten kan op alle platformtypes worden gevormd. Gebruik verschillende class-maps binnen de beleidskaarten om verkeer te segmenteren.

QoS met Secure Socket Layer (SSL) VPN

Tot ASA versie 9.2, behoudt de ASA de ToS bits niet.

SSL VPN-tunneling wordt niet ondersteund met deze functionaliteit. Zie Cisco bug-ID CSCsl73211 voor meer informatie.

```
   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)#
```

> **Opmerking:** Wanneer gebruikers met telefoon-VPN de AnyConnect-client en Datagram Transport Layer Security (DTLS) gebruiken om hun telefoon te versleutelen, werkt prioritering niet omdat AnyConnect de DSCP-vlag in de DTLS-insluiting niet bewaart. Raadpleeg een verzoek om versterking van CSCtq43909 voor meer informatie.

QoS-overwegingen

Hier zijn een paar punten om over QoS na te denken.

- Het wordt op strikte of hiërarchische wijze toegepast via het modulaire beleidskader: Toezicht, vormgeving, LLQ.

  Kan alleen verkeer beïnvloeden dat al van de Network Interface Card (NIC) naar de DP (Data Path) wordt doorgegevenGebruikt om overschrijdingen te bestrijden (ze gebeuren te vroeg), tenzij toegepast op een bijkomend apparaat

- Controle wordt toegepast op de invoer nadat het pakket is toegestaan en op de uitvoer vóór de NIC.

  Vlak nadat u een Layer 2 (L2) adres opnieuw schrijft op de uitvoer

- Het vormt uitgaande bandbreedte voor al het verkeer op een interface.

  Handig met beperkte uplink-bandbreedte (zoals 1 Gigabit Ethernet (GE)-link naar 10MB-modem)Niet ondersteund op hoogwaardige ASA 558x-modellen

- Prioritaire wachtrijen kunnen het best-inspanningsverkeer verhongeren.

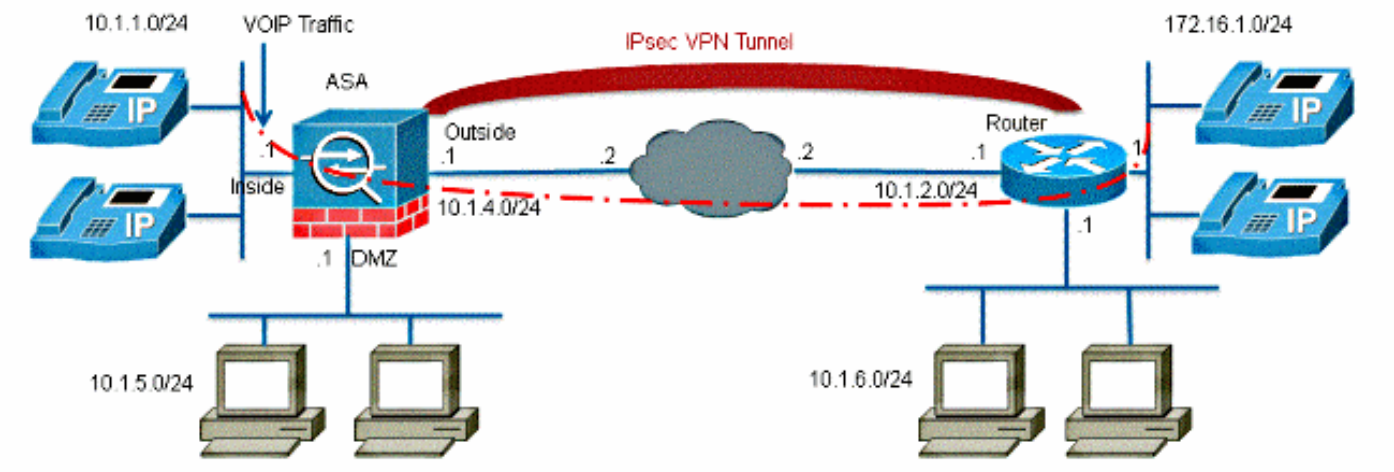
  Niet ondersteund op 10 GE interfaces op ASA 5580 of VLAN-subinterfacesDe grootte van de interfacekring kan verder worden afgestemd op optimale prestaties

Configuratievoorbeelden

QoS voor VoIP Traffic Engineering van VPN-tunnels

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: Zorg ervoor dat IP-telefoons en hosts in verschillende segmenten (subnetwerken) worden geplaatst. Dit wordt aanbevolen voor een goed netwerkontwerp.

Dit document gebruikt deze configuraties:

- QoS-configuratie gebaseerd op DSCP
- QoS gebaseerd op DSCP met VPN-configuratie
- QoS-configuratie gebaseerd op ACL
- QoS gebaseerd op ACL's met VPN-configuratie

QoS-configuratie gebaseerd op 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
```

Opmerking: De DSCP waarde van "ef" verwijst naar versnelde verzending die overeenkomt met het VoIP-RTP-verkeer.

QoS gebaseerd op DSCP met VPN-configuratie

```
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
```

QoS-configuratie gebaseerd op 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 op basis van ACL met VPN-configuratie

```
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
```

> **Opmerking:** Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten in deze sectie.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

politie van het televisiebeleid

Om de QoS statistieken voor het verkeer te bekijken, gebruikt u de opdracht **showservice-beleid** met het **politie-**sleutelwoord:

```
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
```

prioriteit van het dienstbeleid tonen

Om statistieken voor dienstenbeleid te bekijken dat het **prioritaire** bevel uitvoert, gebruik de **show service-beleid** bevel met het **prioritaire** sleutelwoord:

```
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
```

vorm van het dienstverleningsbeleid

```
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
```

statistieken over prioriteitswachtrij tonen

Om de prioriteitswachtrij statistieken voor een interface weer te geven, gebruikt u de opdracht **Statistieken** met **prioriteit** in een bevoorrechte EXEC-modus. De resultaten tonen de statistieken voor zowel de best-inspanning (BE) wachtrij als de LLQ. Dit voorbeeld toont het gebruik van het bevel van de **tonen prioriteit-rij statistiek** voor de interface die buiten wordt genoemd, en de opdrachtoutput.

```
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 dit statistische rapport wordt de betekenis van de posten als volgt gedefinieerd:

- "Packets Dropped" verwijst naar het totale aantal pakketten dat in deze wachtrij is gevallen.
- "Packets Transmit" staat voor het totale aantal pakketten dat in deze wachtrij is verzonden.
- "Packets Enwachtrij" staat voor het totale aantal pakketten dat in deze wachtrij is geplaatst.
- "Huidige lengte van Q" verwijst naar de huidige diepte van deze wachtrij.
- "Max. lengte Q" betekent de maximale diepte die ooit in deze rij is voorgekomen.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Aanvullende informatie

Hier zijn een aantal insecten die door de verkeersafdeling worden geïntroduceerd:

Cisco bug-ID CSCsq08550	Traffic Shaping met prioriteitswachtrij veroorzaakt verkeerstekorten op ASA
Cisco bug-id CSCsx07862	Traffic Shaping met prioriteitswachtrij zorgt voor pakketvertraging en -druppels
Cisco bug-id CSCsq07395	Het toevoegen van vormgeving van het servicebeleid mislukt als de beleidskaa bewerkt

FAQ

Deze paragraaf geeft een antwoord op een van de meest gestelde vragen met betrekking tot de in dit document beschreven informatie.

Worden QoS-markeringen bewaard wanneer de VPN-tunnel werd overgelopen?

Ja. De QoS-markeringen worden in de tunnel bewaard omdat ze door de providernetwerken lopen als de provider ze niet op doorreis haalt.

> **Tip**: Raadpleeg het gedeelte DSCP en DiffServ-behoud van het *CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.2* voor meer informatie.

Gerelateerde informatie

- Cisco ASA Series Firewallconfiguratie CLI, Quality-of-Service
- QoS-beleid toepassen
- De betekenis van functies die niet worden ondersteund in Clientloze SSL VPN
- QoS configureren
- Technische ondersteuning en documentatie – Cisco Systems