

Configure Quality of Service on Adaptive Security Appliance

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Traffic Policing](#)

[Traffic Shaping](#)

[Priority Queueing](#)

[QoS For Traffic Through a VPN Tunnel](#)

[QoS with IPsec VPN](#)

[Policing on an IPsec Tunnel](#)

[QoS with Secure Sockets Layer \(SSL\) VPN](#)

[QoS Considerations](#)

[Configuration Examples](#)

[QoS for VoIP Traffic on VPN Tunnels Configuration Example](#)

[Network Diagram](#)

[QoS Configuration Based on DSCP](#)

[QoS Based on DSCP with VPN Configuration](#)

[QoS Configuration Based on ACL](#)

[QoS Based on ACL with VPN Configuration](#)

[Verify](#)

[show service-policy police](#)

[show service-policy priority](#)

[show service-policy shape](#)

[show priority-queue statistics](#)

[Troubleshoot](#)

[Additional Information](#)

[FAQ](#)

[Are QoS markings preserved when the VPN tunnel is traversed?](#)

[Related Information](#)

Introduction

This document describes how Quality of Service (QoS) works on Cisco Adaptive Security Appliance and also provides examples on how to implement it.

Prerequisites

Requirements

Cisco recommends that you have knowledge of [Modular Policy Framework \(MPF\)](#).

Components Used

The information in this document is based on an Adaptive Security Appliance (ASA) that runs Version 9.2, but earlier versions can be used as well.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

You can configure QoS on the security appliance in order to provide rate limiting on selected network traffic for both individual flows and VPN tunnel flows, in order to ensure that all traffic gets its fair share of limited bandwidth. The feature was integrated with Cisco bug ID [CSCsk06260](#).

QoS is a network feature that allows you to give priority to certain types of Internet traffic. As Internet users upgrade their access points from modems to high-speed broadband connections like Digital Subscriber Line (DSL) and cable, the likelihood increases that at any given time, a single user is able to absorb most, if not all, of the available bandwidth, thus starving the other users. In order to prevent any one user or site-to-site connection from consuming more than its fair share of bandwidth, QoS provides a policing feature that regulates the maximum bandwidth that any user can use.

QoS refers to the capability of a network to provide better service to selected network traffic over various technologies for the best overall services with limited bandwidth of the underlying technologies.

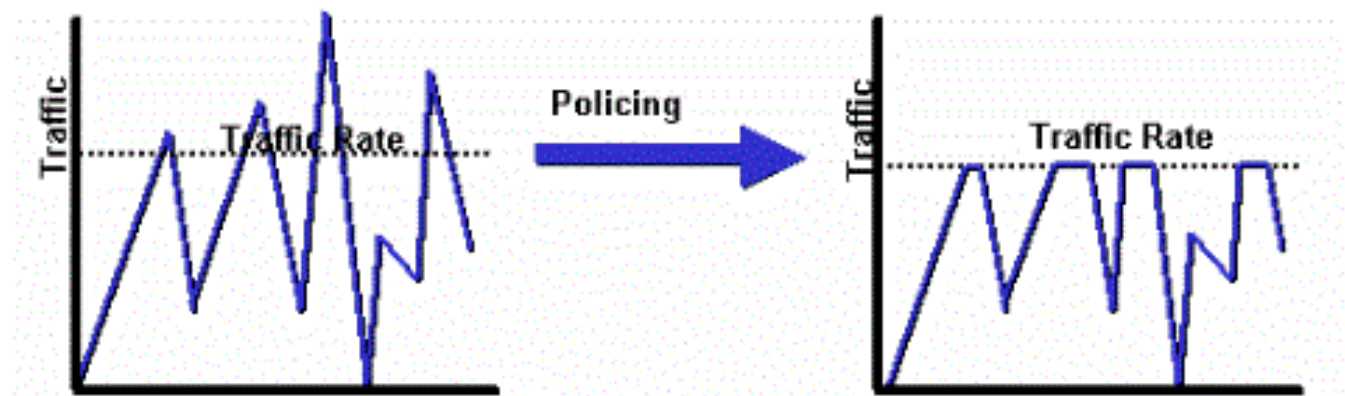
The primary goal of QoS in the security appliance is to provide rate limiting on selected network traffic for both individual flow or VPN tunnel flow to ensure that all traffic gets its fair share of limited bandwidth. A flow can be defined in a number of ways. In the security appliance, QoS can apply to a combination of source and destination IP addresses, source and destination port number, and the Type of Service (ToS) byte of the IP header.

There are three kinds of QoS you can implement on the ASA: Policing, Shaping, and Priority Queueing.

Traffic Policing

With policing, traffic over a specified limit is dropped. Policing is a way to ensure that no traffic exceeds the maximum rate (in bits/second) that you configure, which ensures that no one traffic flow or class can take over the entire resource. When traffic exceeds the maximum rate, the ASA drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

This diagram illustrates what traffic policing does when the traffic rate reaches the configured maximum rate, excess traffic is dropped. The result is an output rate that appears as a saw-tooth with crests and troughs.



This example shows how to throttle the bandwidth to 1 Mbps for a specific user in the outbound direction:

```

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

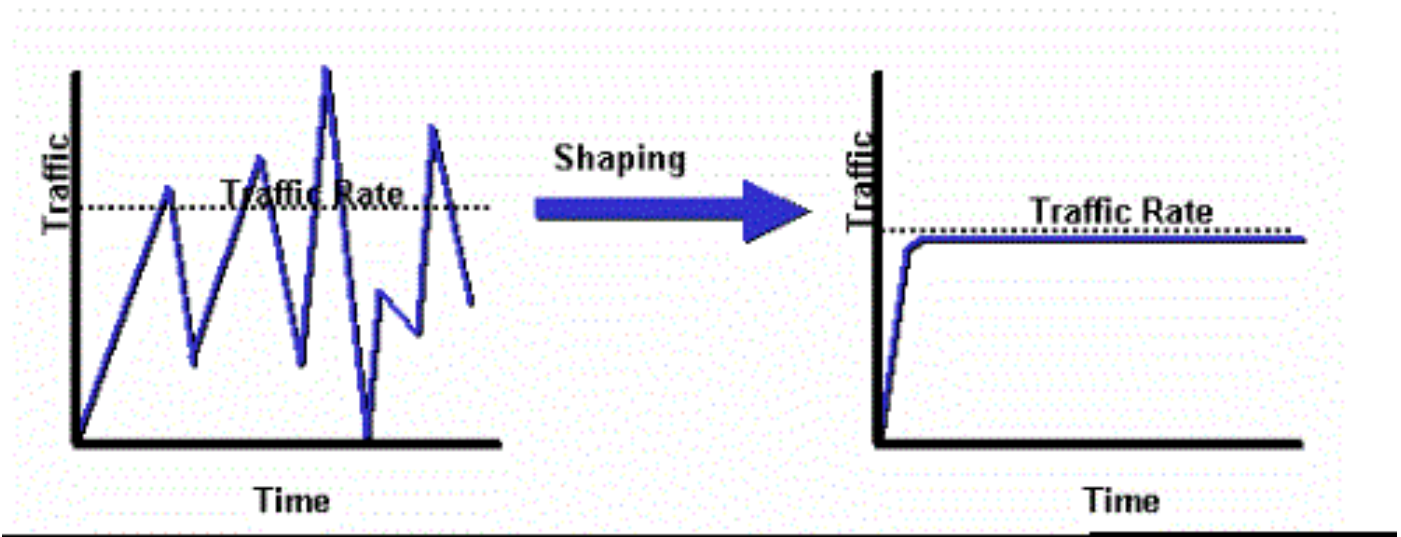
```


Traffic Shaping

Traffic shaping is used in order to match device and link speeds, which controls packet loss, variable delay, and link saturation, which can cause jitter and delay. Traffic shaping on the security appliance allows the device to limit the flow of traffic. This mechanism buffers traffic over the speed limit, and attempts to send the traffic later.

Shaping cannot be configured for certain types of traffic. The shaped traffic includes traffic passing through the device, as well as traffic that is sourced from the device.

This diagram illustrates what traffic shaping does; it retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate.




 **Note:** Traffic shaping is only supported on ASA Versions 5505, 5510, 5520, 5540, and 5550. Multicore models (such as the 5500-X) do not support shaping.

With traffic shaping, traffic that exceeds a certain limit is queued (buffered) and sent during the next timeslice.


Traffic shaping on the firewall is most useful if an upstream device imposes a bottleneck on network traffic. A good example would be an ASA that has 100 Mbit interfaces, with an upstream connection to the Internet via a cable modem or T1 that terminates on a router. Traffic shaping allows the user to configure the maximum outbound throughput on an interface (the outside interface for example); the firewall transmits traffic out of that interface up to the specified bandwidth, and then attempts to buffer the excessive traffic for transmission later when the link is less saturated.

Shaping is applied to all aggregate traffic that egresses the specified interface. You cannot choose to only shape certain traffic flows.

 **Note:** Shaping is done after encryption and does not allow for prioritization on the inner packet or tunnel-group basis for VPN.

Priority Queuing


With priority queuing, you are able to place a specific class of traffic in the Low Latency Queue (LLQ), which is processed before the standard queue.

 **Note:** If you prioritize traffic under a shaping policy, you cannot use inner packet details. The firewall can only perform LLQ, unlike the routers that can provide more sophisticated queuing and QoS mechanisms (Weighted Fair Queueing (WFQ), Class-Based Weighted Fair Queueing (CBWFQ), and so on).

The hierarchical QoS policy provides a mechanism for users to specify the QoS policy in a hierarchical fashion. For example, if users want to shape traffic on an interface and furthermore within the shaped interface traffic, provide priority queuing for VoIP traffic, then users can specify a traffic shaping policy at the top and a priority queuing policy under the shape policy. The hierarchical QoS policy support is limited in scope.

The only options allowed are:

- Traffic shaping at the top level.
- Priority queueing at the next level.

 **Note:** If you prioritize traffic under a shaping policy, you cannot use inner packet details. The firewall can only perform LLQ, unlike the routers that can provide more sophisticated queuing and QoS mechanisms (WFQ, CBWFQ, and so on).

This example uses the hierarchical QoS Policy in order to shape all outbound traffic on the outside interface to 2 Mbps like the shaping example, but it also specifies that Voice packets with the Differentiated Services Code Point (DSCP) value ef, as well as Secure Shell (SSH) traffic, shall receive priority.

Create the priority queue on the interface on which you want to enable the feature:

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

A class to match DSCP ef:

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

A class to match port TCP/22 SSH traffic:

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

A policy map to apply prioritization of Voice and SSH traffic:

```
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
```

A policy map to apply shaping to all traffic and attach prioritized Voice and SSH traffic:

```
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
```

Finally, attach the shaping policy to the interface on which to shape and prioritize outbound traffic:

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

QoS For Traffic Through a VPN Tunnel

QoS with IPsec VPN

As per [RFC 2401](#) Type of Service (ToS) bits in the original IP header are copied to the IP header of the encrypted packet so that QoS policies can be enforced after encryption. This allows the DSCP/DiffServ bits to be used for priority anywhere in the QoS policy.

Policing on an IPsec Tunnel

Policing can also be done for specific VPN tunnels. In order to select a tunnel-group on which to police, you use the **match tunnel-group <tunnel>** command in your class-map and the **match flow ip destination address** command.

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

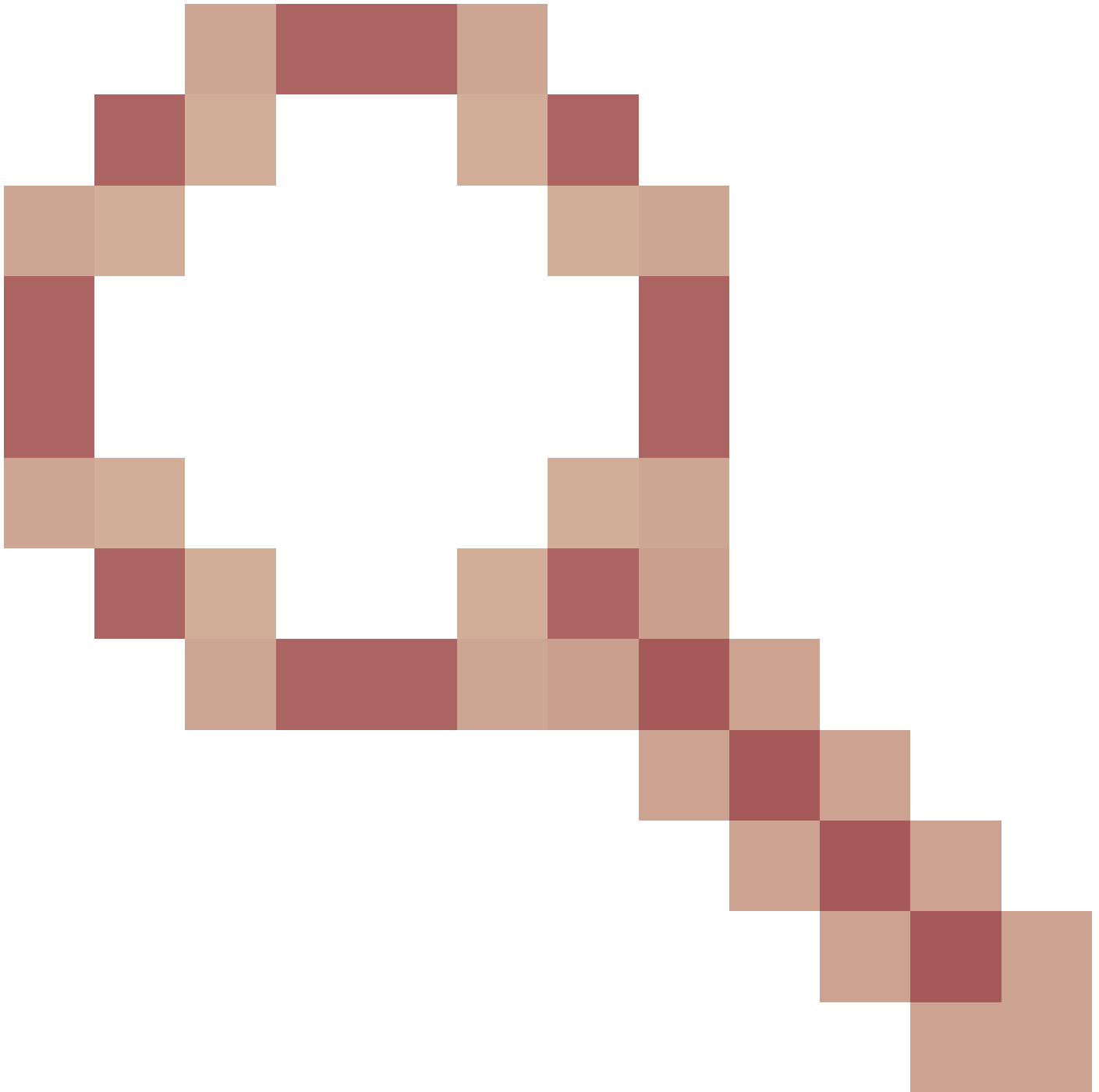
Input policing does not work at this time when you use the **match tunnel-group** command; see Cisco bug ID [CSCth48255](#) for more information. If you try to do input policing with the **match flow ip destination-address**, you receive this error:

```
<#root>
```

```
  police input 10000000
  ERROR:
```

Input policing cannot be done on a flow destination basis

Input policing does not appear to work at this time when you use **match tunnel-group** (Cisco bug ID [CSCth48255](#)).



If input policing works, you would need to use a class-map without the match flow ip destination-address address.

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


If you try to police output on a class-map that does not have the match ip destination address, you receive:

<#root>

```
police output 10000000
ERROR:
```

tunnel-group can only be policed on a flow basis

It is also possible to perform QoS on the inner flow information with the use of Access Control Lists (ACLs), DSCP, and so on. Due to the previously mentioned bug, ACLs are the way to be able to do input policing right now.

 **Note:** A maximum of 64 policy-maps can be configured on all platform types. Use different class-maps within the policy-maps in order to segment traffic.


QoS with Secure Sockets Layer (SSL) VPN

Until ASA Version 9.2, the ASA did not preserve the ToS bits.

SSL VPN tunneling is not supported with this functionality. See Cisco bug ID [CSCs173211](#) for more information.

```
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)#
```

 **Note:** When users with phone-vpn use the AnyConnect client and Datagram Transport Layer Security (DTLS) to encrypt their phone, prioritization does not work because AnyConnect does not preserve the DSCP flag in the DTLS encapsulation.

Refer to enhancement request Cisco bug ID [CSCtq43909](#) for details.

QoS Considerations

Here are some points to consider about QoS.

- It is applied through Modular Policy Framework (MPF) in strict or hierarchical fashion: Policing, Shaping, LLQ.
- Can only influence traffic that is already passed from the Network Interface Card (NIC) to the DP (Data Path).
- Useless to fight overruns (they happen too early) unless applied on an adjacent device.

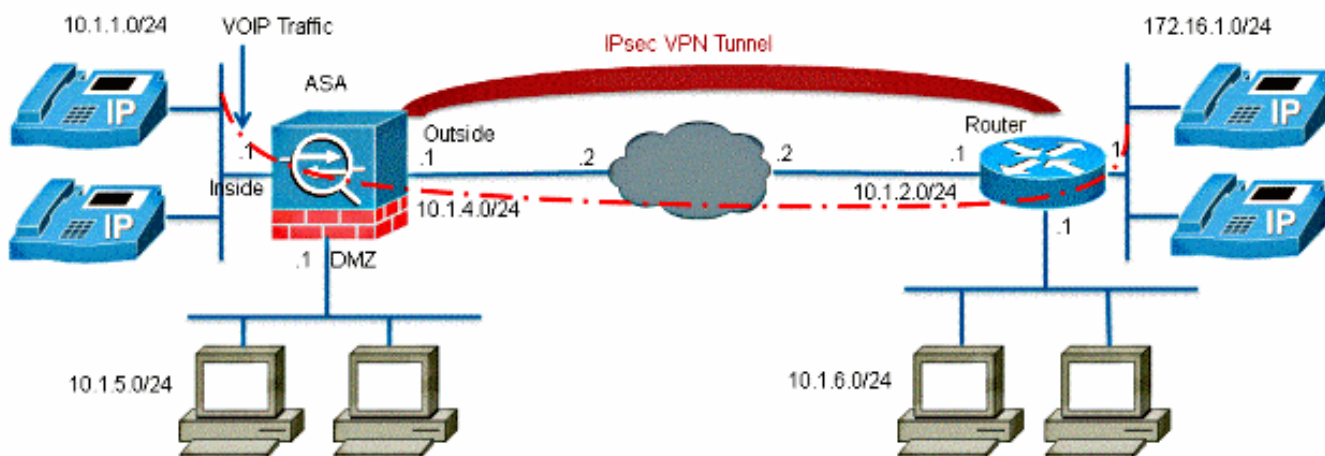
- Policing is applied on the input after the packet is permitted, and on the output before the NIC.
- Right after you rewrite a Layer 2 (L2) address on the output.
- It shapes outbound bandwidth for all traffic on an interface.
- Useful with limited uplink bandwidth (such as 1 Gigabit Ethernet (GE) link to 10Mb modem).
- Not supported on high-performance ASA558x models.
- Priority queuing can starve best-effort traffic.
- Not supported on 10GE interfaces on ASA5580 or VLAN subinterfaces.
- Interface ring size can be further tuned for optimal performance.

Configuration Examples

QoS for VoIP Traffic on VPN Tunnels Configuration Example

Network Diagram

This document uses this network setup:



Note: Ensure that IP phones and hosts are placed in different segments (subnets). This is recommended for a good network design.

This document uses these configurations:

- QoS Configuration Based on DSCP
- QoS Based on DSCP with VPN Configuration
- QoS Configuration Based on ACL
- QoS Based on ACL with VPN Configuration

QoS Configuration Based on 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
```



Note: The DSCP value of ef refers to expedited forwarding that matches VoIP-RTP traffic.

QoS Based on DSCP with VPN Configuration

<#root>

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 Configuration Based on 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 Based on ACL with VPN Configuration

```
<#root>
```

```
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
```

 **Note:** Use the [Command Lookup Tool](#) ([registered](#) customers only) in order to obtain more information the commands used in this section.

Verify

Use this section in order to confirm that your configuration works properly.

show service-policy police

In order to view the QoS statistics for traffic policing, use the **show service-policy** command with the **police** keyword:

```
<#root>
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

In order to view statistics for service policies that implement the **priority** command, use the **show service-policy** command with the **priority** keyword:

```
<#root>
```

```
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

```
<#root>
```

```
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

In order to display the priority-queue statistics for an interface, use the **show priority-queue statistics** command in privileged EXEC mode. The results show the statistics for both the best-effort (BE) queue and the LLQ. This example shows the use of the **show priority-queue statistics** command for the interface named outside, and the command output.

```
<#root>
```

```
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 this statistical report, the meaning of the line items is as follows:

- Packets Dropped denotes the overall number of packets that have been dropped in this queue.
- Packets Transmit denotes the overall number of packets that have been transmitted in this queue.
- Packets Enqueued denotes the overall number of packets that have been queued in this queue.
- Current Q Length denotes the current depth of this queue.
- Max Q Length denotes the maximum depth that ever occurred in this queue.

The [Output Interpreter Tool](#) (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Additional Information

Here are some bugs introduced by the traffic shaping feature:

Cisco bug ID CSCsq08550	Traffic shaping with priority queueing causes traffic failure on ASA.
Cisco bug ID CSCsx07862	Traffic shaping with priority queueing causes packet delay and drops.
Cisco bug ID CSCsq07395	Adding shaping service-policy fails if policy-map has been edited.

FAQ

This section provides an answer to one of the most frequently asked questions in regards to the information that is described in this document.

Are QoS markings preserved when the VPN tunnel is traversed?

Yes. The QoS markings are preserved in the tunnel as they traverse the provider networks if the provider does not strip them in transit.



Tip: Refer to the [DSCP and DiffServ Preservation](#) section of the CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.2 for more details.

Related Information

- [Cisco ASA Series Firewall CLI configuration Guide, Quality of Service](#)

- [Applying QoS Policies](#)
- [Technical Support & Documentation - Cisco Systems](#)