



## IPsec and Quality of Service

---

The IPsec and Quality of Service feature allows Cisco IOS quality of service (QoS) policies to be applied to IP Security (IPsec) packet flows on the basis of a QoS group that can be added to the current Internet Security Association and Key Management Protocol (ISAKMP) profile.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for IPsec and Quality of Service, page 1](#)
- [Restrictions for IPsec and Quality of Service, page 2](#)
- [Information About IPsec and Quality of Service, page 2](#)
- [How to Configure IPsec and Quality of Service, page 2](#)
- [Configuration Examples for IPsec and Quality of Service, page 4](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)

## Prerequisites for IPsec and Quality of Service

- You should be familiar with IPsec and the concept of ISAKMP profiles.
- You should be familiar with Cisco IOS QoS.



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

## Restrictions for IPsec and Quality of Service

- This feature can be applied only via the ISAKMP profile. The limit of 128 QoS groups that exists for QoS applications applies to this feature as well.
- You can apply an IPsec QoS group only to outbound service policies.
- QoS is not supported for software encryption.

## Information About IPsec and Quality of Service

To configure the IPsec and Quality of Service feature, you should understand the following concept:

- [IPsec and Quality of Service Overview, page 2](#)

## IPsec and Quality of Service Overview

The IPsec and Quality of Service feature allows you to apply QoS policies, such as traffic policing and shaping, to IPsec-protected packets by adding a QoS group to ISAKMP profiles. After the QoS group has been added, this group value will be mapped to the same QoS group as defined in QoS class maps. Any current QoS method that makes use of this QoS group tag can be applied to IPsec packet flows. Common groupings of packet flows can have specific policy classes applied by having the IPsec QoS group made available to the QoS mechanism. Marking IPsec flows allows QoS mechanisms to be applied to classes of traffic that could provide support for such things as restricting the amount of bandwidth that is available to specific groups or devices or marking the type of service (ToS) bits on certain flows.

The application of the QoS group is applied at the ISAKMP profile level because it is the profile that can uniquely identify devices through its concept of match identity criteria. These criteria are on the basis of the Internet Key Exchange (IKE) identity that is presented by incoming IKE connections and includes such things as IP address, fully qualified domain name (FQDN), and group (that is, the virtual private network [VPN] remote client grouping). The granularity of the match identity criteria will impose the granularity of the specified QoS policy, for example, to mark all traffic belonging to the VPN client group named “Engineering” as “TOS 5”. Another example of having the granularity of a specified QoS policy imposed would be to allocate 30 percent of the bandwidth on an outbound WAN link to a specific group of remote VPN devices.

## How to Configure IPsec and Quality of Service

This section includes the following procedures:

- [Configuring IPsec and Quality of Service, page 2](#) (required)
- [Verifying IPsec and Quality of Service Sessions, page 3](#) (optional)
- [Troubleshooting Tips, page 4](#) (optional)

## Configuring IPsec and Quality of Service

To apply QoS policies to an ISAKMP profile, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp-profile** *profile-name*
4. **qos-group** *group-number*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto isakmp-profile</b> <i>profile-number</i>  <b>Example:</b> Router (config)# crypto isakmp-profile vpnprofile	Defines an ISAKMP profile, audits IPsec user sessions, and enters ISAKMP profile configuration mode.
Step 4	<b>qos-group</b> <i>group-number</i>  <b>Example:</b> Router(config-isa-prof)# qos-group 1	Applies a QoS group value to an ISAKMP profile.

## Verifying IPsec and Quality of Service Sessions

To verify your IPsec and QoS sessions, perform the following steps. The **show** commands can be used in any order or independent of each other.

## SUMMARY STEPS

1. **enable**
2. **show crypto isakmp profile**
3. **show crypto ipsec sa**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<code>show crypto isakmp profile</code>  <b>Example:</b> Router# show crypto isakmp profile	Shows that the QoS group is applied to the profile.
<b>Step 3</b>	<code>show crypto ipsec sa</code>  <b>Example:</b> Router# show crypto ipsec sa	Shows that the QoS group is applied to a particular pair of IPsec security associations (SAs).

**Troubleshooting Tips**

If you have a problem with your IPsec and QoS sessions, ensure that you have done the following:

- Validated the application of QoS by the QoS service using the QoS-specific commands in the [Cisco IOS Quality of Service Solutions Command Reference](#).
- Configured a QoS policy on the router that matches the same QoS group as that specified for the class map match criterion.
- Applied the service policy to the same interface to which a crypto map is applied.

**Configuration Examples for IPsec and Quality of Service**

This section provides the following output examples:

- [QoS Policy Applied to Two Groups of Remote Users: Example, page 4](#)
- [show crypto isakmp profile Command: Example, page 6](#)
- [show crypto ipsec sa Command: Example, page 6](#)

**QoS Policy Applied to Two Groups of Remote Users: Example**

In the following example, a specific QoS policy is applied to two groups of remote users. Two ISAKMP profiles are configured so that upon initial connection via IKE, remote users are mapped to a specific profile. From that profile, all IPsec SAs that have been created for that remote will be marked with the specific QoS group. As traffic leaves the outbound interface, the QoS service will map the IPsec set QoS group with the QoS group that is specified in the class maps that comprise the service policy that is applied on that outbound interface.

```
version 12.3
!
aaa authentication login group group radius
aaa authorization network autho local
aaa accounting update periodic 1
```

```
aaa session-id common
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
class-map match-all yellow
  match qos-group 3
class-map match-all blue
  match qos-group 2
!
!
policy-map clients
  class blue
    set precedence 5
  class yellow
    set precedence 7
!
!
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
  lifetime 300
!
crypto isakmp keepalive 10 periodic
crypto isakmp xauth timeout 20
!
crypto isakmp client configuration group blue
  key cisco
  dns 10.2.2.2 10.2.2.3
  wins 10.6.6.6
  pool blue
  save-password
  include-local-lan
  backup-gateway corkyl.cisco.com
!
crypto isakmp client configuration group yellow
  dns 10.2.2.2 10.2.2.3
  wins 10.6.6.5
  pool yellow
!
crypto isakmp profile blue
  match identity group cisco
  client authentication list autho
  isakmp authorization list autho
  client configuration address respond
  qos-group 2
crypto isakmp profile yellow
  match identity group yellow
  match identity address 10.0.0.11 255.255.255.255
  client authentication list autho
  isakmp authorization list autho
  client configuration address respond
  qos-group 3
!
!
crypto ipsec transform-set combo ah-sha-hmac esp-3des esp-sha-hmac
crypto ipsec transform-set client esp-3des esp-sha-hmac comp-lzs
!
crypto dynamic-map mode 1
  set security-association lifetime seconds 180
```

```

set transform-set client
set isakmp-profile blue
reverse-route
crypto dynamic-map mode 2
set transform-set combo
set isakmp-profile yellow
reverse-route
!
crypto map mode 1 ipsec-isakmp dynamic mode
!
interface FastEthernet0/0
ip address 10.0.0.110 255.255.255.0
no ip redirects
no ip proxy-arp
no ip mroute-cache
duplex half
no cdp enable
crypto map mode
service-policy out clients
!
ip local pool yellow 192.168.2.1 192.168.2.10
ip local pool blue 192.168.6.1 192.168.6.6
no ip classless
!
radius-server host 10.0.0.13 auth-port 1645 acct-port 1646
radius-server key XXXXXX
radius-server vsa send accounting
radius-server vsa send authentication

```

## show crypto isakmp profile Command: Example

The following output shows that QoS group “2” has been applied to the ISAKMP profile “blue” and that QoS group “3” has been applied to the ISAKMP profile “yellow”:

```

Router# show crypto isakmp profile

ISAKMP PROFILE blue
  Identities matched are:
    group blue
  QoS Group 2 is applied

ISAKMP PROFILE yellow
  Identities matched are:
    ip-address 10.0.0.13 255.255.255.255
    group yellow
  QoS Group 3 is applied

```

## show crypto ipsec sa Command: Example

The following output shows that the QoS group has been applied to a particular pair of IPsec SAs:

```

Router# show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: mode, local addr. 10.0.0.110

protected vrf:
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.12.12.0/255.255.255.0/0/0)
  current_peer: 10.0.0.11:500

```

```

PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

      qos group is set to 2

```

## Additional References

The following sections provide references related to the IPsec and Quality of Service feature.

### Related Documents

Related Topic	Document Title
IPsec	<a href="#">Configuring Security for VPNs with IPsec</a>
QoS options	Cisco IOS Quality of Service Solutions Configuration Guide on Cisco.com
QoS commands	<a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>
Security commands	<a href="#">Cisco IOS Security Command Reference</a>

### Standards

Standards	Title
No new or modified standards are supported by this feature.	—

### MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# Feature Information for IPsec and Quality of Service

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

**Table 1** Feature Information for IPsec and Quality of Service

Feature Name	Releases	Feature Information
IPsec and Quality of Service	12.3(8)T	<p>The IPsec and Quality of Service feature allows Cisco IOS quality of service (QoS) policies to be applied to IP Security (IPsec) packet flows on the basis of a QoS group that can be added to the current Internet Security Association and Key Management Protocol (ISAKMP) profile.</p> <p>In Cisco IOS Release 12.3(8)T, this feature was introduced.</p> <p>The following commands were introduced or modified:  <b>qos-group.</b></p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009–2010 Cisco Systems, Inc. All rights reserved.

