

Configuring CBWFQ for IPsec VPN

Introduction

This document describes how to configure Quality of Service (QoS) for traffic between a Hub router (Cisco 7200 Series Router) and a spoke router (Cisco 3745 Router). The QoS policy is enabled on the public interface, and it examines the traffic before being encrypted. The policy is configured using the Modular Quality of Service Command Line Interface (MQC).

Prerequisites

The sample QoS configuration is based on the following assumptions:

- The IPsec peer destination address is usually static, but could be dynamic.
- The QoS policy is required only on the outbound.
- There are defined network addresses or applications for CBWFQ classification.

Components Used

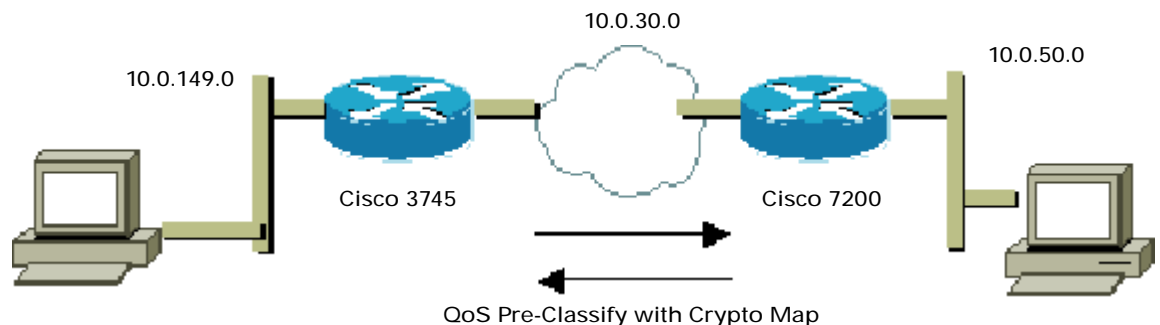
The sample configuration uses the following releases of the software and hardware:

- Cisco 7200 with Cisco IOS® Software Release 12.2(13)T (C7200-IK9O3S-M)
- Cisco 3745 with Cisco IOS® Software Release 12.2(8)T5 (C3745-JK9S-M)

Figure 1 illustrates the network for the sample configuration.

The information presented in this document was created from devices in a specific lab environment. All of the devices started with a cleared (default) configuration. If you are working in a live network, it is imperative to understand the potential impact of any command before implementing it.

Figure 1
 Network Diagram





QoS Configuration Options

The sample configuration minimizes bandwidth guarantees and maximizes bandwidth policing. Additional QoS features that can be used in the policy map include low latency queuing, traffic shaping, and random early detection.

In the sample configuration, the class-map matches the original unencrypted packets. To match the unencrypted packet, you use the qos-preclassify command as documented in the [QoS for Virtual Private Networks](#). The matching for the traffic is made with the ACL. Any of the unencrypted packet information specified in the ACL can be used for matching a specific class and applying a different service policy to different classes for the outbound traffic.

The service policy can be applied on the input or on the output of the public or private interface of both routers. The sample configuration shows the service policy applied to output traffic on the hub and the spoke router.

For additional information about configuring QoS, refer to [Cisco IOS Quality of Service Solutions Configuration Guide](#).

Cisco 7200 VPN Router Configuration

```
!  
version 12.2  
service timestamps debug datetime  
service timestamps log datetime  
no service password-encryption  
!  
hostname "c7200-12"  
!  
ip subnet-zero  
ip cef  
!  
class-map match-any sitel  
  match access-group 120  
!  
!  
policy-map output  
  class sitel  
    bandwidth 200  
    police cir 5000000  
!  
!  
crypto isakmp policy 1  
  authentication pre-share  
  group 2  
crypto isakmp key bigsecret address 10.0.30.245  
!  
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac  
!  
crypto map static-crypt 6 ipsec-isakmp  
  set peer 10.0.30.245  
  set transform-set vpn-test  
  match address 101  
  qos pre-classify  
!  
controller ISA 6/1  
!  
!  
interface FastEthernet0/0
```



```
ip address 10.0.30.212 255.255.255.0
duplex full
service-policy output output
crypto map static-crypt
!
interface FastEthernet1/0
ip address 10.0.50.212 255.255.255.0
ip accounting output-packets
duplex full
!
ip classless
ip route 10.0.149.0 255.255.255.0 10.0.30.245
!
!
access-list 101 permit ip 10.0.50.0 0.0.0.255 10.0.149.0 0.0.0.255
access-list 120 permit ip 10.0.50.0 0.0.0.255 10.0.149.0 0.0.0.255
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
end
```

Configuring the Cisco 3745 VPN Router

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c3745-20
!
ip subnet-zero
!
!
class-map match-any hub
  match access-group 120
!
policy-map mqcp
  class hub
    bandwidth 200
    police cir 5000000
!
!
crypto isakmp policy 1
  authentication pre-share
  group 2
crypto isakmp key bigsecret address 10.0.30.212
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto map test 1 ipsec-isakmp
  set peer 10.0.30.212
```



```
set transform-set vpn-test
match address 101
qos pre-classify
!
interface FastEthernet0/0
ip address 10.0.149.220 255.255.255.0
load-interval 30
speed 100
full-duplex
!
interface FastEthernet0/1
ip address 10.0.30.245 255.255.255.0
speed 100
full-duplex
service-policy output mqcp
crypto map test
!
ip classless
ip route 10.0.50.0 255.255.255.0 10.0.30.212
!
access-list 101 permit ip 10.0.149.0 0.0.0.255 10.0.50.0 0.0.0.255
access-list 120 permit ip 10.0.149.0 0.0.0.255 10.0.50.0 0.0.0.255
!
line con 0
exec-timeout 60 0
line aux 0
line vty 0 4
login
!
end
```

Verifying the Results

This section provides information you can use to confirm that your configuration is working properly.

```
c3745-20#show policy-map
```

```
Policy Map mqcp
Class hub
  Weighted Fair Queueing
    Bandwidth 200 (kbps) Max Threshold 64 (packets)
  police cir 5000000 bc 156250
    conform-action transmit
    exceed-action drop
```

```
c3745-20#show policy-map interface fastEthernet 0/1
FastEthernet0/1
```

```
Service-policy output: mqcp
```

```
Class-map: hub (match-any)
  4605058 packets, 2567115168 bytes
  30 second offered rate 9550000 bps, drop rate 0 bps
Match: access-group 120
  3884074 packets, 2141735456 bytes
  30 second rate 9550000 bps
```



```
Weighted Fair Queueing
Output Queue: Conversation 265
Bandwidth 200 (kbps) Max Threshold 64 (packets)
(pkts matched/bytes matched) 2044996/1186842912
(depth/total drops/no-buffer drops) 0/0/0
police:
  cir 5000000 bps, bc 156250 bytes
conformed 2230228 packets, 1237348128 bytes; actions:
  transmit
exceeded 2374831 packets, 1329767552 bytes; actions:
  drop
  conformed 4999000 bps, exceed 4550000 bps,
```

```
Class-map: class-default (match-any)
  532380 packets, 313976237 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
c3745-20#show access-list
Extended IP access list 101
  permit ip 10.0.149.0 0.0.0.255 10.0.50.0 0.0.0.255 (4227393 matches)
Extended IP access list 120
  permit ip 10.0.149.0 0.0.0.255 10.0.50.0 0.0.0.255 (3887076 matches)
```

Troubleshooting the Configuration

Certain show commands are supported by the [Output Interpreter Tool](#) (registered customers only), which analyzes show command output.

Note: Before issuing debug commands, see [Important Information about Debug Commands](#).

- debug crypto isakmp—Displays errors during Phase 1.
- debug crypto ipsec—Displays errors during Phase 2.
- debug crypto engine—Displays information from the crypto engine.
- debug ip your routing protocol—Displays information about routing transactions of your routing protocol.
- clear crypto connection connection-id [slot | rsm | vip]—Terminates an encrypted session currently in progress. Encrypted sessions normally terminate when the session times out. Use the show crypto cisco connections command to see the connection-id value.
- clear crypto isakmp—Clears the Phase 1 security associations.
- clear crypto sa—Clears the Phase 2 security associations.



Related Information

[IPsec Support Page](#)

[An Introduction to IP Security \(IPsec\) Encryption](#)

[QoS for Virtual Private Networks](#)

[Configuring IPsec Network Security](#)

[Configuring Internet Key Exchange Security Protocol](#)

[Command Lookup Tool \(registered customers only\)](#)

[Technical Support - Cisco Systems](#)



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)