

Configuring Group Bandwidth Management with IPsec Easy VPN

Introduction

This document describes the Group Bandwidth Management configuration, which demonstrates how a system administrator sets a QoS service policy for groups. The system administrator specifies QoS parameters that are available for a group. Examples of the parameters are minimum bandwidth, traffic shaping, and the number of users admitted in a group. The system administrator administers the IP addresses allocated in the dynamic address pool, and then manages QoS for the group with a service policy. This scenario is applicable to the IPsec configuration with Easy VPN.

Prerequisites

The sample configuration is based on the following assumptions:

- Multiple groups access the Easy VPN Server.

- The QoS policy is assigned to the entire group.
- QoS management is configured only on the downstream at the hub.

Components Used

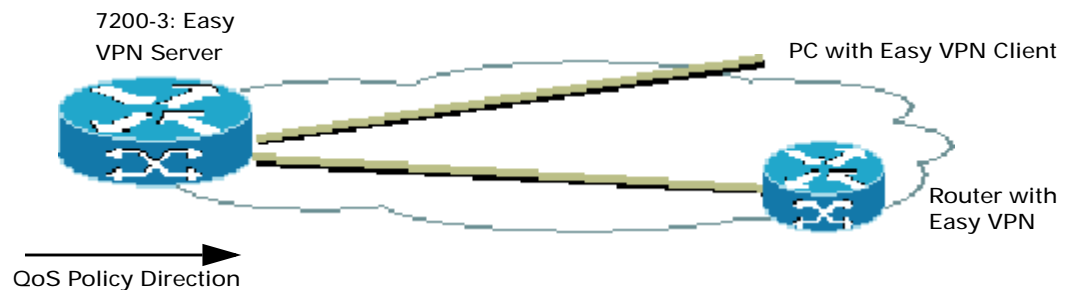
The sample configuration uses the following release of the software and hardware:

- Cisco 7200 with Cisco IOS® Software Release 12.2(13)T (C7200-IK9O3S-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





Group Bandwidth Configurations

The bandwidth policy is applied to each group, and users within a group share the service policy applied to the group. The sample configuration uses the service policy on the outbound of the interface.

Identify Users

Users are identified by their IP addresses. In an Easy VPN configuration, the addresses are dynamically allocated from an address pool. Each group needs to have a different address pool. The address range in the address pool identifies which group members have an ACL.

Forwarding QoS

Using policy-maps, the administrator can set the forwarding characteristics. The QoS policy supports configuring minimum bandwidth, policing, traffic shaping, weighted random early detection (WRED), low latency queuing, and marking of the packets. Users within a group share a specific service policy map. The sample configuration enables specific minimum bandwidth and traffic shaping for the groups.

Maximum Users in a Group

To limit the maximum number of connections in each group, configure the IP address pool with the required number of IP addresses. When all of the address pool is reserved, the connection to the Easy VPN Server fails during security policy negotiations, causing the Easy VPN client connection to fail or to try another Easy VPN Server if it is configured to do so.

Access Hours

Using the time range command option in the ACL, the router can activate a time range during which the Bandwidth management is allowed for a particular group. Based on the time of the day, ACLs get applied and a group member is allowed with the desired QoS.

Cisco 7200 Easy VPN Router Configuration

```
Cisco 7200 Router
Version 12.2(11)T
!
aaa new-model
!
!
aaa authentication login groupname local
aaa authentication login default local
aaa authorization network groupname local
aaa session-id common
!
username user1 password 0 test1111
username user2 password 0 test2222
username user3 password 0 test3333
username user4 password 0 test4444
username user5 password 0 test5555
!
class-map match-any group1
  match access-group 141
```



```
class-map match-any group2
  match access-group 142
class-map match-any group3
  match access-group 143
!
policy-map groupbwm
  class group1
    bandwidth percent 10
    shape peak 1000000
  class group2
    bandwidth percent 10
    shape peak 1000000
  class group3
    bandwidth percent 10
    shape peak 1000000
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key test1234 address 0.0.0.0 0.0.0.0
!
crypto isakmp client configuration group group1
  key testgroup1
  dns 171.70.168.183
  wins 171.68.235.228
  domain cisco.com
  pool group1pool
!
crypto isakmp client configuration group group2
  key testgroup1
  dns 171.70.168.183
  wins 171.68.235.228
  domain cisco.com
  pool group2pool
!
crypto isakmp client configuration group group3
  key testgroup1
  dns 171.70.168.183
  wins 171.68.235.228
  domain cisco.com
  pool group3pool
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto dynamic-map vpn-test 1
  set transform-set vpn-test
  reverse-route
!
crypto map ws client authentication list local
crypto map ws isakmp authorization list groupname
crypto map ws client configuration address respond
crypto map ws 1 ipsec-isakmp dynamic vpn-test
!
interface Ethernet3/4
  ip address 172.19.196.39 255.255.255.0
  load-interval 30
```



```
duplex full
service-policy output groupbwm
no cdp enable
crypto map ws
!
ip local pool group1pool 10.0.149.232 10.0.149.235
ip local pool group2pool 10.0.149.236 10.0.149.239
ip local pool group3pool 10.0.149.240 10.0.149.243
!
access-list 141 permit ip any 10.0.149.232 0.0.0.3
access-list 142 permit ip any 10.0.149.236 0.0.0.3
access-list 143 permit ip any 10.0.149.240 0.0.0.3 any time-range timename
!
time-range timename
  periodic daily 8:00 to 5:00
!
end
```

Verifying the Results

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

```
7200-3#sh access-list
```

```
7200-3#sh access-list
```

```
Extended IP access list 141
```

```
  permit ip any 10.0.149.232 0.0.0.3 (2422 matches)
```

```
Extended IP access list 142
```

```
  permit ip any 10.0.149.236 0.0.0.3 (1023 matches)
```

```
Extended IP access list 143
```

```
  permit ip any 10.0.149.240 0.0.0.3 time-range timename (active)
```

To verify the actual traffic withing each pool, use the following command

```
7200-3#sh policy-map int ether 3/4
```

```
Ethernet3/4
```

```
Service-policy output: groupbwm
```

```
Class-map: group1 (match-any)
```

```
 7581 packets, 8752306 bytes
```

```
 30 second offered rate 395000 bps, drop rate 0 bps
```

```
Match: access-group 141
```

```
 7581 packets, 8752306 bytes
```

```
 30 second rate 395000 bps
```

```
Queueing
```

```
Output Queue: Conversation 265
```

```
Bandwidth 1 (%)
```

```
Bandwidth 100 (kbps) Max Threshold 64 (packets)
```

```
(pkts matched/bytes matched) 2323/2852226
```

```
(depth/total drops/no-buffer drops) 0/0/0
```

```
Traffic Shaping
```

```
Target/Average Byte Sustain Excess Interval Increment
```



Rate	Limit	bits/int	bits/int	(ms)	(bytes)
2000000/1000000	6250	25000	25000	25	6250

Adapt Queue	Packets	Bytes	Packets	Bytes	Shaping
Active Depth			Delayed	Delayed	Active
- 0	7584	9151836	2311	2842050	no

Class-map: group2 (match-any)

0 packets, 0 bytes
 30 second offered rate 0 bps, drop rate 0 bps
 Match: access-group 142
 0 packets, 0 bytes
 30 second rate 0 bps

Queueing

Output Queue: Conversation 266
 Bandwidth 1 (%)
 Bandwidth 100 (kbps) Max Threshold 64 (packets)
 (pkts matched/bytes matched) 0/0
 (depth/total drops/no-buffer drops) 0/0/0

Traffic Shaping

Target/Average	Byte	Sustain	Excess	Interval	Increment
Rate	Limit	bits/int	bits/int	(ms)	(bytes)
2000000/1000000	6250	25000	25000	25	6250

Adapt Queue	Packets	Bytes	Packets	Bytes	Shaping
Active Depth			Delayed	Delayed	Active
- 0	0	0	0	0	no

Class-map: group3 (match-any)

0 packets, 0 bytes
 30 second offered rate 0 bps, drop rate 0 bps
 Match: access-group 143
 0 packets, 0 bytes
 30 second rate 0 bps

Queueing

Output Queue: Conversation 267
 Bandwidth 1 (%)
 Bandwidth 100 (kbps) Max Threshold 64 (packets)
 (pkts matched/bytes matched) 0/0
 (depth/total drops/no-buffer drops) 0/0/0

Traffic Shaping

Target/Average	Byte	Sustain	Excess	Interval	Increment
Rate	Limit	bits/int	bits/int	(ms)	(bytes)
2000000/1000000	6250	25000	25000	25	6250

Adapt Queue	Packets	Bytes	Packets	Bytes	Shaping
Active Depth			Delayed	Delayed	Active
- 0	0	0	0	0	no

Class-map: class-default (match-any)



19 packets, 1206 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any 476 packets, 382748 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
7200-3#

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)