Configuring ISG Policies for Regulating Network Access

Last Updated: December 19, 2012

Intelligent Services Gateway (ISG) is a Cisco IOS software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG supports the use of policies for governing subscriber session bandwidth and network accessibility. This module provides information about the following methods of regulating session bandwidth and network access: Modular Quality of Service (QoS) command-line interface (CLI) policies, Dynamic Subscriber Bandwidth Selection (DBS), per-subscriber firewalls, and ISG policing.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for ISG Policies for Regulating Network Access

Beginning in Cisco IOS Release 12.2(33)SRC, the Cisco 7600 router supports this feature with the following limitation:

- You cannot configure policing that requires the traffic class feature.

Information About ISG Policies for Regulating Network Access

Methods of Regulating Network Access

ISG supports the following methods of regulating network access. Each of these methods can be applied to an ISG session and can be dynamically updated.

Modular QoS CLI (MQC) Policies

QoS policies configured using the MQC are supported for subscriber sessions only. MQC policies cannot be applied to ISG services.

Dynamic Subscriber Bandwidth Selection (DBS)

DBS enables you to control bandwidth at the ATM virtual circuit (VC) level. ATM QoS parameters from the subscriber domain are applied to the ATM permanent virtual circuit (PVC) on which a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) session has been established.

Note DBS is not supported on the Cisco 7600 series router in Cisco IOS Release 12.2(33)SRC.

Per-Subscriber Firewalls

Per-subscriber firewalls are access control lists (ACLs) that are used to prevent subscribers, services, and pass-through traffic from accessing specific IP addresses and ports. Per-subscriber firewalls can be configured in user profiles and service profiles.

ISG Policing

ISG policing supports policing of upstream and downstream traffic. ISG policing differs from policing configured using the MQC in that ISG policing can be configured in service profiles to support policing of traffic flows. MQC policies cannot be configured in service profiles. ISG policing can also be configured in user profiles and service profiles to support session policing.

Note ISG Policing is not supported on the Cisco 7600 series router in Cisco IOS Release 12.2(33)SRC.

Overview of ISG Policing

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface. Policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic

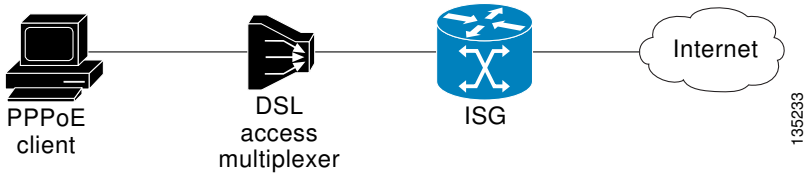
that falls within the rate parameters is sent, whereas traffic that exceeds the parameters is dropped or sent with a different priority.

ISG policing supports policing of upstream and downstream traffic and can be applied to a session or a flow. The following sections describe session-based policing and flow-based policing.

Session-Based Policing

Session-based policing applies to the aggregate of subscriber traffic for a session. In the figure below, session policing would be applied to all traffic moving from the PPPoE client to ISG and from ISG to the PPPoE client.

Figure 1 Session-Based Policing

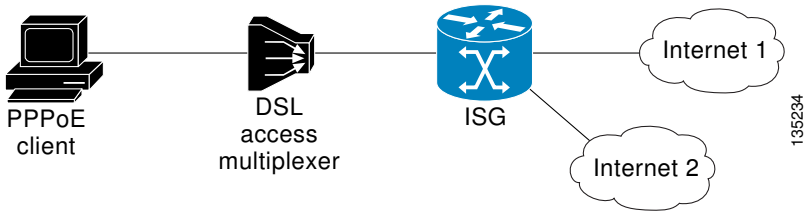


Session-based policing parameters can be configured on a AAA server in either a user profile or a service profile that does not specify a traffic class. It can also be configured on the router in a service policy map. Session-based policing parameters that are configured in a user profile take precedence over session-based policing parameters configured in a service profile or service policy map.

Flow-Based Policing

Flow-based policing applies only to the destination-based traffic flows that are specified by a traffic class. In the figure below, flow-based policing would allow you to police the traffic between the PPPoE client and Internet 1 or Internet 2.

Figure 2 Flow-Based Policing



Flow-based policing can be configured on a AAA server in a service profile that specifies a traffic class. It can also be configured on the router under a traffic class in a service policy map. Flow-based policing and session-based policing can coexist and operate simultaneously on subscriber traffic.

Per-Subscriber Firewalls

Per-subscriber firewalls are Cisco IOS ACLs that are used to prevent subscribers, services, and pass-through traffic from accessing specific IP addresses and ports.

ACLs can be configured in user profiles or service profiles on a AAA server or in service policy maps on ISG. The ACLs can be numbered or named access lists that are configured on ISG, or the ACL statements can be included in the profile configuration.

When an ACL is added to a service, all subscribers of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

When an ACL attribute is added to a user profile, it applies globally to all traffic for the subscriber.

How to Configure ISG Policies for Regulating Network Access

Configuring ISG Policing

Configuring Policing in a Service Policy Map on the Router

Perform this task to configure ISG policing on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*]**class type traffic** *class-map-name*
5. **police input** *committed-rate normal-burst excess-burst*
6. **police output** *committed-rate normal-burst excess-burst*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose
Step 3 **policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4 [*priority*]**class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic silver`	Associates a previously configured traffic class with the policy map.
Step 5 **police input** *committed-rate normal-burst excess-burst* **Example:** `Router(config-service-policymap-class-traffic)# police input 20000 30000 60000`	Configures ISG policing of upstream traffic. • These parameters will be used to limit traffic flowing from the subscriber toward the network.
Step 6 **police output** *committed-rate normal-burst excess-burst* **Example:** `Router(config-service-policymap-class-traffic)# police output 21000 31500 63000`	Configures ISG policing of downstream traffic. • These parameters will be used to limit the traffic flowing from the network toward the subscriber.

• What to Do Next, page 5

What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring Policing in a Service Profile or User Profile on the AAA Server

SUMMARY STEPS

1. Do one of the following:
   - Add the following Policing vendor-specific attribute (VSA) to the user profile on the AAA server.
   - 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*;D;*committed-rate*;*normal-burst*;*excess-burst*"
   -
   - Add the following Policing VSA to the service profile on the AAA server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Add the following Policing vendor-specific attribute (VSA) to the user profile on the AAA server. • 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*;D;*committed-rate*;*normal-burst*;*excess-burst*" • • Add the following Policing VSA to the service profile on the AAA server. **Example:** `26,9,251 "QU;`*committed-rate*`;`*normal-burst*`;`*excess-burst*`;D;`*committed-rate*`;`*normal-burst*`;`*excess-burst*"	Enables ISG policing of upstream and downstream traffic. • If you specify the committed rate and normal burst, excess burst will be calculated automatically. • You can specify upstream or downstream parameters first.

• What to Do Next, page 6

What to Do Next

You may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Verifying ISG Policing

Perform this task to verify ISG policing configuration.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Command or Action	Purpose
Step 2 **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISG subscriber session information.

Examples

The following example shows output for the **show subscriber session** command when policing parameters have been configured in the service profile. The "Config level" field indicates where the policing parameters are configured; in this case, in the service profile.

```
Router# show subscriber session detailed
Current Subscriber Information: Total sessions 2
Unique Session ID: 1
.....
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Service
Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service
.....
```

The following example shows output for the **show subscriber session** command where upstream policing parameters are specified in a user profile and downstream policing parameters are specified in a service profile.

```
Router# show subscriber session all
Current Subscriber Information: Total sessions 2
Unique Session ID: 2
.....
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Per-user  ============> Upstream parameters are specified in
the user profile.
Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service =============> No downstream parameters in the user
profile, hence the parameters in the service profile are applied.
.....
```

Configuring Per-Subscriber Firewalls

Configuring Per-Subscriber Firewalls in User Profiles or Service Profiles on a AAA Server

Perform this task to configure per-subscriber firewalls in user profiles or service profiles on a AAA server. This task assumes that you know how to configure access control lists. Only IP ACLs are supported. IPX and IPv6 ACLs are not supported.

SUMMARY STEPS

1. Do one of the following:
   - Add the Upstream Access Control List Cisco AV-Pair attribute to the user profile or service profile.
   - Cisco-AVpair="ip:inacl=*ACL-number*"
   -
   -
   -
2. Do one of the following:
   - Add the Downstream Access Control List Cisco AV-Pair attribute to the user profile or service profile.
   - Cisco-AVpair="ip:outacl=*ACL-number*"
   -
   -
   -

DETAILED STEPS

Command or Action	Purpose

Step 1 Do one of the following:
• Add the Upstream Access Control List Cisco AV-Pair attribute to the user profile or service profile.
• Cisco-AVpair="ip:inacl=*ACL-number*"
•
•
•
 	
Example:
`Cisco-AVpair="ip:inacl=`*ACL-name*`"`
 	
Example:
 	
Example:
 	
Example:
 	
Example:
`Cisco-AVpair="ip:inacl[`*#number*`]=`*ACL-statement*`"`
	Specifies a Cisco IOS ACL to be applied to traffic coming from the subscriber.
	• The *ACL-number* and *ACL-name*arguments refer to ACLs that are configured on the router.
	• The *ACL-statement* argument is an ACL definition that is included in the attribute configuration on the AAA server.
	• Multiple instances of the Upstream Access Control List attribute can occur within a single profile. Use one attribute for each ACL statement.
	• Multiple attributes can be used for the same ACL.

Command or Action	Purpose

Step 2 Do one of the following:
• Add the Downstream Access Control List Cisco AV-Pair attribute to the user profile or service profile.
• Cisco-AVpair="ip:outacl=*ACL-number*"
•
•
•
Example:
`Cisco-AVpair="ip:outacl=`*ACL-name*`"`
Example:
Example:
Example:
Example:
`Cisco-AVpair="ip:outacl[`*#number*`]=`*ACL-statement*`"`
	Specifies a Cisco IOS ACL to be applied to traffic going to the subscriber.
	• The *ACL-number* and *ACL-name*arguments refer to ACLs that are configured on the router.
	• The *ACL-statement* argument is an ACL definition that is included in the attribute configuration on the AAA server.
	• Multiple instances of the Downstream Access Control List attribute can occur within a single profile. Use one attribute for each ACL statement.
	• Multiple attributes can be used for the same ACL.

• What to Do Next, page 10

What to Do Next

You may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring Per-Subscriber Firewalls in a Service Policy Map

Perform this task to configure a per-subscriber firewall in a service policy map on ISG.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**} **Example:** `Router(config-service-policymap)# ip access-group 100 in`	Applies an access control list to control packet access. • Multiple instances of this command can be used in a single service policy map.

• What to Do Next, page 11

What to Do Next

You may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuration Examples for ISG Policies for Regulating Network Access

ISG Policing Examples

Flow-Based Policing Configured in a Service Policy Map Using the CLI

The following example shows the configuration of ISG flow-based policing in a service policy map:

```
class-map type traffic match-any C3
 match access-group in 103
 match access-group out 203
policy-map type service P3
 class type traffic C3
  police input 20000 30000 60000
  police output 21000 31500 63000
```

Session-Based Policing Configured in a User Profile on a AAA Server

The following example shows policing configured in a user profile:

```
Cisco:Account-Info = "QU;23465;8000;12000;D;64000"
```

Session-Based Policing Configured in a Service Profile on a AAA Server

The following example shows policing configured in a service profile:

```
Cisco:Service-Info = "QU;16000;D;31000"
```

Per-Subscriber Firewalls Examples

The following example shows per-subscriber firewalls configured in a user profile or service profile on the AAA server. In this case the ACLs 104 and 105 are configured on the router. “In” and “out” represent the inbound and outbound directions of ACL application.

```
Cisco-AVpair="ip:inacl=104",
Cisco-AVpair="ip:outacl=105"
```

The following example shows per-subscriber firewalls configured in a user profile or service profile on the AAA server. In this case the named ACLs are configured on the router.

```
Cisco-AVpair="ip:inacl=named-inacl-123",
Cisco-AVpair="ip:outacl=named-outacl-123"
```

The following example of per-subscriber firewall configuration includes the individual ACL statements in the user profile or service profile configuration:

```
Cisco-AVpair="ip:inacl#1=deny icmp host 10.0.25.25 host 10.0.3.3",
```

```
Cisco-AVpair="ip:inacl#2=permit ip any any",
Cisco-AVpair="ip:outacl#1=permit ip any any"
```

Verifying ISG Per-Subscriber Firewalls

Perform this task to verify the configuration of ISG per-subscriber firewalls.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]
3. **show ip access-list** [*access-list-number* | *access-list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISG subscriber session information.
Step 3	**show ip access-list** [*access-list-number* | *access-list-name*] **Example:** `Router# show ip access-list`	Displays the contents of all current IP access lists.

Examples

The following example is sample output for the **show subscriber session detailed** command. Information about per-subscriber firewalls appears in the “Session inbound features” and “Session outbound features” fields.

```
Router# show subscriber session detailed

Current Subscriber Information: Total sessions 1
------------------------------------------------
Session inbound features:
 Feature: Access lists
  Active IP access list:
  104
Session outbound features:
 Feature: Access lists
  Active IP access list:
  subscriber_feature#102341017649
```

The **show ip access-lists** command can be used to display access list statements. The following example is sample output for the **show ip access-lists** command:

```
Router# show ip access-lists
Extended IP access list 104 (Compiled)
    10 permit ip host 10.0.1.6 any (500 matches)
Extended IP access list subscriber_feature#102341017649 (per-user)
    10 deny icmp host 10.0.25.25 host 10.0.3.3
    20 permit ip any any
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
How to configure QoS policies using the MQC	"Applying QoS Features Using MQC" module in the *Cisco IOS XEQuality of Service Configuration Guide*
How to configure DBS	"Controlling Subscriber Bandwidth" module in the *Cisco IOS XEBroadband Access Aggregation and DSL Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for ISG Policies for Regulating Network Access

The following table provides release information about the feature or features described in this module. This table 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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Policies for Regulating Network Access

Feature Name	Releases	Feature Configuration Information
ISG: Flow Control: QoS Control: Dynamic Rate Limiting	12.2(28)SB 12.2(33)SRC	ISG can change the allowed bandwidth of a session or flow by dynamically applying rate-limiting policies. In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7600 router.