Configuring ISA Policies for Regulating Network Access

The Intelligent Service Architecture (ISA) is a core set of Cisco IOS components that provide a structured framework in which edge access devices can deliver flexible and scalable services to subscribers. A Cisco device that is running a Cisco IOS image with ISA is called an Intelligent Service Gateway (ISG). ISA 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 ISA policing.

Module History
This module was first published on April 28, 2005, and last updated on April 28, 2005.

Finding Feature Information in This Module
Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the “Feature Information for ISA Policies for Regulating Network Access” section on page 185.

Contents

- Information About ISA Policies for Regulating Network Access, page 174
- How to Configure ISA Policies for Regulating Network Access, page 174
- Configuration Examples for ISA Policies for Regulating Network Access, page 184
- Additional References, page 185
- Feature Information for ISA Policies for Regulating Network Access, page 185
Information About ISA Policies for Regulating Network Access

Before you configure ISA policies for regulating network access, you should understand the following concept:

- Methods of Regulating Network Access, page 174

Methods of Regulating Network Access

ISA supports the following methods of regulating network access. Each of these methods can be applied to an ISA 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 ISA 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.

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.

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

How to Configure ISA Policies for Regulating Network Access

This section contains procedures for configuring ISA policing and per-subscriber firewalls. See the “Additional References” section on page 185 for references to information on how to configure MQC policies, DBS, and support for dynamic updates to policies for regulating network access.

This section contains the following tasks:

- Configuring ISA Policing, page 174
- Configuring Per-Subscriber Firewalls, page 179

Configuring ISA Policing

Before you configure ISA policing, you should understand the following concept:

- Overview of ISA Policing, page 175
To configure ISA policing, perform the following tasks:

- Configuring Policing in a Service Policy Map on the Router, page 176
- Configuring Policing in a Service Profile or User Profile on the AAA Server, page 177
- Verifying ISA Policing, page 178

Overview of ISA 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.

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

Session-Based Policing

Session-based policing applies to the aggregate of subscriber traffic for a session. In Figure 3, session policing would be applied to all traffic moving from the PPPoE client to ISG and from ISG to the PPPoE client.

Figure 3  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 Figure 4 flow-based policing would allow you to police the traffic between the PPPoE client and Internet 1 or Internet 2.

Figure 4  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.

**Configuring Policing in a Service Policy Map on the Router**

Perform this task to configure ISA policing on the router using the CLI.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `policy-map type service policy-map-name`
4. `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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> policy-map type service policy-map-name</td>
<td>Creates or modifies a service policy map, which is used to define an ISA service.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# policy-map type service service1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> class type traffic class-map-name</td>
<td>Associates a previously configured traffic class with the policy map.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-service-policymap)# class type traffic silver</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> police input committed-rate normal-burst excess-burst</td>
<td>Configures ISA policing of upstream traffic.</td>
</tr>
<tr>
<td>Example:</td>
<td>• These parameters will be used to limit traffic flowing from the subscriber toward the network.</td>
</tr>
<tr>
<td>Router(config-service-policymap-class-traffic)# police input 20000 30000 60000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> police output committed-rate normal-burst excess-burst</td>
<td>Configures ISA policing of downstream traffic.</td>
</tr>
<tr>
<td>Example:</td>
<td>• These parameters will be used to limit the traffic flowing from the network toward the subscriber.</td>
</tr>
<tr>
<td>Router(config-service-policymap-class-traffic)# police output 21000 31500 63000</td>
<td></td>
</tr>
</tbody>
</table>

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 ISA Subscriber Services.”

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

SUMMARY STEPS

1. Add the Policing VSA to the user profile or service profile on the AAA server.
DETAILED STEPS

**Command or Action**

| Step 1 | 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"

or

Add the following Policing VSA to the service profile on the AAA server.  
26,9,251  
"QU;committed-rate;normal-burst;excess-burst;D;committed-rate;normal-burst;excess-burst" |
| Purpose | Enables ISA 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

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 ISA Subscriber Services.”

Verifying ISA Policing

Perform this task to verify ISA policing configuration.

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| Example:          |         |
| Router> enable    |         |
| Step 2 show subscriber session [detailed] [identifier identifier | uid session-id | username name] | Displays ISA subscriber session information. |
| Example:          |         |
| Router# show subscriber session detailed |         |

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.
Configuring ISA Policies for Regulating Network Access

How to Configure ISA Policies for Regulating Network Access

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
  Downstream 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

Session outbound features:
Feature: Policing
  Downstream Params:
  Average rate = 16000, Normal burst = 3000, Excess burst = 6000
  Config level = Service

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

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

**Configuring Per-Subscriber Firewalls**

Before you configure per-subscriber firewalls, you should understand the following concepts:

- Per-Subscriber Firewalls, page 180
- Prerequisites, page 180
- Restrictions, page 180

To configure per-session ACLs, perform the following tasks:

- Configuring Per-Subscriber Firewalls in User Profiles or Service Profiles on a AAA Server, page 180
- Configuring Per-Subscriber Firewalls in a Service Policy Map, page 181
- Verifying ISA Per-Subscriber Firewalls, page 182
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 the ISG. The ACLs can be numbered or named access lists that are configured on the 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.

Prerequisites

This task assumes that you know how to configure access control lists.

Restrictions

Only IP ACLs are supported on flows, IP subscriber sessions, and forwarded sessions. IPX and IPv6 ACLs are not supported.

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.

**SUMMARY STEPS**

1. Add the Upstream Access Control List Cisco AV-Pair attribute to the user profile or service profile.
2. Add the Downstream Access Control List Cisco AV-Pair attribute to the user profile or service profile.
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Add the Upstream Access Control List Cisco AV-Pair attribute to the user profile or service profile.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|Cisco-AVpair="ip:inacl[#number]=ACL-number"  
or  
|Cisco-AVpair="ip:inacl[#number]=ACL-name"  
or  
|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. Multiple attributes are downloaded according to the number specified by the #number argument and are executed in that order. |
| **Step 2** | Add the Downstream Access Control List Cisco AV-Pair attribute to the user profile or service profile. |
| 
|Cisco-AVpair="ip:outacl[#number]=ACL-number"  
or  
|Cisco-AVpair="ip:outacl[#number]=ACL-name"  
or  
|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. Multiple attributes are downloaded according to the number specified by the #number argument and are executed in that order. |

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 ISA 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 the 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

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

### 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 ISA Subscriber Services.”

### Verifying ISA Per-Subscriber Firewalls

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

### SUMMARY STEPS

1. **enable**
2. **show subscriber session detailed**
3. **show ip access-lists**
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 (enable)</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 (show subscriber session [detailed] [identifier identifier</td>
<td>Displays ISA subscriber session information.</td>
</tr>
<tr>
<td>Example:</td>
<td>&lt;uid&gt; session-id</td>
</tr>
<tr>
<td>Router# show subscriber session detailed</td>
<td></td>
</tr>
<tr>
<td>Step 3 (show ip access-list [access-list-number</td>
<td>Displays the contents of all current IP access lists.</td>
</tr>
<tr>
<td>Example:</td>
<td>access-list-name]</td>
</tr>
<tr>
<td>Router# show ip access-list</td>
<td></td>
</tr>
</tbody>
</table>

**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 25.25.25.25 host 3.3.3.3
  20 permit ip any any
```
Configuration Examples for ISA Policies for Regulating Network Access

This section contains the following examples:

- ISA Policing: Examples, page 184
- Per-Subscriber Firewalls: Examples, page 184

### ISA Policing: Examples

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

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

```plaintext
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: Example

The following example shows policing configured in a user profile:

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

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

The following example shows policing configured in a service profile:

```plaintext
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 direction of ACL application.

```plaintext
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.

```plaintext
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:

```plaintext
Cisco-AVpair="ip:inacl#1=deny icmp host 25.25.25.25 host 3.3.3.3",
Cisco-AVpair="ip:inacl#2=permit ip any any",
Cisco-AVpair="ip:outacl#1=permit ip any any"
```
Additional References

The following sections provide references related to ISA policies for regulating network access.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA commands</td>
<td>Cisco IOS Intelligent Service Architecture Command Reference</td>
</tr>
<tr>
<td>How to configure QoS policies using the MQC.</td>
<td>Cisco IOS Quality of Service Configuration Guide, Release 12.2.</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a></td>
</tr>
</tbody>
</table>

Feature Information for ISA Policies for Regulating Network Access

Table 17 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(27)SBA or later releases appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

If you are looking for information on a feature in this technology that is not documented here, see the "Intelligent Service Architecture Features Roadmap."

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. 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.

Note: Table 17 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.
## Feature Information for Policies for Regulating Network Access

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA: Flow Control: QoS Control: Dynamic Rate</td>
<td>12.2(27)SBA</td>
<td>ISA can change the allowed bandwidth of a session or flow by dynamically applying rate-limiting policies.</td>
</tr>
<tr>
<td>Limiting</td>
<td></td>
<td>The following sections provide information about this feature:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Methods of Regulating Network Access, page 174</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuring ISA Policing, page 174</td>
</tr>
</tbody>
</table>

---

Copyright © 2005 Cisco Systems, Inc. All rights reserved.
This module first published April 28, 2005. Last updated April 28, 2005.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)