Enabling ISA to Interact with External Policy Servers

Intelligent Service Architecture (ISA) is a core set of Cisco IOS components that provide a structured framework in which access edge 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). This document describes how to enable ISA to retrieve session policies or accept dynamic updates to session policies from external policy servers.

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 Interaction with External Policy Servers" section on page 88.

Contents

Restrictions for ISA Interaction with External Policy Servers

The ISG and external policy servers should be in the same virtual routing and forwarding instance (VRF).

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

Information About ISA Interaction with External Policy Servers

- Initial and Dynamic Authorization, page 84

Initial and Dynamic Authorization

ISA works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISA supports two models of interaction between ISA and external policy servers: initial authorization and dynamic authorization.

In the initial authorization model, ISA must retrieve policies from the external policy server at specific points in a session. In this model, the external policy server is typically an authentication, authorization, and accounting (AAA) server that uses RADIUS. The ISG is the RADIUS client. Instead of a AAA server, some systems use a RADIUS proxy component that converts to other database protocols such as Lightweight Directory Access Protocol (LDAP).

The dynamic authorization model allows the external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of some algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

How to Enable ISA to Interact With External Policy Servers

This section contains the following tasks:

- Configuring the ISG as a AAA Client, page 84
- Configuring the ISG as a AAA Server, page 86

Configuring the ISG as a AAA Client

Perform this task to configure AAA method lists and enable ISA to retrieve policies from a AAA server. This task must be performed for both initial and dynamic authorization models.

Prerequisites

The servers and server groups referenced by the AAA methods must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands level** | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]

6. **aaa authorization subscriber-service {default |** *list-name*} *method1* [*method2...*]
7. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands level**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*

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	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login PPP1 group radius`	Specifies one or more AAA authentication methods to be used at login.
Step 4	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default group radius`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 5	**aaa authorization** {**network** | **exec** | **commands level** | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]] **Example:** `Router(config)# aaa authorization network NET1 radius`	Specifies one or more AAA authorization methods to be used for restricting subscriber access to a network.
Step 6	**aaa authorization subscriber-service** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authorization subscriber-service default radius`	Specifies one or more AAA authorization methods for ISA to use in providing a service.
Step 7	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands level**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname* **Example:** `Router(config)# aaa accounting network default start-stop group radius`	Enables AAA accounting of requested services for billing or security purposes.

Configuring the ISG as a AAA Server

Dynamic authorization allows a policy server to dynamically send policies to ISA. Perform this task configure the ISG as a AAA server and enable dynamic authorization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client** {**name** | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*]
5. **port** *port-number*
6. **server-key** [**0** | **7**] *word*
7. **auth-type** {**all** | **any** | **session-key**}
8. **ignore** {**server-key** | **session-key**}

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	`aaa server radius dynamic-author`
	Example:
	`Router(config)# aaa server radius dynamic-author`
		Configures the ISG as a AAA server.

Step 4	**client** {**name** | *ip-address*} [**key** [0 | 7] *word*] [**vrf** *vrf-id*] **Example:** `Router(config-locsvr-da-radius)#`	Specifies a client with which ISA will be communicating.
Step 5	**port** *port-number* **Example:** `Router(config-locsvr-da-radius)# port 1600`	Specifies the RADIUS server port. • Default is 1700.
Step 6	**server-key** [0 | 7] *word* **Example:** `Router(config-locsvr-da-radius)# server-key cisco`	Specifies the encryption key shared with the RADIUS client.

	Command or Action	Purpose

Step 7	**auth-type** {**all** | **any** | **session-key**}
	Example:
	`Router(config-locsvr-da-radius)# auth-type all`
		Specifies the attributes to be used for session authorization.

Step 8	**ignore** {**server-key** | **session-key**}
	Example:
	`Router(config-locsvr-da-radius)# ignore session-key`
		Configures ISA to ignore the shared encryption key or attribute 151.

Configuration Examples for ISA Interaction with External Policy Servers

This section contains the following example:

- ISA Interaction with External Policy Servers: Example, page 87

ISA Interaction with External Policy Servers: Example

The following example configures ISA to interact with external policy servers:

```
aaa authentication login LOGIN group radius
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network default start-stop group radius
!
aaa server radius dynamic-author
 client 10.76.86.90 key cisco
 client 172.19.192.25 vrf VRF1 key cisco
 client 172.19.192.25 vrf VRF2 key cisco
 client 172.19.192.25 key cisco
 message-authenticator ignore
```

Additional References

The following sections provide references related to ISA interaction with external policy servers.

Related Documents

Related Topic	Document Title
ISA commands	*Cisco IOS Intelligent Service Architecture Command Reference*
AAA configuration tasks	The Authentication, Authorization, and Accounting (AAA) section in the *Cisco IOS Security Configuration Guide*, Release 12.2.
AAA commands	The Authentication, Authorization, and Accounting (AAA) section in the *Cisco IOS Security Command Reference*, Release 12.2.

Technical Assistance

Description	Link
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.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for ISA Interaction with External Policy Servers

Table 9 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 9 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.

Table 9 Feature Information for ISA Interaction with External Policy Servers

Feature Name	Releases	Feature Configuration Information
ISA:Policy Control:Policy Server:CoA	12.2(27)SBA	This feature provides ISA support for the RADIUS Change of Authorization (CoA) extension, which facilitates dynamic authorization. The following sections provide information about this feature: • Initial and Dynamic Authorization, page 84 • How to Enable ISA to Interact With External Policy Servers, page 84

This module first published April 28, 2005. Last updated April 28, 2005.