Enabling ISG to Interact with External Policy Servers

Last Updated: August 21, 2011

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document describes how to enable ISG to retrieve session policies or accept dynamic updates to session policies from external policy servers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 Interaction with External Policy Servers

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

Information About ISG Interaction with External Policy Servers

Initial and Dynamic Authorization

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

In the initial authorization model, ISG 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. 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.

Triple-Key Authentication for ISG

Triple-key authentication is a method of authenticating users based on their username, password, and location after ISG redirects them to the Cisco Service Management Engine (SME) portal. The SME server provides the location based on the source IP address of the subscriber being authenticated. Before the Triple Key Authentication Support feature was introduced, users were authenticated on the basis of the username and password only (two-key authentication). The triple-key authentication feature also eases migration from Service Selection Gateway (SSG) to an ISG platform because SSG uses triple-key authentication.

For SSG, the Cisco Subscriber Edge Services Manager (SESM) server populates RADIUS attribute 31 (calling-station ID) in the user-login request that it sends to SSG with a string containing the subscriber's location. SSG then includes this value in the access-request message that it sends to the RADIUS server where the login is authenticated based on the username, password, and location string.

With ISG triple-key authentication, the location string that SME sends to ISG in attribute 31 in the CoA account-logon request is repeated in the access-request packet that ISG sends to the RADIUS server to authenticate the subscriber. ISG sends the location string within a Cisco vendor-specific attribute (VSA) included in the access-request message to the RADIUS server.

If the account-logon request from SME contains location information in both attribute 31 and the Cisco VSA, the value of the Cisco VSA location string takes precedence. The location information is received from SME as either attribute 31 or Cisco VSA 250. The location information is included in session authentication requests, session accounting requests from ISG, and prepaid authorization requests.

The table below shows the Cisco vendor-specific non-AVPair attribute used for triple-key authentication.

Table 1 Cisco Vendor-Specific Non-AVPair Attribute

Sub-AttrID	Attribute Type	Value	Function	Example	Used in
250	account-info	L<location-string>	Third key in triple-key authentication	LWiFiHotSpot 001	Acc-Req CoA Req Accounting

How to Enable ISG to Interact with External Policy Servers

Configuring the ISG as a AAA Client

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

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** *group-name*
8. **end**

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	**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 ISG 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** *group-name* **Example:** `Router(config)# aaa accounting network default start-stop group radius`	Enables AAA accounting of requested services for billing or security purposes.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring the ISG as a AAA Server

Dynamic authorization allows a policy server to dynamically send policies to ISG. Perform this task to 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**}
9. **end**

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. • Enters dynamic authorization local server configuration mode.

	Command or Action	Purpose
Step 4	**client** {**name** | *ip-address*} [**key** [**0**|**7**] *word*] [**vrf** *vrf-id*] **Example:** `Router(config-locsvr-da-radius)# client 10.76.86.90 key cisco`	Specifies a client with which ISG 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.
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 ISG to ignore the shared encryption key or attribute 151.
Step 9	**end** **Example:** `Router(config-locsvr-da-radius)# end`	Exits global configuration mode.

Enabling the Location VSA for Triple-Key Authentication

To enable ISG to include the location VSA in authentication and accounting requests, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server vsa send accounting**
5. **radius-server vsa send authentication**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	**radius-server vsa send accounting** **Example:** `Router(config)# radius-server vsa send accounting`	Enables ISG to recognize and use accounting VSAs as defined by RADIUS attribute 26.
Step 5	**radius-server vsa send authentication** **Example:** `Router(config)# radius-server vsa send authentication`	Enables ISG to recognize and use authentication VSAs as defined by RADIUS attribute 26.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Examples

The following example shows how to configure ISG to use VSAs for accounting and authentication:

```
aaa new-model
!
!
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuration Examples for ISG Interaction with External Policy Servers

Example ISG Interaction with External Policy Servers

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

```
!
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
!
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

Example Triple-Key Authentication

The following example shows an authentication record with the session information including the location attribute. You can display this output by using the **debug radius accounting** command or the **gw-accounting syslog** command.

```
*Feb  5 01:20:50.413: RADIUS/ENCODE: Best Local IP-Address 10.0.1.1 for Radius-Server
```

```
10.0.1.2
*Feb  5 01:20:50.425: RADIUS(0000000F): Send Access-Request to 10.0.1.2:1645 id 1645/5,
len 107
*Feb  5 01:20:50.425: RADIUS:  authenticator 4D 86 12 BC BD E9 B4 9B - CB FC B8 7E 4C 8F
B6 CA
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  19
*Feb  5 01:20:50.425: RADIUS:   ssg-account-info   [250] 13  "LWiFiHotSpot001"
*Feb  5 01:20:50.425: RADIUS:  Calling-Station-Id  [31]  16  "AAAA.BBBB.CCCC"
*Feb  5 01:20:50.425: RADIUS:  User-Name           [1]   7   "george"
*Feb  5 01:20:50.425: RADIUS:  User-Password       [2]   18  *
*Feb  5 01:20:50.425: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
*Feb  5 01:20:50.425: RADIUS:  NAS-Port            [5]   6   0
*Feb  5 01:20:50.425: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Feb  5 01:20:50.425: RADIUS:  NAS-IP-Address      [4]   6   10.0.1.1
*Feb  5 01:20:50.425: RADIUS(0000000F): Started 5 sec timeout
*Feb  5 01:20:50.425: RADIUS: Received from id 1645/5 10.0.1.2:1645, Access-Accept, len 68
*Feb  5 01:20:50.425: RADIUS:  authenticator 49 A1 2C 7F C5 E7 9D 1A - 97 B3 E3 72 F3 EA
56 56
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  17
*Feb  5 01:20:50.425: RADIUS:   ssg-account-info   [250] 11  "S10.0.0.2"
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  31
*Feb  5 01:20:50.425: RADIUS:   Cisco AVpair       [1]   25  "accounting-list=default"
*Feb  5 01:20:50.433: RADIUS(0000000F): Received from id 1645/5
*Feb  5 01:20:50.437: RADIUS/ENCODE(0000000F):Orig. component type = Iedge IP SIP
*Feb  5 01:20:50.437: RADIUS(0000000F): Config NAS IP: 0.0.0.0
*Feb  5 01:20:50.437: RADIUS(0000000F): sending
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
AAA configuration tasks	Part 1, “Authentication, Authorization, and Accounting (AAA),” *Cisco IOS XESecurity Configuration Guide*
AAA commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

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/cisco/web/support/index.html

Feature Information for ISG Interaction with External Policy Servers

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 2 Feature Information for ISG Interaction with External Policy Servers

Feature Name	Releases	Feature Information
ISG: Policy Control: Policy Server: CoA	Cisco IOS XE Release 2.2 Cisco IOS XE Release 2.4	This feature provides ISG support for the RADIUS Change of Authorization (CoA) extension, which facilitates dynamic authorization. This feature was integrated into Cisco IOS XE Release 2.4.
ISG: Session: Lifecycle: Packet of Disconnect (POD)	Cisco IOS XE Release 2.2	This feature enables an external policy server to terminate an ISG session when it receives a RADIUS Packet of Disconnect (POD).
ISG: Triple Key Authentication Support	Cisco IOS XE Release 3.1S	This feature enables triple-key authentication by passing the location information from SESM to the RADIUS server in the access-request message.