Configuring ISG Integration with SCE

Intelligent Services Gateway (ISG) is a software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure ISG and Cisco Service Control Engine (SCE) to function as a single policy enforcement point for subscriber sessions.

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.

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.

Prerequisites for Configuring ISG Integration with SCE

Hardware Requirements

- An SCE platform

- Two connections between the ISG device and the SCE:
  - A control path, through which the ISG device and SCE can exchange policy information
  - A data path that carries the subscriber traffic
- A policy server configured to communicate with the ISG platform. The ISG-SCE integration removes any need for a communication layer between the policy server and the SCE.

Software Requirements

- Configure control and access policies, accounting, session maintenance, and network access regulation for ISG. For details on these configurations, see the *Intelligent Services Gateway Configuration Guide.*
- Cisco Software Release 3.1.0 or later on the SCE
- Configure SCE appropriately. For instructions on configuring SCE, see the *Cisco Service Control Engine (SCE) Software Configuration Guide,* Release 3.1.

Restrictions for Configuring ISG Integration with SCE

The following restrictions apply to the integration of the ISG and an SCE:

- When an SCE policy is deactivated, the policy is removed from the session on the SCE, and the session policy reverts to the default SCE policy.
- Only one SCE policy at a time may be applied to a session. Applying additional policies will override the policy previously applied on the SCE.

This feature requires a control bus communication protocol, which runs over RADIUS and RADIUS extensions (as specified in RFC 3576), operating in two modes; PUSH and PULL.

- In PULL mode the ISG device waits for a query from the SCE.
- In PUSH mode the download of an external feature is initiated by the ISG device as soon as an external service is activated on the subscriber session.

To work with the SCE for subscriber management, the control bus protocol must do the following:

- Support pushing a session and make relevant changes to a session to the SCE.
- Allow a session, its relevant identity, and the SCE policy profile to be pulled from the ISG device by using an identity-based query.
- Support accounting events, including the following:
  - Accepting SCE initiated accounting events asynchronously.
  - Correlating SCE accounting data to the appropriate ISG session.
  - Parsing the SCE accounting data to perform protocol translation.

The per-user IP subnet assigned to Point-to-Point Protocol (PPP) users during login is not communicated to SCE. A per-user static route is downloaded to PPP users through the framed-route RADIUS attribute during login. ISG does not send the per-user subnet address for a PPP session to SCE in the CoA provision session (ProvSess) attribute.

Information About Configuring ISG Integration with SCE

Overview of ISG-SCE Integration

The ISG Integration with SCE feature integrates ISG and SCE at the policy plane level so that for purposes of subscriber provisioning, ISG and SCE function as a single logical entity. The ISG device and SCE communicate to manage subscriber sessions jointly, minimizing the requirements for coordination with additional external components. ISG handles subscriber management at Layer 4 and below. SCE is primarily focused at Layer 4 and above. When ISG and SCE are configured to work together, they provide tools for these functions:

- Subscriber mapping--Subscriber awareness is distributed between ISG and the SCE. The shared subscriber session is referenced by both devices using a unique session identifier allocated by the ISG. Identity keys such as IP Address, IP Subnet, network access server (NAS) identifier, and NAS port are also associated to the session. SCE policies that should be enabled on the session are identified by their policy names.
- Subscriber policy updates--Change subscriber policies in real time.

ISG and SCE Roles in Subscriber Management

The table below shows the specific roles of ISG and SCE in subscriber management.

Table 1: ISG and SCE Roles in Subscriber Management

Provided by ISG	Provided by SCE
Subscriber aggregation (broadband remote access service--BRAS) Subscriber authorization or authentication Policy management Policy enforcement for • Quality of service (QoS) • Multiprotocol label switching (MPLS) virtual private network (VPN) • Redirection • Session termination • Postpaid billing	Policy enforcement for • Application-aware services • Redirection and application-based policy management • Service security • Behavioral classification • URL caching and filtering • Value-added services • Parental controls • Usage and content billing

ISG pushes policies (or external services) to the SCE for a given subscriber session, in the form of RADIUS change of authorization (CoA) messages. External service activation can be triggered by the policy manager component inside the ISG or by an external authentication, authorization, and accounting (AAA) server. The SCE sees the ISG as the policy manager. ISG serves as a proxy for service activation requests from the external AAA server to the SCE. The SCE sends accounting records to the ISG. The ISG, if configured to do so, serves as a proxy that sends the accounting records to an external AAA server. SCE can also query the ISG about session information for unprovisioned sessions. ISG informs SCE when a session terminates by means of a RADIUS Packet of Disconnect (PoD).

How to Configure ISG Integration with SCE

Configuring Communication Between SCE and ISG

Communication between the SCE and the ISG device is managed by an external policy delegation (EPD) handler module in Cisco IOS software. The EPD implements the control bus on the ISG and handles all messaging between the ISG device and SCE. This task is necessary to establish the parameters for the communication between the ISG device and the SCE, including the following:

- Port to which CoA messages are sent from the ISG device and SCE
- Port on which ISG should receive access, accounting, and connection management requests from SCE
- Shared secret between the ISG device and SCE

To configure communication between SCE and the ISG device, enter the following commands on the ISG device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius** {**sesm** | **proxy** | **policy-device**}
4. **client** *ipaddress* [**port** c*oa destination port*] [**key** *shared secret]*
5. **authentication port** *port-number*
6. **accounting port** *port-number*
7. **key** *shared-secret*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius** {**sesm** | **proxy** | **policy-device**} **Example:** `Router(config)# aaa server radius policy-device`	Enters RADIUS server configuration mode and configures the RADIUS profile.
Step 4	**client** *ipaddress* [**port** c*oa destination port*] [**key** *shared secret]* **Example:** `Router(config-locsvr-radius)# client 10.10.10.1 key cisco port 1431`	Configures client-specific details. • The IP address identifies the destination for CoA messages. If no port is configured, the default port (3799) is used. ISG sends CoA messages to the SCE to provision, update, or deactivate a session and activate or deactivate policies. • A shared secret configured for a specific client overrides the key configured using the **key shared-secret**command.
Step 5	**authentication port** *port-number* **Example:** `Router(config-locsvr-radius)# authentication port 1433`	Specifies the port on which the EPD handler listens for session and identity query requests from SCE. • If no port is specified, the default port (1645) is used.
Step 6	**accounting port** *port-number* **Example:** `Router(config-locsvr-radius)# accounting port 1435`	Specifies the port on which the EPD handler listens for accounting and peering requests and maintenance packets from SCE. • If no port is specified, the default port (1646) is used.
Step 7	**key** *shared-secret* **Example:** `Router(config-locsvr-radius)# key xxxxxxxxxx`	Configures the secret shared between the EPD handler and SCE. • This key is used if no per-client shared secret is configured.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-locsvr-rasius)# exit`	Exits RADIUS server configuration mode.

Configuring SCE Connection Parameter on ISG

To configure the server connection management on either a per-server or a global basis, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-peer address** *ip-address* **keepalive** *seconds*
4. **policy-peer keepalive** *seconds*
5. **exit**

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-peer address** *ip-address* **keepalive** *seconds* **Example:** `Router(config)# policy-peer address 10.10.10.1 keepalive 6`	Configures the keepalive value, in seconds, for a specific policy defined by the given IP address. • Valid values are from 5 to 3600. • The default value is zero (0). • If the default value is in effect on the ISG device, the keepalive value proposed by the external policy device is used.

	Command or Action	Purpose
Step 4	**policy-peer keepalive** *seconds* **Example:** `Router(config)# policy-peer keepalive 10`	Configures the keepalive value, in seconds, globally. • The range of valid values is from 5 to 3600. • The default value is zero (0). • If no per-server keepalive value is configured, the global value is used. • If different values are configured on the ISG device and the SCE, the lower value is used as the keepalive interval. • If neither a per-server nor a global value is configured, the default value of zero is used.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Control Policy on the Policy Manager

To configure the policy manager to download a service, through rules configured by Cisco IOS commands, follow the steps in this section.

Configuring Control Policy on the ISG

To configure the control policy on the ISG device, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **service-policy type service name** *service-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control GOLD_POLICY`	Configures the specified policy-map on the ISG and enters policy map configuration mode.
Step 4	**class type control** {*class-map-name* | **always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control always event acct-notification`	Specifies to apply actions matching conditions defined by the class-map-name or always for an event type. • Event types include the following: account-logoff, account-logon, acct-notification, credit-exhausted, quota-depleted, service-failed, service-start, service-stop, session-default-service, session-restart, session-service-found, session-start, and timed-policy-expiry.
Step 5	*action-number* **service-policy type service name** *service-name* **Example:** `Router(config-control-policymap)# 1 service-policy type service name sce-service`	Defines the list of actions to be performed when the control policy is matched.
Step 6	**exit** **Example:** `Router(config-control-policymap)# exit`	Exits policy map configuration mode.

Configuring Auto Service on the AAA Server

To download a service to the ISG by means of auto service, perform the steps in this section.

SUMMARY STEPS

1. Cisco-Avpair="subscriber: auto-logon-service=sce-service"

DETAILED STEPS

Cisco-Avpair="subscriber: auto-logon-service=sce-service"
Downloads a service name from the SCE to the ISG device.

Configuring Services

To configure services, perform the steps in this section. You can configure this feature either on the ISG device, using the Cisco IOS command line interface (CLI) commands, or on the AAA server.

Configuring Services on ISG

To configure a service containing accounting features and to activate an external policy on the SCE device, follow the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-map-name*
4. **class-map type traffic** *class-map-name*
5. **accounting aaa list** *listname*
6. **sg-service-type external-policy**
7. **policy-name** *name*
8. **service-monitor enable**
9. **exit**

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	**policy-map type service** *service-map-name* **Example:** `Router(config-traffic-classmap)# policy-map type service SVC`	Creates a service and enters traffic class map configuration mode.
Step 4	**class-map type traffic** *class-map-name* **Example:** `Router(config-control-policymap-class-control)# class-map type traffic bar`	Defines a traffic class and enters control policy-map class configuration mode.
Step 5	**accounting aaa list** *listname* **Example:** `Router(config-service-policymap)# accounting aaa list list1`	Configures accounting for ISG and enters service policy map configuration mode.
Step 6	**sg-service-type external-policy** **Example:** `Router(config-control-policymap)# sg-service-type external-policy`	Defines the service as an external policy and enters policy map configuration mode.
Step 7	**policy-name** *name* **Example:** `Router(config-control-policymap)# policy-name gold` **Example:**	Defines a corresponding external policy name on the SCE.
Step 8	**service-monitor enable** **Example:** `Router(config-control-policymap)# service-monitor enable` **Example:**	Enables service monitoring for the external policy device.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(config-pol-map)# exit`	Exits policy map configuration mode.

Configuring Services on the AAA Server

To configure a service on the external AAA server, perform the steps in this section.

SUMMARY STEPS

1. Cisco:Avpair="subscriber:sg-service-type=external-policy"
2. Cisco:Avpair="subscriber:policy-name=gold"
3. Cisco:Avpair="subscriber:service-monitor=1"
4. Cisco:Avpair="accounting-list=list1"

DETAILED STEPS

Step 1 Cisco:Avpair="subscriber:sg-service-type=external-policy"
Defines the service as an external policy.

Step 2 Cisco:Avpair="subscriber:policy-name=gold"
Defines a corresponding external policy name on the ISG.

Step 3 Cisco:Avpair="subscriber:service-monitor=1"
Enables service monitoring for the external policy device.

Step 4 Cisco:Avpair="accounting-list=list1"
Configures accounting for ISG.

Troubleshooting Tips

The following command can be used to troubleshoot the integration of ISG with SCE:

- **show subscriber policy peer { address** *ip-address* **| handle** *connection-handle* **|** *id* **| all }**

Examples

This section contains sample output of the **show subscriber policy peer**command.

show subscriber policy peer all

The following example shows sample output of the command when the **all** keyword is used.

```
Router# show subscriber policy peer all
Peer IP: 10.0.0.10
Conn ID: 11
Mode   : PULL
State  : ACTIVE
Version: 1.0
Conn up time: 00:00:14
Conf keepalive: 0
Negotiated keepalive: 1000
Time since last keepalive: 00:00:14
Remove owner on pull: TRUE
```

show subscriber policy peer all detail

The following example shows sample output for the **show subscriber policy peer**command when the **detail** keyword is added.

```
Router# show subscriber policy peer all detail
Peer IP: 10.0.0.10
Conn ID: 11
Mode   : PULL
State  : ACTIVE
Version: 1.0
Conn up time: 00:04:00
Conf keepalive: 0
Negotiated keepalive: 1000
Time since last keepalive: 00:04:00
Remove owner on pull: TRUE
Associated session details:
12.134.4.5session_guid_str
12.34.4.5session_guid_str
```

Configuration Examples for ISG Integration with SCE

ISG Control Bus Configuration Example

The following example shows how to configure the ISG control bus with the SCE management IP address and shared authentication key:

```
aaa server radius policy-device
 client 10.10.10.10
 key cisco
 message-authenticator ignore
!
policy-peer address 10.10.10.10 keepalive 60
!
interface GigabitEthernet5/1/1
 ip address 10.10.10.1 255.255.255.0
!
```

ISG Integration with SCE Example

The following example shows how to configure two SCEs, each with the same authentication and accounting ports. ISG handles CoA messages on port 1700 for one SCE and on default port 3799 for the other SCE. Peering is maintained for each SCE with the ISG via different keepalive intervals.

When a user session starts, POLICY-LOCAL is applied. If the user's profile at the AAA server has auto-logon, the session will begin using the SCE-SERVICE-LOCAL service. This service has the SCE service-monitor facility enabled. If the user profile does not specify auto-logon to the SCE-SERVICE-LOCAL service, SCE will use its default values for the *policy-name* argument and the **service-monitor**command, which are configured at the SCE.

```
aaa accounting network service_acct start-stop group radius
aaa accounting network session_acct start-stop group radius
aaa server radius policy-device
 authentication port 1343
 accounting port 1345
 message-authenticator ignore
 client 10.10.10.1 port 1341 key cisco
class-map type traffic match-any bar
 match access-group input 102
access-list 102 permit ip any any
policy-map type service sce_service
 class type traffic bar
  accounting aaa list service_acct
 sg-service-type external-policy
 policy-name gold
 service-monitor enable
policy-map type control sce_policy
 class type control always event session-start
   1 service-policy type service sce_service
 class type control always event acct-notification
  1 proxy aaa list session_acct
```

SCE Control Bus Configuration Examples

SCE Control Bus Setup Configured in PUSH Mode

The following example shows how to configure the SCE control bus in PUSH mode:

```
scmp
scmp name ISG radius 10.10.10.2 secret cisco auth 1433 acct 1435
scmp subscriber send-session-start
interface LineCard 0
 subscriber anonymous-group name all IP-range
  192.168.12.0:0xffffff00 scmp name ISG
```

SCE Control Bus Setup Configured in PULL Mode

The following example shows how to configure the SCE control bus in PULL mode:

```
scmp
scmp name ISG radius 10.10.10.2 secret cisco auth 1433 acct 1435
interface LineCard 0
 subscriber anaonymous-group name all IP-range
  192.168.12.0:0xffffff00 scmp name ISG
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Intelligent Services Gateway Command Reference
AAA configuration tasks	The "Authentication, Authorization, and Accounting (AAA)" module in the*Security Configuration Guide*
AAA commands	The "Authentication, Authorization, and Accounting (AAA)" module in the *Cisco IOS Security Command Reference*
SCE configuration	Cisco Service Control Engine (SCE) Software Configuration Guide, Release 3.1

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 Configuring ISG Integration with SCE

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 Integration with SCE

Feature Name	Releases	Feature Information
ISG: Policy Control: ISG-SCE Control Bus	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server. The following commands were introduced or modified: **aaa server radius policy-device**, **class type control**, **clear subscriber policy peer**, **clear subscriber policy peer session, policy-name**, **policy peer**, **proxy (ISG RADIUS proxy)**, **service-monitor**, **sg-service-type external policy**, **show subscriber policy peer**.