Redirecting Subscriber Traffic Using ISG Layer 4 Redirect

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 module describes how to configure ISG to redirect subscriber traffic by using the ISG Layer 4 Redirect feature. The ISG Layer 4 Redirect feature enables service providers to better control the user experience by allowing subscriber TCP or User Datagram Protocol (UDP) packets to be redirected to specified servers for appropriate handling. ISG Layer 4 redirection can be used to facilitate subscriber authentication, initial and periodic advertising captivation, redirection of application traffic, and Domain Name System (DNS) redirection.

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 Redirecting ISG Subscriber Traffic

The ISG Layer 4 Redirect feature applies only to TCP or UDP traffic.

A Layer 4 Redirect feature and a Traffic-Class (TC) service containing a Layer 4 Redirect feature cannot be applied on the same session. A Layer 4 Redirect feature can be applied either on a session or on a TC on the session.

In Cisco IOS XE software, access lists cannot be configured as match criteria in an ISG Layer 4 redirect configuration. As an alternative, Layer 4 redirect should be configured in ISG traffic class services.

Information About Redirecting ISG Subscriber Traffic

Overview of ISG Layer 4 Redirect

The ISG Layer 4 Redirect feature redirects specified packets to servers that handle the packets in a specified manner. For example, packets sent upstream by unauthorized users can be forwarded to a server that redirects the users to a login page. Similarly, if users try to access a service to which they have not logged in, the packets can be redirected to a server that provides a service login screen.

The Layer 4 Redirect feature supports three types of redirection, which can be applied to subscriber sessions or to flows:

- Initial redirection--Specified traffic is redirected for a specific duration of the time only, starting from when the feature is applied.
- Periodic redirection--Specified traffic is periodically redirected. The traffic is redirected for a specified duration of time. The redirection is then suspended for another specified duration. This cycle is repeated. During periodic redirect, all new TCP connections are redirected until the duration of the redirect is over. After that time any new incoming TCP connections will not be redirected. However, all existing TCP connections that were initiated during this redirection will still be redirected so as not to break the connections.
- Permanent redirection--Specified traffic is redirected to the specified server all the time.

A redirect server can be any server that is programmed to respond to the redirected packets. If ISG is used with a web portal, unauthenticated subscribers can be sent automatically to a login page when they start a browser session. Web portal applications can also redirect to service login pages, advertising pages, and message pages.

Redirected packets are sent to an individual redirect server or redirect server group that consists of one or more servers. ISG selects one server from the group on a rotating basis to receive the redirected packets.

When traffic is redirected, ISG modifies the destination IP address and TCP port of upstream packets to reflect the destination server. For downstream packets, ISG changes the destination IP address and port to the original packet’s source.

When traffic is selected by a policy map that includes a **redirection** command, packets are fed back into the policy map classification scheme for a second service selection. The modified IP headers can be subject to different classification criteria. For example, if two class maps exist, each with different **redirection** commands, packets could be redirected, selected by the first class map, and redirected a second time. To avoid this situation, configure traffic class maps so that two consecutive redirections cannot be applied to the same packet.

Layer 4 Redirect Applications

The Layer 4 Redirect feature supports the following applications:

- TCP redirection for unauthenticated users and unauthorized services

HTTP traffic from subscribers can be redirected to a web dashboard where the subscribers can log in so that authentication and authorization can be performed.

- Initial and periodic redirection for advertising captivation

Subscriber traffic can be redirected to a sponsor's web page for a brief period of time at the start of the session or periodically throughout the session.

- Redirection of application traffic

Application traffic from a subscriber can be redirected so as to provide value-added services. For example, a subscriber's Simple Mail Transfer Protocol (SMTP) traffic can be redirected to a local mail server that can function as a forwarding agent for the mail.

- DNS redirection

DNS queries may be redirected to a local DNS server. In some deployments, such as public wireless LAN (PWLAN) hot spots, subscribers may have a static DNS server addresses, which may not be reachable at certain locations. Redirecting DNS queries to a local DNS server allows applications to work properly without requiring reconfiguration.

How to Configure ISG Layer 4 Redirect

There are three ways to apply Layer 4 redirection to sessions. One way is to configure redirection directly on a physical main interface or logical subinterface. A second way is to configure a service profile or service policy map with the Layer 4 redirect attribute in it, and apply that service to the session. A third way is to configure the Layer 4 redirect attribute in the user profile.

The following tasks describe how to configure Layer 4 redirection. The first task is optional. One or more of the next three tasks is required. The last task is optional.

For examples of Layer 4 redirection configuration for specific applications (such as unauthenticated user redirect), see the "Configuration Examples for ISG Layer 4 Redirect" section.

Defining a Redirect Server Group

Perform this task to define a group of one or more servers to which traffic will be redirected. Traffic will be forwarded to servers on a rotating basis.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redirect server-group** *group-name*
4. **server ip** *ip-address* **port** *port-number*

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	**redirect server-group** *group-name* **Example:** `Router(config)# redirect server-group ADVT-SERVER`	Enters redirect server-group configuration mode to define a group of servers in a named redirection server group.
Step 4	**server ip** *ip-address* **port** *port-number* **Example:** `Router(config-sg-l4redirect-group)# server ip 10.0.0.1 port 8080`	Adds a server to a redirect server group. • You can enter this command more than one time to add multiple servers to the server group.

Configuring Layer 4 Redirection in a Service Policy Map

Perform this task to configure Layer 4 redirection in a service policy map.

The ISG Layer 4 Redirect feature is configured under a traffic class within a service policy map. This task assumes that you have defined the traffic class map. See the "Configuring ISG Subscriber Services" module for more information.

Note Only ISG policing and accounting features can be enabled in conjunction with redirection on the same service policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redirect session-limit** *maximum-number*
4. **policy-map type service** *policy-map-name*
5. **class type traffic** *class-name*
6. **redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*]

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	**redirect session-limit** *maximum-number* **Example:** `Router(config)# redirect session-limit 5`	(Optional) Sets the maximum number of Layer 4 redirects allowed for each subscriber session.
Step 4	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Enters service policy-map configuration mode to create or modify a service policy map, which is used to define an ISG service.

	Command or Action	Purpose

Step 5	**class type traffic** *class-name*
	Example:
	`Router(config-service-policymap)# class type traffic class1`
		(Optional) Enters traffic class map configuration mode to specify a traffic class map that identifies the traffic to which this service applies.

Step 6	**redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to ip 10.10.10.10`	Redirects traffic to a specified server or server group.

- What to Do Next, page 6

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 Layer 4 Redirection in a Service Profile or User Profile on the AAA Server

The Layer 4 Redirect feature can be configured as a Cisco vendor-specific attribute (VSA) in a user or service profile on an authentication, authorization, and accounting (AAA) server. This attribute can appear more than once in a profile to define different types of redirections for a session and can be used in both user and non-TC service profiles simultaneously.

SUMMARY STEPS

1. Add the Layer 4 Redirect VSA to the user profile or subscriber profile on the AAA server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Layer 4 Redirect VSA to the user profile or subscriber profile on the AAA server. **Example:** `Cisco-AVPair = “ip:l4redirect=redirect to {group` *server-group-name* `| ip` *ip-address* `[port` *port-number*`]} [duration` *seconds*`] [frequency` *seconds*`]”`	Redirects traffic to a specified server or server group.

- What to Do Next, page 7

What to Do Next

If you configure ISG Layer 4 redirection in a service profile, 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 "Configuring ISG Subscriber Services" module.

Verifying ISG Traffic Redirection

Perform this task to verify the configuration and operation of ISG Layer 4 traffic redirection. The commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show redirect translations** [**ip** *ip-address*]
3. **show redirect group** [*group-name*]
4. **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.
Step 2	**show redirect translations** [**ip** *ip-address*] **Example:** `Router# show redirect translations ip 10.0.0.0`	Displays ISG Layer 4 redirect translations for sessions.
Step 3	**show redirect group** [*group-name*] **Example:** `Router# show redirect group redirect1`	Displays information about ISG redirect server groups.
Step 4	**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 is sample output from the **show redirect translations** command:

```
Router# show redirect translations ip 10.53.0.2
Destination IP/port    Server IP/port         Prot  In Flags  Out Flags  Timestamp
172.20.0.2       23     10.2.36.253      23     TCP   none      none       May 08 2003
12:37:10
```

The following is sample output from the **show subscriber session** command. This output shows that Layer 4 redirect is being applied from the service profile.

```
Router# show subscriber session uid 135
Subscriber session handle: 7C000114, state: connected, service: Local Term
Unique Session ID: 135
Identifier: blind-rdt
SIP subscriber access type(s): IP-Interface
Root SIP Handle: CF000020, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 40 minutes, 30 seconds, Last Changed: 40 minutes, 30 seconds
AAA unique ID: 135
Switch handle: F000086
Interface: ATM2/0.53
Policy information:
  Authentication status: unauthen
  Config downloaded for session policy:
  From Access-Type: IP-Interface, Client: SM, Event: Service Selection Request, Service
    Profile name: blind-rdt, 2 references
      username             "blind-rdt"
      l4redirect           "redirect to group sesm-grp"
  Rules, actions and conditions executed:
    subscriber rule-map blind-rdt
      condition always event session-start
        action 1 service-policy type service name blind-rdt
Session inbound features:
 Feature: Layer 4 Redirect
  Rule  Cfg  Definition
  #1    SVC  Redirect to group sesm-grp  !! applied redirect
Configuration sources associated with this session:
Service: blind-rdt, Active Time = 40 minutes, 32 seconds
Interface: ATM2/0.53, Active Time = 40 minutes, 32 seconds
```

The following is sample output from the **show subscriber session**command for a session in which the Layer 4 redirection is applied on the interface:

```
Router# show subscriber session uid 133
Subscriber session handle: D7000110, state: connected, service: Local Term
Unique Session ID: 133
Identifier:
SIP subscriber access type(s): IP-Interface
Root SIP Handle: 1E, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 42 minutes, 54 seconds, Last Changed: 42 minutes, 54 seconds
AAA unique ID: 133
Switch handle: 17000084
Interface: FastEthernet0/0.505
Policy information:
  Authentication status: unauthen
Session inbound features:
 Feature: Layer 4 Redirect
  Rule  Cfg  Definition
  #1    INT  Redirect to group sesm-grp
Configuration sources associated with this session:
Interface: FastEthernet0/0.505, Active Time = 42 minutes, 54 seconds
```

Configuration Examples for ISG Layer 4 Redirect

Redirecting Unauthenticated Subscriber Traffic Example

In the following example, Layer 4 redirection is configured in the service policy map “BLIND-RDT.” This policy is applied to all sessions at session start and redirects subscriber TCP traffic to the server group called “PORTAL.” At account login the subscriber is authenticated and the redirection is not applied.

```
Service-policy type control DEFAULT-IP-POLICY
policy-map type control DEFAULT-IP-POLICY
 class type control always event session-start
  1 service-policy type service BLIND-RDT
!
 class type control always event account-logon
  1 authenticate aaa list AUTH-LIST
  2 service-policy type service unapply BLIND-RDT
policy-map type service BLIND-RDT
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

Redirecting Unauthorized Subscriber Traffic Example

The following example shows the configuration of redirection for unauthorized subscribers. If the subscriber is not logged into the service called “svc,” traffic that matches “svc” is redirected to the server group “PORTAL.” Once the subscriber logs on to the service, the traffic is no longer redirected. When the subscriber logs off the service, redirection is applied again.

```
service-policy type control THE_RULE
!
class-map type traffic match-any CLASS-ALL
!
class-map type traffic match-any CLASS-100_110
 match access-group input 100
 match access-group output 110
!
policy-map type service blind-rdt
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
policy-map type service svc-rdt
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
policy-map type service svc
 class type traffic CLASS-100_110
 class type traffic default in-out
  drop

!


policy-map type control THE_RULE
 class type control alwyas event account-logon
  1 authenticate
  2 service-policy type service name svc-rdt
 class type control cond-svc-logon event service-start
```

```
  1 service-policy type service unapply name svc-rdt
  2 service-policy type service identifier service-name
 class type control cond-svc-logon event service-stop
  1 service-policy type service unapply name svc
  2 service-policy type service name svc-rdt
 !
class-map type control match-all cond-svc-logon
 match identifier service-name svc
!
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

Initial ISG Redirection Example

The following example shows ISG configured to redirect the Layer 4 traffic of all subscribers to a server group called “ADVT” for the initial 60 seconds of the session. After the initial 60 seconds, ISG will stop redirecting the traffic for the rest of the lifetime of the session.

```
service-policy type control initial-rdt
policy-map type control intial-rdt
 class type control always event session-start
  1 service-policy type service name initial-rdt-profile
 !
policy-map type service initial-rdt-profile
 class type traffic CLASS-ALL
  redirect to group ADVT duration 60
```

Periodic ISG Redirection Example

The following example shows how to redirect all subscriber traffic for a period of 60 seconds every 3600 seconds:

```
service-policy control periodic-rdt session-start
!
policy-map type control periodic-rdt
 class type control always event session-start
  1 service-policy service periodic-rdt-profile
 !
policy-map type service periodic-rdt-profile
```

redirect to group ADVT duration 60 frequency 3600

Redirecting DNS Traffic Example

The following example shows how to redirect all subscriber DNS packets to the server group “DNS-server”:

service-policy type control DNS-rdt

```
policy-map type control DNS-rdt
 class type control event session-start
  1 service-policy type service name DNS-rdt-profile
  !
policy-map type service DNS-rdt-profile
 class type traffic CLASS-ALL
  redirect to group DNS-server
```

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*
Configuring ISG subscriber services	"Configuring ISG Subscriber Services" module in this guide

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

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 Redirecting ISG Subscriber Traffic

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 Redirecting ISG Subscriber Traffic

Feature Name	Releases	Feature Information
ISG: Flow Control: Flow Redirect	Cisco IOS XE Release 2.2	The ISG Layer 4 Redirect feature enables service providers to better control the user experience by allowing subscriber TCP or UDP packets to be redirected to specified servers for appropriate handling. ISG Layer 4 redirection can be applied to individual subscriber sessions or flows.
Parameterization for ACL and Layer 4 Redirect	Cisco IOS XE Release 2.4	The Parameterization for ACL and Layer 4 Redirect feature provides parameterization enhancements for access control lists and Layer 4 redirect.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.