Configuring ISG Control Policies

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. ISG control policies are a means of defining the actions the system will take in response to specified conditions and events. A wide variety of system actions, conditions, and events can be combined using a consistent policy language, providing a flexible and precise way of configuring ISG. This module provides information about how to configure ISG control policies.

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.

Prerequisites for ISG Control Policies

Authentication, authorization, and accounting (AAA) method lists must be configured prior to defining authentication and authorization actions.

Restrictions for ISG Control Policies

Control policies are activated for specific contexts, not directly on sessions. Control policies apply to all sessions hosted on the context.

Only one control policy map may be applied to a given context.

Control policies can be defined only through the router's command-line interface (CLI).

Not all actions may be associated with all events.

A new control class may not be inserted between existing control classes once a control policy map has been defined.

Information About ISG Control Policies

Control Policies

Control policies define the actions that the system will take in response to specified events and conditions. For example, a control policy can be configured to authenticate specific subscribers and then provide them with access to specific services.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed.

Three steps are involved in defining a control policy:

1 Create one or more control class maps.

A control class map specifies the conditions that must be met for a policy to be activated, and, optionally, the event that causes the class to be evaluated. A control class map may contain multiple conditions, each of which will evaluate to either true or false. Match directives can be used to specify whether all, any, or none of the individual conditions must evaluate true in order for the class to evaluate true.

1 Create a control policy map.

A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.

1 Apply the control policy map.

A control policy map is activated by applying it to a context. A control policy map can be applied to one or more of the following types of contexts. In the following list, the context types are listed in order of precedence. For example, a control policy map that is applied to a PVC takes precedence over a control policy map that is applied to an interface.

-
  - Permanent virtual circuit (PVC)
  - Virtual circuit (VC) class
  - Virtual template
  - Subinterface
  - Interface
  - Global

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts.

Note Traffic policies are another type of policy used by ISG. Traffic policies define the handling of data packets and are configured in service policy maps or service profiles. For more information about traffic policies, see the "Configuring ISG Subscriber Services" module.

- Differentiated Initial Policy Control, page 3

Differentiated Initial Policy Control

Authentication failure for a subscriber may happen for an access-reject (which means a RADIUS server responded with a Reject) or due to an access request timeout (RADIUS server is unreachable).

Using ISG control policies, and actions configured for the 'radius-timeout' and 'access-reject' events, the system can distinguish between the different reasons for an authentication failure. Different events are thrown by the system (for example, a received authentication reject or an unavailable RADIUS server event). This allows the control policy to specify different actions for each type of authentication failure. For example, if the RADIUS server is down or unreachable, temporary access can be given to subscribers.

This feature is available only for IP-based sessions for subscriber authentication. This feature does not support the Point-to-Point Protocol over Ethernet (PPPoE) sessions.

Uses of Control Policies

Use control policies to configure an ISG to perform specific actions in response to specific events and conditions. For example, control policies could be used for the following purposes:

- To activate a default service when a subscriber session is first detected
- To sequence the gathering of subscriber identity, where a control protocol exists on the access side
- To determine how the system responds to an idle timeout or to a subscriber who has run out of credit
- To enable transparent automatic login, which enables authorization on the basis of an IP address or MAC address
- To configure the maximum amount of time a session can remain unauthenticated
- To send periodic session state information to other devices

How to Configure an ISG Control Policy

- Configuring a Control Class Map, page 4

- Configuring a Control Policy Map, page 10
- Applying the Control Policy Map, page 14
- Monitoring and Maintaining ISG Control Policies, page 17

Configuring a Control Class Map

A control class map contains conditions that must be met for a control policy to be executed. A control class map can contain one or more conditions. Perform this task to configure a control class map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type control** [**match-all**|**match-any**|**match-none**] *class-map-name*
4. **available** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
5. **greater-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
6. **greater-than-or-equal** [**not**]**nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
7. **less-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
8. **less-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
9. **match authen-status** {**authenticated** | **unauthenticated**}
10. **match authenticated-domain** {*domain-name* | **regexp** *regular-expression*}
11. **match authenticated-username** {*username* | **regexp** *regular-expression*}
12. **match dnis** {*dnis* | **regexp** *regular-expression*}
13. **match media** {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**}
14. **match mlp-negotiated** {**no** | **yes**}
15. **match nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** {**async** | **atm** | **basic-rate**| **enm** | **ether** | **fxo** | **fxs** | **none** | **primary-rate** | **synch** | **vlan** | **vty**} | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
16. **match no-username** {**no** | **yes**}
17. **match protocol** {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**}
18. **match service-name** {*service-name* | **regexp** *regular-expression*}
19. **match source-ip-address** *ip-address subnet-mask*
20. **match timer** {*timer-name* | **regexp** *regular-expression*}
21. **match tunnel-name** {*tunnel-name* | **regexp** *regular-expression*}
22. **match unauthenticated-domain** {*domain-name* | **regexp** *regular-expression*}
23. **match unauthenticated-username** {*username* | **regexp** *regular-expression*}
24. **match vrf** {*vrf-name* | **regexp** *regular-expression}*

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	**class-map type control** [**match-all**|**match-any**|**match-none**] *class-map-name*
	Example:
	`Router(config)# class-map type control match-all class1`
		Creates or modifies a control class map, which defines the conditions under which the actions of a control policy map will be executed, and enters control class map mode.

Step 4	**available** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
	Example:
	`Router(config-control-classmap)# available nas-port`
		(Optional) Creates a condition that evaluates true if the specified subscriber identifier is locally available.

Step 5	**greater-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# greater-than nas-port type atm vpi 200 vci 100`
		(Optional) Creates a condition that evaluates true if the subscriber network access server (NAS) port identifier is greater than the specified value.

	Command or Action	Purpose

Step 6	**greater-than-or-equal** [**not**]**nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# greater-than-or-equal nas-port vlan 10`
		(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is greater than or equal to the specified value.

Step 7	**less-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# less-than nas-port type atm vpi 200 vci 105`
		(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is less than the specified value.

Step 8	**less-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# less-than-or-equal nas-port ipaddr 10.10.10.10`
		(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is less than or equal to the specified value.

Step 9	**match authen-status** {**authenticated** | **unauthenticated**}
	Example:
	`Router(config-control-classmap)# match authen-status authenticated`
		(Optional) Creates a condition that evaluates true if a subscriber’s authentication status matches the specified authentication status.

Step 10	**match authenticated-domain** {*domain-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match authenticated-domain cisco.com`
		(Optional) Creates a condition that evaluates true if a subscriber’s authenticated domain matches the specified domain.

	Command or Action	Purpose

Step 11	**match authenticated-username** {*username* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match authenticated-username regexp "admin@.*com"`
		(Optional) Creates a condition that evaluates true if a subscriber’s authenticated username matches the specified username.

Step 12	**match dnis** {*dnis* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match dnis reg-exp 5551212`
		(Optional) Creates a condition that evaluates true if a subscriber’s Dialed Number Identification Service number (DNIS number, also referred to as *called-party number*) matches the specified DNIS number.

Step 13	**match media** {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**}
	Example:
	`Router(config-control-classmap)# match media atm`
		(Optional) Creates a condition that evaluates true if a subscriber’s access media type matches the specified media type.

Step 14	**match mlp-negotiated** {**no** | **yes**}
	Example:
	`Router(config-control-classmap)# match mlp-negotiated yes`
		(Optional) Creates a condition that evaluates true or false depending on whether the subscriber’s session was established using multilink PPP negotiation.
		• If the **yes** keyword is used, the condition evaluates true if the subscriber’s session was established using multilink PPP negotiation.

Step 15	**match nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** {**async** | **atm** | **basic-rate**| **enm** | **ether** | **fxo** | **fxs** | **none** | **primary-rate** | **synch** | **vlan** | **vty**} | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
	Example:
	`Router(config-control-classmap)# match nas-port type ether slot 3`
		(Optional) Creates a condition that evaluates true if a subscriber’s NAS port identifier matches the specified value.

	Command or Action	Purpose

Step 16	**match no-username** {**no** | **yes**}
	Example:
	`Router(config-control-classmap)# match no-username yes`
		(Optional) Creates a condition that evaluates true or false depending on whether or not a subscriber's username is available.
		• If the **yes** keyword is used, the condition evaluates true if the subscriber's username is not available.

Step 17	**match protocol** {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**}
	Example:
	`Router(config-control-classmap)# match protocol ip`
		(Optional) Creates a condition that evaluates true if a subscriber's access protocol type matches the specified protocol type.

Step 18	**match service-name** {*service-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match service-name service1`
		(Optional) Creates a condition that evaluates true if the service name associated with a subscriber matches the specified service name.

Step 19	**match source-ip-address** *ip-address subnet-mask* **Example:** `Router(config-control-classmap)# match source-ip-address 10.10.10.10 255.255.255.255`	(Optional) Creates a condition that evaluates true if a subscriber's source IP address matches the specified IP address.

Step 20	**match timer** {*timer-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match timer TIMERA`
		(Optional) Creates a condition that evaluates true upon expiry of a specified policy timer.

Step 21	**match tunnel-name** {*tunnel-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match tunnel-name regexp L.*`
		(Optional) Creates a condition that evaluates true if a subscriber's virtual private dialup network (VPDN) tunnel name matches the specified tunnel name.

Step 22	**match unauthenticated-domain** {*domain-name* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match unauthenticated-domain example.com`
		(Optional) Creates a condition that evaluates true if a subscriber's unauthenticated domain name matches the specified domain name.

	Command or Action	Purpose

Step 23	**match unauthenticated-username** {*username* | **regexp** *regular-expression*}
	Example:
	`Router(config-control-classmap)# match unauthenticated-username regexp examplename1`
		(Optional) Creates a condition that evaluates true if a subscriber's unauthenticated username matches the specified username.

Step 24	**match vrf** {*vrf-name* | **regexp** *regular-expression}*
	Example:
	`Router(config-control-classmap)# match vrf regexp examplename2`
		(Optional) Creates a condition that evaluates true if a subscriber's VPN routing and forwarding (VRF) matches the specified VRF.

Configuring a Control Policy Map

A control policy map contains one or more control policy rules that associate a control class with one or more actions. Perform this task to configure a control policy map.

Note The actions that can be configured in a policy rule depend on the type of event that is specified by the **class type control** command. For example, if the **account-logoff** event is specified, the only action that can be configured in that policy rule is **service**. The procedure in this section shows all actions that can be configured in a policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} [**event** {**access-reject**| **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **quota-depleted** | **radius-timeout** | **service-failed**| **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}]
5. *action-number* **authenticate aaa list** *list-name*
6. *action-number* **authorize use method** {**aaa**|**legacy**|**rm**|**sgf**|**ssg**|**xconnect**}[**aaa** *parameter-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect**| **circuit-id**| **dnis** | **mac-address** | **nas-port** | **remote-id**| **source-ip-address** | **tunnel-name**| **unauthenticated-domain** | **unauthenticated-username**|**vendor-class-id**}
7. *action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username | vrf**}
8. *action-number* **if upon network-service-found** {**continue** | **stop**}
9. *action-number* **proxy accounting aaa list** {*list-name*| **default**}
10. *action-number* **service** [**disconnect** | **local** | **vpdn**]
11. *action-number* **service-policy type control** *policy-map-name*
12. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
13. *action-number* **set** *name* **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address**| **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**| **vrf**}
14. *action-number* **set-timer** *name-of-timer minutes*
15. *action-number* **substitute** *name matching-pattern pattern-string*
16. **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	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control MY-POLICY`	Creates or modifies a control policy map, which is used to define a control policy.

Step 4	**class type control** {*control-class-name* | **always**} [**event** {**access-reject**| **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **quota-depleted** | **radius-timeout** | **service-failed**| **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}]
	Example:
	`Router(config-control-policymap)# class type control always event session-start`
		Specifies a control class for which actions may be configured.
		• A policy rule for which the control class is **always** will always be treated as the lowest priority rule within the control policy map.

Step 5	*action-number* **authenticate aaa list** *list-name* **Example:** `Router(config-control-policymap-class-control)# 1 authenticate aaa list LIST1`	(Optional) Initiates an authentication request.

Step 6	*action-number* **authorize use method** {**aaa**|**legacy**|**rm**|**sgf**|**ssg**|**xconnect**}[**aaa** *parameter-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect**| **circuit-id**| **dnis** | **mac-address** | **nas-port** | **remote-id**| **source-ip-address** | **tunnel-name**| **unauthenticated-domain** | **unauthenticated-username**|**vendor-class-id**}
	Example:
	`Router(config-control-policymap-class-control)# 1 authorize identifier source-ip-address`
		(Optional) Initiates a request for authorization on the basis of the specified identifier.

	Command or Action	Purpose

Step 7	*action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username** | **vrf**}
	Example:
	`Router(config-control-policymap-class-control)# 1 collect identifier authen-status`
		(Optional) Collects the specified subscriber identifier from the access protocol.

Step 8	*action-number* **if upon network-service-found** {**continue** | **stop**}
	Example:
	`Router(config-control-policymap-class-control)# 2 if upon network-service-found stop`
		(Optional) Specifies whether the system should continue processing policy rules once the subscriber's network service has been identified.

Step 9	*action-number* **proxy accounting aaa list** {*list-name*| **default**} **Example:** `Router(config-control-policymap-class-control)# 1 proxy accounting aaa list default`	(Optional) Specifies the list that the request should be proxied to.
Step 10	*action-number* **service** [**disconnect** | **local** | **vpdn**] **Example:** `Router(config-control-policymap-class-control)# 3 service disconnect`	(Optional) Specifies a network service type for PPP sessions.
Step 11	*action-number* **service-policy type control** *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# service-policy type control domain based access`	(Optional) Nests the specified control policy map within a parent control policy map.

	Command or Action	Purpose

Step 12	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** |**unauthenticated-domain** | **unauthenticated-username**}}
	Example:
	`Router(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT`
		(Optional) Activates an ISG service.
		• Specifying an identifier instead of a service name will activate a service that has the same name as the specified identifier.

Step 13	*action-number* **set** *name* **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address**| **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**|**vrf**}
	Example:
	`Router(config-control-policymap-class-control)# 1 set APJ identifier authen-status`
		(Optional) Sets a variable name.

Step 14	*action-number* **set-timer** *name-of-timer minutes* **Example:** `Router(config-control-policymap-class-control)# 1 set-timer TIMERA 5`	(Optional) Starts a named policy timer. • Expiration of the timer generates the event timed-policy-expiry.
Step 15	*action-number* **substitute** *name matching-pattern pattern-string* **Example:** `Router(config-control-policymap-class-control)# 1 substitute TPK SUBA SUBB`	(Optional) Substitutes a matching pattern in variable content by a rewrite pattern.

Step 16	**end**
	Example:
	`Router(config-control-policymap-class-control)# end`
		(Optional) Ends the current configuration session and returns to privileged EXEC mode.

Applying the Control Policy Map

A control policy map must be activated by applying it to a context. Perform one or more of the following tasks to apply a control policy to a context:

- Applying a Control Policy Map Globally on the Router, page 15
- Applying an ISG Control Policy Map to an Interface or Subinterface, page 15

- Applying an ISG Control Policy Map to a Virtual Template, page 16

Applying a Control Policy Map Globally on the Router

Perform this task to apply a control policy globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service-policy type control** *policy-map-name*

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	**service-policy type control** *policy-map-name* **Example:** `Router(config)# service-policy type control policy1`	Applies a control policy.

Applying an ISG Control Policy Map to an Interface or Subinterface

Perform this task to apply an ISG control policy to an interface or subinterface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [**.** *subinterface-number*]
4. **service-policy type control** *policy-map-name*

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	**interface** *type number* [**.** *subinterface-number*] **Example:** `Router(config)# interface gigabitethernet 0/0/1.1`	Specifies an interface and enters interface configuration mode.
Step 4	**service-policy type control** *policy-map-name* **Example:** `Router(config-if)# service-policy type control policy1`	Applies a control policy.

Applying an ISG Control Policy Map to a Virtual Template

Perform this task to apply an ISG control policy map to a virtual template.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **service-policy type control** *policy-map-name*

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	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template0`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**service-policy type control** *policy-map-name* **Example:** `Router(config-if)# service-policy type control policy1`	Applies a control policy.

Monitoring and Maintaining ISG Control Policies

Optionally, you can perform this task to monitor and maintain ISG control policy operation. Steps can be performed in any order.

SUMMARY STEPS

1. **enable**
2. **show class-map type control**
3. **show policy-map type control**
4. **clear class-map control**
5. **clear policy-map control**

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	**show class-map type control** **Example:** `Router# show class-map type control`	Displays information about ISG control class maps. • The display includes statistics on the number of times a particular class has been evaluated and what the results were.
Step 3	**show policy-map type control** **Example:** `Router# show policy-map type control`	Displays information about ISG control policy maps. • The display includes statistics on the number of times each policy rule within the policy map has been executed.
Step 4	**clear class-map control** **Example:** `Router# clear class-map control`	Clears the control class map counters.
Step 5	**clear policy-map control** **Example:** `Router# clear policy-map control`	Clears the control policy map counters.

Configuration Examples for ISG Control Policies

Control Policy for Layer 2 Access and Service Provisioning Example

The following example shows how to configure a control policy that produces the following results:

- VPDN forwarding is applied to anyone dialing in from “example1.com”.
- Access to locally terminated Layer 3 network resources is provided to anyone dialing in from “example2.com”.
- Anyone else is barred.

```
! Configure the control class maps.
class-map type control match-all MY-FORWARDED-USERS
```

```
 match unauthenticated-domain "example1.com"
!

class-map type control match-all MY-LOCAL-USERS
 match unauthenticated-domain "example2.com"
!
! Configure the control policy map.
policy-map type control MY-POLICY
 class type control MY-FORWARDED-USERS event session-start
  1 service-policy type service identifier nas-port
  2 service local
!
 class type control MY-LOCAL-USERS event session-start
  1 service local
!
 class type control always event session-start
  2 service disconnect
!
! Apply the control policy to dialer interface 1.
interface Dialer1
 service-policy type control MY-POLICY
```

Verifying a Control Policy Examples

The following examples show sample output generated from the configuration in the Control Policy for Layer 2 Access and Service Provisioning Example:

```
Router# show users

Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00
Interface User Mode Idle Peer Address
Vi1.1 user1@xyz.com PPPoE - 10.1.126.14
Vi1.2 user2@abc.com PPPoE - 10.1.126.15

Router# show subscriber session

Current Subscriber Information: Total sessions 2
Uniq ID Interface State Service Identifier Up-time
2022 Vi1.1 authen Local Term user1@xyz.com 00:08:41
2023 Vi1.2 authen Local Term user2@abc.com 00:08:40
MCP_BBA_8#show subscriber session
MCP_BBA_8#show subscriber session uid 2022 detailed
Unique Session ID: 2022
Identifier: user1@xyz.com
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:08:57, Last Changed: 00:08:57
Interface: Virtual-Access1.1
Policy information:
Context 2C655DF0: Handle A2070D8D
AAA_id 00007DE8: Flow_handle 0
Authentication status: authen
Downloaded User profile, excluding services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Downloaded User profile, including services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Config history for session (recent to oldest):
Access-type: PPP Client: SM
Policy event: Process Config Connecting
Profile name: apply-config-only, 3 references
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
```

```
ssg-account-info ''QU;10000;D;20000''
Rules, actions and conditions executed:
subscriber rule-map ppp-users
condition always event session-start
1 collect identifier unauthenticated-domain
2 service-policy type control MY-POLICY
subscriber condition-map match-all MY-FORWARDING-USERS
match identifier unauthenticated-domain xyz.com [TRUE]
subscriber rule-map MY-POLICY
condition MY-FORWARDING-USERS event session-start
1 service local
subscriber rule-map ppp-users
condition always event session-start
2 service-policy type control MY-POLICY
Session inbound features:
Feature: Policing
Upstream Params:
Average rate = 10000, Normal burst = 1875, Excess burst = 3750
Config level = Per-user
Session outbound features:
Feature: Policing
Dnstream Params:
Average rate = 20000, Normal burst = 3750, Excess burst = 7500
Config level = Per-user
Non-datapath features:
Feature: Session Timeout
Timeout value is 720 seconds
Time remaining is 00:02:56
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:09:03
Router# show subscriber session uid 2023 detailed
Unique Session ID: 2023
Identifier: user2@abc.com
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:09:17, Last Changed: 00:09:17
Interface: Virtual-Access1.2
Policy information:
Context 2C656120: Handle F4070D8E
AAA_id 00007DE9: Flow_handle 0
Authentication status: authen
Downloaded User profile, excluding services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Downloaded User profile, including services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Config history for session (recent to oldest):
Access-type: PPP Client: SM
Policy event: Process Config Connecting
Profile name: apply-config-only, 3 references
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Rules, actions and conditions executed:
subscriber rule-map ppp-users
condition always event session-start
1 collect identifier unauthenticated-domain
2 service-policy type control MY-POLICY
subscriber condition-map match-all MY-FORWARDING-USERS
match identifier unauthenticated-domain xyz.com [FALSE]
subscriber rule-map MY-POLICY
condition MY-FORWARDING-USERS event session-start
subscriber condition-map match-all MY-LOCAL-USERS
match identifier unauthenticated-domain abc.com [TRUE]
subscriber rule-map MY-POLICY
condition MY-LOCAL-USERS event session-start
1 service local
```

```
subscriber rule-map ppp-users
condition always event session-start
2 service-policy type control MY-POLICY
Session inbound features:
Feature: Policing
Upstream Params:
Average rate = 10000, Normal burst = 1875, Excess burst = 3750
Config level = Per-user
Session outbound features:
Feature: Policing
Dnstream Params:
Average rate = 20000, Normal burst = 3750, Excess burst = 7500
Config level = Per-user
Non-datapath features:
Feature: Session Timeout
Timeout value is 720 seconds
Time remaining is 00:02:40
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:09:19
```

Control Policy for Restricting Access on the Basis of Interface and Access Media Example

This example shows how to configure a control policy to allow access only to users who enter the router from a particular interface and access type. In this case, only PPPoE users will be allowed; everyone else is barred.

The first condition class map “MATCHING-USERS” evaluates true only if all of the lines within it also evaluate true; however, within “MATCHING-USERS” is a nested class map (second condition), “NOT-ATM”. This nested class map represents a subcondition that must also evaluate to true. Note that the class map “NOT-ATM” specifies “match-none”. This means that “NOT-ATM” evaluates to true only if every condition line within it evaluates to false.

The third condition specifies matching on the NAS port associated with this subscriber. Specifically, only subscribers that arrive on a Gigabit Ethernet interface and on slot 3 will evaluate to true.

```
! Configure the control class maps.
class-map type control match-all MATCHING-USERS
 class type control NOT-ATM
 match media ether
 match nas-port type ether slot 3
!
class-map type control match-none NOT-ATM
 match media atm
!
```

If the conditions in the class map “MATCHING-USERS” evaluate to true, the first action to be executed is to authenticate the user. If authentication is successful, the service named “service1” will be downloaded and applied. Finally, a Layer 3 service is provided.

If “MATCHING-USERS” is not evaluated as true, the “always” class will apply, which results in barring anyone who does not match “MATCHING-USERS”.

```
! Configure the control policy map.
policy-map type control my-pppoe-rule
 class type control MATCHING-USERS event session-start
  1 authenticate aaa list XYZ
  2 service-policy type service service1
  3 service local
!
```

class type control always

```
  1 service disconnect
```

```
!
! Apply the control policy to an interface.
interface gigabitethernet3/0/0
 service-policy type control my-pppoe-rule
```

Finally, the policy is associated with an interface.

Default Method Lists

If you specify the default method list for any of the control policy actions, the default list will not display in the output from the **show running-config** command. For example, if you configure the following command:

```
Router(config-control-policymap-class-control)# 1 authenticate aaa list default
```

The following will display in the output from the **show running-config** command:

```
1 authenticate
```

Control Policies for Automatic Subscriber Login Example

In the following example, if the client is from the a subnet, automatic subscriber login is applied and an authorization request is sent to the list TALLIST with the subscriber’s source IP address as the username. If the authorization request is successful, any automatic activation services specified in the returned user profile are activated for the session and the execution of rules within the control policy stops. If the authorization is not successful, the rule execution proceeds, and the subscriber is redirected to the policy server to log in. If the subscriber does not log in within five minutes, the session is disconnected.

```
interface GigabitEthernet0/0/0
 service-policy type control RULEA
aaa authentication login TALLIST group radius
aaa authentication login LOCAL local
access-list 100 permit ip any any
class-map type traffic match-any all-traffic
 match access-group input 100
 match access-group output 100
```

policy-map type service redirectprofile

```
 class type traffic all-traffic
  redirect to ip 10.0.0.148 port 8080
class-map type control match-all CONDA
 match source-ip-address 209.165.201.1 255.255.255.0
!
class-map type control match-all CONDF
 match timer TIMERB
 match authen-status unauthenticated
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 apply aaa list LOCAL service redirectprofile
  3 set-timer TIMERB 5 minutes
 class type control CONDF event timed-policy-expiry
```

1 service disconnect

Additional References

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*
Traffic Policies	"Configuring ISG Subscriber Services" module in this guide

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	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 Control Policies

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 ISG Control Policies

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: Policy: Domain Based (Autodomain, Proxy)	Cisco IOS XE Release 2.2	ISG control policies manage the primary services and rules used to enforce particular contracts. These policies include programmable interfaces to dynamic triggers and conditional logic to be applied to flows within a session, or other characteristics of a session, upon meeting the policy criteria. Policies can be configured to interpret the domain as a request to activate the service associated with that domain name, allowing users to automatically receive services in accordance with the domain to which they are attempting to connect.
ISG: Policy Control: Policy: Triggers	Cisco IOS XE Release 2.2	ISG control policies can be configured with time-based, volume-based, and duration-based policy triggers. Time-based triggers use an internal clock, allowing policies to be applied at specific times. Volume-based triggers are based on packet count; when the packet count reaches a specified value, the specified policy is applied. Duration-based triggers are based on an internal timer. Upon expiration of the timer, the specified policy is applied.

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: Multidimensional Identity per Session	Cisco IOS XE Release 2.2	ISG control policies provide a flexible way to collect pieces of subscriber identity information during session establishment. Control policies also allow session policy to be applied iteratively as more elements of identity information become available to the system.
ISG: Policy Control: Cisco Policy Language	Cisco IOS XE Release 2.2	ISG control policies are a structured replacement for feature-specific configuration commands and allow configurable functionality to be expressed in terms of an event, a condition, and an action. Control policies provide an intuitive and extensible framework, with a consistent set of CLI commands, for specifying system behavior.
ISG: Policy Control: Differentiated Initial Policy Control	Cisco IOS XE Release 2.5.0	This features provides the ability to distinguish RADIUS authentication rejects from RADIUS server unavailability. It allows minimal or temporary network access to the subscribers when the RADIUS servers are down or cannot be accessed because of network problems or when an authentication reject is received for a subscriber. In Cisco IOS Release 12.2(33)XNE, support was added for the Cisco 10000 Series Routers. The following command was introduced or modified:**class type control**.

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.