po - pq

police

To apply QoS policing to a class map, use the **police** command in class configuration mode. To remove rate limiting, use the **no** form of this command.

police { **output** | **input** } *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]
no police

Syntax Description

conform-rate	Sets the rate limit for this traffic class, from 8000 and 2000000000 bits per second. For the ASA virtual and Firepower 4100/9300, the range is 8000-100000000000. For example, to limit traffic to 5Mbps, enter 5000000.
conform-burst	Specifies the maximum number of instantaneous bytes allowed in a sustained burst before throttling to the conforming rate value, between 1000 and 512000000 bytes. For the ASA virtual and Firepower 4100/9300, the range is 1000-25600000000. If you omit this parameter, the default value is 1/32 of the conform-rate in bytes (that is, with a conform rate of 100,000, the default conform-burst value would be 100,000/32 = 3,125). Note that the conform-rate is in bits/second, whereas the conform-burst is in bytes.
conform-action [**drop** | **transmit**]	Sets the action to take when the traffic is below the policing rate and burst size. You can **drop** or **transmit** the traffic. The default is to transmit the traffic.
exceed-action [**drop** | **transmit**]	Sets the action to take when traffic exceeds the policing rate and burst size. You can **drop** or **transmit** packets that exceed the policing rate and burst size. The default is to drop excess packets.
input	Enables policing of traffic flowing in the input direction.
output	Enables policing of traffic flowing in the output direction.

Command Default

No default behavior or variables.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The **input** option was added. Policing traffic in the inbound direction is now supported.

Usage Guidelines

Policing is a way of ensuring that no traffic exceeds the maximum rate (in bits/second) that you configure, thus ensuring that no one traffic flow can take over the entire resource. When traffic exceeds the maximum rate, the ASA drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

To enable policing, use the Modular Policy Framework:

1.class-map—Identify the traffic on which you want to perform policing.

2.policy-map—Identify the actions associated with each class map.

- **a.class**—Identify the class map on which you want to perform actions.
- **b.police**—Enable policing for the class map.

3.service-policy—Assigns the policy map to an interface or globally.

You can configure each of the QoS features alone if desired for the ASA. Often, though, you configure multiple QoS features on the ASA so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + policing (for the rest of the traffic).

You cannot configure priority queuing and policing for the same set of traffic.

- Traffic shaping (for all traffic on an interface) + hierarchical priority queuing (for a subset of traffic).

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the ASA does not restrict you from configuring this.

See the following guidelines:

- QoS is applied unidirectionally; only traffic that enters the interface to which you apply the policy map is affected (or exits the interface, depending on the whether you specify **input** or **output**).
- If a service policy is applied or removed from an interface that has existing traffic already established, the QoS policy is not applied or removed from the traffic stream. To apply or remove the QoS policy for such connections, you must clear the connections and re-establish them. See the **clear conn** command.
- To-the-box traffic is not supported.
- Traffic to and from a VPN tunnel bypass interface is not supported.
- When you match a tunnel group class map, only outbound policing is supported.

Examples

The following is an example of a **police** command for the output direction that sets the conform rate to 100,000 bits per second, with a burst value of 20,000 bytes.

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class-map firstclass
ciscoasa(config-cmap)# class localclass

ciscoasa(config-pmap-c)# police output 100000 20000
ciscoasa(config-cmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

The following example shows how to do rate-limiting on traffic destined to an internal web server:

```
ciscoasa# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
ciscoasa# class-map http_traffic
ciscoasa(config-cmap)# match access-list http_traffic
ciscoasa(config-cmap)# policy-map outside_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# police input 56000
ciscoasa(config-pmap-c)# service-policy outside_policy interface outside
ciscoasa(config)#
```

Related Commands

class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

policy

To specify the source for retrieving the CRL, use the **policy** command in ca-crl configuration mode.

policy { **static** | **cdp** | **both** }

Syntax Description

both	Specifies that if obtaining a CRL using the CRL distribution point fails, retry using static CDPs up to a limit of five.
cdp	Uses the CDP extension embedded within the certificate being checked. In this case, the ASA retrieves up to five CRL distributions points from the CDP extension of the certificate being verified and augments their information with the configured default values, if necessary. If the ASA attempt to retrieve a CRL using the primary CDP fails, it retries using the next available CDP in the list. This continues until either the ASA retrieves a CRL or exhausts the list.
static	Uses up to five static CRL distribution points. If you specify this option, specify also the LDAP or HTTP URLs with the **protocol** command.

Command Default

The default setting is **cdp**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crl configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters ca-crl configuration mode, and configures CRL retrieval to occur using the CRL distribution point extension in the certificate being checked or if that fails, to use static CDPs:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# policy both
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
url	Creates and maintains a list of static URLs for retrieving CRLs.

policy-list

To create a Border Gateway Protocol (BGP) policy list, use the **policy-list** command in policy-map configuration mode. To remove a policy list, use the **no** form of this command.

policy-list *policy-list-name* { **permit** | **deny** }
no policy-list *policy-list-name*

Syntax Description

policy-list-name	Name of the configured policy list.
permit	Permits access for matching conditions.
deny	Denies access for matching conditions.

Command Default

This command is not enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

When a policy list is referenced within a route map, all the match statements within the policy list are evaluated and processed. Two or more policy lists can be configured with a route map. Policy- lists configured within a route map are evaluated with AND semantics or OR semantics. A policy list can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy list. When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

The policy-list sub-commands are listed here:

Sub-Commands	Details
match as-path [path-list-number]	Matches as-path and it can take multiple as-path path-list numbers
Match community[community-name][exact-match]	Community name is must and exact-match is optional. Multiple names can be given
Match interface [interface-name]	Can take Multiple interface names

Sub-Commands	Details
match metric <0-4294967295>	It can take multiple numbers
Match ip address [acl name prefix-list [prefix-listname]]	Can take multiple names for acl and also for prefix-list, but one cannot exist with other – either policy-list can have prefixlist or acl
Match ip next-hop [acl name | prefix-list [prefix-listname]]	Can take multiple names for acl and also for prefix-list, but one cannot exist with other – either policy-list can have prefixlist or acl
Match ip route-source [acl name | prefix-list [prefix-listname]]	Can take multiple names for acl and also for prefix-list, but one cannot exist with other – either policy-list can have prefixlist or acl
Default match	Default will have all above options under “match”
Help	Helps for the subsequent commands
No	Negation of the commands
Exit	Exit policy-map mode

Examples

In the following example, a policy list is configured that permits all network prefixes that match AS 1 and metric 10:

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-1 permit
ciscoasa(config-policy-list)# match as-path 1
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

In the following example, a policy list is configured that permits traffic that matches community 20 and metric 10:

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-2 permit
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

In the following example, a policy list is configured that denies traffic that matches community 20 and metric 10:

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-3 deny
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
```

policy-map

When using the Modular Policy Framework, assign actions to traffic that you identified with a Layer 3/4 class map (the **class-map** or **class-map type management** command) by using the **policy-map** command (without the **type** keyword) in global configuration mode. To remove a Layer 3/4 policy map, use the **no** form of this command.

policy-map*name*
no policy-map *name*

Syntax Description

name	Specifies the name for this policy map up to 40 characters in length. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map.

Command Default

By default, the configuration includes a policy that matches all default application inspection traffic and applies certain inspections to the traffic on all interfaces (a global policy). Not all inspections are enabled by default. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one. (An interface policy overrides the global policy for a particular feature.)

The default policy includes the following application inspections:

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP Options

The default policy configuration includes the following commands:

```
class-map inspection_default
 match default-inspection-traffic
```

```
policy-map type inspect dns preset_dns_map
 parameters
message-length maximum client auto
message-length maximum 512
dns-guard
protocol-enforcement
nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1.Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.

2.(Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.

3.Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.

4.Activate the actions on an interface using the **service-policy** command.

The maximum number of policy maps is 64, but you can only apply one policy map per interface. You can apply the same policy map to multiple interfaces. You can identify multiple Layer 3/4 class maps in a Layer 3/4 policy map (see the **class** command), and you can assign multiple actions from one or more feature types to each class map.

Examples

The following is an example of a **policy-map** command for connection policy. It limits the number of connections allowed to the web server 10.1.1.1:

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

The following example shows how multi-match works in a policy map:

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

The following example shows how traffic matches the first available class map, and will not match any subsequent class maps that specify actions in the same feature domain:

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

When a Telnet connection is initiated, it matches **class telnet_traffic**. Similarly, if an FTP connection is initiated, it matches **class ftp_traffic**. For any TCP connection other than Telnet and FTP, it will match **class tcp_traffic**. Even though a Telnet or FTP connection can match **class tcp_traffic**, the ASA does not make this match because they previously matched other classes.

NetFlow events are configured through Modular Policy Framework. If Modular Policy Framework is not configured for NetFlow, no events are logged. Traffic is matched based on the order in which classes are configured. After a match is detected, no other classes are checked. For NetFlow events, the configuration requirements are as follows:

- A flow-export destination (that is, a NetFlow collector) is uniquely identified by its IP address.

- Supported event types are flow-create, flow-teardown, flow-denied, flow-update, and all, which include the four previously listed event types.
- Use the **flow-export event-type** {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination** command to configure the address of NetFlow collectors and filters to determine which NetFlow records should be sent to each collector.
- Flow-export actions are not supported in interface policies.
- Flow-export actions are only supported in the **class-default** command and in classes with the **match any** or **match access-list** command.
- If no NetFlow collector has been defined, no configuration actions occur.
- NetFlow Secure Event Logging filtering is order-independent.

The following example exports all NetFlow events between hosts 10.1.1.1 and 20.1.1.1 to destination 15.1.1.1.

```
ciscoasa(config)# access-list
 flow_export_acl
 permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_classciscoasa(config-cmap)# match access-list
flow_export_aclciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class
flow_export_classciscoasa(config-pmap-c)# flow-export event-type all destination
15.1.1.1
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
clear configure policy-map	Removes all policy map configuration. If a policy map is in use in a **service-policy** command, that policy map is not removed.
class-map	Defines a traffic class map.
service-policy	Assigns the policy map to an interface or globally to all interfaces.
show running-config policy-map	Display all current policy map configurations.

policy-map type inspect

When using the Modular Policy Framework, define special actions for inspection application traffic by using the **policy-map type inspect** command in global configuration mode. To remove an inspection policy map, use the **no** form of this command.

policy-map type inspect *application policy_map_name*
no policy-map [**type inspect** *application*] *policy_map_name*

Syntax Description

application — Specifies the type of application traffic you want to act upon. Available types include:

- **dcerpc**
- **diameter**
- **dns**
- **esmtp**
- **ftp**
- **gtp**
- **h323**
- **http**
- **im**
- **ip-options**
- **ipsec-pass-thru**
- **ipv6**
- **lisp**
- **m3ua**
- **mgcp**
- **netbios**
- **radius-accounting**
- **rtsp**
- **scansafe**
- **sctp**
- **sip**
- **skinny**
- **snmp**

policy_map_name	Specifies the name for this policy map up to 40 characters in length. Names that begin with "_internal" or "_default" are reserved and cannot be used. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.2(1)	The **ipv6** keyword was added to support IPv6 inspection.
9.0(1)	The **scansafe** keyword was added to support Cloud Web Security.
9.5(2)	The **lisp** keyword was added to support LISP inspection.
9.5(2)	The **diameter** and **sctp** keywords were added.
9.6(2)	The **m3ua** keywords were added.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine using the **inspect** command in the Layer 3/4 policy map (the **policy-map** command), you can also optionally enable actions as defined in an inspection policy map created by the **policy-map type inspect** command. For example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

An inspection policy map consists of one or more of the following commands entered in policy-map configuration mode. The exact commands available for an inspection policy map depends on the application.

- **match** command—You can define a **match** command directly in the inspection policy map to match application traffic to criteria specific to the application, such as a URL string. Then you enable actions in match configuration mode such as **drop**, **reset**, **log**, and so on. The **match** commands available depend on the application.
- **class** command—This command identifies an inspection class map in the policy map (see the **class-map type inspect** command to create the inspection class map). An inspection class map includes **match** commands that match application traffic with criteria specific to the application, such as a URL string, for which you then enable actions in the policy map. The difference between creating a class map and using a **match** command directly in the inspection policy map is that you can group multiple matches, and you can reuse class maps.

- **parameters** command—Parameters affect the behavior of the inspection engine. The commands available in parameters configuration mode depend on the application.

You can specify multiple **class** or **match** commands in the policy map.

Some **match** commands can specify regular expressions to match text inside a packet. See the **regex** command and the **class-map type regex** command, which groups multiple regular expressions.

The default inspection policy map configuration includes the following commands:

```
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
```

If a packet matches multiple different **match** or **class** commands, then the order in which the ASA applies the actions is determined by internal ASA rules, and not by the order they are added to the policy map. The internal rules are determined by the application type and the logical progression of parsing a packet, and are not user-configurable. For example for HTTP traffic, parsing a Request Method field precedes parsing the Header Host Length field; an action for the Request Method field occurs before the action for the Header Host Length field. For example, the following match commands can be entered in any order, but the **match request method get** command is matched first.

```
ciscoasa(config-pmap)# match request header host length gt 100
ciscoasa(config-pmap-c)# reset
ciscoasa(config-pmap-c)# match request method get
ciscoasa(config-pmap-c)# log
```

If an action drops a packet, then no further actions are performed. For example, if the first action is to reset the connection, then it will never match any further **match** commands. If the first action is to log the packet, then a second action, such as resetting the connection, can occur. (You can configure both the **reset** (or **drop-connection**, and so on.) and the **log** action for the same **match** command, in which case the packet is logged before it is reset for a given match.)

If a packet matches multiple **match** or **class** commands that are the same, then they are matched in the order they appear in the policy map. For example, for a packet with the header length of 1001, it will match the first command below, and be logged, and then will match the second command and be reset. If you reverse the order of the two **match** commands, then the packet will be dropped and the connection reset before it can match the second **match** command; it will never be logged.

```
ciscoasa(config-pmap)# match request header length gt 100
ciscoasa(config-pmap-c)# log
ciscoasa(config-pmap-c)# match request header length gt 1000
ciscoasa(config-pmap-c)# reset
```

A class map is determined to be the same type as another class map or **match** command based on the lowest priority **match** command in the class map (the priority is based on the internal rules). If a class map has the same type of lowest priority **match** command as another class map, then the class maps are matched according to the order they are added to the policy map. If the lowest priority command for each class map is different, then the class map with the higher priority **match** command is matched first.

If you want to exchange an in-use inspection policy map for a different map name, you must remove the **inspect** *protocol map* command, and enter it again with the new map. For example:

```
ciscoasa(config)# policy-map test
ciscoasa(config-pmap)# class sip
ciscoasa(config-pmap-c)# no
 inspect sip sip-map1
ciscoasa(config-pmap-c)# inspect sip sip-map2
```

Examples

The following is an example of an HTTP inspection policy map and the related class maps. This policy map is activated by the Layer 3/4 policy map, which is enabled by the service policy.

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match
 regex
 example
ciscoasa(config-cmap)# match
 regex
 example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
(a Layer 3/4 class map not shown)
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy inbound_policy interface outside
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
parameters	Enters parameter configuration mode for an inspection policy map.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

policy-route

To configure policy-based routing on an interface, use the **policy-route** command in interface configuration mode.

policy-route { **route-map** *route_map_name* | **cost** *value* | **path-monitoring** { **IPv4** | **IPv6** | **auto** | **auto4** | **auto6** }
no policy-route { **route-map** *route_map_name* | **cost** *value* | **path-monitoring** { **IPv4** | **IPv6** | **auto** | **auto4** | **auto6** }

Syntax Description

cost *value*	Sets the relative cost of the interface for policy-based routing evaluation. The value can be 1-65535. The default is 0, which you can reset by using the **no** version of the command. The lower the number, the higher the priority. For example, 1 has priority over 2.
route-map*route_map_name*	Specifies the name of the route map to use for policy-based routing.
path-monitoring	Set the monitoring type for the interface's peer to collect the flexible metrics.

Command Default

There is no default route map. The default cost is 0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.
9.17(1)	The **cost** keyword was added.
9.18(1)	This command was enhanced to include path-monitoring feature for PBR to determine the best path for routing traffic.

Usage Guidelines

After configuring the route-map that specifies the match criteria and the resulting action if all of the match clauses are met, use the **policy-route route-map** command to apply it to a particular interface.

If you use **set adaptive-interface cost** as a criteria in the route map, set the cost on the interface using the **policy-route cost** command.

When you set policy-route cost, and use the **set adaptive-interface cost** command in the route map, the egress traffic is round-robin load balanced across any selected interfaces (assuming they are up) that have the same interface cost. If costs are different, higher cost interfaces are used as backups to the lowest cost interface.

For example, by setting the same cost on 2 WAN links, you can load balance the traffic across those links to perhaps improve performance. However, if one WAN link has higher bandwidth than the other, you can set the higher bandwidth link's cost to 1, and the lower bandwidth link to 2, so that the lower bandwidth link is used only if the higher bandwidth link is down.

Examples

The following example applies a route map to an interface for policy-based routing.

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmapv4
ciscoasa(config)# show run interface GigabitEthernet0/0
!
interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  policy-route route-map testmapv4
!
ciscoasa(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
       ip address (access-lists): testaclv4
   Set clauses:
               ip next-hop 1.1.1.1
```

The following example sets unequal costs, so that output1 is the preferred link, and output2 is used only if output1 is down. To configure load balancing across the interfaces, set equal cost values.

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

The path monitoring feature detects a failure in a route link or path that is no longer forwarding traffic. It enables threat defense to collect performance metrics like RTT, jitter, packet loss, and Mean Opinion Score (MOS) to determine the best path for forwarding the traffic.

To configure path monitoring, use the **policy-route** command. You must specify the monitoring type that the device must use to collect the performance metrics from the peer gateway. For the auto option, the next-hop of the default route is used as the peer to monitor. IPv4 is attempted first, and then IPv6. For VTI interfaces, the auto option is not supported. You must specify the IPv4 or IPv6 address of its peer.

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost             set interface cost
  path-monitoring  Keyword for path monitoring
  route-map        Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D     peer-ipv4
  X:X:X:X::X  peer-ipv6
  auto        Use remote peer IPv4/6 based on config
  auto4       Use only IPv4 address based on config
  auto6       Use only IPv6 address based on config
```

```
ciscoasa(config-if)# policy-route path-monitoring auto
```

policy-server-secret (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To configure a secret key used to encrypt authentication requests to a SiteMinder SSO server, use the **policy-server-secret** command in webvpn-sso-siteminder configuration mode. To remove a secret key, use the **no** form of this command.

policy-server-secret *secret-key*
no policy-server-secret

Note This command is required for SiteMinder SSO authentication.

Syntax Description

secret-key	The character string used as a secret key to encrypt authentication communications. There is no minimum or maximum number of characters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Config-webvpn-sso-siteminder configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. You first create the SSO server using the **sso-server** command. For SiteMinder SSO servers, the **policy-server-secret** command secures authentication communications between the ASA and the SSO server.

The command argument, *secret-key*, is similar to a password: you create it, save it, and configure it. It is configured on both the ASA using the **policy-server-secret** command and on the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.

This command applies only to the SiteMinder type of SSO server.

Examples

The following command, entered in config-webvpn-sso-siteminder mode and including a random character string as an argument, creates a secret key for SiteMinder SSO server authentication communications:

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
ciscoasa(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the ASA retries a failed SSO authentication attempt.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device
sso-server	Creates a single sign-on server.
test sso-server	Tests an SSO server with a trial authentication request.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

policy static sgt

To apply a policy to a manually configured Cisco TrustSec link, use the **policy static sgt** command in cts manual interface configuration mode. To remove a policy to a manually configured CTS link, use the **no** form of this command.

policy static sgt *sgt_number* [**trusted**]
no policy static sgt *sgt_number* [**trusted**]

Syntax Description

sgt *sgt_number*	Specifies the SGT number to apply to incoming traffic from the peer. Valid values are from 2-65519.
static	Specifies an SGT policy to incoming traffic on the link.
trusted	Indicates that ingress traffic on the interface with the SGT specified in the command should not have its SGT overwritten. Untrusted is the default.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cts manual interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

This command applies a policy to a manually configured CTS link.

Restrictions

- Supported only on physical interfaces, VLAN interfaces, port channel interfaces, and redundant interfaces.
- Not supported on logical interfaces or virtual interfaces, such as BVI, TVI, and VNI.

Examples

The following example enables an interface for Layer 2 SGT imposition and defines whether or not the interface is trusted:

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

Related Commands

Command	Description
cts manual	Enables Layer 2 SGT Imposition and enters cts manual interface configuration mode.
propagate sgt	Propagates a security group tag (called **sgt**) on an interface. Propagation is enabled by default.

polltime interface

To specify the data interface polltime and holdtime in an Active/Active failover configuration, use the **polltime interface** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

polltime interface [**msec**] *polltime* [**holdtime** *time*]
no polltime interface [**msec**] *polltime* [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time (as a calculation) between the last-received hello message from the peer unit and the commencement of interface tests to determine the health of the interface. It also sets the duration of each interface test as *holdtime* /16. Valid values are from 5 to 75 seconds. The default is 5 times the *polltime* . You cannot enter a holdtime value that is less than five times the *polltime* . To calculate the time before starting interface tests (y): **1.** x = (*holdtime* /*polltime)/2* , rounded to the nearest integer. (.4 and down rounds down; .5 and up rounds up.) **2.** y = x**polltime* For example, if you use the default holdtime of 25 and polltime of 5, then y = 15 seconds.
interface *time*	Specifies how long to wait between sending a hello packet to the peer. Valid values range from 1 to 15 seconds. The default is 5. If the optional **msec** keyword is used, the valid values are from 500 to 999 milliseconds.
msec	(Optional) Specifies that the given time is in milliseconds.

Command Default

The poll *time* is 5 seconds.

The **holdtime** *time* is 5 times the poll *time*.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The command was changed to include the optional **holdtime** *time* value and the ability to specify the poll time in milliseconds.

This command is available for Active/Active failover only. Use the **failover polltime interface** command in Active/Standby failover configurations.

With a faster polltime, the ASA can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested.

You can include both **polltime unit** and **polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through a ASA in a failover configuration, you should decrease the failover hold time on the ASA to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following partial example shows a possible configuration for a failover group. The interface poll time is set to 500 milliseconds and the hold time to 5 seconds for data interfaces in failover group 1.

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover polltime	Specifies the unit failover poll and hold times.
failover polltime interface	Specifies the interface poll and hold times for Active/Standby failover configurations.

poll-timer

To specify the timer during which the ASA queries the DNS server to resolve fully qualified domain names (FQDN) that are defined in a network object group, use the **poll-timer** command in dns server-group configuration mode for the DefaultDNS server group only. To remove the timer, use the **no** form of this command.

poll-timer minutes *minutes*
no poll-timer minutes *minutes*

Syntax Description

minutes *minutes*	Specifies the timer in minutes. Valid values are from 1 to 65535 minutes.

Command Default

By default, the DNS timer is 240 minutes or 4 hours.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
dns server-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command is supported for the DefaultDNS server group only.

This command specifies the timer during which the ASA queries the DNS server to resolve the FQDN that was defined in a network object group. A FQDN is resolved periodically when the poll DNS timer has expired or when the TTL of the resolved IP entry has expired, whichever comes first.

This command has effect only when at least one network object group has been activated.

Examples

The following example sets the DNS poll timer to 240 minutes:

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# poll-timer minutes 240
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.

Command	Description
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server-group configurations.

pop3s (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To enter POP3S configuration mode, use the **pop3s** command in global configuration mode. To remove any commands entered in POP3S command mode, use the **no** version of this command.

POP3 is a client/server protocol in which your Internet server receives and holds e-mail for you. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. This standard protocol is built into most popular e-mail products. POP3S lets you receive e-mail over an SSL connection.

pop3s
no pop3

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Examples

The following example shows how to enter POP3S configuration mode:

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)#
```

Related Commands

Command	Description
clear configure pop3s	Removes the POP3S configuration.

Command	Description
show running-config pop3s	Displays the running configuration for POP3S.

port (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify the port an e-mail proxy listens to, use the **port** command in the applicable e-mail proxy command mode. To revert to the default value, use the **no** version of this command.

port *portnum*
no port

Syntax Description

portnum	The port for the e-mail proxy to use. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Command Default

The default ports for e-mail proxies are as follows:

E-mail Proxy	Default Port
IMAP4S	993
POP3S	995
SMTPS	988

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Pop3s	• Yes	—	• Yes	—	—
Imap4s	• Yes	—	• Yes	—	—
Smtps	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Usage Guidelines

To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Examples

The following example shows how to set port 1066 for the IMAP4S e-mail proxy:

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)# port 1066
```

portal-access-rule(Deprecated)

This command allows customers to configure a global clientless SSL VPN access policy to permit or deny clientless SSL VPN sessions based on the data present in HTTP header. If denied, an error code is returned to the clients. This denial is performed before user authentication and thus minimizes the use of processing resources.

portal-access-rule none
no portal-access-rule *priority* [{ **permit** | **deny** [**code** *code*] } { **any** | **user-agent match** *string* }
no portal-access-rule *priority* [{ **permit** | **deny** [**code** *code*] } { **any** | **user-agent match** *string* }]
clear configure webvpn portal-access-rule

Syntax Description

none	Removes all portal access rules. Clientless SSL VPN sessions will not restricted based on HTTP header.
priority	Priority of rule. Range: 1-65535.
permit	Permit access based upon HTTP header.
deny	Deny access based upon HTTP header.
code	Permit or deny access based on a returned HTTP status code. Default: 403.
code	The HTTP status code number based on which you want to permit or deny access. Range: 200-599.
any	Match any HTTP header string.
user-agent match	Enable comparison of strings in HTTP headers.
string	Specify the string to match in the HTTP header. Surround the string you are searching for with wildcards (*) for a match that contains your string or do not use wildcards to specify an exact match of your string. **Note** We recommend using wildcards in your search string. Without them, the rule may not match any strings or many fewer than you expect. If the string you are searching for has a space in it, the string must be enclosed in quotations; for example, "*a string* ". When using both quotations and wild cards, your search string would look like this: "**a string* *".
no portal-access-rule	Use to delete a single portal-access-rule.
clear configure webvpn portal-access-rule	Equivalent to portal-access-rule none command.

Command Default

portal-access-rule none

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(5)	This command was added simultaneously in ASA 8.2.5 and 8.4(2).
8.4(2)	This command was added simultaneously in ASA 8.2.5 and 8.4(2).
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

This check is performed prior to user authentication.

Examples

The following example creates three portal access rules:

- Portal access rule 1 denies attempted clientless SSL VPN connections when the ASA returns code 403 and Thunderbird is in the HTTP header.
- Portal access rule 10 permits attempted clientless SSL VPN connections when MSIE 8.0 (Microsoft Internet Explorer 8.0) is in the HTTP header.
- Portal access rule 65535 permits all other attempted clientless SSL VPN connections.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
ciscoasa(config-webvpn)# portal-access-rule 10 permit user-agent match "*MSIE 8.0*"
ciscoasa(config-webvpn)# portal-access-rule 65535 permit any
```

Note If HostScan is installed, the port-access-rule feature does not stop the ASA from opening pages like Cisco Secure Desktop portal. To avoid the Cisco Secure Desktop port, HostScan needs to be uninstalled.

Related Commands

Command	Description
show run webvpn	Displays webvpn configuration including all portal-access-rules.
show vpn-sessiondb detail webvpn	Display information about VPN sessions. The command includes options for displaying information in full or in detail, lets you specify type of sessions to display, and provides options to filter and sort the information.
debug webvpn request *n*	Enables logging of debug messages at a particular level of debugging. Default: 1. Range: 1-255.

port-channel load-balance

For EtherChannels, to specify the load-balancing algorithm, use the **port-channel load-balance** command in interface configuration mode. To set the value to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

port-channel load-balance { **dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port** }
no port-channel load-balance

Syntax Description

dst-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • Destination IP address
dst-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Destination IP address • Destination Port
dst-mac	Balances the packet load on interfaces according to the following characteristics of the packet: • Destination MAC address
dst-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Destination port
src-dst-ip	(Default) Balances the packet load on interfaces according to the following characteristics of the packet: • Source IP address • Destination IP address

src-dst-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Source IP address • Destination IP address • Source Port • Destination Port
src-dst-mac	Balances the packet load on interfaces according to the following characteristics of the packet: • Source MAC address • Destination MAC address
src-dst-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Source port • Destination port
src-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • Source IP address
src-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Source IP address • Source port
src-mac	Balances the packet load on interfaces according to the following characteristics of the packet: • Source MAC address
src-port	Balances the packet load on interfaces according to the following characteristics of the packet: • Source port
vlan-dst-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Destination IP address

vlan-dst-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Destination IP address • Destination port
vlan-only	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN
vlan-src-dst-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Source IP address • Destination IP address
vlan-src-dst-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Source IP address • Destination IP address • Source port • Destination port
vlan-src-ip	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Source IP address
vlan-src-ip-port	Balances the packet load on interfaces according to the following characteristics of the packet: • VLAN • Source IP address • Source port

Command Default

The default is **src-dst-ip**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

The ASA distributes packets to the interfaces in the EtherChannel by hashing the source and destination IP address of the packet (**src-dst-ip**). The resulting hash is divided by the number of active links in a modulo operation where the resulting remainder determines which interface owns the flow. All packets with a *hash_value* **mod** *active_links* result of 0 go to the first interface in the EtherChannel, packets with a result of 1 go to the second interface, packets with a result of 2 go to the third interface, and so on. For example, if you have 15 active links, then the modulo operation provides values from 0 to 14. For 6 active links, the values are 0 to 5, and so on.

For a spanned EtherChannel in clustering, load balancing occurs on a per ASA basis. For example, if you have 32 active interfaces in the spanned EtherChannel across 8 ASAs, with 4 interfaces per ASA in the EtherChannel, then load balancing only occurs across the 4 interfaces on the ASA.

If an active interface goes down and is not replaced by a standby interface, then traffic is rebalanced between the remaining links. The failure is masked from both Spanning Tree at Layer 2 and the routing table at Layer 3, so the switchover is transparent to other network devices.

Examples

The following example sets the load-balancing algorithm to use the source and destination IP addresses and ports:

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel load-balance src-dst-ip-port
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.

Command	Description
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

port-channel min-bundle

For EtherChannels, to specify the minimum number of active interfaces required for the port-channel interface to become active, use the **port-channel min-bundle** command in interface configuration mode. To set the value to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

port-channel min-bundle *number*
no port-channel min-bundle

Syntax Description

number	Specifies the minimum number of active interfaces required for the port-channel interface to become active, between 1 and 8; for 9.2(1) and later, the active interfaces can be between 1 and 16.

Command Default

The default is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.
9.2(1)	The number of active interfaces was increased from 8 to 16.

Usage Guidelines

Enter this command for a port-channel interface. If the active interfaces in the channel group falls below this value, then the port-channel interface goes down, and could trigger a device-level failover.

Examples

The following example sets the minimum number of active interfaces required for the port-channel to become active to two:

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel min-bundle 2
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.

Command	Description
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

port-channel span-cluster

To sets this EtherChannel as a spanned EtherChannel in an ASA cluster, use the **port-channel span-cluster** command in interface configuration mode. To disable spanning, use the **no** form of this command.

Note Supported on ASA hardware models only. Other models implicitly set data EtherChannels to spanned mode.

port-channel span-cluster [**vss-load-balance**]
no port-channel span-cluster [**vss-load-balance**]

Syntax Description

vss-load-balance	(Optional) Enables VSS load balancing. If you are connecting the ASA to two switches in a VSS or vPC, then you should enable VSS load balancing. This feature ensures that the physical link connections between the ASAs to the VSS (or vPC) pair are balanced. You must configure the **vss-id** keyword in the **channel-group** command for each member interface before enabling load balancing.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You must be in spanned EtherChannel mode (**cluster interface-mode spanned**) to use this feature.

This feature lets you group one or more interfaces per unit into an EtherChannel that spans all units in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel. A spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed mode, the EtherChannel is configured as a routed interface with a single IP address. In transparent mode, the IP address is assigned to the bridge group, not to the interface. The EtherChannel inherently provides load balancing as part of basic operation.

Examples

The following example creates an EtherChannel (port-channel 2) with the tengigabitethernet 0/8 interface as the only member, and then spans the EtherChannel across the cluster. Two subinterfaces are added to port-channel 2.

```
interface tengigabitethernet 0/8
channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
interface port-channel 2.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
cluster interface-mode	Sets the cluster interface mode, for either Spanned EtherChannels or individual interfaces.

port-forward(Deprecated)

To configure the set of applications that users of clientless SSL VPN session can access over forwarded TCP ports, use the **port-forward** command in webvpn configuration mode.

port-forward { *list_name local_port remote_server remote_port description* }

To configure access to multiple applications, use this command with the same *list_name* multiple times, once for each application.

To remove a configured application from a list, use the **no port-forward** *list_name local_port* command (you need not include the *remote_server* and *remote_port* parameters).

no port-forward *listname localport*

To remove an entire configured list, use the **no port-forward** *list_name* command.

no port-forward *list_name*

Syntax Description

description	Provides the application name or short description that displays on the end user Port Forwarding Java applet screen. Maximum 64 characters.
list_name	Groups the set of applications (forwarded TCP ports) users of clientless SSL VPN sessions can access. Maximum 64 characters.
local_port	Specifies the local port that listens for TCP traffic for an application. You can use a local port number only once for a *list_name*. Enter a port number in the range 1-65535. To avoid conflicts with existing services, use a port number greater than 1024.
remote_port	Specifies the port to connect to for this application on the remote server. This is the actual port the application uses. Enter a port number in the range 1-65535 or port name.
remote_server	Provides the DNS name or IP address of the remote server for an application. If you enter the IP address, you may enter it in either IPv4 or IPv6 format. We recommend using a host name so that you do not have to configure the client applications for a specific IP addresses. The dns server-group command **name-server** must resolve the host name to an IP address.

Command Default

There is no default port forwarding list.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The command mode was changed to webvpn.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

Port forwarding does not support Microsoft Outlook Exchange (MAPI) proxy. However, you can configure Smart Tunnel support for Microsoft Outlook Exchange 2010.

Examples

The following table shows the values used for example applications.

Application	Local Port	Server DNS Name	Remote Port	Description
IMAP4S e-mail	20143	IMAP4Sserver	143	Get Mail
SMTPS e-mail	20025	SMTPSserver	25	Send Mail
DDTS over SSH	20022	DDTSserver	22	DDTS over SSH
Telnet	20023	Telnetserver	23	Telnet

The following example shows how to create a port forwarding list called *SalesGroupPorts* that provides access to these applications:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

Related Commands

Command	Description
port-forward auto-start	Entered in group-policy webvpn or username webvpn mode, this command starts port forwarding automatically and assigns the specified port forwarding list when the user logs onto a clientless SSL VPN session.
port-forward enable	Entered in group-policy webvpn or username webvpn mode, this command starts assigns the specified port forwarding list when the user logs on, but requires the user to start port forwarding manually, using the **Application Access** > **Start Applications** button on the clientless SSL VPN portal page.

Command	Description
port-forward disable	Entered in group-policy webvpn or username webvpn mode, this command turns off port forwarding.

port-forward-name(Deprecated)

To configure the display name that identifies TCP port forwarding to end users for a particular user or group policy, use the **port-forward-name** command in webvpn mode, which you enter from group-policy or username mode. To delete the display name, including a null value created by using the **port-forward-name none** command**,** use the no form of the command. The **no** option restores the default name, "Application Access." To prevent a display name, use the **port-forward none** command.

port-forward-name { **value** *name* | **none** }
no port-forward-name

Syntax Description

none	Indicates that there is no display name. Sets a null value, thereby disallowing a display name. Prevents inheriting a value.
value *name*	Describes port forwarding to end users. Maximum of 255 characters.

Command Default

The default name is "Application Access."

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Examples

The following example shows how to set the name, "Remote Access TCP Applications," for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

port-object

To add a port object to a service object group of the type TCP, UDP, or TCP-UDP, use the **port-object** command in object-group service configuration mode. To remove port objects, use the **no** form of this command.

port-object { **eq** *port* | **range** *begin_port end_port* }
no port-object { **eq** *port* | **range** *begin_port end_port* }

Syntax Description

range *begin_port end_port*	Specifies a range of ports (inclusive), between 0 and 65535.
eq *port*	Specifies the decimal number (between 0 and 65535) or name of a TCP or UDP port for a service object.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object-network service configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **port-object** command is used with the **object-group service** *protocol* command to define an object that is either a specific port or a range of ports.

If a name is specified for a TCP or UDP service, it must be one of the supported TCP or/and UDP names, and must be consistent with the protocol type of the object group. For instance, for a protocol types of tcp, udp, and tcp-udp, the names must be a valid TCP service name, a valid UDP service name, or a valid TCP and UDP service name, respectively.

If a number is specified, translation to its corresponding name (if one exists) based on the protocol type will be made when showing the object.

The following service names are supported:

TCP	UDP	TCP and UDP
bgp	biff	discard
chargen	bootpc	domain

TCP	UDP	TCP and UDP
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

Examples

This example shows how to use the **port-object** command in service configuration mode to create a new port (service) object group:

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service)# port-object eq smtp
ciscoasa(config-service)# port-object eq telnet
ciscoasa(config)# object-group service eng_service udp
ciscoasa(config-service)# port-object eq snmp
ciscoasa(config)# object-group service eng_service tcp-udp
ciscoasa(config-service)# port-object eq domain
ciscoasa(config-service)# port-object range 2000 2005
ciscoasa(config-service)# quit
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

post-max-size

To specify the maximum size allowed for an object to post, use the **post-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

post-max-size *size*
no post-max-size

Syntax Description

size	Specifies the maximum size allowed for a posted object. The range is 0 through 2147483647. Setting the size to 0 effectively disallows object posting.

Command Default

The default size is 2147483647.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example sets the maximum size for a posted object to 1500 bytes:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
post-max-size 1500
```

Related Commands

Command	Description
download-max-size	Specifies the maximum size of an object to download.
upload-max-size	Specifies the maximum size of an object to upload.

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

power inline

To enable or disable Power over Ethernet+ (PoE+) on the Firepower 1010 Ethernet 1/7 or 1/8 interface, use the **power inline** command in interface configuration mode. To return to the default state, use the **no** form of this command.

power inline { **auto** | **never** | **consumption wattage** *milliwatts* }

Note Supported for the Firepower 1010 only. Not supported for the Firepower 1010E.

Syntax Description

consumption wattage *milliwatts*	Manually specifies the wattage in milliwatts, from 4000 to 30000. Use this command if you want to set the watts manually and disable LLDP negotiation.
auto	Delivers power automatically to the powered device using a wattage appropriate to the class of the powered device. The Firepower 1010 uses LLDP to further negotiate the correct wattage.
never	Disables PoE.

Command Default

The default is **auto**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

The Firepower 1010 supports both IEEE 802.3af (PoE) and 802.3at (PoE+). PoE+ uses Link Layer Discovery Protocol (LLDP) to negotiate the power level. PoE+ can deliver up to 30 watts to a powered device. Power is only supplied when needed.

If you shut down the interface, then you disable power to the device. For the Firepower 1010, Ethernet 1/7 and 1/8 support PoE+.

Examples

The following example manually sets the wattage for Ethernet 1/7 and sets the power to auto for Ethernet 1/8:

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

Related Commands

Command	Description
show power inline	Shows PoE status.

power-supply

For dual power supplies in the ISA 3000, to establish dual power supplies as the expected configuration in the ASA OS, use the **power-supply** command in global configuration mode. To disable the dual power supply, use the **no** form of this command.

power-supply dual
no power-supply dual

Syntax Description

dual	Specifies a dual power supply.

Command Default

By default, the dual power supply is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

If one power supply fails, the ASA issues an alarm. By default, the ASA expects a single power supply and won't issue an alarm as long as it includes one working power supply.

Examples

The following example establishes the dual power supply:

```
ciscoasa(config)# power-supply dual
```

pppoe client route distance

To configure an administrative distance for routes learned through PPPoE, use the **pppoe client route distance** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

pppoe client route distance *distance*
no pppoe client route distance *distance*

Syntax Description

distance	The administrative distance to apply to routes learned through PPPoE. Valid values are from 1 to 255.

Command Default

Routes learned through PPPoE are given an administrative distance of 1 by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **pppoe client route distance** command is checked only when a route is learned from PPPoE. If the **pppoe client route distance** command is entered after a route is learned from PPPoE, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enablgin PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
```

```
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route track	Associates routes learned through PPPoE with a tracking entry object.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

pppoe client route track

To configure the PPPoE client to associate added routes with a specified tracked object number, use the **pppoe client route track** command in interface configuration mode. To remove the PPPoE route tracking, use the **no** form of this command.

pppoe client route track *number*
no pppoe client route track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **pppoe client route track** command is checked only when a route is learned from PPPoE. If the **pppoe client route track** command is entered after a route is learned from PPPoE, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enabling PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
```

```
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route distance	Assigns an administrative distance to routes learned through PPPoE.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

pppoe client secondary

To configure the PPPoE client to register as a client of a tracked object and to be brought up or down based on the tracking state, use the **pppoe client secondary** command in interface configuration mode. To remove the client registration, use the **no** form of this command.

pppoe client secondary track *number*
no pppoe client secondary track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **pppoe client secondary** command is checked only when PPPoE session starts. If the **pppoe client route track** command is entered after a route is learned from PPPoE, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enabling PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
```

```
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route distance	Assigns an administrative distance to routes learned through PPPoE.
pppoe client route track	Associates routes learned through PPPoE with a tracking entry object.
sla monitor	Defines an SLA monitoring operation.

prc-interval

To customize IS-IS throttling of partial route calculations (PRC), use the **prc-interval** command in router isis configuration mode. To restore default values, use the **no** form of this command.

prc-interval *prc-max-wait* [*prc-initial-wait prc-second-wait*]
no prc-interval

Syntax Description

prc-max-wait	Indicates the maximum interval between two consecutive PRC calculations. The range is 1 to 120 seconds.
prc-initial-wait	(Optional) Indicates the initial PRC calculation delay after a topology change. The range is 1 to 120,000 milliseconds. The default is 2000 milliseconds.
prc-second-wait	(Optional) Indicates the hold time between the first and second PRC calculation (in milliseconds). The range is 1 to 120,000 milliseconds.

Command Default

The default are:

prc-max-wait: 5 seconds

prc-initial-wait: 2000 milliseconds

prc-second-wait: 5000 milliseconds

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

PRC is the software process of calculating routes without performing a shortest path first (SPF) calculation. This is possible when the topology of the routing system itself has not changed, but a change is detected in the information announced by a particular IS or when it is necessary to attempt to reinstall such routes in the Routing Information Base (RIB).

The following description helps in determining whether to change the default values of this command:

- The *prc-initial-wait* argument indicates the initial wait time (in milliseconds) before generating the first LSP.
- The *prc-second-wait* argument indicates the amount of time to wait (in milliseconds) between the first and second LSP generation.

- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *prc-max-wait* interval specified, so this value causes the throttling or slowing down of the PRC calculation after the initial and second intervals. Once this interval is reached, the wait interval continues at this interval until the network calms down.
- After the network calms down and there are no triggers for two times the *prc-max-wait* interval, fast behavior is restored (the initial wait time).

Examples

The following example intervals for PRC.

```
ciscoasa(config)# router isis
ciscoasa(config-router)# prc-interval 2 50 100
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.

Command	Description
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.

Command	Description
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.