po - pq

管制

要将 QoS 策略管制应用于类映射，请在类配置模式下使用 **police**命令。要取消速率限制，请使用此命 **no**令的形式。

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

Syntax Description

合格率	设置此流量类别的速率限制，范围为每秒 8000 至 2000000000 比特。对于 ASA virtual 和 Firepower 4100/9300，范围为 8000-100000000000。例如，要将流量限制为 5Mbps，请输入 5000000。
conform-burst	指定控制到符合速率值之前连续突发中允许的最大即时字节数，该值介于 1000 到 512000000 字节之间。对于 ASA virtual 和 Firepower 4100/9300，范围为 1000-25600000000。 如果省略此参数，则默认值为 conform-rate（以字节为单位）的 1/32（也就是说，在符合率为 100,000 的情况下，默认 conform-burst 值为 100,000/32 = 3,125）。请注意，conform-rate 的单位为位/秒，而 conform-burst 的单位为字节。
conform-action[**drop** | **transmit**]	设置流量低于管制速率和突发大小时要执行的操作。您可以**drop**或**transmit**流量。默认为传输流量。
exceed-action[**drop** | **transmit**]	设置流量超过策略管制速率和突发大小时要执行的操作。您可以拦截超出监管速率和突发大小的数 **drop**据 **transmit**包。默认情况下会丢弃多余的数据包。
input	启用输入方向的流量监管。
output	启用输出方向的流量监管。

Command Default

无默认行为或变量。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
类配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	添加了 **input** 选项。现在支持入站方向的策略管制。

使用指南

监管是一种确保没有流量超过您配置的最大速率（以比特/秒为单位）的方法，从而确保没有任何一个流量可以接管整个资源。如果流量超过最大速率，ASA 将丢弃超额的流量。策略管制还设定了允许的单次最大突发流量。

要启用策略管制，请使用模块化策略框架：

1.class-map—识别要执行监管的流量。

2.policy-map- 标识与每个类映射关联的操作。

- **a.class**- 标识要对其执行操作的类映射。
- **b.police**- 为类映射启用策略管制。

3.service-policy- 将策略映射分配到接口或全局。

如果需要，可以为 ASA 单独配置各种 QoS 功能。不过，ASA 上通常会配置多种 QoS 功能以便可以优先排列某些流量，并防止其他流量导致带宽问题。

请参阅以下每个接口支持的功能组合：

- 标准优先级排队（针对特定流量）+ 监管（针对其余流量）。

无法对同一组的流量配置优先级排队和策略管制。

- 流量整形（适用于接口上的所有流量）+ 分级式优先级排队（适用于一部分流量）。

通常，如果您启用流量整形，也不会为相同的流量启用策略管制，但ASA不限制您进行这种配置。

请参阅以下准则：

- QoS 是单向应用的；只有进入应用策略映射的接口的流量才会受到影响（或退出接口，取决于您是否指定 **input**或 **output**）。
- 如果从已建立现有流量的接口应用或删除服务策略，则 QoS 策略不会从流量流应用或删除。要为此类连接应用或删除 QoS 策略，您必须清除连接并重新建立连接。查看命令。 **clearconn**
- 不支持到箱流量。
- 不支持进出 VPN 隧道绕行接口的流量。
- 当您匹配隧道组类映射时，仅支持出站监管。

CR_Examples

以下是输出方向的 **police** 命令的示例，该命令将符合速率设置为 100,000 位/秒，突发值为 20,000 字节。

```
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)#
```

以下示例展示如何对发往内部 Web 服务器的流量执行速率限制：

```
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	指定用于流量分类的类映射。
clearconfigurepolicy-map	删除所有策略映射配置，但如果策略映射正在用于服务策略命令，则不会删除该策略映射。
policy-map	配置策略；即流量类与一个或多个操作的关联。
showrunning-configpolicy-map	— 确定您想要执行操作的类映射。

策略

要指定检索 CRL 的源，请在 ca-crl 配置模式下使用 **policy** 命令。

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

Syntax Description

both	指定如果使用 CRL 分发点获取 CRL 失败，则使用静态 CDP 重试，最多可重试 5。
cdp	使用正在检查的证书中嵌入的 CDP 扩展。在此情况下，ASA 从正在验证的证书的 CDP 扩展检索最多五个 CRL 分发点，并在必要时使用已配置的默认值扩充其信息。如果 ASA 尝试使用主 CDP 检索 CRL 失败，它将使用列表中的下一个可用 CDP 重试。这个过程会一直持续到 ASA 检索到 CRL 或排尽列表。
static	最多使用五个静态 CRL 分发点。如果指定此选项，还需使用 **protocol** 命令指定 LDAP 或 HTTP URL。

Command Default

默认设置为 **cdp**。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Crl 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples

以下示例进入 ca-crl 配置模式，并使用正在检查的证书中的 CRL 分发点扩展来配置 CRL 检索，或者如果失败，则使用静态 CDP：

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

Related Commands

命令	说明
crlconfigure	进入 ca-crl 配置模式。
cryptocatrustpoint	进入 trustpoint 配置模式。

命令	说明
url	创建和维护用于检索 CRL 的静态 URL 列表。

policy-list

要创建边界网关协议 (BGP) 策略列表，请在策略映射配置模式下使用 **policy-list** 命令。要删除策略列表，请使用此命 **no**令的形式。

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

Syntax Description

policy-list-name	配置的策略列表的名称。
permit	允许符合条件的访问。
deny	因条件匹配而拒绝访问。

Command Default

默认情况下不启用此命令。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.2(1)	添加了此命令。

使用指南

当在路由映射中引用策略列表时，将评估和处理策略列表中的所有匹配语句。通过一个路由映射可以配置两个或更多策略列表。策略 — 使用 AND 语义或 OR 语义评估路由映射内配置的列表。策略列表也可以与任何其他预先存在的匹配共存，并设置在同一路径映射内部、策略列表外部配置的语句。当多个策略列表在路由映射条目中执行匹配时，所有策略列表仅在传入属性上进行匹配。

此处列出 policy-list 子命令：

子命令	详细信息
match as-path [path-list-number]	匹配 as-path，并且它可以采用多个 as-path 路径列表号
匹配社区 *[社区名称][精确匹配]*	社区名称是必须的，精确匹配可为可选项。可以指定多个名称
Match interface [interface-name]	可以采用多个接口名称

子命令	详细信息
匹配指标 *(0-4294967295)*	它可能需要多个号码
Match ip address [acl name prefix-list [prefix-listname]]	ACL 和前缀列表可以使用多个名称，但一个名称不能与其他名称共存 - 策略列表可以包含前缀列表，或前缀列表可以包含 ACL
Matchipnext-hop[acl name | aclname]prefix-list[prefix-listname]]	ACL 和前缀列表可以使用多个名称，但一个名称不能与其他名称共存 - 策略列表可以包含前缀列表，或前缀列表可以包含 ACL
Match ip route-source [acl 名称| prefix-list [prefix-listname]]	ACL 和前缀列表可以使用多个名称，但一个名称不能与其他名称共存 - 策略列表可以包含前缀列表，或前缀列表可以包含 ACL
默认匹配	默认情况下，“match”下将包含上述所有选项
Help	后续命令的帮助
否	命令的否定
Exit	退出策略映射模式

CR_Examples

在以下示例中，配置了一个策略列表，允许与 AS 1 和指标 10 匹配的所有网络前缀：

```
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
```

在以下示例中，配置了一个策略列表，允许与社区 20 和指标 10 匹配的流量：

```
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
```

在以下示例中，配置了一个策略列表来拒绝与社区 20 和指标 10 匹配的流量：

```
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

使用模块化策略框架时，在全局配置模式下使用 **policy-map**命令（不带 **type** 关键字）可以为使用第 3/4 层类映射（ **class-map** 或 **class-map type management** 命令）标识的流量分配操作。要删除第 3/4 层策略映射，请使用此命令的 **no** 形式。

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

Syntax Description

name	指定此策略映射的名称，长度最大为 40 个字符。所有类型的策略映射都使用同一命名空间，因此无法重复使用已被另一类型的策略映射使用的名称。

Command Default

默认情况下，配置包含一项策略（全局策略），该策略匹配所有默认应用检测流量并将某些检测应用到所有接口上的流量。并非所有检测都默认被启用。仅能应用一个全局策略，因此如果想要改变全局策略，则需要编辑默认策略或禁用默认策略并应用新策略。（对于某项特定功能，接口策略覆盖全局策略。）

默认策略包括以下应用检测：

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

默认策略配置包括以下命令：

```
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

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

配置模块化策略框架包括四项任务：

1. 标识要使用**class-map** 或 **class-maptypemanagement** 命令应用操作的第 3 层和第 4 层流量。

2.（仅限应用检测）使用 **policy-maptypeinspect** 命令定义应用检测流量的特殊操作。

3. 使用 **policy-map** 命令对第 3 层和第 4 层流量应用操作。

4. 使用 **service-policy** 命令在接口上激活这些操作。

策略映射最大数量为64个，但每个接口只能应用一个策略映射。可以将同一策略映射应用到多个接口。您可以在第3/4层策略映射中识别多个第3/4层类映射（请参阅命令），并且可以将来自一个或多个功能类型的 **class**多个操作分配给每个类映射。

CR_Examples

以下 **policy-map**是连接策略命令的示例。它限制了允许到达 Web 服务器 10.1.1.1 的连接数：

```
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
```

以下示例显示多匹配在策略映射中如何运行：

```
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
```

以下示例显示流量如何与第一个可用的类映射匹配而不匹配同一功能域中指定操作的任何后续类映射：

```
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
```

当发起 Telnet 连接时，它会匹配。**classtelnet_traffic** 类似地，如果发起了 FTP 连接，则匹配。 **classftp_traffic** 对于除 Telnet 和 FTP 之外的任何 TCP 连接，它都会匹配。 **classtcp_traffic** 即使 Telnet 或 FTP 连接可以匹配 **classtcp_traffic**，ASA 也不会进行此匹配，因为它们之前已匹配其他类。

NetFlow 事件通过模块化策略框架进行配置。如果没有为 NetFlow 配置模块化策略框架，则不会记录任何事件。流量将根据类的配置顺序进行匹配。检测到某个匹配后，不检查任何其他类。对于 NetFlow 事件，配置要求如下：

- 流导出目的地（即 NetFlow 收集器）由其 IP 地址唯一标识。

- 支持的事件类型为 flow-create、flow-teardown、flow-denied、flow-update 等，其中包括前面列出的四种事件类型。
- 使用 **flow-exportevent-type** {**all** | **flow-create** | [] **flow-denied** | [] **flow-update** | [] **flow-teardown**} **destination** 命令来配置 NetFlow 收集器和过滤器的地址，以确定应将哪些 NetFlow 记录发送到每个收集器。
- 接口策略不支持流导出操作。
- 仅在 **class-default** 命令中以及在使用 **matchany** 或 **matchaccess-list** 命令的类中支持流导出操作。
- 如果未定义 NetFlow 收集器，则不会发生任何配置操作。
- 接口策略不支持流导出操作。

以下示例将主机 10.1.1.1 和 20.1.1.1 之间的所有 NetFlow 事件导出到目标 15.1.1.1。

```
ciscoasa(config)# access-listflow_export_aclpermit 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

命令	说明
class	在策略映射中标识类映射名称。
clearconfigurepolicy-map	删除所有策略映射配置。如果策略映射正在用于 **service-policy** 命令中，则不会删除该策略映射。
class-map	定义流量类映射。
service-policy	将策略映射分配给某个接口或全局分配给所有接口。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

policy-map type inspect

使用模块化策略框架时，通过在全局配置模式下使用 **policy-map type inspect**命令为检测应用流量定义特殊操作。要删除检测策略映射，请使用此命令的 **no** 形式。

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

Syntax Description

应用	指定要对其执行操作的应用流量类型。可用类型包括： • **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	指定此策略映射的名称，长度最大为 40 个字符。以“_internal”或“_default”开头的名称为预留名称，无法使用。所有类型的策略映射都使用同一命名空间，因此无法重复使用已被另一类型的策略映射使用的名称。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。
8.2(1)	添加 **ipv6** 关键字是为了支持 IPv6 检测。
9.0(1)	添加 **scansafe** 关键字是为了支持云网络安全。
9.5(2)	添加 **lisp** 关键字是为了支持 LISP 检查。
9.5(2)	添加了 **diameter** 和 **sctp** 关键字。
9.6(2)	添加了 **m3ua** 关键字。

使用指南

通过模块化策略框架，您可以为许多应用检测配置特殊操作。当您使用第 3/4 层策略映射中的 **inspect** 命令（ **policy-map** 命令）启用检测引擎时，您还可以选择启用 **policy-maptypeinspect** 命令创建的检测策略映射中定义的操作。例如，输入 **inspecthttphttp_policy_map** 命令，其中 http_policy_map 是检测策略映射的名称。

检测策略映射包含在 策略映射配置模式下输入的以下一个或多个命令组成。检查策略图可用的确切命令取决于应用程序。

- **match** 命令 - 您可以直接在检测策略映射中定义 **match** 命令，以便将应用流量与特定于应用的条件（例如 URL 字符串）进行匹配。然后，在匹配配置模式下启用操作，例如 **drop**、 **reset**、 **log**等。可用的 **match**命令取决于应用程序。
- **class**命令 - 此命令标识策略映射中的检测类映射（请参阅 **class-maptypeinspect** 命令以创建检测类映射）。检测类映射包括 **match** 命令，这些命令将应用流量与应用特定的条件（例如 URL 字符串）进行匹配，然后可在策略映射中为其启用操作。创建类映射和直接在检查策略映射中使用命 **match**令之间的区别在于，您可以对多个匹配进行分组，并且可以重复使用类映射。
- 命**parameters**令——参数影响检查引擎的行为。参数配置模式下可用的命令取决于应用。

您可以在策略映射中指定多个 **class**或 **match**命令。

有些 **match** 命令可以指定正则表达式来匹配数据包内的文本。请参阅 **regex** 命令和 **class-maptyperegex** 命令，它将多个正则表达式分组。

默认检查策略图配置包括以下命令：

```
policy-map type inspect dns preset_dns_map
 parameters
```

```
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
```

如果数据包与多个 **match**不同的命令匹 **class**配，则 ASA 应用操作的顺序由内部 ASA 规则决定，而不是由它们添加到策略映射的顺序决定。内部规则由应用类型和解析数据包的逻辑顺序确定，并且不可由用户配置。例如，对于 HTTP 流量，解析 Request Method 字段优先于解析 Header Host Length 字段；Request Method 字段的操作早于 Header Host Length 字段的操作。例如，以下匹配命令可以按任意顺序输入，但该 **matchrequestmethodget**命令首先匹配。

```
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
```

如果某个操作丢弃了一个数据包，则不会执行进一步的操作。例如，如果第一个操作是重置连接，那么它将永远不会匹配任何进一步 **match**的命令。如果第一个操作是记录数据包，则会发生第二个操作，例如，重置连接。（可以为同一 **match** 命令同时配置 **reset** （或 **drop-connection**等。）和 **log** 操作，在这种情况下，将在针对给定匹配重置数据包之前记录数据包。）

如果数据包匹配多个 **match**或 **class**相同的命令，则按照它们在策略图中出现的顺序进行匹配。例如，如果一个数据包的报头长度为 1001，则该数据包匹配以下第一个命令，执行记录，然后再匹配第二个命令并进行重置。如果您颠倒这两 **match**个命令的顺序，那么在数据包能够匹配第二个命令之前，它将被丢弃并且连接将被重 **match**置；它将永远不会被记录。

```
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
```

根据类映射中优先级最低的 **match**命令来确定一个类映射是否与另一个类映射或**match**命令属于同一类型（优先级基于内部规则）。如果一个类映射具有与另一个类映射相同类型的最低优 **match**先级命令，则类映射将按照添加到策略映射的顺序进行匹配。如果每个类映射的最低优先级命令不同，则首先匹配 **match**具有较高优先级命令的类映射。

如果要将正在使用的检查策略映射交换为不同的 **inspect**映射名称，则必须删除协议 映 射命令，然后使用新映射再次输入该命令。例如：

```
ciscoasa(config)# policy-map test
ciscoasa(config-pmap)# class sip
ciscoasa(config-pmap-c)# noinspect sip sip-map1
ciscoasa(config-pmap-c)# inspect sip sip-map2
```

CR_Examples

以下是 HTTP 检测策略映射和相关类映射的示例。此策略映射由第 3/4 层策略映射激活，而第 3/4 层策略映射由服务策略启用。

```
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)# matchregexexample
ciscoasa(config-cmap)# matchregexexample2
```

```
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

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	创建检查类映射以匹配特定于应用的流量。
parameters	进入检查策略图的参数配置模式。
policy-map	创建第 3/4 层策略映射。
showrunning-configpolicy-map	显示所有当前的策略映射配置。

policy-route

要在接口上配置基于策略的路由，请在接口配置模式下使用 **policy-route** 命令。

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

Syntax Description

cost*value*	为基于策略的路由评估设置接口的相对开销。值可以是 1-65535。默认值为 0，您可以使用命令中的 **no** 版本进行重置。数值越低，优先级越高。例如，1 的优先级高于 2。
route-map*route_map_name*	指定要用于基于策略的路由的路由映射的名称。
path-monitoring	设置接口对等体的监控类型以收集灵活的指标。

Command Default

没有默认路由映射。默认成本为 0。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.4(1)	添加了此命令。
9.17(1)	添加了 **cost** 关键字。
9.18(1)	此命令已增强，包括用于 PBR 的路径监控功能，以确定路由流量的最佳路径。

使用指南

配置指定匹配条件的路由映射以及在所有匹配子句得到满足时生成的操作后，使用 **policy-route route-map** 命令将其应用于特定接口。

如果在路由图中使用 **set adaptive-interface cost**它作为标准，请使用命令设置接口上的 **policy-route cost**成本。

当您设置策略-路由成本，并在路由映射中使用 **set adaptive-interface cost** 命令时，出口流量将在具有相同接口成本的任何选定接口（假设它们处于启用状态）之间进行循环负载均衡。如果成本不同，则使用成本较高的接口作为成本最低的接口的备选。

例如，通过在 2 个 WAN 链路上设置相同的成本，您可以负载均衡这些链路上的流量以提高性能。但是，如果一条 WAN 链路的带宽高于另一条 WAN 链路，则可以将带宽较高的链路的成本设置为 1，将带宽较低的链路设置为 2，以便仅在带宽较高的链路关闭时使用带宽较低的链路。

CR_Examples

以下示例将路由映射应用于基于策略的路由的接口。

```
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
```

以下示例设置了不平等的成本，因此 output1 是首选链接，并且仅当 output1 发生故障时才使用 output2。要跨接口配置负载均衡，请设置相等开销值。

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

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

路径监控功能检测到不再转发流量的路由链路或路径存在故障。它使威胁防御能够收集 RTT、抖动、丢包和平均意见得分 (MOS) 等性能指标，以确定转发流量的最佳路径。

要配置路径监控，请使用 **policy-route** 命令。您必须指定设备从对等网关收集性能指标时必须使用的监控类型。对于自动选项，默认路由的下一跳将用作要监控的对等体。首先尝试 IPv4，然后尝试 IPv6。对于 VTI 接口，不支持 auto 选项。必须指定其对等体的 IPv4 或 IPv6 地址。

```
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 (已弃用)

注释 支持此命令的最后一个版本是版本 9.5(1)。

如要配置用于加密发送到 SiteMinder SSO 服务器的身份验证请求的密钥，请在 webvpn-sso-siteminder 配置模式下使用 **policy-server-secret** 命令。要删除密钥，请使用此 **no**命令的形式。

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

注释 SiteMinder SSO 身份验证需要此命令。

Syntax Description

secret-key 用作加密身份验证通信的密钥的字符串。无字符最小或最大数量限制。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Config-webvpn-sso-siteminder 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。
9.5(2)	为了支持 SAML 2.0，此命令已弃用。

使用指南

单点登录支持，仅供 WebVPN 使用，可让用户能够访问不同服务器不同安全服务，无需多次输入用户名和密码。您首先使用 **sso-server** 命令创建 SSO 服务器。对于 SiteMinder SSO 服务器，**policy-server-secret** 命令可保护 ASA 与 SSO 服务器之间的身份验证通信。

命令参数 *secret-key*类似于密码：您创建它、保存它并配置它。它在 ASA 上使用命令进行配置，并在 **policy-server-secret** SiteMinder 策略服务器上使用 Cisco Java 插件身份验证方案进行配置。

此命令仅适用于 SiteMinder 类型的 SSO 服务器。

CR_Examples

在 config-webvpn-sso-siteminder 模式下输入的以下命令包含一个随机字符串作为参数，用于创建 SiteMinder SSO 服务器身份验证通信的密钥：

```
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

命令	说明
max-retry-attempts	配置 ASA 重试失败的 SSO 身份验证的次数。
request-timeout	指定失败的 SSO 身份验证尝试超时之前的秒数。
show webvpn sso-server	显示在安全设备上配置的所有 SSO 服务器的运行统计信息
sso-server	创建单点登录服务器。
test sso-server	使用试用身份验证请求测试 SSO 服务器。
web-agent-url	指定 ASA 向其发出 SiteMinder SSO 身份验证请求的 SSO 服务器 URL。

policy static sgt

要将策略应用于手动配置的思科 TrustSec 链路，请在 cts 手动接口配置模式下使用 **policy static sgt** 命令。要删除手动配置的 CTS 链路下的策略，请使用此命令的 **no** 形式。

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

Syntax Description

sgt*sgt_number*	指定应用于来自对等方的传入流量的 SGT 编号。有效值为 2 到 65519。
static	为链路上的传入流量指定 SGT 策略。
trusted	表示命令中指定的 SGT 的接口上的入口流量不应被其 SGT 覆盖。默认设置为 Untrusted。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Cts 手动接口配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.3(1)	添加了此命令。

使用指南

此命令将策略应用于手动配置的 CTS 链接。

限制

- 仅支持物理接口、VLAN 接口、端口通道接口和冗余接口。
- 不支持逻辑接口或虚拟接口，例如 BVI、TVI 和 VNI。

CR_Examples

以下示例为第 2 层 SGT 实施启用接口并定义此接口是否可信：

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

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

Related Commands

命令	说明
ctsmanual	启用第 2 层 SGT 强制并进入 cts 手动接口配置模式。
propagatesgt	在接口上传播安全组标签（称为 **sgt**）。默认情况下，传送被启用。

polltime interface

要在主用/主用故障转移配置中指定数据接口轮询时间和保持时间，请在故障转移组配置模式下使用 **polltime interface** 命令。要恢复默认值，请使用此命 **no**令的形式。

轮询polltime interface[**msec**][**holdtime**时 间]
轮询no polltime interface[**msec**][**holdtime**时 间]

Syntax Description

holdtime时间	（可选）设置从对等单元最后收到的 hello 消息与开始接口测试之间的时间（作为计算），以确定接口的健康状况。它还将每次接口测试的持续时间设置为 保持时间/16。有效值范围为 5 至 75 秒。默认值是 *polltime* 的 5 倍。您不能输入小于轮询时间五倍的保持时间值。 要计算开始接口测试之前的时间（y），请执行以下操作： **1.** x = (*holdtime* /*polltime)/2* ，四舍五入到最接近的整数。（.4 和向下四舍五入； 0.5 和向上四舍五入。） **2.** y = x**polltime* 例如，如果使用默认保持时间25和轮询时间5，则y = 15秒。
interface时间	指定向对等方发送 hello 数据包之间等待的时间。有效值范围为 1 至 15 秒。默认值为 5。如果使用可选关 **msec**键字，则有效值为 500 至 999 毫秒。
msec	（可选）指定给定时间，以毫秒为单位。

Command Default

轮询 时间为5秒。

holdtime时间 为轮询 时间 的5 倍。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
故障转移组配置	• 是	• 支持	—	—	• 是

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	已更改 命令，以包含可选的**holdtime**时间 值，并且可以以毫秒为单位指定轮询时间。

此命令仅适用于主用/主用故障转移。请在主用/备用故障转移配置中使用 **failoverpolltimeinterface** 命令。

通过更快的轮询时间，ASA 可以更快地检测故障并触发故障转移。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。

您可以在配置中同时包含 **polltimeunit** 和 **polltimeinterface** 命令。

注释 当 CTIQBE 流量通过故障转移配置中的 ASA 时，应将 ASA 上的故障转移保持时间减少到 30 秒以下。CTIQBE 保持连接超时为 30 秒，并且在故障转移情况下可能在发生故障转移之前超时。如果 CTIQBE 超时，与思科 CallManager 的思科 IP SoftPhone 连接将被丢弃，并且 IP SoftPhone 客户端需要向 CallManager 重新注册。

CR_Examples

以下部分示例显示了故障转移组的一种可能配置。对于故障转移组 1 中的数据接口，接口轮询时间设置为 500 毫秒，保持时间设置为 5 秒。

```
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

命令	说明
failovergroup	定义主用/主动故障转移的故障转移组。
failoverpolltime	指定设备故障转移轮询和保持时间。
failoverpolltimeinterface	指定主用/备用故障转移配置的接口轮询和保持时间。

poll-timer

要指定 ASA 在多长时间内查询 DNS 服务器以解析网络对象组中定义的完全限定域名 (FQDN)，请在 dns 服务器组配置模式下仅对 DefaultDNS 服务器组使用 **poll-timer**命令。要删除计时器，请使用此命 **no**令的形式。

poll-timer minutes分钟
no poll-timer minutes分钟

Syntax Description

minutes分钟	指定计时器（以分钟为单位）。有效值为 1 至 65535 分钟。

Command Default

默认情况下，DNS 计时器为 240 分钟或 4 小时。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
dns server-group 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
8.4(2)	添加了此命令。

使用指南

此命令仅支持 DefaultDNS 服务器组。

此命令指定 ASA 查询 DNS 服务器以解析网络对象组中定义的 FQDN 的计时器。当轮询 DNS 计时器到期或已解析 IP 条目的 TTL 到期时（以先到者为准），会定期解析 FQDN。

此命令仅当至少激活一个网络对象组时才生效。

CR_Examples

以下示例将 DNS 轮询计时器设置为 240 分钟：

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

Related Commands

命令	说明
clearconfiguredns	删除所有 DNS 命令。

命令	说明
dnsserver-group	进入 dns-server-group 模式，在此模式下，您可以配置 DNS 服务器组。
show running-config dns-server group	显示一个或所有现有的 DNS 服务器组配置。

pop3s (已弃用)

注释 支持此命令的最后一个版本是版本 9.5(1)。

要进入POP3S配置模式，请使用全局配置模式下的 **pop3s** 命令。要删除在 POP3S 命令模式下输入的任何命令，请使用此命令的 **no**版本。

POP3 是一种客户端/服务器协议，您的互联网服务器可以使用该协议接收并保留邮件。您（或您的客户端邮件收件人）应定期检查服务器上的邮箱并下载所有邮件。此标准协议内置于大多数常用邮件产品中。POP3S 使您可以通过 SSL 连接接收邮件。

pop3s
no pop3

Syntax Description

此命令没有任何参数或关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	—	—	• 是

Command History

版本	修改
7.0(1)	添加了此命令。
9.5(2)	此命令已弃用。

CR_Examples

以下示例显示如何进入 POP3S 配置模式：

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

Related Commands

命令	说明
clearconfigurepop3s	删除 POP3S 配置。

命令	说明
showrunning-configpop3s	显示 POP3S 的运行配置。

port (已弃用)

注释 支持此命令的最后一个版本是版本 9.5(1)。

要指定邮件代理侦听的端口，请在适用的邮件代理命令模式下使用 **port** 命令。要恢复默认值，请使用此命令的 **no**版本。

port*portnum*
no port

Syntax Description

portnum	供邮件代理要使用的端口。为避免与本地 TCP 服务冲突，请使用 1024 到 65535 范围内的端口号。

Command Default

邮件代理的默认端口如下：

邮件代理	默认端口
IMAP4S	993
POP3S	995
SMTPS	988

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Pop3s	• 是	—	• 是	—	—
Imap4s	• 是	—	• 是	—	—
Smtps	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.5(2)	此命令已弃用。

使用指南

为避免与本地 TCP 服务冲突，请使用 1024 到 65535 范围内的端口号。

CR_Examples

以下示例显示如何为 IMAP4S 邮件代理设置端口 1066：

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

portal-access-rule（已弃用）

此命令允许客户配置全局无客户端 SSL VPN 访问策略，以根据 HTTP 标头中的数据允许或拒绝无客户端 SSL VPN 会话。如果访问遭到拒绝，系统会向客户端返回错误代码。由于此拒绝操作是在用户身份验证之前发生的，所以可以减少处理资源的使用。

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

Syntax Description

无	删除所有门户访问规则。无客户端 SSL VPN 会话不会基于 HTTP 报头进行限制。
priority	规则的优先级。范围：1-65535。
permit	允许基于 HTTP 标头进行访问。
deny	根据 HTTP 标头拒绝访问。
代码	根据返回的 HTTP 状态代码允许或拒绝访问。默认值：403。
code	允许或拒绝访问所依据的 HTTP 状态代码编号。范围：200-599。
任意	匹配任何 HTTP 报头字符串。
user-agent match	启用 HTTP 报头中字符串的比较。
string	在HTTP报头中指定要匹配的字符串。对于包含您的字符串的匹配项，使用通配符 (*) 将您要搜索的字符串括起来，或者不使用通配符指定您的字符串的精确匹配项。 注释 建议在搜索字符串中使用通配符。如果没有它们，规则可能无法匹配任何字符串，或者匹配的字符串可能比您预期的要少得多。 如果您要搜索的字符串中包含空格，则必须将该字符串括在引号中；例如“*a string*”。同时使用引号和通配符时，搜索字符串将如下所示：“**a string **”。
no portal-access-rule	使用 来删除单个门户访问规则。
清除配置 webvpn 门户访问规则	相当于 portal-access-rule none 命令。

Command Default

portal-access-rulenone

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
webvpn配置模式	• 是	—	• 是	—	—

Command History

版本	修改
8.2(5)	此命令同时添加到 ASA 8.2.5 和 8.4(2) 中。
8.4(2)	此命令同时添加到 ASA 8.2.5 和 8.4(2) 中。
9.17(1)	由于取消了对 Web VPN 的支持，此命令已被弃用。

使用指南

此检查在用户身份验证之前执行。

CR_Examples

以下示例创建三个门户访问规则：

- 当 ASA 返回代码 403 且 Thunderbird 位于 HTTP 报头中时，门户访问规则 1 拒绝尝试的无客户端 SSL VPN 连接。
- 当 MSIE 8.0 (Microsoft Internet Explorer 8.0) 在 HTTP 报头中时，门户访问规则 10 允许尝试的无客户端 SSL VPN 连接。
- 门户访问规则 65535 允许所有其他尝试的无客户端 SSL VPN 连接。

```
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
```

注释 如果已安装HostScan，则端口访问规则功能不会阻止ASA打开思科安全桌面门户等页面。为了避开思科安全桌面端口，需要卸载 HostScan。

Related Commands

命令	说明
showrunwebvpn	显示 webvpn 配置，包括所有门户访问规则。
showvpn-sessiondbdetailwebvpn	显示有关 VPN 会话的信息。命令包括用于完整或详细显示信息的选项，可让您指定要显示的会话的类型，并提供用于对信息进行过滤和排序的选项。

命令	说明
debugwebvpnrequest*n*	启用特定调试级别的调试消息的日志记录。默认值：1。范围：1-255。

port-channel load-balance

对于 EtherChannel，要指定负载均衡算法，请在接口配置模式下使用**port-channelload-balance**命令。要将值设置为默认值，请使用此命 **no**令的形式。

注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

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	根据数据包的以下特征来均衡接口上的数据包负载： • 目标 IP 地址 (Destination IP address)
dst-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • 目标 IP 地址 (Destination IP address) • 目标端口 (Destination Port)
dst-mac	根据数据包的以下特征来均衡接口上的数据包负载： • 目标 MAC 地址
dst-port	根据数据包的以下特征来均衡接口上的数据包负载： • 目标端口
src-dst-ip	（默认）根据数据包的以下特征来均衡接口上的数据包负载： • 源 IP 地址 • 目的 IP 地址
src-dst-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • 源 IP 地址 • 目的 IP 地址 • 源端口 (Source Port) • 目的端口

src-dst-mac	根据数据包的以下特征来均衡接口上的数据包负载： • 源 MAC 地址 • 目的 MAC 地址
src-dst-port	根据数据包的以下特征来均衡接口上的数据包负载： • 源端口 • 目的端口
src-ip	根据数据包的以下特征来均衡接口上的数据包负载： • 源 IP 地址
src-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • 源 IP 地址 • 源端口
src-mac	根据数据包的以下特征来均衡接口上的数据包负载： • 源 MAC 地址
src-port	根据数据包的以下特征来均衡接口上的数据包负载： • 源端口
vlan-dst-ip	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 目标 IP 地址 (Destination IP address)
vlan-dst-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 目标 IP 地址 (Destination IP address) • 目标端口
vlan-only	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN

vlan-src-dst-ip	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 源 IP 地址 • 目的 IP 地址
vlan-src-dst-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 源 IP 地址 • 目的 IP 地址 • 源端口 • 目的端口
vlan-src-ip	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 源 IP 地址
vlan-src-ip-port	根据数据包的以下特征来均衡接口上的数据包负载： • VLAN • 源 IP 地址 • 源端口

Command Default

默认值为 **src-dst-ip**。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
8.4(1)	添加了此命令。

使用指南

ASA 通过对数据包的源和目标 IP 地址进行哈希处理 (**src-dst-ip**) 将数据包分发到 EtherChannel 中的接口。在模数运算中，将得到的散列值除以主用链路数，得到的余数确定哪个接口拥有流量。*hash_value***mod***active_links* 结果为 0 的所有数据包都将转到 EtherChannel 中的第一个接口，结果为 1 的数据包将转到第二个接口，结果为 2 的数据包将转到第三个接口，依此类推。例如，如果您有 15 个主用链路，则模数运算的值为 0 到 14。如果有 6 个主用链路，则值为 0 到 5，依此类推。

对于集群中跨网络 EtherChannel，系统会逐个 ASA 进行负载均衡。例如，如果 8 个 ASA 之间的跨网络 EtherChannel 中有 32 个主用接口，而 EtherChannel 中的每个 ASA 又有 4 个接口，则仅会在 ASA 上的 4 个接口之间进行负载均衡。

如果主用接口发生故障且未由备用接口替代，则流量会在剩余的链路之间重新均衡。该故障会在第 2 层的生成树和第 3 层的路由表中被屏蔽，因此故障转移对其他网络设备是透明的。

CR_Examples

以下示例将负载均衡算法设置为使用源及目标 IP 地址和端口：

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

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

port-channel min-bundle

对于以太网通道，要指定端口通道接口变为活动状态所需的最小活动接口数，请在**port-channel min-bundle** 接口配置模式下使用该命令。要将值设置为默认值，请使用此命 **no**令的形式。

注释 仅在 ASA 硬件型号和 ISA 3000 上受支持。

port-channelmin-bundle*number*
no port-channelmin-bundle

Syntax Description

number	指定端口通道接口变为活动状态所需的最小活动接口数（介于 1 和 8 之间）；对于 9.2(1) 及更高版本，活动接口可介于 1 和 16 之间。

Command Default

默认值为 1。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
8.4(1)	添加了此命令。
9.2(1)	主用接口数量从 8 增加到 16。

使用指南

为端口通道接口输入此命令。如果通道组中的主用接口数小于此值，则端口通道接口将会发生故障，并可能会触发设备级故障转移。

CR_Examples

以下示例将端口通道变为活动状态所需的最小活动接口数设置为两个：

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

Related Commands

命令	说明
channel-group	将接口添加到以太网通道。

命令	说明
interfaceport-channel	配置以太网通道。
lacpmax-bundle	指定通道组中允许的最大活动接口数。
lacpport-priority	设置通道组中物理接口的优先级。
lacpsystem-priority	设置 LACP 系统优先级。
port-channelload-balance	配置负载平衡算法。
port-channelmin-bundle	指定端口通道接口变为活动状态所需的最小活动接口数。
showlacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
showport-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
showport-channelload-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

port-channel span-cluster

要在 ASA 集群中将此 EtherChannel 设置为跨区以太网通道，请在接口配置模式下使用 **port-channelspan-cluster** 命令。要禁用跨越，请使用此命 **no**令的形式。

注释 仅在 ASA 硬件型号上受支持。其他型号隐式将数据 EtherChannel 设置为跨区模式。

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

Syntax Description

vss-load-balance	（可选）启用 VSS 负载均衡。如果将 ASA 连接到 VSS 或 vPC 中的两个交换机，则应启用 VSS 负载平衡。此功能可确保 ASA 与 VSS（或 vPC ）对之间的物理链路连接实现均衡。启用 **vss-id**负载均衡前，必须为每个成员接口配置命令中 **channel-group**的关键字。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

您必须处于跨区以太网通道模式 (**clusterinterface-modespanned**) 才能使用此功能。

此功能允许您将每个单元的一个或多个接口分组到跨集群中所有单元的以太网通道中。EtherChannel 汇聚通道中所有可用活动接口上的流量。跨网以太网通道可以在路由和透明防火墙模式下配置。在路由模式下，EtherChannel 配置为具有单个 IP 地址的路由接口。在透明模式下，IP 地址分配给桥接组，而不是接口。负载均衡属于 EtherChannel 固有的基本操作。

CR_Examples

以下示例创建 EtherChannel（端口通道 2），并将 tengigabitethernet 0/8 接口作为唯一成员，然后在整个集群中扩展 EtherChannel。两个子接口添加到端口通道 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

命令	说明
interface	进入接口配置模式。
clusterinterface-mode	为跨网络 EtherChannel 或单个接口设置集群接口模式。

port-forward（已弃用）

要配置无客户端 SSL VPN 会话用户可通过转发的 TCP 端口访问的应用集，请在 webvpn 配置模式下使用 **port-forward** 命令。

port-forward{*list_namelocal_portremote_serverremote_portdescription*}

要配置对多个应用的访问权限，请多次将此命令与相同的 *list_name* 配合使用，每个应用一次。

要从列表中删除已配置应用，请使用 **no port-forward***list_namelocal_port* 命令（无需包括 *remote_server* 和 *remote_port* 参数）。

no port-forward*listnamelocalport*

要删除整个配置的列表，请使用 **no port-forward***list_name* 命令。

no port-forward*list_name*

Syntax Description

description	提供在最终用户端口转发 Java 小程序屏幕上显示的应用名称或简短说明。最多 64 个字符。
list_name	无客户端 SSL VPN 会话用户可以访问的应用集（转发的 TCP 端口）的组。最多 64 个字符。
local_port	指定侦听应用程序 TCP 流量的本地端口。对于 *list_name*，您只能使用一次本地端口号。输入 1-65535 范围内的端口号。如要避免与现有服务冲突，请使用大于 1024 的端口号。
remote_port	指定此应用在远程服务器上的连接端口。这是应用使用的实际端口。请输入 1-65535 范围内的端口号或端口名称。
remote_server	为应用程序提供远程服务器的 DNS 名称或 IP 地址。如果输入 IP 地址，可以使用 IPv4 或 IPv6 格式输入。我们建议使用主机名，这样您就不必为特定的 IP 地址配置客户端应用程序。dns server-group 命令 **name-server** 必须将主机名解析为 IP 地址。

Command Default

没有默认端口转发列表。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
WebVPN配置模式	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.0(2)	命令模式已更改为 webvpn。
9.17(1)	由于取消了对 Web VPN 的支持，此命令已被弃用。

使用指南

端口转发不支持 Microsoft Outlook Exchange (MAPI) 代理。但是，您可以为 Microsoft Outlook Exchange 2010 配置智能隧道支持。

CR_Examples

下表显示用于示例应用的值。

应用程序	本地端口	服务器 DNS 名称	远程端口	说明
IMAP4S 邮件	20143	IMAP4S 服务器	143	获取邮件
SMTPS 邮件	20025	SMTPS 服务器	25	发送邮件
基于 SSH 的 DDTS	20022	DDTS 服务器	22	基于 SSH 的 DDTS
Telnet	20023	Telnet服务器	23	Telnet

以下示例显示如何创建名为 *SalesGroupPorts* 的端口转发列表，该列表提供对这些应用的访问：

```
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

命令	说明
port-forwardauto-start	此命令是在 group-policy webvpn 或 username webvpn 模式下输入的，可以自动启动端口转发，并在用户登录无客户端 SSL VPN 会话时分配指定的端口转发列表。

命令	说明
port-forwardenable	此命令在组策略 webvpn 或用户名 webvpn 模式下输入后，将在用户登录时开始分配指定的端口转发列表，但要求用户使用无客户端 SSL VPN 门户上的 **ApplicationAccess** = **StartApplications** 按钮手动启动端口转发。页面上。
port-forwarddisable	在 group-policy webvpn 或 username webvpn 模式下输入此命令可关闭端口转发。

port-forward-name（已弃用）

要为特定用户或策略组配置标识TCP端口转发到最终用户的显示名称，请在**port-forward-name**webvpn模式下使用从组策略或用户名模式输入的命令。要删除显示名称（包括使用该命令创建的**port-forward-namenone** 空值），请使**,** 用该命令的 no 形式。该 **no** 选项恢复默认名称“应用程序访问”。要防止显示名称，请使用该 **port-forwardnone** 命令。

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

Syntax Description

none	表示无显示名称。设置空值，从而不允许显示名称。防止继承值。
value*name*	向最终用户介绍端口转发。最多 255 个字符。

Command Default

默认名称是“应用程序访问”。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Webvpn	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。
9.17(1)	由于取消了对 Web VPN 的支持，此命令已被弃用。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略设置名称“远程访问 TCP 应用程序”：

```
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

命令	说明
webvpn	在组策略配置模式或用户名配置模式下使用。让您可以进入 WebVPN模式以配置应用于组策略或用户名的参数。

命令	说明
webvpn	在全局配置模式下使用。让您可以配置 WebVPN 的全局设置。

端口对象

要将端口对象添加至 TCP、UDP 或 TCP-UDP 类型的服务对象组，请在 object-group 服务配置模式下使用 **port-object** 命令。要删除端口对象，请使用此命令的 **no** 形式。

port-object {**eq***port* | **range***begin_portend_port*}
no port-object {**eq***port* | **range***begin_portend_port*}

Syntax Description

range*begin_port end_port*	指定端口范围（含 0 和 65535）。
eq端口	指定服务对象的十进制数（介于 0 和 65535 之间）或 TCP 或 UDP 端口名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
对象网络服务配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

port-object 命令与 **object-groupservice***protocol* 命令配合使用，定义为特定端口或端口范围的对象。

如果为 TCP 或 UDP 服务指定了名称，则名称必须是受支持的 TCP 或/和 UDP 名称之一，并且必须与对象组的协议类型一致。例如，对于 tcp、udp 和 tcp-udp 协议类型，names 必须分别为有效的 TCP 服务名称、有效的 UDP 服务名称或有效的 TCP 和 UDP 服务名称。

如果指定了编号，则在显示对象时，将根据协议类型转换为其相应名称（如果存在）。

支持以下服务名称：

TCP	UDP	TCP 和 UDP
bgp	biff	discard
chargen	bootpc	domain

TCP	UDP	TCP 和 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		

CR_Examples

此示例显示如何在服务配置模式下使用 **port-object**命令创建新的端口（服务）对象组：

```
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

命令	说明
clearconfigureobject-group	从配置中 **object-group**删除所有命令。
group-object	添加网络对象组。
network-object	向网络对象组添加网络对象。
object-group	定义对象组以优化您的配置。
showrunning-configobject-group	显示当前对象组。

post-max-size

要指定允许发布的对象的最大大小，请在 **post-max-size**组策略 webvpn 配置模式下使用该命令。要从配置中删除此对象，请使用此命令的 **no**版本。

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

Syntax Description

size	指定允许发布对象的最大大小。范围为 0 到 2147483647。将大小设置为 0 可以有效地禁止对象发布。

Command Default

默认大小为 2147483647。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
组策略 webvpn 配置模式	• 是	—	• 是	—	—

Command History

版本	修改
8.0(2)	添加了此命令。

CR_Examples

以下示例将发布对象的最大大小设置为 1500 字节：

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

Related Commands

命令	说明
download-max-size	指定要下载的对象的最大大小。
upload-max-size	指定要上传的对象的最大大小。

命令	说明
webvpn	在组策略配置模式或用户名配置模式下使用。让您可以进入 WebVPN模式以配置应用于组策略或用户名的参数。
webvpn	在全局配置模式下使用。让您可以配置 WebVPN 的全局设置。

内嵌式电源

要在支持的端口上启用或禁用以太网供电 (PoE)，请在接口配置模式下使用 **powerinline** 命令。要返回默认状态，请使用此命 **no**令的形式。

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

注释 仅支持 5505、1010 和 1210CP。不支持 1010E/1210CE/1220CX。

Syntax Description

consumptionwattage 毫瓦	手动指定瓦数（毫瓦），从 4000 到 30000 （1010）或 90000（1210CP）。如果您要手动设置功率而不是使用通过 LLDP 协商的功率，请使用此命令。
auto	使用适合受电设备类别的功率自动向受电设备供电。防火墙使用 LLDP 进一步协商正确的瓦数。当连接某个类别的设备时，它会被调配到该等级的最大功率，以防需要使用更多电能。例如，如果您添加请求的功率为 12.95W 的 4 类设备，即使它当前没有使用该功率，系统也会为其分配 30W。某些设备可以重新协商电源需求。如果您知道您的设备所需的电量少于分配的电量，您可以 **consumption wattage**手动设置以释放电量用于其他设备。
never	禁用 PoE。

Command Default

默认值为 **auto**。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
7.2(1)	添加了此命令。
9.13(1)	增加了对 Firepower 1010 的支持。
9.22(1)	添加了对 Cisco Secure Firewall 1210CP 的支持。
9.23(1)	1210CP 增加了对 IEEE 802.3bt（PoE++ 和 Hi-PoE）的支持，以及每端口最高 90 瓦的功率。还增加了对多上下文模式的支持。

使用指南

PoE 在以下端口上可用：

- ASA 5505 - 以太网 0/6 和以太网 0/7 使用 IEEE 802.3af (PoE)，每个端口最高 15 瓦，总计最高 30 瓦。
- Firepower 1010 - 使用 IEEE 802.3af (PoE) 和 802.3at (PoE+) 的以太网 1/7 和 1/8，每个端口最高 30 瓦，总功率最高 60 瓦。
- Cisco Secure Firewall 1210CP - 以太网 1/5、1/6、1/7 和 1/8，使用 IEEE 802.3af (PoE)、802.3at (PoE+)和 802.3bt（PoE++ 和 Hi-PoE），每个端口最高 90 瓦，合计最高 120 瓦。

注释 1010E、1210CE 和 1220CX 不支持 PoE。

PoE+ 或更高版本使用链路层发现协议 (LLDP) 来协商功率级别。仅在需要时提供功率。

如果关闭接口，则会禁用设备电源。

CR_Examples

以下示例为以太网 1/7 手动设置功率，为以太网 1/8 设置功率为自动：

```
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

命令	说明
showpowerinline	显示 PoE 状态。

power-supply

对于 ISA 3000 中的双电源，要在 ASA OS 中将双电源建立为预期配置，请在全局配置模式下使用该 **power-supply**命令。要禁用双电源，请使用此命令的 **no** 形式。

power-supply dual
no power-supply dual

Syntax Description

dual	指定双电源。

Command Default

默认情况下，双电源处于禁用状态。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	—

Command History

版本	修改
9.6(1)	我们引入了此命令。

使用指南

如果其中一个电源发生故障，ASA会发出报警。默认情况下，ASA需要单个电源，只要它包含一个工作电源，就不会发出警报。

CR_Examples

以下示例建立双电源：

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

pppoe client route distance

要配置通过 PPPoE 获知的路由的管理距离，请在接口配置模式下使用 **pppoeclientroutedistance**命令。要恢复默认设置，请使用此命 **no**令的形式。

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

Syntax Description

distance	要应用于通过 PPPoE 学习的路由的管理距离。有效值为从 1 到 255。

Command Default

默认情况下，通过 PPPoE 获知的路由的管理距离为 1。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

仅当路由通过 PPPoE 获知时，才会检查 **pppoeclientroutedistance** 命令。如果在从 PPPoE 获知路由后输入 **pppoeclientroutedistance** 命令，则指定的管理距离不会影响现有获知的路由。只有在输入 命令后获知的路由才具有指定的管理距离。

您必须在 [**ipaddressppppoe** 命令中指定 **setroute** 选项，才能通过 PPPoE 获取路由。

如果在多个接口上配置了 PPPoE，则必须在每个接口上使用 **pppoeclientroutedistance** 命令来指示已安装的路由的优先级。在多个接口上启用 PPPoE 客户端仅支持对象跟踪。

如果使用 PPPoE 获取 IP 地址，则无法配置故障转移。

CR_Examples

以下示例通过 GigabitEhternet0/2 上的 PPPoE 获取默认路由。通过跟踪条目对象 1 来跟踪路由。SLA 操作会监控外部接口的 10.1.1.1 网关的可用性。如果 SLA 操作失败，则使用通过 PPPoE 在 GigabitEthernet0/3 上获取的辅助路由。

```
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

命令	说明
ipaddresspppoe	使用通过 PPPoE 获取的 IP 地址配置指定接口。
ppoeclientsecondary	为辅助 PPPoE 客户端接口配置跟踪。
pppoeclientroutetrack	关联通过 PPPoE 获知的路由与 跟踪条目对象。
slamonitor	定义 SLA 监控操作。
trackrtr	创建跟踪条目以轮询 SLA。

pppoe client route track

如要将 PPPoE 客户端配置为将添加的路由与指定的被跟踪对象编号相关联，请在接口配置模式下使用 **pppoe client route track** 命令。要删除 PPPoE 路由跟踪，请使用此命 **no**令的形式。

pppoe client route track编号
no pppoe client route track

Syntax Description

number	跟踪条目对象 ID。有效值范围为 1 至 500。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

仅当路由通过 PPPoE 获知时，才会检查 **pppoeclientroutetrack** 命令。如果在从 PPPoE 获知路由后输入 **pppoeclientroutetrack**命令，则现有的获知路由不与跟踪对象关联。只有在输入 命令后获知的路由才能与指定的跟踪对象关联。

您必须在 [**ipaddresspppoe** 命令中指定 **setroute** 选项，才能通过 PPPoE 获取路由。

如果在多个接口上配置了 PPPoE，则必须在每个接口上使用 **pppoeclientroutedistance** 命令来指示已安装的路由的优先级。仅对象跟踪支持在多个接口上启用 PPPoE 客户端。

如果使用 PPPoE 获取 IP 地址，则无法配置故障转移。

CR_Examples

以下示例通过 GigabitEhternet0/2 上的 PPPoE 获取默认路由。通过跟踪条目对象 1 来跟踪路由。SLA 操作会监控外部接口的 10.1.1.1 网关的可用性。如果 SLA 操作失败，则使用通过 PPPoE 在 GigabitEthernet0/3 上获取的辅助路由。

```
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

命令	说明
ipaddresspppoe	使用通过 PPPoE 获取的 IP 地址配置指定接口。
ppoeclientsecondary	为辅助 PPPoE 客户端接口配置跟踪。
pppoeclientroutedistance	为通过 PPPoE 获知的路由分配管理距离。
slamonitor	定义 SLA 监控操作。
trackrtr	创建跟踪条目以轮询 SLA。

pppoe client secondary

如要将 PPPoE 客户端配置为注册为被跟踪对象的客户端，并根据跟踪状态启动或关闭，请在接口配置模式下使用 **pppoeclientsecondary** 命令。要删除客户端注册，请使用此命 **no**令的形式。

pppoe client secondary track编号
no pppoe client secondary track

Syntax Description

number	跟踪条目对象 ID。有效值范围为 1 至 500。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

仅当 PPPoE 会话启动时，才会检查 **pppoeclientsecondary** 命令。如果在从 PPPoE 获知路由后输入 **pppoeclientroutetrack**命令，则现有的获知路由不与跟踪对象关联。只有在输入 命令后获知的路由才能与指定的跟踪对象关联。

您必须在 [**ipaddressppppoe** 命令中指定 **setroute** 选项，才能通过 PPPoE 获取路由。

如果在多个接口上配置了 PPPoE，则必须在每个接口上使用 **pppoeclientroutedistance** 命令来指示已安装的路由的优先级。仅对象跟踪支持在多个接口上启用 PPPoE 客户端。

如果使用 PPPoE 获取 IP 地址，则无法配置故障转移。

CR_Examples

以下示例通过 GigabitEhternet0/2 上的 PPPoE 获取默认路由。通过跟踪条目对象 1 来跟踪路由。SLA 操作会监控外部接口的 10.1.1.1 网关的可用性。如果 SLA 操作失败，则使用通过 PPPoE 在 GigabitEthernet0/3 上获取的辅助路由。

```
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

命令	说明
ipaddresspppoe	使用通过 PPPoE 获取的 IP 地址配置指定接口。
ppoeclientsecondary	为辅助 PPPoE 客户端接口配置跟踪。
pppoeclientroutedistance	为通过 PPPoE 获知的路由分配管理距离。
pppoeclientroutetrack	关联通过 PPPoE 获知的路由与 跟踪条目对象。
slamonitor	定义 SLA 监控操作。

prc-interval

要自定义部分路由计算 (PRC) 的 IS-IS 限制，请在路由器 isis 配置模式下使用 **prc-interval** 命令。要恢复默认值，请使用此命 **no**令的形式。

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

Syntax Description

prc 最大等待	指示两次连续PRC计算之间的最大间隔。范围为 1 到 120 秒。
prc-initial-wait	（可选）表示拓扑更改后的初始 PRC 计算延迟。范围为 1 到 120,000 毫秒。默认值为 2000 毫秒。
prc-second-wait	（可选）表示第一次和第二次PRC计算之间的保持时间（以毫秒为单位）。范围为 1 到 120,000 毫秒。

Command Default

默认值包括：

prc-max-wait： 5 秒

prc-initial-wait： 2000 毫秒

prc-second-wait： 5000 毫秒

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器 isis 配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

PRC 是一种不执行最短路径优先 (SPF) 计算的路由计算软件过程。当路由系统本身的拓扑结构没有改变，但在特定 IS 宣布的信息中检测到变化，或者当需要尝试在路由信息库 (RIB) 中重新安装此类路由时，这种情况是可能的。

以下说明有助于确定是否更改此命令的默认值：

- *prc-initial-* wait 参数表示生成第一个 LSP 之前的初始等待时间（以毫秒为单位）。
- *prc-second-wait* 参数表示首次和第二个 LSP 生成之间的等待时长（以毫秒为单位）。

- 每个后续等待间隔都是前一个等待间隔的两倍，直到等待间隔达到指定的*prcmax-wait*为止，因此，在初始和第二个间隔之后，该值会导致PRC计算节流或减慢。一旦达到此间隔，等待间隔就会以此间隔继续，直到网络稳定下来。
- 网络平稳运行并且在两倍的 *prc-max-wait* 间隔内没有触发器后，快速行为将恢复（初始等待时间）。

CR_Examples

以下是 PRC 的间隔示例。

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

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置ASA忽略收到的带有内部校验和错误的IS-IS LSP，而不是清除LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型

命令	说明
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。

命令	说明
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
routeprioorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。