服务策略

使用模块化策略框架的服务策略提供一致而灵活的配置ASA功能的方式。例如，可以使用服务策略创建特定于某项TCP应用而非应用于所有TCP应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。

关于服务策略

以下主题介绍服务策略的工作原理。

服务策略的组件

服务策略的关键意义在于，将高级服务应用于允许的流量。任何被访问规则允许的流量都可以应用服务策略，从而接受特殊处理，例如被重定向到服务模块，或者实施应用检测。

提供有以下类型的服务策略：

- 一项应用到所有接口的全局策略。
- 一项应用到单个接口的服务策略。该策略可以是通过设备的流量类和在ASA接口上定向而非通过的管理流量类的混合。

每项服务策略都由以下要素组成：

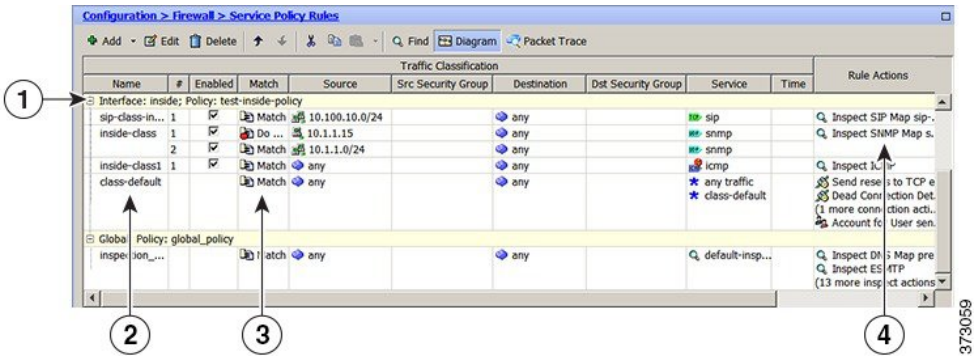
1. 服务策略映射。这是一组按顺序排列的规则集，根据 **service-policy** 命令命名。在 ASDM 中，策略映射表示为 Service Policy Rules 页面上的一个文件夹。

2. 规则。每条规则都是服务策略映射中的 **class** 命令，以及与 **class** 命令相关联的命令。在 ASDM 中，每条规则都显示于不同的行，规则名称为类名称。

   class 命令定义匹配规则条件的流量。

   与类相关联的命令（例如 **inspect** 和 **set connection timeout**），定义应用于匹配流量的服务和限制。请注意，检测命令可以指向检测策略映射，以此定义应用于被检测流量的操作。请记住，检测策略映射不同于服务策略映射。

以下示例将服务策略在 CLI 中的显示方式与在 ASDM 中的显示方式进行了对比。请注意，图中编号和 CLI 中的行之间没有一对一映射关系。



以下 CLI 由上图中显示的规则生成。

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all but v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
```

```
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

使用服务策略配置的功能

下表列出了使用服务策略配置的功能。

表 *1:* 使用服务策略配置的功能

功能	适用于直通流量？	适用于管理流量？	请参阅：
应用检测（多种类型）	全部，除 RADIUS 记账以外	仅限 **RADIUS** 记账	• 应用层协议检测入门。 • 基本互联网协议检测。 • 语音和视频协议检测。 • 移动网络检测。
NetFlow 安全事件记录过滤	是	是	请参阅 NetFlow 实施指南。
QoS 输入和输出策略管制	是	否	服务质量。
QoS 标准优先级队列	是	否	服务质量。
TCP 和 UDP 连接限制与超时，以及 TCP 序列号随机化	是	是	连接设置。
TCP 规范化	是	否	连接设置。

功能	适用于直通流量？	适用于管理流量？	请参阅：
TCP 状态绕行	是	否	连接设置。
身份防火墙用户统计信息	是	是	请参阅命令参考中的 **user-statistics** 命令。

功能方向性

可以操作将双向或单向应用到流量，具体情况视功能而定。对于双向应用的功能，如果流量在两个方向上都匹配类映射，所有流入或流出应用了策略映射的接口的流量都会受到影响。

注释 当使用全局策略时，所有功能都是单向的；通常在应用到单一接口时为双向的功能，在全局应用时仅应用到每个接口的入口。因为策略应用到所有接口，策略将在两个方向上应用，因此在这种情况下，双向性是多余的。

对于单向应用的功能（例如 QoS 优先级队列），仅流入（或流出，具体取决于功能）应用了策略映射的接口的流量会受到影响。请参见下表，了解每项功能的方向性。

表 *2:* 功能方向性

功能	单一接口方向	全局方向
应用检测（多种类型）	双向	入口
NetFlow 安全事件记录过滤	N/A	入口
QoS 输入策略管制	入口	入口
QoS 输出策略管制	出口	出口
QoS 标准优先级队列	出口	出口
TCP 和 UDP 连接限制与超时，以及 TCP 序列号随机化	双向	入口
TCP 规范化	双向	入口
TCP 状态绕行	双向	入口
身份防火墙用户统计信息	双向	入口

服务策略中的功能匹配

数据包根据以下规则，匹配给定接口的策略映射中的类映射：

1. 对于每个功能类型，数据包只能与策略映射中的一个类映射匹配。
2. 在数据包匹配某个功能类型的类映射后，ASA 不会再尝试将其与该功能类型的任何后续类映射匹配。
3. 但是，如果该数据包与其他功能类型的后续类映射匹配，则 ASA 也会应用适用于该后续类映射的操作（如果支持）。请参阅某些功能操作的不兼容性，第 6 页，了解有关不受支持的组合的详细信息。

注释 应用检测包括多种检测类型，大部分类型都相互排斥。对于可以组合在一起的检测，每项检测都被视为一项独立功能。

数据包匹配示例

例如：

- 如果数据包不仅与连接限制的类映射匹配，还与应用检测的类映射匹配，则会同时应用两项操作。
- 如果数据包不仅与 HTTP 检测的类映射匹配，还与包含 HTTP 检测的另一个类映射匹配，则不会应用第二项类映射操作。
- 如果数据包不仅与 HTTP 检测的类映射匹配，还与包含 FTP 检测的另一个类映射匹配，则不会应用第二项类映射操作，因为 HTTP 和 FTP 检测无法合并。
- 如果数据包不仅与 HTTP 检测的类映射匹配，还与包含 IPv6 检测的另一个类映射匹配，则会同时应用两项操作，因为 IPv6 检测可与任何类型的检测合并。

多种功能操作的应用顺序

不同类型的操作在策略映射中的执行顺序独立于操作在策略映射中的显示顺序。

按以下顺序执行操作：

1. QoS 输入策略管制
2. TCP 规范化、TCP 和 UDP 连接限制与超时、TCP 序列号随机化以及 TCP 状态绕行。

注释 当 ASA 执行代理服务（例如 AAA）或修改 TCP 负载（例如 FTP 检测）时，TCP 规范器在双重模式下运行，即于代理或负载修改服务之前和之后进行应用。

3. 可以与其他检测合并在一起的应用检测：
    1. IPv6
    2. IP 选项

3. WAAS

4. 无法与其他检测合并在一起的应用检测。有关详细信息，请参阅某些功能操作的不兼容性，第 6 页。

5. QoS 输出策略管制

6. QoS 标准优先级队列

注释 NetFlow 安全事件记录过滤和身份防火墙用户统计信息与顺序无关。

某些功能操作的不兼容性

某些功能对于同一流量互不兼容。下表可能不包含所有不兼容性；有关每项功能兼容性的详细信息，请参阅功能对应的章节：

- 无法对同一组的流量配置优先级队列和策略管制。
- 大多数检测不应与其他检测整合使用，所以当为相同流量配置了多种检测时，ASA 仅应用一种检测。多种功能操作的应用顺序，第 5 页 中列出了其他例外情况。

注释 默认全局策略中使用的 **match default-inspection-traffic** 命令是用来匹配所有检测的默认端口的特殊 CLI 快捷方式。在策略映射中使用时，该类映射可以根据流量的目标端口确保应用到每个数据包的检测都正确。例如，当端口 69 的 UDP 流量到达 ASA 时，ASA 会应用 TFTP 检测；当端口 21 的 TCP 流量到达时，ASA 会应用 FTP 检测。因此只有在这种情况下，才能为同一类映射配置多项检测。通常，ASA 不会使用端口号来确定应用哪种检测，因此您可以灵活地对非标准端口等应用检测。

错误配置示例：在同一策略映射中配置多个检测，并且不使用 default-inspection-traffic 快捷方式。在第一个示例中，误为 FTP 和 HTTP 检测都配置了流向端口 21 的流量。在第二个示例中，误为 FTP 和 HTTP 检测都配置了流向端口 80 的流量。在这两种错误配置示例的情况下，系统仅会应用 FTP 检测，因为按照应用检测的顺序，FTP 先于 HTTP。

示例 1：FTP 数据包错误配置：也配置了 HTTP 检测

```
class-map ftp
   match port tcp eq 21
class-map http
   match port tcp eq 21 [it should be 80]
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

示例 2：HTTP 数据包错误配置：也配置了 FTP 检测

```
class-map ftp
   match port tcp eq 80 [it should be 21]
class-map http
   match port tcp eq 80
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

多个服务策略的功能匹配

对于 TCP 和 UDP 流量（以及启用状态性 ICMP 检测时的 ICMP），服务策略不仅在单个数据包上运行，还在流量上运行。如果流量为现有连接的一部分且该现有连接匹配一个接口上的策略中的某项功能，那么该流量无法匹配另一个接口上的策略中的同一项功能；仅使用第一项策略。

例如，如果 HTTP 流量匹配内部接口上的检查 HTTP 流量的策略，而且在 HTTP 检测的外部接口上有独立策略，该流量不会同时在外部接口的出口被检测。同样，该连接的返回流量不会被外部接口的入口策略检测，也不会被内部接口的出口策略检测。

对于未被当作流量处理的流量，例如，不启用状态性ICMP检测时的ICMP，返回流量可以匹配返回接口上的另一个策略映射。

服务策略准则

检测准则

本文以有单独的主题详细介绍用于应用检测服务策略的准则。请参阅应用检测准则。

IPv6 准则

支持在以下功能中使用 IPv6：

- 服务器（但并非所有）、协议的应用检测。有关详细信息，请参阅应用检测准则。
- NetFlow 安全事件记录过滤
- SCTP 状态绕行
- TCP 和 UDP 连接限制与超时，TCP 系列号随机化
- TCP 规范化
- TCP 状态绕行
- 身份防火墙用户统计信息

类映射（流量类）准则

所有类型的最大类映射（流量类）数量在单一模式下为 255，在多模式下视情景而定。类映射包括下列类型：

- 第 3/4 层类映射（对于直通流量和管理流量）。
- 检测类映射
- 正则表达式类映射
- **match** 直接在检测策略映射下使用的命令

该限制还包括所有类型的默认类映射，将用户配置的类映射限制为大约 235 个。

策略映射准则

请参阅下列有关使用策略映射的准则：

- 对于每个接口，只能分配一个策略映射。对于低端防火墙，最多可在配置中创建 64 个策略映射；对于功能更强大的防火墙，最多可创建 128 个策略映射。
- 可以将同一策略映射应用到多个接口。
- 可以在第 3/4 层映射中识别多达 63 个第 3/4 层类映射。
- 对于每个类映射，在支持的情况下，可以从一种或多种功能类型分配多项操作。请参阅某些功能操作的不兼容性，第 6 页。

服务策略准则

- 对于给定功能，入口接口上的接口服务策略优先级高于全局服务策略。例如，如果有 FTP 检测全局策略和 TCP 规范化接口策略，则系统将 FTP 检测和 TCP 规范化应用到接口。不过，如果有 FTP 检测全局策略和 FTP 检测入口接口策略，则仅向该接口应用入口接口策略 FTP 检测。如果没有入口或全局策略来实施功能，则应用出口接口上指定该功能的接口服务策略。
- 只能应用一项全局策略。例如，无法创建一个包含功能集 1 的全局策略和另一个包含功能集 2 的全局策略。所有功能都必须包含在单一策略中。
- 当对配置进行服务策略更改后，所有新连接都将使用新的服务策略。现有连接将继续使用在连接建立时配置的策略。**show** 命令输出不包含有关旧连接的数据。

  例如，如果从接口中删除 QoS 服务策略，再添加修改的版本，则 **show service-policy** 命令仅显示与匹配新服务策略的新连接相关的 QoS 计数器；命令输出中不再显示旧策略上的现有连接。

  要确保所有连接都使用新策略，需要断开当前连接，以便使用新策略重新连接。使用 **clear conn** 或 **clear local-host** 命令。

服务策略默认设置

以下主题介绍服务策略和模块化策略框架的默认设置。

默认服务策略配置

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
- SIP
- NetBios
- TFTP
- IP Options

默认类映射（流量类）

该配置包括 ASA 在默认全局策略（称为 default-inspection-traffic）中使用的默认第 3/4 层类映射（流量类）；它与默认检测流量匹配。该类在默认全局策略中使用，是一个用来匹配所有检测的默认端口的特殊快捷方式。

在策略中使用时，该类可以根据流量的目标端口，确保应用到每个数据包的检测都正确。例如，当端口 69 的 UDP 流量到达 ASA 时，ASA 会应用 TFTP 检测；当端口 21 的 TCP 流量到达时，ASA 会应用 FTP 检测。因此只有在这种情况下，才能为同一类映射配置多项检测。通常，ASA 不会使用端口号来确定应用哪种检测，因此您可以灵活地对非标准端口等应用检测。

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

默认配置中存在的另一种类映射是 class-default，它与所有流量均匹配。此类映射显示在所有第 3/4 层策略映射的末尾，基本上是告知ASA不要对任何其他流量执行任何操作。如果需要，您可以使用 class-default 类，而不是使用 Any 流量类建立自己的 **match any** 类映射。实际上，有些功能仅适用于 class-default。

```
class-map class-default
 match any
```

配置服务策略

要使用模块化策略框架配置服务策略，请执行以下步骤：

过程

步骤 1 按照身份流量（第 3/4 层类映射），第 11 页中所述，通过创建第 3/4 层类映射标识要对其执行操作的流量。

例如，您可能希望对通过 ASA 的所有流量执行操作，也可能希望仅对从 10.1.1.0/24 到任何目标地址的流量执行某些操作。

步骤 2 或者，在某些检测流量上执行其他操作。

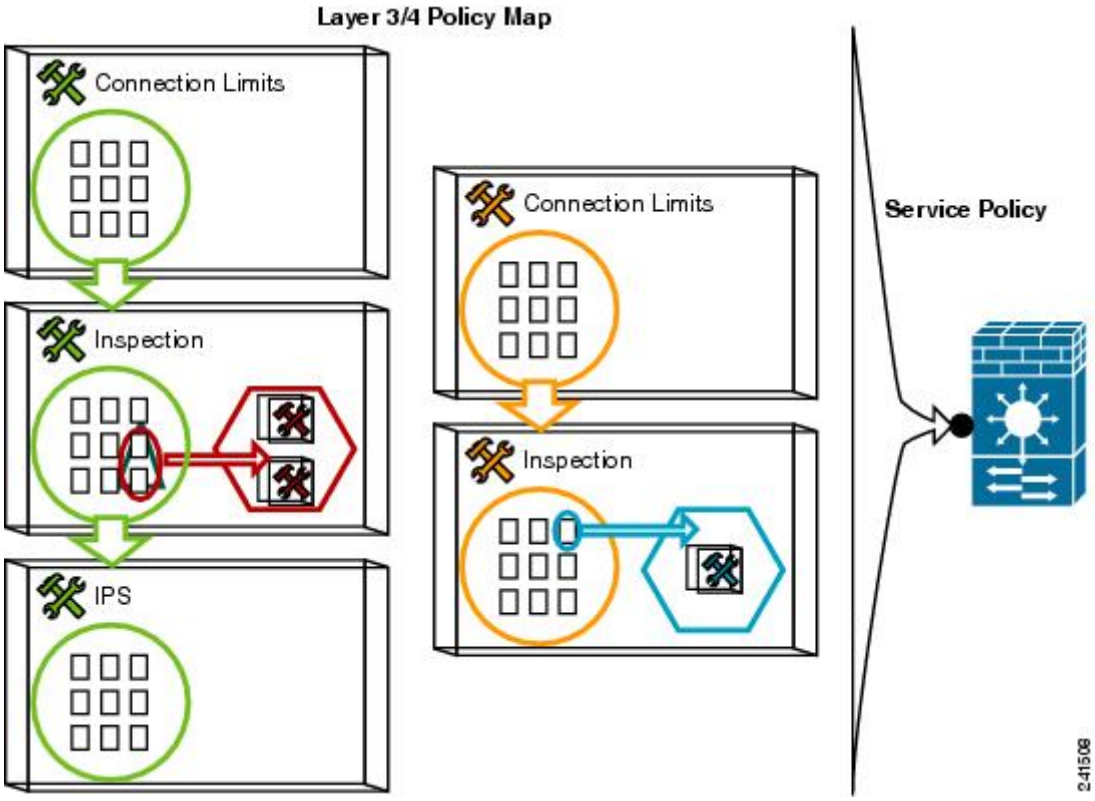
如果要执行的操作之一是应用检测，并想在某些检测流量上执行附加操作，请创建检测策略映射。检测策略映射可以识别流量并指定对流量执行的操作。

例如，您可能想丢弃所有正文长度大于 1000 字节的 HTTP 请求。

可以创建一个独立检测策略映射，该映射直接使用 **match** 命令识别流量；或者，创建一个可重复使用或进行更复杂匹配的检测类映射。例如，可以使用一个正则表达式或一组正则表达式（一个正则表达式类映射）匹配被检测数据包中的文本，并基于更小的条件范围指定操作。例如，可能想丢弃所有 URL 中包含“example.com”文本的 HTTP 请求。

请参阅配置应用层协议检测。

步骤 3 创建第 3/4 层策略映射，定义要在每个第 3/4 层类映射上执行的操作，如定义操作（第 3/4 层策略映射），第 15 页中所述。



步骤 4 确定要应用策略映射的接口，或者全局应用策略映射，如面向接口的应用操作（服务策略），第 17 页中所述。

身份流量（第 3/4 层类映射）

第 3/4 层类映射标识要应用操作的第 3 层和第 4 层流量。可以为每个第 3/4 层策略映射创建多个第 3/4 层类映射。

为通过流量创建第 3/4 层类映射

第 3/4 层类映射根据协议、端口、IP 地址和其他第 3 或 4 层属性匹配流量。

提示 我们建议您仅检测期待其中应用流量的端口上的流量；如果检测所有流量（例如使用 **match any**），ASA 的性能可能会受到影响。

过程

步骤 1 创建第 3/4 层类映射：**class-map** *class_map_name*

其中，*class_map_name* 是最多可包含 40 个字符的字符串。

保留名称“class-default”。所有类型的类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类映射使用的名称。CLI 进入类映射配置模式。

示例：

```
hostname(config)# class-map all_udp
```

步骤 2 （可选）向类映射添加说明。

description *string*

示例：

```
hostname(config-cmap)# description All UDP traffic
```

步骤 3 使用以下某个命令匹配流量。除非另有规定，否则只能在类映射中包含一条 **match** 命令。

- **match any** - 匹配所有流量。

  ```
  hostname(config-cmap)# match any
  ```

- **match access-list** *access_list_name* - 匹配扩展 ACL 指定的流量。

  ```
  hostname(config-cmap)# match access-list udp
  ```

- **match port** {**tcp** | **udp** | **sctp**} {**eq** *port_num* | **range** *port_num port_num*} - 匹配指示协议的目标端口，可以是单一端口或连续的端口范围。对于使用多个非连续端口的应用，请使用 **match access-list** 命令并定义 ACE 来匹配每个端口。

  ```
  hostname(config-cmap)# match tcp eq 80
  ```

- **match default-inspection-traffic** - 匹配默认检测流量：ASA 可检测的所有应用使用的默认 TCP 和 UDP 端口。

```
hostname(config-cmap)# match default-inspection-traffic
```

  默认全局策略中使用的此命令在用于策略映射中时是一种特殊 CLI 快捷方式，可确保根据流量的目标端口对每个数据包应用正确的检测。例如，当端口 69 的 UDP 流量到达 ASA 时，ASA 会应用 TFTP 检测；当端口 21 的 TCP 流量到达时，ASA 会应用 FTP 检测。因此仅在这种情况下，可以为同一类映射配置多个检测（WAAS 检测除外，该检测可以通过其他检测配置。请参阅某些功能操作的不兼容性，第 6 页，了解有关整合操作的详细信息）。通常，ASA 不会使用端口号来确定应用的检测，因此您可以灵活地对非标准端口等应用检测。

  请参阅默认检测和 NAT 限制，查看默认端口列表。默认情况下，不是端口包含在 **match default-inspection-traffic** 命令中的所有应用都在策略映射中启用。

  可以指定 **match access-list** 命令连同 **match default-inspection-traffic** 命令来缩小匹配的流量范围。由于 **match default-inspection-traffic** 命令指定了要匹配的端口和协议，ACL 中的任意端口和协议都将被忽略。

- **match dscp** *value1* [*value2*] [...] [*value8*] - 匹配 IP 报头中的 DSCP 值，最多 8 个 DSCP 值。

```
hostname(config-cmap)# match dscp af43 cs1 ef
```

- **match precedence** *value1* [*value2*] [*value3*] [*value4*] - 最多匹配 IP 报头中以 TOS 字节表示的四个优先级值，优先级值可以是 0 到 7。

```
hostname(config-cmap)# match precedence 1 4
```

- **match rtp** *starting_port range* - 匹配 RTP 流量，其中 *starting_port* 指定介于 2000 和 65534 之间的偶数 UDP 目标端口。*range* 指定要匹配上述 *starting_port* 的额外 UDP 端口的数量，介于 0 和 16383 之间。

```
hostname(config-cmap)# match rtp 4004 100
```

- **match tunnel-group** *name* - 匹配要应用 QoS 的 VPN 隧道组流量。

  还可以指定另一个 **match** 命令，细化流量匹配。可以指定上述命令中除 **match any**、**match access-list** 或 **match default-inspection-traffic** 之外的的任意命令。或者，还可以输入 **match flow ip destination-address** 命令，匹配隧道组中流向每个 IP 地址的流。

```
hostname(config-cmap)# match tunnel-group group1
hostname(config-cmap)# match flow ip destination-address
```

示例

以下是 **class-map** 命令的示例：

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

为管理流量创建第 3/4 层类映射

对于流入ASA的管理流量，您可能希望执行特定于此类流量的操作。可以指定能够匹配ACL、TCP或 UDP 端口的管理类映射。可用于策略映射中的管理类映射的操作类型专用于管理流量。

过程

步骤 1 创建管理类映射：**class-map type management** *class_map_name*

其中，*class_map_name* 是最多可包含 40 个字符的字符串。

保留名称“class-default”。所有类型的类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类映射使用的名称。CLI 进入类映射配置模式。

示例：

```
hostname(config)# class-map management all_udp
```

步骤 2 （可选）向类映射添加说明。

description *string*

示例：

```
hostname(config-cmap)# description All UDP traffic
```

步骤 3 使用以下某个命令匹配流量。

- **match access-list** *access_list_name* - 匹配扩展 ACL 指定的流量。

```
hostname(config-cmap)# match access-list udp
```

- **match port** {**tcp** | **udp** | **sctp**} {**eq** *port_num* | **range** *port_num port_num*} - 匹配指示协议的目标端口，可以是单一端口或连续的端口范围。对于使用多个非连续端口的应用，请使用 **match access-list** 命令并定义 ACE 来匹配每个端口。

```
hostname(config-cmap)# match tcp eq 80
```

定义操作（第 3/4 层策略映射）

配置第 3/4 层类映射识别流量之后，使用第 3/4 层策略映射将操作与这些类关联起来。

提示 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。

过程

步骤 1 添加策略映射：**policy-map** *policy_map_name*

其中 *policy_map_name* 为策略映射的名称，最长包括 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。CLI 将进入策略映射配置模式。

示例：

```
hostname(config)# policy-map global_policy
```

步骤 2 指定以前配置的第 3/4 层类映射：**class** *class_map_name*

其中，*class_map_name* 是类映射的名称。

请参阅身份流量（第 3/4 层类映射），第 11 页，添加类映射。

示例：

```
hostname(config-pmap)# class all_http
```

步骤 3 为该类映射指定一项或多项操作。

请参阅使用服务策略配置的功能，第 3 页。

注释

如果类映射中不存在 **match default-inspection-traffic** 命令，则允许在该类下最多配置一个 **inspect** 命令。

步骤 4 为想添加到策略映射中的每个类映射重复此过程。

示例

以下是用于连接策略的 **policy-map** 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：

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(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：

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout idle 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：

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

```
hostname(config-pmap-c)# set connection conn-max 2000
```

当发起 Telnet 连接时，它将与 **class telnet_traffic** 匹配。同样，如果启动 FTP 连接，则它会与 **class ftp_traffic** 进行匹配。对于除 Telnet 和 FTP 外的任何 TCP 连接，它将与 **class tcp_traffic** 进行匹配。虽然 Telnet 或 FTP 连接可与 **class tcp_traffic** 匹配，但由于它们之前已与其他类匹配，所以 ASA 不会进行此匹配。

面向接口的应用操作（服务策略）

要激活第 3/4 层策略映射，请创建一项将其应用到一个或多个接口或将其全局应用到所有接口的服务策略。使用以下命令：

service-policy *policy_map_name* {**global** | **interface** *interface_name*} [**fail-close**]

其中：

- *policy_map_name* 是策略映射的名称。
- **global** 可以创建一项应用于所有没有特定策略的接口的服务策略。

  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。默认情况下，配置包括与所有默认应用检测流量匹配的全局策略，并且将检测全局应用到流量。默认服务策略包含以下命令：**service-policy global_policy global**。
- **interface** *interface_name* 通过将策略映射与接口相关联，创建服务策略。
- **fail-close** 为不支持 IPv6 流量的应用检测丢弃的 IPv6 流量生成系统日志 (767001)。默认情况下不生成系统日志。

示例

例如，以下命令可以在外部接口上启用 inbound_policy 策略映射：

```
hostname(config)# service-policy inbound_policy interface outside
```

以下命令可禁用默认全局策略，并启用一个名为 new_global_policy 的新策略

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

监控服务策略

要监控服务策略，请输入以下命令：

- **show service-policy**

  显示服务策略统计信息。

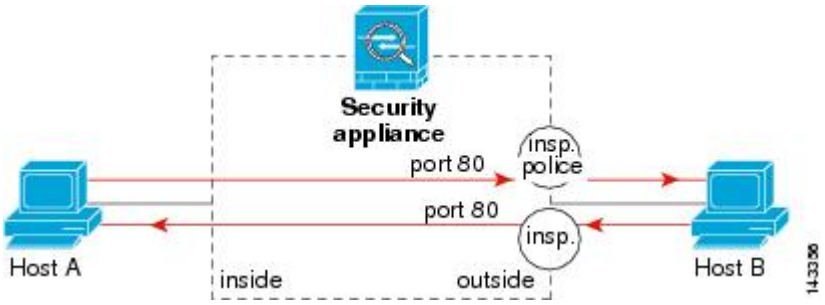
服务策略（模块化策略框架）示例

本节包括若干模块化策略框架示例。

向 HTTP 流量应用检测和 QoS 策略管制

在本例中，任何通过外部接口进出 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测进行分类。任何流出外部接口的 HTTP 流量针对策略管制进行分类。

图 *1: HTTP* 检测和 *QoS* 策略管制



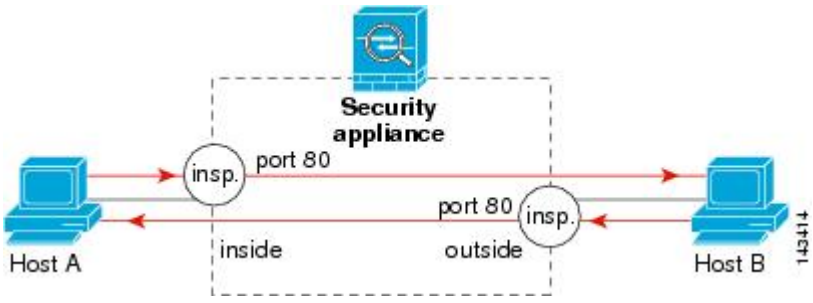
请见以下适用于本示例的命令：

```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy interface outside
```

对 HTTP 流量应用全局检测

在本例中，任何通过 any 接口进入 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测进行分类。由于采用了全局策略，检测仅在流量流入每个接口时发生。

图 *2:* 全局 *HTTP* 检测



请见以下适用于本示例的命令：

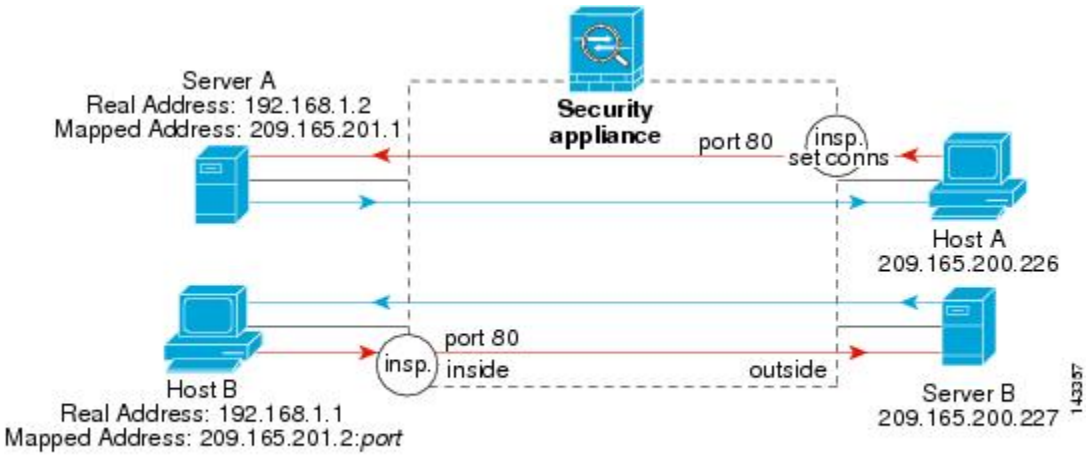
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy global
```

向流入特定服务器的 HTTP 流量应用检测和连接限制

在本例中，任何通过外部接口进入 ASA 流入服务器 A 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测和最大连接限制进行分类。从服务器 A 发起到主机 A 的连接不匹配类映射中的 ACL，因此这些连接不会受到影响。

任何通过内部接口进入 ASA 流入服务器 B 的 HTTP 连接都针对 HTTP 检测进行分类。从服务器 B 发起到主机 B 的连接不匹配类映射中的 ACL，因此这些连接不会受到影响。

图 *3:* 对于特定服务器的 *HTTP* 检测和连接限制



请见以下适用于本示例的命令：

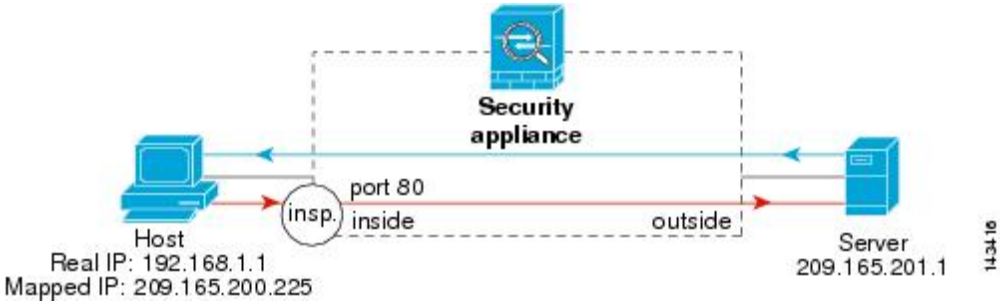
```
hostname(config)# object network obj-192.168.1.2
hostname(config-network-object)# host 192.168.1.2
hostname(config-network-object)# nat (inside,outside) static 209.165.201.1
hostname(config)# object network obj-192.168.1.0
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 209.165.201.2
hostname(config)# access-list serverA extended permit tcp any host 209.165.201.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 209.165.200.227 eq 80

hostname(config)# class-map http_serverA
hostname(config-cmap)# match access-list serverA
hostname(config)# class-map http_serverB
hostname(config-cmap)# match access-list serverB

hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA
```

```
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

通过 NAT 对 HTTP 流量应用检测

在本例中，内部网络上的主机有两个地址：一个是实际地址 192.168.1.1，另一个是在外部网络上使用的映射 IP 地址 209.165.200.225。在类映射中的 ACL 中，必须使用实际 IP 地址。如果已将其应用到外部接口，也可以使用实际地址。

图 *4:* 通过 *NAT* 进行的 *HTTP* 检测



请见以下适用于本示例的命令：

```
hostname(config)# object network obj-192.168.1.1
hostname(config-network-object)# host 192.168.1.1
hostname(config-network-object)# nat (VM1,outside) static 209.165.200.225

hostname(config)# access-list http_client extended permit tcp host 192.168.1.1 any eq 80

hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client

hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy http_client interface inside
```

服务策略的历史记录

功能名称	版本	说明
模块化策略框架	7.0(1)	引入了模块化策略框架。

功能名称	版本	说明
与 RADIUS 记账流量一起使用的管理类映射	7.2(1)	引入了管理类映射，与RADIUS 记账流量一起使用。引入了以下命令：**class-map type management** 和 **inspect radius-accounting**。
检测策略映射	7.2(1)	引入了检测策略映射。引入了以下命令：**class-map type inspect**。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，将其用于检查策略映射下。引入了以下命令：**class-map type regex**、**regex**、**match regex**。
检测策略映射的 match any	8.0(2)	引入了关键字 **match any**，与检测策略映射一起使用：流量可以匹配一个或多个条件以匹配类映射。过去，仅**match all** 可用。

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。