# 应用层协议检测入门

以下主题介绍如何配置应用层协议检测。



# 应用层协议检测

针对在用户数据包内嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用检测引擎。这些协议需要 ASA 执行深度数据包检测，而不是通过快速路径传递数据包。因此，检测引擎可能会影响整体吞吐量。默认情况下，ASA 上启用了几个常见检测引擎，但您可能需要根据您的网络启用其他检测引擎。

以下主题详细说明应用检测。

## 何时使用应用协议检测

当用户建立连接时，ASA 会对照 ACL 检查数据包、创建地址转换并为快速路径中的会话创建条目，以便后续数据包可绕过耗时的检查。但是，快速路径依赖于可预测的端口号，且不在数据包内执行地址转换。

许多协议开放辅助 TCP 或 UDP 端口。已知端口上的初始会话用于协商动态分配的端口号。

其他应用在需要与源地址匹配的数据包中嵌入 IP 地址，源地址通常在通过 ASA 时被转换。

如果使用类似的应用，需要启用应用检测。

当您对嵌入 IP 地址的服务启用应用检测时，ASA 转换嵌入的地址并更新受转换影响的所有校验和或其他字段。

当您对使用动态分配的端口的服务启用应用检测时，ASA 监控会话以标识动态端口分配并允许特定会话期间在这些端口上进行数据交换。

# 检测策略映射

可以使用检测策略映射为许多应用检测配置特殊操作。这些映射是可选的：无需配置映射，即可为支持检测策略映射的协议启用检测。仅在需要执行非默认检测操作的情况下，才需要这些映射。

检测策略映射由下列一个或多个要素组成。检测策略映射的确切可用选项视应用而定。

- 流量匹配条件 - 将应用流量与特定于应用的条件进行匹配（例如 URL 字符串，随后可以对这些条件启用操作）。

  对于某些流量匹配条件，可使用正则表达式来匹配数据包中的文本。请务必在配置策略映射之前，在正则表达式类映射中单独或集中创建和测试正则表达式。

- 检测类映射 - 某些检测策略映射可以实现使用检测类映射包含多个流量匹配条件。然后，可以在检测策略映射中识别检测类映射，并整体启用用于类的操作。创建类映射和直接在检测策略映射中定义流量匹配的差别在于，您可以创建更复杂的匹配条件和重复使用类映射。然而，您无法为不同的匹配设置不同操作。
- 参数 - 参数会影响检测引擎的行为。

以下主题提供更多详细信息。

## 更换正在使用的检测策略映射

如果在服务策略中已启用使用某一策略映射的检测，则更换策略映射需要分两步进行。首先，必须删除该检测。然后，为策略映射提供新的名称，再将其重新添加到策略中。

例如，要将 SIP 检测中的 sip-map1 替换为 sip-map2，请使用以下命令序列：

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

## 如何处理多个流量类

在检测策略映射中可以指定多个检测类映射或直接匹配。

如果一个数据包匹配不同的类或直接匹配，则 ASA 应用操作的顺序由内部 ASA 规则决定，而不是按操作添加到检测策略映射的顺序应用应用。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，但首先匹配的是 **match request method get** 命令。

```
match request header host length gt 100
  reset
match request method get
  log
```

如果操作丢弃数据包，则在检测策略映射中将不会执行进一步操作。例如，如果第一个操作是重置连接，将不会匹配任何进一步的匹配条件。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。

如果一个数据包匹配多个相同的匹配条件，则按策略映射中显示匹配条件的顺序匹配它们。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。如果颠倒两个 **match** 命令的顺序，则该数据包在匹配第二个 **match** 命令之前会被丢弃并重置连接，而从不会进行日志记录。

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

根据类映射中的最低优先级匹配选项（优先级以内部规则为准），确定一个类映射与另一个类映射的类型相同或直接匹配。如果某个类映射具有与另一个类映射相同的最低优先级匹配选项类型，则根据类映射添加到策略映射的顺序来匹配类映射。如果每个类映射的最低优先级匹配选项不同，则首先匹配具有较高优先级匹配选项的类映射。 例如，以下三个类映射包含两类 **match** 命令：**match request-cmd**（优先级较高）和 **match filename**（优先级较低）。ftp3 类映射包括这两种命令，但它们根据最低优先级命令 **match filename** 排序。ftp1 类映射包括最高优先级命令，所以首先进行匹配，不考虑它在策略映射中的顺序。ftp3 类映射的排序优先级与同样包含 **match filename** 命令的 ftp2 类映射相同。它们按照在策略映射中所处的顺序进行匹配：ftp3 先于 ftp2。

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

# 应用检测准则

### 故障转移

需要检测的多媒体会话的状态信息不通过用于状态故障转移的状态链路进行传递。但通过状态链路进行复制的 GTP、M3UA, 和 SIP 例外。您必须在 M3UA 检测中配置严格应用服务器进程 (ASP) 状态检查，才能执行状态故障转移。

### 集群

集群中不支持以下检测：

- CTIQBE
- H323、H225 和 RAS
- IPsec 穿透

- MGCP
- MMP
- RTSP
- SCCP（瘦客户端）
- WAAS

### IPv6

以下检测中支持 IPv6：

- Diameter
- DNS over UDP
- FTP
- GTP
- HTTP
- ICMP
- IPSec 直通
- IPv6
- M3UA
- SCCP（瘦客户端）
- SCTP
- SIP
- SMTP
- VXLAN

以下检测中支持 NAT64：

- DNS over UDP
- FTP
- HTTP
- ICMP
- SCTP

### 其他准则

- 某些检测引擎不支持 PAT、NAT、外部 NAT 或相同安全接口之间的 NAT。有关 NAT 支持的详细信息，请参阅默认检测和 NAT 限制，第 5 页。
- 对于所有应用检测，ASA 允许同时活动的数据连接数限为 200 个连接。例如，如果 FTP 客户端打开多个辅助连接，FTP 检测引擎只允许 200 个活动连接，第 201 个连接将被丢弃，并且自适应安全设备将生成系统错误消息。
- 检测的协议受制于高级 TCP 状态跟踪，这些连接的 TCP 状态不会自动复制。如果这些连接复制到备用设备，将会尽力尝试重新建立 TCP 状态。
- 如果系统确定 TCP 连接需要检测，系统在检测之前，将会清除除关于数据包的 MSS 和选择性确认 (SACK) 选项以外的所有 TCP 选项。其他选项将被清除，即使您在应用于连接的 TCP 映射中允许这些选项。
- 默认检测定向到 ASA（流向接口）的 TCP/UDP 流量。但是，即使启用 ICMP 检测，也不会检测流向接口的 ICMP 流量。因此，到接口的 ping（回应请求）可能会在特定情况下失败，例如，如果回应请求来自 ASA 可以通过备用默认路由到达的源。

# 应用检测的默认设置

以下主题介绍应用检测的默认操作。

## 默认检测和 NAT 限制

默认情况下，配置包括会匹配所有默认应用检测流量并对所有接口的流量应用检测的策略（全局策略）。默认应用检测流量包括流向各个协议的默认端口的流量。只能应用一个全局策略，因此如果要改变全局策略（例如，要对非标准端口应用检测，或者要添加默认情况下未启用的检测），需要编辑默认策略或者禁用默认策略并应用新策略。

下表列出了所有支持的检测、用于默认类映射的默认端口和默认打开的检测引擎（以粗体显示）。该表中还对任何 NAT 限制作了备注。在该表中：

- 默认情况下为默认端口启用的检测引擎以粗体显示。
- ASA 符合指示的标准，但它不会对要检测的数据包执行合规性。例如，FTP 命令应采用特定的顺序，但 ASA 不执行该顺序。

表 *1:* 支持的应用检测引擎

| 应用 | 默认协议、端口 | NAT 限制 | 标准 | 备注 |
|---|---|---|---|---|
| CTIQBE | TCP/2748 | 无扩展 PAT。<br>无 NAT64。<br>（集群）无静态 PAT。 | — | — |
| DCERPC | TCP/135 | 无 NAT64。 | — | — |

| 应用 | 默认协议、端口 | NAT 限制 | 标准 | 备注 |
|---|---|---|---|---|
| Diameter | TCP/3868<br>TCP/5868（用于 TCP/TLS）<br>SCTP/3868 | 无 NAT/PAT。 | RFC 6733 | 需要 Carrier 许可证。 |
| **DNS over UDP**<br>DNS over TCP | UDP/53<br>UDP/443<br>TCP/53 | 无可用于通过 WINS 进行名称解析的 NAT 支持。 | RFC 1123 | 要检测 DNS over TCP，必须在 DNS 检测策略映射中启用 DNS/TCP 检测。<br>UDP/443 仅用于思科 Umbrella DNScrypt 会话。 |
| **FTP** | TCP/21 | （集群）无静态 PAT。 | RFC 959 | — |
| GTP | UDP/3386 (GTPv0)<br>UDP/2123 (GTPv1+) | 无扩展 PAT。<br>无 NAT。 | — | 需要 Carrier 许可证。 |
| **H.323 H.225** 和 **RAS** | TCP/1720 UDP/1718 UDP (RAS) 1718-1719 | （集群）无静态 PAT。<br>无扩展 PAT。<br>不支持对同类安全接口执行 NAT。<br>无 NAT64。 | ITU-T H.323、H.245、H225.0、Q.931、Q.932 | — |
| HTTP | TCP/80 | — | RFC 2616 | 请注意，MTU 限制会去除 ActiveX 和 Java。如果 MTU 因为太小而不允许在一个数据包中包含 Java 或 ActiveX 标记，可能不会出现去除操作。 |
| ICMP | ICMP | — | — | 不会检测流向 ASA 接口的 ICMP 流量。 |
| ICMP 错误 | ICMP | — | — | — |
| ILS (LDAP) | TCP/389 | 无扩展 PAT。<br>无 NAT64。 | — | — |
| 即时消息 (IM) | 因客户端而异 | 无扩展 PAT。<br>无 NAT64。 | RFC 3860 | — |
| **IP** 选项 | RSVP | 无 NAT64。 | RFC 791、RFC 2113 | — |

| 应用 | 默认协议、端口 | NAT 限制 | 标准 | 备注 |
|---|---|---|---|---|
| IPSec 穿透 | UDP/500 | 无 PAT。<br>无 NAT64。 | — | — |
| IPv6 | — | 无 NAT64。 | RFC 2460 | — |
| LISP | — | 无 NAT 或 PAT。 | — | — |
| M3UA | SCTP/2905 | 无面向嵌入式地址的 NAT 或 PAT。 | RFC 4666 | 需要 Carrier 许可证。 |
| MGCP | UDP/2427、2727 | 无扩展 PAT。<br>无 NAT64。<br>（集群）无静态 PAT。 | RFC 2705bis-05 | — |
| MMP | TCP/5443 | 无扩展 PAT。<br>无 NAT64。 | — | — |
| 基于 IP 的 **NetBIOS 名称服务器** | UDP/137、138（源端口） | 无扩展 PAT。<br>无 NAT64。 | — | 通过执行 NBNS UDP 端口 137 和 NBDS UDP 端口 138 的数据包 NAT 来支持 NetBIOS。 |
| PPTP | TCP/1723 | 无 NAT64。<br>（集群）无静态 PAT。 | RFC 2637 | — |
| RADIUS 记账 | UDP/1646 | 无 NAT64。 | RFC 2865 | — |
| **RSH** | TCP/514 | 无 PAT。<br>无 NAT64。<br>（集群）无静态 PAT。 | Berkeley UNIX | — |
| **RTSP** | TCP/554 | 无扩展 PAT。<br>无 NAT64。<br>（集群）无静态 PAT。 | RFC 2326、2327、1889 | 无 HTTP 掩蔽处理。 |
| SCTP | SCTP | — | RFC 4960 | 需要 Carrier 许可证。<br>虽然可以对 SCTP 流量执行静态网络对象 NAT（无动态 NAT/PAT），但检测引擎不用于 NAT。 |

| 应用 | 默认协议、端口 | NAT 限制 | 标准 | 备注 |
|---|---|---|---|---|
| **SIP** | TCP/5060<br>UDP/5060 | 在安全级别相同或低于较高安全级别的接口上无 NAT/PAT。<br>无扩展 PAT。<br>无 NAT64 或 NAT46。<br>（集群）无静态 PAT。 | RFC 2543 | 某些情况下不处理 TFTP 上传的思科 IP 电话配置。 |
| **瘦客户端 (SCCP)** | TCP/2000 | 不支持对同类安全接口执行 NAT。<br>无扩展 PAT。<br>无 NAT64、NAT46 或 NAT66。<br>（集群）无静态 PAT。 | — | 某些情况下不处理 TFTP 上传的思科 IP 电话配置。 |
| **SMTP** 和 **ESMTP** | TCP/25 | 无 NAT64。 | RFC 821、1123 | — |
| SNMP | UDP/161、162<br>同样运行 Cisco Secure Firewall eXtensible 操作系统 (FXOS) 的平台上的 UDP/4161。 | 无 NAT 或 PAT。 | RFC 1155、1157、1212、1213、1215 | v.2 RFC 1902-1908；v.3 RFC 2570-2580。<br>在 FXOS 平台上，如果配置了 SNMP，则会自动启用该检测功能，且无法禁用。 |
| **SQL*Net** | TCP/1521 | 无扩展 PAT。<br>无 NAT64。<br>（集群）无静态 PAT。 | — | v.1 和 v.2。 |
| STUN | TCP/3478<br>UDP/3478 | (WebRTC) 仅静态 NAT/PAT44。<br>（思科 Spark）静态 NAT/PAT44 和 64；动态 NAT/PAT。 | RFC 5245、5389 | — |
| **Sun RPC** | TCP/111<br>UDP/111 | 无扩展 PAT。<br>无 NAT64。 | — | — |
| **TFTP** | UDP/69 | 无 NAT64。<br>（集群）无静态 PAT。 | RFC 1350 | 不转换负载 IP 地址。 |
| WAAS | TCP/1 - 65535 | 无扩展 PAT。<br>无 NAT64。 | — | — |

| 应用 | 默认协议、端口 | NAT 限制 | 标准 | 备注 |
|---|---|---|---|---|
| XDMCP | UDP/177 | 无扩展 PAT。<br>无 NAT64。<br>（集群）无静态 PAT。 | — | — |
| VXLAN | UDP/4789 | 不适用 | RFC 7348 | 虚拟可扩展局域网。 |

## 默认检测策略映射

某些检测类型使用隐藏的默认策略映射。例如，如果启用 ESMTP 检测但不指定映射，将会使用 _default_esmtp_map。

说明每种检测类型的各节中介绍了默认检测。可以使用 **show running-config all policy-map** 命令查看这些默认映射。

DNS 检测是唯一一种采用明确配置的默认映射 preset_dns_map 的检测。

# 配置应用层协议检测

应用检测在服务策略中进行配置。

某些使用标准端口和协议的应用，默认已在所有接口上全局启用检测。有关默认检测的详细信息，请参阅默认检测和 NAT 限制，第 5 页。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

### 开始之前

对于某些应用，在配置检测策略映射来启用检测时，可以执行特殊操作。此操作步骤后面的表显示了哪些协议允许检测策略映射，还提供了指向相关配置说明的链接。如果希望配置这些高级功能，请首先创建映射，再配置检测。

### 过程

**步骤 1** 除非是向现有类映射中添加检测，否则可创建一个 L3/L4 类映射来标识要应用该检测的流量。

```
class-map name
match parameter
```

**示例：**

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

在默认全局策略中，inspection_default 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。只有 inspection_default 类可以有多项检测，而且可能需要简单地编辑应用检测默认操作的现有全局策略。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。有关选择哪种类映射的详细信息，请参阅选择适合检测的流量类，第 14 页。

有关匹配语句的信息，请参阅为通过流量创建第 3/4 层类映射。有关使用管理层 3/4 类的 RADIUS 计费检测，请参阅配置 RADIUS 计费检测。

**步骤 2** 添加或编辑第 3/4 层策略映射，以用于设置要对类映射流量执行的操作：**policy-map** *name*

**示例：**

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

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

**步骤 3** 标识正在用于检测的第 3/4 层类映射：**class** *name*

**示例：**

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

要编辑默认策略，或者在新策略中使用特殊的 inspection_default 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的操作步骤中创建的类。

必要时可以将多个类映射合并在同一策略中，因此可以创建一个类映射来匹配某些流量，创建另一个类映射来匹配不同流量。但是，如果流量匹配包含检测命令的某个类映射，然后匹配也包含检测命令的另一个类映射，将会仅使用第一个匹配的类。例如，SNMP 匹配 inspection_default 类映射。要启用 SNMP 检测，请启用默认类的 SNMP 检测。请勿添加另一个匹配 SNMP 的类。

**步骤 4** 启用应用检测：**inspect** *protocol*

*protocol* 是以下其中一个值：

**表 *2:* 检测协议关键字**

| 关键字 | 注 |
|---|---|
| **ctiqbe** | 请参阅 CTIQBE 检测。 |
| **dcerpc** [*map_name*] | 请参阅 DCERPC 检测。<br>如果已按照配置 DCERPC 检测策略映射中所述添加了 DCERPC 检测策略映射，请在此命令中识别映射名称。 |

| 关键字 | 注 |
| --- | --- |
| **diameter** [*map_name*] [ **tls-proxy** *proxy_name*] | 请参阅Diameter 检测。<br>如果已按照配置 Diameter 检测策略映射中所述添加了 Diameter 检测策略映射，请在此命令中识别映射名称。<br>**tls-proxy** *proxy_name* 标识用于此检测的 TLS 代理。仅在要启用加密流量检测时，才需要 TLS 代理。 |
| **dns** [*map_name*] [**dynamic-filter-snoop**] | 请参阅 DNS 检测。<br>如果已按照配置 DNS 检测策略映射中所述添加了 DNS 检测策略映射，请在此命令中识别映射名称。默认 DNS 检测策略映射名称为“preset_dns_map”。<br>**dynamic-filter-snoop** 启用僵尸网络流量过滤器专用的动态过滤器监听。应仅在使用僵尸网络流量过滤时包含此关键字。我们建议仅在有外部 DNS 请求经过的接口上启用 DNS 监听。在所有 UDP DNS 流量（包括流向内部 DNS 服务器的流量）上启用 DNS 监听会为 ASA 形成不必要的负载。 |
| **esmtp** [*map_name*] | 请参阅 SMTP 和扩展 SMTP 检测。<br>如果已按照配置 ESMTP 检测策略映射中所述添加了 ESMTP 检测策略映射，请在此命令中识别映射名称。 |
| **ftp** [**strict** [*map_name*]] | 请参阅 FTP 检测。<br>使用 **strict** 关键字防止网络浏览器在 FTP 请求中发送嵌入式命令，从而提高受保护网络的安全。有关详细信息，请参阅严格 FTP。<br>如果已按照配置 FTP 检测策略映射中所述添加了 FTP 检测策略映射，请在此命令中识别映射名称。 |
| **gtp** [*map_name*] | 请参阅 GTP 检测概述。<br>如果已按照配置 GTP 检测策略映射中所述添加了 GTP 检测策略映射，请在此命令中识别映射名称。 |
| **h323 h225** [*map_name*] | 请参阅 H.323 检测。<br>如果已按照配置 H.323 检测策略映射中所述添加了 H323 检测策略映射，请在此命令中识别映射名称。 |
| **h323 ras** [*map_name*] | 请参阅 H.323 检测。<br>如果已按照配置 H.323 检测策略映射中所述添加了 H323 检测策略映射，请在此命令中识别映射名称。 |

| 关键字 | 注 |
| --- | --- |
| **http** [*map_name*] | 请参阅 HTTP 检测。<br>如果已按照配置 HTTP 检测策略映射中所述添加了 HTTP 检测策略映射，请在此命令中识别映射名称。 |
| **ICMP** | 请参阅 ICMP 检查。 |
| **icmp error** | 请参阅 ICMP 错误检测。 |
| **ils** | 请参阅 ILS 检测。 |
| **im** [*map_name*] | 请参阅即时消息检测。<br>如果添加了即时消息检测策略映射，请在此命令中识别映射名称。 |
| **ip-options** [*map_name*] | 请参阅IP 选项检测。<br>如果已按照配置 IP 选项检测策略映射中所述添加了 IP 选项检测策略映射，请在此命令中识别映射名称。 |
| **ipsec-pass-thru** [*map_name*] | 请参阅IPsec 穿透检测。<br>如果已按照配置 IPsec 穿透检测策略映射中所述添加了 IPSec 直通检测策略映射，请在此命令中识别映射名称。 |
| **ipv6** [*map_name*] | 请参阅 Ipv6 检测。<br>如果已按照配置 IPv6 检测策略映射中所述添加了 IPv6 检测策略映射，请在此命令中识别映射名称。 |
| **lisp** [*map_name*] | 有关配置 LISP 的详细信息（包括检测），请参阅一般配置指南中的“集群”一章。<br>如果添加了 LISP 检测策略映射，请在此命令中识别映射名称。 |
| **m3ua** [*map_name*] | 请参阅M3UA 检测。<br>如果已按照配置 M3UA 检测策略映射中所述添加了 M3UA 检测策略映射，请在此命令中识别映射名称。 |
| **mgcp** [*map_name*] | 请参阅 MGCP 检测。<br>如果已按照配置 MGCP 检测策略映射中所述添加了 MGCP 检测策略映射，请在此命令中识别映射名称。 |
| **netbios** [*map_name*] | 请参阅NetBIOS 检测。<br>如果添加了 NetBIOS 检测策略映射，请在此命令中识别映射名称。 |
| **pptp** | 请参阅 PPTP 检测。 |

| 关键字 | 注 |
| --- | --- |
| **radius-accounting** *map_name* | 请参阅 RADIUS 计费检测概述。<br>**radius-accounting** 关键字仅适用于管理类映射。必须指定 RADIUS 记账检测策略映射；请参阅配置 RADIUS 计费检测策略映射。 |
| **rsh** | 请参阅 RSH 检测。 |
| **rtsp** [*map_name*] | 请参阅 RTSP 检测。<br>如果已按照配置 RTSP 检测策略映射中所述添加了 RTSP 检测策略映射，请在此命令中识别映射名称。 |
| **sctp** [*map_name*] | 请参阅SCTP 应用层检测。<br>如果已按照配置 SCTP 检测策略映射中所述添加了 SCTP 检测策略映射，请在此命令中识别映射名称。 |
| **sip** [*map_name*] [**tls-proxy** *proxy_name*] | 请参阅 SIP 检测。<br>如果已按照配置 SIP 检测策略映射中所述添加了 SIP 检测策略映射，请在此命令中识别映射名称。<br>**tls-proxy** *proxy_name* 标识用于这项检测的 TLS 代理。仅在要启用加密流量检测时，才需要 TLS 代理。 |
| **skinny** [*map_name*] | 请参阅瘦客户端 (SCCP) 检测。<br>如果已按照配置瘦小客户端 (SCCP) 检测策略映射中所述添加了瘦客户端检测策略映射，请在此命令中识别映射名称。 |
| **snmp** [*map_name*] | 请参阅 SNMP 检测。<br>如果添加了 SNMP 检测策略映射，请在此命令中识别映射名称。 |
| **sqlnet** | 请参阅SQL*Net 检测。 |
| **stun** | 请参阅STUN 检测。 |
| **sunrpc** | 请参阅 Sun RPC 检测。<br>默认类映射包括 UDP 端口 111；如果要为 TCP 端口 111 启用 Sun RPC 检测，需要创建一个匹配 TCP 端口 111 的新类映射，将该类添加到策略中，再向该类应用 **inspect sunrpc** 命令。 |
| **tftp** | 请参阅 TFTP 检测。 |
| **waas** | 启用 TCP 选项 33 解析。部署思科广域应用服务产品时使用。 |
| **xdmcp** | 请参阅 XDMCP 检测。 |
| **vxlan** | 请参阅 VXLAN 检测。 |

**注释**
如果要编辑默认全局策略（或任何使用中的策略）来使用不同的检测策略映射，必须使用 **no inspect** *protocol* 命令删除旧的检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

**示例：**

```
hostname(config-class)# no inspect sip
hostname(config-class)# inspect sip sip-map
```

**步骤 5** 如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

**service-policy** *policymap_name* {**global** | **interface** *interface_name*}

**示例：**

```
hostname(config)# service-policy global_policy global
```

**Global** 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

# 选择适合检测的流量类

直通流量的默认第 3/4 层类映射称为“inspection_default”。该类映射与使用特殊 **match** 命令 **match default-inspection-traffic** 的流量匹配，以便匹配每个应用协议的默认协议和端口。此流量类（以及通常不用于检测的 **match any**）匹配支持 IPv6 检测的 IPv4 和 IPv6 流量。有关支持 IPv6 的检测的列表，请参阅应用检测准则，第 3 页。

可以指定 **match access-list** 命令连同 **match default-inspection-traffic** 命令来缩小流向特定 IP 地址的匹配流量范围。由于 **match default-inspection-traffic** 命令指定了要匹配的端口和协议，所以 ACL 中的任何端口将被忽略。

**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。

如果要匹配非标准端口，请创建适用于非标准端口的新的类映射。有关每个检测引擎的标准端口，请参阅默认检测和 NAT 限制，第 5 页。必要时可以将多个类映射合并在同一策略中，因此可以创建一个类映射来匹配某些流量，创建另一个类映射来匹配不同流量。但是，如果流量匹配包含检测命令的某个类映射，然后匹配也包含检测命令的另一个类映射，将会仅使用第一个匹配的类。例如，SNMP 匹配 inspection_default 类。要启用 SNMP 检测，请启用默认类的 SNMP 检测。请勿添加另一个匹配 SNMP 的类。

例如，要使用默认类映射将检测限制为针对从 10.1.1.0 到 192.168.1.0 的流量，请输入以下命令：

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

使用以下命令可查看整个类映射：

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
 match default-inspection-traffic
 match access-list inspect
!
```

要检测端口 21 和 1056（非标准端口）上的 FTP 流量，请创建指定端口的 ACL，并将其分配给一个新的类映射：

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

# 配置正则表达式

正则表达式定义文本字符串的模式匹配。可以在某些协议检测映射中使用这些表达式根据字符串（例如，URL 或特定报头字段的内容）来匹配数据包。

## 创建正则表达式

正则表达式可逐字地完全匹配文本字符串，或者，可以使用 *metacharacters* 来匹配文本字符串的多个变体。可以使用正则表达式匹配某些应用流量的内容，例如，可以匹配 HTTP 数据包中的 URL 字符串。

### 开始之前

使用 **Ctrl+V** 对 CLI 中的所有特殊字符进行转义，例如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]?g** 以在配置中输入 **d?g**。

有关将正则表达式匹配数据包时对性能造成影响的信息，请参阅命令参考中的 **regex** 命令。一般来说，匹配长输入字符串或尝试匹配大量的正则表达式将会降低系统性能。

**注释** 为了优化性能，ASA 可在去模糊化的 URL 中搜索。去模糊化处理将多个正斜杠 (/) 压缩为一个斜杠。对于通常使用双斜杠的字符串（例如“http://”），请务必搜索“http:/”。

下表列出了有特殊意义的元字符。

表 *3:* 正则表达式元字符

| 字符 | 说明 | 注 |
|---|---|---|
| . | 点 | 匹配任何单个字符。例如，**d.g** 匹配 dog、dag、dtg 以及任何含有这些字符的单词，如 doggonnit。 |
| (*exp*) | 子表达式 | 子表达式将字符与其周围的字符分隔开，从而可以在子表达式上使用其他元字符。例如，**d(o\|a)g** 匹配 dog 和 dag，但是，**do\|ag** 匹配 do 和 ag。子表达式还可以与重复限定符配合使用，以区分意味着重复的字符。例如，**ab(xy){3}z** 匹配 abxyxyxyz。 |
| \| | 交替 | 匹配其分隔的任意一个表达式。例如，**dog\|cat** 匹配 dog 或 cat。 |
| ? | 问号 | 一个限定符，表示前面有 0 个或 1 个表达式。例如，**lo?se** 匹配 lse 或 lose。 |
| * | 星号 | 一个限定符，表示前面有 0 个、1 个或任意数量的表达式。例如，**lo*se** 匹配 lse、lose、loose 等等。 |
| + | 加号 | 一个限定符，表示前面至少有 1 个表达式。例如，**lo+se** 匹配 lose 和 loose，但不匹配 lse。 |
| {*x*} 或 {*x*,} | 最小重复限定符 | 至少重复 *x* 次。例如，**ab(xy){2,}z** 匹配 abxyxyz、abxyxyxyz 等等。 |
| [*abc*] | 字符类 | 匹配方括号中的任意字符。例如，**[abc]** 匹配 a、b 或 c。 |
| [^*abc*] | 求反字符类 | 匹配不包含在方括号中的单个字符。例如，**[^abc]** 匹配 a、b 或 c 以外的任意字符。**[^A-Z]** 匹配非大写字母形式的任意单个字符。 |
| [*a-c*] | 字符范围类 | 匹配范围内的任意字符。**[a-z]** 匹配任意小写字母。可以混合使用字符和字符范围：**[abcq-z]** 匹配 a、b、c、q、r、s、t、u、v、w、x、y 和 z，**[a-cq-z]** 也是匹配这些字符。<br>破折号 (-) 字符仅在是括号中的最后一个或第一个字符时，才是原义字符：例如，**[abc-]** 或 **[-abc]**。 |
| “ ” | 引号 | 保留字符串中的尾随空格或前导空格。例如，**" test"**在查找匹配时会保留前导空格。 |
| ^ | 脱字号 | 指定行首。 |

| 字符 | 说明 | 注 |
| --- | --- | --- |
| \ | 转义字符 | 当与元字符一起使用时，可以匹配原义字符。例如，**\[** 匹配左方括号。 |
| *char* | 字符 | 当字符不是元字符时，匹配原义字符。 |
| \r | 回车符 | 匹配回车符 0x0d。 |
| \n | 换行符 | 匹配换行符 0x0a。 |
| \t | Tab | 匹配制表符 0x09。 |
| \f | 换页符 | 匹配换页符 0x0c。 |
| \x*NN* | 转义的十六进制数字 | 匹配十六进制的 ASCII 字符（必须是两位数）。 |
| *NNN* | 转义的八进制数字 | 匹配八进制的 ASCII 字符（必须是三位数）。例如，字符 040 代表空格。 |

### 过程

**步骤 1** 测试正则表达式，以确保其匹配内容与您的预期相符：**test regex** *input_text regular_expression*

其中 *input_text* 参数为使用正则表达式要匹配的字符串，最长为 201 个字符。*regular_expression* 参数最多可包含 100 个字符。

使用 **Ctrl+V** 可转义 CLI 中的所有特殊字符。例如，要在 **test regex** 命令的输入文本中输入制表符，必须输入 **test regex "test[Ctrl+V Tab]" "test\t"**。

如果正则表达式匹配输入文本，您将看到以下消息：

```
INFO: Regular expression match succeeded.
```

如果正则表达式不匹配输入文本，您将看到以下消息：

```
INFO: Regular expression match failed.
```

**步骤 2** 若在测试后要添加正则表达式，请输入以下命令：**regex** *name regular_expression*

其中，*name* 参数最多可包含 40 个字符。*regular_expression* 参数最多可包含 100 个字符。

### 示例

以下示例创建两个用于检测策略映射的正则表达式：

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

# 创建正则表达式类映射

正则表达式类映射识别一个或多个正则表达式，是正则表达式对象的集合。在很多情况下，可以使用正则表达式类映射代替正则表达式对象。

### 过程

**步骤 1** 创建正则表达式类映射：**class-map type regex match-any** *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。

**match-any** 关键字指明如果流量至少匹配类映射中的一个正则表达式，那么它匹配类映射。

**步骤 2** （可选）向类映射添加说明：**description** *string*

**步骤 3** 通过为每个正则表达式输入以下命令标识要包括的正则表达式：**match regex** *regex_name*

### 示例

以下示例创建两个正则表达式，并将它们添加到正则表达式类映射。如果流量包含字符串“example.com”或“example2.com”，则其匹配该类映射。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
```

# 监控检测策略

要监控检测服务策略，请输入以下命令。有关详细的语法和示例，请参阅 Cisco.com 上的命令参考。

- **show service-policy inspect** *protocol*

  显示检测服务策略的统计信息。*protocol* 指来自检测命令的协议，例如 **dns**。但是，并非所有检测协议的统计信息均通过此命令显示。例如：

```
asa# show service-policy inspect dns

Global policy:
  Service-policy: global_policy
```

```
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
asa#
```

- **show conn**

  显示流经设备的流量的当前连接。此命令包括各种关键字，让您可获取有关各种协议的信息。

- 用于特定检测协议的其他命令：
  - **show ctiqbe**

    显示 CTIQBE 检测引擎所分配媒体连接的相关信息.

  - **show h225**

    显示 H.225 会话的相关信息。

  - **show h245**

    显示终端使用慢启动 (slow start) 建立的 H.245 会话的相关信息。

  - **show h323 ras**

    显示网守与其 H.323 终端之间建立的 H.323 RAS 会话的连接信息。

  - **show mgcp**{**commands** |**sessions** }

    显示命令队列中的 MGCP 命令数量或现有的 MGCP 会话数量。

  - **show sip**

    显示 SIP 会话的相关信息。

  - **show skinny**

    显示瘦小客户端控制协议 (SCCP) 会话的信息。

  - **show sunrpc-server active**

    显示为 Sun RPC 服务打开的针孔。

# 应用检测的历史记录

| 功能名称 | 版本 | 说明 |
| --- | --- | --- |
| 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**。 |

| 功能名称 | 版本 | 说明 |
| --- | --- | --- |
| 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。