语音和视频协议检测

以下主题介绍针对语音和视频协议的应用检测。有关为何需要对某些协议进行检测以及应用检测的总体方法的基本信息，请参阅应用层协议检测入门。

CTIQBE 检测

CTIQBE 协议检测支持 NAT、PAT 和双向 NAT。借此，思科 IP SoftPhone 及其他思科 TAPI/JTAPI 应用可协同思科 CallManager 在 ASA 范围内成功进行呼叫建立。

许多思科 VoIP 应用都使用 TAPI 和 JTAPI。思科 TSP 通过 CTIQBE 与 Cisco CallManager 通信。

有关启用 CTIQBE 检测的信息，请参阅配置应用层协议检测。

CTIQBE 检测的局限性

不支持 CTIQBE 呼叫状态故障转移。

下面总结了在特定情况下使用 CTIQBE 应用检测时的特殊注意事项：

- 如果两个思科 IP SoftPhone 注册到不同的思科 CallManager，且这两个思科 CallManager 连接到不同的 ASA 接口，则两个电话之间的呼叫将会失败。
- 当 Cisco CallManager 位于比 Cisco IP SoftPhone 更高的安全接口上时，如果 Cisco CallManager IP 地址必须执行 NAT 或外部 NAT，则映射必须为静态，因为 Cisco IP SoftPhone 需要在 PC 上的思科 TSP 配置中明确指定 Cisco CallManager IP 地址。

- 当使用 PAT 或外部 PAT 时，如果要转换 Cisco CallManager IP 地址，则必须将其 TCP 端口 2748 静态映射到 PAT（接口）地址的同一端口上，以便成功注册 Cisco IP SoftPhone。CTIQBE 侦听端口 (TCP 2748) 是固定的，用户不能在 Cisco CallManager、Cisco IP SoftPhone 或思科 TSP 上进行配置。

H.323 检测

H.323 检测支持 RAS、H.225 和 H.245，这项检测功能会转换所有嵌入式 IP 地址和端口。H.323 检测执行状态跟踪和过滤，并且可以激活很多检测功能。H.323 检测支持电话号码过滤、动态 T.120 控制、H.245 隧道控制、HSI 组、协议状态跟踪、H.323 呼叫持续时间限制、T.38 传真和音频/视频控制。

默认情况下，H.323 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。

以下各节介绍 H.323 应用检测。

H.323 检测概述

H.323 检测支持符合 H.323 规范的应用，例如思科 CallManager。H.323 是国际电信联盟制定的一套协议，用于通过 LAN 进行多媒体会议。ASA 最高支持 H.323 版本 6，其中包括 H.323 版本 3“支持在一个呼叫信令通道上进行多个呼叫”的功能。

启用 H.323 检测后，ASA 支持在同一呼叫信令通道上进行多个呼叫（此功能在 H.323 版本 3 中引入）。此功能可缩短呼叫建立时间并减少 ASA 上端口的使用。

H.323 检测具有如下两个主要功能：

- 对 H.225 和 H.245 消息中必要的嵌入式 IPv4 地址进行 NAT 转换。由于 H.323 消息以 PER 编码格式编码，所以 ASA 使用 ASN.1 解码器来解码 H.323 消息。
- 动态分配协商的 H.245 和 RTP/RTCP 连接。使用 RAS 时，也可以动态分配 H.225 连接。

H.323 工作原理

H.323 协议集合总共最多可以使用两个 TCP 连接和四到八个 UDP 连接。FastConnect 仅使用一个 TCP 连接，且 RAS 使用单个 UDP 连接用于注册、准入和状态。

首先，H.323 客户端可以使用 TCP 端口 1720 与 H.323 服务器之间初步建立 TCP 连接，以请求建立 Q.931 呼叫。在呼叫建立过程中，H.323 终端向客户端提供用于 H.245 TCP 连接的端口号。在使用 H.323 网守的环境中，初始数据包使用 UDP 进行传输。

H.323 检测会监控 Q.931 TCP 连接，以确定 H.245 端口号。如果 H.323 终端使用的不是 FastConnect，ASA 将基于 H.225 消息的检测动态分配 H.245 连接。使用 RAS 时，也可以动态分配 H.225 连接。

在每个 H.245 消息中，H.323 终端交换用于后续 UDP 数据流的端口号。H.323 检测会检测 H.245 消息来标识这些端口，并动态创建用于媒体交换的连接。RTP 使用协商的端口号，而 RTCP 使用下一个更高的端口号。

H.323 控制信道处理 H.225、H.245 和 H.323 RAS。H.323 检测使用以下端口。

- 1718 - 网守发现 UDP 端口
- 1719 - RAS UDP 端口
- 1720 - TCP 控制端口

要实现 RAS 信令，必须允许已知 H.323 端口 1719 的流量。此外，要实现 H.225 呼叫信令，必须允许已知 H.323 端口 1720 的流量；但是，H.245 信令端口要在 H.225 信令中的终端之间协商。使用 H.323 网守时，ASA 将基于 ACF 和 RCF 消息的检测打开 H.225 连接。

检测 H.225 消息后，ASA 将打开 H.245 通道，然后也会检测通过 H.245 通道发送的流量。通过 ASA 传递的所有 H.245 消息均会接受 H.245 应用检测，即转换嵌入的 IP 地址并打开 H.245 消息中协商的媒体通道。

每个具有通过 H.323 检测的数据包的 UDP 连接都将被标记为 H.323 连接，且每个连接均按照使用 **timeout** 命令配置的 H.323 超时值设置超时值。

注释 如果网守在网络内部，可以在 H.323 终端之间启用呼叫建立。ASA 包括基于 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息打开呼叫针孔的选项。由于这些 RRQ/RCF 消息会进出网守，所以呼叫终端的 IP 地址未知且 ASA 会通过源 IP 地址/端口 0/0 打开针孔。默认情况下，此选项已禁用。要在 H.323 终端之间启用呼叫建立，请在创建 H.323 检测策略映射时在参数配置模式期间输入 **ras-rcf-pinholes enable** 命令。

H.245 消息中的 H.239 支持

ASA 位于两个 H.323 终端之间。当两个 H.323 终端建立电话演示会话以便终端可收发数据演示（例如电子表格数据）时，ASA 可确保两个终端之间成功进行 H.239 协商。

H.239 是一项标准，使 H.300 系列终端能够在单个呼叫中打开另外一个视频信道。在呼叫中，终端（例如视频电话）会发送视频信道和数据演示信道。H.239 协商发生于 H.245 信道上。

ASA 可为更多媒体信道和媒体控制信道打开针孔。终端使用开放逻辑信道 (OLC) 消息来发出有关新信道创建的信息。消息扩展是 H.245 v13 的一部分。

默认情况下，电话演示会话的解码和编码已启用。H.239 的编码和解码由 ASN.1 编码器执行。

H.323 检测的局限性

H.323 检测已经过测试，受思科统一通信管理器 (CUCM) 7.0 支持。CUCM 8.0 及更高版本不支持这项检测。H.323 检测可能适用于其他版本和产品。

以下是 H.323 应用检测的某些已知问题和局限性：

- 支持 PAT，但扩展 PAT 或每会话 PAT 除外。

- 静态 PAT 可能无法正确转换 H.323 消息内嵌入到可选字段中的 IP 地址。如果遇到这种问题，请勿对 H.323 使用静态 PAT。
- 不支持同一安全级别接口之间的 NAT。
- 不支持 NAT64。
- 带有 H.323 检测的 NAT 直接在终端上执行时与 NAT 不兼容。如果在终端上执行 NAT，请禁用 H.323 检测。

配置 H.323 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 H.323 检测策略映射以自定义 H.323 检测操作。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 （可选）执行以下步骤创建 H.323 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect h323** [**match-all** | **match-any**] *class_map_name*

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定如果流量匹配至少一个条件，则匹配类映射。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

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

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*} - 将被叫方与指定的正则表达式或正则表达式类进行匹配。

- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*} - 将主叫方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **media-type** {**audio** | **data** | **video**} - 匹配媒体类型。

步骤 2 创建 H.323 检测策略映射：**policy-map type inspect h323** *policy_map_name*

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description** *string*

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅如何处理多个流量类。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 H.323 类映射，请输入以下命令对其进行指定：**class** *class_map_name*
- 对 H.323 类映射使用上述 **match** 命令之一，以直接在策略映射中指定流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop** [**log**] - 丢弃数据包。对于媒体类型匹配，可以包括 **log** 关键字以发送系统日志消息。
- **drop-connection** - 丢弃数据包并关闭连接。此选项适用于被叫方匹配或主叫方匹配。
- **reset** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。此选项适用于被叫方匹配或主叫方匹配。

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **ras-rcf-pinholes enable** - 启用 H.323 终端之间的呼叫建立。如果网守在网络内部，可以在 H.323 终端之间启用呼叫建立。使用此选项可根据 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息为呼叫打开针孔。由于这些 RRQ/RCF 消息会进出网守，所以呼叫终端的 IP 地址未知且 ASA 会通过源 IP 地址/端口 0/0 打开针孔。默认情况下，此选项已禁用。
- **timeout users** *time* - 设置 H.323 呼叫持续时间限制（格式为 hh:mm:ss）。如果不想设置超时，请指定 00:00:00。超时范围是 0:0:0 到 1193:0:0。
- **call-party-number** - 在呼叫建立过程中强制发送主叫方号码。
- **h245-tunnel-block action** {**drop-connection** | **log**} - 强制阻止 H.245 隧道。指定是要断开连接还是仅记录连接。

- **rtp-conformance** [**enforce-payloadtype**] - 检查流经针孔的 RTP 数据包的协议符合性。可选的 enforce-payloadtype 关键字基于信令交换将负载类型限制为音频或视频。
- **state-checking** {**h225** | **ras**} - 启用状态检查验证。可以分别为 H.225 和 RAS 输入此命令来启用状态检查。
- **early-message** *message_type* - 是否允许指定类型的 H.225 消息在 H.225 SETUP 消息之前到达可以按照 H.460.18 允许 **facility** 消息提前到达。

  如果遇到呼叫建立问题（使用 H.323/H.225 时连接会在完成之前被关闭），请使用此命令允许消息提前到达。此外，请确保为 H.323 RAS 和 H.225 启用检测（默认情况下，它们处于启用状态）。

步骤 6 可以在仍处于参数配置模式下时配置 HSI 组。

a) 定义 HSI 组并进入 HSI 组配置模式：**hsi-group** *id*

   其中 *id* 为 HSI 组 ID。范围为 0 至 2147483647。

b) 使用以下 IP 地址向 HSI 组中添加 HSI：**hsi** *ip_address*

   每个 HSI 组最多可以添加 5 台主机。

c) 向 HSI 组中添加终端：**endpoint** *ip_address if_name*

   其中 *ip_address* 为要添加的终端，*if_name* 为终端连接到 ASA 使用的接口。每个 HSI 组最多可以添加 10 个终端。

示例

以下示例显示如何配置电话号码过滤：

```
hostname(config)# regex caller 1 “5551234567”
hostname(config)# regex caller 2 “5552345678”
hostname(config)# regex caller 3 “5553456789”

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅配置应用层协议检测。

MGCP 检测

MGCP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用这项检测。但是，默认检测类确实包括默认 MGCP 端口，因此，只需简单地编辑默认全局检测策略，即可添加 MGCP 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

以下各节介绍 MGCP 应用检测。

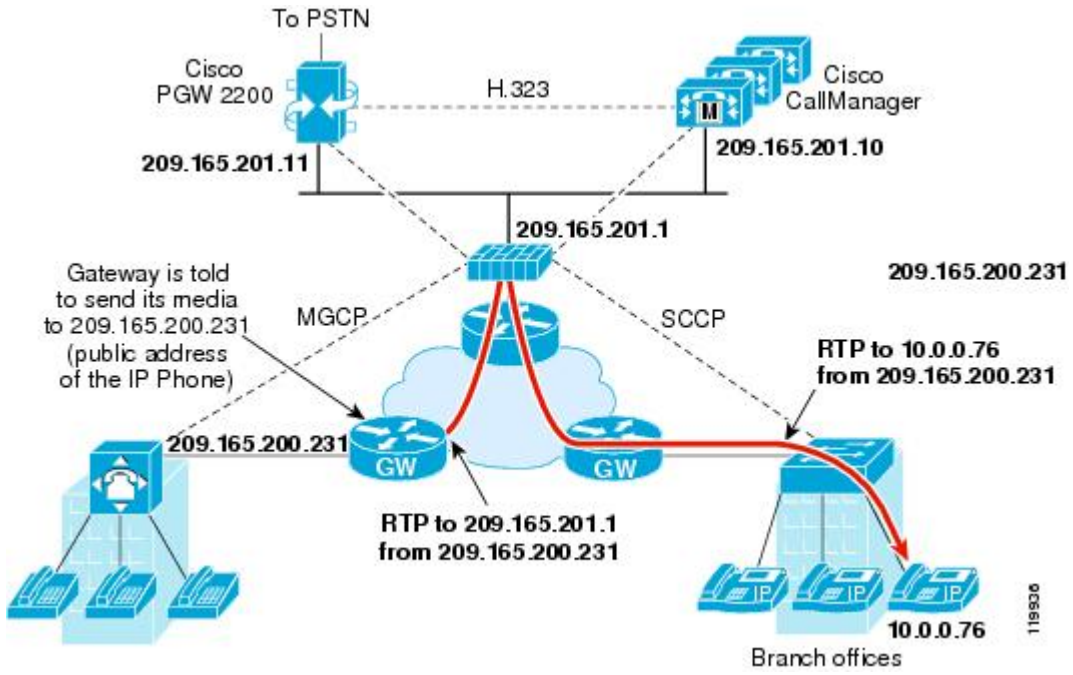
MGCP 检测概述

MGCP 用于控制来自称为媒体网关控制器或呼叫代理的外部呼叫控制元件的媒体网关。媒体网关通常是一个网络元素，用于在电话电路上传送的音频信号和互联网上或其他数据包网络上传送的数据包之间提供转换。借助具有 MGCP 的 NAT 和 PAT，可以使用一组有限的外部（全局）地址来支持内部网络中的大量设备。媒体网关示例如下：

- 中继网关：用于在电话网络和 IP 语音网络之间建立连接。这种网关通常管理大量的数字电路。
- 家庭网关：提供用于连接到 IP 语音网络的传统模拟 (RJ11) 接口。电缆调制解调器/电缆机顶盒、xDSL 设备、宽带无线设备都是家庭网关示例。
- 业务网关：提供用于连接到 IP 语音网络的传统数字 PBX 接口或集成软 PBX 接口。

MGCP 消息通过 UDP 传输。响应会发送回命令的源地址（IP 地址和 UDP 端口号），但响应可能不会到达收到命令的同一地址。如果在同一故障转移配置中使用多个呼叫代理，且接收命令的呼叫代理已经将控制转交给备用呼叫代理，由备用呼叫代理来发送响应，可能会发生这种情况。下图说明如何配合使用 NAT 与 MGCP。

图 *1:* 配合使用 ***NAT*** 与 ***MGCP***



MGCP 终端是数据的物理或虚拟源及目标。媒体网关包含终端，呼叫代理可以在这些终端上创建、修改和删除连接，从而建立并控制与其他多媒体终端之间的媒体会话。此外，呼叫代理可以指示终端检测某些事件和生成信号。终端会自动将服务状态变化情况告知呼叫代理。

- 网关通常会侦听 UDP 端口 2427 以接收来自呼叫代理的命令。
- 呼叫代理所在的端口接收来自网关的命令。呼叫代理通常会侦听 UDP 端口 2727 以接收来自网关的命令。

注释 MGCP 检测不支持对 MGCP 信令和 RTP 数据使用不同的 IP 地址。通常建议的做法是从弹性 IP 地址（例如回环或虚拟 IP 地址）发送 RTP 数据，但 ASA 要求 RTP 数据的发出地址与 MFCP 信令相同。

配置 MGCP 检测策略映射

如果网络中包含多个 ASA 必须为其打开针孔的呼叫代理和网关，请创建 MGCP 映射。然后，可以在启用 MGCP 检测时应用所创建的 MGCP 映射。

过程

步骤 1 创建 MGCP 检测策略映射：**policy-map type inspect mgcp** *policy_map_name*

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description** *string*

步骤 3 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

步骤 4 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项。

- **call-agent** *ip_address group_id* - 配置可以管理一个或多个网关的呼叫代理组。呼叫代理组信息用于为组内的呼叫代理打开连接（而不是只为网关向其发送命令的那个呼叫代理打开连接），以使任何呼叫代理都可以发送响应。具有相同 group_id 的呼叫代理属于同一个组。一个呼叫代理可以同时属于多个组。group_id 是一个编号，范围介于 0 到 4294967295 之间。ip_address 选项指定呼叫代理的 IP 地址。

  注释
  MGCP 呼叫代理发送 AUEP 消息，以确定 MGCP 终端是否存在。这样将通过 ASA 建立一个数据流，并允许 MGCP 终端注册到呼叫代理。

- **gateway** *ip_address group_id* - 标识哪个呼叫代理组在管理特定网关。使用 ip_address 选项指定网关的 IP 地址。group_id 选项是一个介于 0 到 4294967295 之间的编号，必须与管理网关的呼叫代理的 group_id 相对应。一个网关可能只属于一个组。
- **command-queue** *command_limit* - 设置 MGCP 命令队列允许的最大命令数，范围是 1 到 2147483647。默认值为 200。

示例

以下示例显示如何定义 MGCP 映射：

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅配置应用层协议检测。

RTSP 检测

默认情况下，RTSP检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。以下各节介绍 RTSP 应用检测。

RTSP 检测概述

RTSP 检测引擎允许 ASA 传送 RTSP 数据包。RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer 和思科 IP/TV 连接都使用 RTSP。

注释　对于思科 IP/TV，请使用 RTSP TCP 端口 554 和 8554。

RTSP 应用使用已知 TCP（很少用 UDP）端口 554 作为控制信道。根据 RFC 2326 要求，ASA 仅支持 TCP。该TCP控制信道用于根据客户端配置的传输模式协商用于传输音频/视频流量的数据信道。

支持如下 RDT 传输：rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp 和 x-pn-tng/udp。

ASA 使用状态代码 200 解析建立响应消息。如果响应消息要入站，服务器需相对于 ASA 处于外部，并需要为连接从服务器进入站内打开动态信道。如果响应消息要出站，则ASA无需打开动态信道。

RTSP 检测不支持 PAT 或双 NAT。另外，ASA 无法识别 HTTP 掩蔽，其中 RTSP 消息隐藏在 HTTP 消息中。

RealPlayer 配置要求

使用 RealPlayer 时，正确配置传输模式非常重要。对于 ASA，请将 **access-list** 命令从服务器添加到客户端，或者从客户端添加到服务器。对于 RealPlayer，依次点击 **Options**>**Preferences**>**Transport**>**RTSP Settings** 更改传输模式。

如果 RealPlayer 使用 TCP 模式，请选择 **Use TCP to Connect to Server** 和 **Attempt to use TCP for all content** 复选框。在 ASA 上无需配置检测引擎。

如果在 RealPlayer 上使用 UDP 模式，请勾选 **Use TCP to Connect to Server** 和 **Attempt to use UDP for static content** 复选框；对于无法通过组播获得的实时内容，也请勾选上述复选框。在 ASA 中添加 **inspect rtsp** 命令。

RSTP 检测的局限性

RSTP 检测有以下局限性。

- ASA 不支持通过 UDP 的组播 RTSP 或 RTSP 消息。
- ASA 无法识别 RTSP 消息隐藏在 HTTP 消息中的 HTTP 掩蔽技术。

- ASA 无法对 RTSP 消息执行 NAT，因为嵌入式 IP 地址作为 HTTP 或 RTSP 消息的一部分包含在 SDP 文件中。数据包可以分段，但 ASA 无法对分段的数据包执行 NAT。
- 对于思科 IP/TV，ASA 对消息 SDP 部分可执行的转换数与内容管理器中的程序列表数呈正比（每个程序列表至少可包含六个嵌入式 IP 地址）。
- 可以为 Apple QuickTime 4 或 RealPlayer 配置 NAT。如果查看器和内容管理器位于外部网络，而服务器位于内部网络，则思科 IP/TV 只能采用 NAT。

配置 RTSP 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 RTSP 检测策略映射来自定义 RTSP 检测操作。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 （可选）执行以下步骤创建 RTSP 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect rtsp** [**match-all** | **match-any**] *class_map_name*

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定如果流量匹配至少一个条件，则匹配类映射。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

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

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **request-method** *method* - 匹配 RTSP 请求方法。这些方法包括：announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameter、teardown。

- **match** [**not**] **url-filter regex** {*regex_name* | **class** *class_name*} - 将 URL 与指定的正则表达式或正则表达式类进行匹配。

步骤 2 要创建 RTSP 检测策略映射：**policy-map type inspect rtsp** *policy_map_name*

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description** *string*

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 RTSP 类映射，请输入以下命令对其进行指定：**class** *class_map_name*
- 要直接在策略映射中指定流量，请对 RTSP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop-connection** [**log**] - 丢弃数据包，关闭连接，并选择性地发送系统日志消息。此选项适用于 URL 匹配。
- **log** - 发送系统日志消息。
- **rate-limit** *message_rate* - 限制每秒发生消息的速率。此选项适用于请求方法匹配。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅如何处理多个流量类。

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **reserve-port-protect** - 在媒体协商期间限制保留端口的使用。
- **url-length-limit** *bytes* - 设置消息中使用的 URL 的长度限制（0 到 6000 字节）。

示例

以下示例显示如何定义 RTSP 检测策略映射。

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp
```

```
hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global
```

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅配置应用层协议检测。

SIP 检测

SIP是一种广泛用于网络会议、电话、展示、事件通知和即时消息的协议。部分原因是SIP本质上是文本协议，部分原因是其具有灵活性，因此，SIP 网络面临大量安全威胁。

SIP 应用检测会在消息信头和正文中提供地址转换，会动态打开端口，还会执行基本健全性检查。SIP应用检测还支持应用安全和协议符合性（此功能强制对SIP消息进行健全性检查，以及检测基于 SIP 的攻击）。

默认情况下，SIP 检测已启用。只有需要非默认处理时，或者要标识 TLS 代理来启用加密流量检测时，才需要配置这项检测。以下主题详细说明 SIP 检测。

SIP 检测概述

如 IETF 所定义，SIP 能够实现呼叫处理会话，特别是双方音频会议（又称为“通话”）。SIP 可与 SDP 配合使用来实现呼叫信令。SDP 指定用于媒体流的端口。使用 SIP，ASA 可支持任何 SIP VoIP 网关和 VoIP 代理服务器。SIP 和 SDP 在以下 RFC 中定义：

- SIP：会话初始协议，RFC 3261
- SDP：会话描述协议，RFC 2327

为了支持 SIP 呼叫通过 ASA，必须检测媒体连接地址、媒体端口和媒体初期连接的信令消息，因为在已知目标端口 (UDP/TCP 5060) 上发送信令时，系统会动态分配媒体流。此外，SIP 还会在 IP 数据包的用户数据部分嵌入 IP 地址。请注意，ASA 支持的最大 SIP 请求 URI 长度为 255。

即时消息 (IM) 应用也使用 SIP 扩展（定义见 RFC 3428）和 SIP 特定的事件通知 (RFC 3265)。用户发起聊天会话（注册/订用）之后，当用户相互聊天时，IM 应用会使用 MESSAGE/INFO 方法和 202

Accept 响应。例如，两个用户可以随时在线，但几个小时都不聊天。因此，SIP 检测引擎会根据配置的 SIP 超时值打开超时的针孔。该值必须配置为比订用持续时间至少长 5 分钟。订用持续时间在 Contact Expires 值中定义，通常是 30 分钟。

由于 MESSAGE/INFO 请求通常使用动态分配的端口（而不是端口 5060）发送，因此，这些请求必须通过 SIP 检测引擎。

注释 SIP 检测仅支持聊天功能。不支持白板、文件传输和应用共享。不支持 RTC Client 5.0。

SIP 检查的限制

SIP 检测已经过测试，受思科统一通信管理器 (CUCM) 7.0、8.0、8.6 和 10.5 支持。CUCM 8.5 或 9.x 不支持这项检测。SIP 检测可能适用于其他版本和产品。

如果发现 SIP 电话无法连接到呼叫管理器，可以尝试使用以下命令在 CLI 中增加未处理 TCP 网段的最大数量：**sysopt connection tcp-max-unprocessed-seg** *6-24*。默认值为 6，请尝试更高的值。

SIP 检查不支持 T.38 MIME 互联网传真协议 (IFP)。SIP 检测会放弃使用 T.38 MIME 音频子类型的 SIP 邀请。如果需要允许这种类型，请禁用 SIP 检测并编写允许 RTP 流的访问控制规则。

SIP 检测的 NAT 限制

- SIP 检测适用于嵌入式 IP 地址的 NAT。但是，如果配置 NAT 来转换源地址和目标地址，将不会重写外部地址（“trying”响应消息的 SIP 报头中的“from”）。因此，在处理 SIP 流量时应使用对象 NAT，从而避免转换目标地址。
- 请勿为安全级别相同、较低（源）或较高（目标）的接口配置 NAT 或 PAT。不支持此配置。
- 如果为目标流量类（即非 inspection_default 流量类）配置 SIP 检测，请确保使用双向 ACL，并仅指定 5060 目的地端口。否则，您可能会遇到 NAT 问题，即使 IP 数据包已正确转换，但 SIP 报头中的 IP 地址仍无法转换。
- 如果在 SIP 邀请的 VIA 标头中硬编码映射地址，则不要启用 SIP 检测。如果使用静态 NAT 转换客户端源地址，而默认路由的接口与客户端使用的连接路由的接口不同，就会出现问题。

SIP 检测的 PAT 限制

当与 SIP 结合使用 PAT 时，有以下限制和限定：

- 如果远程终端尝试在 ASA 保护的网络上注册 SIP 代理，在非常特殊的条件下注册会失败，如下所示：
  - 对远程终端配置了 PAT。
  - SIP 注册服务器位于外部网络。
  - 在终端发送给代理服务器的 REGISTER 消息中，联系人字段中的端口缺失。

- 如果在 SIP 设备传输数据包时，该数据包的 SDP 部分的所有者/创建者字段 (o=) 中的 IP 地址与连接字段 (c=) 中的 IP 地址不同，则可能未正确转换 o= 字段中的 IP 地址。这是 SIP 协议的如下局限性造成的：不在 o= 字段中提供端口值。由于 PAT 需要使用端口进行转换，所以转换会失败。
- 使用 PAT 时，任何包含无端口的内部 IP 地址的 SIP 报头字段都可能不会转换，因此，内部 IP 地址将向外泄漏。如果要避免这种泄漏，请配置 NAT 来代替 PAT。

默认 SIP 检测

默认情况下，SIP 检测已通过默认检测映射启用，具体以下：

- SIP 即时消息 (IM) 扩展：已启用。
- SIP 端口的非 SIP 流量：丢弃 (Dropped)。
- 隐藏服务器和终端的 IP 地址：已禁用。
- 掩蔽软件版本和非 SIP URI：已禁用。
- 确保到目标的跳数大于 0：已启用。
- RTP 符合性：未执行。
- SIP 符合性：不执行状态检查和报头验证。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

配置 SIP 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 SIP 检测策略映射来自定义 SIP 检测操作。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 （可选）执行以下步骤创建 SIP 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect sip** [**match-all** | **match-any**] *class_map_name*

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。match-any 关键字指定只要流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

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

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*} - 将 To 报头中指定的被叫方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*} - 将 From 报头中指定的主叫方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **content length gt** *bytes* - 匹配在 SIP 报头中的内容长度大于指定字节数（0 到 65536）的消息。
- **match** [**not**] **content type** {**sdp** | **regex** {*regex_name* | **class** *class_name*} - 将内容类型匹配为 SDP 或者与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **im-subscriber regex** {*regex_name* | **class** *class_name*} - 将 SIP IM 用户与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **message-path regex** {*regex_name* | **class** *class_name*} - 将 SIP Via 报头与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **request-method** *method* - 匹配 SIP 请求方法：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- **match** [**not**] **third-party-registration regex** {*regex_name* | **class** *class_name*} - 将第三方注册的请求方与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **uri {sip | tel} length gt** *bytes* - 匹配长度大于指定长度（0 到 65536 字节）的选定类型（SIP 或 TEL）的 SIP 报头 URI。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 SIP 检测策略映射：**policy-map type inspect sip** *policy_map_name*

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description** *string*

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 SIP 类映射，请输入以下命令对其进行指定：**class** *class_map_name*

- 要直接在策略映射中指定流量，请对 SIP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop** - 丢弃匹配的所有数据包。
- **drop-connection** - 丢弃数据包并关闭连接。
- **reset** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。
- **log** - 发送系统日志消息。您可以单独使用此选项，也可以与其他某项操作一起使用。
- **rate-limit** *message_rate* - 限制发出消息的速率。速率限制仅适用于匹配“invite”和“register”的请求方法。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅如何处理多个流量类。

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **im** - 启用即时消息。
- **ip-address-privacy** - 启用 IP 地址隐私（即，隐藏服务器和终端的 IP 地址）。
- **max-forwards-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**] - 检查 Max-Forwards 报头值（在到达目标之前，此值不能为 0）。必须选择要对不符合要求的流量执行的操作（丢弃数据包、断开连接、重置连接或记录连接）以及是启用还是禁用日志记录。
- **rtp-conformance** [**enforce-payloadtype**] - 检查流经针孔的 RTP 数据包的协议符合性。可选的 enforce-payloadtype 关键字基于信令交换将负载类型限制为音频或视频。
- **software-version action** {**mask** [**log**] | **log**} - 使用 Server 和 User-Agent（终端）报头字段标识软件版本。可以在 SIP 消息中掩蔽软件版本以及（可选）进行有关记录，或者仅进行有关记录。
- **state-checking action** {**drop** | **drop-connection** | **reset** | **log**} [**log**] - 启用状态转换检查。必须选择要对不符合要求的流量执行的操作（丢弃数据包、断开连接、重置连接或记录连接）以及是启用还是禁用日志记录。
- **strict-header-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**] - 根据 RFC 3261 对 SIP 消息中的报头字段启用严格验证。必须选择要对不符合要求的流量执行的操作（丢弃数据包、断开连接、重置连接或记录连接）以及是启用还是禁用日志记录。
- **traffic-non-sip** - 允许已知 SIP 信令端口上出现非 SIP 流量。

- **trust-verification-server ip** *ip_address* - 标识信任验证服务服务器（这些服务器使思科统一 IP 电话在 HTTPS 建立过程中可以对应用服务器进行身份验证）。最多可以输入命令四次来标识四台服务器。SIP 检测会为每个已注册的电话打开用于连接到每台服务器的针孔，由电话确定使用哪个针孔。可在 CUCM 服务器上配置信任验证服务服务器。
- **trust-verification-server port** *number* - 标识信任验证服务端口。默认端口是 2445，因此，请仅在服务器使用其他端口的情况下使用此命令。允许的端口范围是 1026 到 32768。
- **uri-non-sip action** {**mask [log]** | **log**} - 标识在 Alert-Info 和 Call-Info 报头字段中出现的非 SIP URI。可以在 SIP 消息中掩蔽这部分信息以及（可选）进行有关记录，或者仅进行有关记录。

示例

以下示例显示如何禁用采用 SIP 的即时消息：

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

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

以下示例显示如何标识四个信任验证服务服务器。

```
hostname(config)# policy-map type inspect sip sample_sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.1
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.2
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.3
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.4
hostname(config-pmap-p)# trust-verification-server port 2445
```

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅配置应用层协议检测。

瘦客户端 (SCCP) 检测

SCCP（瘦客户端）应用检测对数据包数据中的嵌入式 IP 地址和端口号执行转换，并会动态打开针孔。它还执行其他协议符合性检查和基本状态跟踪。

默认情况下，SCCP 检测已启用。只有需要非默认处理时，或者要标识 TLS 代理来启用加密流量检测时，才需要配置这项检测。

以下各节介绍 SCCP 应用检测。

SCCP 检测概述

瘦客户端 (SCCP) 是用于 VoIP 网络的简化协议。使用 SCCP 的思科 IP 电话可共存于 H.323 环境中。与 Cisco CallManager 一起使用时，SCCP 客户端可以与兼容 H.323 的终端进行互操作。

对于 SCCP，ASA 支持 PAT 和 NAT。如果要使用的 IP 电话多于 IP 电话可使用的全局 IP 地址，必须进行 PAT。通过支持 SCCP 信令数据包的 NAT 和 PAT，瘦应用检测可确保所有 SCCP 信令和媒体数据包均可通过 ASA。

Cisco CallManager 与思科 IP 电话之间的正常流量使用 SCCP，这些流量由 SCCP 检测处理，无需任何特殊配置。另外，ASA 还支持 DHCP 选项 150 和 66，将 TFTP 服务器的位置发送到思科 IP 电话及其他 DHCP 客户端即可完成操作。思科 IP 电话可能在请求中还包含 DHCP 选项 3（该选项用于设置默认路由）。

注释 ASA 支持检测来自运行 SCCP 协议版本 22 及更早版本的思科 IP 电话的流量。

支持思科 IP 电话

在思科 CallManager 位于思科 IP 电话较高安全性接口的拓扑中，如果需要对思科 CallManager IP 地址执行 NAT，则映射必须为静态，因为思科 IP 电话需要在其配置中显式指定思科 CallManager IP 地址。静态身份条目允许安全性较高的接口中的思科 CallManager 接受来自思科 IP 电话的注册。

思科 IP 电话需要访问 TFTP 服务器，以下载它们连接到 Cisco CallManager 服务器所需要的配置信息。

当思科 IP 电话位于比 TFTP 服务器低的安全接口上时，必须使用 ACL 来与 UDP 端口 69 上的受保护 TFTP 服务器连接。虽然需要对 TFTP 服务器使用静态条目，但该静态条目不一定必须是身份静态条目。使用 NAT 时，身份静态条目会映射到同一 IP 地址。使用 PAT 时，它会映射到同一 IP 地址和端口。

当思科 IP 电话位于比 TFTP 服务器和思科 CallManager 安全性更高的接口上时，无需 ACL 或静态条目即可允许思科 IP 电话发起连接。

SCCP 检测的局限性

SCCP 检测已经过测试，受思科统一通信管理器 (CUCM) 7.0、8.0、8.6 和 10.5 支持。CUCM 8.5 或 9.x 不支持这项检测。SCCP 检测可能适用于其他版本和产品。

如果为 NAT 或 PAT 配置的内部思科 CallManager 的地址为不同的 IP 地址或端口，则注册外部思科 IP 电话将会失败，因为 ASA 对于通过 TFTP 传输的文件内容不支持 NAT 或 PAT。虽然 ASA 支持 TFTP 消息的 NAT 并会为 TFTP 文件打开针孔，但在电话注册期间，ASA 无法转换通过 TFTP 传输的思科 IP 电话配置文件中嵌入的思科 CallManager IP 地址和端口。

注释 ASA 支持 SCCP 呼叫的状态故障转移，但呼叫建立过程中的呼叫除外。

默认 SCCP 检测

默认情况下，SCCP 检测已启用，默认设置如下：

- 注册：未执行。
- 最大消息 ID：0x181。
- 最小前缀长度：4
- 媒体超时：00:05:00
- 信令超时：01:00:00。
- RTP 符合性：未执行。

配置瘦小客户端 (SCCP) 检测策略映射

要指定消息违反参数时要执行的操作，请创建 SCCP 检测策略映射。然后，可以在启用 SCCP 检测时应用所创建的检测策略映射。

过程

步骤 1 创建 SCCP 检测策略映射：**policy-map type inspect skinny** *policy_map_name*

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description** *string*

步骤 3 （可选）根据 SCCP 消息的站消息 ID 字段丢弃流量。

a) 根据十六进制的站消息 ID 值（0x0 到 0xffff）标识流量。使用 **match** [**not**] **message-id** 命令可以指定单个 ID 或 ID 范围。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

match message-id {*value* | **range** *start_value end_value*}

示例：

```
hostname(config-pmap)# match message-id 0x181
hostname(config-pmap)# match message-id range 0x200 0xffff
```

b) 指定要对匹配的数据包执行的操作。可以丢弃数据包和或者记录数据包：**drop** [**log**]

c) 重复以上步骤，直至标识出所有要丢弃的消息 ID。

步骤 4 配置影响检测引擎的参数。

a) 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **enforce-registration** - 要求必须进行注册才能发出呼叫。
- **message-ID max** *hex_value* - 设置允许的 SCCP 站消息 ID 的最大值。消息 ID 采用十六进制，默认最大值是 0x181。
- **rtp-conformance** [**enforce-payloadtype**] - 检查流经针孔的 RTP 数据包的协议符合性。可选的 enforce-payloadtype 关键字基于信令交换将负载类型限制为音频或视频。
- **sccp-prefix-len** {**max** | **min**} *length* - 设置允许的最大或最小 SCCP 前缀长度值。请输入此命令两次，以设置最小值和最大值。默认最小值是 4，没有默认最大值。
- **timeout** {**media** | **signaling**} *time* - 为媒体和信令连接设置超时（格式为 hh:mm:ss）。如果不想设置超时，请指定数字 0。默认的媒体超时是 5 分钟，默认的信令超时是 1 小时。

示例

以下示例显示如何定义 SCCP 检测策略映射。

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅配置应用层协议检测。

STUN 检测

WebRTC 客户端使用 RFC 5389 中定义的 NAT 会话穿越工具 (STUN) 进行基于浏览器的实时通信，因而不需要插件。WebRTC 客户端通常使用云 STUN 服务器获悉它们的公共 IP 地址和端口。WebRTC 使用交互式连接建立（ICE，RFC 5245）来验证客户端之间的连接。虽然这些客户端可以使用 TCP 或其他协议，但它们通常使用 UDP。

由于防火墙通常会阻止传出 UDP 流量，所以思科 Spark 等 WebRTC 产品在完成连接时可能会遇到问题。如果两端已确认连接检查，STUN 检测可为 STUN 终端打开针孔并实现基本的 STUN 和 ICE 合规，以便允许进行客户端通信。由此，可避免在访问规则中开放新端口来启用这些应用。

对于默认检测类启用 STUN 检测时，系统会监视 TCP/UDP 端口 3478 中的 STUN 流量。该检测仅支持 IPv4 地址和 TCP/UDP。

STUN 检测在 NAT 方面存在一些局限性。对于 WebRTC 流量，支持静态 NAT/PAT44。由于思科 Spark 不需要针孔，所以 Spark 可以支持其他类型的 NAT。另外，您还可以为思科 Spark 使用 NAT/PAT64，包括动态 NAT/PAT。

故障转移和集群模式支持 STUN 检查，因为针孔被复制。但是，节点之间不进行事务 ID 的复制。如果节点在收到 STUN 请求后发生故障，并且另一个节点收到 STUN 响应，则该 STUN 响应将被丢弃。

注释 STUN 检查使用事务 ID 来匹配请求和响应。如果使用调试来排除连接丢包，请注意，系统会更改调试输出的 ID 格式（字节序），因此它们与 pcap 中的 ID 无法直接比较。

有关启用 STUN 检测的信息，请参阅配置应用层协议检测。

语音和视频协议检测的历史记录

功能名称	版本	功能信息
对 IPv6 的 SIP、SCCP 和 TLS 代理支持	9.3(1)	现在使用 SIP、SCCP 和 TLS 代理（使用 SIP 或 SCCP）时可检查 IPv6 流量。 未修改任何命令。
适用于信任验证服务、NAT66、CUCM 10.5 和 8831 型号电话的 SIP 支持。	9.3(2)	现在，可以在 SIP 检测中配置信任验证服务服务器。还可以使用 NAT66。使用 CUCM 10.5 对 SIP 检测进行了测试。 添加了 **trust-verification-server** 参数命令。
改进了多核心 ASA 上的 SIP 检测性能。	9.4(1)	如果有多条 SIP 信令流通过多核 ASA，表明 SIP 检查性能已经改进。但是，如果您使用的是 TLS、电话或 IME 代理，则不会看到性能改进。 未修改任何命令。
ASA 集群中的 SIP 检查支持	9.4(1)	您现在可以在 ASA 集群上配置 SIP 检查。控制流可以在任何设备上创建（由于负载均衡），但其子数据流必须驻留在同一设备上。不支持 TLS 代理配置。 引入了以下命令：**show cluster service-policy**。
取消了对电话代理和 UC-IME 代理的 SIP 检查支持。	9.4(1)	配置 SIP 检查后，将无法再使用电话代理或 UC-IME 代理。使用 TLS 代理检查加密流量。 删除了以下命令：**phone-proxy** 和 **uc-ime**。从 **inspect sip** 命令中删除了 **phone-proxy** 和 **uc-ime** 关键字。

功能名称	版本	功能信息
H.323 检测支持 H.255 FACILITY 消息先于 H.460.18 兼容性的 H.225 SETUP 消息到达。	9.6(1)	现在，当终端符合 H.460.18 的要求时，可将 H.323 检查策略映射配置为允许在 H.225 SETUP 消息之前发出 H.225 FACILITY 消息。 引入了以下命令：**early-message**
NAT 会话穿透工具 (STUN) 检测。	9.6(2)	现在，您可以检测 WebRTC 应用程序的 STUN 流量，包括思科 Spark。检测会打开返回流量所需的针孔。 添加或修改了以下命令：**inspect stun**、 **show asp drop**、**show conn detail**、**show service-policy inspect stun**。
在 TLS 代理和思科统一通信管理器 10.5.2 中支持 TLSv1.2。	9.7(1)	现在，您可以将包含 TLS 代理的 TLSv1.2 与思科 Unified Communications Manager 10.5.2 一起用于加密 SIP 或 SCCP 检查。TLS 代理支持作为 **client cipher-suite** 命令的一部分添加的附加 TLSv1.2 密码套件。 修改了以下命令：**client cipher-suite**。
已弃用用于 SCCP （Skinny）检测的 TLS 代理。	9.13(1)	已弃用 **tls-proxy** 关键字以及对 SCCP/Skinny 加密检测的支持。在未来版本中，将从 **inspect skinny** 命令中删除该关键字。
SCCP (Skinny) 检查取消了 TLS 代理支持。	9.14(1)	已删除 **tls-proxy** 关键字，以及对 SCCP/Skinny 加密检测的支持。
默认 SIP 检测策略映射会丢弃非 SIP 流量。	9.16（1）	对于 SIP 检查的流量，现在默认为丢弃非 SIP 流量。以前的默认设置是允许在检查 SIP 的端口上允许非 SIP 流量。 我们更改了默认 SIP 策略映射以包含 **no traffic-non-sip** 命令。

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。