移动网络检测

以下主题介绍用于 LTE 等移动网络协议的应用检测。这些检测需要使用 Carrier 许可证。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信息，请参阅应用层协议检测入门。

移动网络检测概述

以下主题介绍可用于 LTE 等移动网络协议的检测。除检测之外，还有可用于 SCTP 流量的其他服务。

GTP 检测概述

GPRS 隧道协议用于 GSM、UMTS 和 LTE 网络的通用分组无线服务 (GPRS) 流量。GTP 提供隧道控制和管理协议，通过创建、修改和删除隧道来为移动站提供 GPRS 网络接入。此外，GTP 还使用隧道机制来传送用户数据包。

服务提供商网络使用 GTP 通过终端之间的 GPRS 主干隧道传输多协议数据包。在 GTPv0-1 中，GTP 用于网关 GPRS 支持节点 (GGSN) 和服务 GPRS 支持节点 (SGSN) 之间的信令。在 GTPv2 中，信令位于数据包数据网络网关 (PGW) 和服务网关 (SGW) 以及其他终端之间。GGSN/PGW 是 GPRS 无线数据网络与其他网络之间的接口。SGSN/SGW 可执行移动、数据会话管理和数据压缩。

您可以使用 ASA 来防御欺诈漫游的合作伙伴。将设备放在主 GGSN/PGW 和被访问的 SGSN/SGW 终端之间，并对流量应用 GTP 检测。GTP 检测仅可在这些终端之间的流量上运行。在 GTPv2 中，这称为 S5/S8 接口。

GTP 和相关标准由 3GPP（第 3 代合作伙伴项目）定义。有关详细信息，请参阅 http://www.3gpp.org。

跟踪移动站位置更改

可以使用 GTP 检测跟踪移动站位置更改。跟踪位置更改可能会帮助您识别欺诈漫游费用，例如，如果您看到移动站在不太可能的时间断内从一个位置移至另一个位置，例如在 30 分钟内从美国的一个小区移至欧洲的一个小区。

当您启用位置日志记录时，系统会生成每个国际移动用户身份 (IMSI) 新建或更改后位置的系统日志消息。

- 324010 表示创建新的 PDP 上下文，包括移动国家代码 (MCC)、移动网络代码 (MNC)、信息元素，以及可选的用户当前注册的小区 ID。单元 ID 从单元全局标识 (CGI) 或 E-UTRAN 单元全局标识符 (ECGI) 中提取。
- 324011 指示 IMSI 已从 PDP 情景创建过程中存储的位置移开。此消息显示上一个和当前的 MCC/MNC、信息元素以及可选的单元 ID。

默认情况下，系统日志消息不包含时间戳信息。如果您计划分析这些消息来识别不太可能漫游时，还必须启用时间戳。时间戳日志记录不作为 GTP 检测映射的一部分。使用 **logging timestamp** 命令。

有关启用位置日志记录的信息，请参阅 配置 GTP 检测策略映射 ， 第 9 页。

GTP 检测的局限性

以下是 GTP 检测的一些局限性：

- 不支持 GTPv2 捎带消息。它们始终会被丢弃。
- 仅在包含 IMSI（国际移动用户识别码）时支持 GTPv2 紧急 UE 连接。
- GTP 检测不检查早期数据。即恰好在创建会话请求之后但在创建会话响应之前从 PGW 或 SGW 发送的数据。
- 对于 GTPv2，检测最高支持 3GPP 29.274 V15.5.0。对于 GTPv1，最高支持 3GPP 29.060 V15.2.0。对于 GTPv0，最高支持版本 8。
- GTP 检测不支持 Inter SGSN 切换到辅助 PDP 情景。检测需要对主 PDP 情景和辅助 PDP 情景执行交接。
- 启用 GTP 检测后，使用 GTP-in-GTP 封装的连接始终会被丢弃。

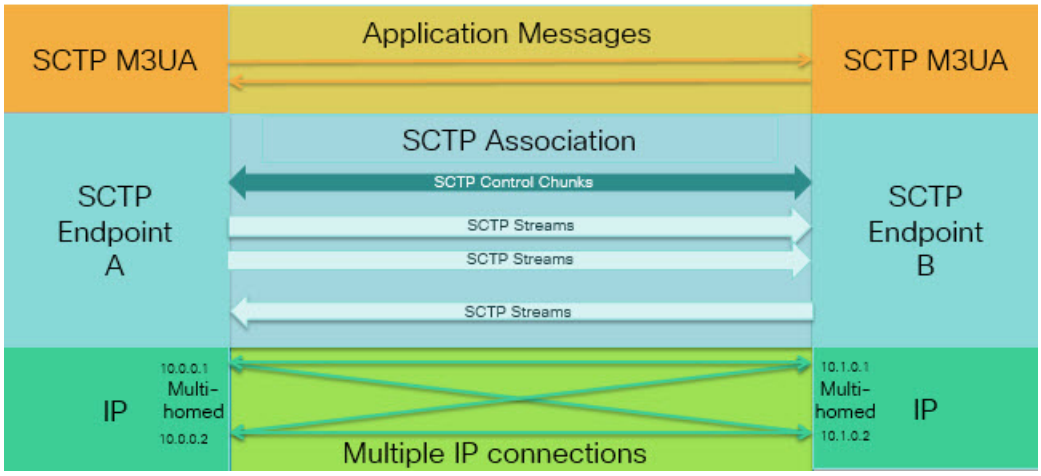
流控制传输协议 (SCTP) 检测和访问控制

RFC 4960 中介绍了 SCTP（流控制传输协议）。该协议支持基于 IP 的电话信令协议 SS7，也是适用于 4G LTE 移动网络架构中多个接口的传输协议。

SCTP 是在协议栈中基于 IP 运行的传输层协议，与 TCP 和 UDP 类似。但是，SCTP 可在基于一个或多个源或目标 IP 地址的两个终端节点之间创建一条逻辑通信通道，称为“关联”。这种行为称为多宿主。关联可在每个节点上定义一组 IP 地址（源和目标）和一个端口。该组中的任何 IP 地址均可作为与此关联相关的数据包的源或目标 IP 地址，从而形成多个连接。在每个连接中，可能存在多个发送消息的流。SCTP 中的流表示逻辑应用数据信道。

下图说明了关联与其流之间的关系。

图 *1: SCTP* 关联与流之间的关系



如果有SCTP流量通过ASA，您可以基于SCTP端口控制访问，并实施应用层检测来启用连接和（可选）过滤负载协议 ID，以便选择性地丢弃应用、记录应用或限制应用速率。

注释 每个节点最多可包含三个IP地址。超过三个这一上限的任何地址都将被忽略，不会包含到关联中。此时，辅助 IP 地址的针孔会自动打开。您无需写入访问控制规则来启用它们。

以下部分更加详细地介绍可用于 SCTP 流量的服务。

SCTP 状态检测

SCTP 流量与 TCP 类似，由系统在第 4 层自动检测以确保流量的结构良好并符合具有限制性的 RFC 4960 实施要求。检测和实施以下协议元素：

- 数据块类型、标志和长度。
- 验证标志。
- 源端口和目标端口，以防止关联重定向攻击。
- 执行 ping 操作时没有任何问题。

SCTP 状态检测根据关联状态接受或拒绝数据包：

- 验证初始关联建立的 4 向打开和关闭序列。
- 验证关联和数据流内的 TSN 转发进阶。
- 当由于心跳故障看到 ABORT 数据库时终止关联。SCTP 终端可能发送 ABORT 数据块来响应炸弹攻击。

如果确定不希望执行这些实施检查，可以为特定流量类配置 SCTP 状态绕行，如配置特定流量类的连接设置（所有服务）中所述。

SCTP 访问控制

您可以为 SCTP 流量创建访问规则。这些规则与基于 TCP/UDP 端口的规则类似，您只需使用 **sctp** 作为协议，端口号为 SCTP 端口。您可以为 SCTP 创建服务对象或组，或者直接指定端口。请参阅以下主题。

- 配置服务对象和服务组
- 添加扩展 ACE 以执行基于端口的匹配

SCTP NAT

您可以向 SCTP 关联建立消息中的地址应用静态网络对象 NAT。虽然您可以配置静态两次 NAT，但不建议这样做，因为 SCTP 关联的目的地部分的拓扑未知。不能使用动态 NAT/PAT。

SCTP 的 NAT 依赖于 SCTP 状态检测，而不是 SCTP 应用层检测。因此，如果配置了 SCTP 状态绕行，则无法对流量应用 NAT。

SCTP 应用层检测

通过在 SCTP 应用上启用 SCTP 检测和过滤，可以进一步优化您的访问规则。您可以根据负载协议标识符 (PPID)，选择性地丢弃、记录或按速率限制 SCTP 流量类。

如果决定对 PPID 进行过滤，请记住以下几点：

- PPID 位于数据分块中，特定数据包可包含多个数据分块，甚至包含一个控制数据块。如果数据包包含一个控制数据块或多个数据分块，即便对其分配的操作为丢弃，该数据包也不会被丢弃。
- 如果使用 PPID 过滤来丢弃数据包或限制数据包速率，请注意发射器会重新发送被丢弃的任何数据包。虽然下次尝试时可能会让 PPID 速率受限制的数据包通过，但 PPID 丢弃的数据包仍会被丢弃。您可能需要评估网络中反复出现这些丢弃所带来的最终结果。

SCTP 的局限性

SCTP 支持包括以下局限性。

- 每个节点最多可包含三个 IP 地址。超过三个这一上限的任何地址都将被忽略，不会包含到关联中。此时，辅助 IP 地址的针孔会自动打开。您无需写入访问控制规则来启用它们。
- 未使用的针孔将在 5 分钟后超时。
- 不支持多宿主终端上的双堆栈 IPv4 和 IPv6 地址。
- 唯一支持的 NAT 类型是网络对象静态 NAT。此外，不支持 NAT46 和 NAT64。
- 仅对 Diameter、M3UA 和基于 SCTP PPID 的检测处理的流量完成 SCTP 数据包分段和重组。
- 不支持 SCTP 中用于动态添加或删除 IP 地址的 ASCONF 数据块。

- 不支持 INIT 和 INIT-ACK SCTP 消息中的主机名参数，它们用于指定可被解析为 IP 地址的主机名。
- 无论是在ASA上还是在网络中的其他位置配置，SCTP/M3UA都不支持等价多路径路由(ECMP)。利用 ECMP，可通过多个最佳路径将数据包路由至目标。但是，对单一目标的 SCTP/M3UA 数据包响应必须返回到所退出的同一接口。即使该响应可能来自任何 M3UA 服务器，但它必须始终返回到所退出的同一接口。此问题的症状是，SCTP INIT-ACK 数据包被丢弃，您可以在 **show asp drop flow sctp-chunk-init-timeout** 计数器中进行查看：

```
Flow drop:
SCTP INIT timed out (not receiving INIT ACK)(sctp-chunk-init-timeout)
```

  如果您遇到此问题，可通过配置到 M3UA 服务器的静态路由，或通过配置基于策略的路由来实施能够确保该 INIT-ACK 数据包经过与 INIT 数据包相同的接口的网络设计，从而解决此问题。

Diameter 检测

Diameter 是用于下一代移动和固定电信网络（例如用于 LTE（长期演进）和 IMS（多媒体子系统）的 EPS（演进的数据包系统）的身份验证、授权和记账 (AAA) 协议。在这些网络中，该协议将取代 RADIUS 和 TACACS。

Diameter 使用 TCP 和 SCTP 作为传输层，并使用 TCP/TLS 和 SCTP/DTLS 保障通信安全。另外，它也可以选择性地提供数据对象加密。有关 Diameter 的详细信息，请参阅 RFC 6733。

Diameter应用执行服务管理任务，例如决定用户权限、服务授权、服务质量和收费率。虽然Diameter应用可出现在 LTE 架构的许多不同控制面板接口上，但 ASA 仅检测以下接口的 Diameter 命令编码和属性-值对 (AVP)：

- S6a：移动管理实体 (MME) - 家庭订用服务(HSS)。
- S9：PDN 网关 (PDG) - 3GPP AAA 代理/服务器。
- Rx：策略收费规则功能 (PCRF) - 呼叫会话控制功能 (CSCF)。

Diameter检测为 Diameter终端打开针孔，以允许通信。该检测支持 3GPP 版本 12，并符合 RFC 6733 要求。您可以将其用于 TCP/TLS（通过在启用检测时指定 TLS 代理），但不能将其用于 SCTP。使用 Ipsec 可保障 SCTP Diameter 会话的安全。

您可以选择性地使用 Diameter 检测策略映射根据应用 ID、命令代码和 AVP 来过滤流量，以便应用特殊操作，例如丢弃数据包或连接或记录它们。可以为新注册的Diameter应用创建自定义 AVP。通过过滤，可以优化您在网络上允许的流量。

注释 默认情况下，允许其他接口上运行的应用的 Diameter 消息通过。虽然无法基于这些不支持应用的命令代码或 AVP 指定操作，但您可以配置 Diameter 检测策略映射，根据应用 ID 丢弃这些应用。

M3UA 检测

MTP3 User Adaptation (M3UA) 是客户端/服务器协议，为基于 IP 的应用提供连接 SS7 网络的网关，以便连接 SS7 消息传递部分 3 (MTP3) 层。使用 M3UA，可以通过 IP 网络运行 SS7 用户部分（例如 ISUP）。M3UA 在 RFC 4666 中定义。

M3UA 使用 SCTP 作为传输层。默认端口为 SCTP 端口 2905。

MTP3 层提供网络功能，例如路由和节点寻址，但使用点代码来识别节点。M3UA 层可交换源点码 (OPC) 和目标点码 (DPC)。这与 IP 使用 IP 地址识别节点的方式类似。

M3UA 检测提供的协议符合具有限制性。您可以选择性地地为特定消息实施严格应用服务器进程 (ASP) 状态检查和其他消息验证。如果要进行状态故障转移或在集群内操作，需要执行严格 ASP 状态检查。但是，严格 ASP 状态检查只能在覆盖模式下运行，如果在 Loadsharing 或广播模式下运行则不起作用（根据 RFC 4666）。该检测假设每个终端有一个且只有一个 ASP。

您可以基于点代码或服务指示符 (SI) 选择性地应用访问策略。此外，还可以基于消息类和类型应用速率限制。

M3UA 协议符合性

M3UA 检测提供以下具有限制性的协议执行。检测丢弃和记录不符合要求的数据包。

- 常见消息信头。检测验证常见信头中的所有字段。
  - 仅限版本 1。
  - 消息长度必须正确。
  - 禁止使用具有保留值的消息类型类。
  - 禁止在消息类内使用无效的消息 ID。
- 负载数据消息。
  - 对于特定类型只允许使用一个参数。
  - 禁止 SCTP 流 0 中存在数据消息。
- 以下消息中必须存在 Affected Point Code 字段，否则该消息将被丢弃：目标可用 (DAVA)、目标不可用 (DUNA)、目标状态审核 (DAUD)、信令拥塞 (SCON)、目标用户部分不可用 (DUPU)、目标受限 (DRST)。
- 如果为以下消息启用了消息标记验证，系统将检查和验证某些字段的内容。验证失败的消息将被丢弃。
  - 目标用户部分不可用 (DUPU) - User/Cause 字段必须存在，并且其中必须仅包含有效的原因和用户代码。
  - 错误 - 所有必填字段必须都存在，并且仅包含允许的值。每个错误消息都必须包含该错误代码的必填字段。
  - 通知 - 状态类型和状态信息字段必须仅包含允许的值。

- 如果启用了严格应用服务器进程 (ASP) 状态验证，系统将维护 M3UA 会话的 ASP 状态并基于验证结果允许或丢弃 ASP 消息。如果未启用严格 ASP 状态验证，系统将转发所有 ASP 消息而不进行检测。

M3UA 检测的局限性

以下是 M3UA 检测的一些局限性。

- 对于 M3UA 数据中嵌入的 IP 地址，不支持 NAT。
- M3UA 严格应用服务器进程 (ASP) 状态验证依赖于 SCTP 状态检测。不会对相同流量实施 SCTP 状态绕行和 M3UA 严格 ASP 验证。
- 如果要进行状态故障转移或在集群内操作，需要执行严格 ASP 状态检查。但是，严格 ASP 状态检查只能在覆盖模式下运行，如果在 Loadsharing 或广播模式下运行则不起作用（根据 RFC 4666）。该检测假设每个终端有一个且只有一个 ASP。

RADIUS 计费检测概述

RADIUS 计费检测是为了防止使用 RADIUS 服务器的 GPRS 网络上出现过度计费攻击。虽然实施 RADIUS 计费检测无需 Carrier 许可证，但它毫无意义，除非您正在实施 GTP 检测并已设置 GPRS。

GPRS 网络上的过度计费攻击会导致消费者为他们未使用的服务付费。在这种情况下，恶意攻击者会建立与服务器之间的连接，并从 SGSN 获取 IP 地址。即使攻击者结束呼叫，恶意服务器仍会向其发送数据包；虽然 GGSN 会丢弃这些数据包，但来自服务器的连接仍会保持活动状态。分配给恶意攻击者的 IP 地址将被释放，并重新分配给某个合法用户（该用户将需要为攻击者将会使用的服务付费）。

RADIUS 计费检测可确保流经 GGSN 的流量都是合法流量，从而防止此类攻击。正确配置 RADIUS 计费功能后，ASA 将基于 Radius 计费请求开始消息中的框架 IP 属性与 Radius 计费请求停止消息的匹配终止连接。如果发现停止消息包含框架 IP 属性中的匹配 IP 地址，ASA 将查找源与该 IP 地址匹配的所有连接。

您可以选择配置一个与 RADIUS 服务器预共享的密钥，以便 ASA 可验证消息。如果未配置共享密钥，ASA 则仅检查源 IP 地址是否为允许发送 RADIUS 消息的已配置地址之一。

注释 在启用 GPRS 的情形下使用 RADIUS 计费检测时，ASA 会检查计费请求 STOP 消息中的 3GPP-Session-Stop-Indicator，以便正确处理辅助 PDP 情景。特别是，ASA 要求计费请求 STOP 消息必须包含 3GPP-SGSN-Address 属性，才能终止用户会话和所有相关连接。默认情况下，某些第三方 GGSN 可能不发送此属性。

移动网络协议检测的许可

以下协议的检测需要下表中列出的许可证。

- GTP
- SCTP
- Diameter
- M3UA

型号	许可证要求
ASA Virtual（所有型号）	Carrier 许可证 （默认启用）
Cisco Secure Firewall 3100	运营商许可证
Firepower 4100	运营商许可证
Firepower 9300	运营商许可证
所有其他型号	Carrier 许可证在其他型号上不可用。无法检查这些协议。

GTP 检测默认设置

默认情况下，GTP 检测未启用。但是，如果在未指定检测映射的情况下启用 GTP 检测，将会使用提供以下处理的默认映射。仅在需要不同值的情况下，才需要配置映射。

- 不允许错误。
- 最大请求数为 200。
- 最大隧道数为 500。此值相当于 PDP 情景（终端）的数量。
- GTP 终端超时为 30 分钟。终端包括 GSN（GTPv0、1）和 SGW/PGW (GTPv2)。
- PDP 情景超时是 30 分钟。在 GTPv2 中，此值为承载情景超时。
- 请求超时为 1 分钟。
- 信令超时是 30 分钟。
- 隧道超时为 1 小时。
- T3 响应超时为 20 秒。
- 可以接受任何未知的消息 ID。可以配置 **match message v1/v2 id range** 命令来丢弃并记录不支持或想要允许的任何命令。如果消息未定义或是在系统不支持的 GTP 版本中进行了定义，则会被视为未知消息。

配置移动网络检测

默认情况下，移动网络中使用的协议检测未启用。如果要支持移动网络，必须进行配置。

过程

步骤 1 （可选。）配置 GTP 检测策略映射， 第 9 页。

步骤 2 （可选。）配置 SCTP 检测策略映射， 第 13 页。

步骤 3 （可选。）配置 Diameter 检测策略映射， 第 15 页。

如果要对软件中尚不支持的属性-值对 (AVP) 进行过滤，可以创建自定义 AVP 以用于 Diameter 检测策略映射。请参阅创建自定义 Diameter 属性-值对 (AVP)， 第 19 页。

步骤 4 （可选。）如果要检测加密的 Diameter TCP/TLS 流量，可按如下部分所述创建所需的 TLS 代理：检查加密的 Diameter 会话， 第 20 页

步骤 5 （可选。） 配置 M3UA 检测策略映射， 第 31 页

步骤 6 配置移动网络检测服务策略 ， 第 34 页。

步骤 7 （可选。）配置 RADIUS 计费检测， 第 36 页。

RADIUS 会计检测可防止超额计费 (over-billing) 攻击。

配置 GTP 检测策略映射

如果要对 GTP 流量执行其他参数，而默认映射不能满足需求，则可以创建并配置 GTP 映射。

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 创建 GTP 检测策略映射：**policy-map type inspect gtp** *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 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**] **apn regex** {*regex_name* | **class** *class_name*} - 根据指定的正则表达式或正则表达式类匹配接入点名称 (APN)。
- **match** [**not**] **message** {**v1** | **v2**} **id** {*message_id* | **range** *message_id_1 message_id_2*} - 匹配消息 ID，该值可介于 1 到 255 之间。可以指定单个 ID 或 ID 范围。必须指定该消息是否适用于 GTPv0/1 (**v1**) 或 GTPv2 (**v2**)。
- **match** [**not**] **message length min** *bytes* **max** *bytes* - 匹配 UDP 负载长度（GTP 报头加上消息其余部分）介于最小值和最大值（1 到 65536）之间的消息。
- **match** [**not**] **msisdn regex** {*regex_name* | **class** *class_name*} - 根据指定的正则表达式或正则表达式类来匹配“创建 PDP 情景”请求、“创建会话”请求和“修改载体响应”消息中的移动站国际用户目录号 (MSISDN) 信息元素。正则表达式可根据前 x 位数识别特定的 MSISDN 或 MSISDN 范围。MSISDN 过滤仅支持 GTPv1 和 GTPv2。
- **match** [**not**] **selection-mode** *mode_value* - 匹配创建 PDP 情景请求中的选择模式信息元素。选择模式指定消息中的无线接入点名称 (APN) 来源，可以是以下项目之一。选择模式过滤仅支持 GTPv1 和 GTPv2。
  - 0 - 已验证。由移动站点或网络提供 APN，并且已验证订用。
  - 1 - 移动站点。由移动站点提供 APN，并且已验证订用。
  - 2 - 网络。由网络提供 APN，并且已验证订用。
  - 3 - 保留，未使用。
- **match** [**not**] **version** {*version_id* | **range** *version_id_1 version_id_2*} - 匹配 GTP 版本（版本范围是可以是 0 到 255）。可以指定单个版本或版本范围。

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**] - 丢弃匹配的所有数据包。添加 **log** 关键字，以同时发送一条系统日志消息。
- **rate-limit** *Message_rate* - 限制消息的速率。此选项仅对 **message id** 可用。

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

步骤 4 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：

- **anti-replay** [*window_size*] - 通过为 GTP-U 消息指定滑动窗口来启用防重放。滑动窗口的大小取决于消息的数量，可以为 128、256、512 或 1024。如果未指定大小，您将获得默认值 512。当有效消息出现时，窗口会移动到新的序列号。序列号在 0 至 65535 范围内，在其达

到最大值时回卷，并且它们对每个 PDP 情景都是唯一的。如果消息的序列号在窗口以内，则视为有效消息。防重放有助于防范会话劫持或 DoS 攻击，在黑客捕获 GTP 数据包并进行重放时，可能发生这些攻击。

- **permit errors** - 允许无效 GTP 数据包或者那些无法解析并将被丢弃的数据包。
- **request-queue** *max_requests* - 设置排队等待响应的最大 GTP 请求数。默认值为 200。达到限制后，如果有新请求到达，将会删除队列中等待时间最长的请求。错误提示、不支持的版本和 SGSN 情景确认消息不被视为请求，且不会进入请求队列中等待响应。
- **tunnel-limit** *max_tunnels* - 设置允许的最大活动 GTP 隧道数。该值相当于 PDP 情景或终端数量。默认值为 500。达到此命令指定的隧道数后，新请求将被丢弃。
- **timeout** {**endpoint** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *time* - 设置指定服务的空闲超时（采用“小时:分钟:秒”格式）。如果不想设置超时，请指定数字 0。为每个超时分别输入此命令。
  - **endpoint**- 删除 GTP 终端之前允许处于非活动状态的最长时间。
  - **pdp-context**- 删除 GTP 会话的 PDP 情景前允许处于非活动状态的最长时间。在 GTPv2 中，这属于承载情景。
  - **request**- 从请求队列中删除某个请求之前允许处于非活动状态的最长时间。对丢弃请求的任何后续响应也将被丢弃。
  - **signaling**- 删除 GTP 信令之前允许处于非活动状态的最长时间。
  - **t3-response**- 删除连接前等待响应的最长时间。
  - **tunnel**- 终止 GTP 隧道之前允许处于非活动状态的最长时间。

步骤 5 仍在参数配置模式下，配置 GTP-U 检查 IP 数据包和反欺骗。

gtp-u-header-check [**anti-spoofing** [**gtpv2-dhcp-bypass** | **gtpv2-dhcp-drop**]]

不带关键字时，该命令会检查 GTP 数据包的内部负载是否是有效的 IP 数据包，如果包含非 IP 报头则将数据包丢弃。

如果包含 **anti-spoofing** 关键字，系统还会检查内部负载的 IP 报头中的移动用户 IP 地址是否与 GTP 控制消息（例如创建会话响应）中分配的 IP 地址匹配，如果 IP 地址不匹配，则将 GTP-U 消息丢弃。此检查支持 IPv4、IPv6、IPv4v6 PDN 类型。如果移动站点使用 DHCP 获取其地址，GTPv2 中的最终用户 IP 地址将为 0.0.0.0 (IPv4) 或 *prefix*::0 (IPv6)，那么在这种情况下，系统将会使用在内部数据包中找到的第一个 IP 地址来更新最终用户 IP 地址。您可以使用以下关键字来更改 DHCP 获取的地址的默认行为：

- **gtpv2-dhcp-bypass** - 不要更新 0.0.0.0 或 *prefix*::0 地址。而是允许最终用户 IP 地址为 0.0.0.0 或 *prefix*::0 的数据包。使用 DHCP 获取 IP 地址时，此选项会绕过防欺骗检查。
- **gtpv2-dhcp-drop** - 不要更新 0.0.0.0 或 *prefix*::0 地址。而是丢弃最终用户 IP 地址为 0.0.0.0 或 *prefix*::0 的所有数据包。此选项可防止使用 DHCP 获取 IP 地址的用户访问。

步骤 6 如有需要，可以在仍处于参数配置模式下时配置 IMSI 前缀过滤：

mcc *country_code* **mnc** *network_code*

drop mcc *country_code* **mnc** *network_code*

您可以根据需要多次输入命令，以指定所有目标 MCC/MNC 对，但策略映射中的所有命令都必须是 **mcc** 或 **drop mcc**。这些命令不能组合使用。

默认情况下，GTP 检测不检查移动国家/地区代码 (MCC)/移动网络代码 (MNC) 组合的有效性。如果配置 IMSI 前缀过滤，接收到的数据包 IMSI 中的 MCC 和 MNC 将会与配置的 MCC/MNC 组合进行比较。然后，系统会根据命令采取以下行动之一：

- **mcc** 命令 - 如果数据包不匹配，则丢弃该数据包。
- **drop mcc** 命令 - 如果数据包匹配，则将其丢弃。

移动设备国家/地区代码是非零的三位数值；应在一位或两位数值前添加零作为前缀。移动网络代码是两位或三位数值。

添加您希望允许或放弃的所有 MCC 和 MNC 组合。默认情况下，ASA 不会检查 MNC 和 MCC 组合的有效性，所以您必须验证配置组合的有效性。有关 MCC 和 MNC 代码的详细信息，请参阅 ITU E.212 建议《*Identification Plan for Land Mobile Stations*》（陆地移动站识别计划）。

步骤 7 如有需要，可以在仍处于参数配置模式下时启用位置日志记录。

location-logging [**cell-id**]

记录用户的位置，以跟踪移动站的位置变化。跟踪位置更改有助于识别存在的欺诈性漫游费用。当您启用位置日志记录时，系统会生成每个国际移动用户身份 (IMSI) 新建位置（消息 324010）或更改后位置（消息 324011）的系统日志消息。

如果希望日志信息包括用户当前注册的单元 ID，请指定 **cell-id** 参数。单元 ID 从单元全局标识 (CGI) 或 E-UTRAN 单元全局标识符 (ECGI) 中提取。

步骤 8 如有需要，可以在仍处于参数配置模式下时配置 GSN 或 PGW 轮询：

permit-response to-object-group *SGSN-SGW_name* **from-object-group** *GSN-PGW_pool*

当 ASA 执行 GTP 检测时，ASA 默认会丢弃来自 GSN 或 PGW 而 GTP 请求中未指定的 GTP 响应。在 GSN 或 PGW 池中使用负载均衡来提供 GPRS 的效率和扩展性时，会发生这种情况。

要创建 GSN/PGW 轮询以便支持负载均衡，请创建一个指定 GSN/PGW 终端的网络对象组，并在 **from-object-group** 参数中指定该组。同样，为 SGSN/SGW 创建一个网络对象组并在 **to-object-group** 参数中选择该组。如果 GSN/PGW 响应与 GTP 请求被发送到的 GSN/PGW 属于同一个对象组，并且 SGSN/SGW 位于允许响应 GSN/PGW 向其发送 GTP 响应的对象组中，则 ASA 允许该响应。

网络对象组可通过主机地址或包含终端的子网标识它们。

示例：

以下是一个 GSN/PGW 轮询的示例。整个 C 类网络均被定义为 GSN/PGW 池，但您可以标识多个单独的 IP 地址，每个 **network-object** 命令标识一个，而不是标识整个网络。然后，此示例修改 GTP 检测映射，以允许响应从池传输到 SGSN/SgW。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
```

```
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100

hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit-response to-object-group sgsn32
from-object-group gsnpool32
```

示例

以下示例显示如何限制网络中隧道的数量：

```
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap

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。请参阅配置移动网络检测服务策略 ， 第 34 页。

配置 SCTP 检测策略映射

要基于速率限制等特定应用的负载协议标识符 (PPID) 将替代操作应用于 SCTP 流量，请创建服务策略要使用的 SCTP 检测策略映射。

注释 PPID 位于数据分块中，特定数据包可包含多个数据分块，甚至包含一个控制数据块。如果数据包包含一个控制数据块或多个数据分块，即便对其分配的操作为丢弃，该数据包也不会被丢弃。例如，如果将 SCTP 检测策略映射配置为丢弃 PPID 26，而 PPID 26 数据分块与包含 Diameter PPID 数据分块的数据包组合在一起，则该数据包不会被丢弃。

过程

步骤 1 创建 SCTP 检测策略映射：**policy-map type inspect sctp** *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 基于 SCTP 数据分块中的 PPID 丢弃、按速率限制或记录流量。

a) 基于 PPID 标识流量。

match [**not**] **ppid** *ppid_1* [*ppid_2*]

其中 *ppid_1* 是 PPID 编号 (0-4294967295) 或名称（有关可用的名称，请参阅 CLI 帮助）。可以添加第二个（更高级别）PPID - *ppid_2*，用于指定 PPID 的范围。使用 **match not ppid** 来标识不匹配 PPID 或范围的流量。

您可以在以下网址查找当前的 SCTP PPID 列表：
http://www.iana.org/assignments/sctp-parameters/sctp-parameters.xhtml#sctp-parameters-25。

b) 指定要对匹配的数据包执行的操作。

- **drop**- 丢弃并记录匹配的所有数据包。
- **log**- 发送系统日志消息。
- **rate-limit** *rate* - 限制消息的速率。速率单位为千位/秒 (Kbps)。

c) 重复该步骤，直到标识要选择性处理的所有 PPID。

示例

以下示例创建的检测策略映射将丢弃未分配的 PPID（写入此示例时未分配）、按速率限制 PPID 32-40，并记录 Diameter PPID。该服务策略会对向匹配所有 SCTP 流量的 inspection_default 类应用检测。

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
  drop
 match ppid 26
  drop
 match ppid 49
  drop
 match ppid 32 40
  rate-limit 1000
 match ppid diameter
  log

policy-map global_policy
 class inspection_default
  inspect sctp sctp-pmap
!
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。请参阅配置移动网络检测服务策略 ， 第 34 页。

配置 Diameter 检测策略映射

您可以创建 Diameter 检测策略映射来过滤各种 Diameter 协议元素。然后，可以选择性地丢弃或记录连接。

要配置Diameter消息过滤，必须按照RFC和技术规范中的定义充分了解这些协议元素。例如，IETF包含注册应用、命令代码和属性-值对的列表（网址：http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml），但 Diameter 检测并非支持列出的所有项目。有关它们的技术规范，请参阅 3GPP 网站。

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）通过执行以下步骤创建 Diameter 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 diameter** [**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**] **application-id** *app_id* [*app_id_2*] - 匹配应用标识符，其中 *app_id* 为 Diameter 应用名称或编号 (0-4294967295)。如果要匹配某个连续编号的应用范围，可以再添加一个 ID。您可以按应用名称或编号来定义范围，该范围将适用于第一个 ID 和第二个 ID 之间的所有编号。

  这些应用会注册到IANA。以下是支持的核心应用，但您可以对其他应用进行过滤。有关应用名称的列表，请参阅 CLI 帮助。

- **3gpp-rx-ts29214** (16777236)
- **3gpp-s6a** (16777251)
- **3gpp-s9** (16777267)
- **common-message** (0)。这是基础 Diameter 协议。

- **match** [**not**] **command-code** *code* [*code_2*] - 匹配命令代码，其中 *code* 为 Diameter 命令代码名称或编号 (0-4294967295)。如果要匹配某个连续编号的命令代码范围，可以再添加一个代码。您可以按命令代码名称或编号来定义范围，该范围将适用于第一个代码和第二个代码之间的所有编号。

  例如，以下命令匹配“功能交换请求/应答”命令编码：

  ```
  match command-code cer-cea
  ```

- 匹配属性-值对 (AVP)。

  要仅按属性匹配 AVP，请使用以下命令：

  match [**not**] **avp** *code* [*code_2*] [**vendor-id** *id_number*]

  要基于属性的值匹配 AVP，请使用以下命令：

  match [**not**] **avp** *code* [**vendor-id** *id_number*] *value*

  其中：

  - *code* - 属性-值对的名称或编号 (1-4294967295)。对于第一个代码，您可以指定自定义 AVP 的名称或已在 RFC 或 3GPP 技术规范中注册且受该软件直接支持的某个 AVP 的名称。如果要匹配 AVP 的范围，请仅按编号指定第二个代码。如果要按值匹配 AVP，则无法指定第二个代码。有关 AVP 名称的列表，请参阅 CLI 帮助。
  - **vendor-id** *id_number* -（可选。）也要一并匹配的供应商的 ID 编号，范围为 0-4294967295。例如，3GPP 供应商 ID 为 10415，IETF 为 0。
  - *value* - AVP 的值部分。只有 AVP 的数据类型受支持，才能配置此项目。例如，可以为具有地址数据类型的 AVP 指定 IP 地址。下面是受支持的数据类型的值部分的特定语法：
    - Diameter Identity、Diameter URI、Octet String - 使用正则表达式或正则表达式类对象匹配这些数据类型。

      { **regex** *regex_name* | **class** *regex_class*}
    - Address - 指定要匹配的 IPv4 或 IPv6 地址。例如，10.100.10.10 或 2001:DB8::0DB8:800:200C:417A。
    - Time - 指定开始和结束日期及时间。两者均为必填项目。时间采用 24 小时格式。

      date *year month day* **time** *hh:mm:ss* **date** *year month day* **time** *hh:mm:ss*

      例如：

```
date 2015 feb 5 time 12:00:00 date 2015 mar 9 time 12:00:00
```

- Numeric - 指定编号的范围：

  range *number_1 number_2*

  有效的编号范围取决于数据类型：

  - Integer32：-2147483647 到 2147483647
  - Integer64：-9223372036854775807 到 9223372036854775807
  - Unsigned32：0 到 4294967295
  - Unsigned64：0 到 18446744073709551615
  - Float32：小数点表示方式，精度为 8 位数
  - Float64：小数点表示方式，精度为 16 位数

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 Diameter 检测策略映射：**policy-map type inspect diameter** *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 Diameter 类映射，请输入以下命令对其进行指定：**class** *class_map_name*
- 使用为 Diameter 类映射而介绍的 **match** 命令之一，直接在策略映射中指定流量。

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。
- **log**- 发送系统日志消息。

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。

示例：

```
hostname(config)# policy-map type inspect diameter diameter-map
hostname(config-pmap)# class diameter-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match command-code cer-cea
hostname(config-pmap-c)# log
```

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。

- **unsupported** {**application-id** |**command-code** |**avp**} **action log** 针对不受支持的 Diameter 元素启用日志记录。这些选项指定该软件不直接支持的应用 ID、命令代码和 AVP。默认设置为允许这些元素而不对它们进行日志记录。您可以输入该命令三次以对所有元素启用日志记录。
- **strict-diameter** {**state** | **session**} - 启用符合 RFC 6733 要求的严格 Diameter 协议。默认情况下，检测可确保 Diameter 框架符合 RFC。您可以添加 **state** 机器验证或 **session** 相关的消息验证，或通过输入该命令两次来添加两种验证。

示例：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# unsupported application-id action log
hostname(config-pmap-p)# unsupported command-code action log
hostname(config-pmap-p)# unsupported avp action log
hostname(config-pmap-p)# strict-diameter state
hostname(config-pmap-p)# strict-diameter session
```

示例

以下示例显示如何记录某些应用和阻止特定 IP 地址。

```
class-map type inspect diameter match-any log_app
  match application-id 3gpp-s6a
  match application-id 3gpp-s13

class-map type inspect diameter match-all block_ip
  match command-code cer-cea
  match avp host-ip-address 1.1.1.1

policy-map type inspect diameter diameter_map
  parameters
    unsupported application-id log
  class log_app
    log
  class block_ip
    drop-connection

policy-map global_policy
  class inspection_default
    inspect diameter diameter_map

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。请参阅配置移动网络检测服务策略 ， 第 34 页。

创建自定义 Diameter 属性-值对 (AVP)

定义和注册新属性-值对 (AVP) 后，即可创建自定义 Diameter AVP 在 Diameter 检测策略映射中定义和使用它们。通过 RFC 或定义 AVP 的其他来源可获得创建 AVP 所需的信息。

仅当希望在用于 AVP 匹配的 Diameter 检测策略映射或类映射中使用自定义 AVP 时创建它们。

过程

创建自定义 Diameter AVP。

diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]

其中：

- *name* - 要创建的自定义 AVP 的名称，最长为 32 个字符。在 Diameter 检测策略映射或类映射的 match avp 命令中可引用此名称。
- **code** *Value* - 自定义 AVP 代码值，介于 256-4294967295 之间。不能输入系统中已定义的代码和供应商 ID 组合。
- **data-type** *Type* - AVP 的数据类型。可以定义以下类型的 AVP。如果新 AVP 的类型与之不同，则无法为其创建自定义 AVP。
  - **address**- 适用于 IP 地址。
  - **diameter-identity**- Diameter 身份数据。
  - **diameter-uri**- Diameter 统一资源标识符 (URI)。
  - **float32**- 32 位浮点数值。
  - **float64**- 64 位浮点数值。
  - **int32**- 32 位整数。
  - **int64**- 64 位整数。
  - **octetstring**- 八位组字符串。
  - **time**- 时间值。
  - **uint32**- 32 位无符号整数。
  - **uint64**- 64 位无符号整数。
- **vendor-id** *id_number* -（可选。）定义 AVP 的供应商的 ID 编号，范围介于 0-4294967295 之间。例如，3GPP 供应商 ID 为 10415，IETF 为 0。

- **description** *Text* -（可选。）AVP 的说明，最长 80 个字符。如果包含空格，请将说明放在引号内。

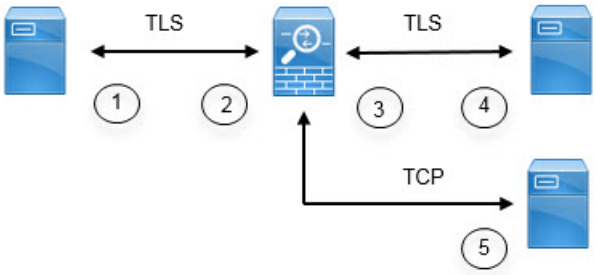
检查加密的 Diameter 会话

如果 Diameter 应用通过 TCP 使用加密数据，则检测功能看不到数据包的内部来实施消息过滤规则。因此，如果创建过滤规则和并希望也将它们应用于加密的 TCP 流量，必须配置 TLS 代理。另外，当希望对加密流量实施严格协议时，也需要代理。此配置不适用于 SCTP/DTLS 流量。

TLS 代理相当于中间人。它可以解密流量、进行检测、重新加密，再将其发送到预期目标。因此，连接的两端、Diameter 服务器和 Diameter 客户端必须信任 ASA，而且所有各方必须具有所需的证书。您必须全面了解实施 TLS 代理所需的数字证书。请阅读 ASA 常规配置指南中关于数字证书的一章。

下图显示 Diameter 客户端与服务器及 ASA 之间的关系以及建立证书所需的认证。在此模式中，Diameter 客户端是 MME（移动管理模块），而非最终用户。链路两端的 CA 证书分别用于对链路另一端的证书签名。例如，ASA 代理 TLS 服务器 CA 证书用于对 Diameter/TLS 客户端证书签名。

图 *2: Diameter TLS* 检测



1	Diameter TLS 客户端 (MME) • 客户端身份证书 • 用来对 ASA TLS 代理服务器身份证书签名的 CA 证书	2	ASA 代理 TLS 服务器 • 服务器身份证书 • 用来对 Diameter TLS 客户端身份证书签名的 CA 证书
3	ASA 代理 TLS 客户端 • 客户端身份（静态或 LDC）证书 • 用来对 Diameter TLS 服务器身份证书签名的 CA 证书	4	Diameter TLS 服务器（完全代理） • 服务器身份证书 • 用来对 ASA 代理 TLS 客户端身份证书签名的 CA 证书
5	Diameter TCP 服务器（TLS 卸载）。	-	—

您可以使用以下选项为 Diameter 检测配置 TLS 代理：

- 完全 TLS 代理 - 加密 ASA 与 Diameter 客户端以及 ASA 与 Diameter 服务器之间的流量。您可以使用以下选项建立与 TLS 服务器之间的信任关系：
  - 使用静态代理客户端信任点。当与 Diameter 服务器通信时，ASA 会为每个 Diameter 客户端提供相同的证书。一方面，由于所有客户端看起来相同，所以 Diameter 服务器无法为每个客户端提供不同的服务。另一方面，此选项比 LDC 方法的速度更快。
  - 使用本地动态证书 (LDC)。如果使用此选项，当与 Diameter 服务器通信时，ASA 会为每个 Diameter 客户端提供唯一证书。除公共密钥和来自 ASA 的新签名外，LDC 会保留收到的客户端身份证书的所有字段。使用这种方法，Diameter 服务器可更好地监控客户端流量，从而可以基于客户端证书特征提供不同的服务。
- TLS 卸载 - 加密 ASA 与 Diameter 客户端之间的流量，但在 ASA 与 Diameter 服务器之间使用明文连接。如果 Diameter 服务器与 ASA 位于同一数据中心，而您确定设备之间的流量不会离开受保护区域，则此选项是可行的。由于使用 TLS 卸载可减少所需的加密处理工作量，故可以提高性能。该方法应该是这些选项中速度最快的选项。Diameter 服务器只能基于客户端 IP 地址应用不同的服务。

以上三个选项对 ASA 与 Diameter 客户端之间的信任关系均采用相同的配置。

注释 TLS 代理使用 TLSv1.0 - 1.2。您可以配置 TLS 版本和加密套件。

以下主题介绍如何为 Diameter 检测配置 TLS 代理。

配置服务器与 Diameter 客户端的信任关系

ASA 相当于与 Diameter 客户端相关的 TLS 代理服务器。要建立互信关系，请执行以下操作：

- 需要将用于对 ASA 服务器证书签名的证书颁发机构 (CA) 证书导入到 Diameter 客户端。此证书可能位于客户端的 CA 证书存储中或客户端使用的某些其他位置。有关证书使用的具体详细信息，请参阅客户端文档。
- 需要导入用于对 Diameter TLS 客户端证书签名的 CA 证书，以便 ASA 可信任该客户端。

以下操作步骤介绍如何导入用于对 Diameter 客户端证书签名的 CA 证书，以及如何导入用于 ASA TLS 代理服务器的身份证书。您可以不导入身份证书，而是在 ASA 上创建自签名证书。

过程

步骤 1 将用于对 Diameter 客户端证书签名的 CA 证书导入到 ASA 信任点。

此步骤使 ASA 可以信任 Diameter 客户端。

a) 为 Diameter 客户端创建信任点。

在本例中，**enrollment terminal** 表示将证书粘贴到 CLI 中。该信任点称为 **diameter-clients**。

```
ciscoasa(config)# crypto ca trustpoint diameter-clients
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 添加证书。

```
ciscoasa(config)# crypto ca authenticate diameter-clients
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

步骤 2 导入证书，并为 ASA 代理服务器的身份证书和密钥对创建信任点。

此步骤使 Diameter 客户端可以信任 ASA。

a) 导入 pkcs12 格式的证书。

在以下示例中，**tls-proxy-server-tp** 为信任点名称，“**123**”为解密密码。使用自己的信任点名称和密码。

```
ciscoasa (config)# crypto ca import tls-proxy-server-tp pkcs12 "123"

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[PKCS12 data omitted]

quit

INFO: Import PKCS12 operation completed successfully

ciscoasa (config)#
```

b) 配置信任点。

```
ciscoasa(config)# crypto ca trustpoint tls-proxy-server-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

使用静态客户端证书为 Diameter 检测配置完整 TLS 代理

如果 Diameter 服务器可接受所有客户端使用同一证书，您可以为 ASA 设置一个静态客户端证书，用来与 Diameter 服务器通信。

要实现此配置，需要在 ASA 与客户端（详见配置服务器与 Diameter 客户端的信任关系，第 21 页）以及 ASA 与 Diameter 服务器之间建立互信关系。以下是 ASA 和 Diameter 服务器的信任要求。

- 您需要导入用来对 Diameter 服务器身份证书签名的 CA 证书，以便 ASA 在 TLS 握手期间可验证该服务器的身份证书。
- 需要导入也受 Diameter 服务器信任的客户端证书。如果 Diameter 服务器尚不信任该证书，请将用于签名的 CA 证书导入该服务器。有关详细信息，请参阅 Diameter 服务器的文档。

过程

步骤 1 将用于对 Diameter 服务器证书签名的 CA 证书导入 ASA 信任点。

此步骤使 ASA 可以信任 Diameter 服务器。

a) 为 Diameter 服务器创建信任点。

在本例中，**enrollment terminal** 表示将证书粘贴到 CLI 中。此外，也可以使用注册 url 指定自动注册 (SCEP) 到 CA。该信任点称为 **diameter-server**。

```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 添加证书。

```
ciscoasa(config)# crypto ca authenticate diameter-server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

步骤 2 导入证书，并为 ASA 代理客户端的身份证书和密钥对创建信任点。

此步骤使 Diameter 服务器可以信任 ASA。

a) 导入 pkcs12 格式的证书。

在以下示例中，**tls-proxy-client-tp** 为信任点名称，“**123**”为解密密码。使用自己的信任点名称和密码。

```
ciscoasa (config)# crypto ca import tls-proxy-client-tp pkcs12 "123"

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[PKCS12 data omitted]

quit

INFO: Import PKCS12 operation completed successfully

ciscoasa (config)#
```

b) 配置信任点。

```
ciscoasa(config)# crypto ca trustpoint tls-proxy-client-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

步骤 3 配置 TLS 代理。

a) 为 TLS 代理命名，并进入 TLS 代理配置模式。

tls-proxy *name*

b) 标识 ASA 充当与 Diameter 客户端相关的代理服务器时使用的信任点。

server trust-point *trustpoint_name*

注释
为了便于测试，或者如果您确定可以信任 Diameter 客户端，可以跳过此步骤并在 TLS 代理配置中添加 **no server authenticate-client** 命令。

c) 标识 ASA 充当与 Diameter 服务器相关的代理客户端时使用的信任点。

client trust-point *name*

d) （可选。）定义客户端可使用的密码。

client cipher-suite *cipher-list*

其中 *cipher-list* 可包括以下项目的任意组合：

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令定义的全局密码套件。默认情况下，全局密码等级为中等，这意味着除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 之外，所有密码均可用。仅在不希望使用 ASA 上通用的套件而使用其他套件时指定 **client cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 客户端连接的最低 TLS 版本，请参阅 **ssl client-version**ssl client-version**ssl client-version** 命令。默认值为 TLS v1.0。

e) （可选。）定义服务器可使用的密码。

server cipher-suite *cipher-list*

其中 *cipher-list* 可包括以下项目的任意组合：

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令定义的全局密码套件。默认情况下，全局密码等级为中等，这意味着除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 之外，所有密码均可用。仅在不希望使用 ASA 上通用的套件而使用其他套件时指定 **server cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 服务器连接的最低 TLS 版本，请参阅 **ssl server-version**ssl client-version**ssl server-version** 命令。默认值为 TLS v1.0。

示例：

```
ciscoasa(config)# tls-proxy diameter-tls-static-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client trust-point tls-proxy-client-tp
```

下一步做什么

现在，您即可在 Diameter 检测中使用 TLS 代理。请参阅配置移动网络检测服务策略 ， 第 34 页。

为 Diameter 检测配置支持本地动态证书的完全 TLS 代理

如果 Diameter 服务器对于每个客户端需要唯一的证书，可以配置 ASA 来生成本地动态证书 (LDC)。这些证书可在客户端连接持续时间内共存，然后则被删除。

要实现此配置，需要在 ASA 与客户端（详见配置服务器与 Diameter 客户端的信任关系，第 21 页）以及 ASA 与 Diameter 服务器之间建立互信关系。该配置与使用静态客户端证书为 Diameter 检测配置完整 TLS 代理，第 23 页中所述的配置类似，但不是导入 Diameter 客户端证书，而是在 ASA 上设置 LDC。以下是 ASA 和 Diameter 服务器的信任要求。

- 您需要导入用来对 Diameter 服务器身份证书签名的 CA 证书，以便 ASA 在 TLS 握手期间可验证该服务器的身份证书。
- 需要创建 LDC 信任点。需要导出 LDC 服务器的 CA 证书，并将其导入到 Diameter 服务器。导出步骤如下所述。有关导入证书的信息，请参阅 Diameter 服务器文档。

过程

步骤 1 将用于对 Diameter 服务器证书签名的 CA 证书导入 ASA 信任点。

此步骤使 ASA 可以信任 Diameter 服务器。

a) 为 Diameter 服务器创建信任点。

在本例中，**enrollment terminal** 表示将证书粘贴到 CLI 中。此外，也可以使用注册 url 指定自动注册 (SCEP) 到 CA。该信任点称为 **diameter-server**。

```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 添加证书。

```
ciscoasa(config)# crypto ca authenticate diameter-server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

步骤 2 创建用于对本地动态证书 (LDC) 签名的本地 CA。

a) 为该信任点创建一个 RSA 密钥对。

在本例中，该密钥对名为 ldc-signer-key。

```
ciscoasa(config)# crypto key generate rsa label ldc-signer-key
INFO: The name for the keys will be: ldc-signer-key
Keypair generation process
ciscoasa(config)#
```

b) 创建 LDC 颁发机构信任点。

在本例中，该信任点名为**ldc-server**，已使用上面创建的密钥对，已指定自签名注册（**enrollment self**，必需要求），并且 ASA 的通用名称被作为主题名称添加在内。检查 Diameter 应用对于主题名称是否具有特定要求。

proxy-ldc-issuer 命令为该信任点定义了本地 CA 角色，以便为 TLS 代理颁发动态证书。

```
ciscoasa(config)# crypto ca trustpoint ldc-server
ciscoasa(ca-trustpoint)# keypair ldc-signer-key
ciscoasa(ca-trustpoint)# subject-name CN=asa3
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# proxy-ldc-issuer
ciscoasa(ca-trustpoint)# exit
```

c) 注册该信任点。

```
ciscoasa(config)# crypto ca enroll ldc-server
```

步骤 3 配置 TLS 代理。

a) 为 TLS 代理命名，并进入 TLS 代理配置模式。

tls-proxy *name*

b) 标识 ASA 充当与 Diameter 客户端相关的服务器时使用的信任点。

server trust-point *trustpoint_name*

注释
为了便于测试，或者如果您确定可以信任 Diameter 客户端，可以跳过此步骤并在 TLS 代理配置中添加 **no server authenticate-client** 命令。

c) 标识 ASA 颁发动态证书和充当与 Diameter 服务器相关的客户端时使用的信任点。

client ldc issuer *name*

d) 标识 LDC 密钥对。指定在 LDC 信任点定义的同一密钥。

client ldc key-pair *name*

e) （可选。）定义客户端可使用的密码。

client cipher-suite *cipher-list*

其中 *cipher-list* 可包括以下项目的任意组合：

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令定义的全局密码套件。默认情况下，全局密码等级为中等，这意味着除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 之外，所有密码均可用。仅在不希望使用 ASA 上通用的套件而使用其他套件时指定 **client cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 客户端连接的最低 TLS 版本，请参阅 **ssl client-version**ssl client-version**ssl client-version** 命令。默认值为 TLS v1.0。

f) （可选。）定义服务器可使用的密码。

server cipher-suite *cipher-list*

其中 *cipher-list* 可包括以下项目的任意组合：

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令定义的全局密码套件。默认情况下，全局密码等级为中等，这意味着除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 之外，所有密码均可用。仅在不希望使用 ASA 上通用的套件而使用其他套件时指定 **server cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 服务器连接的最低 TLS 版本，请参阅 **ssl server-version**ssl client-version**ssl server-version** 命令。默认值为 TLS v1.0。

示例：

```
ciscoasa(config)# tls-proxy diameter-tls-ldc-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client ldc issuer ldc-server
```

```
ciscoasa(config-tlsp)# client ldc key-pair ldc-signer-key
```

步骤 4 导出 LDC CA 证书，并将其导入到 Diameter 服务器。

a) 导出证书。

在以下示例中，LDC 信任点是 ldc-server；指定自己的 LDC 信任点名称。

```
ciscoasa(config)# crypto ca export ldc-server identity-certificate
-----BEGIN CERTIFICATE-----
MIIDbDCCAlSgAwIBAgIQfWOQvGFpj7hCCB49+kS4CjANBgkqhkiG9w0BAQUFADAT
MREwDwYDVQQDEwhIdW5ueUJlZTAeFw0xMzA2MjUwMTE5MzJaFw00ODA2MjUwMTI5
...[data omitted]...
lJZ48NoI64RqfGC/KHUsOQ==
-----END CERTIFICATE-----
```

b) 复制证书数据并将其保存到文件中。

现在即可将其导入到 Diameter 服务器。有关操作步骤，请参阅 Diameter 服务器文档。请注意，这些数据为 Base64 格式。如果您的服务器需要二进制或 DER 格式，需要使用 OpenSSL 工具来转换格式。

下一步做什么

现在，您即可在 Diameter 检测中使用 TLS 代理。请参阅配置移动网络检测服务策略 ， 第 34 页。

为 Diameter 检测配置支持 TLS 分流的 TLS 代理

如果确定 ASA 与 Diameter 服务器之间的网络路径安全，可避免 ASA 与服务器之间加密数据的性能成本。使用 TLS 分流，TLS 代理可加密/解密 Diameter 客户端与 ASA 之间的会话，但对于 Diameter 服务器则使用明文。

要实现这种配置，只需在 ASA 与客户端之间建立互信关系，由此可简化配置。在执行以下步骤之前，请完成配置服务器与 Diameter 客户端的信任关系 ， 第 21 页中的步骤。

过程

步骤 1 配置支持 TLS 分流的 TLS 代理。

a) 为 TLS 代理命名，并进入 TLS 代理配置模式。

tls-proxy *name*

b) 标识 ASA 充当与 Diameter 客户端相关的服务器时使用的信任点。

server trust-point *trustpoint_name*

注释
为了便于测试，或者如果您确定可以信任 Diameter 客户端，可以跳过此步骤并在 TLS 代理配置中添加 **no server authenticate-client** 命令。

c) （可选。）定义服务器可使用的密码。

server cipher-suite *cipher-list*

其中 *cipher-list* 可包括以下项目的任意组合：

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令定义的全局密码套件。默认情况下，全局密码等级为中等，这意味着除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 之外，所有密码均可用。仅在不希望使用 ASA 上通用的套件而使用其他套件时指定 **server cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 服务器连接的最低 TLS 版本，请参阅 **ssl server-version**ssl client-version**ssl server-version** 命令。默认值为 TLS v1.0。

d) 指定 ASA 与 Diameter 服务器之间的通信应为明文。在此关系中，ASA 充当 Diameter 服务器的客户端。

client clear-text

示例：

```
ciscoasa(config)# tls-proxy diameter-tls-offload-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client clear-text
```

步骤 2 由于 Diameter 端口与 TCP 和 TLS 不同，所以需配置一个 NAT 规则将 TCP 端口转换为 TLS 端口，以便流量从 Diameter 服务器流到客户端。

为每台 Diameter 服务器创建一个对象 NAT 规则。每个规则应可以：

- 为 Diameter 服务器地址执行静态身份 NAT。即对象中的 IP 地址应与 NAT 规则中的转换地址相同。
- 将实际端口 3868（即默认 Diameter TCP 端口号）转换为 5868（默认 Diameter TLS 端口号）。
- 源接口是连接到 Diameter 服务器的接口，而目标接口是连接到 Diameter 客户端的接口。

以下示例将端口 3868 上从 10.29.29.29 Diameter 服务器传到外部接口的 TCP 流量转换到内部接口上的端口 5868。

```
ciscoasa(config)# object network diameter-client
ciscoasa(config-network-object)# host 10.29.29.29
ciscoasa(config-network-object)# nat (outside,inside) static 10.29.29.29
service tcp 3868 5868
```

下一步做什么

现在，您即可在 Diameter 检测中使用 TLS 代理。请参阅配置移动网络检测服务策略 ， 第 34 页。

配置 M3UA 检测策略映射

使用 M3UA 检测策略映射可基于点代码配置访问控制。此外，也可以按类和类型丢弃消息和对其应用速率限制。

默认点代码格式为 ITU。如果您使用其他格式，请在策略映射中指定所需的格式。

如果不希望基于点代码或消息类应用策略，则无需配置 M3UA 策略映射。可以启用不含映射的检测。

过程

步骤 1 创建 M3UA 检测策略映射： **policy-map type inspect m3ua** *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 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**] **message class** *class_id* [**id** *message_id*] - 匹配 M3UA 消息类和类型。下表列出了可能的值。有关这些消息的详细信息，请参阅 M3UA RFC 和文档。

M3UA 消息类	消息 ID 类型
0（管理消息）	0-1
1（传输消息）	1
2（SS7 信令网络管理消息）	1-6
3（ASP 状态维护消息）	1-6
4（ASP 流量维护消息）	1-4
9（路由密钥管理消息）	1-4

- **match** [**not**] **opc** *code* - 匹配数据消息中的始发点代码，即流量源。点代码为 *zone-region-sp* 格式，其中每个元素可能的值取决于 SS7 变量：
  - **ITU**- 点代码为 14 位，格式为 3-8-3。值范围为 [0-7]-[0-255]-[0-7]。
  - **ANSI**- 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。
  - **Japan**- 点代码为 16 位，格式为 5-4-7。值范围为 [0-31]-[0-15]-[0-127]。
  - **China**- 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。
- **match** [**not**] **dpc** *code* - 匹配数据消息中的目的点代码。点代码为 *zone-region-sp* 格式，如同所述的 **match opc** 相关内容。
- **match** [**not**] **service-indicator** *number* - 匹配服务指示符编号：0-15。下面是可用的服务指示符。有关这些服务指示符的详细信息，请参阅 M3UA RFC 和文档。
  - 0 - 信令网络管理消息
  - 1 - 信令网络测试和维护消息
  - 2 - 信令网络测试和维护特殊消息
  - 3 - SCCP
  - 4 - 电话用户部分
  - 5 - ISDN 用户部分
  - 6 - 数据用户部分（呼叫和电路相关消息）
  - 7 - 数据用户部分（设备注册和取消消息）
  - 8 - 预留用于 MTP 测试用户部分
  - 9 - 宽带 ISDN 用户部分
  - 10 - 卫星 ISDN 用户设备
  - 11 - 预留
  - 12 - AAL 第 2 类信令
  - 13 - 承载独立呼叫控制
  - 14 - 网关控制协议
  - 15 - 预留

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**] - 丢弃匹配的所有数据包。或者，发送系统日志消息。
- **rate-limit** *Message_rate* - 限制消息的速率。此选项仅适用于 **match message class**。

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

步骤 4 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：

- **message-tag-validation** {**dupu** | **error** | **notify**} - 确保已检查和验证指定消息类型的某些字段的内容。验证失败的消息将被丢弃。验证因消息类型而异。
  - 目标用户部分不可用 (DUPU) - User/Cause 字段必须存在，并且其中必须仅包含有效的原因和用户代码。
  - 错误 - 所有必填字段必须都存在，并且仅包含允许的值。每个错误消息都必须包含该错误代码的必填字段。
  - 通知 - 状态类型和状态信息字段必须仅包含允许的值。
- **ss7 variant** {**ITU** | **ANSI** | **JAPAN** | **CHINA**} - 标识网络中使用的 SS7 的变量。此选项决定点编码的有效格式。配置该选项并部署 M3UA 策略后，无法再对其更改，除非首先删除该策略。默认变量为 ITU。
- **strict-asp-state**- 执行应用服务器进程 (ASP) 状态验证。系统将维护 M3UA 会话的 ASP 状态，并基于验证结果允许或丢弃 ASP 消息。如果未启用严格 ASP 状态验证，系统将转发所有 ASP 消息而不进行检测。如果要进行状态故障转移或在集群内操作，需要执行严格 ASP 状态检查。但是，严格 ASP 状态检查只能在覆盖模式下运行，如果在 Loadsharing 或广播模式下运行则不起作用（根据 RFC 4666）。该检测假设每个终端有一个且只有一个 ASP。
- **timeout endpoint** *time* - 设置空闲超时，以便删除 M3UA 终端的统计信息；该值的格式为 hh:mm:ss。若不设置超时，请指定 0。默认值为 30 分钟 (00:30:00)。
- **timeout session** *time* - 如果启用严格 ASP 状态验证，则设置空闲超时，以便删除 M3UA 会话，该值的格式为 hh:mm:ss。若不设置超时，请指定 0。默认值为 30 分钟 (00:30:00)。禁用此超时可防止系统删除过时的会话。

示例

以下示例表示 M3UA 策略映射和服务策略。

```
hostname(config)# policy-map type inspect m3ua m3ua-map
hostname(config-pmap)# match message class 2 id 6
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match message class 9
```

```
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match dpc 1-5-1
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# ss7 variant ITU
hostname(config-pmap-p)# timeout endpoint 00:45:00

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect m3ua m3ua-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。请参阅配置移动网络检测服务策略 ，第 34 页。

配置移动网络检测服务策略

移动网络使用的协议检测在默认检测策略中未启用，所以如果需要这些检测，必须启用它们。可以简单地编辑默认全局检测策略来添加这些检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

过程

步骤 1 如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

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

示例：

```
hostname(config)# class-map mobile_class_map
hostname(config-cmap)# match access-list mobile
```

在默认全局策略中，inspection_default 类映射是一种特殊类映射，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**)。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。

有关匹配语句的信息，请参阅为通过流量创建第 3/4 层类映射。

步骤 2 添加或编辑策略映射，设置要对类映射流量采取的操作：**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。

步骤 4 启用检测。

在以下命令中，检测策略映射是可选的。如果您创建了其中任何映射来自定义检测，请在相应命令中指定它们的名称。 对于 Diameter，也可以指定 TLS 代理来启用加密消息检测。

- **inspect gtp** [*map_name*] - 启用 GTP 检测。
- **inspect sctp** [*map_name*] - 启用 SCTP 检测。
- **inspect diameter** [*map_name*] [**tls-proxy** *proxy_name*] - 启用 Diameter 检测。

  注释
  如果为 Diameter 检测指定 TLS 代理并对 Diameter 服务器流量应用 NAT 端口重定向（例如，将服务器流量从端口 5868 重定向到 3868），请配置全局检测或仅在传出接口上配置检测。如果对传出接口应用检测，则通过 NAT 连接的 Diameter 流量将绕过检测。

- **inspect m3ua** [*map_name*] - 启用 M3UA 检测。

示例：

```
hostname(config-class)# inspect gtp
hostname(config-class)# inspect sctp
hostname(config-class)# inspect diameter
hostname(config-class)# inspect m3ua
```

注释
如果是编辑默认全局策略（或正在使用的任何策略）以使用不同的检测策略映射，必须使用命令的 **no inspect** 版本删除检测，然后再使用新的检测策略映射名称重新添加该检测。例如，要更改用于 GTP 的策略映射，请执行以下操作：

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-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。

配置 RADIUS 计费检测

默认情况下，RADIUS 计费检测未启用。如果需要 RADIUS 计费检测，必须对其进行配置。

过程

步骤 1 配置 RADIUS 计费检测策略映射，第 36 页。

步骤 2 配置 RADIUS 计费检测服务策略，第 37 页。

配置 RADIUS 计费检测策略映射

要配置 RADIUS 计费检测所需的属性，必须创建 RADIUS 计费检测策略映射。

过程

步骤 1 创建 RADIUS 计费检测策略映射：**policy-map type inspect radius-accounting** *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。

- **send response** - 指示 ASA 向这些消息（**host** 命令中已标识）的发件人发送计费请求开始和停止消息。
- **enable gprs** - 实施 GPRS 过度计费防护。ASA 检查计费请求停止和断开消息中的 3GPP VSA 26-10415 属性，以便正确处理辅助 PDP 情景。如果存在此属性，ASA 将终止其源 IP 与已配置接口上的用户 IP 地址匹配的所有连接。
- **validate-attribute** *number* - 接收 Accounting-Request Start 消息时用于构建用户账户表的其他条件。在 ASA 决定是否终止连接时，这些属性可提供帮助。

如果没有指定要验证的其他属性，ASA 将会以 Framed IP Address 属性中的 IP 地址作为唯一依据作出决定。如果配置了其他属性，并且ASA收到的开始计费消息包含当前正在跟踪的地址，但要验证的其他属性不同，则在已将IP地址重新分配给新用户的情况下，使用旧属性启动的所有连接都将被终止。

值范围是 1 到 191，而且可以多次输入命令。有关属性编号及其描述的列表，请访问 http://www.iana.org/assignments/radius-types。

- **host** *ip_address* [**key** *secret*] - RADIUS 服务器或 GGSN 的 IP 地址。您可以选择添加密钥，以便 ASA 可验证消息。如果没有密钥，则只检查 IP 地址。可以重复使用此命令来标识多个 RADIUS 和 GGSN 主机。ASA 收到来自这些主机的 RADIUS 计费消息副本。
- **timeout users** *time* - 设置用户空闲时间（格式为 hh:mm:ss）。如果不想设置超时，请指定 00:00:00。默认值为一小时。

示例

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

配置 RADIUS 计费检测服务策略

RADIUS 计费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。由于 RADIUS 计费检测应用于定向到 ASA 的流量，所以必须将其配置为管理检测规则，而不是标准规则。

过程

步骤 1 创建 L3/L4 管理类映射，以标识要应用检测的流量并确定匹配流量。

```
class-map type management name
match {port | access-list} parameter
```

示例：

```
hostname(config)# class-map type management radius-class-map
```

```
hostname(config-cmap)# match port udp eq radius-acct
```

在本例中，匹配应用于 radius-acct UDP 端口，即 1646。可以指定其他端口或端口范围 (**match port udp range** *number1 number2*)，也可以使用 **match access-list** *acl_name* 和 ACL。

步骤 2 添加或编辑策略映射，设置要对类映射流量采取的操作：**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 RADIUS 计费检测的第 3/4 层管理类映射：**class** *name*

示例：

```
hostname(config-pmap)# class radius-class-map
```

步骤 4 配置 RADIUS 计费检测：**inspect radius-accounting** [*radius-accounting_policy_map*]

其中，*radius_accounting_policy_map* 是在配置 RADIUS 计费检测策略映射，第 36 页中创建的 RADIUS 计费检测策略映射。

示例：

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

注释
如果要编辑使用中的策略来使用不同的检测策略映射，必须使用 **no inspect radius-accounting** 命令删除 RADIUS 计费检测，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。

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。

监控移动网络检测

以下主题介绍如何监控移动网络检测。

监控 GTP 检测

要显示 GTP 配置，请在特权 EXEC 模式下输入 **show service-policy inspect gtp** 命令。

使用 **show service - policy inspect gtp statistics** 命令显示 GTP 检测的统计信息。以下是输出示例：

```
firewall(config)# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

通过在 **show service-policy inspect gtp statistics** *ip_address* 命令中输入 IP 地址，可获取特定 GTP 终端的统计信息。

```
firewall(config)# show service-policy inspect gtp statistics 10.9.9.9
1 in use, 1 most used, timeout 0:30:00
 GTP GSN Statistics for 10.9.9.9, Idle 0:00:34, restart counter 0
  Tunnels Active                    0
  Tunnels Created                   1
  Tunnels Destroyed                 0
  Total Messages Received           1
                         Signalling Messages        Data Messages
  total received                   1                          0
  dropped                          0                          0
  forwarded                        1                          0
```

可使用 **show service-policy inspect gtp pdp-context** 命令显示 PDP 情景相关信息。对于 GTPv2，这是承载情景。例如：

```
ciscoasa(config)# show service-policy inspect gtp pdp-context
4 in use, 5 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
```

```
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146

ciscoasa(config)# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:06:14,   Timeout 3:00:00,   APN ssenoauth146

    user_name (IMSI):  50502410121507    MS address: 2005:a00::250:56ff:fe96:eec
    nsapi: 5                 linked nsapi: 5
    primary pdp: Y         sgsn is Remote
    sgsn_addr_signal: 10.0.203.22    sgsn_addr_data: 10.0.203.22
    ggsn_addr_signal: 10.0.202.22    ggsn_addr_data: 10.0.202.22
    sgsn control teid:     0x00000001    sgsn data teid:        0x000003e8
    ggsn control teid:     0x000f4240    ggsn data teid:        0x001e8480
    signal_sequence:               18     state:    Ready
...
```

PDP 或承载情景通过隧道 ID (TID)（IMSI 与 NSAPI (GTPv0-1) 或 IMSI 与 EBI (GTPv2) 值的组合）标识。GTP 隧道由不同 GSN 或 SGW/PGW 节点中的两个关联情景来定义，并通过隧道 ID 标识。在外部数据包数据网络与移动用户 (MS) 之间转发数据包需要使用 GTP 隧道。

监控 SCTP

您可以使用以下命令来监控 SCTP。

- **show service-policy inspect sctp**

  显示 SCTP 检测统计信息。PPID 每匹配一次丢弃操作，sctp-drop-override 计数器便递增一次，但数据包不会因为包含具有不同 PPID 的数据分块而被丢弃。例如：

  ```
  ciscoasa# show service-policy inspect sctp
  Global policy:
    Service-policy: global_policy
      Class-map: inspection_default
        Inspect: sctp sctp, packet 153302, lock fail 0, drop 20665, reset-drop 0,
  5-min-pkt-rate 0 pkts/sec, v6-fail-close 0, sctp-drop-override 4910
          Match ppid 30 35
             rate-limit 1000 kbps, chunk 2354, dropped 10, bytes 21408, dropped-bytes 958

          Match: ppid 40
             drop, chunk 5849
          Match: ppid 55
             log, chunk 9546
  ```

- **show sctp** [**detail**]

  显示当前的 SCTP cookie 和关联。添加 **detail** 关键字，可查看有关 SCTP 关联的详细信息。详细视图还会显示有关多宿主、多流和分段重组的信息。

  ```
  ciscoasa# show sctp

  AssocID: 71adeb15
  ```

```
Local:  192.168.107.12/50001 (ESTABLISHED)
Remote: 192.168.108.122/2905 (ESTABLISHED)
Secondary Conn List:
    192.168.108.12(192.168.108.12):2905 to 192.168.107.122(192.168.107.122):50001
    192.168.107.122(192.168.107.122):50001 to 192.168.108.12(192.168.108.12):2905
    192.168.108.122(192.168.108.122):2905 to 192.168.107.122(192.168.107.122):50001
    192.168.107.122(192.168.107.122):50001 to 192.168.108.122(192.168.108.122):2905
    192.168.108.12(192.168.108.12):2905 to 192.168.107.12(192.168.107.12):50001
    192.168.107.12(192.168.107.12):50001 to 192.168.108.12(192.168.108.12):2905
```

- **show conn protocol sctp**

  显示有关当前 SCTP 连接的信息。

- **show local-host** [**connection sctp** *start*[*-end*]]

  显示主机上有关使 SCTP 连接在每个接口上通过 ASA 的信息。添加 **connection sctp** 关键字，可仅查看具有指定 SCTP 连接数量或范围的主机。

- **show traffic**

  如果启用 **sysopt traffic detailed-statistics** 命令，则显示每个接口的 SCTP 连接和检测统计信息。

监控 Diameter

您可以使用以下命令来监控 Diameter。

- **show service-policy inspect diameter**

  显示 Diameter 检测统计信息。例如：

```
ciscoasa# show service-policy inspect diameter
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: Diameter Diameter_map, packet 0, lock fail 0, drop 0, -drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        Class-map: log_app
            Log: 5849
         Class-map: block_ip
             drop-connection: 2
```

- **show diameter**

  显示每个 Diameter 连接的状态信息。例如：

```
ciscoasa# show diameter
Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.1.10/45169 to outside:212.1.1.10/3868
...
```

- **show conn detail**

  显示连接信息。Diameter 连接均标有 Q 标志。

- **show tls-proxy**

  如果在 Diameter 检测中使用了 TLS 代理，则此命令显示 TLS 代理的相关信息。

监控 M3UA

您可以使用以下命令来监控 M3UA。

- **show service-policy inspect m3ua drops**

  显示有关 M3UA 检测的丢弃统计信息。

- **show service-policy inspect m3ua endpoint** [*IP_address*]

  显示 M3UA 终端的统计信息。您可以指定终端 IP 地址来查看特定终端的信息。对于高可用性或集群系统，统计信息是相对于每台设备的，不同设备之间的统计数据并不同步。例如：

```
ciscoasa# sh service-policy inspect m3ua endpoint
 M3UA Endpoint Statistics for 10.0.0.100, Idle : 0:00:06 :
                   Forwarded        Dropped          Total Received
 All Messages      21                5                 26
 DATA Messages     9                 5                 14
 M3UA Endpoint Statistics for 10.0.0.110, Idle : 0:00:06 :
                   Forwarded        Dropped          Total Received
 All Messages      21                8                 29
 DATA Messages     9                 8                 17
```

- **show service-policy inspect m3ua session**

  如果启用了强应用服务器进程 (ASP) 状态验证，则显示有关 M3UA 会话的信息。这些信息包括源关联 ID、会话是单一交换还是双重交换，以及在集群中会话是集群所有者会话还是备份会话。在包含 3 台或更多设备的集群中，如果某台设备离开集群然后又返回集群，您可能会看到过时的备份会话。这些过时会话在超时后将被删除，除非您已禁用会话超时。

```
Ciscoasa# show service-policy inspect m3ua session
0 in use, 0 most used
Flags: o - cluster owner session, b - cluster backup session
       d - double exchange      , s - single exchange
AssocID: cfc59fbe in Down state, idle:0:00:05, timeout:0:01:00, bd
AssocID: dac2e123 in Active state, idle:0:00:18, timeout:0:01:00, os
```

- **show service-policy inspect m3ua table**

  显示运行时 M3UA 检测表，包括分类规则。

- **show conn detail**

  显示连接信息。M3UA 连接标有 v 标志。

移动网络检测的历史记录

功能名称	版本	功能信息
GTPv2 检测和 GTPv0/1 检测的改进。	9.5(1)	GTP 检测现在可以处理 GTPv2。此外，所有版本的 GTP 检测现在均支持 IPv6 地址。 已将 **match message id** 命令更改为 **match message** {**v1** |**v2**} **id** *message_id* 。已将 **timeout gsn** 命令替换为 **timeout endpoint**。从 **clear/show service-policy inspect gtp statistics** 命令中删除了 **gsn** 关键字；现在，只需输入终端 ID 即可查看或清除这些统计信息。现在，**clear/show service-policy inspect gtp request** 和 **pdpmcb** 命令包括 **version** 关键字，所以您可以显示有关特定 GTP版本的信息。
SCTP 检测	9.5(2)	现在，您可以对流控制传输协议 (SCTP) 流量应用应用层检测，以便基于负载协议标识符 (PPID) 应用操作。 关键字，所以您可以显示有关特定GTP版本的信息：**clear conn protocol sctp**、**inspect sctp**、**match ppid**、**policy-map type inspect sctp**、**show conn protocol sctp**、**show local-host connection sctp**、**show service-policy inspect sctp**。
Diameter 检测	9.5(2)	现在，您可以对Diameter流量应用应用层检测，也可以基于应用 ID、命令代码和属性值对 (AVP) 过滤应用操作。 添加或修改了以下命令：**class-map type inspect diameter**、**diameter**、**inspect diameter**、**match application-id**、**match avp**、**match command-code**、**policy-map type inspect diameter**、**show conn detail**、**show diameter**、**show service-policy inspect diameter**、**unsupported**。
Diameter 检测的改进	9.6(1)	现在，您可以在集群模式下检测通过 TCP/TLS 的 Diameter 流量、应用严格协议符合性检查及检测通过 SCTP 的 Diameter 流量。 添加或修改了以下命令：**client clear-text**、**inspect diameter**、**strict-diameter**。
集群模式下的 SCTP 状态检测	9.6(1)	SCTP 状态检查现在可在集群模式下进行。还可以在集群模式下配置 SCTP 状态检查旁路。 我们未引入或更改任何命令。

功能名称	版本	功能信息
MTP3 用户适应 (M3UA) 检测。	9.6(2)	现在，您可以检测M3UA流量并基于点编码、服务指标及消息类和类型应用操作。 添加或修改了以下命令：**clear service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}、**inspect m3ua**、**match dpc**、**match opc**、**match service-indicator**、**policy-map type inspect m3ua**、**show asp table classify domain inspect-m3ua**、**show conn detail**、**show service-policy inspect m3ua** {**drops** | **endpoint** [*IP_address*]}、**ss7 variant**、**timeout endpoint**。
支持 SCTP 多流重新排序、重组和分段。支持 SCTP 多宿主，其中 SCTP 终端具有一个以上的 IP 地址。	9.7(1)	现在，系统完全支持 SCTP 多流重新排序、重组和分段，由此改善了 SCTP 流量的 Diameter 和 M3UA 检测效果。该系统还支持 SCTP 多宿主，其中每个 SCTP 终端都有一个以上的IP地址。对于多宿主，该系统可以打开辅助地址的针孔，使您无需编写访问规则即可允许它们访问。必须将每个 SCTP 终端限制为 3 个 IP 地址。 修改了以下命令的输出：**show sctp detail**。
M3UA 检测有所改进。	9.7(1)	M3UA检查现在支持状态化故障转移、半分布式集群和多宿主。另外，您还可以配置严格应用服务器进程 (ASP) 状态验证和各种消息验证。对于状态故障转移和集群，需要使用严格 ASP 状态验证。 添加或修改了以下命令：**clear service-policy inspect m3ua session** [**assocID** *id*]、**match port sctp**、**message-tag-validation**、**show service-policy inspect m3ua drop**、**show service-policy inspect m3ua endpoint**、**show service-policy inspect m3ua session**、**show service-policy inspect m3ua table**、**strict-asp-state**、**timeout session**。
支持设置 TLS 代理服务器 SSL 加密套件。	9.8(1)	现在可在 ASA 作为 TLS 代理服务器时设置 SSL 密码套件。过去，您只能中使用 **ssl cipher** 命令为 ASA 设置全局设置。 引入了以下命令：**server cipher-suite**
MSISDN 的 GTP 检测增强功能和选择模式过滤、防重放以及用户欺骗保护。	9.10(1)	您现在可以配置GTP检测基于移动站点国际用户目录编号 (MSISDN) 或选择模式丢弃创建 PDP 情景消息。您还可以实施防重放和用户防欺骗。 添加了以下命令：**anti-replay**、**gtp-u-header-check**、**match msisdn**、**match selection-mode**。

功能名称	版本	功能信息
支持 GTPv1 版本 10.12。	9.12(1)	系统现在支持 GTPv1 版本 10.12。以前，系统支持版本 6.1。在支持新版本后，系统可以多识别 25 种 GTPv1 消息以及 66 种信息元素。 此外，系统行为也有所变化。现在，系统可以接受任何未知的消息ID。而在过去，未知消息会被丢弃并记入日志。 未添加或更改任何命令。
移动站的位置日志记录 （GTP 检测） 。	9.13(1)	可以配置GTP检测以记录移动站的初始位置和该位置的后续更改。跟踪位置更改有助于识别可能存在的欺诈性漫游费用。 添加了以下命令：**location-logging**。
支持 GTPv2 和 GTPv1 版本 15。	9.13(1)	系统现在支持GTPv2 3GPP 29.274 V15.5.0。对于GTPv1，最高支持 3GPP 29.060 V15.2.0。在支持新版本后，系统可以多识别 2 种消息以及 53 种信息元素。 未添加或更改任何命令。
能够指定要在GTP 检测中丢弃的 IMSI 前缀。	9.16（1）	通过 GTP 检测，您可以配置 IMSI 前缀过滤，以识别允许的移动国家/地区代码/移动网络代码 (MCC/MNC) 组合。现在，您可以对要丢弃的MCC/MNC组合执行IMSI过滤。这样，您可以列出不需要的组合，并默认允许所有其他组合。 添加了以下命令：**drop mcc**。
安全防火墙 3100 支持运营商许可证	9.18(1)	运营商许可证启用 Diameter、GTP/GPRS、SCTP 检测。 新增/修改的命令：**feature carrier**

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。