基本互联网协议检测

以下主题介绍基本互联网协议的应用检测。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信息，请参阅应用层协议检测入门。

DCERPC 检测

DCERPC 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。可以简单地编辑默认全局检测策略来添加 DCERPC 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 DCERPC 检测引擎。

DCERPC 概述

Microsoft 远程过程调用 (MSRPC) 基于 DCERPC，是 Microsoft 分布式客户端和服务器应用广泛使用的协议，允许软件客户端在服务器上远程执行程序。

这通常涉及查询称为终端映射器的服务器（用于侦听已知端口号，以获取所需服务的动态分配网络信息）的客户端。然后，客户端建立与提供服务的服务器实例之间的辅助连接。安全设备允许相应的端口号以及网络地址，如有必要，还会为辅助连接应用 NAT。

DCERPC 检测引擎在已知 TCP 端口 135 上检测 EPM 与客户端之间的本地 TCP 通信。支持客户端的 EPM 映射和查找操作。客户端和服务器可位于任何安全区域。从适用的 EPM 响应消息接收嵌入式服务器 IP 地址和端口号。由于客户端可能尝试多次连接到 EPM 返回的服务器端口，因此，允许使用可配置超时的多个针孔。

DCE 检测支持以下通用唯一标识符 (UUID) 和消息：

- 终端映射器 (EPM) UUID。支持所有 EPM 消息。
- ISystemMapper UUID（非 EPM）。支持的消息如下：
  - RemoteCreateInstance opnum4
  - RemoteGetClassObject opnum3
- OxidResolver UUID（非 EPM）支持的消息如下：
  - ServerAlive2 opnum5
- 不包含 IP 地址或端口信息的任何消息，因为这些消息不需要检测。

配置 DCERPC 检测策略映射

要指定其他 DCERPC 检测参数，请创建 DCERPC 检测策略映射。然后，可以在启用 DCERPC 检测时应用所创建的检测策略映射。

在定义流量匹配条件时，可以创建类映射或者直接在策略映射中包括匹配语句。创建类映射与直接在检测策略映射中定义流量匹配的差别在于，可以重复使用类映射。

过程

步骤 1 （可选）创建 DCERPC 检测类映射。

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 dcerpc** [**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 进入类映射配置模式。

b) 指定要使用以下 **match** 命令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**] **uuid** *type* - 匹配 DCERPC 消息的通用唯一标识符 (UUID)。*type* 可以是下列项目之一：
  - **ms-rpc-epm**- 匹配 Microsoft RPC EPM 消息。
  - **ms-rpc-isystemactivator**- 匹配 ISystemMapper 消息。
  - **ms-rpc-oxidresolver**- 匹配 OxidResolver 消息。

c) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 DCERPC 检测策略映射：**policy-map type inspect dcerpc** *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 DCERPC 类映射，请输入以下命令对其进行指定：**class** *class_map_name*
- 使用介绍用于 DCERPC 类映射的 **match** 命令之一，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：

- **reset** [**log**] - 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。

可以在策略映射中指定多个 **class** 或 **match** 命令。

示例：

```
hostname(config)# policy-map type inspect dcerpc dcerpc-map
hostname(config-pmap)# match uuid ms-rpc-epm
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：

- **timeout pinhole** *hh:mm:ss* - 为 DCERPC 针孔配置超时，并覆盖全局系统针孔超时：2 分钟。超时可以是 00:00:01 到 119:00:00。
- **endpoint-mapper** [**epm-service-only**] [**lookup-operation** [**timeout** *hh:mm:ss*]] - 配置用于终端映射器流量的选项。在绑定期间，**epm-service-only** 关键字将实施终端映射器服务，以便仅处理其服务流量。**lookup-operation** 关键字将启用终端映射器服务的查找操作。可以配置查找操作生成的针孔超时。如果没有为查找操作配置超时，将会使用针孔超时命令或默认值。

示例

以下示例显示如何使用为 DCERPC 针孔配置的超时定义 DCERPC 检测策略映射。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc-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。

DNS 检测

默认情况下，DNS 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 DNS 应用检测。

DNS 检测默认设置

默认情况下，启用 DNS 检测，使用 preset_dns_map 检测类映射：

- 最大 DNS 消息长度为 512 字节。
- 禁用通过 TCP 的 DNS 检测。
- 最大客户端 DNS 消息长度是自动设置的，以与资源记录匹配。
- DNS Guard 已启用，因此 ASA 在转发 DNS 应答后立即终止与 DNS 查询相关的 DNS 会话。另外，ASA 还会监控消息交换，以确保 DNS 应答的 ID 与 DNS 查询的 ID 匹配。
- 根据 NAT 配置的 DNS 记录转换已启用。
- 协议执行已启用，使得可以进行 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。

请参阅以下默认 DNS 检测命令：

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
! ...
service-policy global_policy global
```

配置 DNS 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 DNS 检测策略映射来自定义 DNS 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 DNS 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 dns** [**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**] **header-flag** [**eq**] {*f_name* [*f_name...*] | *f_value*} - 匹配 DNS 标志。*f_name* 参数是以下 DNS 标志名称之一：**AA**（授权应答）、**QR**（查询）、**RA**（可用递归）、**RD**（所需递归）、**TC**（截断）。*f_value* 参数是以 0x 开头的十六进制的 16 位值，范围是 0x0 到 0xffff。Eq 关键字指定精确匹配（完全匹配）；如果没有 **eq** 关键字，数据包只需匹配指定的报头之一（任意匹配）。例如，**match header-flag AA QR**。
- **match** [**not**] **dns-type {eq** {*t_name* | *t_value*} | **range** *t_value1 t_value2*} - 匹配 DNS 类型。*t_name* 参数是以下 DNS 类型名称之一：**A**（IPv4 地址）、**AXFR**（完整区域传送）、**CNAME**（规范名称）、**IXFR**（增量区域传输）、**NS**（授权域名服务器）、**SOA**（授权区域起始）或 **TSIG**（事务数字签名）。t_value 参数为 DNS 类型字段中的任意值 (0-65535)。range 关键字指定范围，eq 关键字指定精确匹配。例如：**match dns-type eq A**。
- **match** [**not**] **dns-class {eq** {**in** | *c_value*} | **range** *c_value1 c_value2*} - 匹配 DNS 类。该类为 **in**（对于互联网）或 c_value（DNS 类字段中的任意值，范围介于 0 到 65535 之间）。range 关键字指定范围，eq 关键字指定精确匹配。例如：**match dns-class eq in**。
- **match** [**not**] {**question** | **resource-record** {**answer** | **authority** | **additional**}} - 匹配 DNS 问题或资源记录。**question** 关键字指定 DNS 消息的问题部分。Resource-record 关键字指定资源记录的以下部分之一：**answer**、authority 或 **additional**。例如：**match resource-record answer**。
- **match** [**not**] **domain-name 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 DNS 消息域名列表。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 DNS 检测策略映射：**policy-map type inspect dns** *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 DNS 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 DNS 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** [**log**] - 丢弃匹配的所有数据包。
- **drop-connection** [**log**] - 丢弃数据包并关闭连接。
- **mask** [**log**] - 掩蔽数据包的匹配部分。此操作仅适用于报头标志匹配项。
- **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。
- **enforce-tsig** [**drop**] [**log**] - 强制消息中包含 TSIG 资源记录。可以丢弃数据包但不丢弃 TSIG 资源记录，可以记录数据包，也可以丢弃并记录数据包。可以将此选项与针对报头标志匹配项的掩蔽操作结合使用；否则，此操作与其他操作相互排斥。

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 dns dns-map
hostname(config-pmap)# class dns-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match header-flag eq aa
hostname(config-pmap-c)# drop 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。

- **dnscrypt**- 启用 DNScrypt 以加密设备与思科 Umbrella 之间的连接。启用 DNScrypt 将使用 Umbrella 解析器启动密钥交换线程。密钥交换线程每小时执行与解析器的握手，并使用新密钥来更新设备。由于 DNScrypt 使用 UDP/443，您必须确保用于 DNS 检测的类映射包含该端口。请注意，默认检测类已在 DNS 检测中包括 UDP/443。
- **dns-guard** - 启用 DNS 保护。ASA 在转发 DNS 应答后立即终止与 DNS 查询相关的 DNS 会话。另外，ASA 还会监控消息交换，以确保 DNS 应答的 ID 与 DNS 查询的 ID 匹配。
- **id-mismatch count** *number* **duration** *seconds* **action log** - 为过多的 DNS ID 不匹配启用日志记录，其中 **count** *number* **duration** *seconds* 参数指定在发送系统消息日志之前允许的最大每秒不匹配实例数量。
- **id-randomization** - 随机化 DNS 查询的 DNS 标识符。

- **message-length maximum** {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}} - 设置最大 DNS 消息长度（512 至 65535 字节）。还可以设置客户端或服务器消息的最大长度。**auto** 关键字将最大长度设置为资源记录中的值。
- **nat-rewrite** - 根据 NAT 配置转换 DNS 记录。
- **protocol-enforcement**- 启用 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。
- **tcp-inspection**- 启用 TCP 上的 DNS 流量检测。确保 DNS/TCP 端口 53 流量是要应用 DNS 检测的类的一部分。该检测的默认类包括 TCP/53。
- **tsig enforced action** {[**drop**] [**log**]} - 要求必须有 TSIG 资源记录。可以**丢弃**和/或**记录**不符合要求的数据包。
- **umbrella** ［**tag** *umbrella_policy*］［**fail-open**］- 启用思科 Umbrella 并选择性地指定要应用于设备的思科 Umbrella 策略的名称 (**tag**)。如果未指定策略，则会应用默认策略。有关详细信息，请参阅思科 Umbrella。

  如果希望 DNS 解析在 Umbrella DNS 服务器不可用条件下运行，则请包含 **fail-open** 关键字。故障时打开的情况下，如果思科 Umbrella DNS 服务器不可用，则 Umbrella 会在该策略映射上自动禁用，并允许向系统上配置的其他 DNS 服务器发送 DNS 请求（若有）。当 DNS 服务器恢复可用状态时，策略映射会恢复使用它们。如果未包含该选项，则 DNS 请求会继续发送至无法访问的 Umbrella 解析器，因此这些请求不会收到任何回复。

示例：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
hostname(config-pmap-p)# message-length maximum 1024
hostname(config-pmap-p)# nat-rewrite
hostname(config-pmap-p)# protocol-enforcement
```

示例

以下示例显示如何在全局默认配置中使用新的检测策略映射：

```
regex domain_example “example\.com”
regex domain_foo “foo\.com”

! define the domain names that the server serves
class-map type inspect regex match-any my_domains
   match regex domain_example
   match regex domain_foo

! Define a DNS map for query only
class-map type inspect dns match-all pub_server_map
   match not header-flag QR
   match question
   match not domain-name regex class my_domains
```

```
policy-map type inspect dns new_dns_map
    class pub_server_map
        drop log
    match header-flag RD
        mask log
    parameters
        message-length maximum client auto
        message-length maximum 512
        dns-guard
        protocol-enforcement
        nat-rewrite

policy-map global_policy
 class inspection_default
  no inspect dns preset_dns_map
  inspect dns new_dns_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。请参阅配置应用层协议检测。

FTP 检测

默认情况下，FTP 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 FTP 检测引擎。

FTP 检测概述

FTP 应用检测用于检测 FTP 会话和执行四种任务：

- 为 FTP 数据传输准备动态辅助数据连接信道。这些信道的端口是通过 PORT 或 PASV 命令协商的。这些信道根据文件上传、文件下载或目录列表事件进行分配。
- 跟踪 FTP 命令响应序列。
- 生成审计追踪。
  - 为检索或上传的每个文件生成审核记录 303002。
  - 如果辅助动态信道准备因内存不足而失败，将会生成审核记录 201005。
- 转换嵌入式 IP 地址。

注释 如果禁用 FTP 检测，出站用户只能在被动模式下启动连接，而所有入站 FTP 将被禁用。

严格 FTP

严格 FTP 可防止 Web 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性。要启用严格 FTP，请在 **inspect ftp** 命令中包含 strict 选项。

在使用严格 FTP 时，您可以选择指定 FTP 检测策略映射来指定不允许通过 ASA 的 FTP 命令。

严格 FTP 检测将执行以下行为：

- 必须先确认 FTP 命令，然后 ASA 才允许使用新命令。
- ASA 丢弃发送嵌入式命令的连接。
- 检查 227 命令和 PORT 命令，以确保这些命令不显示在错误字符串中。

注意 使用严格 FTP 可能会导致没有严格遵从 FTP RFC 的 FTP 客户端故障。此外，您必须确保只对 FTP 端口进行检查（TCP/21 是正常的 FTP 端口）。对非 FTP 流量进行严格的 FTP 检查可能会导致意外的流量损失，尤其是 HTTP 流量。

使用严格 FTP 检测，系统会跟踪以下匿名活动的每个 FTP 命令和响应序列：

- 截断命令 - 检查 PORT 和 PASV 应答命令中逗号的数量是否是五个。如果不是五个，将会截断 PORT 命令并关闭 TCP 连接。
- 错误命令 - 检查 FTP 命令以确定它是否以 <CR><LF> 字符结尾（如 RFC 所要求）。如果不是，将会关闭连接。
- RETR 和 STOR 命令的大小 - 根据某个固定常数检查这些命令的大小。如果命令大小大于该固定常数，将会记录错误消息并关闭连接。
- 命令欺骗 - PORT 命令应始终从客户端发送。如果 PORT 命令是从服务器发送，将会拒绝 TCP 连接。
- 应答欺骗 - PASV 应答命令 (227) 应始终从服务器发送。如果 PASV 应答命令是从客户端发送，将会拒绝 TCP 连接。这样可防止用户执行“227 xxxxx a1, a2, a3, a4, p1, p2.”时出现安全漏洞
- TCP 流编辑 - 如果检测到 TCP 流编辑，ASA 将关闭连接。
- 无效的端口协商 - 检查协商的动态端口值是否小于 1024。由于 1 至 1024 范围内的端口号是为已知连接保留的，因此，如果协商的端口在这个范围内，将会释放 TCP 连接。
- 命令管道 - 将 PORT 和 PASV 应答命令中在端口号后显示的字符数与常数值 8 进行比较。如果该字符数大于 8，将会关闭 TCP 连接。
- ASA 将使用一系列 X 替代 FTP 服务器对 SYST 命令的响应，以防该服务器向 FTP 客户端泄露其系统类型。要覆盖此默认行为，请在 FTP 映射中使用 **no mask-syst-reply** 命令。

配置 FTP 检测策略映射

使用严格 FTP 检测可进行 FTP 命令过滤和安全检查，从而提高安全和加强控制。协议符合性包括数据包长度检查、分隔符和数据包格式检查、命令终止符检查以及命令验证。

也支持根据用户值阻止 FTP，这样，FTP 站点可以发布供下载的文件，但仅允许某些用户访问。可以根据文件类型、服务器名称及其他属性阻止 FTP 连接。如果进行检测后 FTP 连接被拒绝，将会生成系统消息日志。

如果希望 FTP 检测允许 FTP 服务器向 FTP 客户端显示其系统类型，并限制允许的 FTP 命令，可以创建并配置 FTP 检测策略映射。然后，可以在启用 FTP 检测时应用所创建的映射。

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 （可选）执行以下步骤创建 FTP 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 ftp** [**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**] **filename regex** {*regex_name* | **class** *class_name*} - 将 FTP 传输中的文件名与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **filetype regex** {*regex_name* | **class** *class_name*} - 将 FTP 传输中的文件类型与指定的正则表达式或正则表达式类进行匹配。

- **match** [**not**] **request-command** *ftp_command* [*ftp_command...*] - 匹配以下一个或多个 FTP 命令：
  - **APPE** - 附加到文件。
  - **CDUP** - 更改为当前工作目录的父目录。
  - **DELE** - 删除服务器上的文件。
  - **GET** - 从服务器获取文件。
  - **HELP** - 提供帮助信息。
  - **MKD** - 在服务器上创建目录。
  - **PUT** - 向服务器发送文件。
  - **RMD** - 在服务器上删除目录。
  - **RNFR** - 指定“rename-from”文件名
  - **RNTO** - 指定“rename-to”文件名
  - **SITE** - 用于指定服务器特定命令。此命令通常用于远程管理。
  - **STOU** - 用唯一文件名存储文件。
- **match** [**not**] **server regex** {*regex_name* | **class** *class_name*} - 将 FTP 服务器名称与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **username regex** {*regex_name* | **class** *class_name*} - 将 FTP 用户名与指定的正则表达式或正则表达式类进行匹配。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 FTP 检测策略映射：**policy-map type inspect ftp** *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 FTP 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 FTP 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) 输入下列命令，以指定要对匹配流量执行的操作：

- **reset** [**log**] - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。添加 **log** 关键字以发送系统日志消息。

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。

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：

- **mask-banner** - 掩蔽来自 FTP 服务器的问候横幅。
- **mask-syst-reply** 掩蔽对 **syst** 命令的应答。

示例

提交用户名和密码之前，所有 FTP 用户均可以看到问候横幅。默认情况下，该横幅包含对于试图发现系统缺陷的黑客来说很有用的版本信息。以下示例显示如何掩蔽该横幅：

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner

hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp

hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

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

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。

HTTP 检测

HTTP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 HTTP 端口，因此，只需简单地编辑默认全局检测策略即可添加 HTTP 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 HTTP 检测引擎。

HTTP 检测概述

使用 HTTP 检测引擎可防御特定攻击以及与 HTTP 流量相关的其他威胁。

HTTP 应用检测扫描 HTTP 报头和正文，并对数据执行各种检查。这些检查可防止各种 HTTP 构造、内容类型、隧道协议和消息传送协议通过安全设备。

增强型 HTTP 检测功能（又称为应用防火墙，在配置 HTTP 检测策略映射时可使用此功能）有助于防止攻击者使用 HTTP 消息来避开网络安全策略。

HTTP 应用检测可阻止通过隧道传送的应用以及 HTTP 请求和响应中的非 ASCII 字符，从而防止恶意内容到达 Web 服务器。还支持对 HTTP 请求和响应报头中的各个元素进行大小限制、URL 拦截以及 HTTP 服务器报头类型欺骗。

增强型 HTTP 检测验证所有 HTTP 消息是否满足以下条件：

- 符合 RFC 2616 的要求
- 仅使用 RFC 定义的方法。
- 符合其他条件。

配置 HTTP 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 HTTP 检测策略映射。然后，可以在启用 HTTP 检测时应用所创建的检测策略映射。

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 （可选）执行以下步骤创建 HTTP 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 http** [**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**] **req-resp content-type mismatch** - 匹配 HTTP 响应中的 content-type 字段与相应 HTTP 请求消息中的接受字段不匹配的流量。
- **match** [**not**] **request args regex** {*regex_name* | **class** *class_name*} - 将在 HTTP 请求消息参数中找到的文本与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **request body** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*} - 将在 HTTP 请求消息正文中找到的文本与指定的正则表达式或正则表达式类进行匹配，或者匹配请求正文长度大于指定长度的消息。
- **match** [**not**] **request header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*} - 将HTTP请求消息报头中字段的内容与指定的正则表达式或正则表达式类进行匹配。可以明确指定字段名称，或者将字段名称与正则表达式进行匹配。字段名称包括：accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。
- **match** [**not**] **request header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*} - 匹配HTTP请求消息报头中指定字段的长度或报头中的总字段数（数量）。可以明确指定字段名称，或者将字段名称与正则表达式或正则表达式类进行匹配。上一要点中列出了字段名称。
- **match** [**not**] **request header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**} - 匹配 HTTP 请求消息报头的总长度、报头中的总字段数（数量）或包含非 ASCII 字符的报头。
- **match** [**not**] **request method** {*method* | **regex** {*regex_name* | **class** *class_name*}} - 匹配 HTTP 请求方法。可以明确指定方法，或者将方法与正则表达式进行匹配。方法包括：bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。
- **match** [**not**] **request uri** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*} - 将 HTTP 请求消息URI中找到的文本与指定的正则表达式或正则表达式类进行匹配，或者匹配请求URI长度大于指定长度的消息。

- **match** [**not**] **response body** {**active-x** | **java-applet** | **regex** {*regex_name* | **class** *class_name*}} - 将 HTTP 响应消息正文中找到的文本与指定的正则表达式或正则表达式类进行匹配，或者注释掉 Java 小应用程序和 Active X 对象标签以便对其进行过滤。
- **match** [**not**] **response body length gt** *bytes* - 匹配正文长度大于指定长度的 HTTP 响应消息。
- **match** [**not**] **response header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*} }- 将 HTTP 响应消息报头中字段的内容与指定的正则表达式或正则表达式类进行匹配。可以明确指定字段名称，或者将字段名称与正则表达式进行匹配。字段名称包括：accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。
- **match** [**not**] **response header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*} - 匹配 HTTP 响应消息报头中指定字段的长度或报头中的总字段数（数量）。可以明确指定字段名称，或者将字段名称与正则表达式或正则表达式类进行匹配。上一要点中列出了字段名称。
- **match** [**not**] **response header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**} - 匹配 HTTP 响应消息报头的总长度、报头中的总字段数（数量）或包含非 ASCII 字符的报头。
- **match** [**not**] **response status-line regex** {*regex_name* | **class** *class_name*} - 将 HTTP 响应消息状态行中找到的文本与指定的正则表达式或正则表达式类进行匹配。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 HTTP 检测策略映射：**policy-map type inspect http** *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 HTTP 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 HTTP 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**] - 丢弃数据包并关闭连接。
- **reset** [**log**] - 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。

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：

- **body-match-maximum** *number* - 设置应在正文匹配中搜索的 HTTP 消息正文中的最大字符数。默认值为 200 字节。字符数量大将会对性能造成明显影响。
- **protocol-violation action** {**drop-connection** [**log**] | **reset** [**log**] | **log**} - 检查 HTTP 协议违规情况。必须选择要对违规情况执行的操作（断开连接、重置连接或记录连接）以及是否启用或禁用日志记录。
- **spoof-server** *string* - 替代服务器报头字段的字符串。WebVPN 流不受 spoof-server 命令影响。

示例

以下示例显示如何定义如下 HTTP 检测策略映射：允许并记录使用“GET”或“PUT”方法尝试访问“www\.xyz.com/.*\.asp”或“www\.xyz[0-9][0-9]\.com”的任何 HTTP 连接。默认允许 URL/方法的所有其他组合。

```
hostname(config)# regex url1 “www\.xyz.com/.*\.asp”
hostname(config)# regex url2 “www\.xyz[0-9][0-9]\.com”
hostname(config)# regex get “GET”
hostname(config)# regex put “PUT”

hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit

hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit

hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit

hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

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。

ICMP 检查

ICMP 检测引擎允许 ICMP 流量具有“会话”，这样可以像对 TCP 和 UDP 流量那样对这种流量进行检测。如果没有 ICMP 检测引擎，我们建议您在 ACL 中不要允许 ICMP 通过 ASA。如果不进行状态检测，ICMP 可能被用于攻击网络。ICMP 检测引擎确保每个请求只有一个响应，并确保序列号是正确的。

但是，即使已启用 ICMP 检测，也绝不会检测定向到 ASA 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。

注释 即使禁用了 ICMP 检查，NAT 也会在转换数据包时使用 ICMP 检测。

有关启用 ICMP 检测的信息，请参阅配置应用层协议检测。

ICMP 错误检测

当启用 ICMP 错误检测时，ASA 将基于 NAT 配置为发送 ICMP 错误消息的中间跃点创建转换会话。ASA 将使用转换的 IP 地址覆盖数据包。

禁用时，ASA 不会为生成 ICMP 错误消息的中间节点创建转换会话。内部主机与 ASA 之间的中间节点生成的 ICMP 错误消息将会到达外部主机，而不占用任何其他 NAT 资源。如果外部主机使用 traceroute 命令来跟踪连接 ASA 内部目标的跃点，这种方式则不合适。当 ASA 不转换中间跃点时，显示的所有中间跃点将带有映射目标 IP 地址。

注释 如果有可能对 ICMP 数据包使用 NAT，则应始终启用 ICMP 错误检测。由于 NAT 会自动使用 ICMP 检测 ICMP 数据包，因此即使您禁用了 ICMP 检测，使用映射的目标地址作为源地址也会让人觉得扫描仪正在检查您的网络。例如，在未启用 ICMP 错误检测的情况下，如果回应请求数据包的目标已被转换，那么当它被嵌入到 ICMP 超时响应中时，超时请求的外层报头就会使用被转换的目标作为源地址。如果启用 ICMP 错误检测，超时源地址将被设置为正确值。

有关启用 ICMP 错误检测的信息，请参阅配置应用层协议检测。

ILS 检测

互联网定位器服务 (ILS) 检测引擎为使用 LDAP 与 ILS 服务器交换目录信息的 Microsoft NetMeeting、SiteServer 和 Active Directory 产品提供 NAT 支持。在 ILS 检测中不能使用 PAT，因为只有 LDAP 数据库会存储 IP 地址。

为了搜索响应，当 LDAP 服务器位于外部时，请考虑使用 NAT 以允许内部对等体在注册到外部 LDAP 服务器时进行本地通信。如果无需使用 NAT，我们建议您关闭检测引擎以提供更好的性能。

当 ILS 服务器位于 ASA 边界内时，可能需要进行其他配置。这就需要提供一个孔来让外部客户端在指定的端口（通常为 TCP 389）上访问 LDAP 服务器。

注释 由于 ILS 流量（H225 呼叫信号）仅出现在辅助 UDP 信道上，因此，过了 TCP 非活动间隔后，TCP 连接将断开。默认情况下，此间隔为 60 分钟，且可使用 TCP **timeout** 命令进行调整。在 ASDM 中，可在 **Configuration > Firewall > Advanced > Global Timeouts** 窗格上完成此操作。

ILS 检测存在如下局限性：

- 不支持推荐请求和响应。
- 多个目录中的用户不统一。
- NAT 无法标识多个目录中具有多个身份的单一用户。

有关启用 ILS 检测的信息，请参阅配置应用层协议检测。

即时消息检测

使用即时消息 (IM) 检测引擎可以控制 IM 的网络使用情况，以及阻止机密数据泄露、蠕虫传播和针对公司网络的其他威胁。

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

如果决定实施 IM 检测，还可以配置 IM 检测策略映射来指定消息违反参数时采取的操作。以下操作步骤介绍 IM 检测策略映射。

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 （可选）执行以下步骤创建 IM 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 im** [**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**] **protocol {im-yahoo | im-msn}** - 匹配特定 IM 协议（Yahoo 或 MSN）。
- **match** [**not**] **service {chat | file-transfer** | **webcam** | **voice-chat** | **conference** | **games}** - 匹配特定 IM 服务。
- **match** [**not**] **login-name regex** {*regex_name* | **class** *class_name*} - 将 IM 消息的源客户端登录名与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **peer-login-name regex** {*regex_name* | **class** *class_name*} - 将 IM 消息的目标对等体登录名与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **ip-address** *ip_address mask*} - 匹配 IM 消息的源 IP 地址和掩码。
- **match** [**not**] **peer-ip-address** *ip_address mask*} - 匹配 IM 消息的目标 IP 地址和掩码。
- **match** [**not**] **version regex** {*regex_name* | **class** *class_name*} - 将 IM 消息的版本与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*} - 将 IM 消息的文件名与指定的正则表达式或正则表达式类进行匹配。MSN IM 协议不支持这种匹配。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 IM 检测策略映射：**policy-map type inspect im** *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 IM 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 IM 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) 输入下列命令，以指定要对匹配流量执行的操作：

- **drop-connection** [**log**] - 丢弃数据包并关闭连接。
- **reset** [**log**] - 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。

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

以下示例显示如何定义 IM 检测策略映射。

```
hostname(config)# regex loginname1 “ying\@yahoo.com”
hostname(config)# regex loginname2 “Kevin\@yahoo.com”
hostname(config)# regex loginname3 “rahul\@yahoo.com”
hostname(config)# regex loginname4 “darshant\@yahoo.com”
hostname(config)# regex yahoo_version_regex “1\.0”
hostname(config)# regex gif_files “.*\.gif”
hostname(config)# regex exe_files “.*\.exe”

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type inspect im match-any yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex
```

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

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

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。

IP 选项检测

您可以配置 IP 选项检测，以便基于数据包信头 IP Options 字段的内容控制允许的 IP 数据包。您可以丢弃包含不需要选项的数据包、清除选项（并允许数据包）或者允许该数据包而不做任何更改。

IP选项可提供某些情景下需要的控制功能，但在大多数常规通信中可能并不需要这些功能。特别是，IP选项包括时间戳、安全性和特殊路由的调配。并非必须使用IP选项，此字段可能包括零个、一个或多个选项。

有关 IP 选项的列表以及相关 RFC 的参考，请参阅 IANA 页面 (http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml)。

默认情况下已启用 IP 选项检测，但仅限 RSVP 流量。仅当您需要允许默认映射所允许的选项之外的其他选项，或当您需要通过使用非默认检测流量类映射将其应用于其他类型的流量时，才需要配置它。

注释 IP 选项检测不适用于分段的数据包。例如，分段中的选项不会被清除。

以下部分介绍 IP 选项检测。

IP 选项检测默认设置

默认情况下，仅为RSVP流量启用IP选项检测，其中会使用 _default_ip_options_map 检测策略映射。

- 允许使用 Router Alert 选项。

  此选项通知传输路由器检测数据包的内容，即使数据包未流向该路由器。实施 RSVP 以及实施需要路由器沿着数据包传送路径进行相对复杂的处理的类似协议时，这项检测很有用。丢弃包含 Router Alert 选项的 RSVP 数据包可能会导致 VoIP 的实施出现问题。

- 包含任何其他选项（包括不受支持的选项）的

  每次数据包因检测而被丢弃时，都会发出系统日志 106012。该消息会显示是哪个选项导致数据包被丢弃。使用 **show service-policy inspect ip-options** 命令可查看每个选项的统计信息。

以下是策略映射配置：

```
policy-map type inspect ip-options _default_ip_options_map
 description Default IP-OPTIONS policy-map
 parameters
  router-alert action allow
```

配置 IP 选项检测策略映射

如果要执行非默认 IP 选项检测，请创建一个 IP 选项检测策略映射来指定您希望如何处理每种选项类型。

过程

步骤 1 创建 IM 检测策略映射：**policy-map type inspect ip-options** *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 标识希望允许的选项。

可以检测以下选项。在所有情况下，**allow** 操作允许包含指定选项且未经过修改的数据包；**clear** 操作允许包含指定选项的数据包，但会从报头中删除该选项。

使用命令的 **no** 形式可从映射中删除该选项。任何包含映射中未包括的选项的数据包都会被丢弃，即使数据包中包含其他允许或清除的选项。

有关 IP 选项的列表以及相关 RFC 的参考，请参阅 IANA 页面 (http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml)。

- **default action** {**allow** | **clear**} - 为映射中未显式包括的任何选项设置默认操作。如果未设置默认操作 allow 或 clear，包含不允许的选项的数据包将被丢弃
- **basic-security action** {**allow** | **clear**} - 允许或清除“安全”(SEC) 选项。
- **commercial-security action** {**allow** | **clear**} - 允许或清除“商业安全”(CIPSO) 选项。
- **eool action** {**allow** | **clear**} - 允许或清除“选项列表末尾”选项。
- **exp-flow-control action** {**allow** | **clear**} - 允许或清除“实验流控制”(FINN) 选项。

- **exp-measurement action** {**allow** | **clear**} - 允许或清除“实验测量值”(ZSU) 选项。
- **extended-security action** {**allow** | **clear**} - 允许或清除“扩展安全”(E-SEC) 选项。
- **imi-traffic-descriptor action** {**allow** | **clear**} - 允许或清除“IMI 流量描述符”(IMITD) 选项。
- **nop action** {**allow** | **clear**} - 允许或清除“未运行”选项。
- **quick-start action** {**allow** | **clear**} - 允许或清除“快速启动”(QS) 选项。
- **record-route action** {**allow** | **clear**} - 允许或清除“记录路由”(RR) 选项。
- **router-alert action** {**allow** | **clear**} - 允许或清除“路由器警报”(RTRALT) 选项。
- **timestamp action** {**allow** | **clear**} - 允许或清除“时间戳”(TS) 选项。
- {**0-255**} **action** {**allow** | **clear**} - 允许或清除根据选项类型编号标识的选项。该编号是完整的选项类型，八位数（副本、类和选项编号），而不只是八位数的选项编号部分。这些选项类型可能不代表实际选项。非标准选项必须采用互联网协议 RFC 791 定义的预期 type-length-value 格式 (http://tools.ietf.org/html/rfc791)。

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。

IPsec 穿透检测

IPsec 穿透检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 IPsec 端口，因此，只需简单地编辑默认全局检测策略即可添加 IPsec 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 IPsec 穿透检测引擎。

IPsec 穿透检测概述

互联网协议安全 (IPsec) 是一个协议集，用于通过验证和加密数据流的每个 IP 数据包来保护 IP 通信。IPsec 还包括用于会话开始时在代理之间建立相互身份验证以及用于协商将在会话期间使用的加密密钥的协议。IPsec 可用于保护一对主机之间（例如，计算机用户或服务器）、一对安全网关之间（例如，路由器或防火墙）或安全网关与主机之间的数据流。

IPSec 穿透应用检测使得与 IKE UDP 端口 500 连接相关的 ESP （IP 协议 50）和 AH（IP 协议 51）流量可以轻松地通过。这项检测避免了为允许 ESP 和 AH 流量而需要进行冗长的 ACL 配置，并使用超时和最大连接数实现安全性。

可以为 IPsec 穿透检测配置策略映射，以指定 ESP 或 AH 流量的限制。可以为每个客户端设置最大连接数和空闲超时。

允许 NAT 流量和非 NAT 流量。但是，不支持 PAT。

配置 IPsec 穿透检测策略映射

通过 IPsec 穿透映射可以更改用于 IPSec 穿透应用检测的默认配置值。借助 IPsec 穿透映射，无需使用 ACL 即可允许某些数据流。

配置包括默认映射 _default_ipsec_passthru_map，该默认映射设置每个客户端的最大 ESP 连接数，并将 ESP 空闲超时设置为 10 分钟。仅在需要非默认值或者需要设置 AH 值的情况下，才需要配置检测策略映射。

过程

步骤 1 创建 IPsec 穿透检测策略映射：**policy-map type inspect ipsec-pass-thru** *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：

- **esp per-client-max** *number* **timeout** *time* - 允许 ESP 隧道并设置每个客户端的最大允许连接数和空闲超时（格式为 hh:mm:ss）。要允许无限连接数，请指定 0。
- **ah per-client-max** *number* **timeout** *time* - 允许 AH 隧道。这些参数的含义与 esp 命令的含义相同。

示例

以下示例显示如何使用 ACL 来标识 IKE 流量、定义 IPsec 穿透参数映射、定义策略以及将策略应用于外部接口：

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

Ipv6 检测

IPv6 检测根据扩展报头有选择性地记录或丢弃 IPv6 流量。此外，IPv6 检测可以检查 Pv6 数据包中扩展报头的类型和顺序是否符合 RFC 2460 的要求。

IPv6 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。可以简单地编辑默认全局检测策略来添加 IPv6 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

IPv6 检测默认设置

如果启用 IPv6 检测但不指定检测策略映射，将会使用默认 IPv6 检测策略映射并执行以下操作：

- 仅允许已知的 IPv6 扩展报头。丢弃并记录不符合要求的数据包。
- 按照 RFC 2460 规范的规定实施 IPv6 扩展报头顺序。丢弃并记录不符合要求的数据包。
- 丢弃带有路由类型报头的任何数据包。

以下是策略映射配置：

```
policy-map type inspect ipv6 _default_ipv6_map
 description Default IPV6 policy-map
 parameters
  verify-header type
  verify-header order
 match header routing-type range 0 255
  drop log
```

配置 IPv6 检测策略映射

要标识要丢弃或记录的扩展报头，或者要禁用数据包验证，请创建 IPv6 检测策略映射以用于服务策略。

过程

步骤 1 创建 IPv6 检测策略映射：**policy-map type inspect ipv6** *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 IPv6 消息中的报头丢弃或记录流量。

a) 根据 IPv6 报头标识流量：**match header** *type*

其中 *type* 是下列项目之一：

- **ah** - 匹配 IPv6 身份验证扩展报头。
- **count gt** *number* - 指定 IPv6 扩展报头的最大数量（0 至 255）。

- **destination-option** - 匹配 IPv6 目标选项扩展报头。
- **esp** - 匹配 IPv6 封装安全负载 (ESP) 扩展报头。
- **fragment** - 匹配 IPv6 分片扩展报头。
- **hop-by-hop** - 匹配 IPv6 逐跳扩展报头。
- **routing-address count gt** *number* - 设置 IPv6 路由报头类型 0 地址的最大数量（大于 0 至 255 之间的值）。
- **routing-type** {**eq** | **range**} *number* - 匹配 IPv6 路由报头类型（0 至 255）。对于范围，请用空格将各个值隔开，例如，**30 40**。

b) 指定要对匹配的数据包执行的操作。可以丢弃数据包和（可选）记录数据包，或者只记录数据包。如果未输入操作，将会记录数据包。

- **drop [log]** - 丢弃匹配的所有数据包。
- **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。

c) 重复以上步骤，直至标识出所有要丢弃或记录的报头。

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：

- **verify-header type** - 仅允许已知的 IPv6 扩展报头。
- **verify-header order** - 按照 RFC 2460 的规定实施 IPv6 扩展报头顺序。

示例

以下示例创建的检测策略将会丢弃并记录带有逐跳报头、目标选项报头、路由地址报头和路由类型 0 报头的所有 IPv6 数据包。此示例还强制报头顺序和类型。

```
policy-map type inspect ipv6 ipv6-pm
 parameters
  verify-header type
  verify-header order
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
```

```
 match header routing-type eq 0
  drop log

policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
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。

NetBIOS 检测

NetBIOS 应用检测对 NetBIOS 名称服务 (NBNS) 数据包和 NetBIOS 数据报服务数据包中嵌入的 IP 地址执行 NAT。这项检测还会检查各个数量字段和长度字段的一致性，从而强制执行协议符合性。

默认情况下，NetBIOS 检测已启用。或者可以创建策略映射以便丢弃或记录 NetBIOS 协议违规情况。以下操作步骤介绍如何配置 NetBIOS 检测策略映射。

过程

步骤 1 创建 NetBIOS 检测策略映射：**policy-map type inspect netbios** *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 指定要对 NETBIOS 协议违规采取的操作：**protocol-violation action** {**drop** [**log**] | **log**}

其中，**drop** 操作丢弃数据包。如果策略映射与流量匹配，**log** 操作将会发送系统日志消息。

示例

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop log

hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# no inspect netbios
```

```
hostname(config-pmap-c)# inspect netbios netbios_map
```

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。

PPTP 检测

PPTP 是用于对 PPP 流量进行隧道传送的协议。PPTP 会话通常包括一个 TCP 信道和两个 PPTP GRE 隧道。TCP 信道是用于协商和管理 PPTP GRE 隧道的控制信道。GRE 隧道在两台主机之间传送 PPP 会话。

启用后，PPTP 应用检测会检查 PPTP 协议数据包，并动态创建允许 PPTP 流量所需的 GRE 连接和转换。

特别是，ASA 会检测 PPTP 版本通知和对外呼叫请求/响应序列。如 RFC 2637 所要求，仅检测 PPTP 版本 1。如果任一端公布的版本不是版本 1，将会禁用对 TCP 控制信道的进一步检测。此外，还会跟踪传出呼叫请求和应答序列。会根据需要动态分配连接和转换，以允许后续辅助GRE数据流量。

要以 PAT 方式转换 PPTP 流量，必须启用 PPTP 检测引擎。此外，仅对符合如下条件的 GRE 版本执行 PAT：经过修改的（如 RFC2637 所要求）；且是通过 TCP 控制信道协商的。不会对未经修改的 GRE 版本执行 PAT（如 RFC 1701 和 RFC 1702 所要求）。

有关启用 PPTP 检测的信息，请参阅配置应用层协议检测。

RSH 检测

默认情况下，RSH 检测已启用。RSH 协议在 TCP 端口 514 上使用从 RSH 客户端到 TCP RSH 服务器的连接。客户端和服务器协商出 TCP 端口号，客户端会在该端口上侦听 STDERR 输出流。如有必要，RSH 检测支持协商端口号的 NAT。

有关启用 RSH 检测的信息，请参阅配置应用层协议检测。

SMTP 和扩展 SMTP 检测

ESMTP 检测可检测垃圾邮件、网络钓鱼、变形邮件等攻击和缓冲流量上溢/下溢攻击。另外，它还支持应用安全和协议符合性（实施 ESMTP 消息合理性检查及冻结发件人/收件人）并可冻结邮件中继。

默认情况下，ESMTP 检测已启用。仅在希望实施的措施不同于默认检测映射提供的处理操作时，才需要配置该检测。

以下各节介绍 ESMTP 检测引擎。

SMTP 和 ESMTP 检测概述

扩展 SMTP (ESMTP) 应用检测通过限制可通过 ASA 的 SMTP 命令类型和添加监控功能，加强对基于 SMTP 的攻击的防御。ESMTP 是增强型 SMTP 协议，在大多数方面和 SMTP 类似。

ESMTP 应用检测可控制和减少用户可使用的命令数以及服务器返回的消息数。ESMTP 检测主要执行三种任务：

- 将 SMTP 请求限制为七个基本 SMTP 命令和八个扩展命令。支持的命令如下：
  - 扩展 SMTP - AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS 和 VRFY。
  - SMTP (RFC 821) - DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET。
- 监控 SMTP 命令-响应序列。
- 生成审核线索 - 邮件地址中嵌入的无效字符被替换时，会生成审核记录 108002。有关详细信息，请参阅 RFC 821。

ESMTP 检测可监控以下异常签名的命令和响应序列：

- 截断的命令。
- 命令终止错误（不是以 <CR><LR> 终止）。
- MAIL 和 RCPT 命令指定邮件的发件人和收件人。会扫描邮件地址以检测异常字符。竖线 (|) 将被删除（更改为空格）；“<”和“>”只能用于定义邮件地址（“>”前面必须有“<”）。
- SMTP 服务器执行的意外转换。
- 对于未知或不受支持的命令，检测引擎会将数据包中的所有字符更改为 X，它们将被内部服务器拒绝。这将会生成消息，例如“500 Command unknown: 'XXX'”。不完整的命令将被丢弃

  不支持的 ESMTP 命令为 ATRN、ONEX、VERB、CHUNKING 和专用扩展名。
- TCP 数据流编辑。
- 命令管道。

注释 启用 ESMTP 检测后，如果未监测以下命令，用于互动式 SMTP 的 Telnet 会话将被挂起：SMTP 命令必须至少为四个字符；它们必须使用回车符和换行符终止；您必须先等待响应，再发出下一个应答。

ESMTP 检测默认设置

默认情况下，ESMTP 检测已启用，其中会使用 _default_esmtp_map 检测策略映射。

- 会掩蔽服务器横幅。ESMTP 检测引擎将服务器 SMTP 横幅中的字符更改为星号，但对“2”、“0”、“0”字符除外。会忽略回车符 (CR) 和换行符 (LF)。
- 会允许已加密连接，但不进行检测。
- 不会查找发件人和收件人地址中的特殊字符，不会执行任何操作。
- 会丢弃并记录命令行长度大于 512 的连接。
- 会丢弃并记录有多于 100 个收件人的连接。
- 会记录正文长度超过 998 字节的消息。
- 会丢弃并记录报头行长度大于 998 的连接。
- 会丢弃并记录 MIME 文件名超过 255 个字符的消息。
- 会掩蔽匹配“others”的 EHLO 应答参数。

以下是策略映射配置：

```
policy-map type inspect esmtp _default_esmtp_map
 description Default ESMTP policy-map
 parameters
  mask-banner
  no mail-relay
  no special-character
  allow-tls
 match cmd line length gt 512
  drop-connection log
 match cmd RCPT count gt 100
  drop-connection log
 match body line length gt 998
  log
 match header line length gt 998
  drop-connection log
 match sender-address length gt 320
  drop-connection log
 match MIME filename length gt 255
  drop-connection log
 match ehlo-reply-parameter others
  mask
```

配置 ESMTP 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 ESMTP 检测策略映射。然后，可以在启用 ESMTP 检测时应用所创建的检测策略映射。

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 ESMTP 检测策略映射：**policy-map type inspect esmtp** *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**] **body** {**length** | **line length**} **gt** *bytes* - 匹配 ESMTP 消息正文长度或其行长度大于指定字节数的消息。
- **match** [**not**] **cmd verb** *verb1* [*verb2...*] - 匹配消息中的命令谓词。可以指定以下一个或多个命令：auth、data、ehlo、etrn、helo、help、mail、noop、quit、rcpt、rset、saml、soml、vrfy。
- **match** [**not**] **cmd line length gt** *bytes* - 匹配命令谓词中一行的长度大于指定字节数的消息。
- **match** [**not**] **cmd rcpt count gt** *count* - 匹配收件人数量大于指定数量的消息。
- **match** [**not**] **ehlo-reply-parameter** *parameter* [*parameter2...*] - 匹配 ESMTP EHLO 应答参数。可以指定以下一个或多个参数：8bitmime、auth、binaryname、checkpoint、dsn、etrn、others、pipelining、size、vrfy。
- **match** [**not**] **header** {**length** | **line length**} **gt** *bytes* - 匹配 ESMTP 报头长度或其行长度大于指定字节数的消息。
- **match** [**not**] **header to-fields count gt** *count* - 匹配报头中 To 字段数量大于指定数量的消息。
- **match** [**not**] **invalid-recipients count gt** *number* - 匹配无效收件人数量大于指定数量的消息。
- **match** [**not**] **mime filetype regex** {*regex_name* | **class** *class_name*} - 将 MIME 或媒体文件类型与指定的正则表达式或正则表达式类进行匹配。
- **match** [**not**] **mime filename length gt** *bytes* - 匹配文件名长度大于指定字节数的消息。
- **match** [**not**] **mime encoding** *type* [*type2...*] - 匹配 MIME 编码类型。可以指定以下一个或多个类型：7bit、8bit、base64、binary、others、quoted-printable。
- **match** [**not**] **sender-address 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发件人邮件地址。
- **match** [**not**] **sender-address length gt** *bytes* - 匹配发件人地址长度大于指定字节数的消息。

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**] - 丢弃数据包并关闭连接。
- **mask** [**log**] - 掩蔽数据包的匹配部分。此操作仅适用于 **ehlo-reply-parameter** 和 **cmd verb**。

- **reset** [**log**] - 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* - 限制数据包中每秒的消息速率。此选项仅适用于 **cmd verb**，其中可以将此选项用作唯一操作，也可以将其与 **mask** 操作一起使用。

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：

- **mail-relay** *domain-name* **action** {**drop-connection** [**log**] | **log**} - 标识用于邮件转发的域名。可以断开连接和（可选）记录连接，或者只记录连接。
- **mask-banner** - 掩蔽来自 ESMTP 服务器的横幅。
- **special-character action** {**drop-connection** [**log**] | **log**} - 标识要对发件人或收件人邮件地址中包含特殊字符（竖线 (|)、反引号和空字符）的消息执行的操作。可以断开连接和（可选）记录连接，或者只记录连接。
- **allow-tls** [**action log**] - 是否允许 ESMTP 在未经检测的情况下通过 TLS（加密连接）。如有需要，可以记录加密连接。默认设置为允许 TLS 会话，不进行检测。如果指定 **no allow-tls**，系统会从会话连接中去除 STARTTLS 指示符并强制执行纯文本连接。

示例

以下示例显示如何定义 ESMTP 检测策略映射。

```
hostname(config)# regex user1 “user1@cisco.com”
hostname(config)# regex user2 “user2@cisco.com”
hostname(config)# regex user3 “user3@cisco.com”
hostname(config)# class-map type regex senders_black_list
hostname(config-cmap)# description “Regular expressions to filter out undesired senders”
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced_esmtp_map
hostname(config-pmap)# match sender-address regex class senders_black_list
hostname(config-pmap-c)# drop-connection log

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

```
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map

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

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。

SNMP 检测

SNMP 应用检测同时适用于通过设备和通过设备的流量。如果您配置的 SNMP v3 将用户限制在特定 SNMP 主机上，则必须进行此检测。如果未检测，定义的 v3 用户可以从任何允许的主机轮询设备。默认端口已启用 SNMP 检测，因此只有在使用非默认端口时才需要进行配置。默认端口为 UDP/161、162（适用于所有设备类型），对于同时运行 FXOS 的设备，默认端口为 UDP/4161，因为 FXOS 监听 UDP/161。

默认情况下，SNMP 检测会将轮询限制为配置的版本。

注释 如果在同时运行 FXOS 的设备上配置 SNMP，则 SNMP 检测是强制性的，如果禁用，则会重新启用。在包含端口 UDP/4161 的流量类别映射上启用 SNMP 检测。

您还可以选择将 SNMP 流量进一步限制为特定版本的 SNMP。SNMP 早期版本的安全性较低；因此，安全策略可能要求拒绝使用某些 SNMP 版本。系统可能会拒绝 SNMP 1、2、2c 或 3 版本。如下所述，可以创建 SNMP 映射来控制允许的版本。如果不需要控制版本，只需启用 SNMP 检查，无需地图。

过程

创建 SNMP 映射。

使用 **snmp-map** *map_name* 命令创建映射，进入 SNMP 映射配置模式，然后使用 **deny version** *version* 命令标识不允许的版本。版本可能是 1、2、2c 或 3。

示例：

以下示例拒绝 SNMP 1 和 2 版本：

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

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。

SQL*Net 检测

系统已默认启用 SQL*Net 检测。检测引擎支持 SQL*Net 版本 1 和 2，但仅支持透明网络底层 (TNS) 格式。检测不支持表格数据流 (TDS) 格式。系统会扫描嵌入式地址和端口的 SQL*Net 消息，并在需要时应用 NAT 重写。

SQL*Net 的默认端口赋值为 1521。这是 Oracle 用于 SQL*Net 的值，但是，该值与结构化查询语言 (SQL) 的 IANA 端口赋值不符。如果您的应用使用其他端口，请对包含该端口的流量类应用 SQL*Net 检测。

在以下情况下禁用 SQL*Net 检测：

- SQL 数据传输端口与 SQL 控制 TCP 1521 端口相同。安全设备在启用 SQL*Net 检测之后充当代理，且将客户端窗口大小从 65000 缩小至大约 16000，从而导致数据传输问题。
- 对高速 SQL 流量的检查会导致 CPU 使用率出现不可接受的峰值。

禁用 SQL*Net 检测后，使用 **clear conn port 1521** 命令，以便可以在不进行检测的情况下重建连接。

有关启用 SQL*Net 检测的信息，请参阅配置应用层协议检测。

Sun RPC 检测

本节介绍 Sun RPC 应用检测。

Sun RPC 检测概述

Sun RPC 协议检测默认启用。只需管理 Sun RPC 服务器表，即可确定允许穿越防火墙的服务。但是，任何服务器的 NFS 针孔都会打开，即便没有服务器表配置。

Sun RPC 可供 NFS 和 NIS 使用。Sun RPC 服务可在任何端口上运行。当客户端尝试访问服务器上的 Sun RPC 服务时，必须获悉服务运行所在的端口。它通过查询端口映射程序流程执行此操作，通常为 rpcbind，位于公认端口 111。

客户端将发送服务的 Sun RPC 程序号，而端口映射程序流程将用服务的端口号进行响应。客户端发送其 Sun RPC 查询至服务器，指定端口映射程序流程识别的端口。当该服务器应答时，ASA 会拦截此数据包，并在该端口上同时打开初期 TCP 和 UDP 连接。

不支持 Sun RPC 负载信息的 NAT 或 PAT。

管理 Sun RPC 服务

使用 Sun RPC 服务表可基于建立的 Sun RPC 会话来控制 Sun RPC 流量。

过程

步骤 1 配置 Sun RPC 服务属性。

sunrpc-server *interface_name ip_address mask* **service** *service_type* **protocol** {**tcp** | **udp**} *port*[*-port*] **timeout** *hh:mm:ss*

其中：

- *interface_name* - 流量流向服务器数据流所通过的接口。
- *ip_address mask* - Sun RPC 服务器的地址。
- **service** *service_type* - 服务器上的服务类型，即特定服务类型与用于服务的端口号之间的映射。要确定服务类型（例如，100003），请在 Sun RPC 服务器计算机上的 UNIX 或 Linux 命令行处使用 **sunrpcinfo** 命令。
- **protocol** {**tcp** | **udp**} - 服务使用 TCP 还是 UDP。
- *port*[*-port*] - 服务使用的端口或端口范围。要指定端口范围，请使用连字符分隔范围中起始端口号和结束端口号（例如，111-113）。
- **timeout** *hh:mm:ss* - Sun RPC 检测为连接打开的针孔的空闲超时。

示例：

例如，要为使用 IP 地址 192.168.100.2 的 Sun RPC 服务器创建 30 分钟的超时，请输入以下命令。在此示例中，Sun RPC 服务器位于使用 TCP 端口 111 的内部接口上。

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255
service 100003 protocol tcp 111 timeout 00:30:00
```

步骤 2 （可选。）监控为这些服务创建的针孔。

要显示为 Sun RPC 服务打开的针孔，请输入 **show sunrpc-server active** 命令。例如：

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL 列中的条目显示内部接口上客户端或服务器的 IP 地址，而 FOREIGN 列中的值则显示外部接口上客户端或服务器的 IP 地址。

如有必要，可使用 清除这些服务 **clear sunrpc-server active**

TFTP 检测

默认情况下，TFTP 检测已启用。

如 RFC 1350 中所述，TFTP 是用于在 TFTP 服务器与客户端之间读取和写入文件的简单协议。

检测引擎检测 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)，并且如有必要，还会动态创建连接和转换，从而允许在 TFTP 客户端和服务器之间传输文件。

如有必要，在接收有效的读取 (RRQ) 或写入 (WRQ) 请求时会分配动态辅助信道和 PAT 转换。随后，TFTP 会使用该辅助信道进行文件传输或错误通知。

只有 TFTP 服务器可以通过辅助信道发起流量；此外，TFTP 客户端与服务器之间最多只能有一个不完整的辅助信道。服务器发出的错误通知会致使辅助信道关闭。

如果使用静态 PAT 重定向 TFTP 流量，则必须启用 TFTP 检测。

有关启用 TFTP 检测的信息，请参阅配置应用层协议检测。

XDMCP 检测

XDMCP 是使用 UDP 端口 177 来协商 X 会话（建立后使用 TCP）的协议。

为了成功协商和启动 XWindows 会话，ASA 必须允许来自 Xhosted 计算机的 TCP 向后连接。要允许该向后连接，可以使用访问规则来允许 TCP 端口。或者，也可以在 ASA 上使用 **established** 命令。在 XDMCP 协商用于发送显示内容的端口后，系统将调用 **established** 命令来验证是否应允许此向后连接。

在 XWindows 会话期间，管理器将与已知端口 6000 | n 上的显示器 Xserver 通信。使用以下终端设置，每个显示器都会独立连接到 Xserver。

```
setenv DISPLAY Xserver:n
```

其中 *n* 为显示器编号。

使用 XDMCP 时，系统将使用 IP 地址协商显示，以便 ASA 可在需要时应用 NAT。XDCMP 检测不支持 PAT。

有关启用 XDMCP 检测的信息，请参阅配置应用层协议检测。

VXLAN 检测

虚拟可扩展局域网 (VXLAN) 检测适用于流经 ASA 的 VXLAN 封装流量。该检测可确保 VXLAN 报头格式符合标准，丢弃所有格式错误的数据包。系统对于将 ASA 用作 VXLAN 隧道终端 (VTEP) 或 VXLAN 网关的流量不执行 VXLAN 检测，因为在解除 VXLAN 数据包封装的正常环节中会执行那些检测。

VXLAN 数据包为 UDP，通常在端口 4789 上。此端口是默认检测流量类的一部分，因此只需将 VXLAN 检测添加到 inspection_default 服务策略规则中即可。或者，也可以使用端口或 ACL 匹配创建一个类。

基本互联网协议检测的历史记录

功能名称	版本	功能信息
DCERPC 检测支持 ISystemMapper UUID 消息 RemoteGetClassObject opnum3。	9.4(1)	ASA 从版本 8.3 开始支持非 EPM DCERPC 消息，支持 ISystemMapper UUID 消息 RemoteCreateInstance opnum4。此更改扩展了对 RemoteGetClassObject opnum3 消息的支持。 未修改任何命令。
VXLAN 数据包检测	9.4(1)	ASA 可检查 VXLAN 报头以强制遵守标准格式。 引入了以下命令：**inspect vxlan**。
TLS 会话默认行为中的 ESMTP 检测变化。	9.4(1)	已将 ESMTP 检查的默认设置更改为允许 TLS 会话，这些会话不会被检查。不过，此默认设置适用于新的或重新映像的系统。如果您升级了包括 **no allow-tls** 的系统，则该命令不会更改。 还在以下早期版本中进行了此默认行为更改：8.4(7.25)、8.5(1.23)、8.6(1.16)、8.7(1.15)、9.0(4.28)、9.1(6.1)、9.2(3.2)、9.3(1.2)、9.3(2.2)。
改进了 IP 选项检测。	9.5(1)	IP 选项检测现在支持所有可能的 IP 选项。您可以对检测进行调整以允许、清除或丢弃任何标准的或试验性选项，包括尚未定义的选项。还可以为 IP 选项检测图中尚未明确定义的选项设置默认行为。 添加了以下命令：**basic-security**、 **commercial-security**、**default**、**exp-flow-control**、**exp-measure**、**extended-security**、**imi-traffic-description**、**quick-start**、**record-route**、**timestamp** 和 {**0-255**}（指示 IP 选项类型编号）。
DCERPC 检测改进和 UUID 过滤	9.5(2)	DCERPC 检测现在支持 OxidResolver ServerAlive2 opnum5 消息的 NAT。现在您可根据 DCERPC 消息通用唯一标识 (UUID) 进行过滤，以便重置或记录特定消息类型。新 DCERPC 检测类映射可用于 UUID 过滤。 引入了以下命令：**match** [**not**] **uuid**。修改了以下命令：**class-map type inspect**。

功能名称	版本	功能信息
通过 TCP 的 DNS 检测。	9.6(2)	现在，您可以检查通过 TCP 的 DNS 流量 (TCP/53)。 添加了以下命令：**tcp-inspection**。
思科 Umbrella 支持。	9.10(1)	您可以配置设备将 DNS 请求重定向至思科 Umbrella，以便将您在思科 Umbrella 中定义的企业安全策略应用于用户连接。您可以允许或阻止基于 FQDN 的连接，或者，对于可疑的 FQDN，您可以将用户重定向至思科 Umbrella 智能代理，该代理可以执行 URL 筛选。Umbrella 配置是 DNS 检测策略的一部分。 添加或修改了以下命令：**umbrella** (global and policy-map parameters configuration modes)、**token**、**public-key**、**timeout edns**、**dnscrypt**、**show service-policy inspect dns detail**。
思科 Umbrella 增强功能。	9.12(1)	您现在可以标识需要绕过思科 Umbrella 的本地域名。发向这些域的 DNS 请求将直接流向 DNS 服务器，而不经过 Umbrella 处理。此外，您还可以标识用于解析 DNS 请求的 Umbrella 服务器。最后，您可以定义 Umbrella 检测策略以实现故障时自动开放，以确保 Umbrella 服务器不可用时，DNS 请求不会被阻止。 添加或更改了以下命令：**local-domain-bypass**、**resolver**、**umbrella fail-open**。
XDMCP 检测在新安装中默认为禁用。	9.15(1)	以前，所有流量默认情况下都启用 XDMCP 检测。现在，在新安装（包括新系统和重新映像的系统）上，XDMCP 则默认处于关闭状态。如果需要这一检测功能，请启用它。请注意，升级时，您的 XDMCP 检测当前设置会保留，即使您只是通过默认检测设置启用了该设置。

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。