在ASDM 6.3及更高版本上配置IP选项检测

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[配置](#)
[ASDM 配置](#)
[Cisco ASA允许RSVP数据包的默认行为](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文档提供了配置思科自适应安全设备(ASA)以传递启用了某些IP选项的IP数据包的示例配置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本8.3及更高版本的Cisco ASA
- 运行软件版本6.3及更高版本的思科自适应安全管理器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

每个IP数据包都包含一个IP报头，其中包含一个“选项”字段。“选项”字段（通常称为IP选项）提供一些情况下需要的控制功能，但大多数常见通信都不需要这些功能。特别是，IP选项包括时间戳、安全和特殊路由的规定。IP选项的使用是可选的，字段可以包含零、一或多个选项。

IP选项是一种安全风险，如果启用了IP选项字段的IP数据包通过ASA，它会将有关网络内部设置的信息泄露给外部。因此，攻击者可以映射您的网络拓扑。由于Cisco ASA是在企业中实施安全的设备，因此默认情况下，它会丢弃已启用IP选项字段的数据包。此处显示了系统日志消息示例，供您参考：

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||IP10.110.1.34XX.YY.ZZ.ZZ,IP""
```

但是，在视频流量必须通过Cisco ASA的特定部署场景中，必须通过具有某些IP选项的IP数据包，否则视频会议呼叫可能会失败。从Cisco ASA软件版本8.2.2开始，引入了名为“IP选项检测”的新功能。通过此功能，您可以控制哪些具有特定IP选项的数据包可以通过Cisco ASA。

默认情况下，此功能已启用，并且全局策略中启用了以下IP选项的检查。配置此检查会指示ASA允许数据包通过，或清除指定的IP选项，然后允许数据包通过。

- **选项列表结束(EOOL)或IP选项0** — 此选项显示在所有选项的末尾，以标记选项列表的结尾。
- **无操作(NOP)或IP选项**1 — 此选项字段使字段的总长度变量。
- **路由器警报(RTRALT)或IP选项20** — 此选项通知中转路由器检查数据包的内容，即使数据包不是发往该路由器。

配置

本部分提供有关如何配置本文档所述功能的信息。

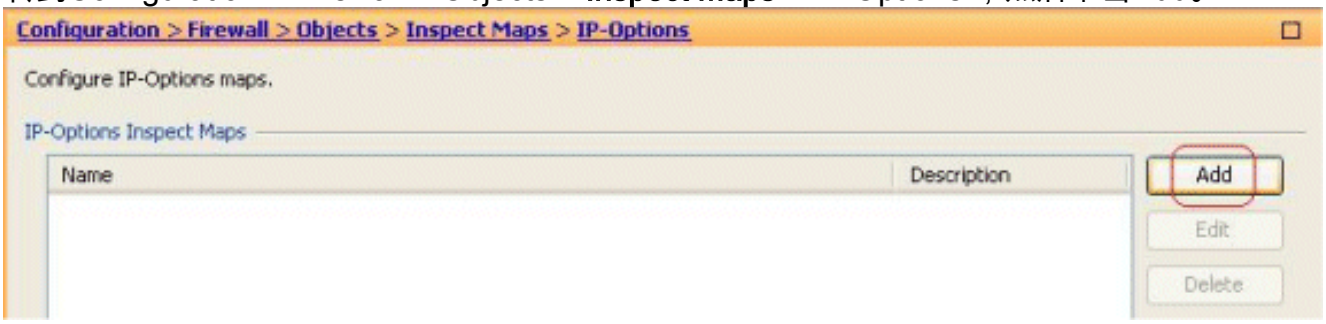
注意：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

ASDM 配置

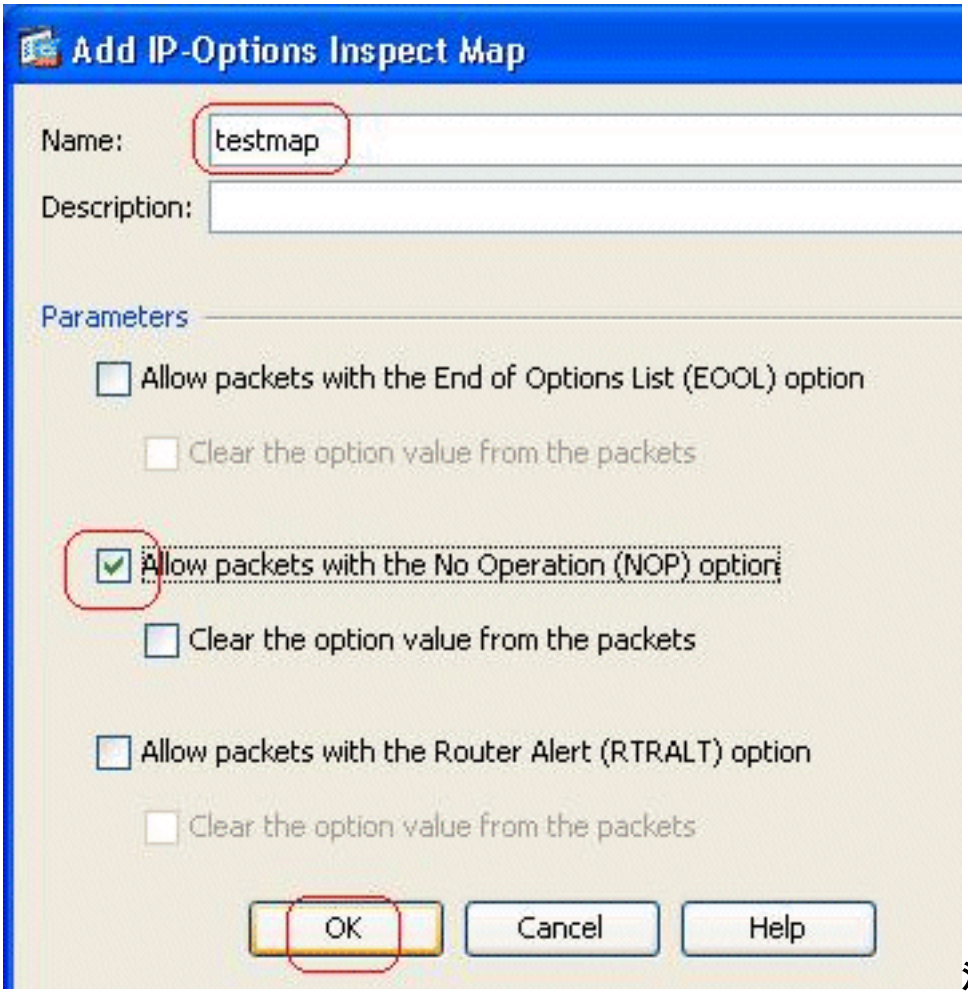
使用ASDM，您可以看到如何启用对具有IP选项字段NOP的IP数据包的检查。

IP报头中的Options字段可以包含零、一或多个选项，这使字段的总长度变量。但是，IP报头必须是32位的倍数。如果所有选项的位数不是32位的倍数，则NOP选项将用作“内部填充”，以便在32位边界上对齐选项。

1. 转到Configuration > Firewall > Objects > **Inspect Maps** > IP-Options ，然后单击Add。

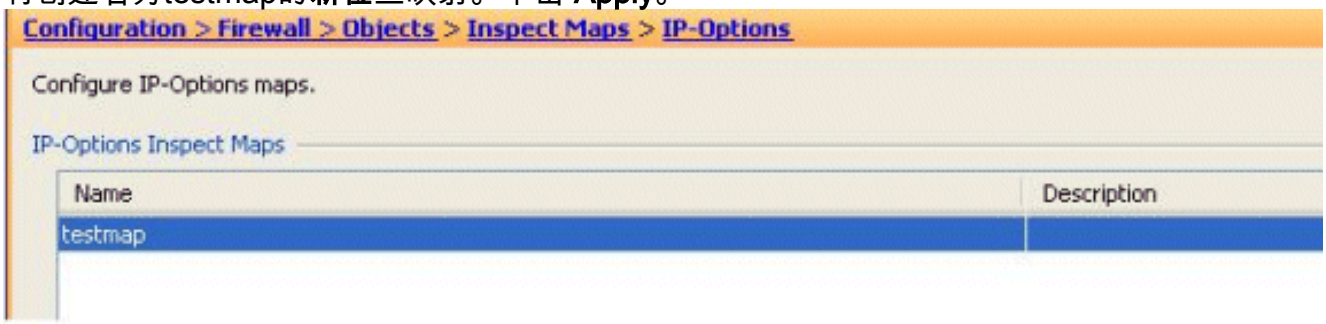


2. 系统将显示Add IP-Options Inspect Map窗口。指定Inspect Map的名称，选择Allow packets with the No Operation(NOP)**选项，然后单击OK**。

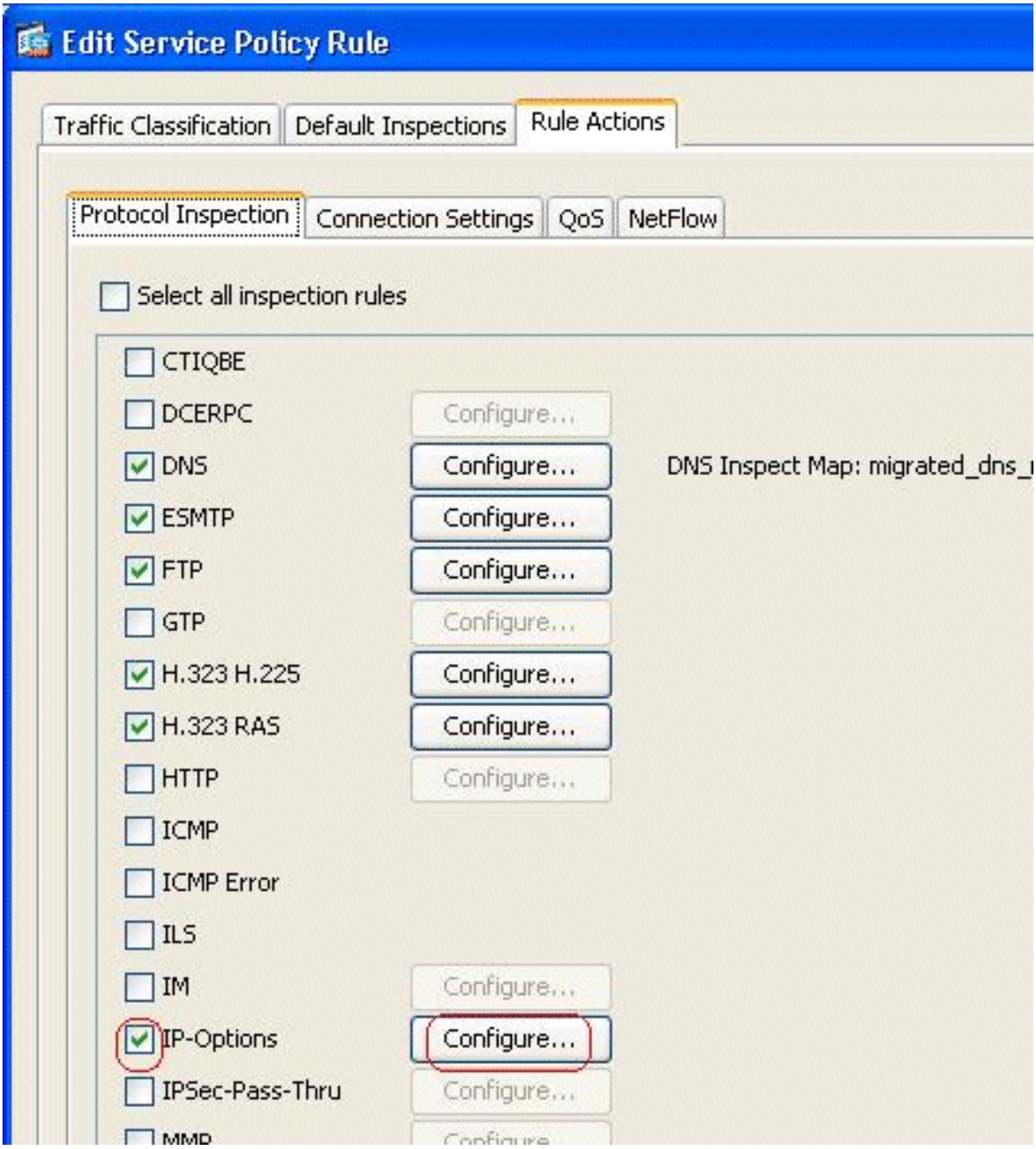


注意：您还可以选择**从数据包中清除选项值**，以便禁用IP数据包中的此字段，并且数据包通过Cisco ASA。

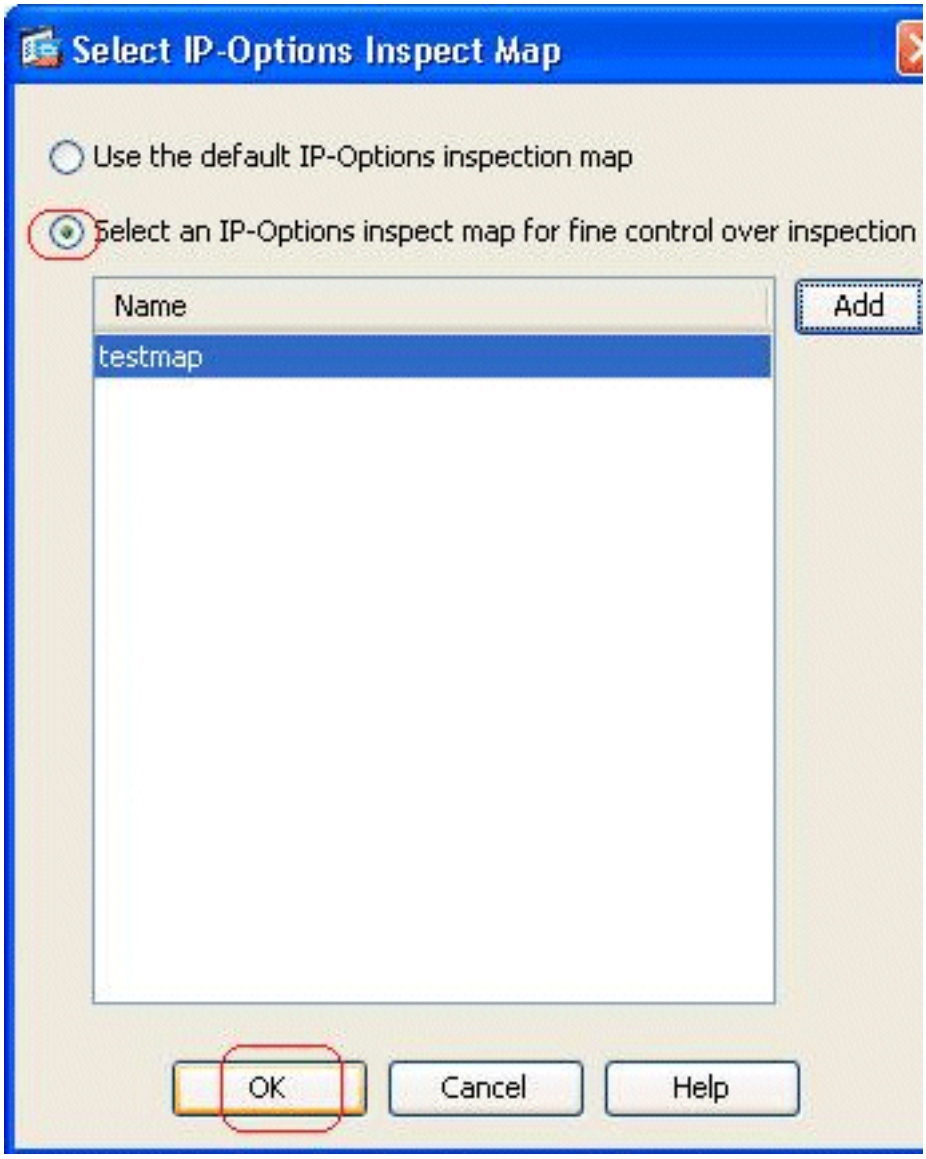
3. 将创建名为testmap的**新检**查映射。单击 **Apply**。



4. 转至**Configuration > Firewall > Service Policy Rules**，选择现有全局策略，然后单击**Edit**。系统将显示Edit Service Policy Rule窗口。选择**Rule Actions选**项卡，选中**IP-Options项**，然后选择**Configure**以分配新创建的检测映射。

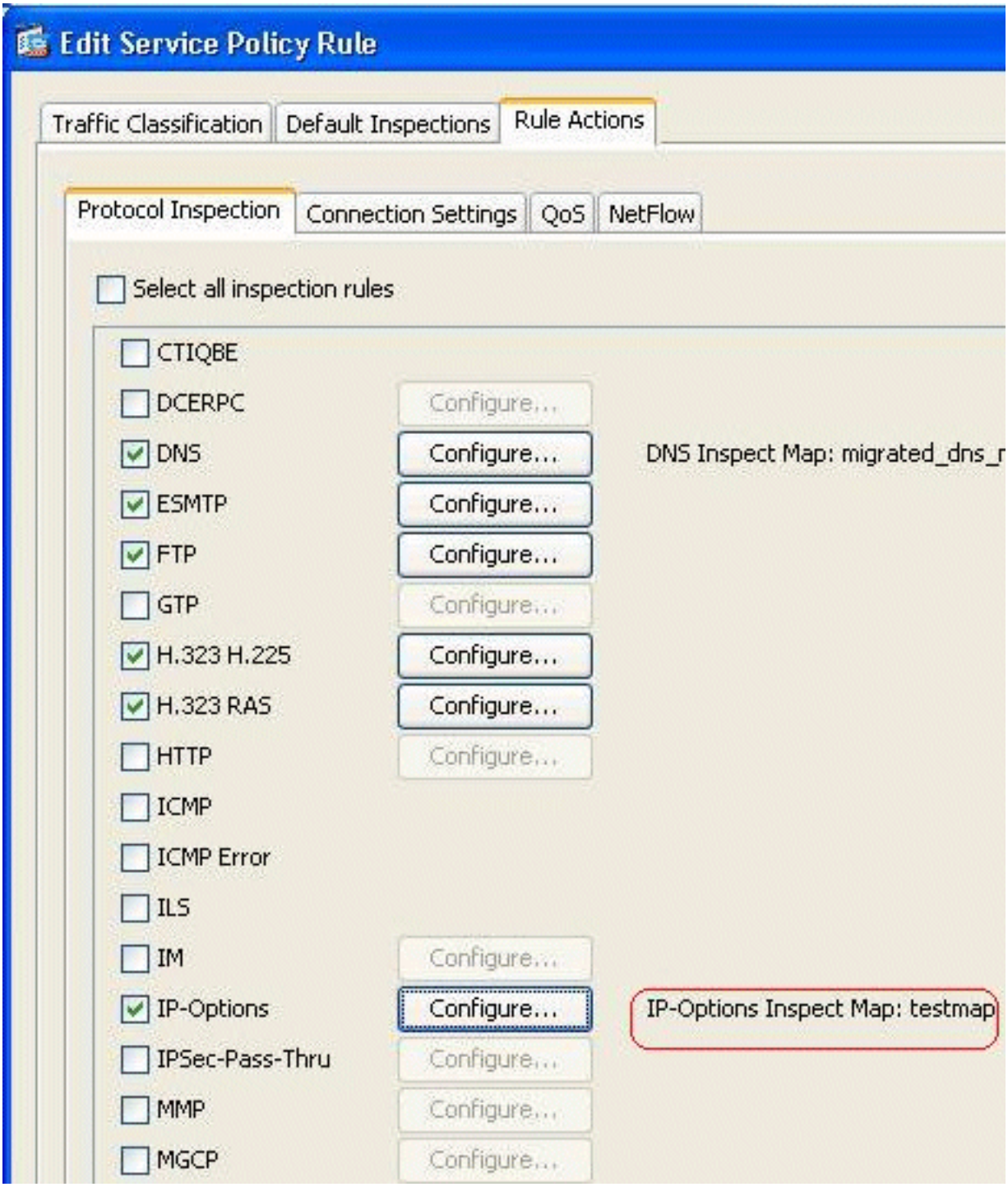


5. 选择Select an IP-Options inspect map for fine control over inspection > testmap，然后单击

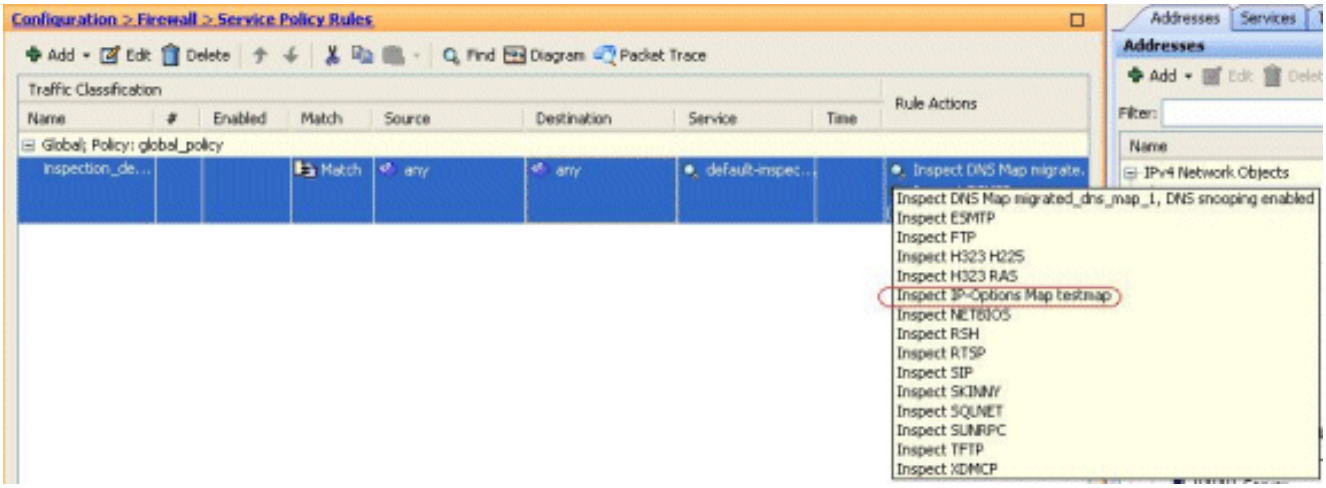


OK。

6. 可在IP-Options字段中查**看所选检查**映射。单击**OK**以恢复到Service Policy Rules选项卡。



7. 用鼠标将鼠标悬停在**Rule Actions**选项卡上，以便找到与此全局映射关联的所有可用协议检测映射。

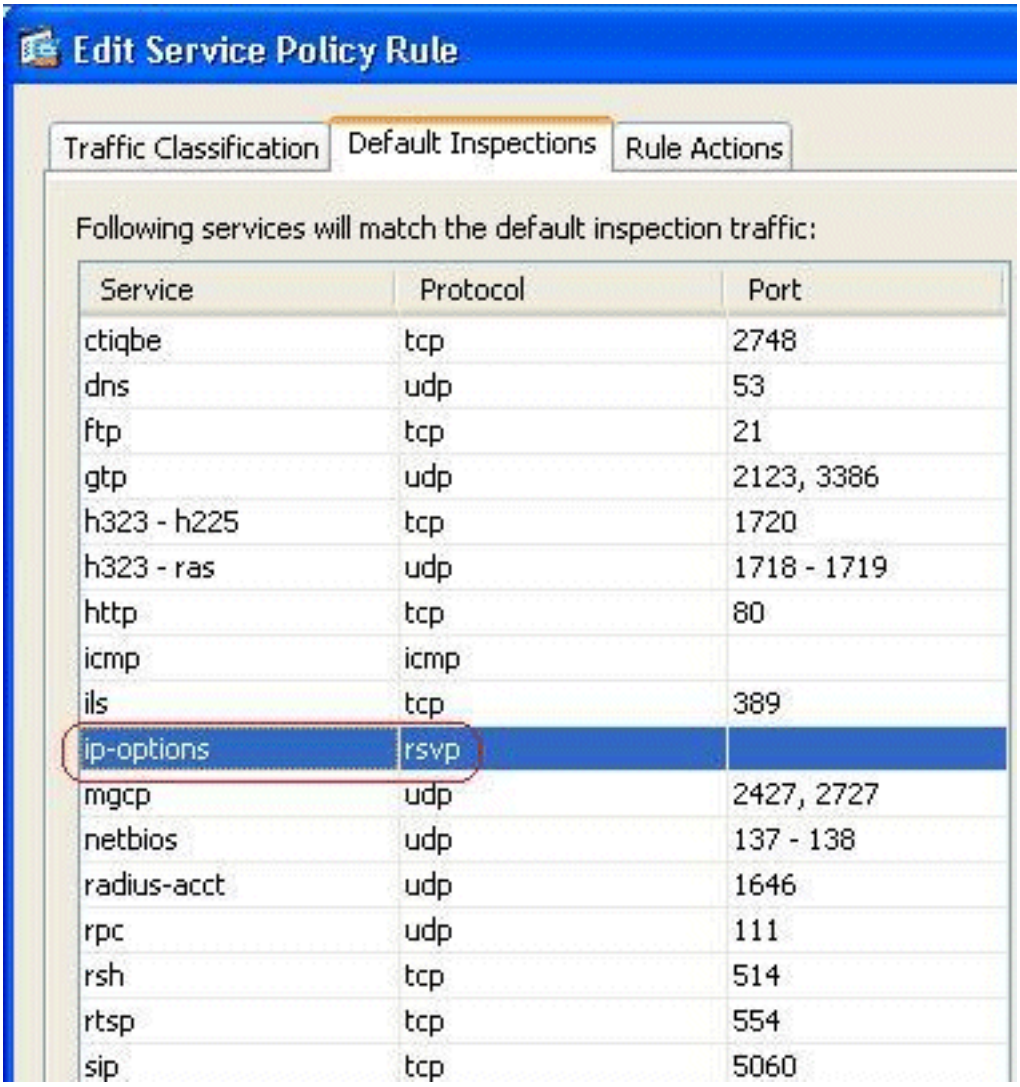


以下是等效CLI配置的示例片段，供您参考：

Cisco ASA
ciscoasa(config)#policy-map type inspect ip-options testmap ciscoasa(config-pmap)#parameters ciscoasa(config-pmap-p)#nop action allow ciscoasa(config-pmap-p)#exit ciscoasa(config)#policy-map global_policy ciscoasa(config-pmap)#class inspection_default ciscoasa(config-pmap-c)#inspect ip-options testmap ciscoasa(config-pmap-p)#exit ciscoasa(config)#write memory

Cisco ASA允许RSVP数据包的默认行为

默认情况下，IP选项检查处于启用状态。转到**Configuration > Firewall > Service Policy Rules**。选择Global Policy，单击**Edit**，然后选择**Default Inspections选**项卡。在此，您将在IP-Options字段中**找到RSVP协**议。这可确保RSVP协议通过Cisco ASA进行检查和允许。因此，建立端到端视频呼叫时不会出现任何问题。



验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show service-policy inspect ip-options** — 显示根据已配置的服务策略规则丢弃和/或允许的数据包数。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco ASA 5500系列自适应安全设备技术支持
- 技术支持和文档 - Cisco Systems