

ASDM 6.3及以后 : Ip options检查配置示例

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](#)

[思科ASA默认行为为了允许RSVP数据包](#)

[验证](#)

[故障排除](#)

[相关信息](#)

[简介](#)

本文提供配置示例如何配置思科可适应安全工具(ASA)为了传递有启用的某Ip options的IP信息包。

[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的Cisco ASA及以后
- Cisco可适应安全经理运行软件版本6.3及以后

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](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[背景信息](#)

每IP数据包包含与选项域的一IP报头。选项域，通常指Ip options，为最普通的通信提供要求在一些情况中的控制功能，但是多余。特别是，Ip options包括向时间戳、安全和特殊路由的提供。使用Ip options可选，并且字段能包含零个，一个，或者更多选项。

Ip options是安全风险，并且，如果与启用的Ip options字段的一IP数据包通过ASA通过，将泄漏关于网络的内部设置的信息对外部。结果，攻击者能映射您的网络拓扑。当思科ASA是在企业中强制执行安全，默认情况下，它的设备丢弃有启用的Ip options字段的数据包。示例系统消息表示此处，供您的参考：

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||Deny10.110.1.34IPXX.YY.ZZ.ZZ Ip options ""
```

然而，在视频流量必须穿过思科ASA的特定部署方案，有某Ip options的IP信息包必须通过视频会议呼叫通过可能否则发生故障。从Cisco ASA软件版本8.2.2向前，呼叫“Ip options的检查的”新特性介绍。使用此功能，您能控制有特定Ip options的哪些数据包通过思科ASA允许。

默认情况下，此功能启用，并且下面的Ip options的检查在全局策略启用。配置此检查指示ASA允许数据包通过，或者清除指定的Ip options然后允许数据包通过。

- **结尾选项列表(EOOL)或IP选项0** -此选项出现在所有选项结束时为了指示结尾的选项列表。
- **没有操作(NOP)或IP选项1** -此选项域做总长度字段变量。
- **路由器警报(RTRALT)或IP选项20** -此选项通知转接路由器检查数据包的内容，既使当数据包为该路由器不是注定的。

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： 使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

ASDM 配置

使用ASDM，您能看到如何启用有Ip options字段的IP信息包的检查，NOP。

IP报头的选项域能包含零个，一个，或者更多选项，做总长度字段变量。然而，IP报头必须是32个位的多个。如果位数量所有选项不是32个位的多个，NOP选项用于作为“内部填充符”为了对齐在32位边界的选项。

1. 去Configuration>防火墙>对象>Inspect映射>Ip options，并且单击添加。



2. Map窗口添加Ip options的Inspect出现。指定Inspect地图的名称，选择允许有没有操作(NOP)选项的数据包，并且点击OK键。

Add IP-Options Inspect Map

Name:

Description:

Parameters

Allow packets with the End of Options List (EOOL) option

Clear the option value from the packets

Allow packets with the No Operation (NOP) option

Clear the option value from the packets

Allow packets with the Router Alert (RTRALT) option

Clear the option value from the packets

注意：您能也选择结算从

数据包选项的选项值，因此IP数据包的此字段禁用，并且数据包穿过Cisco ASA。

3. 呼叫**testmap**的一张新的Inspect地图创建。单击 **Apply**。

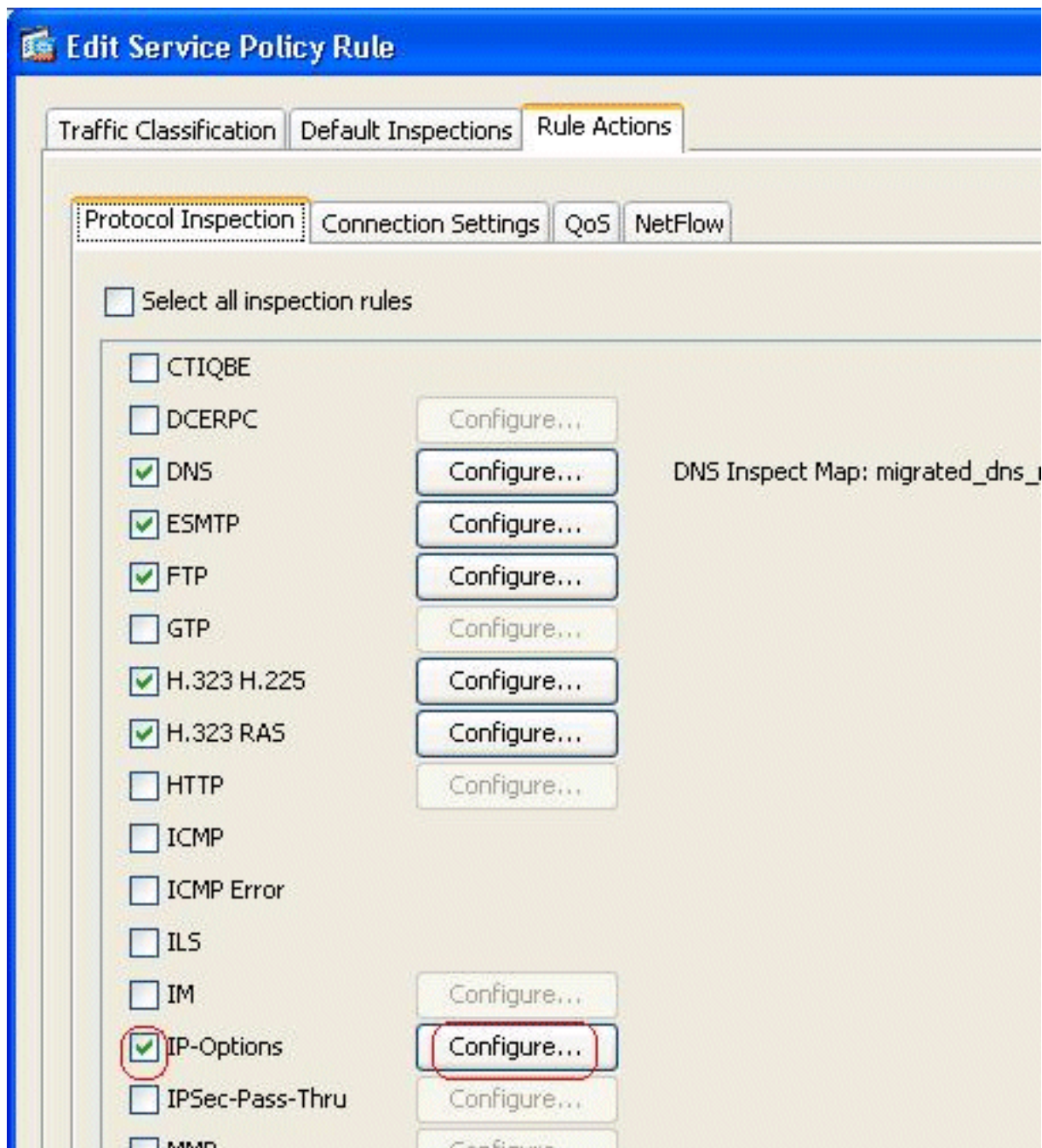
[Configuration](#) > [Firewall](#) > [Objects](#) > [Inspect Maps](#) > [IP-Options](#)

Configure IP-Options maps.

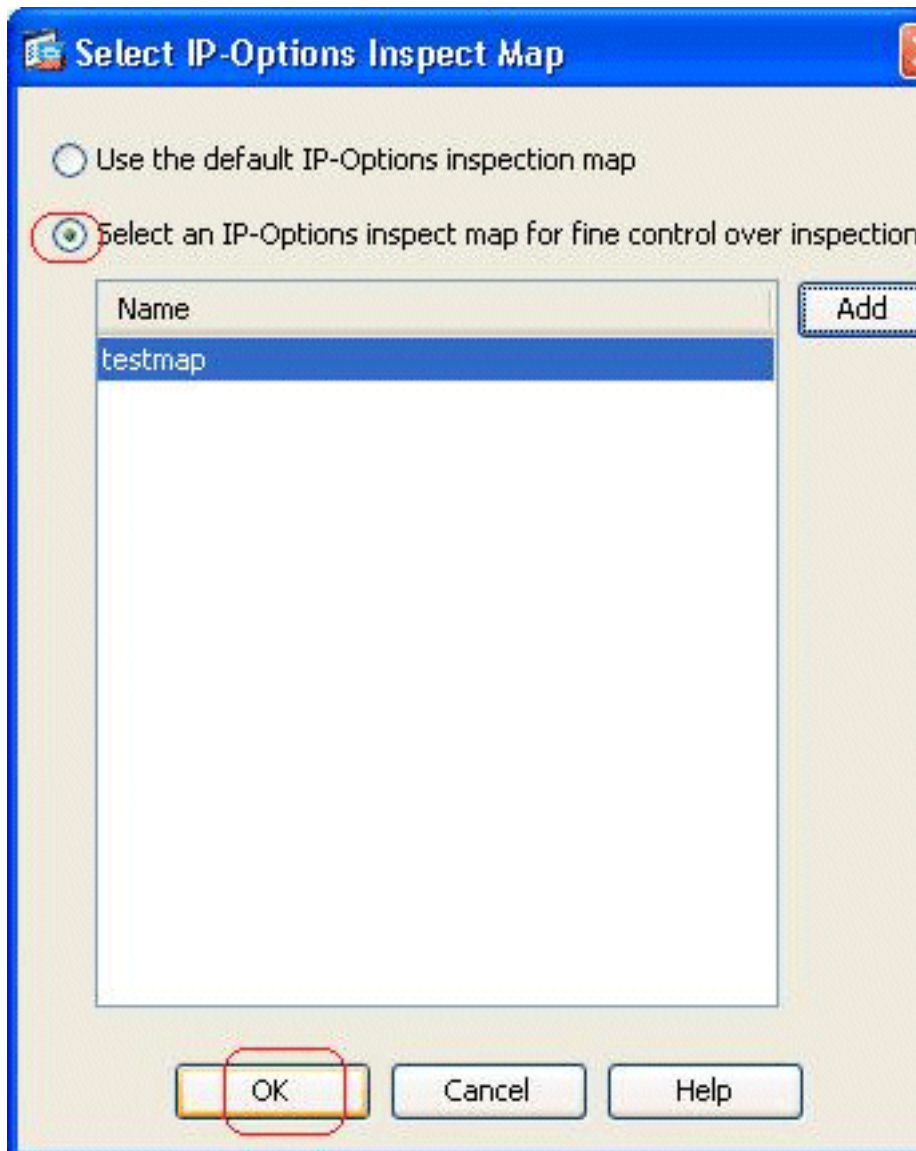
IP-Options Inspect Maps

Name	Description
testmap	

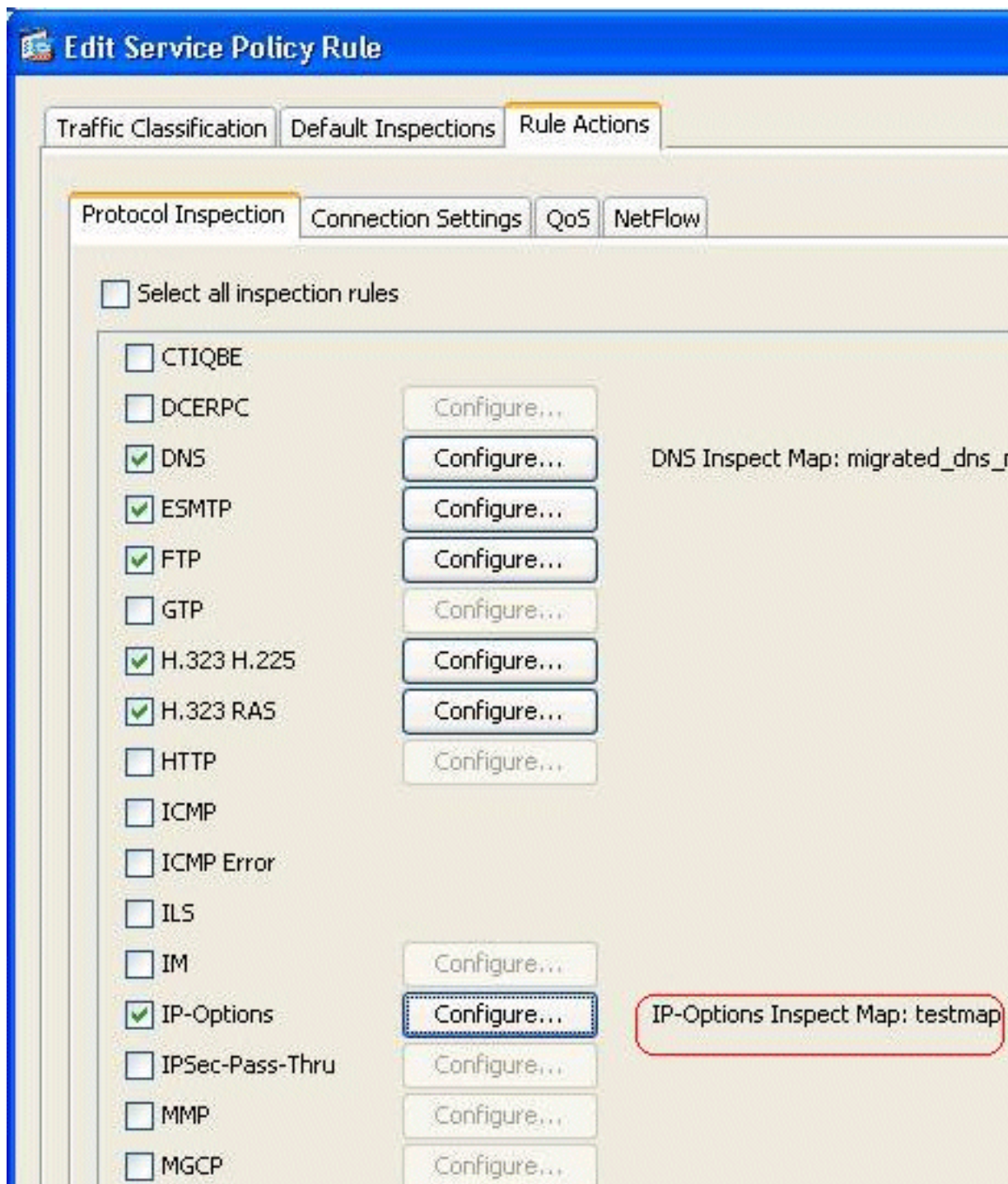
4. 去**Configuration>防火墙>服务策略规则**，选择现有全局策略，并且单击**编辑**。编辑服务策略规则窗口出现。选择**规则操作**选项卡，复选标记**Ip options**项目，并且选择**配置**为了分配新建立的检查地图。



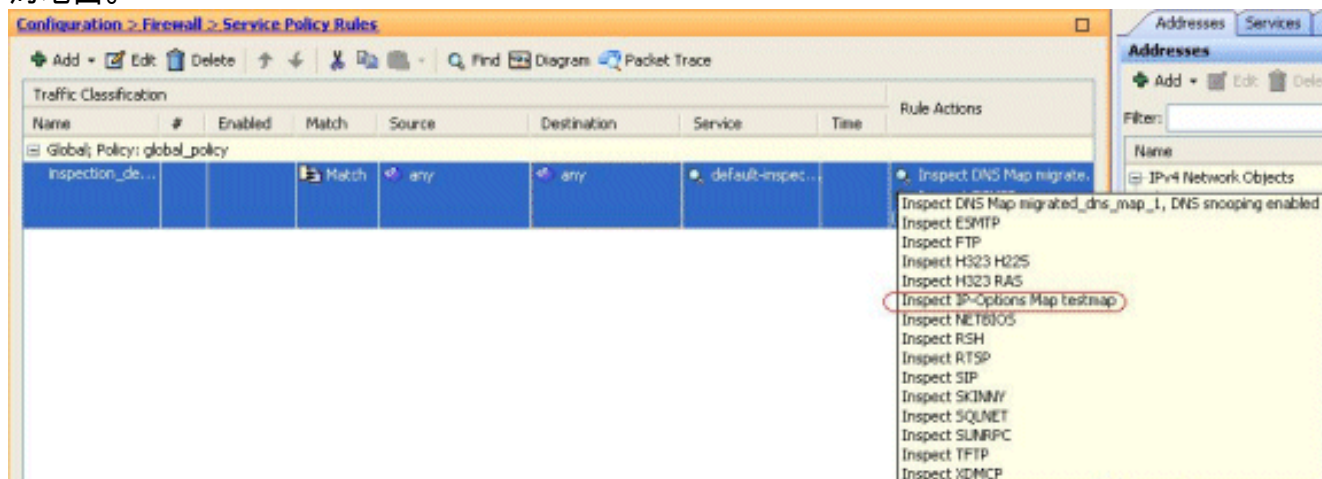
5. 选择精选更细微的控制的一张Ip options Inspect地图对检查> testmap，并且点击OK键。



6. 选定Inspect地图可以在Ip options字段查看。点击OK键为了恢复回到服务策略规则选项卡。



7. 使用您的鼠标，请在规则操作选项卡盘旋，以便您能找到所有可用的协议检测地图关联用此全局地图。



这是等同CLI配置的示例片断，供您的参考：

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

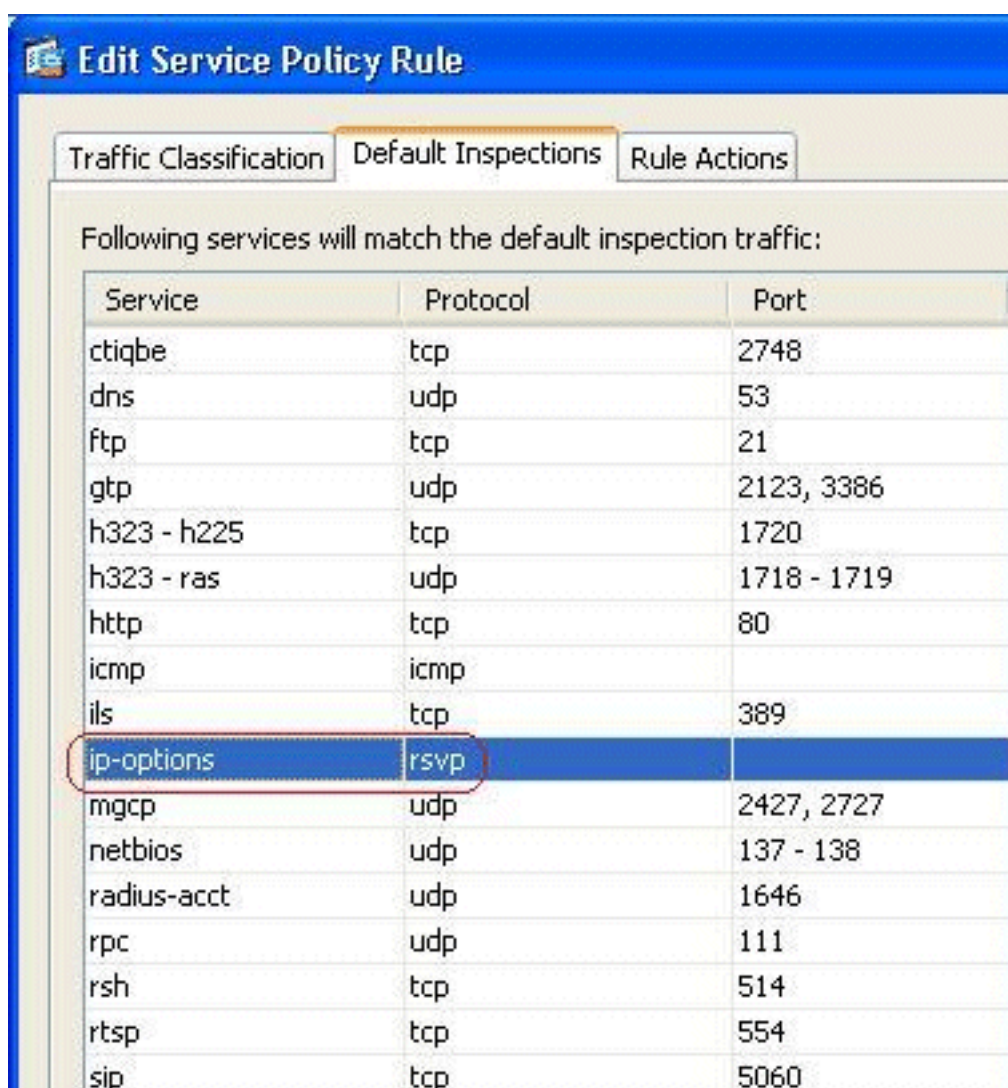
ciscoasa(config-pmap-c)#inspect ip-options testmap

ciscoasa(config-pmap-p)#exit

ciscoasa(config)#write memory
```

思科ASA默认行为为了允许RSVP数据包

默认情况下Ip options检查启用。去**Configuration>防火墙>服务策略规则**。选择全局策略，单击**编辑**，并且选择**默认检验**选项卡。这里，您在**Ip options**字段将查找RSVP协议。这保证RSVP协议通过思科ASA检查并且允许。结果，一端到端视频呼叫建立得不出任何问题。



Following services will match the default inspection traffic:

Service	Protocol	Port
ctiqbe	tcp	2748
dns	udp	53
ftp	tcp	21
gtp	udp	2123, 3386
h323 - h225	tcp	1720
h323 - ras	udp	1718 - 1719
http	tcp	80
icmp	icmp	
ils	tcp	389
ip-options	rsvp	
mgcp	udp	2427, 2727
netbios	udp	137 - 138
radius-acct	udp	1646
rpc	udp	111
rsh	tcp	514
rtsp	tcp	554
sip	tcp	5060

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策略inspect ip options** -显示被丢弃的数据包编号并且/或者允许根据配置的服务策略规则。

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](#)