

# 在ASDM 6.3及更高版本上配置IP選項檢測

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[ASDM配置](#)

[允許RSVP資料包的Cisco ASA的預設行為](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本文提供如何設定思科調適型安全裝置(ASA)的範例組態，以便在啟用某些IP選項的情況下傳遞IP封包。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本8.3及更高版本的Cisco ASA
- 運行軟體版本6.3及更高版本的思科自適應安全管理器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### 慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

## 背景資訊

每個IP資料包都包含一個IP報頭，其中包含「選項」欄位。Options欄位（通常稱為IP Options）提供某些情況下所需的控制功能，但對於大多數普通通訊來說這些功能是不必要的。特別是，IP選項包括時間戳、安全性和特殊路由的規定。IP選項的使用是可選的，欄位可以包含零、一個或多個選項。

IP選項存在安全風險，如果啟用IP選項欄位的IP資料包通過ASA，則會向外部洩漏有關網路內部設定的資訊。因此，攻擊者可以對映網路的拓撲。由於Cisco ASA是在企業中實施安全的裝置，因此預設情況下，它會丟棄已啟用IP選項欄位的資料包。此處顯示系統日誌消息示例，供您參考：

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||10.110.1.34XX.YY.ZZ.ZZ|IP|IP"
```

但是，在影片流量必須通過Cisco ASA的特定部署方案中，必須通過具有某些IP選項的IP資料包，否則影片電話會議可能會失敗。從Cisco ASA軟體版本8.2.2開始，引入了一項稱為「IP選項檢測」的新功能。通過此功能，您可以控制允許哪些具有特定IP選項的資料包通過Cisco ASA。

預設情況下，此功能已啟用，並且在全域性策略中啟用對以下IP選項的檢查。配置此檢測會指示ASA允許資料包通過，或者清除指定的IP選項，然後允許資料包通過。

- **選項清單結束(EOOL)或IP選項0** — 此選項出現在所有選項的結尾，以便標籤選項清單的結尾。
- **無操作(NOP)或IP選項1** — 此選項欄位使欄位的總長度變為變數。
- **路由器警報(RTRALT)或IP選項20** — 此選項會通知傳輸路由器檢查封包的內容，即使封包並非以該路由器為目的地也是如此。

## 設定

本節提供用於設定本文件中所述功能的資訊。

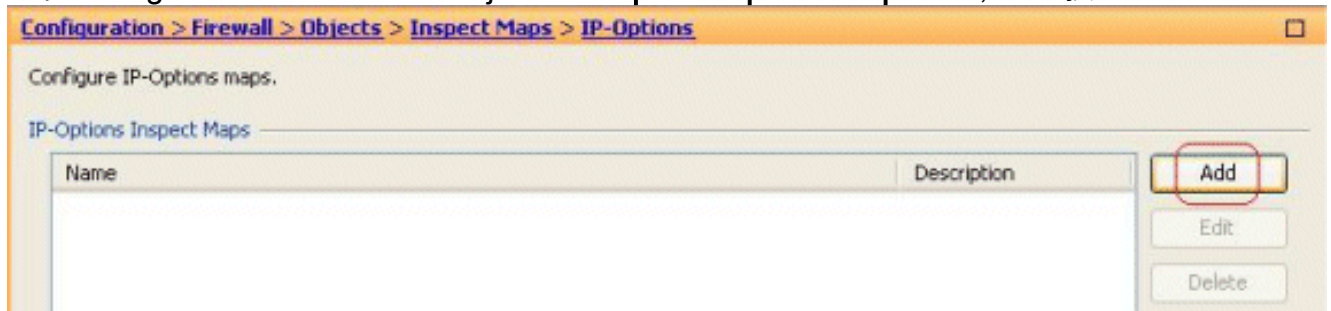
**註：**使用[Command Lookup Tool](#)(僅限[註冊](#)客戶)可獲取本節中使用的命令的詳細資訊。

## ASDM配置

使用ASDM，您可以看到如何對具有IP選項(NOP)欄位的IP資料包啟用檢測。

IP報頭中的Options欄位可以包含零、一個或多個選項，這會使欄位的總長度變為變數。但是，IP報頭必須是32位的倍數。如果所有選項的位數不是32位的倍數，則NOP選項將用作「內部填充」，以便在32位邊界上對齊選項。

1. 前往Configuration > Firewall > Objects > **Inspect Maps** > **IP-Options**，然後按一下Add。



2. 系統將顯示Add IP-Options Inspect Map視窗。指定Inspect Map的名稱，選擇**Allow packets with the No Operation(NOP)**選項，然後按一下OK。

**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：您還可以選擇

**Clear the option value from the packets**選項，以便禁用IP資料包中的此欄位並且資料包通過Cisco ASA。

3. 建立名為**testmap**的新檢查對映。按一下「**Apply**」。

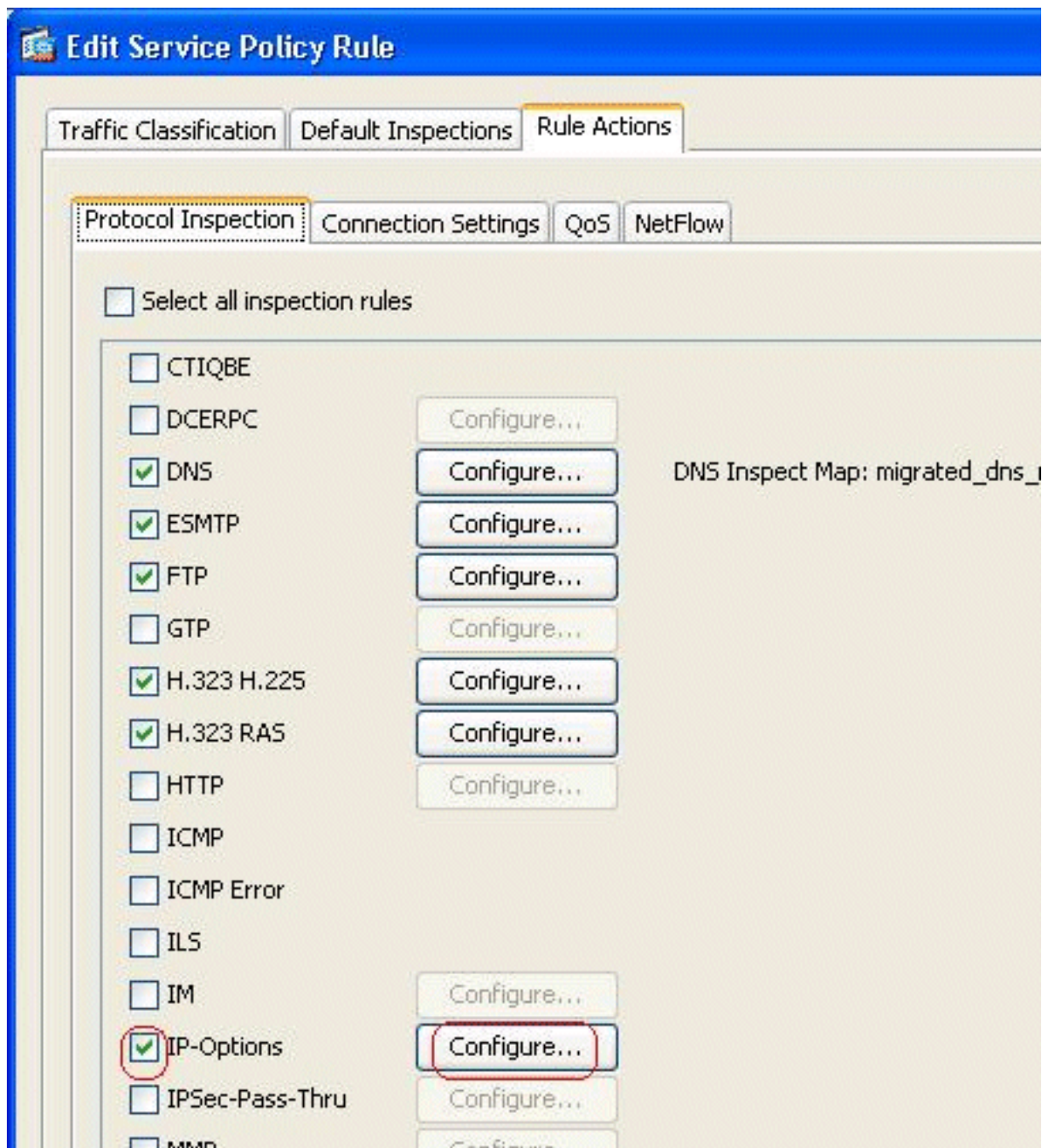
[Configuration](#) > [Firewall](#) > [Objects](#) > [Inspect Maps](#) > [IP-Options](#)

Configure IP-Options maps.

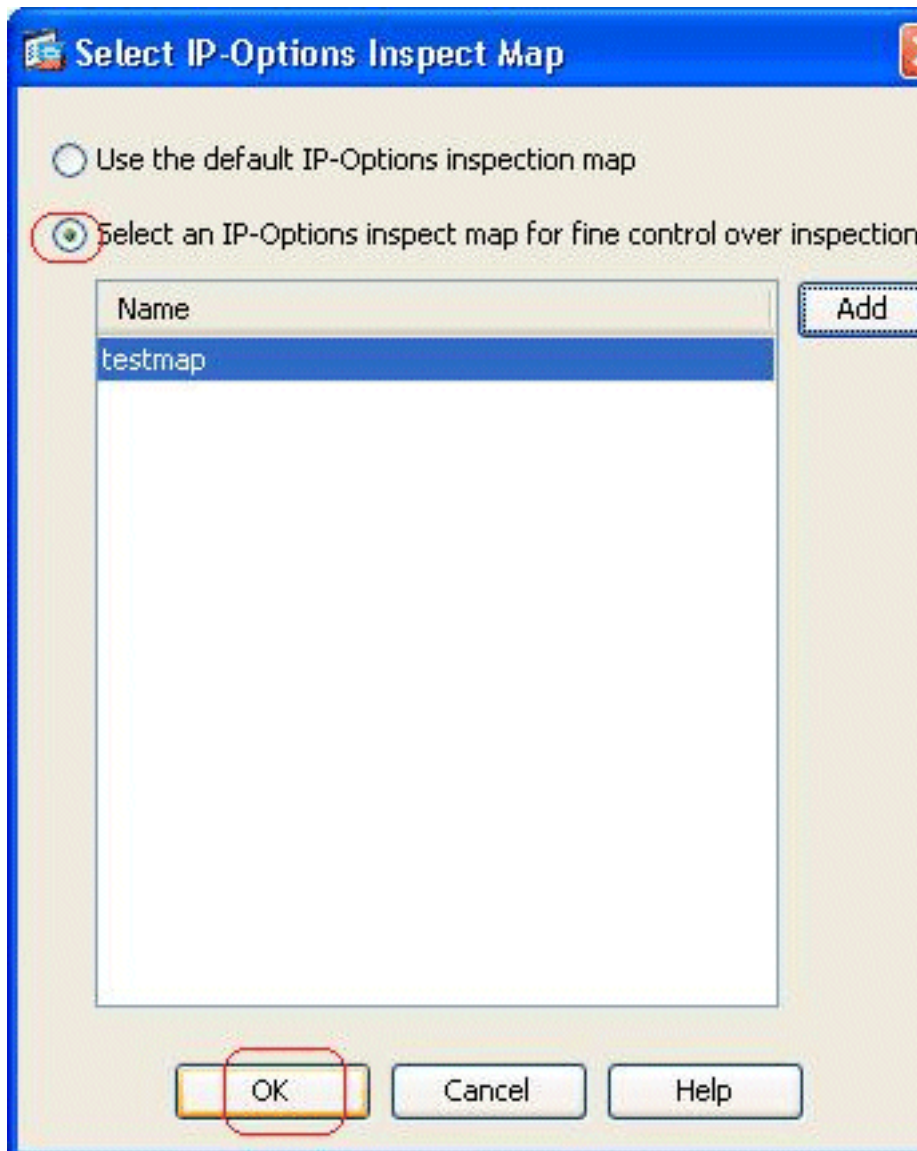
IP-Options Inspect Maps

Name	Description
testmap	

4. 轉至**Configuration > Firewall > Service Policy Rules**，選擇現有的全域性策略，然後按一下**Edit**。系統將顯示Edit Service Policy Rule視窗。選擇**Rule Actions**頁籤，選中標籤**IP-Options**項，然後選擇**Configure**以分配新建立的檢測對映。

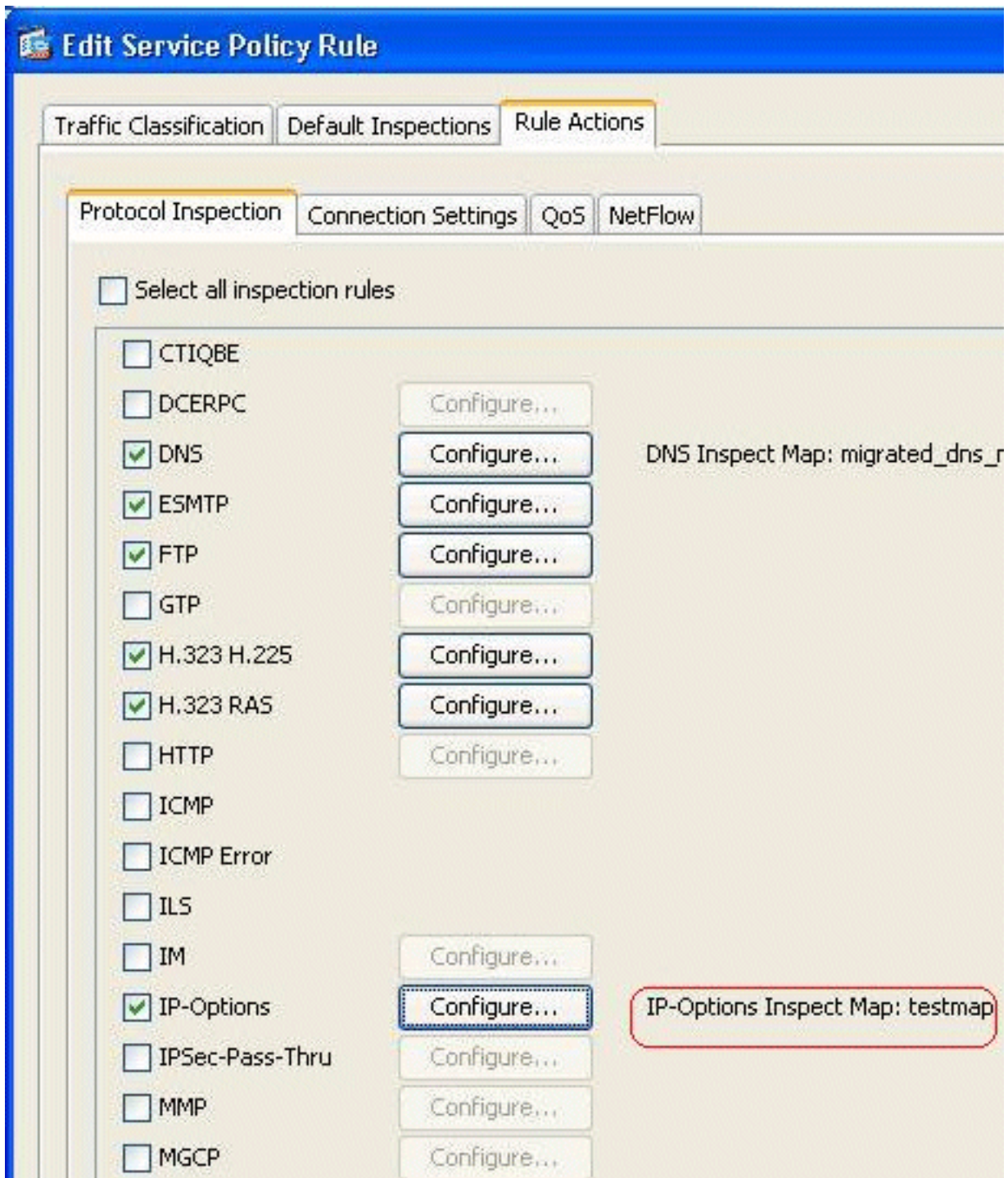


5. 選擇Select an IP-Options inspect map for fine control over inspection > testmap , 然後按一下

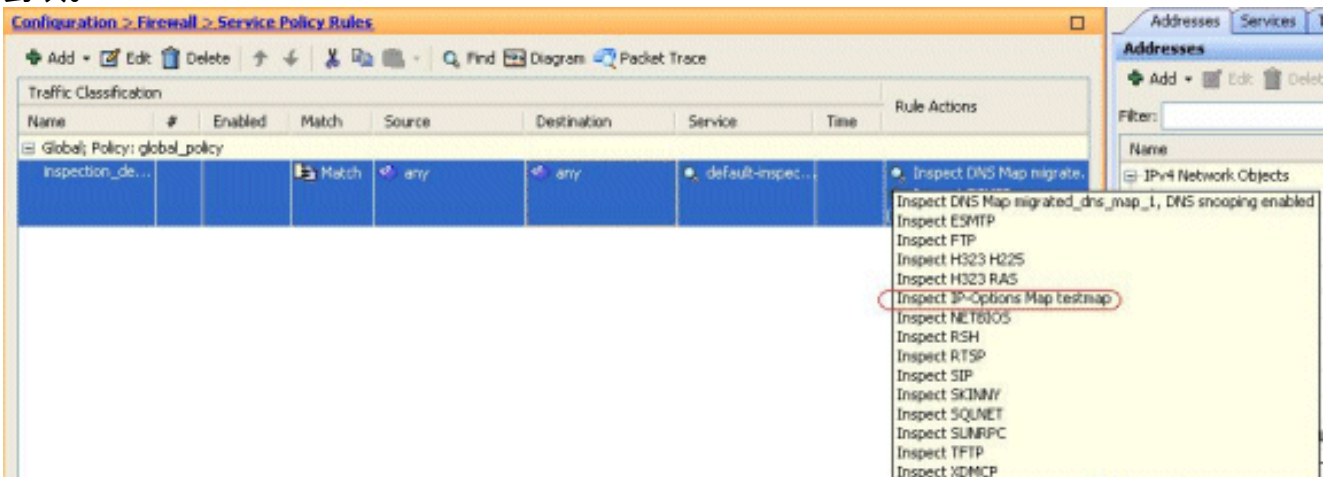


OK。

6. 可以在IP-Options欄位中檢視選定的檢查對映。按一下OK以恢復到Service Policy Rules頁籤



7. 使用滑鼠懸停在Rule Actions頁籤上，以便可以找到與此全域性對映關聯的所有可用協定檢測對映。



以下是等效CLI組態的範例片段，供您參考：

## 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

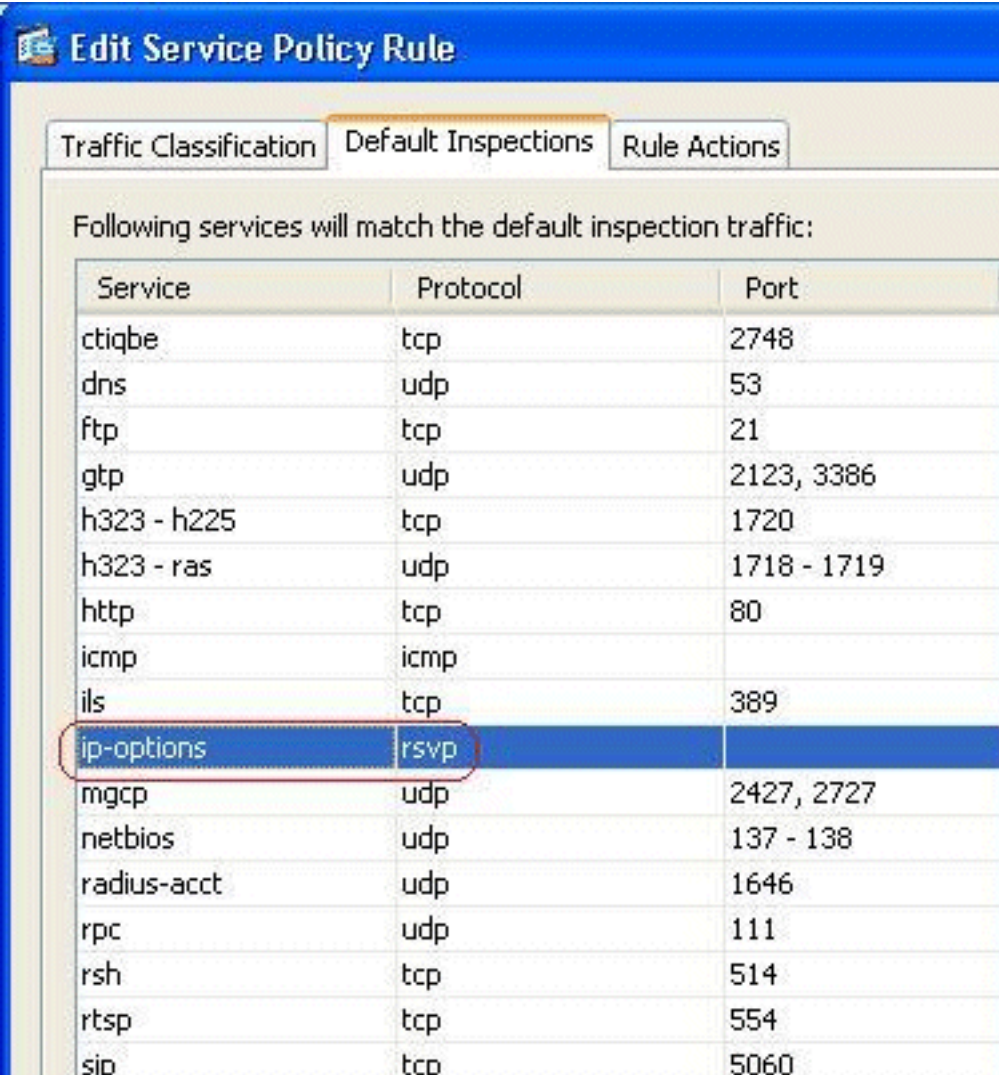
ciscoasa(config-pmap-c)#inspect ip-options testmap

ciscoasa(config-pmap-p)#exit

ciscoasa(config)#write memory
```

### 允許RSVP資料包的Cisco ASA的預設行為

預設情況下，IP選項檢測已啟用。前往**Configuration > Firewall > Service Policy Rules**。選擇全域性策略，按一下**編輯**，然後選擇**預設檢測**頁籤。您可以在此處的**IP-Options**欄位中找到RSVP協定。這可確保通過Cisco ASA檢查並允許RSVP協定。因此，端到端影片呼叫建立起來沒有任何問題。



**Edit Service Policy Rule**

Traffic Classification | **Default Inspections** | Rule Actions

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
<b>ip-options</b>	<b>rsvp</b>	
mgcp	udp	2427, 2727
netbios	udp	137 - 138
radius-acct	udp	1646
rpc	udp	111
rsh	tcp	514
rtsp	tcp	554
sip	tcp	5060

## 驗證

使用本節內容，確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show service-policy inspect ip-options** — 顯示根據已配置的服務策略規則丟棄和/或允許的資料包數。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

## 相關資訊

- [Cisco ASA 5500系列自適應安全裝置技術支援](#)
- [技術支援與文件 - Cisco Systems](#)