# ASDM 6.3 and Later: IP Options Inspection Configuration Example

## Contents

## Introduction

This document provides a sample configuration of how to configure the Cisco Adaptive Security Appliance (ASA) in order to pass the IP packets with certain IP options enabled.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA running software release version 8.3 and later
- Cisco Adaptive Security Manager running software release version 6.3 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

Each IP packet contains an IP header with an Options field. The Options field, commonly referred to as IP Options, provides control functions that are required in some situations, but unnecessary for most common communications. In particular, IP Options includes provisions for time stamps, security, and special routing. Use of IP Options is optional, and the field can contain zero, one, or more options.

IP Options is a security risk and if an IP packet with the IP Options field enabled is passed through ASA, it will leak information about the internal setup of a network to the outside. As a result, an attacker can map the topology of your network. As Cisco ASA is a device that enforces security in the enterprise, by default, it drops the packets that have the IP Options field enabled. A sample syslog message is shown here, for your reference:

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||Deny IP from 10.110.1.34 to XX.YY.ZZ.ZZ, IP options: "Router
Alert"
```

However, in specific deployment scenarios where Video traffic has to pass through Cisco ASA, IP packets with certain IP options has to be passed through otherwise the video conference call may fail. From Cisco ASA software release version 8.2.2 onwards, a new feature called "Inspection for IP options" has been introduced. With this feature, you can control which packets with specific IP options are allowed through Cisco ASA.

By default, this feature is enabled and inspection for the IP Options below are enabled in the global policy. Configuring this inspection instructs the ASA to allow a packet to pass, or to clear the specified IP options and then allow the packet to pass.

- **End of Options List (EOOL)** or **IP Option 0** - This option appears at the end of all options in order to mark the end of a list of options.
- **No Operation (NOP)** or **IP Option 1** - This options field makes the total length of the field variable.
- **Router Alert (RTRALT)** or **IP Option 20** - This option notifies transit routers to inspect the contents of the packet even when the packet is not destined for that router.

## Configure

In this section, you are presented with the information to configure the features described in this document.

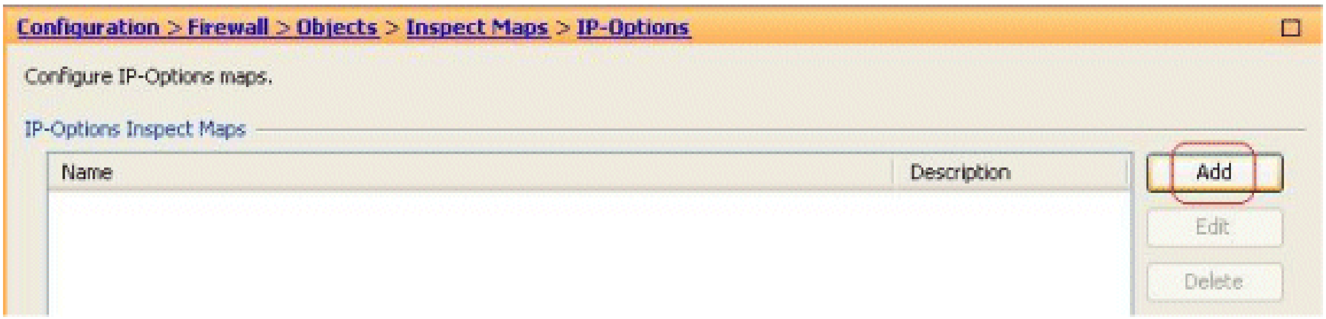
**Note:** Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

### ASDM Configuration

Using the ASDM, you can see how to enable the inspection for the IP packets that have the IP Options field, NOP.

The Options field in the IP header can contain zero, one, or more options, which makes the total length of the field variable. However, the IP header must be a multiple of 32 bits. If the number of bits of all options is not a multiple of 32 bits, the NOP option is used as "internal padding" in order to align the options on a 32-bit boundary.

1. Go to **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **IP-Options**, and click **Add**.



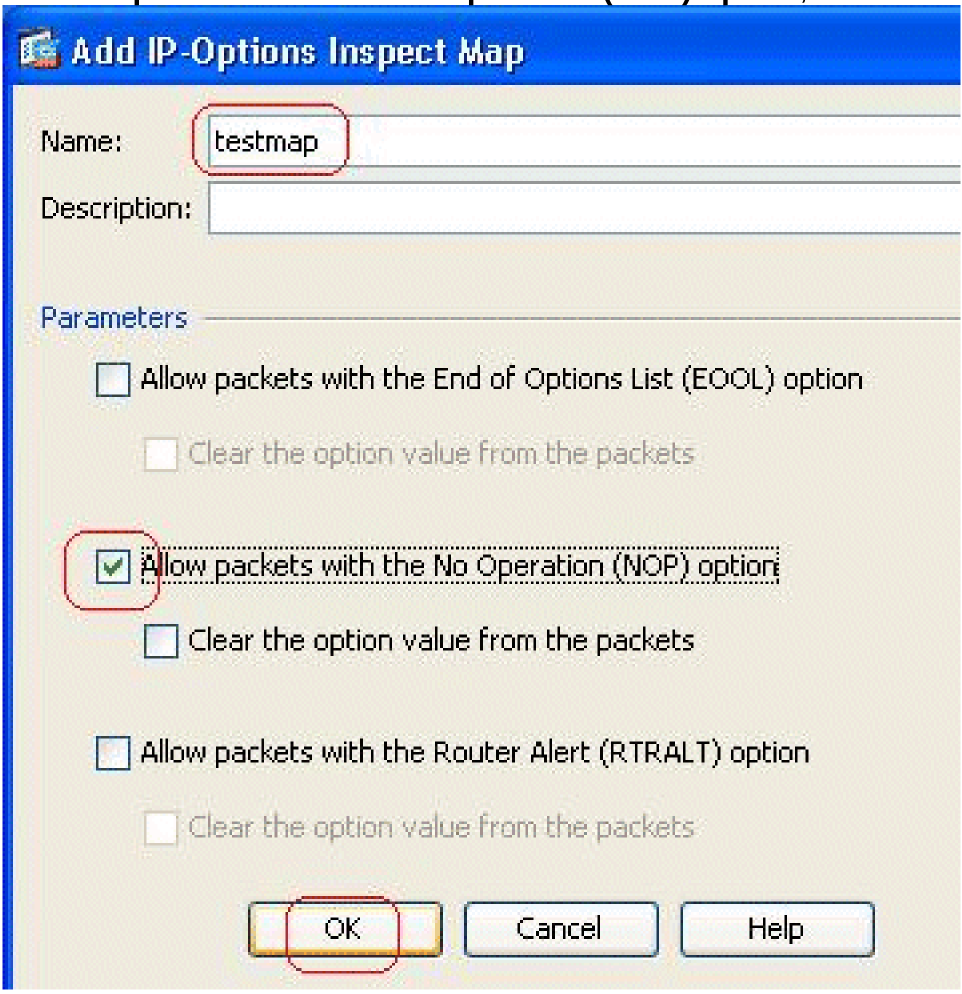
Configuration > Firewall > Objects > Inspect Maps > IP-Options

Configure IP-Options maps.

IP-Options Inspect Maps

| Name | Description |
|---|---|

2. The Add IP-Options Inspect Map window appears. Specify the name of the Inspect Map, select **Allow packets with the No Operation (NOP) option**, and click **OK**. **Note:** You can also select the **Clear the option value from the packets** option, so that this field in the IP packet is disabled, and the packets pass through the Cisco ASA.



Add IP-Options Inspect Map

Name: testmap

Description:

Parameters

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

□ Clear the option value from the packets

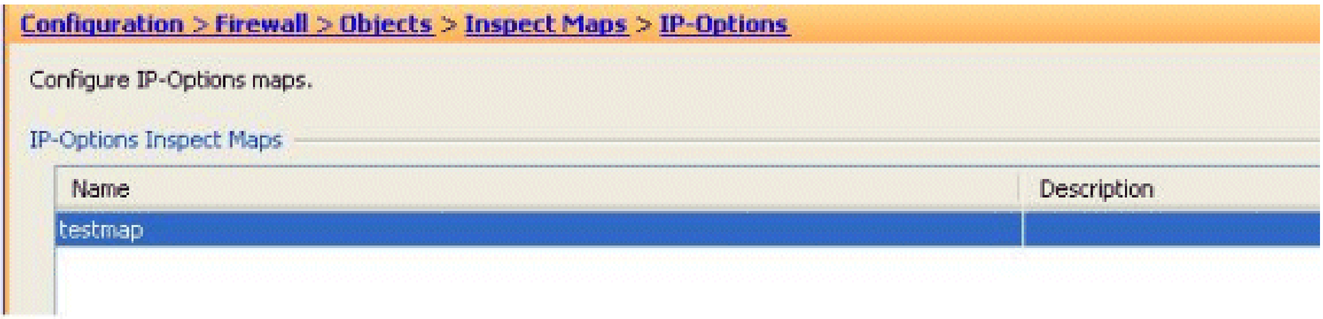
☑ Allow packets with the No Operation (NOP) option

□ Clear the option value from the packets

□ Allow packets with the Router Alert (RTRALT) option

□ Clear the option value from the packets

3. A new inspect map called **testmap** is created. Click **Apply**.



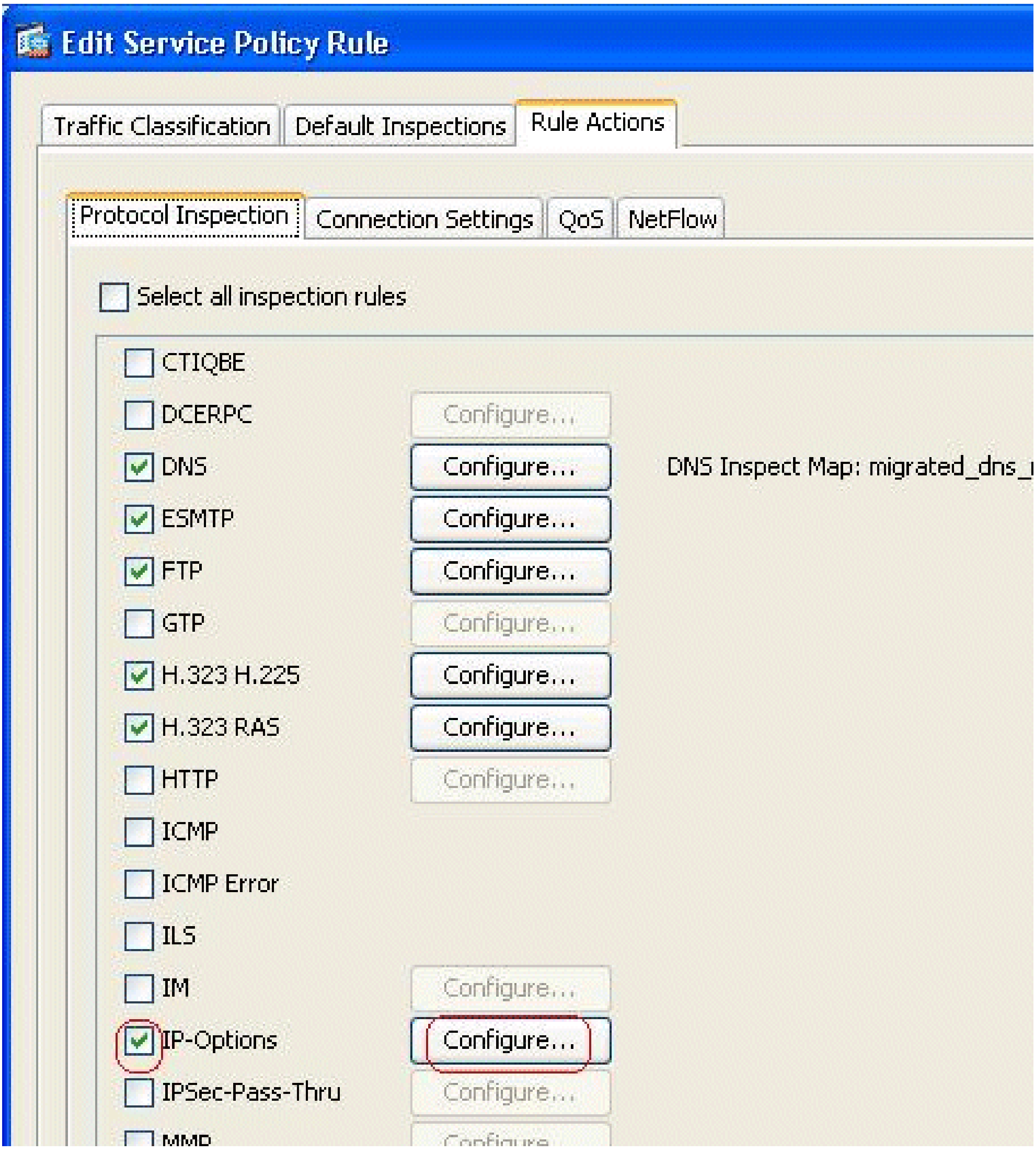
Configuration > Firewall > Objects > Inspect Maps > IP-Options

Configure IP-Options maps.

IP-Options Inspect Maps

| Name | Description |
|---|---|
| testmap | |

4. Go to **Configuration** > **Firewall** > **Service Policy Rules**, select the existing global policy, and click **Edit**. The Edit Service Policy Rule window appears. Select the **Rule Actions** tab, check mark the **IP-Options** item, and choose **Configure** in order to assign the newly created inspection map.



Edit Service Policy Rule

□ Select all inspection rules

□ CTIQBE

□ DCERPC Configure...

☑ DNS Configure... DNS Inspect Map: migrated_dns_

☑ ESMTP Configure...

☑ FTP Configure...

□ GTP Configure...

☑ H.323 H.225 Configure...

☑ H.323 RAS Configure...

□ HTTP Configure...

□ ICMP

□ ICMP Error

□ ILS

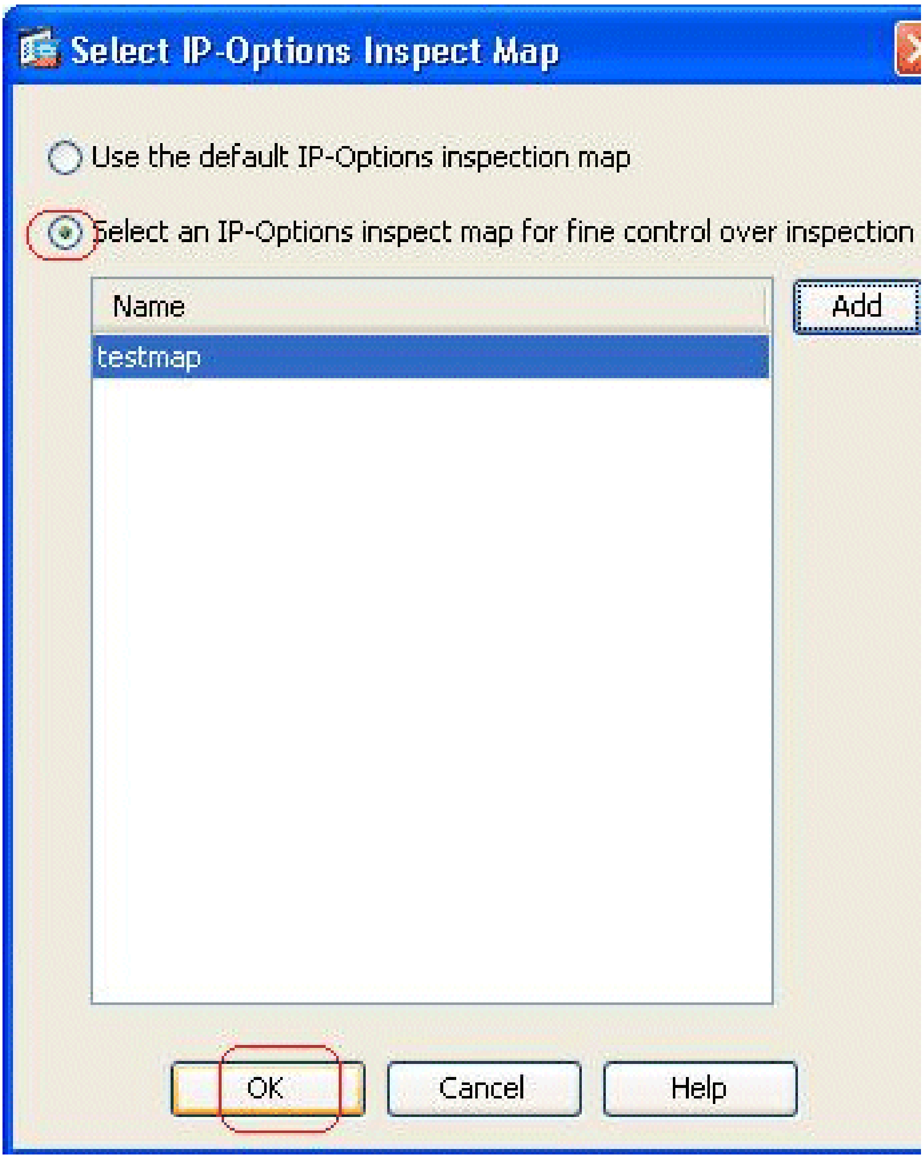
□ IM Configure...

☑ IP-Options Configure...

□ IPSec-Pass-Thru Configure...

□ MMP Configure...

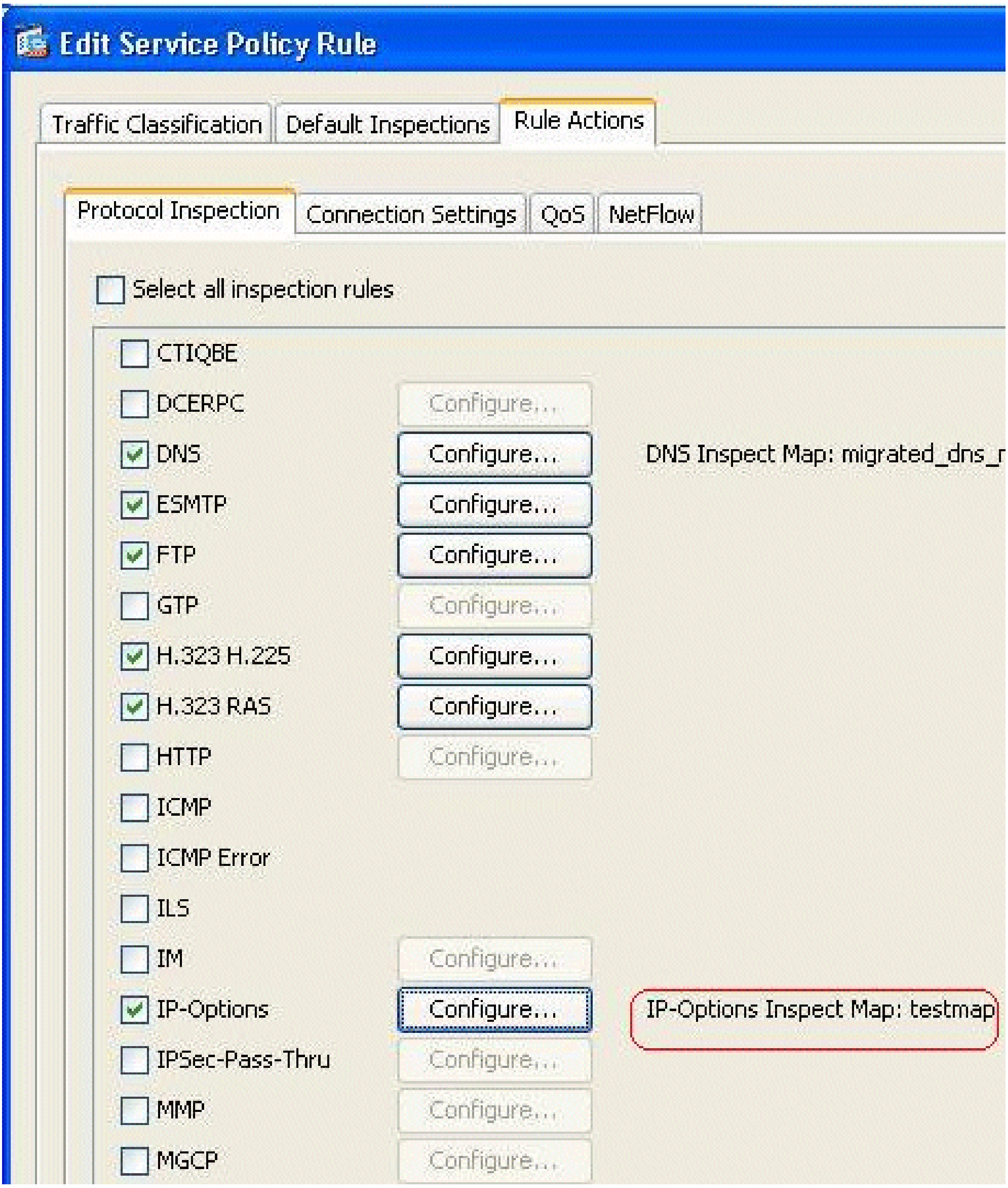
5. Choose **Select an IP-Options inspect map for fine control over inspection** > **testmap**,



Select IP-Options Inspect Map
○ Use the default IP-Options inspection map
● Select an IP-Options inspect map for fine control over inspection
Name
testmap
Add
OK
Cancel
Help

and click **OK**.

6. The selected inspect map can be viewed in the **IP-Options** field. Click **OK** in order to revert back to the Service Policy Rules



Edit Service Policy Rule

Traffic Classification | Default Inspections | Rule Actions

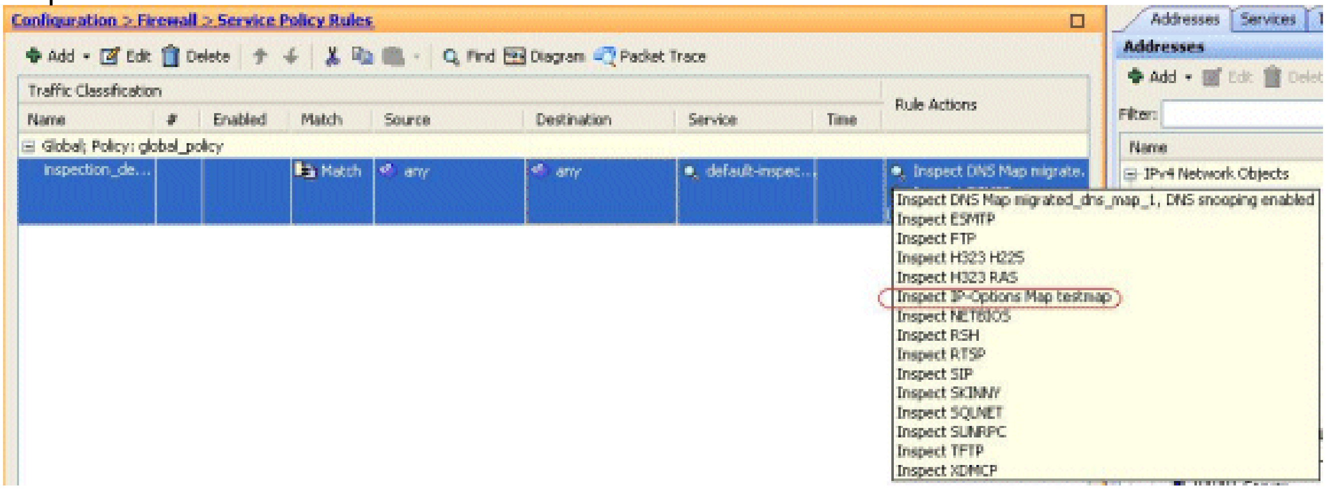
Protocol Inspection | Connection Settings | QoS | NetFlow

☐ Select all inspection rules

- ☐ CTIQBE
- ☐ DCERPC [Configure...]
- ☑ DNS [Configure...] DNS Inspect Map: migrated_dns_r
- ☑ ESMTP [Configure...]
- ☑ FTP [Configure...]
- ☐ GTP [Configure...]
- ☑ H.323 H.225 [Configure...]
- ☑ H.323 RAS [Configure...]
- ☐ HTTP [Configure...]
- ☐ ICMP
- ☐ ICMP Error
- ☐ ILS
- ☐ IM [Configure...]
- ☑ IP-Options [Configure...] IP-Options Inspect Map: testmap
- ☐ IPSec-Pass-Thru [Configure...]
- ☐ MMP [Configure...]
- ☐ MGCP [Configure...]

tab.

7. With your mouse, hover over the **Rule Actions** tab so that you can find all the available protocol inspection maps associated with this global map.



Configuration > Firewall > Service Policy Rules

Add Edit Delete Find Diagram Packet Trace

| Name | # | Enabled | Match | Source | Destination | Service | Time | Rule Actions |
|---|---|---|---|---|---|---|---|---|
| Global; Policy: global_policy | | | | | | | | |
| inspection_de... | | | Match | any | any | default-inspec... | | Inspect DNS Map migrate. |

Inspect DNS Map migrated_dns_map_1, DNS snooping enabled
Inspect ESMTP
Inspect FTP
Inspect H323 H225
Inspect H323 RAS
Inspect IP-Options Map testmap
Inspect NETBIOS
Inspect RSH
Inspect RTSP
Inspect SIP
Inspect SKINNY
Inspect SQLNET
Inspect SUNRPC
Inspect TFTP
Inspect XDMCP

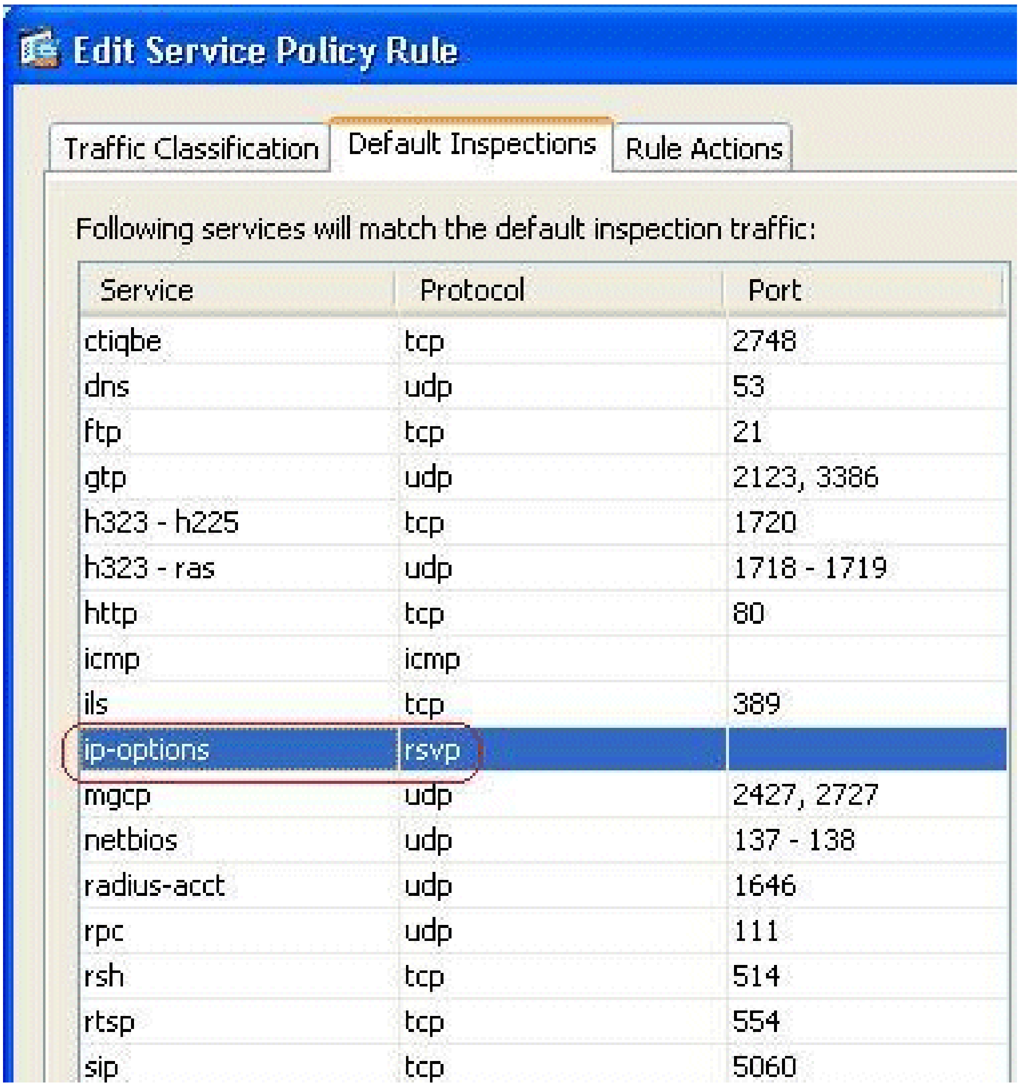
Here is a sample snippet of the equivalent CLI configuration, for your reference:

**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
```

## Default Behavior of Cisco ASA in order to Allow RSVP Packets

The IP Options Inspection is enabled by default. Go to **Configuration** > **Firewall** > **Service Policy Rules**. Select the Global Policy, click **Edit**, and select the **Default Inspections** tab. Here, you will find the RSVP protocol in the **IP-Options** field. This ensures that the RSVP protocol is inspected and allowed through Cisco ASA. As a result, an end-to-end video call is established without any problem.



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 |

## Verify

Use this section in order to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show service-policy inspect ip-options** - Displays the number of packets dropped and/or allowed as per the configured service-policy rule.

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances Technical Support**
- **Technical Support & Documentation - Cisco Systems**