ASDM 6.3 y posterior: Ejemplo de configuración del examen de las opciones IP

Contenido

Introducción

Este documento proporciona una configuración de muestra de cómo configurar el dispositivo de seguridad adaptante de Cisco (ASA) para pasar los paquetes del IP con ciertas opciones IP habilitadas.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de software corriente 8.3 de Cisco ASA y posterior
- Versión de software corriente 6.3 del administrador de seguridad adaptante de Cisco y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Cada paquete del IP contiene un encabezado IP con un campo de opciones. El campo de opciones, designado comúnmente las opciones IP, proporciona las funciones de control que se requieren en algunas situaciones, pero innecesario para la mayoría de las comunicaciones comunes. Particularmente, las opciones IP incluyen las disposiciones para los sellos de fecha/hora, la Seguridad, y la encaminamiento especial. El uso de las opciones IP es opcional, y el campo puede contener cero, una, o más opción.

Las opciones IP son un riesgo de seguridad y si un paquete del IP con el campo de opciones IP habilitado se pasa con el ASA, se escapará la información sobre la configuración interna de una red al exterior. Como consecuencia, un atacante puede asociar la topología de su red. Mientras que es Cisco ASA un dispositivo que aplica la Seguridad en la empresa, por abandono, él cae los paquetes que tienen el campo de opciones IP habilitado. Un mensaje de Syslog de la muestra se muestra aquí, para su referencia:

```
IP 106012|10.110.1.34||XX.YY.ZZ.ZZ||Deny de 10.110.1.34 a XX.YY.ZZ.ZZ, opciones IP: “Alerta del router”
```

Sin embargo, en los escenarios de instrumentación específicos donde el tráfico de video tiene que pasar con Cisco ASA, los paquetes del IP con ciertas opciones IP tienen que ser pasados con la llamada de Video conferencia. pueden fallar de otra manera. De la versión de software 8.2.2 de Cisco ASA hacia adelante, una nueva función llamada “examen para las opciones IP” se ha introducido. Con esta característica, usted puede controlar qué paquetes con las opciones IP específicas se permiten con Cisco ASA.

Por abandono, se habilita esta característica y el examen para las opciones IP abajo se habilita en la política global. Configurar este examen da instrucciones el ASA para permitir un paquete pase, o borre las opciones IP especificadas y después permita que el paquete pase.

- **Final de la lista de opciones (EOOL)** o de la **opción IP 0** - esta opción aparece en el final de todas las opciones para marcar el extremo de una lista de opciones.
- **Ninguna operación (NOP)** o **opción IP 1** - este campo de opciones hace la longitud total de la variable del campo.
- **Alerta del router (RTRALT)** o **opción IP 20** - esta opción notifica a los routeres de tránsito para examinar el contenido del paquete incluso cuando el paquete no es destinado para ese router.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

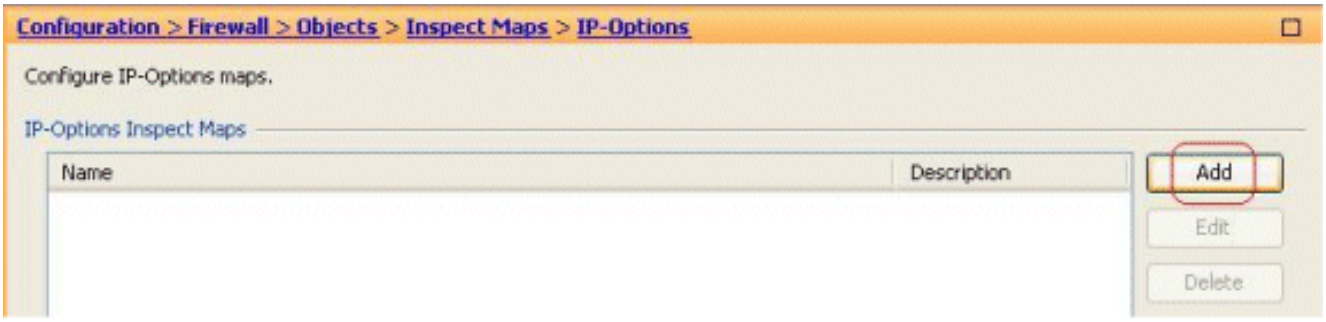
Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Configuración de ASDM

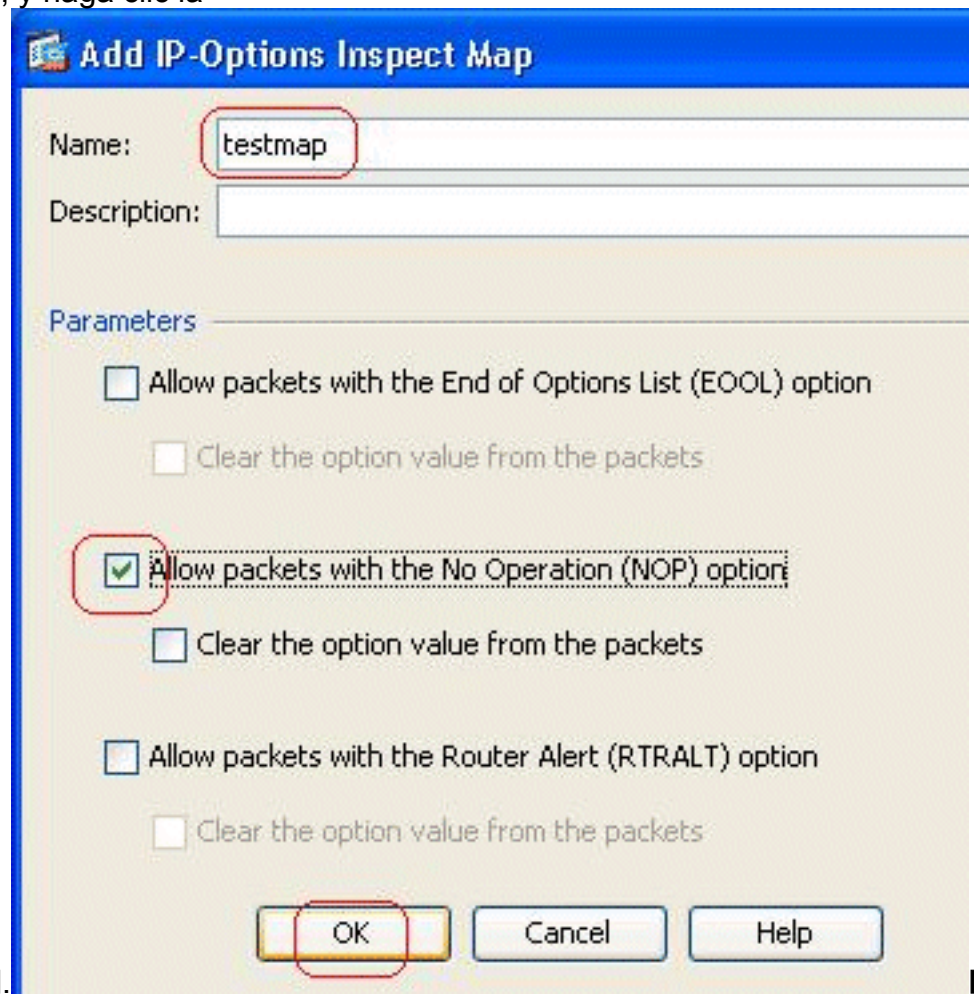
Usando el ASDM, usted puede ver cómo habilitar el examen para los paquetes del IP que tienen el campo de opciones IP, NOP.

El campo de opciones en el encabezado IP puede contener cero, una, o más opción, que hace la longitud total de la variable del campo. Sin embargo, el encabezado IP debe ser un múltiplo de 32 bits. Si el número de bits de todas las opciones no es un múltiplo de 32 bits, la opción NOP se utiliza como “relleno interno” para alinear las opciones en un límite de 32 bits.

1. Vaya a la **configuración** > al **Firewall** > a los **objetos** > **examinan las correspondencias** > las **opciones IP**, y el haga click en Add

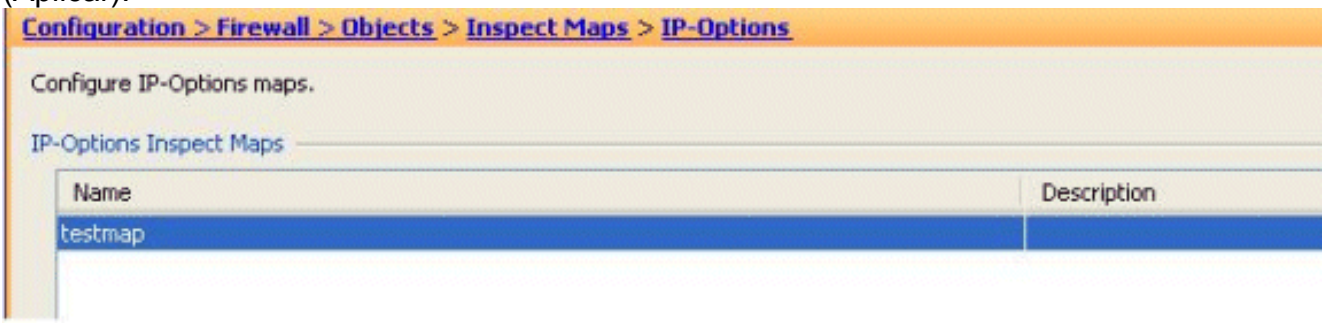


2. Las opciones IP del agregar examinan la ventana del mapa aparecen. Especifique el nombre del mapa de la inspección, selecto **permita los paquetes con la ninguna opción de la operación (NOP)**, y haga clic la AUTORIZACIÓN.

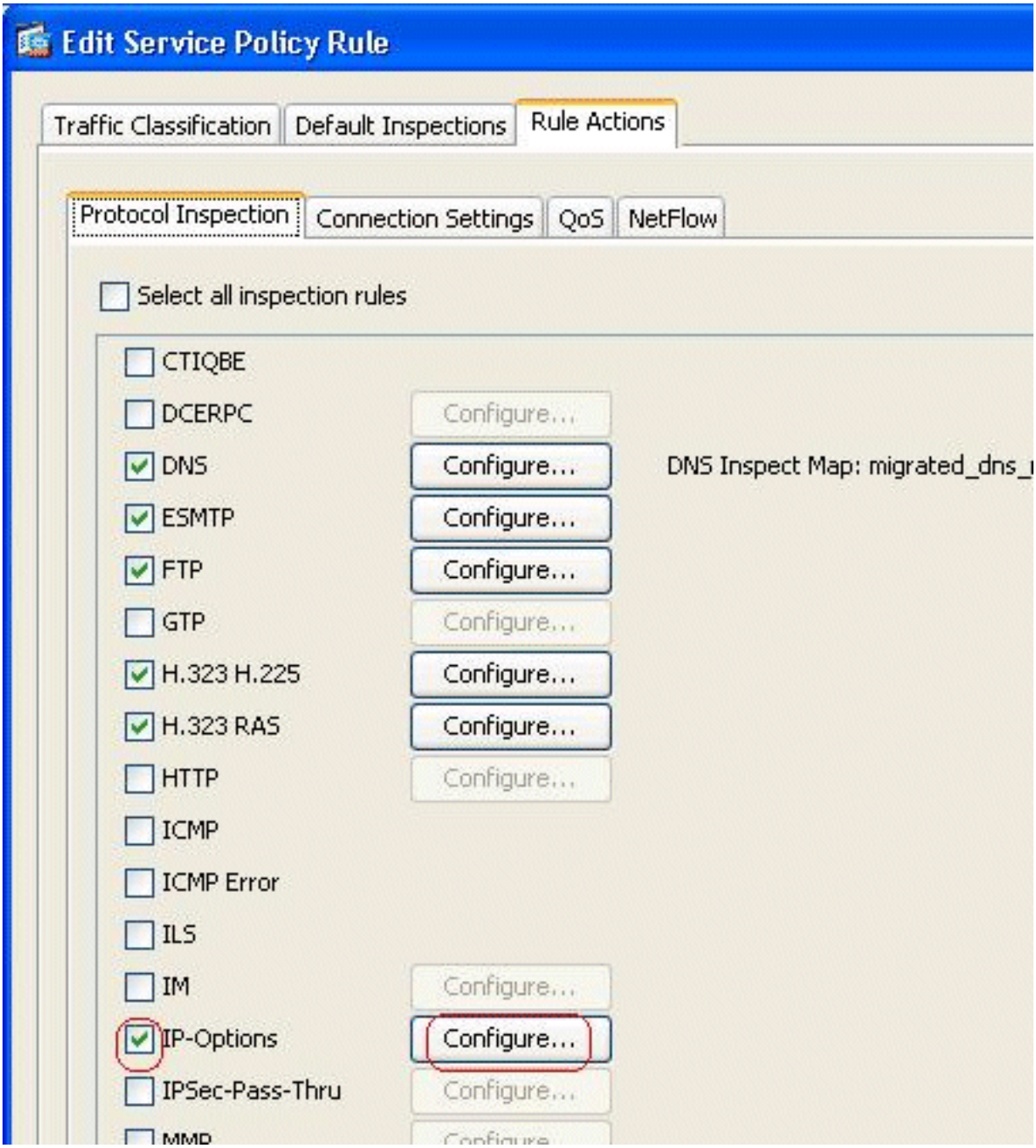


Nota: U sted puede también seleccionar el **claro el valor de la opción de la** opción de los **paquetes**, para inhabilitar este campo en el paquete del IP, y los paquetes pasan con Cisco ASA.

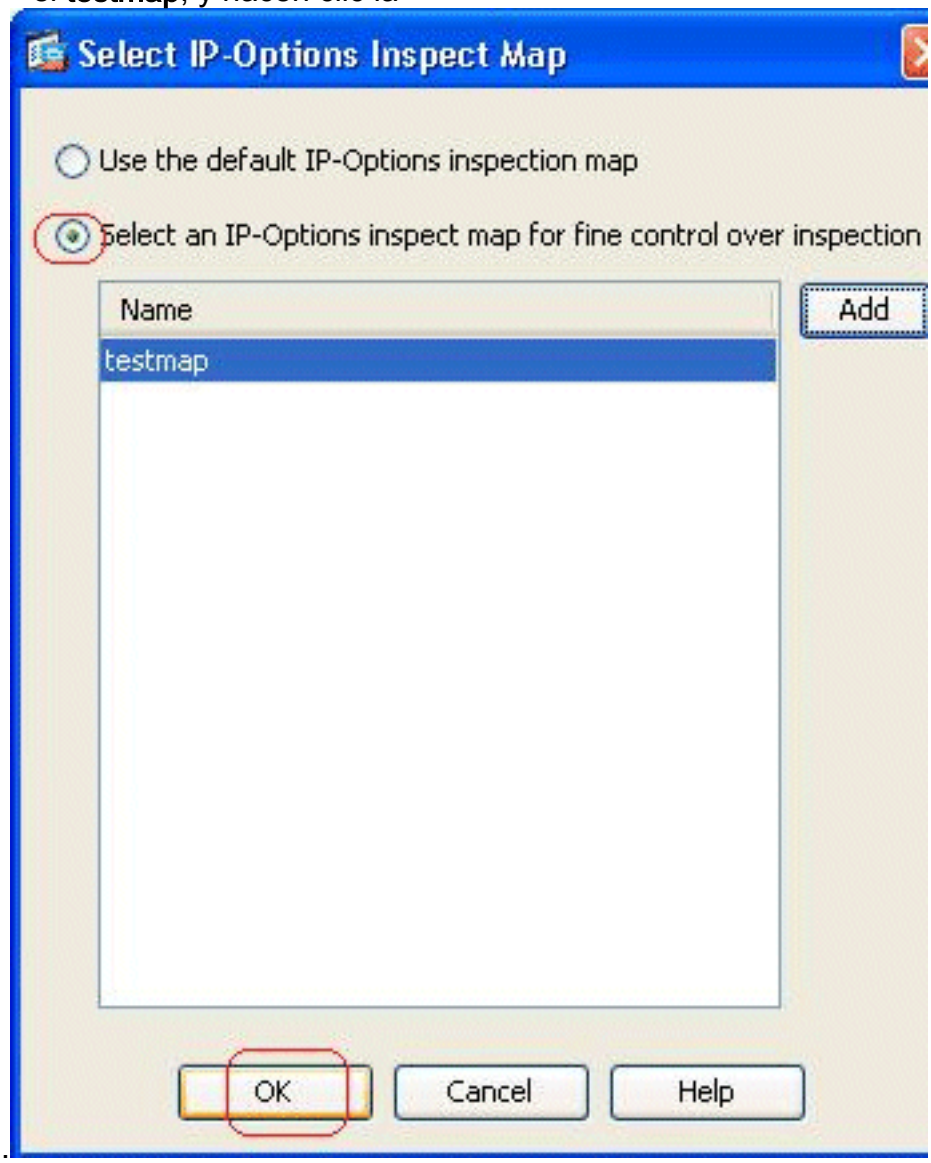
3. Se crea un nuevo examina el **testmap** llamado correspondencia. Haga clic en Apply (Aplicar).



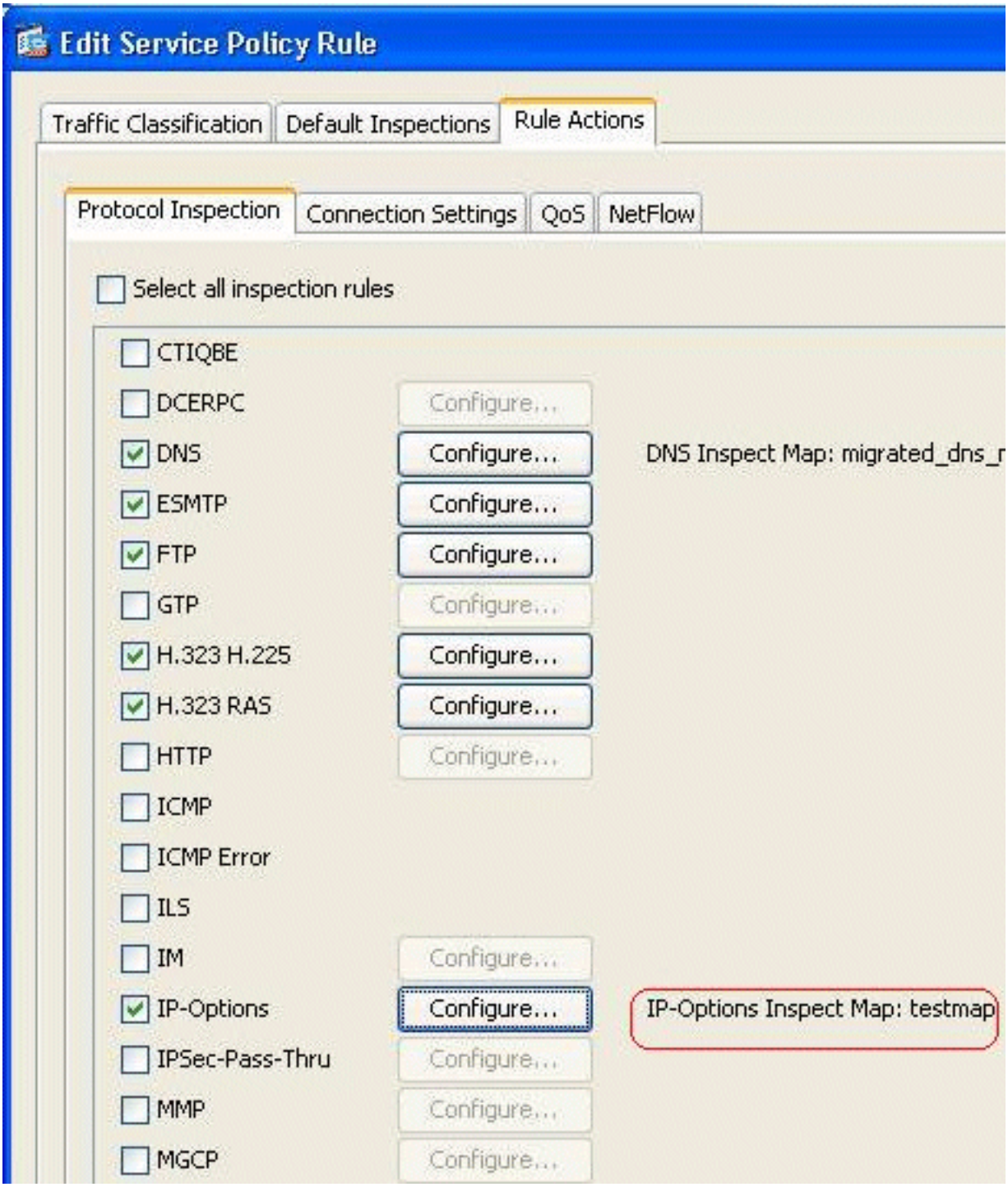
4. Vaya a las **reglas de la configuración** > del **Firewall** > de la **política de servicio**, seleccione la política global existente, y el tecleo **edita**. La ventana de la regla de la política de servicio del editar aparece. Seleccione las **acciones** lengueta de la **regla**, marca de tilde el elemento de las **opciones IP**, y elija la **configuración** para asignar la correspondencia creada recientemente del
examen.



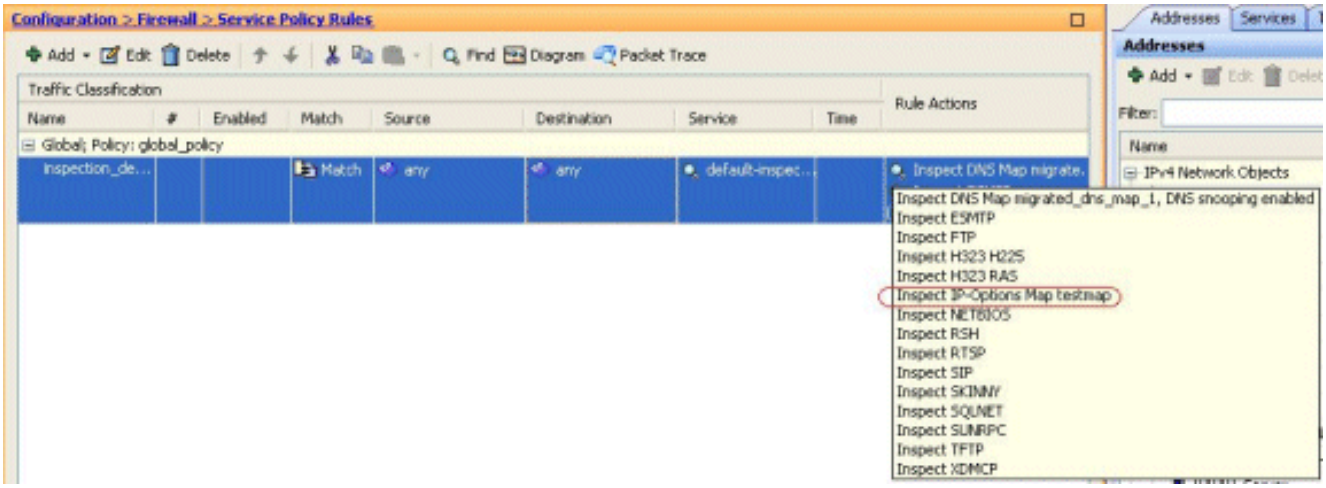
5. Elija **selecto las opciones IP examinan la correspondencia para saber si hay el control fino sobre el examen >** el **testmap**, y hacen clic la **AUTORIZACIÓN**.



6. Seleccionados examinan la correspondencia se pueden ver en el campo de **opciones IP**. Haga Click en OK para invertir de nuevo a la lengueta de las reglas de la política de servicio.



7. Con su ratón, libración sobre la lengueta de las **acciones de la regla** de modo que usted pueda encontrar todas las correspondencias disponibles del examen del protocolo asociadas a esta correspondencia
global.



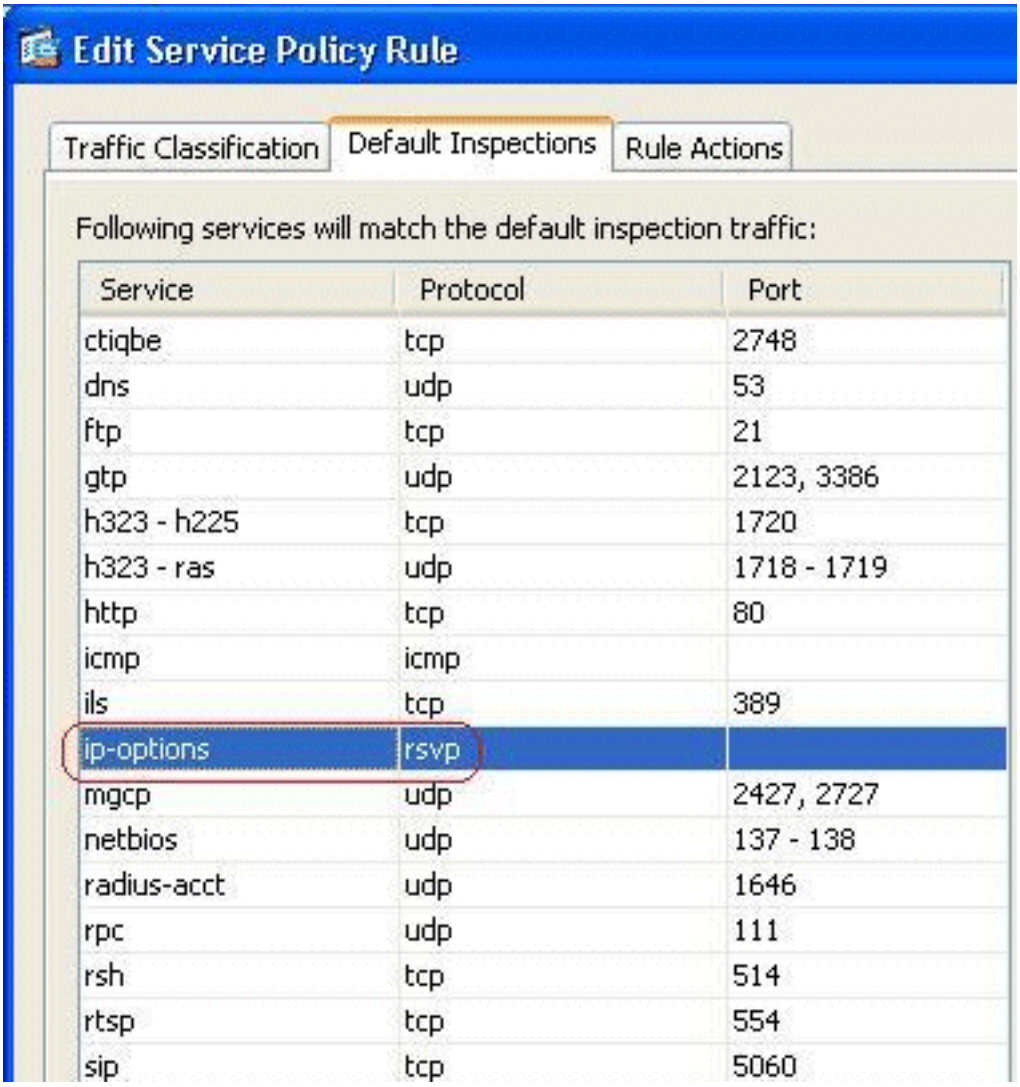
Aquí está un snippet de la muestra de la configuración CLI equivalente, para su referencia:

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
```

Comportamiento predeterminado de Cisco ASA para permitir los paquetes de RSVP

El examen de las opciones IP se habilita por abandono. Vaya a las **reglas de la configuración >** del **Firewall >** de la **política de servicio**. Seleccione la política global, el tecleo **edita**, y selecciona la lengueta de los **exámenes del valor por defecto**. Aquí, usted encontrará el protocolo de RSVP en el campo de **opciones IP**. Esto se asegura de que el protocolo de RSVP esté examinado y permitido con Cisco ASA. Como consecuencia, una llamada video de punta a punta se establece sin ningún problema.



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **la servicio-directiva de la demostración examina las IP-opciones** - Visualiza el número de paquetes caídos y/o permitidos según la regla configurada de la servicio-directiva.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte técnico del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Soporte Técnico y Documentación - Cisco Systems