Configuración de la Inspección de Opciones IP en ASDM 6.3 y posteriores

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de cómo configurar Cisco Adaptive Security Appliance (ASA) para pasar los paquetes IP con ciertas opciones IP habilitadas.

Prerequisites

Requirements

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.

- Cisco ASA que ejecuta la versión de software 8.3 y posteriores
- Cisco Adaptive Security Manager que ejecuta la versión de software 6.3 y posteriores

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.

Convenciones

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

Antecedentes

Cada paquete IP contiene un encabezado IP con un campo Options (Opciones). El campo Opciones, comúnmente denominado Opciones IP, proporciona funciones de control que son necesarias en algunas situaciones, pero innecesarias para la mayoría de las comunicaciones comunes. En particular, las opciones de IP incluyen disposiciones para sellos de hora, seguridad y routing especial. El uso de Opciones IP es opcional y el campo puede contener cero, una o más opciones.

Las opciones IP representan un riesgo para la seguridad y si un paquete IP con el campo Opciones IP habilitado pasa a través de ASA, filtrará información sobre la configuración interna de una red al exterior. Como resultado, un atacante puede asignar la topología de su red. Como Cisco ASA es un dispositivo que aplica la seguridad en la empresa, de forma predeterminada descarta los paquetes que tienen activado el campo Opciones IP. Aquí se muestra un ejemplo de mensaje de syslog para su referencia:

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||Denegar IP de 10.110.1.34 a XX.YY.ZZ.ZZ, opciones de IP:
"Alerta del router"
```

Sin embargo, en escenarios de implementación específicos en los que el tráfico de vídeo debe pasar a través de Cisco ASA, los paquetes IP con ciertas opciones IP deben pasar a través de otro modo, la llamada de videoconferencia podría fallar. A partir de la versión 8.2.2 del software Cisco ASA, se ha introducido una nueva función llamada "Inspección de las opciones IP". Con esta función, puede controlar qué paquetes con opciones IP específicas se permiten a través de Cisco ASA.

De forma predeterminada, esta función está activada y la inspección de las opciones IP siguientes se habilita en la política global. La configuración de esta inspección indica al ASA que permita que pase un paquete, o que borre las opciones IP especificadas y luego permita que pase el paquete.

- **Fin de lista de opciones (EOOL)** o **opción IP 0**: esta opción aparece al final de todas las opciones para marcar el final de una lista de opciones.
- **No Operation (NOP)** ni **IP Option 1**: este campo de opciones hace que la longitud total de la variable de campo sea la longitud total.
- **Alerta del router (RTRALT)** o **Opción IP 20**: esta opción notifica a los routers de tránsito que inspeccionen el contenido del paquete incluso cuando el paquete no está destinado a ese router.

Configurar

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

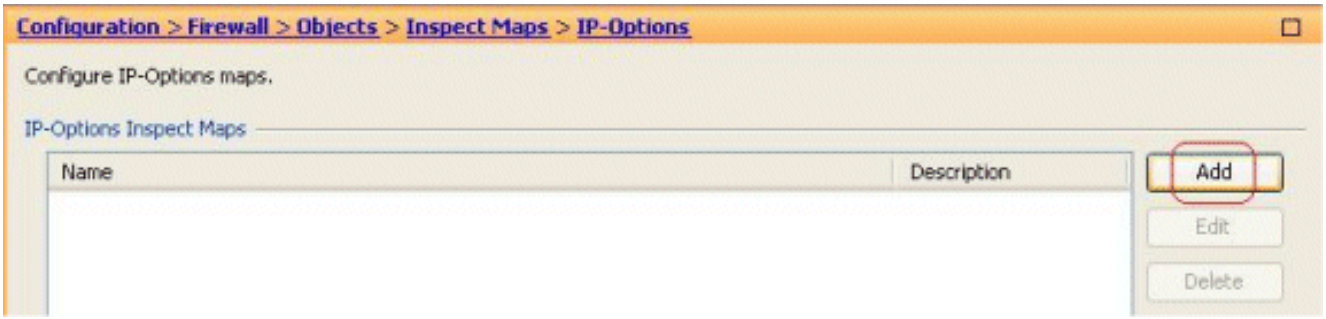
Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Configuración de ASDM

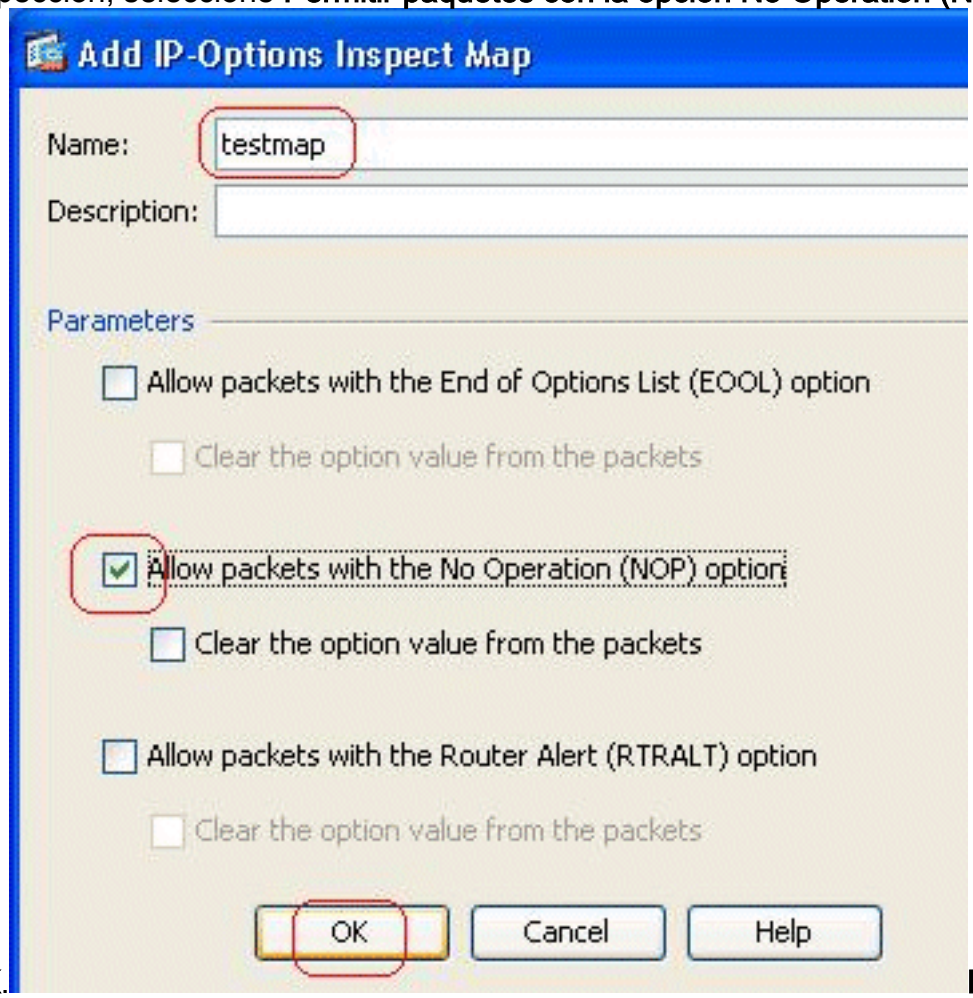
Mediante el ASDM, puede ver cómo habilitar la inspección de los paquetes IP que tienen el campo IP Options (Opciones de IP), NOP.

El campo Options (Opciones) del encabezado IP puede contener cero, una o más opciones, lo que hace que la longitud total de la variable de campo sea la misma. 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 Configuration > Firewall > Objects > **Inspect Maps > IP-Options** y haga clic en **Add**.

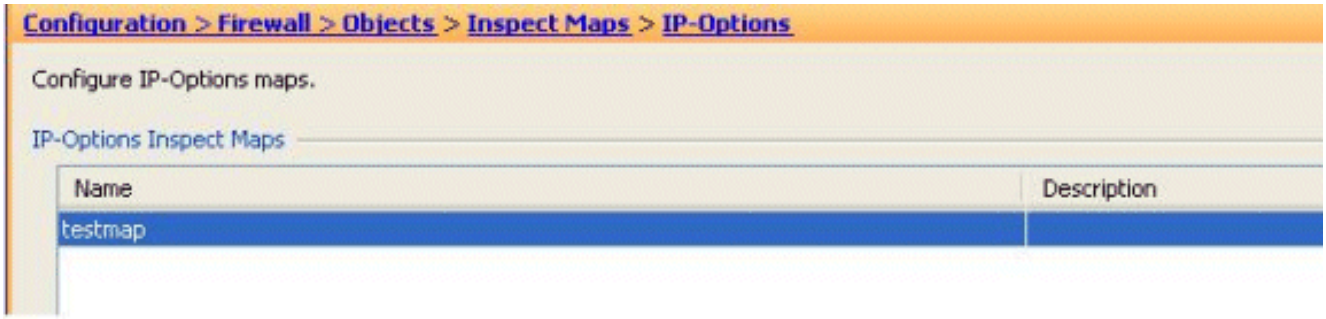


2. Aparece la ventana Add IP-Options Inspect Map . Especifique el nombre del mapa de inspección, seleccione **Permitir paquetes con la opción No Operation (NOP)** y haga clic en **OK**.

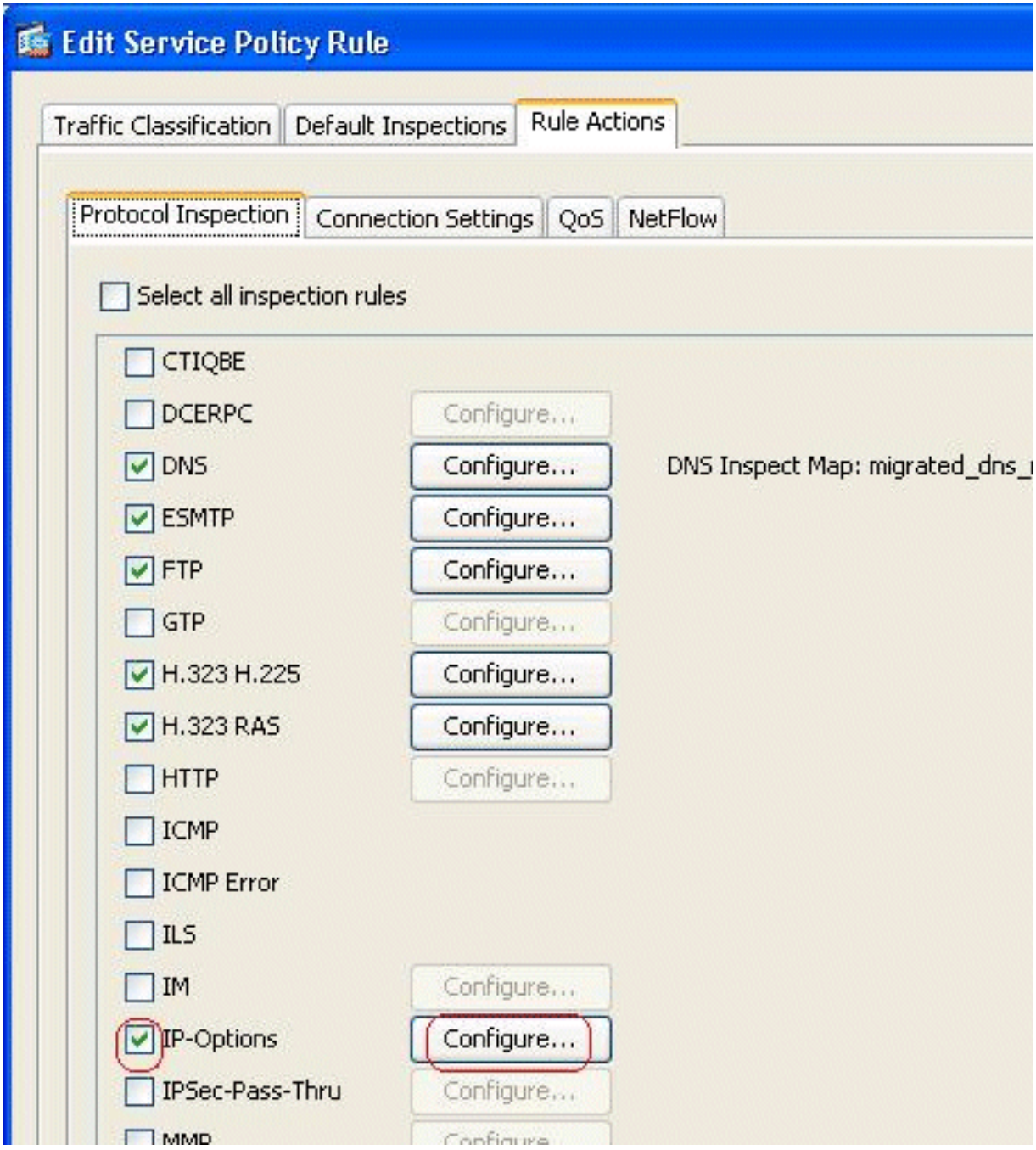


Nota: También puede seleccionar la **opción Borrar el valor de la** opción **de los paquetes**, de modo que este campo en el paquete IP esté inhabilitado y los paquetes pasen a través de Cisco ASA.

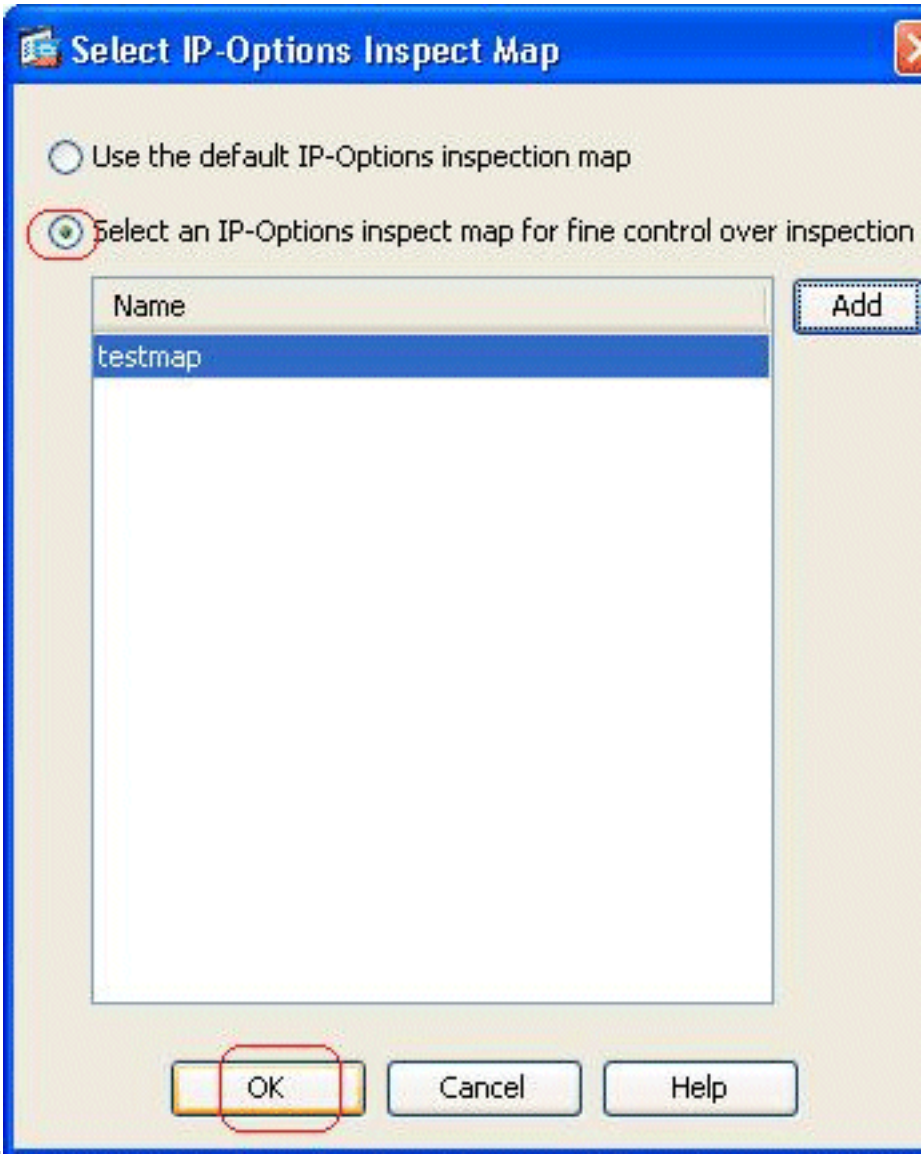
3. Se crea un nuevo mapa de inspección llamado **testmap**. Haga clic en Apply (Aplicar).



4. Vaya a **Configuration > Firewall > Service Policy Rules**, seleccione la política global existente y haga clic en **Edit**. Aparecerá la ventana Editar regla de política de servicio. Seleccione la ficha **Acciones de regla**, marque el **elemento Opciones IP** y elija **Configurar** para asignar el mapa de inspección recién
creado.

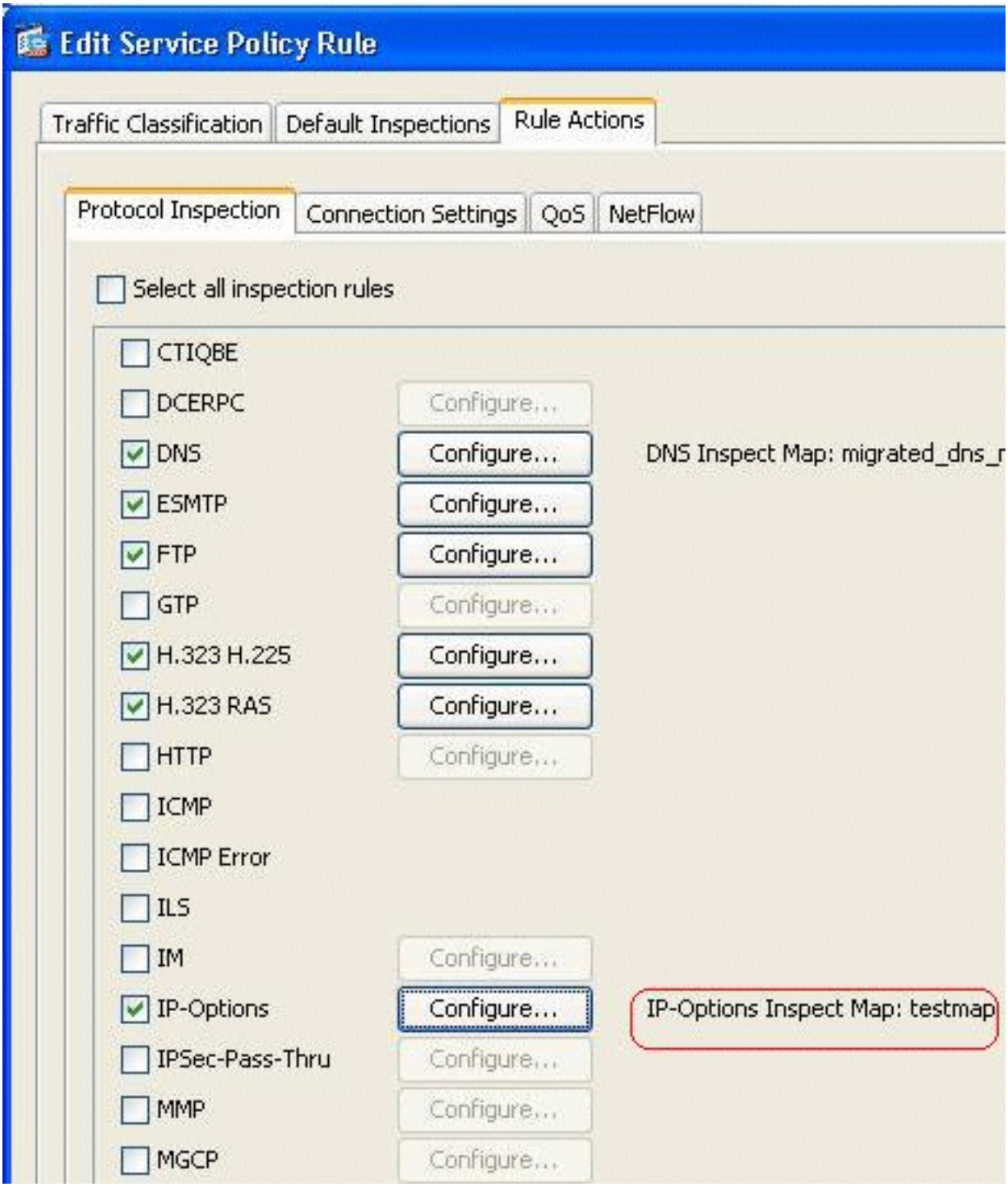


5. Elija **Select an IP-Options inspect map for fine control over inspection > testmap**, y haga clic

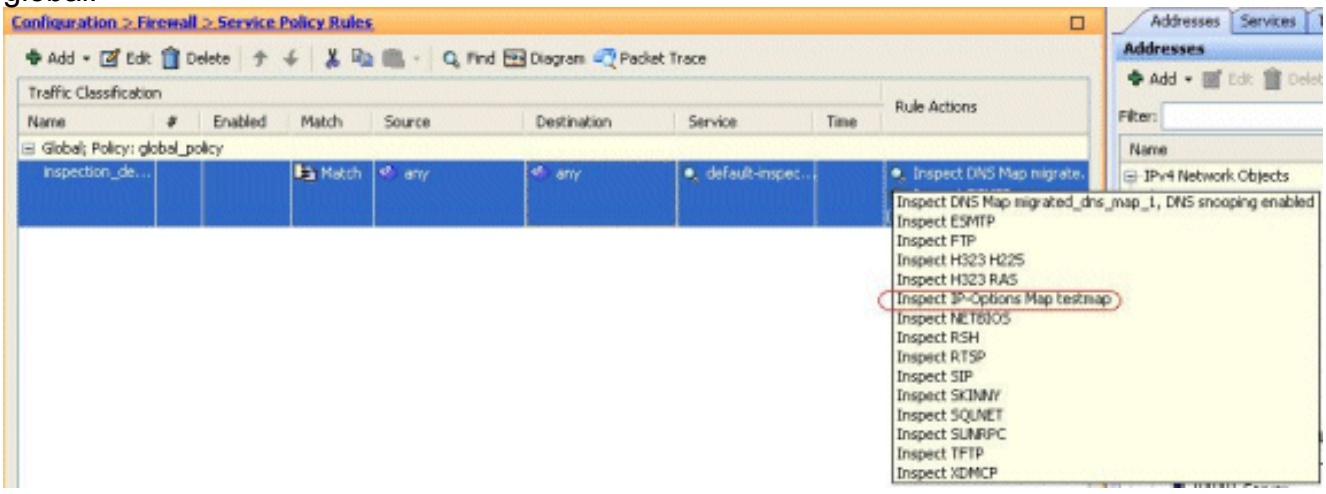


en **OK**.

6. El mapa de inspección seleccionado se puede ver en el campo **IP-Options**. Haga clic en **Aceptar** para volver a la pestaña Reglas de política de servicio.



7. Con el ratón, pase el cursor sobre la ficha **Acciones de regla** para que pueda encontrar todos los mapas de inspección de protocolo disponibles asociados con este mapa global.

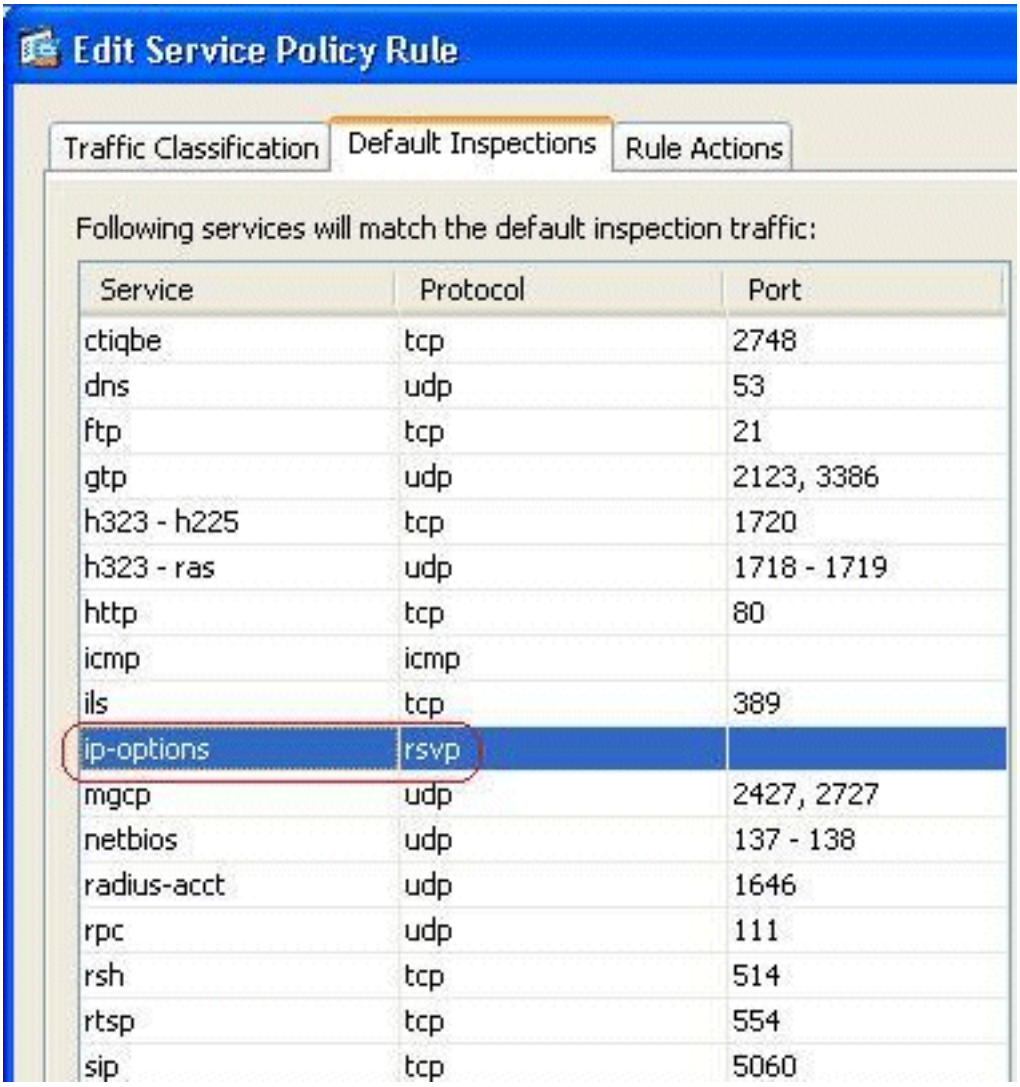


A continuación se muestra un fragmento de ejemplo de la configuración CLI equivalente para su referencia:

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 paquetes RSVP

La inspección de opciones IP está activada de forma predeterminada. Vaya a **Configuration > Firewall > Service Policy Rules**. Seleccione la política global, haga clic en **Editar** y seleccione la **ficha Inspecciones predeterminadas**. Aquí encontrará el protocolo RSVP en el campo **IP-Options**. Esto garantiza que el protocolo RSVP se inspeccione y se permita a través de Cisco ASA. Como resultado, se establece una videollamada de extremo a extremo 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.

- **show service-policy inspect ip-options** - Muestra el número de paquetes perdidos y/o permitidos según la regla de política de servicio configurada.

Troubleshoot

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

Información Relacionada

- Soporte técnico para dispositivos de seguridad adaptable Cisco ASA serie 5500
- Soporte Técnico y Documentación - Cisco Systems