IP-opties configureren: inspectie op ASDM 6.3 en hoger

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie van de manier waarop u de Cisco adaptieve security applicatie (ASA) moet configureren om de IP-pakketten door te geven met bepaalde enabled IP-opties.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA met actieve softwarerelease versie 8.3 en hoger
- Cisco Adaptieve Security Manager met softwarerelease 6.3 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Elk IP-pakket bevat een IP-header met een veld Opties. Het veld Opties, dat doorgaans IP-opties wordt genoemd, biedt bedieningsfuncties die in bepaalde situaties vereist zijn maar niet nodig zijn voor de meeste gebruikelijke communicatie. In het bijzonder, omvatten IP Opties bepalingen voor tijdstempels, veiligheid, en speciale routing. Gebruik van IP-opties is optioneel en het veld kan opties van nul, één of meer bevatten.

IP-opties is een beveiligingsrisico en als een IP-pakket met het veld IP-opties ingeschakeld door ASA wordt doorgegeven, zal dit informatie over de interne installatie van een netwerk naar buiten lekken. Als resultaat, kan een aanvaller de topologie van uw netwerk in kaart brengen. Aangezien Cisco ASA een apparaat is dat veiligheid in de onderneming afdwingt, laat het standaard de pakketten vallen die het veld IP Opties hebben ingeschakeld. Hier verschijnt een voorbeeldmelding voor uw referentie:

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||Dense IP van 10.110.1.34 tot XX.YY.ZZ.ZZ, IP-opties:
"routerwaarschuwing"
```

In specifieke implementatiescenario's waarin videoverkeer door Cisco ASA moet passeren moeten IP-pakketten met bepaalde IP-opties echter door worden doorgegeven anders kan de videoconferentieoproep mislukken. Vanaf Cisco ASA software release versie 8.2.2 is een nieuwe functie met de naam "Inspection for IP Opties" geïntroduceerd. Met deze functie kunt u controleren welke pakketten met specifieke IP-opties door Cisco ASA zijn toegestaan.

Deze optie is standaard ingeschakeld en de inspectie voor de onderstaande IP-opties is ingeschakeld in het wereldwijde beleid. Het configureren van deze inspectie geeft de ASA instructies om een pakje toe te staan om door te geven of om de gespecificeerde IP opties te wissen en dan het pakje toe te laten om door te geven.

- **End-of-life lijst met opties (End-of-life)** of **IP optie 0** - deze optie verschijnt aan het einde van alle opties om het einde van een lijst met opties te markeren.
- **Geen bediening (NOP)** of **IP optie 1** - Het veld Deze opties maakt de totale lengte van de veldvariabele.
- **Router Alert (RTRALT)** of **IP optie 20** - Deze optie meldt doorvoerrouters om de inhoud van het pakket te controleren, zelfs wanneer het pakket niet voor die router is bestemd.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

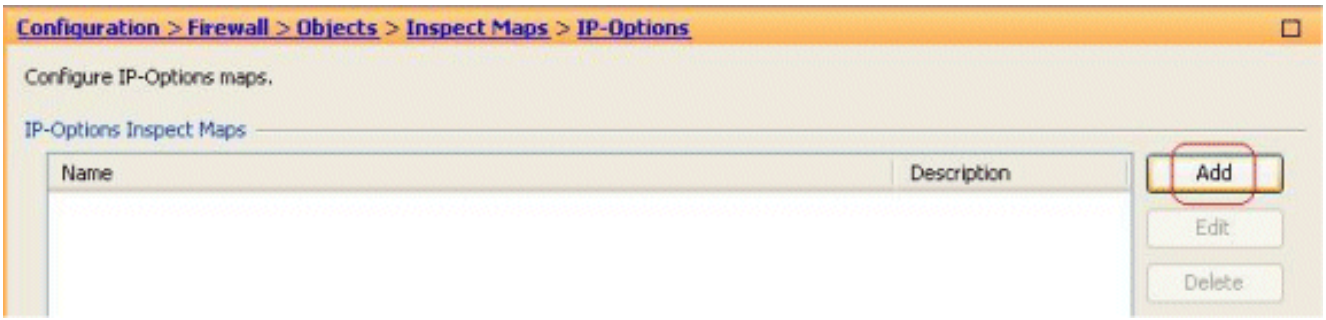
Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

ASDM-configuratie

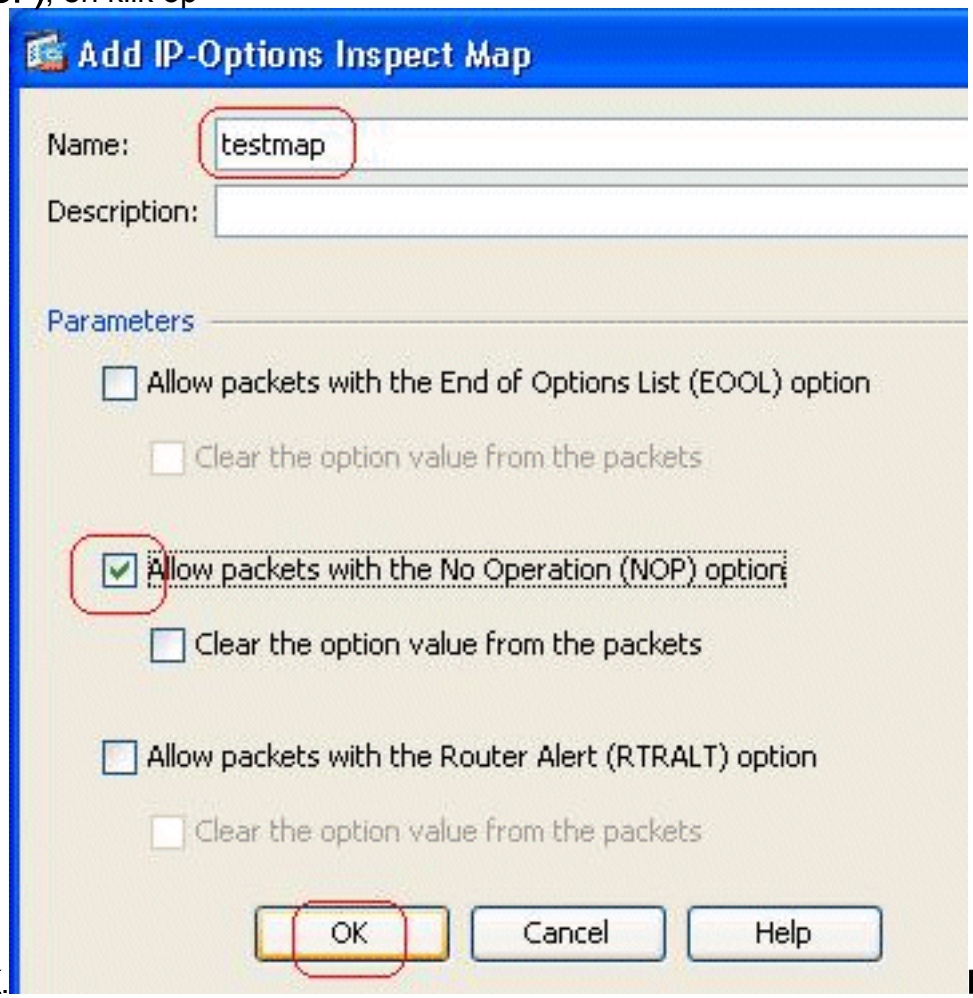
Wanneer u ASDM gebruikt, kunt u zien hoe u de inspectie voor de IP-pakketten kunt inschakelen die het veld IP-opties hebben.

Het veld Opties in de IP-kop kan opties van nul, één of meer bevatten, waardoor de totale lengte van de veldvariabele wordt gemaakt. De IP-header moet echter uit 32 bits bestaan. Als het aantal bits van alle opties geen veelvoud van 32 bits is, wordt de NOP optie gebruikt als "interne padding" om de opties op een 32-bits grens uit te lijnen.

1. Ga naar **Configuration > Firewall > Objects > Kaarten > IP-Opties en klik op Add.**

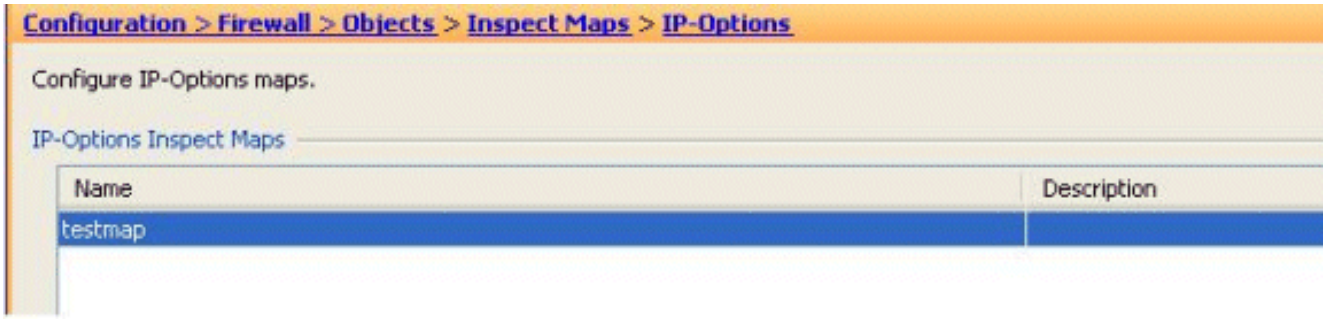


2. Het venster Map toevoegen aan IP-opties voor inspectie verschijnt. Specificeer de naam van de Kaart van de Inspectie, selecteer **toestaan pakketten met de optie Geen Handeling (NOP)**, en klik op **OK**.

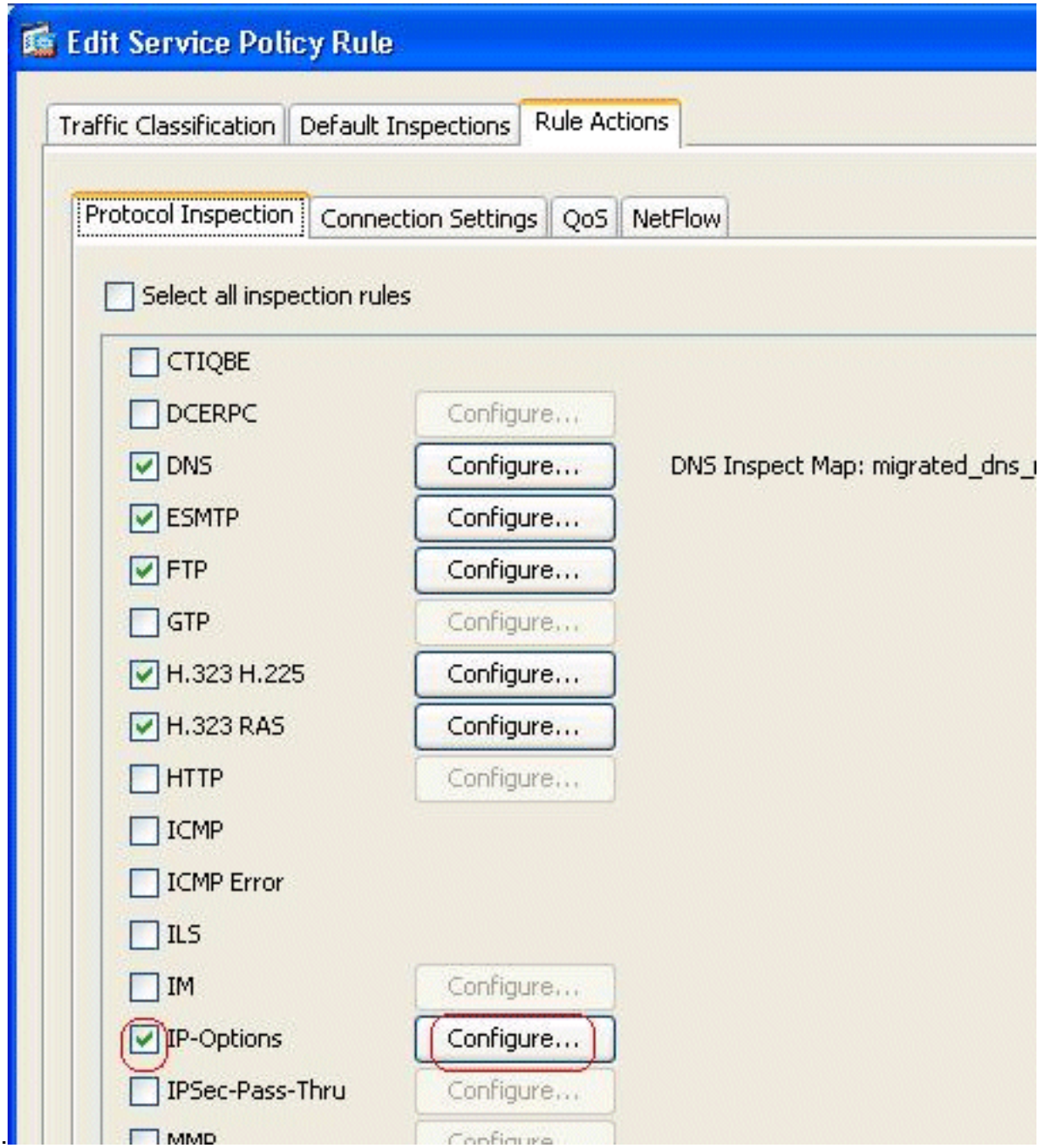


N.B.: U kunt ook de **optie** wissen **uit de** optie **Packets** selecteren, zodat dit veld in het IP-pakket wordt uitgeschakeld en de pakketten door de Cisco ASA worden verzonden.

3. Er wordt een nieuwe inspectiekaart, **testmap** genaamd, gecreëerd. Klik op **Apply** (Toepassen).

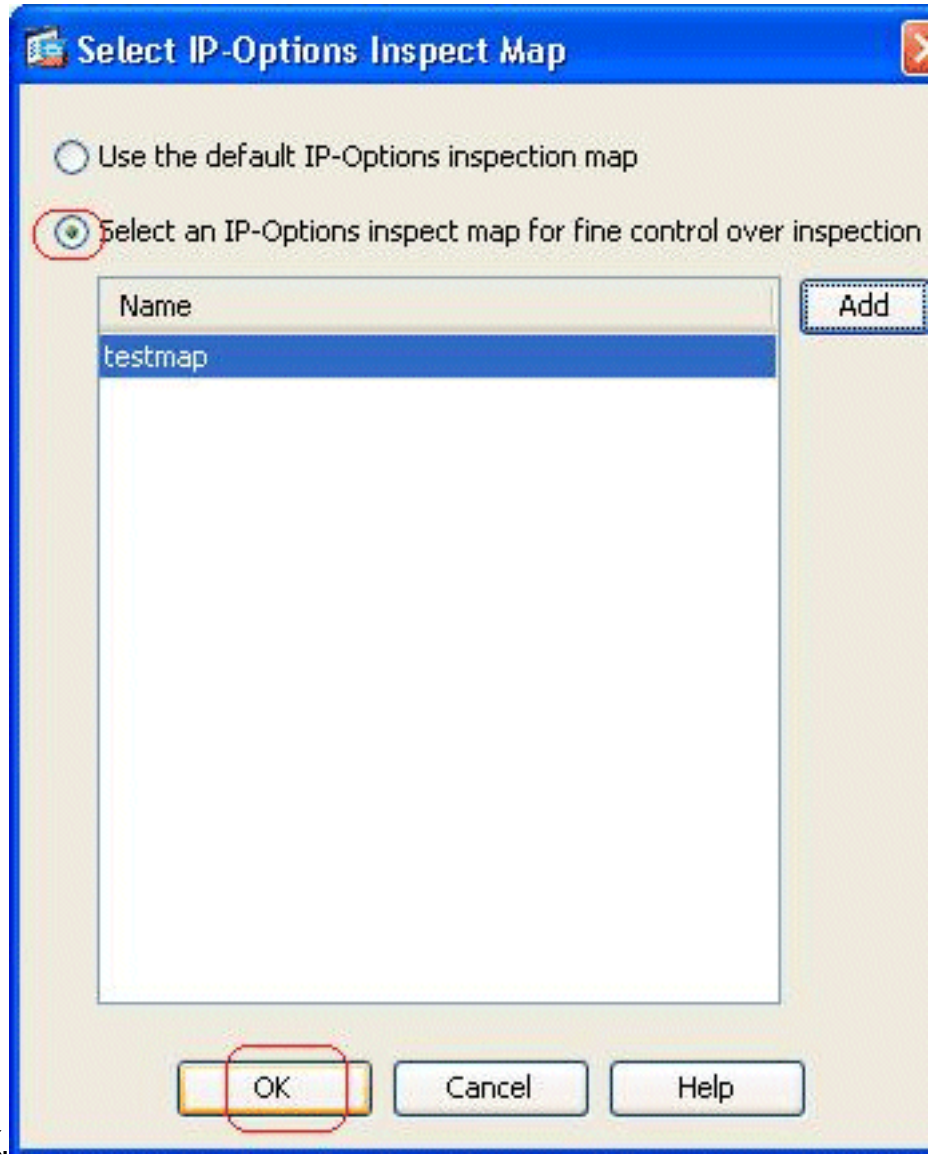


4. Ga naar **Configuration > Firewall > Service Policy Rules**, selecteer het bestaande wereldwijde beleid en klik op **Bewerken**. Het venster Service Policy Rule verschijnt. Selecteer het tabblad **Regel**, controleer de optie **IP-opties** en kies **Configureren** om de nieuwe inspectiekaart toe te



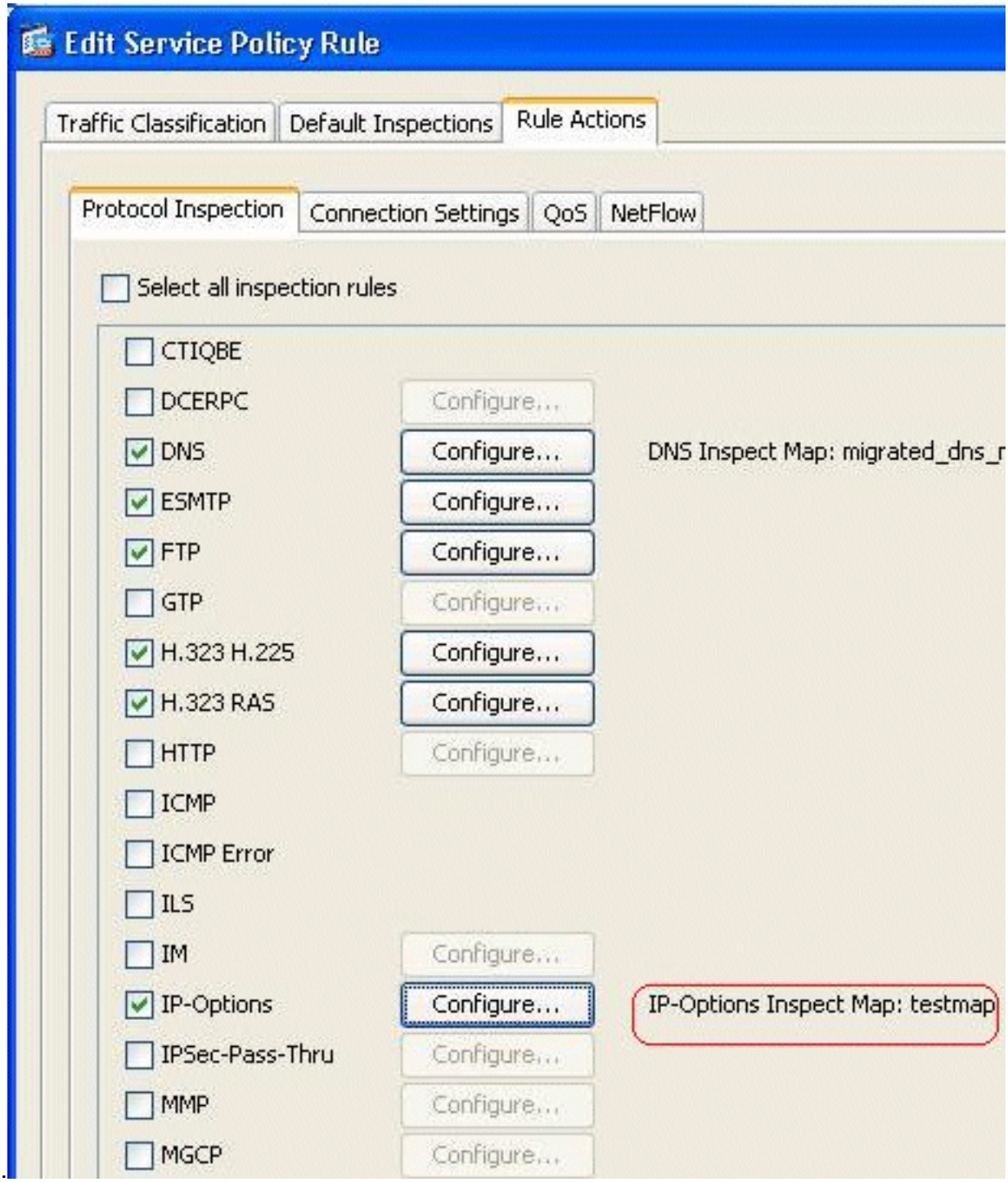
wijzen.

5. Kies **een IP-Opties waarin u een inspectiekaart selecteert voor een fijnere controle over de inspectie > testmap** en klik op



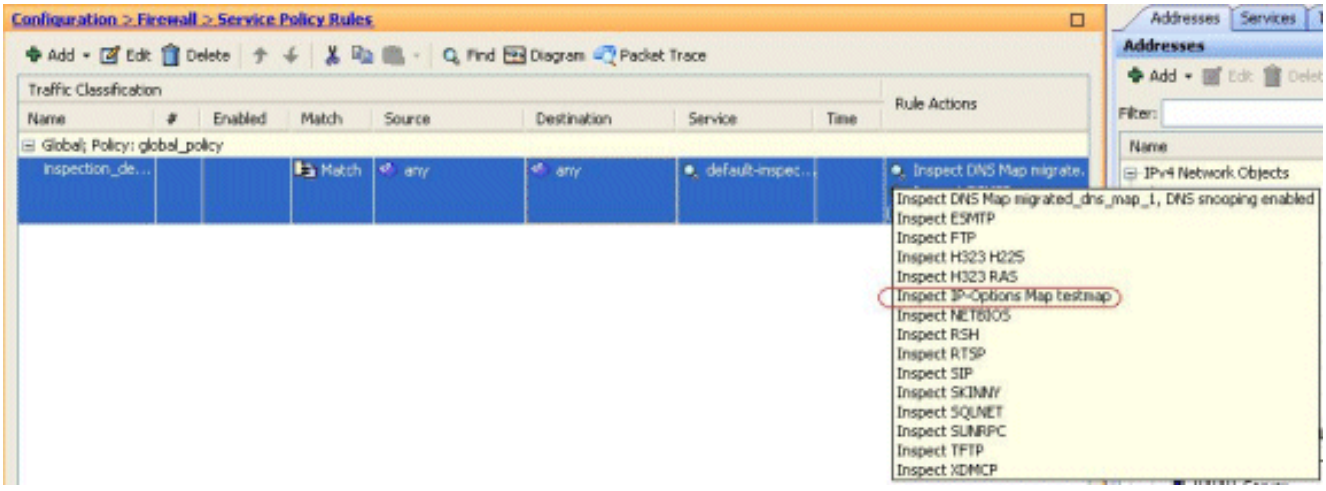
OK.

6. De geselecteerde kaart voor inspectie kan in het veld **IP-opties** worden bekeken. Klik op **OK** om terug te keren naar het tabblad Service Policy



Rules.

7. Met uw muis, beweegt u het tabblad **Regel** zodat u alle beschikbare inspectiekaarten van het protocol kunt vinden die bij deze globale kaart horen.



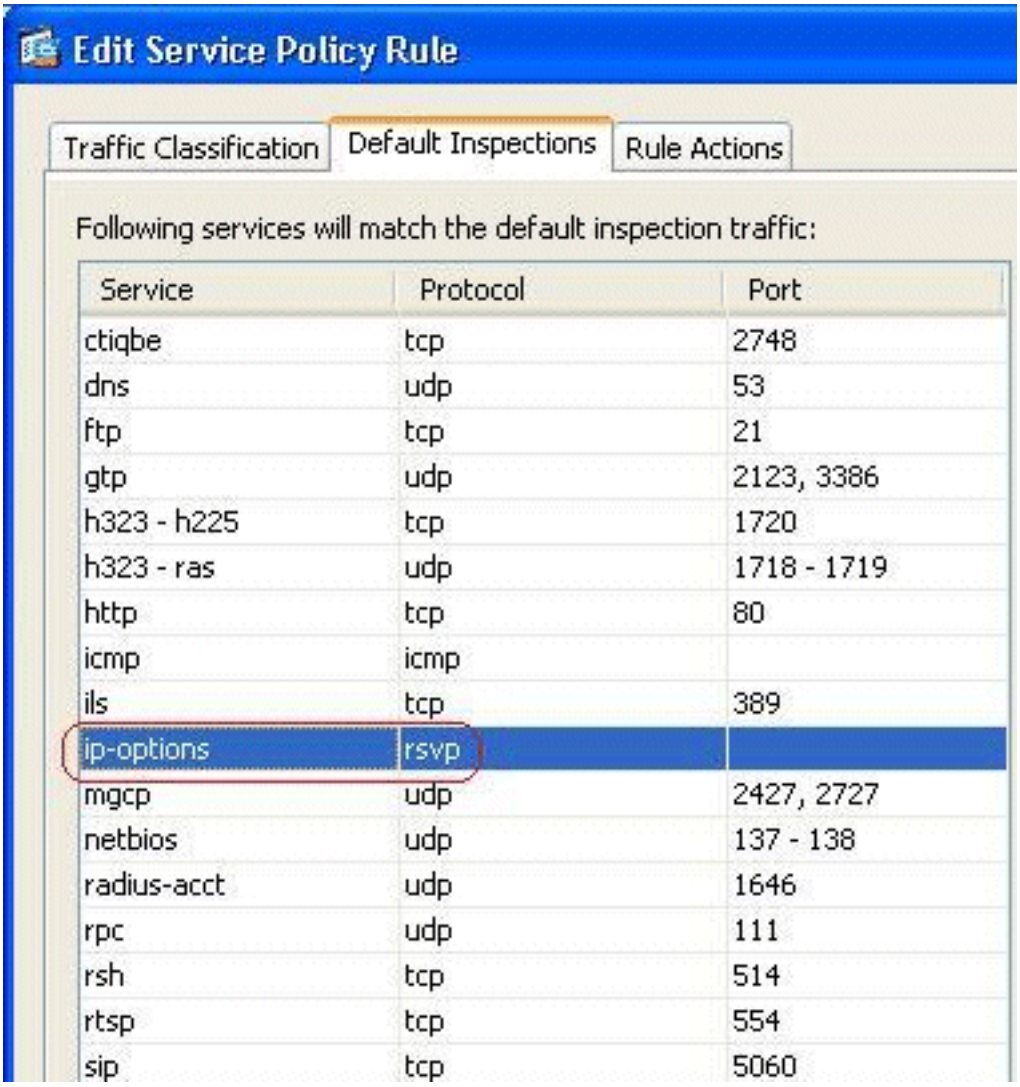
Hier is een voorbeeldfragment van de equivalente CLI-configuratie, voor uw referentie:

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
```

Standaardgedrag van Cisco ASA om RSVP-pakketten toe te staan

De IP-opties zijn standaard ingeschakeld. Ga naar **Configuration > Firewall > Service Policy rules**. Selecteer het tabblad Algemeen, klik op **Bewerken** en selecteer het tabblad **Standaardinspectie**. Hier vindt u het RSVP-protocol in het veld **IP-opties**. Dit garandeert dat het RSVP-protocol via Cisco ASA wordt geïnspecteerd en toegestaan. Als resultaat hiervan wordt een end-to-end videogesprek zonder probleem opgezet.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **Toon service-beleid controle ip-opties** - Toont het aantal pakketten dat is gedropt en/of toegestaan volgens de geconfigureerde service-beleidsregel.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties voor technische ondersteuning
- Technische ondersteuning en documentatie – Cisco Systems