Configurer l'inspection des options IP sur ASDM 6.3 et versions ultérieures

Contenu

Introduction

Ce document fournit un exemple de configuration de la façon de configurer l'appareil de sécurité adaptatif (ASA) de Cisco afin de transmettre les paquets IP avec certaines options IP activées.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASA exécutant la version logicielle 8.3 et ultérieure
- Cisco Adaptive Security Manager exécutant les versions 6.3 et ultérieures du logiciel

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Chaque paquet IP contient un en-tête IP avec un champ Options. Le champ Options, communément appelé Options IP, fournit des fonctions de contrôle requises dans certaines situations, mais inutiles pour la plupart des communications courantes. En particulier, les options IP incluent des dispositions relatives aux horodatages, à la sécurité et au routage spécial. L'utilisation des options IP est facultative et le champ peut contenir zéro, une ou plusieurs options.

Les options IP représentent un risque pour la sécurité et si un paquet IP avec le champ Options IP activé est transmis via ASA, il fuit des informations sur la configuration interne d'un réseau vers l'extérieur. Par conséquent, un pirate peut mapper la topologie de votre réseau. Comme Cisco ASA est un périphérique qui applique la sécurité dans l'entreprise, par défaut, il supprime les paquets dont le champ Options IP est activé. Un exemple de message syslog est affiché ici, pour référence :

```
106012|10.110.1.34||XX.YY.ZZ.ZZ||Refuser IP de 10.110.1.34 à XX.YY.ZZ.ZZ, options IP : « Alerte routeur »
```

Cependant, dans des scénarios de déploiement spécifiques où le trafic vidéo doit passer par Cisco ASA, les paquets IP avec certaines options IP doivent être transmis par le biais de l'option de vidéoconférence. À partir de la version 8.2.2 du logiciel Cisco ASA, une nouvelle fonctionnalité appelée « Inspection des options IP » a été introduite. Avec cette fonctionnalité, vous pouvez contrôler quels paquets avec des options IP spécifiques sont autorisés via Cisco ASA.

Par défaut, cette fonctionnalité est activée et l'inspection des options IP ci-dessous est activée dans la stratégie globale. La configuration de cette inspection demande à l'ASA d'autoriser l'acheminement d'un paquet, ou d'effacer les options IP spécifiées, puis de laisser passer le paquet.

- **End of Options List (EOOL)** ou **IP Option 0** - Cette option apparaît à la fin de toutes les options afin de marquer la fin d'une liste d'options.
- **No Operation (NOP)** ou **IP Option 1** - Ce champ d'options fait la longueur totale de la variable de champ.
- **Router Alert (RTRALT)** ou **IP Option 20** - Cette option avertit les routeurs de transit d'inspecter le contenu du paquet même lorsque le paquet n'est pas destiné à ce routeur.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

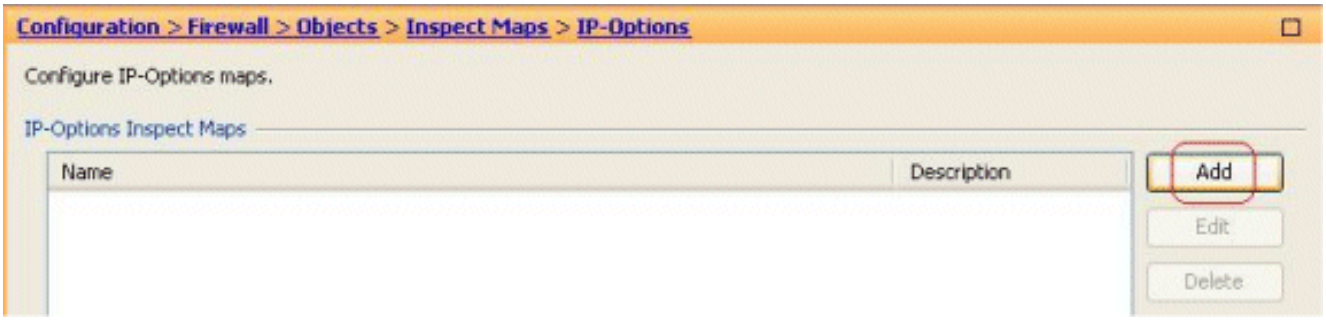
Configuration ASDM

Àl'aide de l'ASDM, vous pouvez voir comment activer l'inspection pour les paquets IP qui ont le

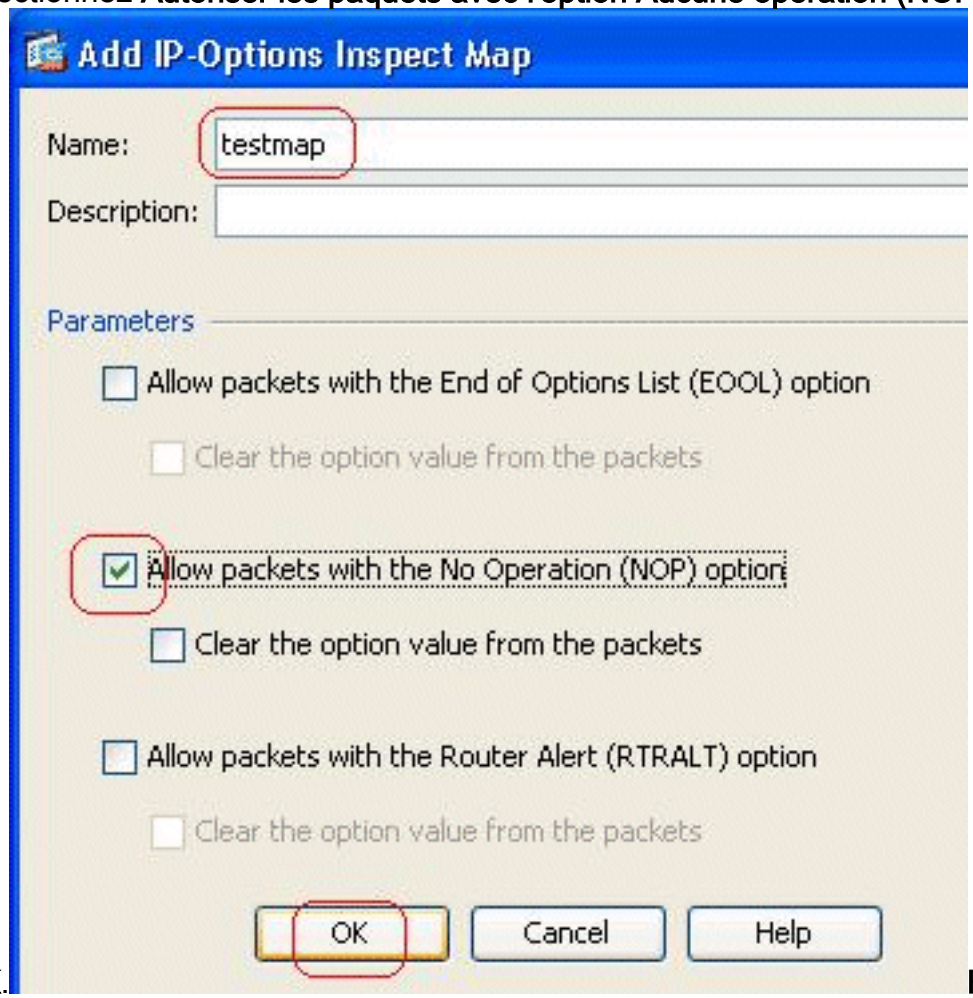
champ Options IP, NOP.

Le champ Options de l'en-tête IP peut contenir zéro, une ou plusieurs options, ce qui fait la longueur totale de la variable de champ. Cependant, l'en-tête IP doit être un multiple de 32 bits. Si le nombre de bits de toutes les options n'est pas un multiple de 32 bits, l'option NOP est utilisée comme « remplissage interne » afin d'aligner les options sur une limite de 32 bits.

1. Accédez à Configuration > Firewall > Objects > **Inspect Maps** > **IP-Options**, puis cliquez sur **Add**.

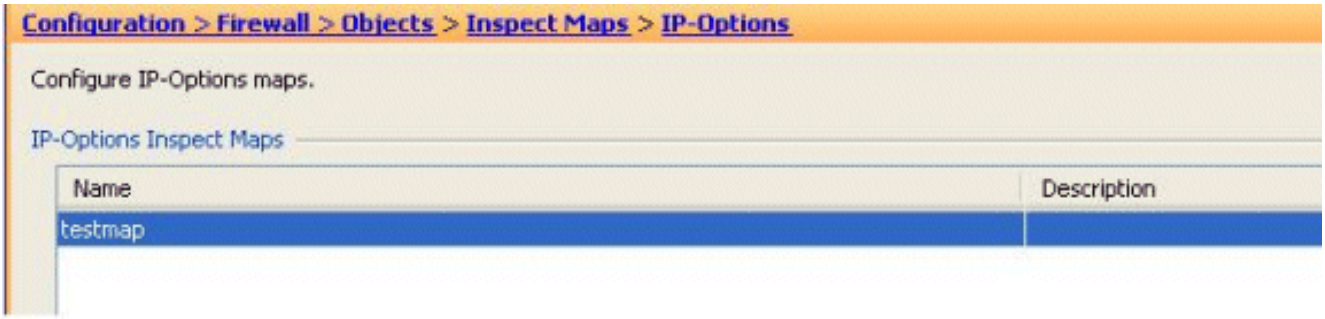


2. La fenêtre Add IP-Options Inspect Map s'affiche. Spécifiez le nom de la carte d'inspection, sélectionnez **Autoriser les paquets avec l'option Aucune opération (NOP)** et cliquez sur **OK**.

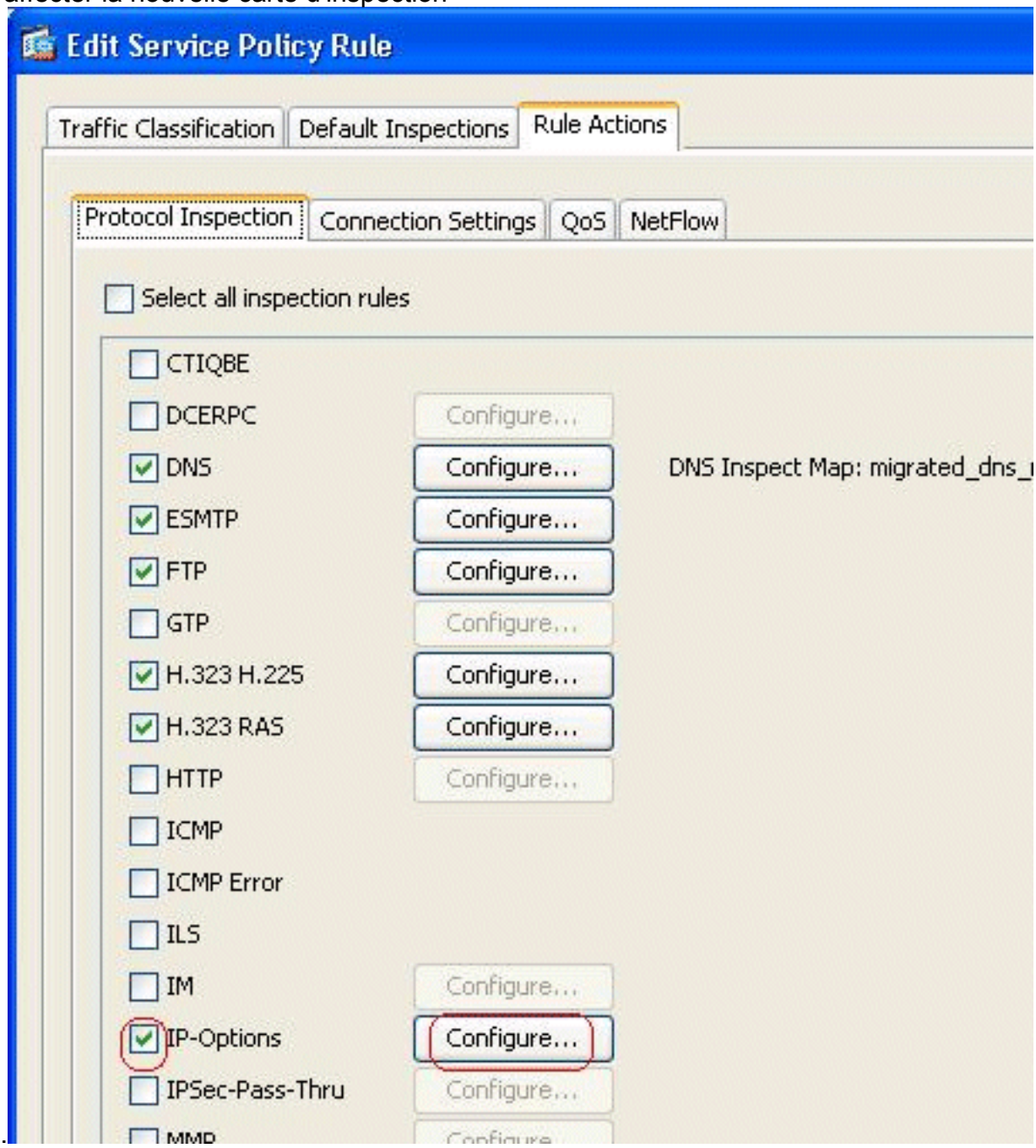


Remarque : Vous pouvez également sélectionner la **valeur Clear the option de l'**option **Packets**, afin que ce champ du paquet IP soit désactivé et que les paquets passent par Cisco ASA.

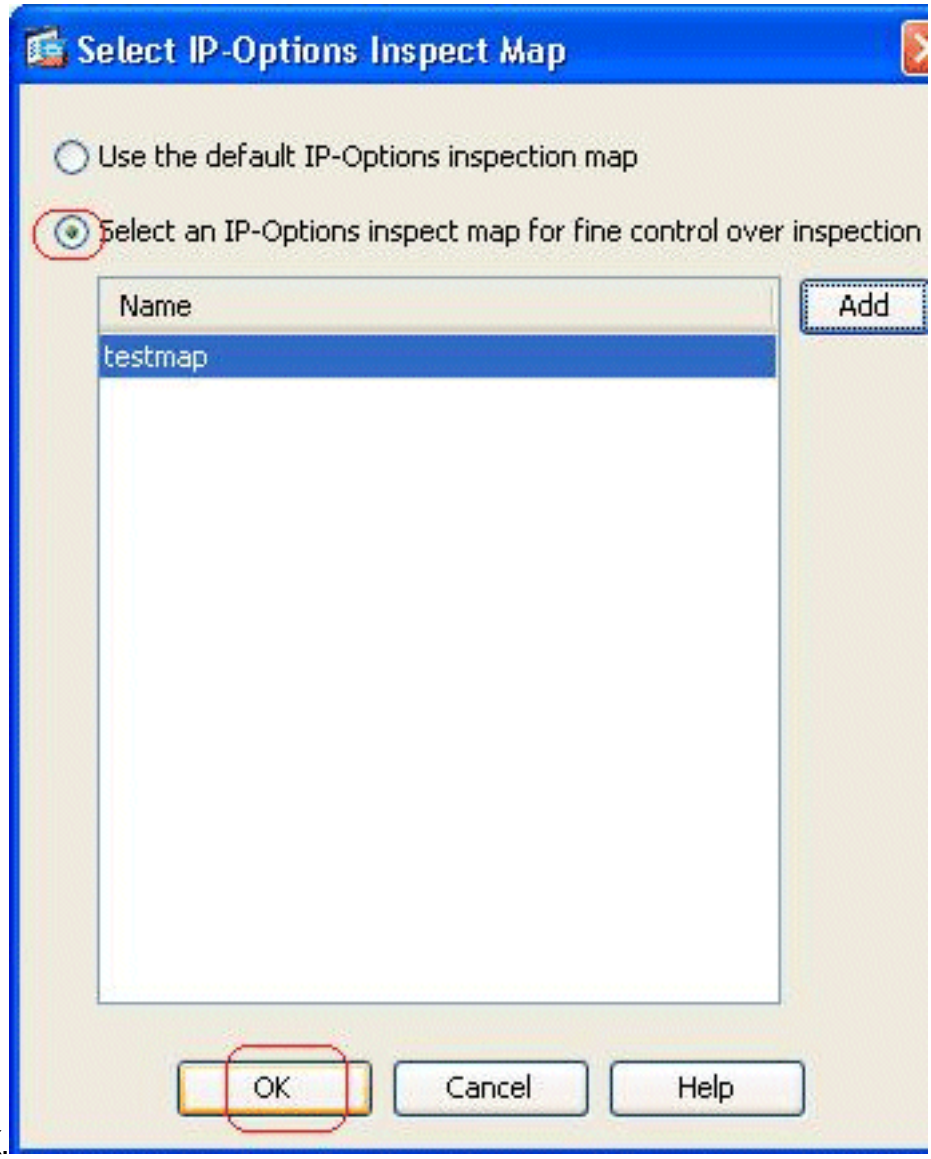
3. Une nouvelle carte d'inspection appelée **testmap** est créée. Cliquez sur Apply.



4. Accédez à **Configuration > Firewall > Service Policy Rules**, sélectionnez la stratégie globale existante et cliquez sur **Edit**. La fenêtre Modifier la règle de stratégie de service s'affiche. Sélectionnez l'onglet **Actions de règle**, cochez l'élément **Options IP** et choisissez **Configurer** afin d'affecter la nouvelle carte d'inspection créée.

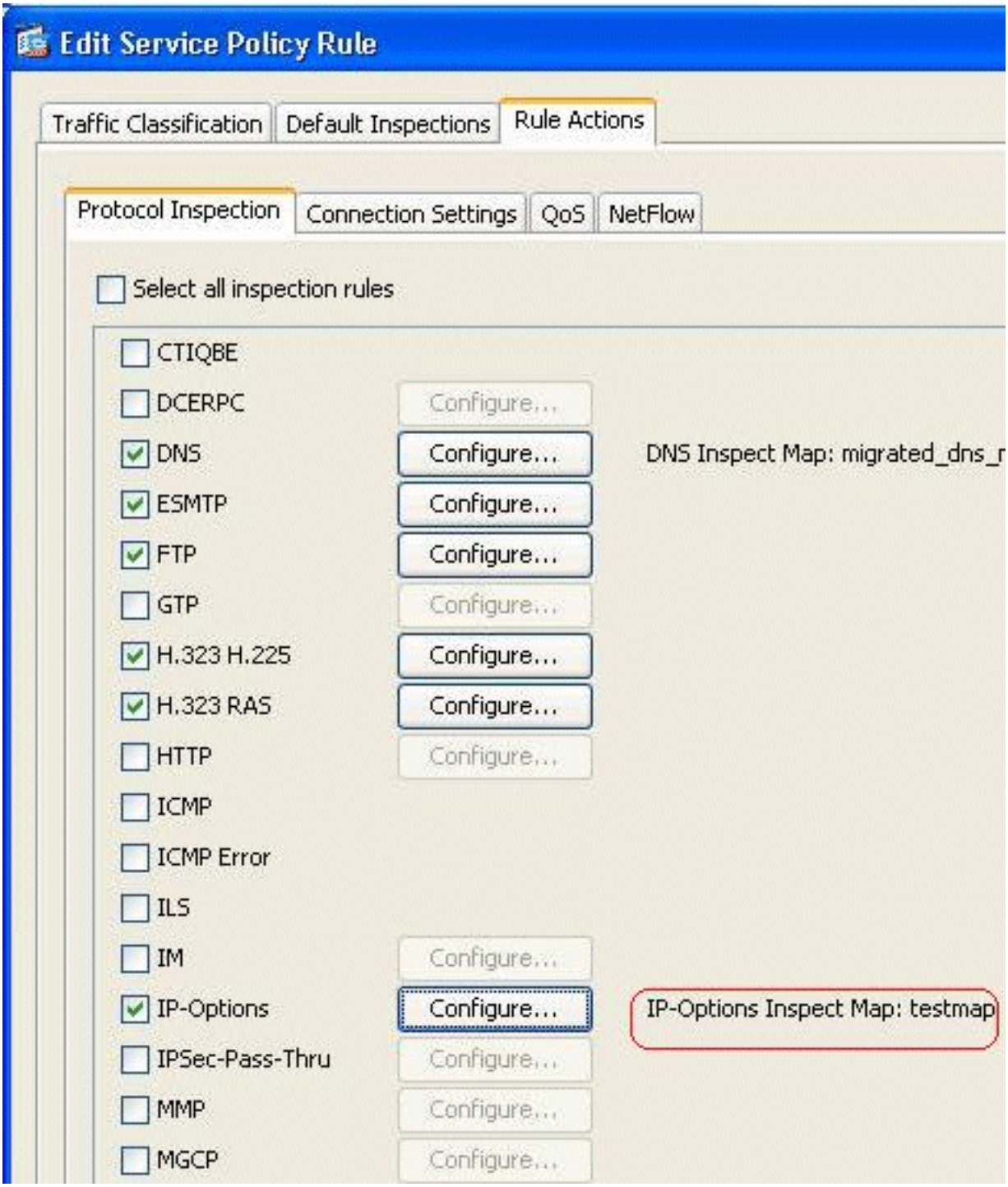


5. Choisissez **Sélectionner une carte d'inspection IP-Options pour un contrôle précis sur l'inspection > testmap**, puis cliquez sur

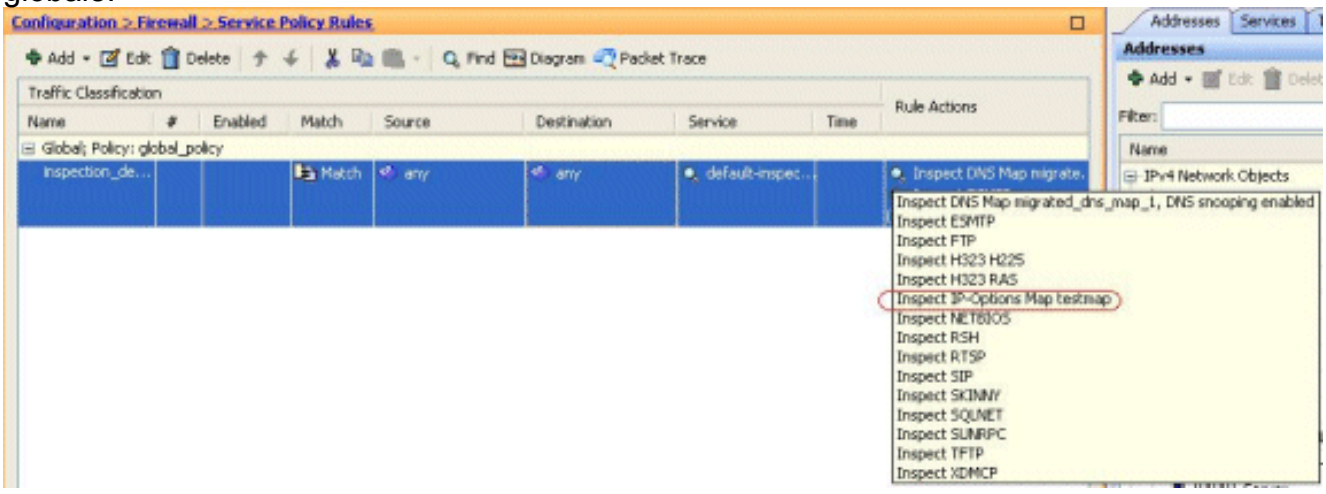


OK.

6. La carte d'inspection sélectionnée peut être affichée dans le champ **Options IP**. Cliquez sur **OK** pour revenir à l'onglet Règles de stratégie de service.



7. Avec la souris, survolez l'onglet **Actions de règle** pour trouver toutes les cartes d'inspection de protocole disponibles associées à cette carte globale.



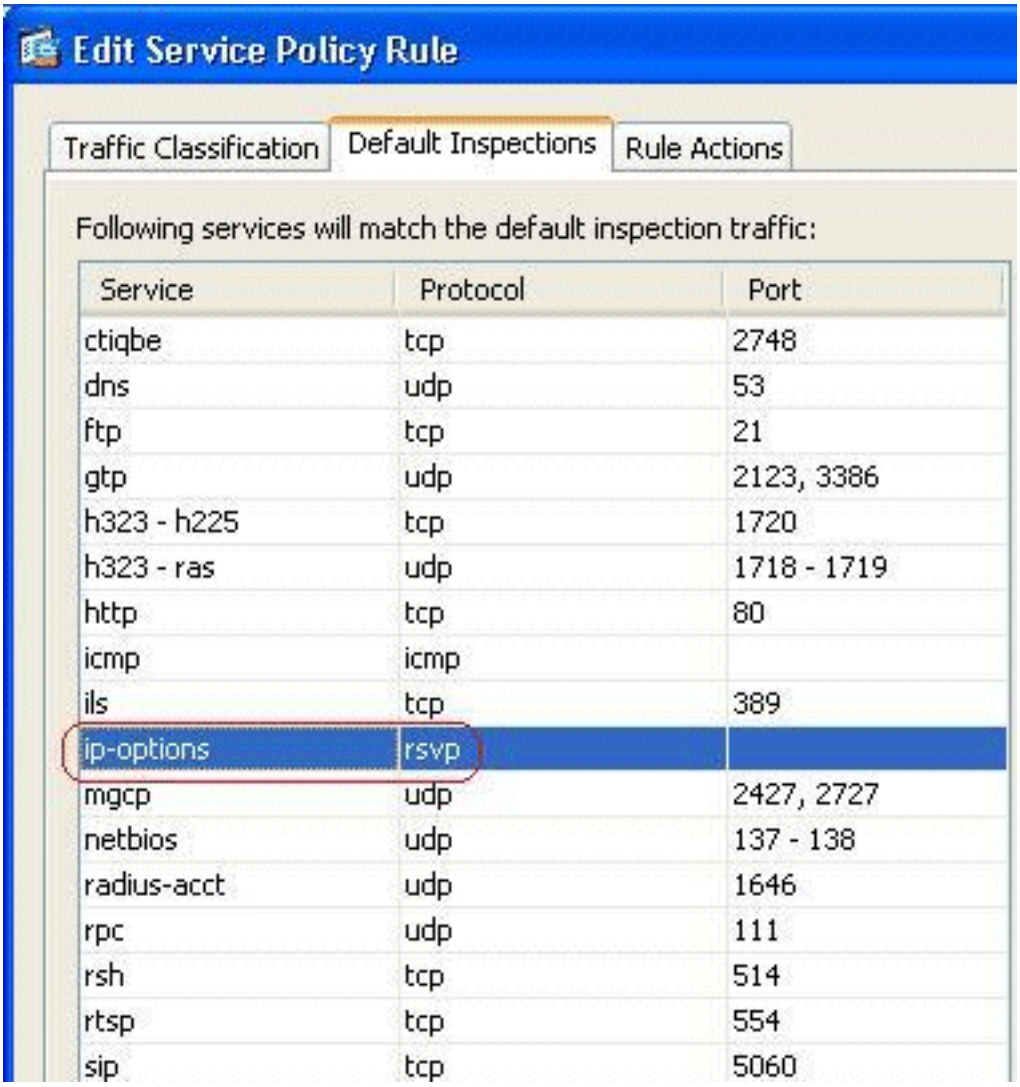
Voici un exemple de configuration CLI équivalente, pour référence :

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
```

Comportement par défaut de Cisco ASA afin d'autoriser les paquets RSVP

L'inspection des options IP est activée par défaut. Accédez à **Configuration > Firewall > Règles de stratégie de service**. Sélectionnez la stratégie globale, cliquez sur **Modifier**, puis sélectionnez l'onglet **Inspections par défaut**. Ici, vous trouverez le protocole RSVP dans le champ **Options IP**. Cela garantit que le protocole RSVP est inspecté et autorisé via Cisco ASA. Par conséquent, un appel vidéo de bout en bout est établi sans aucun problème.



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show service-policy inspect ip-options** - Affiche le nombre de paquets abandonnés et/ou autorisés conformément à la règle service-policy configurée.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Assistance technique sur les appareils de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems