ASDM 6.3 et plus tard : Exemple de configuration d'inspection d'options IP

Contenu

Introduction

Ce document fournit une configuration d'échantillon de la façon configurer l'appliance de sécurité adaptable Cisco (ASA) afin de passer les paquets IP avec certaines options IP activées.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Version de logiciel courante 8.3 de Cisco ASA et plus tard
- Version de logiciel courante adaptative 6.3 de gestionnaire de Sécurité de Cisco et plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

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 une en-tête IP avec un champ d'options. Le champ d'options, généralement désigné sous le nom des options IP, fournit les fonctions de contrôle qui sont exigées dans certaines situations, mais inutile pour la plupart des transmissions communes. En particulier, les options IP inclut des dispositions pour des groupes date/heure, la Sécurité, et le routage spécial. L'utilisation des options IP est facultative, et le champ peut contenir zéro, une, options ou plus.

Les options IP est un risque de sécurité et si un paquet IP avec le champ d'options IP activé est ASA traversée, elle coulera des informations sur l'installation interne d'un réseau à l'extérieur. En conséquence, un attaquant peut tracer la topologie de votre réseau. Pendant que Cisco ASA est un périphérique qui impose la Sécurité à l'entreprise, par défaut, il relâche les paquets qui ont le champ d'options IP activé. Un message de Syslog d'échantillon est affiché ici, pour votre référence :

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

Cependant, dans les scénarios spécifiques de déploiement où le trafic visuel doit traverser Cisco ASA, des paquets IP avec certaines options IP doit être traversés autrement la conférence téléphonique peuvent échouer. De la version de logiciel 8.2.2 de Cisco ASA en avant, une nouvelle caractéristique appelée la « inspection pour des options IP » a été introduite. Avec cette configuration, vous pouvez contrôler quels paquets avec des options spécifiques IP sont permis par Cisco ASA.

Par défaut, cette caractéristique est activée et l'inspection pour les options IP ci-dessous sont activées dans la stratégie globale. Configurer cette inspection demande à l'ASA pour permettre à un paquet pour passer, ou pour effacer les options spécifiées IP et puis pour permettre au paquet pour passer.

- **Fin de la liste d'options (EOOL)** ou de l'**option IP 0** - cette option apparaît à la fin de toutes les options afin de marquer la fin d'une liste d'options.
- **Aucune exécution (NOP)** ou **option IP 1** - ce champ d'options fait toute la longueur de la variable de champ.
- **Alerte de routeur (RTRALT)** ou **option IP 20** - cette option informe des Routeurs de transit d'examiner le contenu du paquet même lorsque le paquet n'est pas destiné à ce routeur.

Configurez

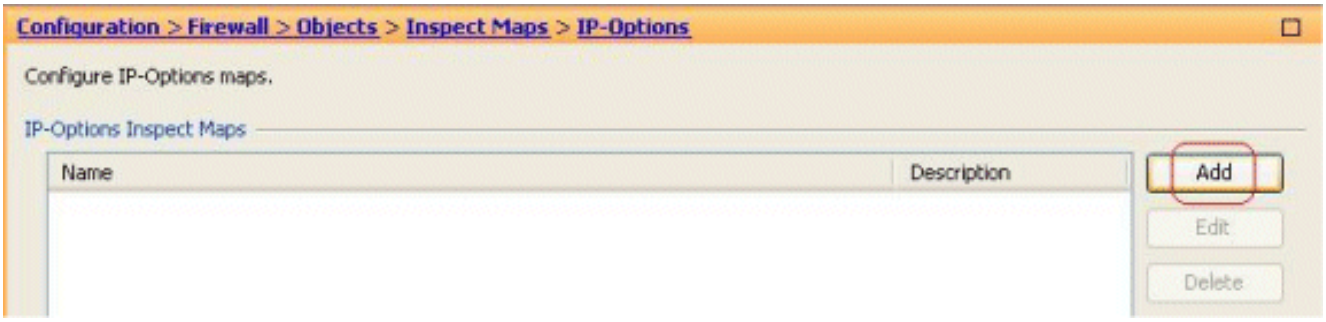
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

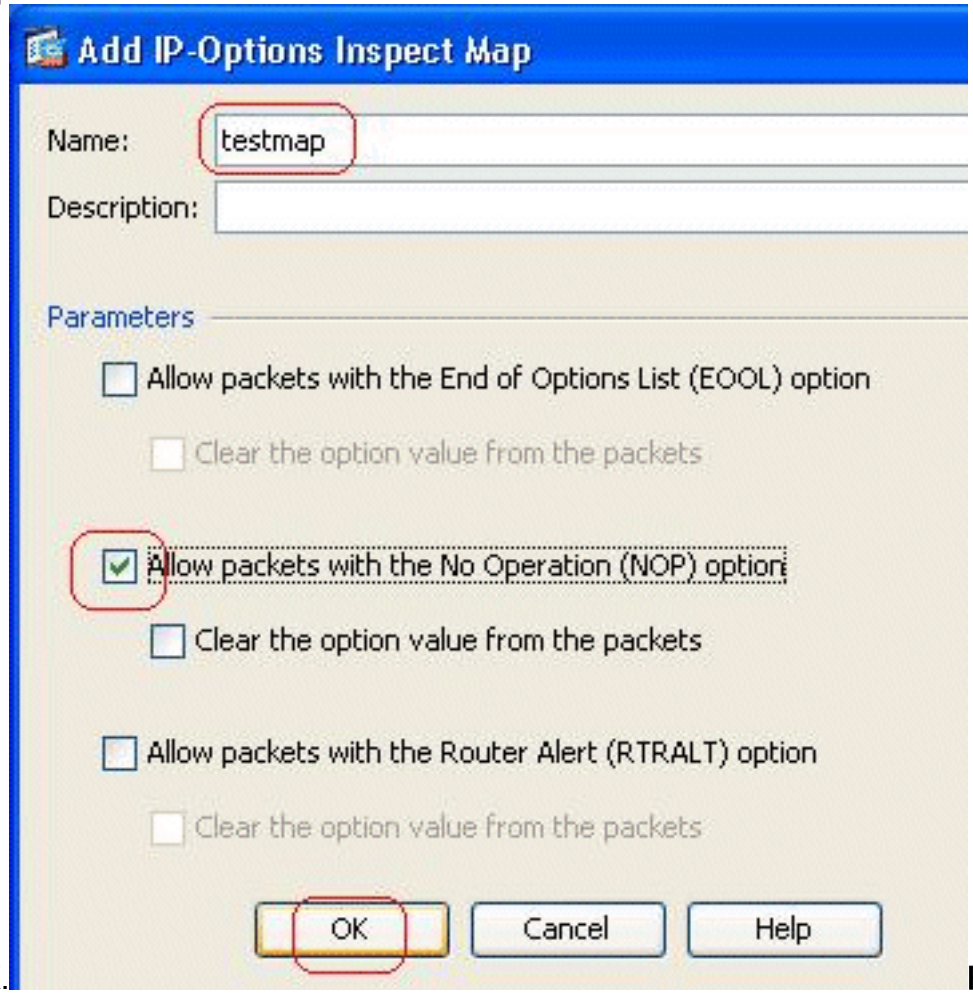
Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configuration ASDM

Utilisant l'ASDM, vous pouvez voir comment activer l'inspection pour les paquets IP qui ont le champ d'options IP, NOP.

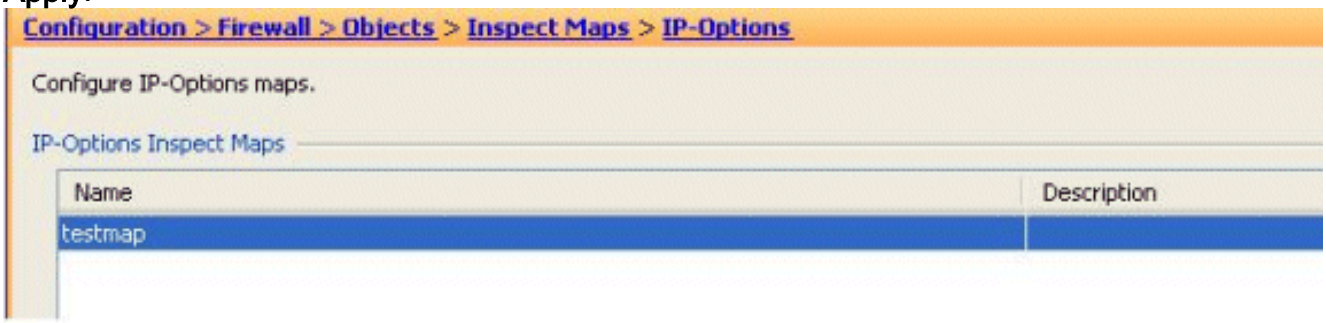
Le champ d'options dans l'en-tête IP peut contenir zéro, une, options ou plus, qui fait toute la longueur de la variable de champ. Cependant, l'en-tête IP doit être un multiple de 32 bits. Si le nombre de bits de toutes les options n'est pas un multiple de 32 bits, l'option NOP est utilisée en tant que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

1. Allez à la **configuration** > au **Pare-feu** > aux **objets** > **examinent des cartes** > des IP-**options**, et cliquent sur
   Add.
   

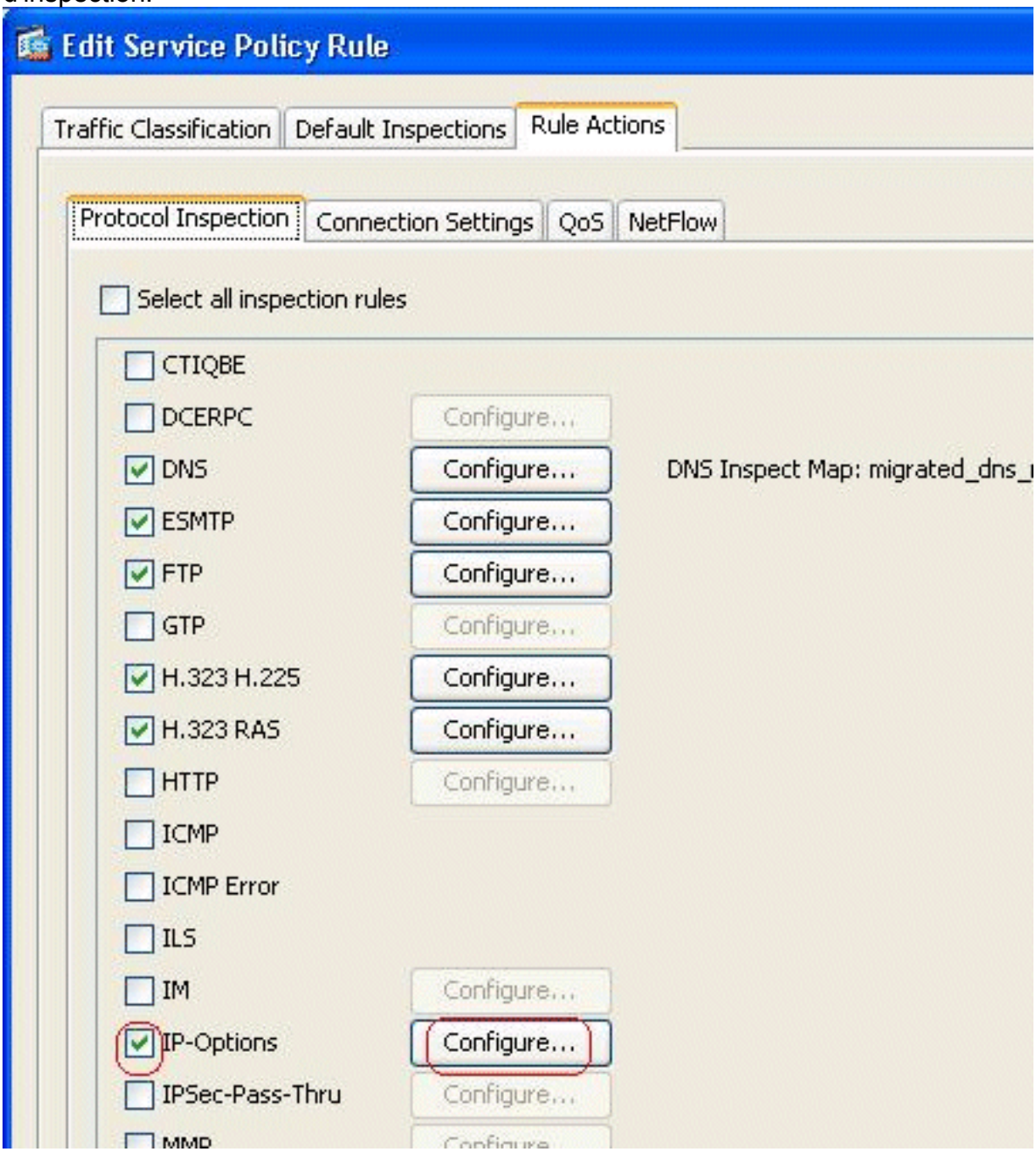
2. Les IP-options d'ajouter examinent la fenêtre de carte apparaît. Spécifiez le nom de la carte d'examiner, choisi **permettez les paquets avec l'aucune option de l'exécution (NOP)**, et cliquez sur
   OK.
   

   Remarque: Vous pouvez également sélectionner le **clair la valeur de l'option de l'**option de **paquets**, de sorte que ce champ dans le paquet IP soit désactivé, et les paquets traversent Cisco ASA.

3. Un nouveau examine le **testmap** appelé par carte est créé. Cliquez sur **Apply**.

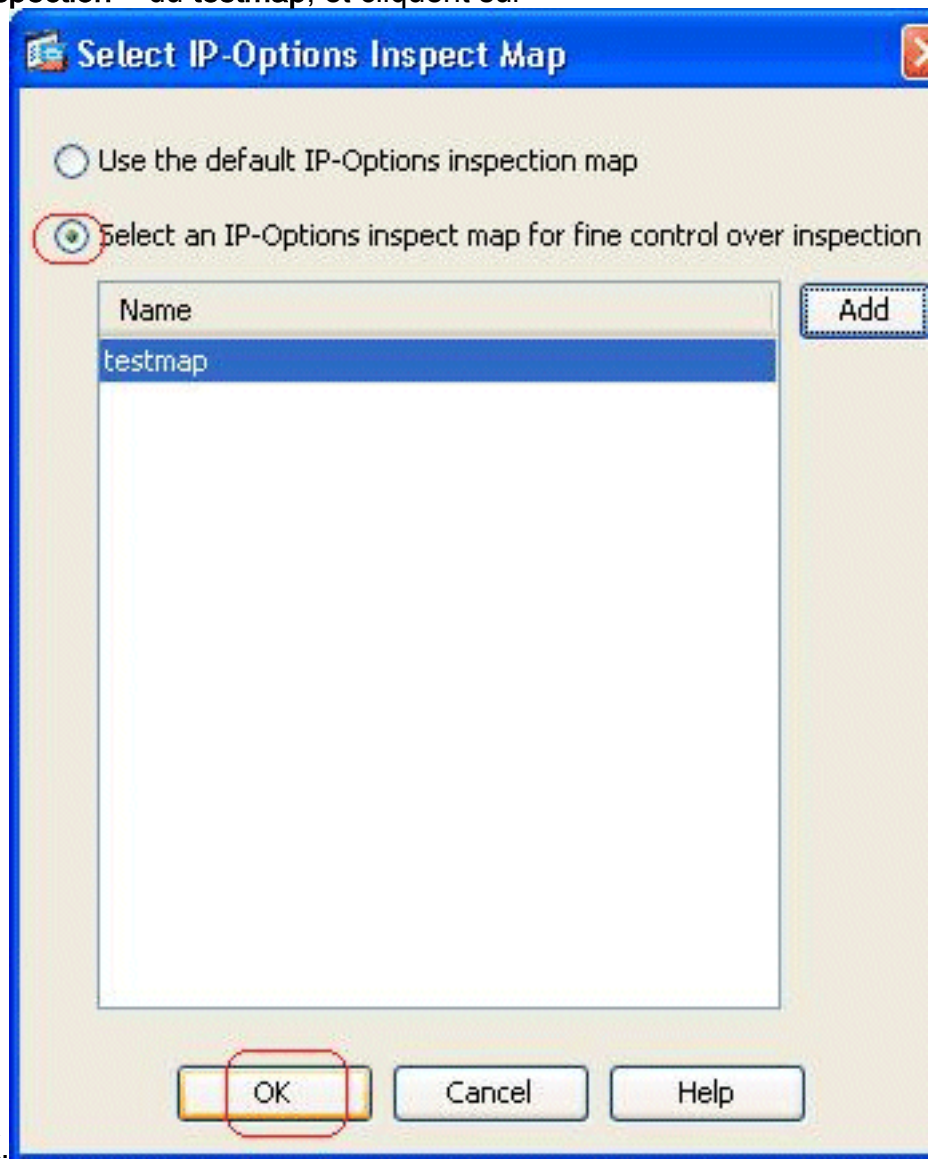


4. Allez aux **règles de configuration** > de **stratégie de Pare-feu** > de **service**, sélectionnez la stratégie globale existante, et cliquez sur Edit. La fenêtre de règle de stratégie de service d'éditer apparaît. Sélectionnez les **actions** onglet de **règle**, coche l'élément d'IP-**options**, et choisissez **configurent** afin d'assigner la carte de création récente d'inspection.



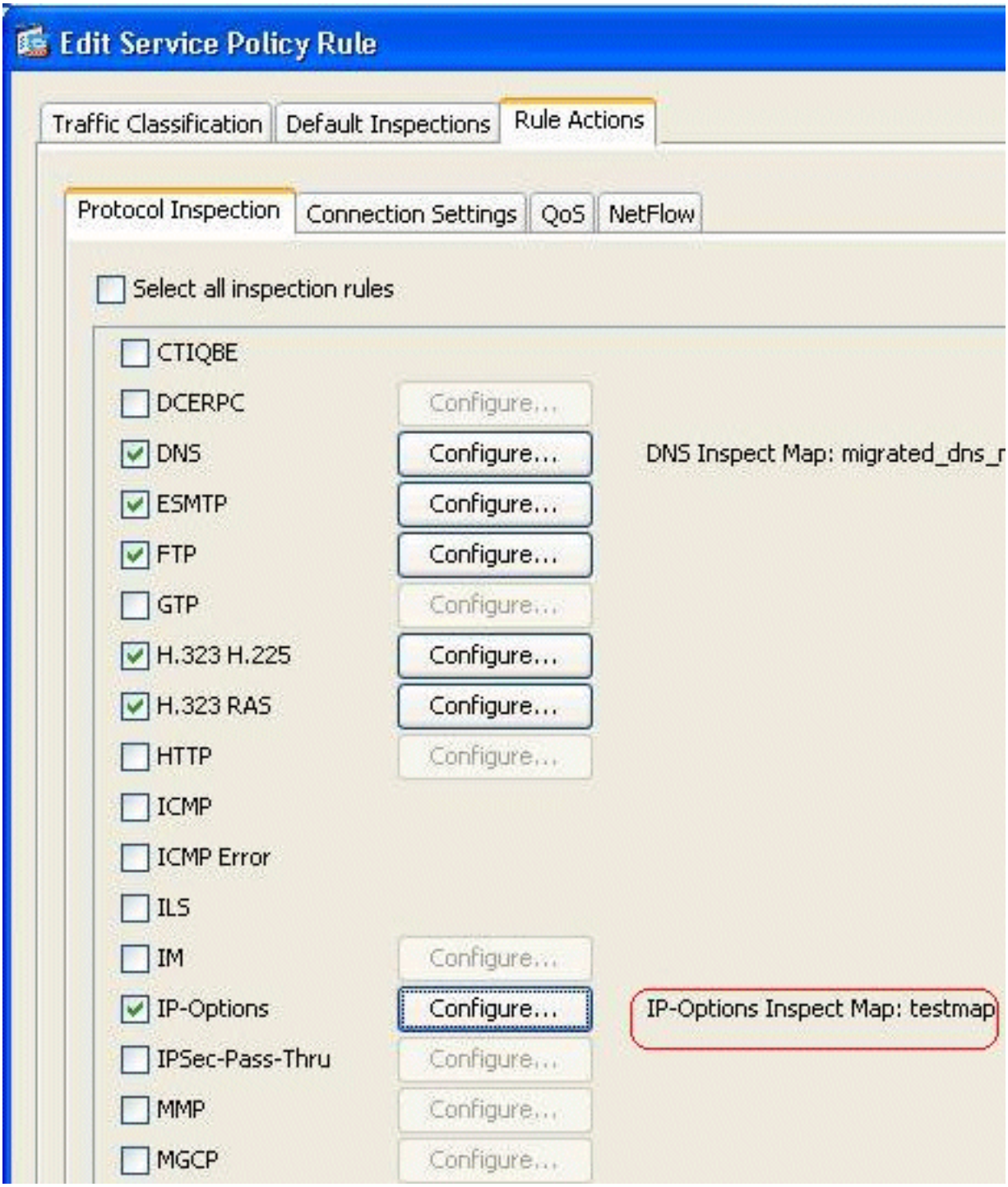
5. Choisissez **choisi des IP-options examinent la carte pour assurer le contrôle correct de**

l'inspection > du **testmap**, et cliquent sur

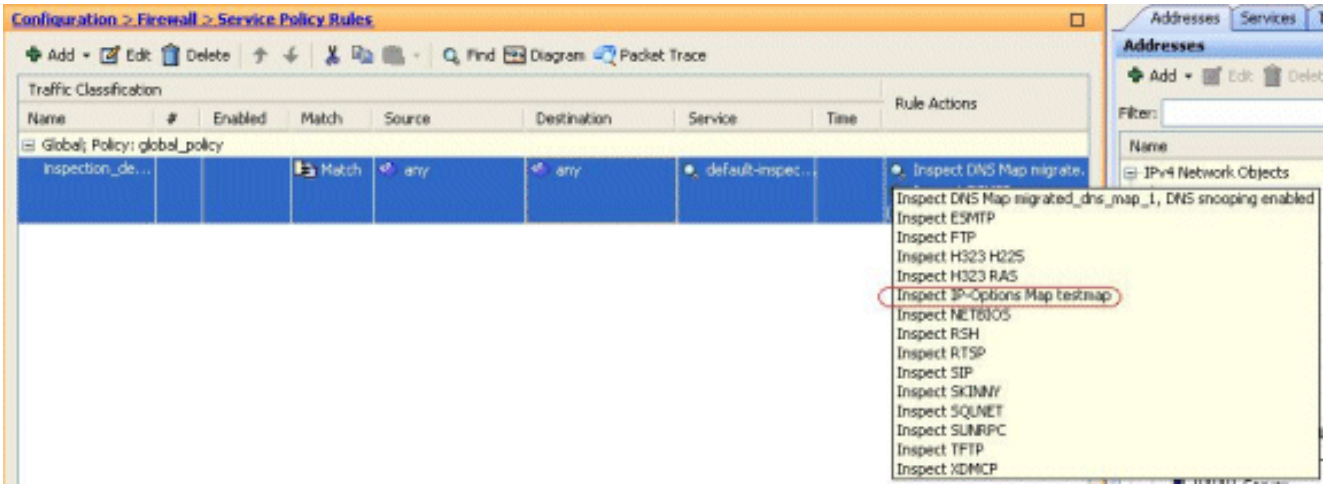


OK.

6. Sélectionnés examinent la carte peuvent être visualisés dans le domaine d'IP-**options**. Cliquez sur OK afin de revenir à l'onglet de règles de stratégie de service.



7. Avec votre souris, vol plané au-dessus de l'onglet d'**actions de règle** de sorte que vous puissiez trouver toutes les cartes disponibles d'inspection de protocole associées avec cette carte
globale.

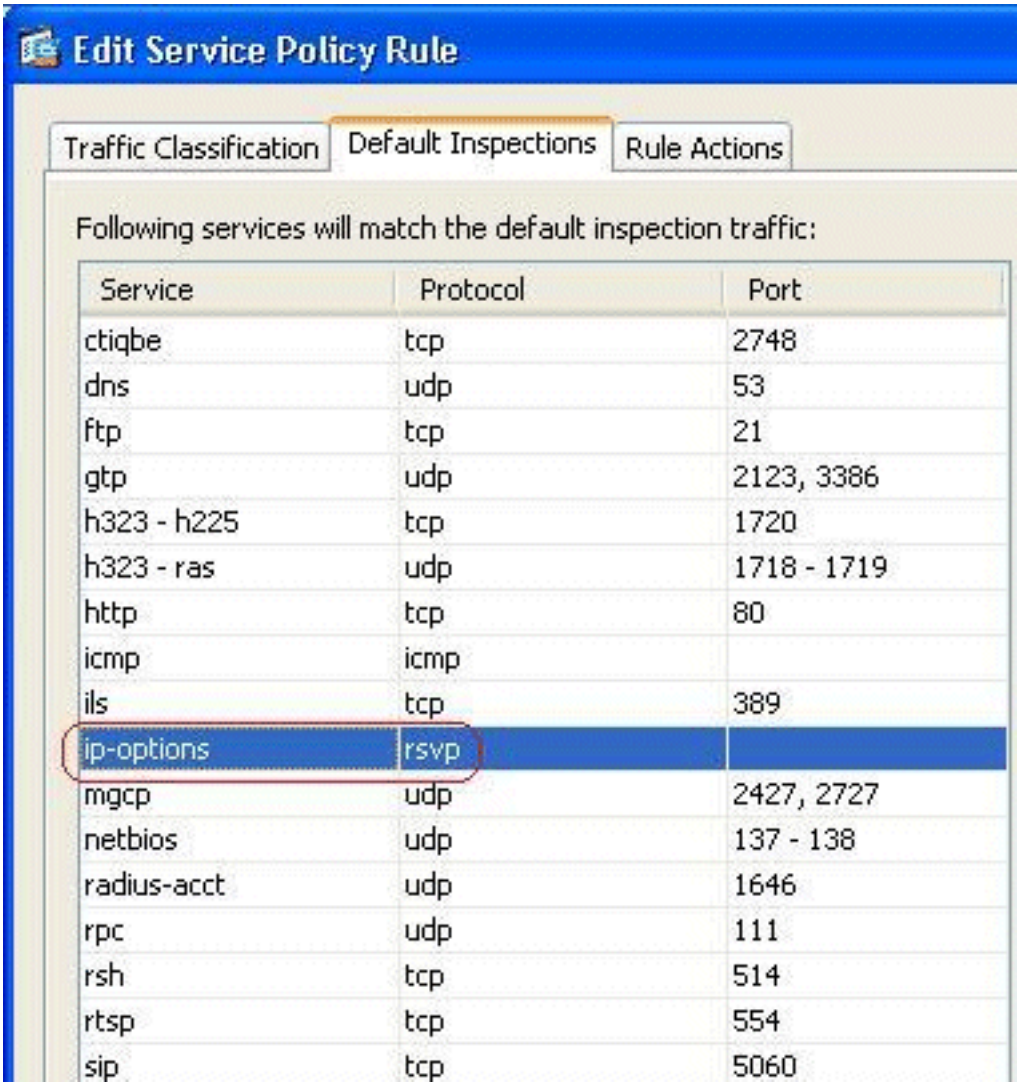


Voici un extrait témoin de la configuration équivalente CLI, pour votre référence :

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 de permettre des paquets de RSVP

L'inspection d'options IP est activée par défaut. Allez aux **règles de configuration >** de **stratégie de Pare-feu >** de **service**. Sélectionnez la stratégie globale, cliquez sur Edit, et sélectionnez l'onglet **par défaut d'inspections**. Ici, vous trouverez le protocole de RSVP dans le domaine d'IP-**options**. Ceci s'assure que le protocole de RSVP est examiné et permis par Cisco ASA. En conséquence, un appel vidéo de bout en bout est établi sans problème.



Vérifiez

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** .

- **le show service-policy examinent des IP-options** - Affiche le nombre de paquets relâchés et/ou permis selon la règle configurée de service-stratégie.

Dépannez

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

Informations connexes

- Soutien technique de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems