تكوين فحص خيارات IP على ASDM 6.3 والإصدارات الأحدث

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين جهاز الأمان القابل للتكيف (ASA) من Cisco لتمرير حزم IP باستخدام خيارات IP معينة ممكنة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج ASA الذي يتم تشغيله الإصدار 8.3 والإصدارات الأحدث من Cisco
- Cisco Adaptive Security Manager الذي يشغل الإصدار 6.3 من البرنامج والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

تحتوي كل حزمة من حزم IP على رأس IP مع حقل خيارات. يوفر حقل "الخيارات"، الذي يشار إليه عادة باسم "خيارات IP"، وظائف التحكم المطلوبة في بعض الحالات، ولكنها غير ضرورية لمعظم الاتصالات الشائعة. بشكل خاص، تتضمن خيارات IP أحكاما لأختام الوقت والأمان والتوجيه الخاص. إستخدام خيارات IP إختياري، ويمكن أن يحتوي الحقل على خيارات صفر أو خيار واحد أو أكثر.

خيارات IP هي خطر أمان وإذا تم تمرير حزمة IP مع حقل خيارات IP الذي تم تمكينه عبر ASA، فإنها ستقوم بتسريب المعلومات حول الإعداد الداخلي للشبكة إلى الخارج. ونتيجة لذلك، يمكن للمهاجم تعيين مخطط الشبكة لديك. بما أن Cisco ASA هو جهاز يفرض الأمان في المؤسسة، بشكل افتراضي، فإنه يسقط الحزم التي يكون فيها حقل خيارات IP ممكنا. يتم عرض عينة رسالة syslog هنا، لمرجعك:

```
" " :IP  XX.YY.ZZ.ZZ  10.110.1.34  IP ||XX.YY.ZZ.ZZ||10.110.1.34|106012
```

ومع ذلك، في سيناريوهات نشر محددة حيث يجب أن تمر حركة مرور بيانات الفيديو عبر Cisco ASA، يجب تمرير حزم IP بخيارات IP معينة من خلال وإلا فقد تفشل مكالمة مؤتمر الفيديو. من الإصدار 8.2.2 من برنامج Cisco ASA وما بعده، تم تقديم ميزة جديدة تسمى "البحث عن خيارات IP". باستخدام هذه الميزة، يمكنك التحكم في الحزم المسموح بها باستخدام خيارات IP المحددة من خلال Cisco ASA.

بشكل افتراضي، يتم تمكين هذه الميزة ويتم تمكين البحث عن خيارات IP أدناه في السياسة العامة. يشكل هذا فحص يرشد ال ASA أن يسمح ربط أن يمر، أو أن يمسح ال يعين ip خيار وبعد ذلك يسمح الربط أن يمر.

- **نهاية قائمة الخيارات (EOOL) أو IP خيار 0** - يظهر هذا خيار في نهاية كل الخيارات لوضع علامة على نهاية قائمة الخيارات.
- **ما من عملية (NOP) أو IP خيار 1** - يجعل هذا خيار مجال الطول الإجمالي من الحقل متغير.
- **تنبيه الموجه (RTRALT) أو خيار IP 20** - يقوم هذا الخيار بإعلام موجهات النقل لفحص محتويات الحزمة حتى عندما تكون الحزمة غير موجهة لذلك الموجه.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

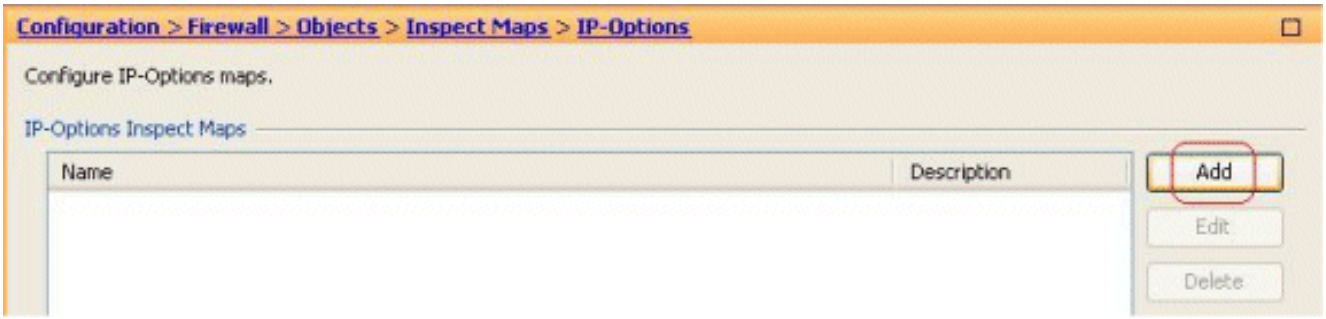
ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

تكوين ASDM

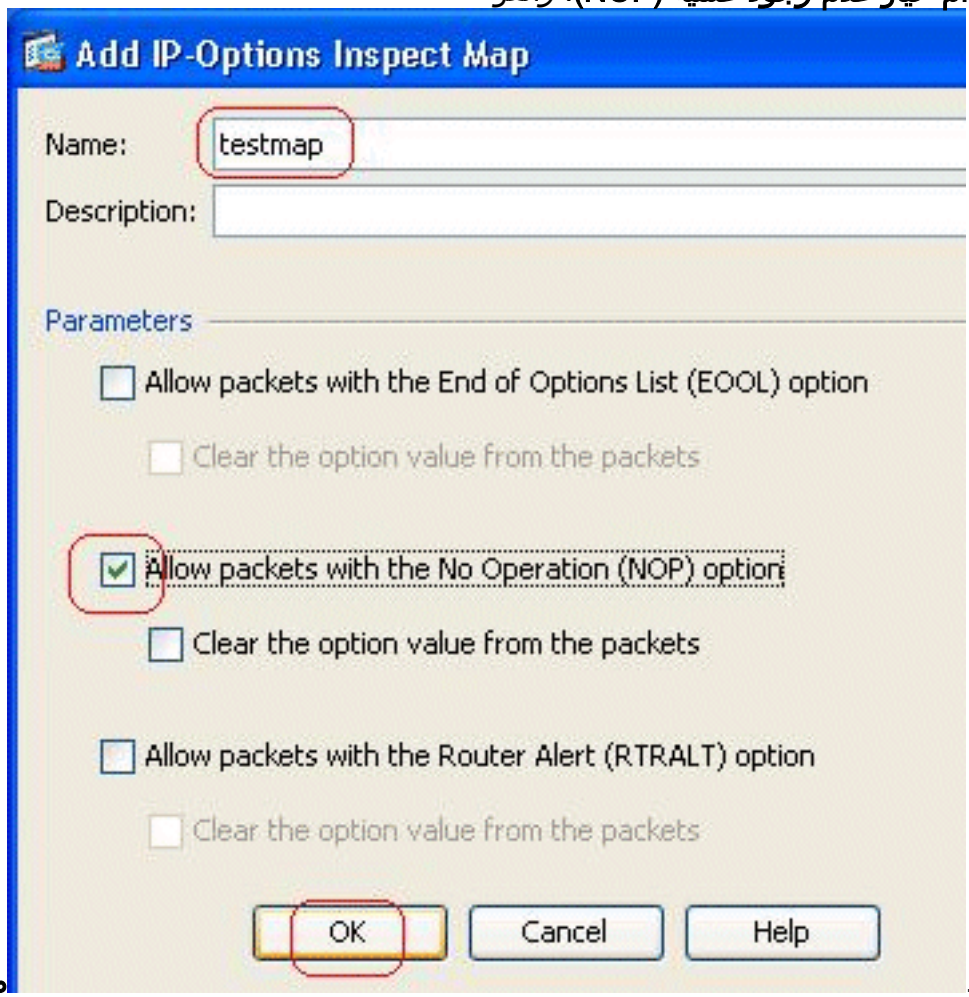
باستخدام ASDM، يمكنك رؤية كيفية تمكين الفحص لحزم IP التي تحتوي على حقل خيارات NOP، IP.

يمكن أن يحتوي حقل الخيارات في رأس IP على خيارات صفرية، واحدة، أو أكثر، مما يجعل الطول الإجمالي لمتغير الحقل. ومع ذلك، يجب أن يكون رأس IP مضاعفا من 32 بت. إذا كان عدد وحدات بت لكل الخيارات ليس مضاعفا ل 32 بت، فإن خيار NOP يتم إستخدامه ك "مساحة داخلية" لمحاذاة الخيارات على حد 32 بت.

1. انتقل إلى التكوين > جدار الحماية > الكائنات>**فحص الخرائط > خيارات IP**، وانقر إضافة.

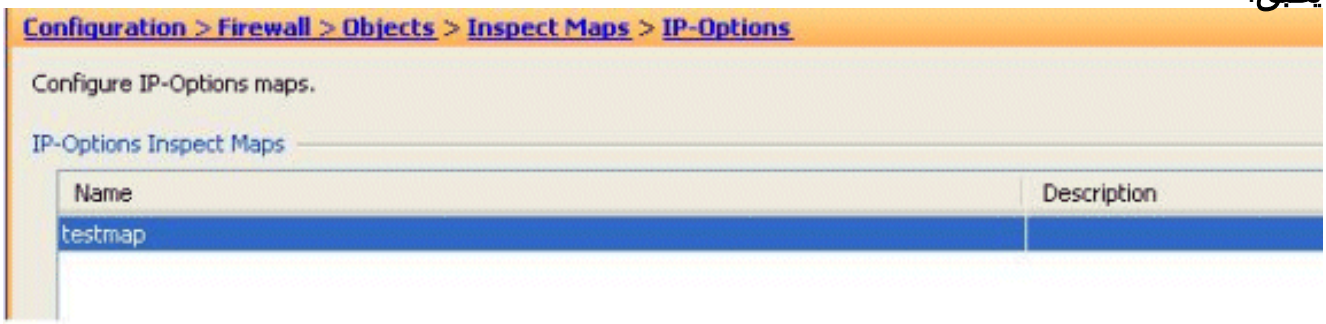


2. تظهر نافذة خريطة إضافة IP-Options Inspection. حدد اسم خريطة المعاينة، وحدد **السماح بالحزم باستخدام خيار عدم وجود عملية (NOP)**، وانقر **موافق**.

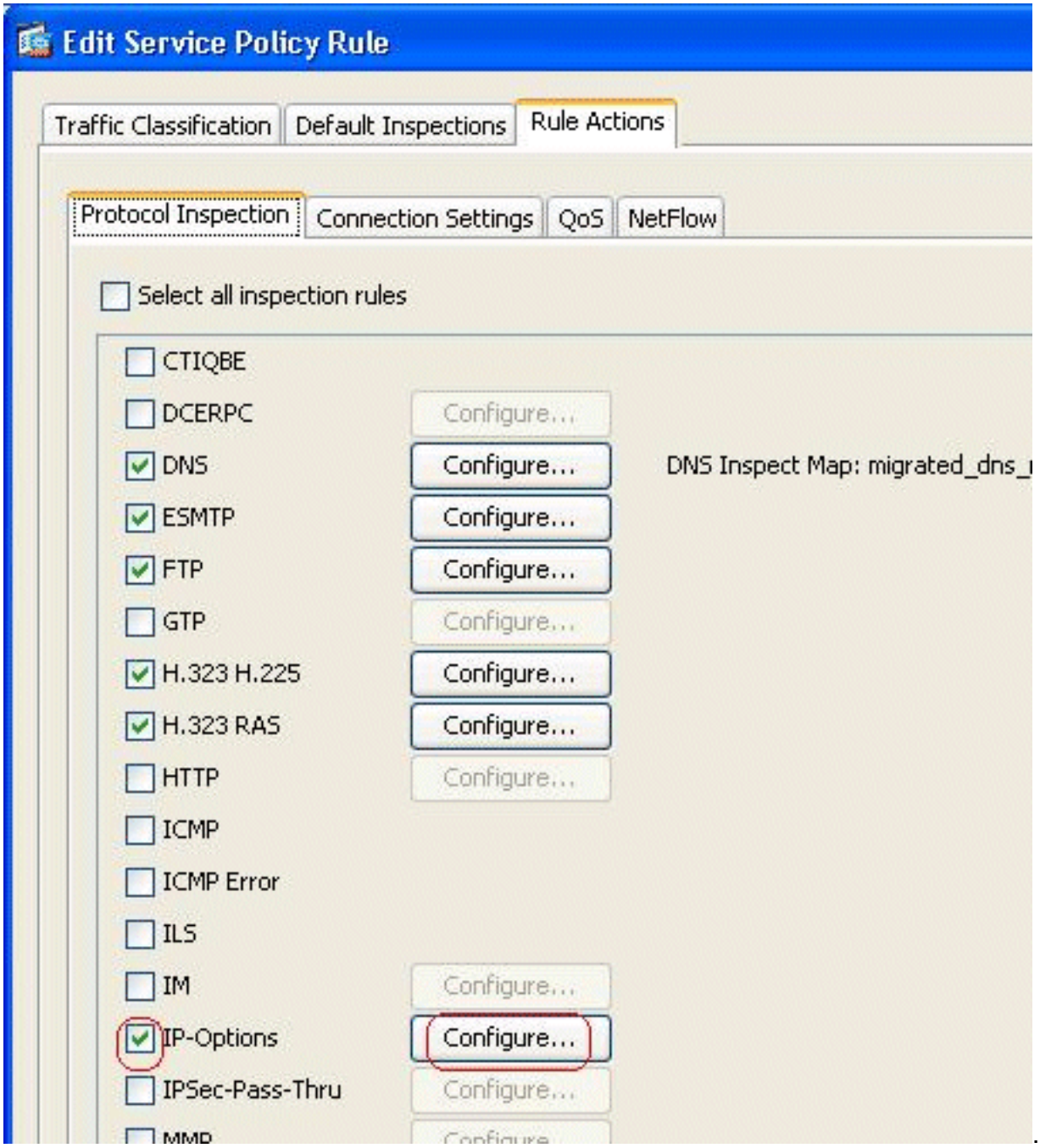


ملاحظة: يمكنك أيضا تحديد **مسح قيمة الخيار من** خيار **الحزم**، حتى يتم تعطيل هذا الحقل في حزمة IP، وتمر الحزم من خلال Cisco ASA.

3. يتم إنشاء خريطة فحص جديدة تسمى **testmap**. طقطقة **يطبق**.

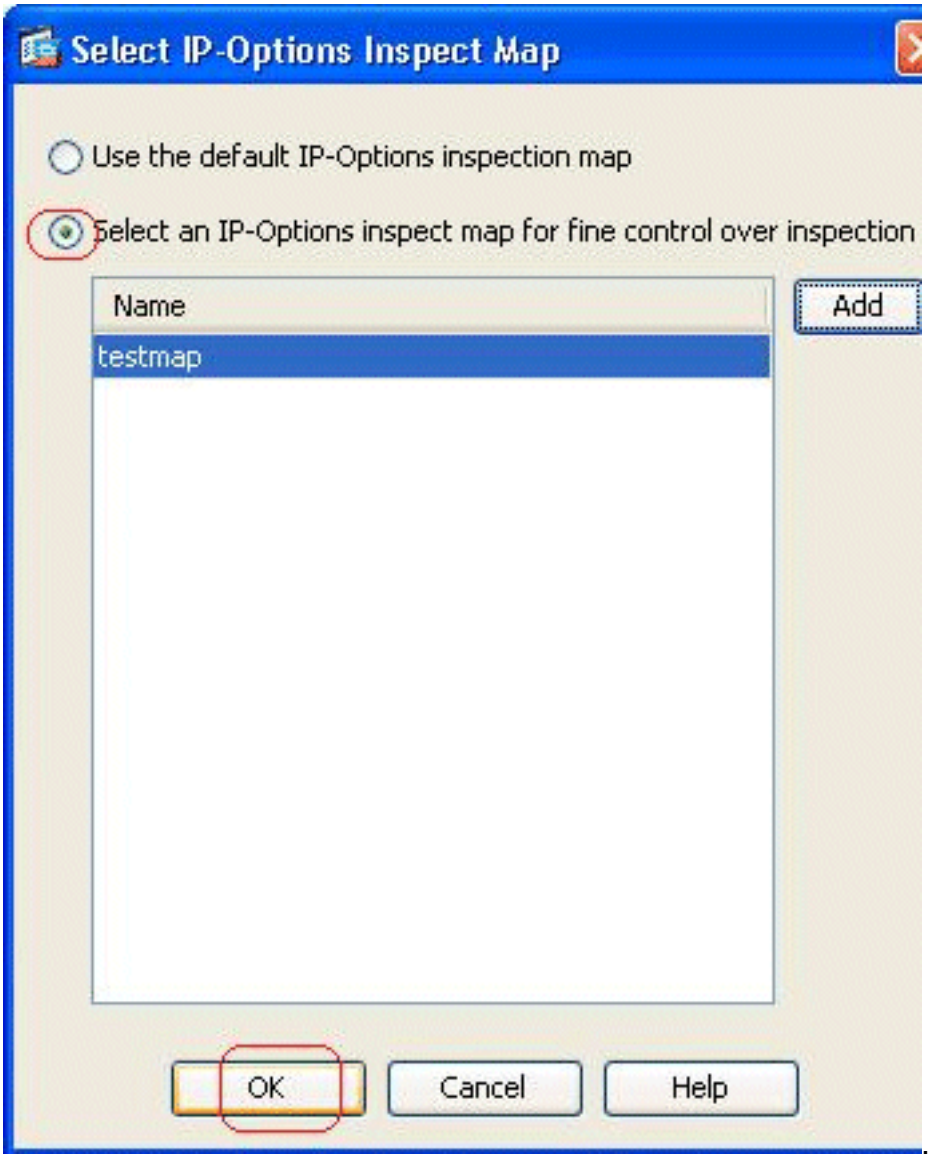


4. انتقل إلى **التكوين > جدار الحماية > قواعد سياسة الخدمة**، وحدد السياسة العامة الموجودة، وانقر فوق **تحرير**. يظهر الإطار "تحرير قاعدة نهج الخدمة". حدد علامة التبويب **إجراءات القاعدة**، وحدد عنصر **خيارات IP**، واختر **تكوين** لتعيين خريطة التفتيش التي تم إنشاؤها



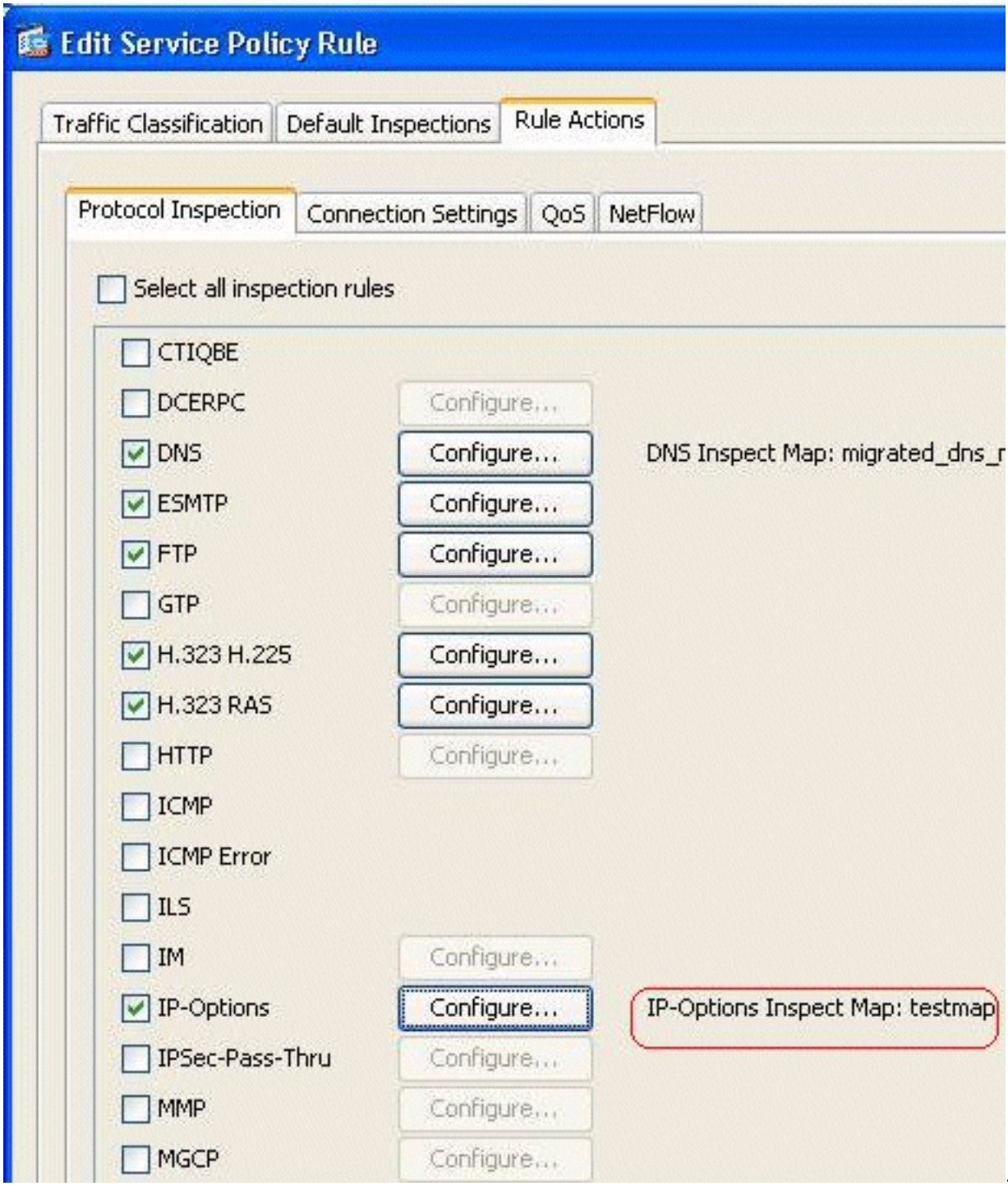
حديثا.

5. أختر **تحديد خريطة فحص خيارات IP للحصول على تحكم دقيق في الفحص > خريطة الاختبار**، وانقر فوق



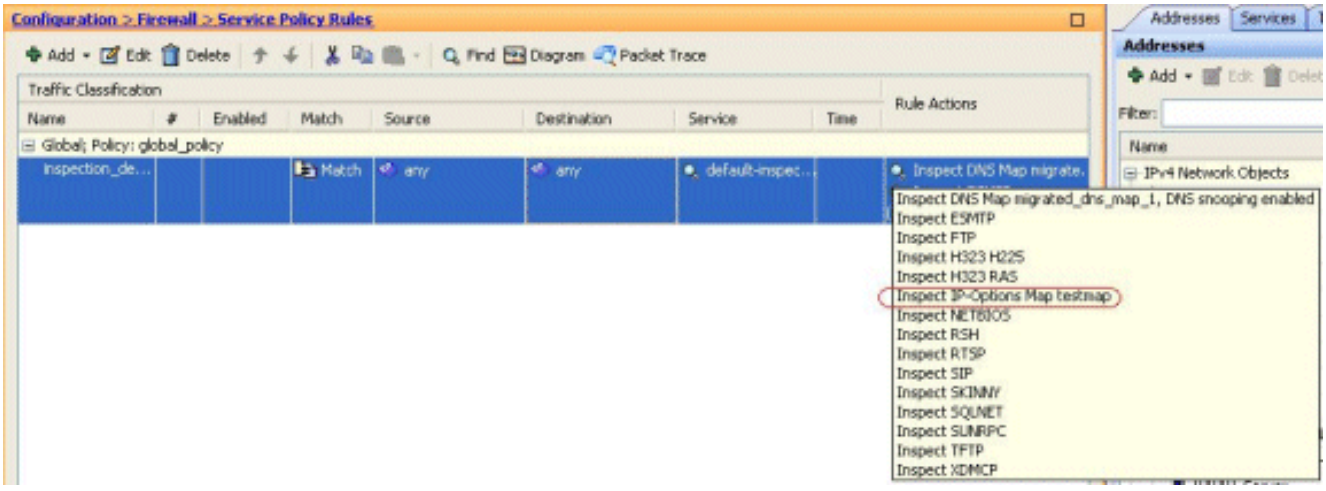
موافق.

6. يمكن عرض خريطة الفحص المحددة في حقل **خيارات IP**. انقر فوق **موافق** للعودة إلى علامة التبويب قواعد سياسة



الخدمة.

7. باستخدام الماوس، قم بالمرور فوق علامة التبويب **إجراءات القواعد** حتى تتمكن من العثور على جميع خرائط فحص البروتوكول المتوفرة المقترنة بهذه الخريطة العامة.

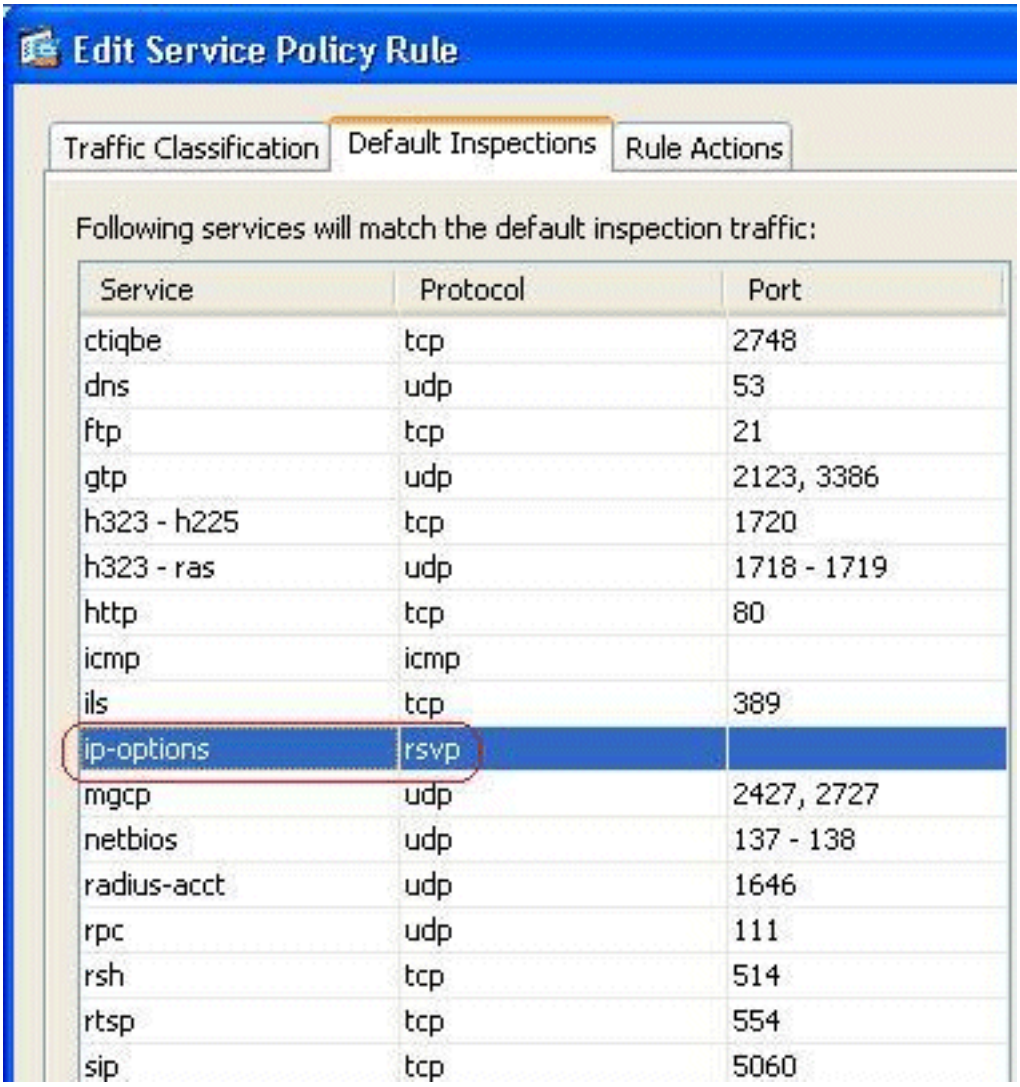


هنا عينة قصاصة من ال يماثل CLI تشكيل، لمرجعك:

Cisco من 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

السلوك الافتراضي ل Cisco ASA للسماح لحزم RSVP

يتم تمكين فحص خيارات IP بشكل افتراضي. انتقل إلى **التكوين > جدار الحماية > قواعد سياسة الخدمة**. حدد النهج العام، وانقر فوق **تحرير**، ثم حدد علامة التبويب **عمليات التفتيش الافتراضية**. هنا، ستجد بروتوكول RSVP في حقل **خيارات IP**. وهذا يضمن فحص بروتوكول RSVP والسماح به من خلال Cisco ASA. ونتيجة لذلك، يتم إجراء مكالمة فيديو شاملة دون أي مشكلة.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

- show service-policy inspection ip-options - يعرض عدد الحزم التي تم إسقاطها و/أو المسموح بها وفقا لقاعدة سياسة الخدمة التي تم تكوينها.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- الدعم الفني لأجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).