تكوين الفحص - تحديث الإصدارات 8.3 والإصدارات الأحدث باستخدام ASDM

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين جهاز الأمان القابل للتكيف (ASA) من Cisco مع الإصدارات 8.3(1) والإصدارات الأحدث حول كيفية إزالة الفحص الافتراضي من السياسة العامة لتطبيق ما وكيفية تمكين الفحص لتطبيق غير افتراضي باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM).

ارجع إلى PIX/ASA 7.x: تعطيل الفحص العام الافتراضي وتمكين فحص التطبيق غير الافتراضي لنفس التكوين على Cisco ASA مع الإصدارات 8.2 والإصدارات الأقدم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco ASA Security Appliance Software، الإصدار 8.3(1) مع ASDM 6.3.

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.

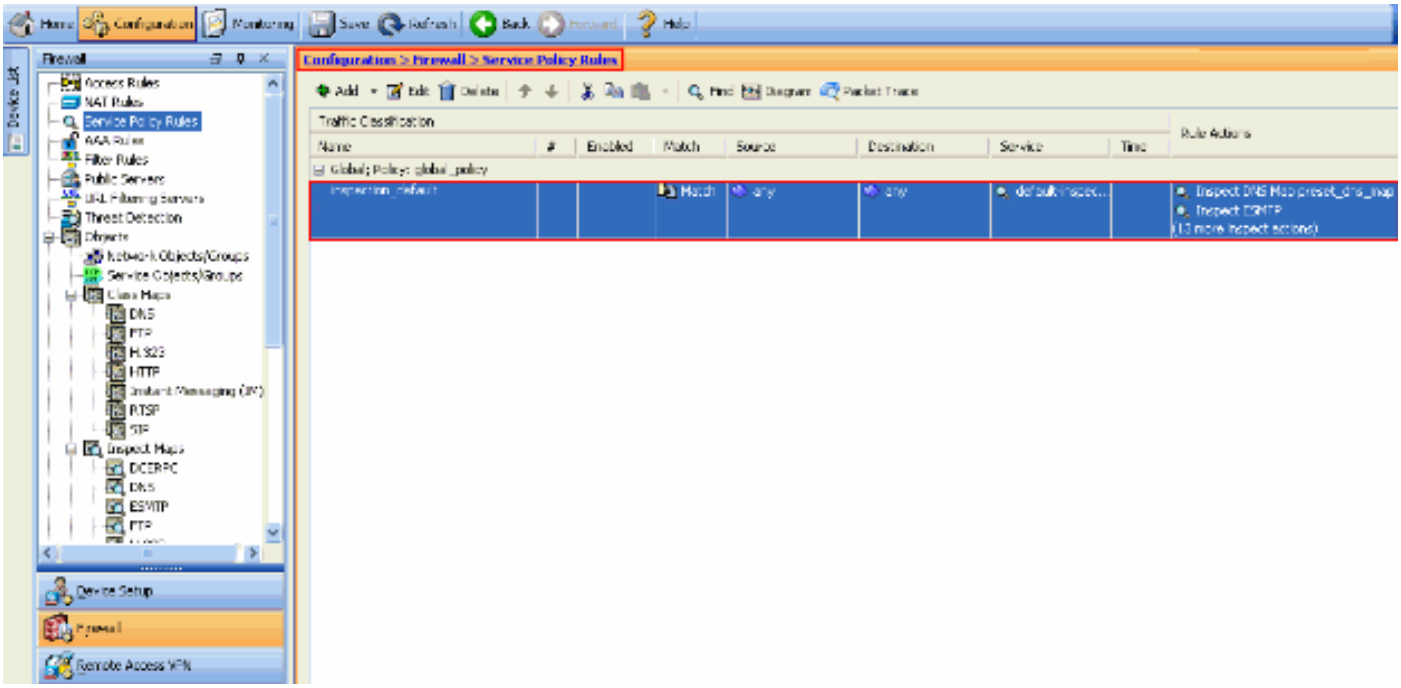
الاصطلاحات

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

السياسة العمومية الافتراضية

بشكل افتراضي، يتضمن التكوين سياسة تطابق كل حركة مرور فحص التطبيق الافتراضية وتطبق بعض عمليات الفحص على حركة المرور على جميع الواجهات (سياسة عامة). ليست كل عمليات التفتيش ممكنة بشكل افتراضي. يمكنك تطبيق نهج عمومي واحد فقط. إذا كنت ترغب في تغيير النهج العام، يجب عليك إما تحرير النهج الافتراضي أو تعطيله وتطبيق نهج جديد. (يتجاوز نهج الواجهة السياسة العامة.)

في ASDM، أختر **تكوين > جدار حماية > قواعد سياسة الخدمة** لعرض السياسة العامة الافتراضية التي تحتوي على فحص التطبيق الافتراضي كما هو موضح هنا:

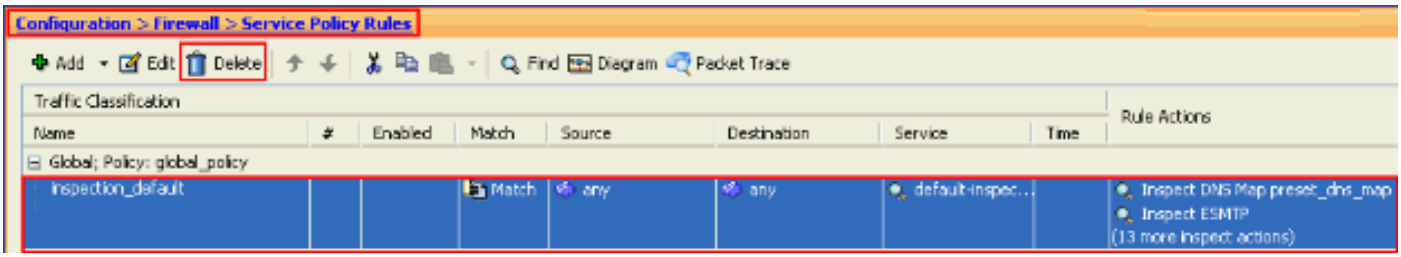


يتضمن تكوين النهج الافتراضي الأوامر التالية:

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
```

إذا كنت بحاجة إلى تعطيل السياسة العامة، فاستخدم الأمر no service-policy global_policy global. لحذف السياسة العامة باستخدام ASDM أختر **تكوين > جدار حماية > قواعد سياسة الخدمة**. ثم حدد النهج العام وانقر فوق

حذف.



ملاحظة: عند حذف نهج الخدمة مع ASDM، يتم حذف مخططات الفئة والنهج المقترنة. ومع ذلك، في حالة حذف نهج الخدمة باستخدام CLI، تتم إزالة نهج الخدمة فقط من الواجهة. تبقى خريطة الفئة وخريطة السياسة بلا تغيير.

تعطيل الفحص العمومي الافتراضي لتطبيق ما

لتعطيل الفحص العام لتطبيق ما، أستخدم الأمر *no* version من **inspection**.

على سبيل المثال، لإزالة الفحص العام لتطبيق FTP الذي يستمع إليه جهاز الأمان، أستخدم الأمر **no inspection ftp** في وضع تكوين الفئة.

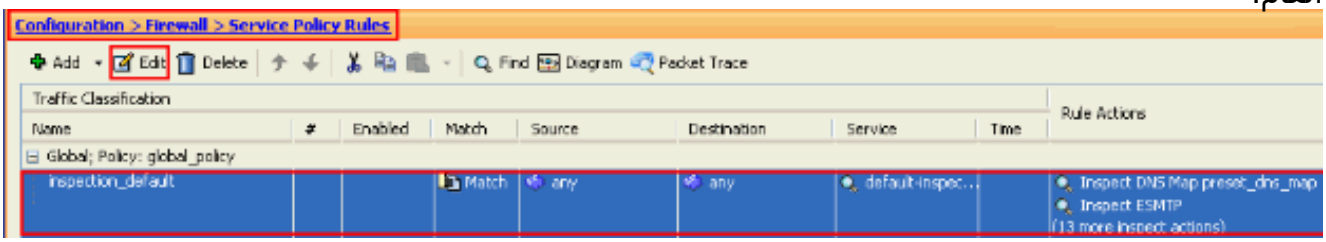
يمكن الوصول إلى وضع تكوين الفئة من وضع تكوين خريطة السياسة. لإزالة التكوين، أستخدم نموذج *no* من الأمر.

```
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#no inspect ftp
```

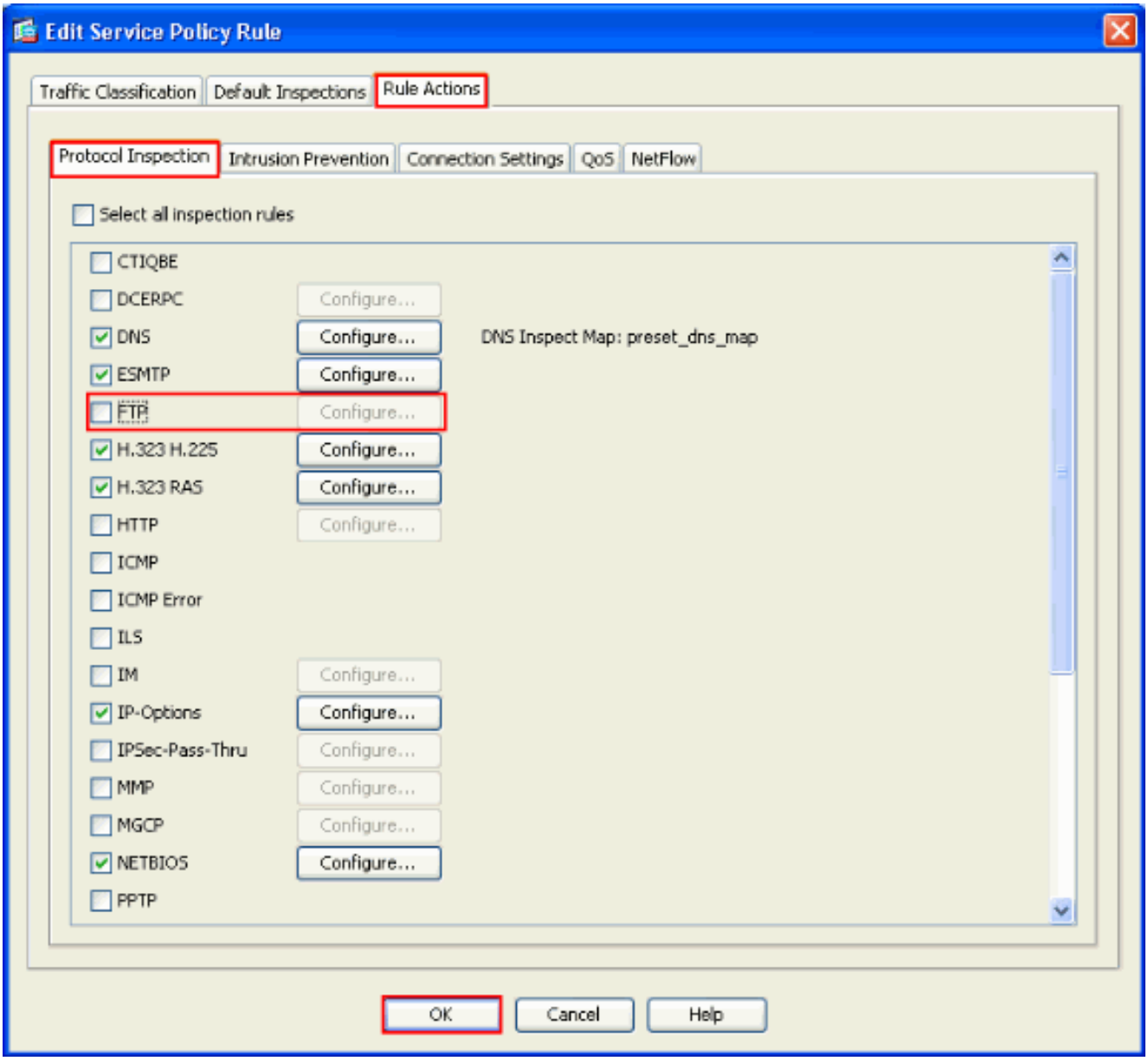
لتعطيل الفحص العام ل FTP باستخدام ASDM، أكمل الخطوات التالية:

ملاحظة: راجع السماح بوصول HTTPS ل ASDM للإعدادات الأساسية للوصول إلى PIX/ASA من خلال ASDM.

1. أختر **تكوين > جدار الحماية > قواعد سياسة الخدمة** وحدد السياسة العامة الافتراضية. بعد ذلك، انقر فوق **تحرير** لتحرير سياسة التفتيش العام.



2. من نافذة "تحرير قاعدة سياسة الخدمة"، أختر **فحص البروتوكول** ضمن علامة التبويب **إجراءات القاعدة**. تأكد من إلغاء تحديد خانة الاختيار **FTP**. يؤدي هذا إلى تعطيل فحص FTP كما هو موضح في الصورة التالية. ثم انقر فوق **موافق** ثم **تطبيق**.



ملاحظة: للحصول على مزيد من المعلومات حول فحص FTP، ارجع إلى PIX/ASA 7.x: تمكين مثال تكوين خدمات FTP/TFTP.

تمكين الفحص للتطبيق غير الافتراضي

يتم تعطيل فحص HTTP المحسن بشكل افتراضي. لتمكين فحص HTTP في global_policy، أستخدم الأمر **فحص http** تحت class inspection_default.

في هذا المثال، يتم تصنيف أي اتصال HTTP (حركة مرور TCP على المنفذ 80) يدخل جهاز الأمان من خلال أي واجهة لفحص HTTP. *لأن السياسة هي سياسة عامة، فإن التفتيش يحدث فقط عند دخول حركة المرور إلى كل واجهة.*

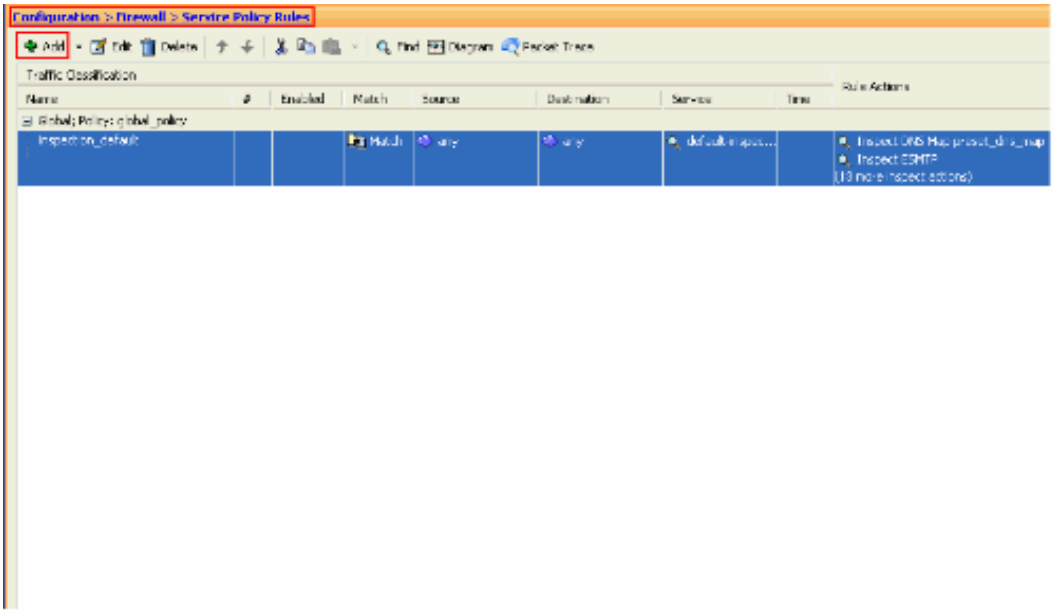
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

في هذا المثال، *يتم تصنيف* أي اتصال HTTP (حركة مرور TCP على المنفذ 80) يدخل جهاز الأمان أو يخرج منه من خلال *الواجهة الخارجية، لفحص HTTP.*

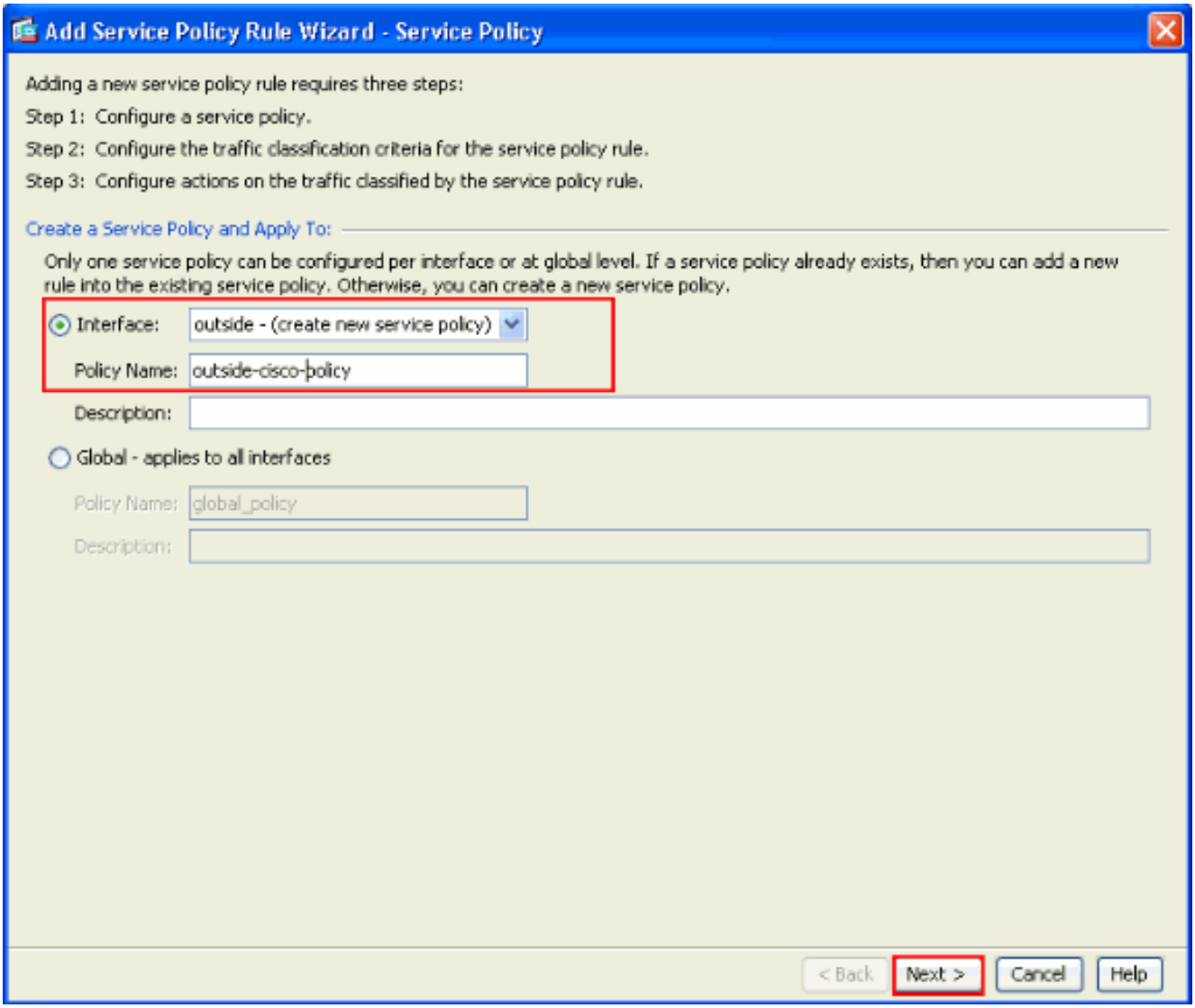
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

قم بإجراء هذه الخطوات لتكوين المثال أعلاه باستخدام ASDM:

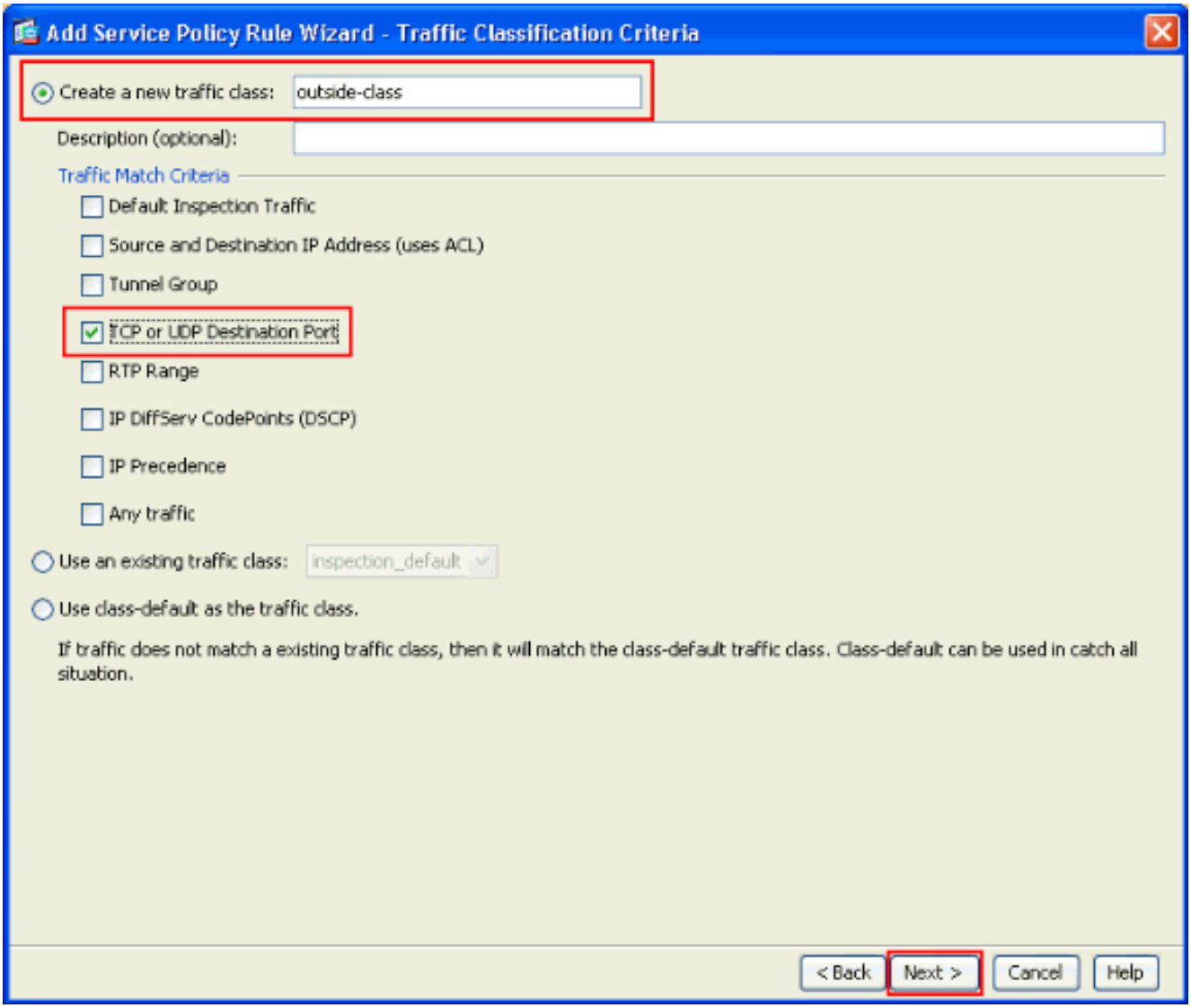
1. أخترت **تشكيل>جدار حماية>خدمة سياسة قاعدة** وطقطقة **يضيف** in order to أضفت جديد خدمة سياسة:



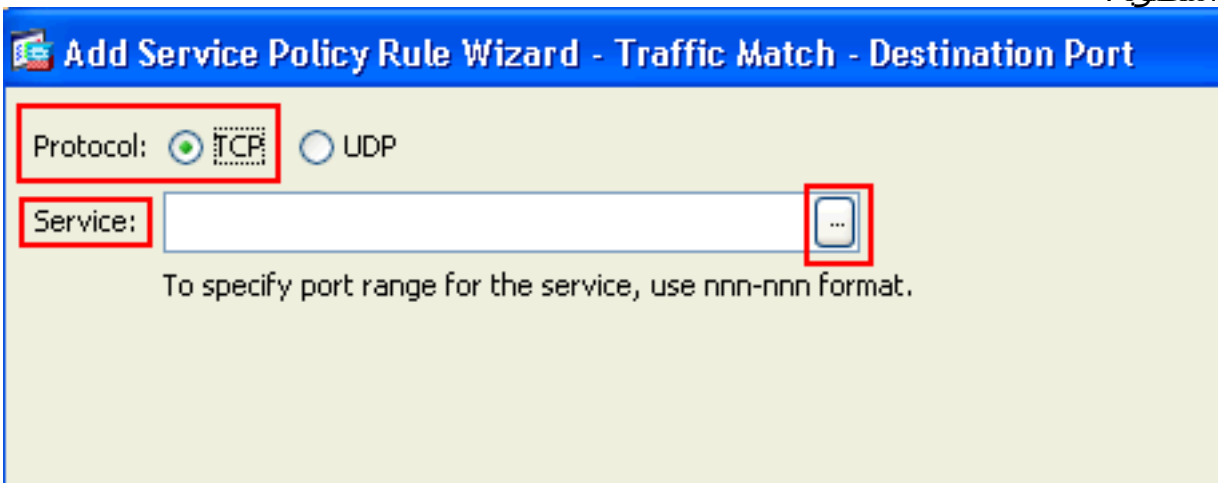
2. من "معالج إضافة قاعدة سياسة الخدمة" - إطار "نهج الخدمة"، أختر زر الاختيار الموجود بجوار **الواجهة**. يطبق هذا النهج الذي تم إنشاؤه على واجهة معينة، والتي هي الواجهة **الخارجية** في هذا المثال. قم بتوفير اسم سياسة، وهو **خارجي-cisco-policy** في هذا المثال. انقر فوق **Next (التالي)**.



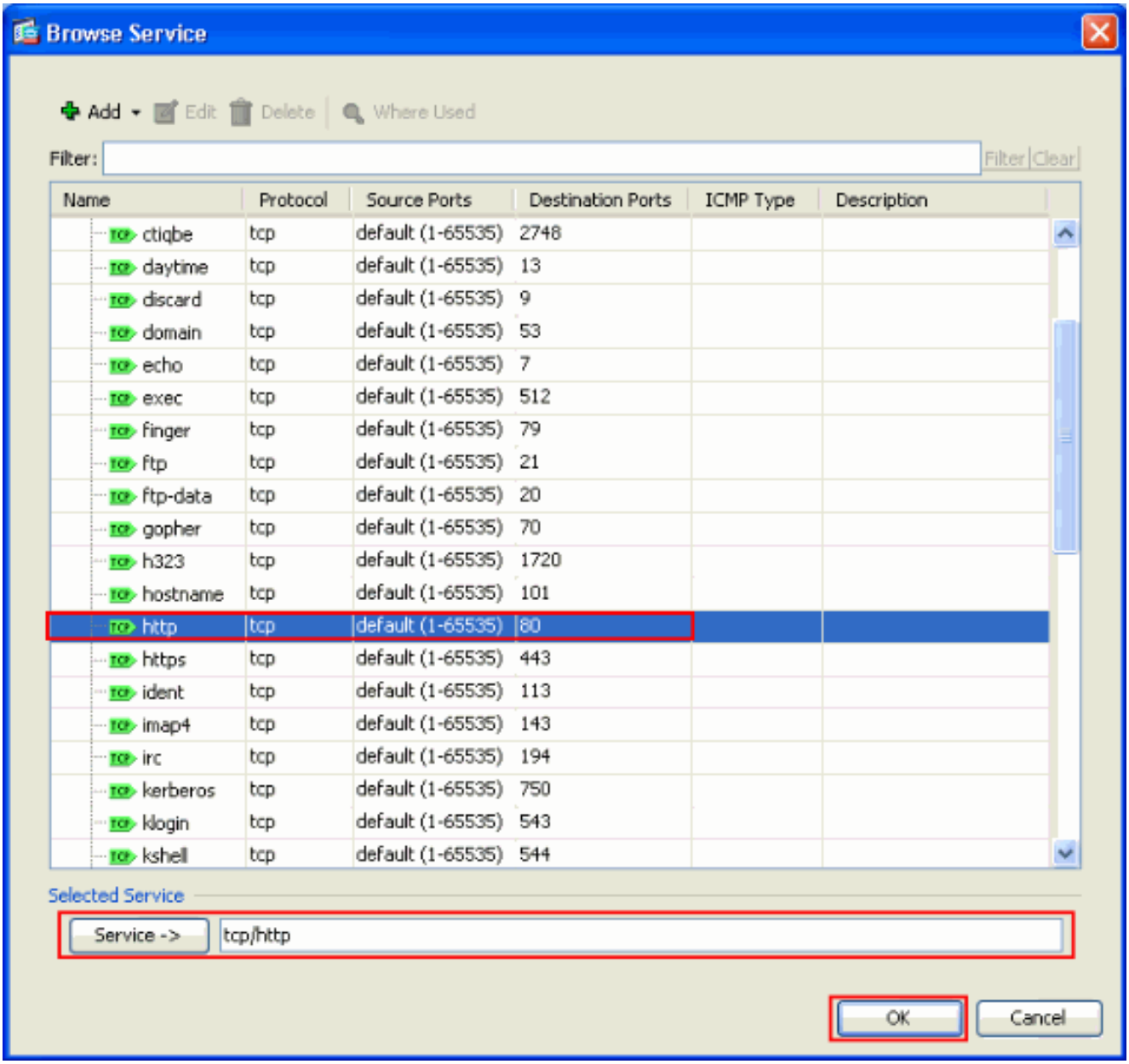
3. من معالج "إضافة قاعدة سياسة الخدمة" - إطار معايير تصنيف حركة المرور، قم بتوفير اسم فئة حركة المرور الجديدة. الاسم المستخدم في هذا المثال هو **خارج الفئة**. ضمنت أن تدقيق صندوق بجوار **TCP أو UDP غاية ميناء** يكون فحصت وطقطقة **بعد ذلك**.



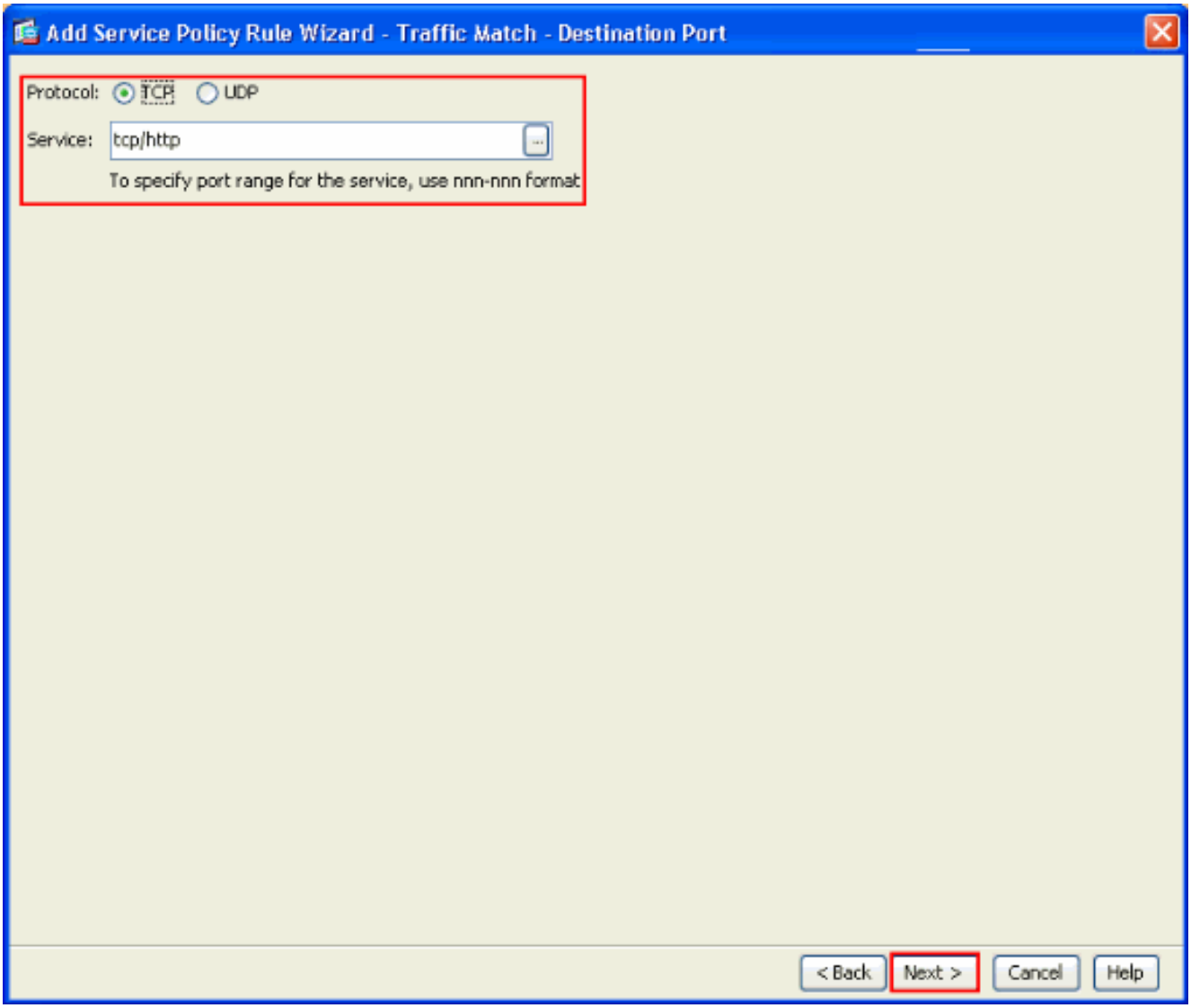
4. من معالج "إضافة قاعدة سياسة خدمة" - تطابق حركة المرور - نافذة المنفذ الوجهة، أختر زر الاختيار الموجود بجوار TCP ضمن قسم **البروتوكول**. ثم انقر فوق الزر الموجود بجوار **الخدمة** لاختيار الخدمة المطلوبة.



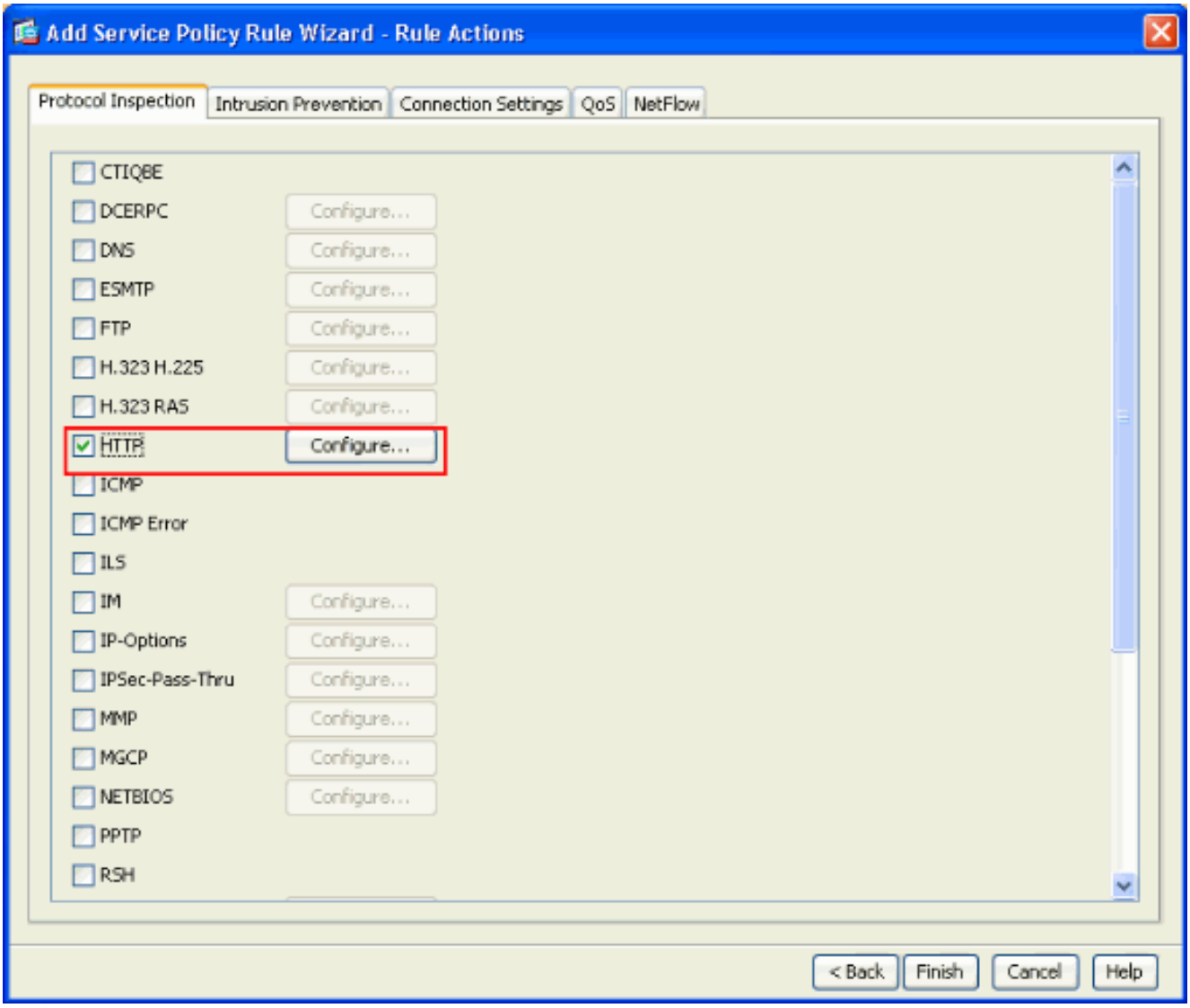
5. من نافذة "إستعراض الخدمة"، أختر HTTP كخدمة. ثم انقر فوق OK.



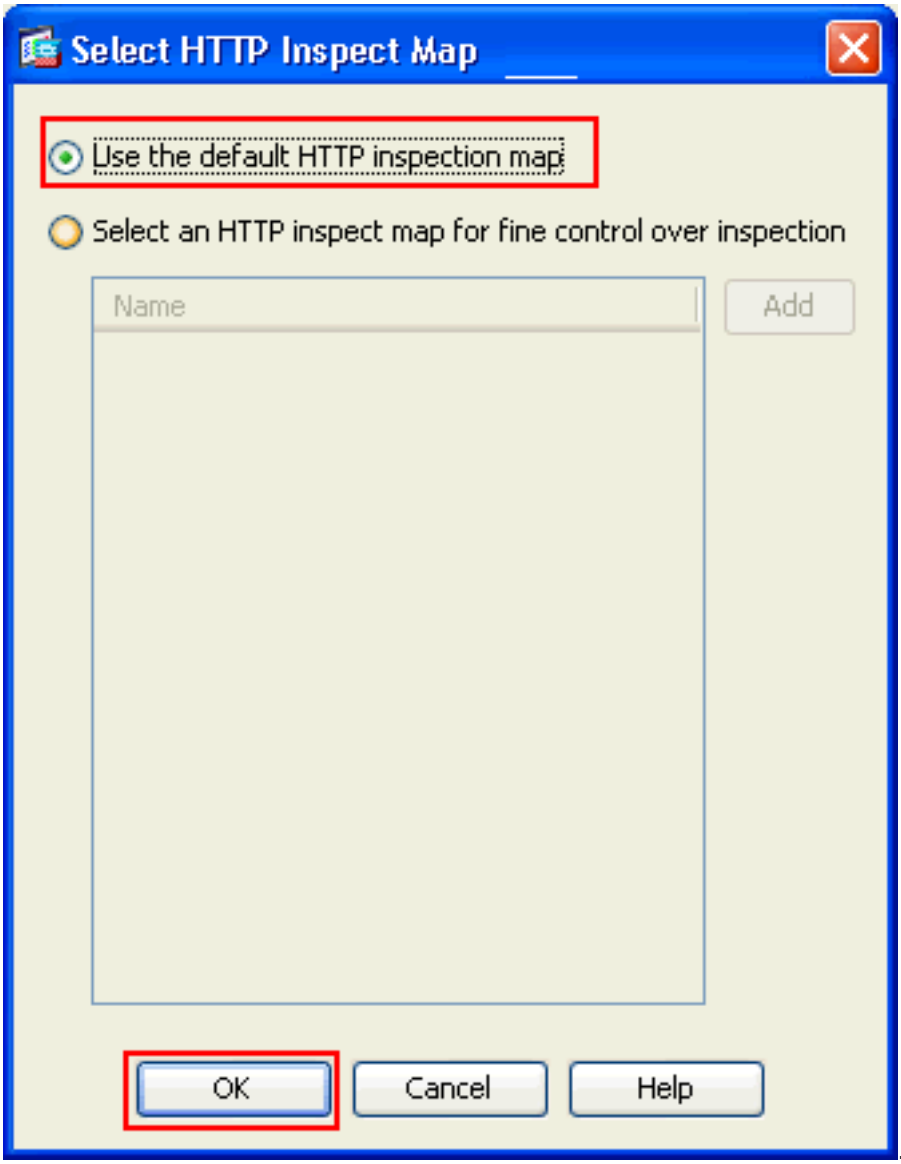
6. من معالج "إضافة قاعدة سياسة خدمة" - تطابق حركة المرور - نافذة المنفذ الوجهة، يمكنك أن ترى أن **الخدمة** المختارة هي **tcp/http**. انقر فوق **Next (التالي)**.



7. من معالج "إضافة قاعدة سياسة الخدمة" - إطار "إجراءات القواعد"، حدد خانة الاختيار الموجودة بجوار **HTTP**.
بعد ذلك، انقر فوق **تكوين** بجوار
HTTP.

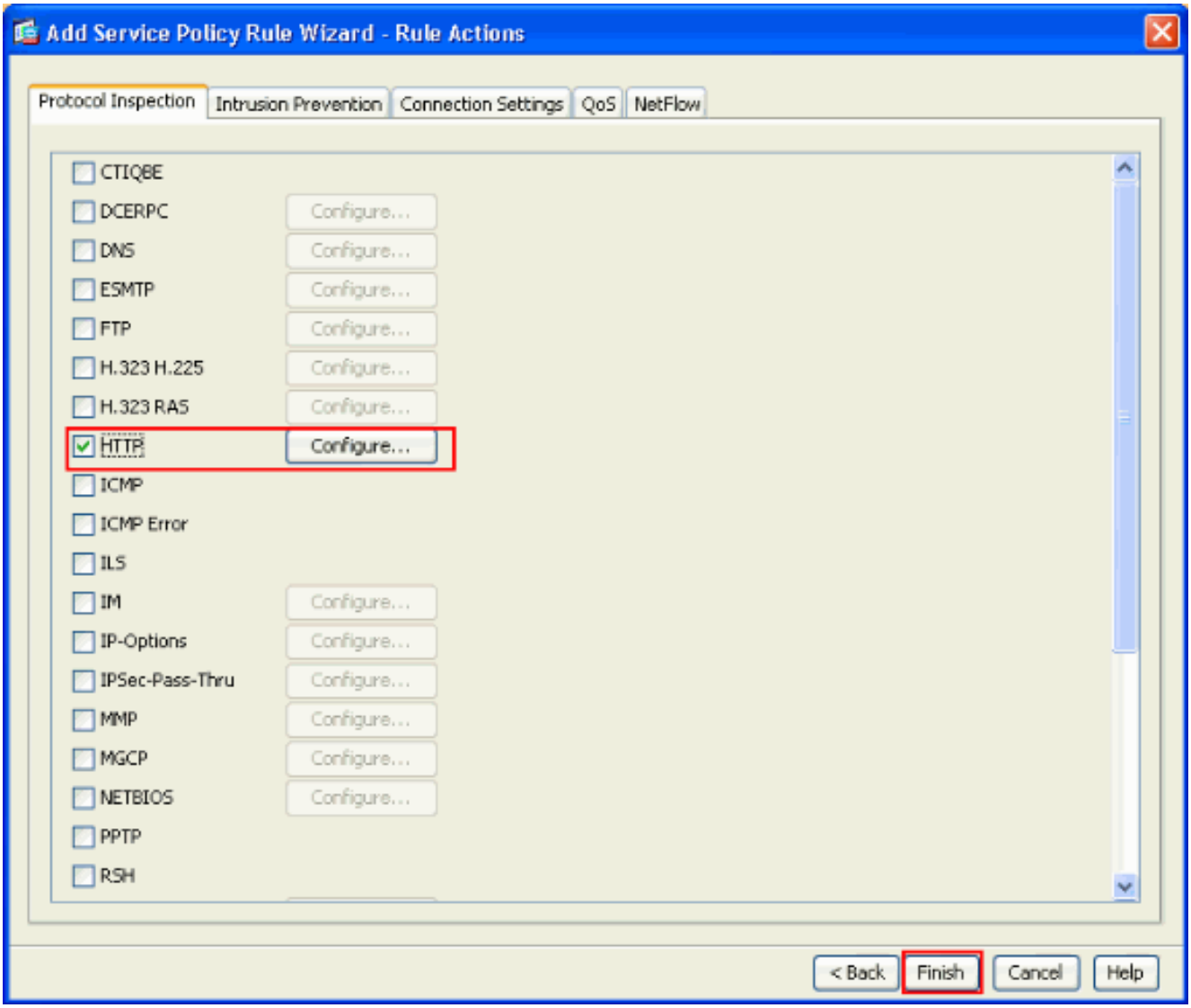


8. من نافذة خريطة فحص HTTP المحددة، تحقق من زر الخيار المجاور **لاستخدام خريطة فحص HTTP الافتراضية**. يتم إستخدام فحص HTTP الافتراضي في هذا المثال. ثم انقر فوق

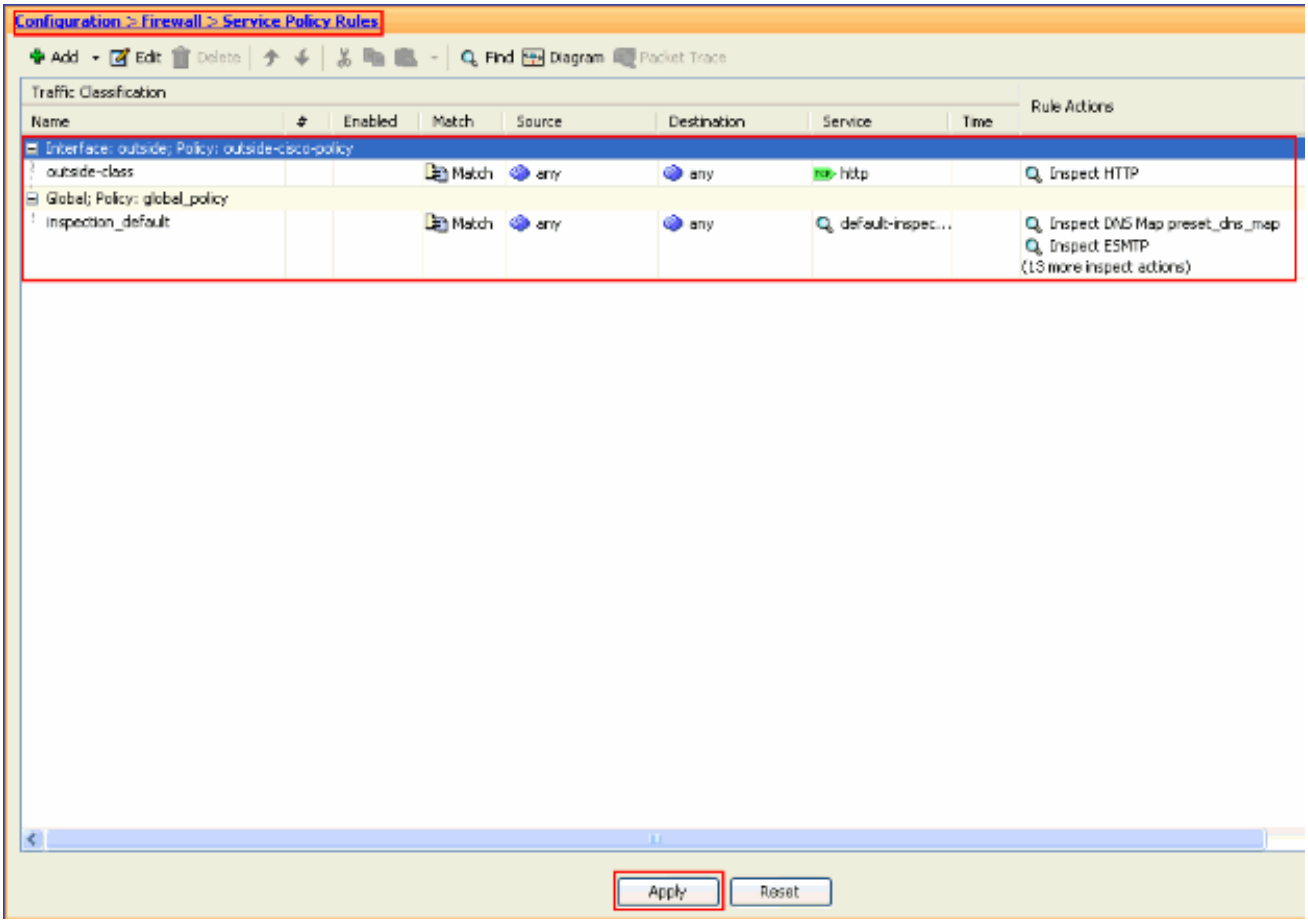


.OK

9. انقر فوق **إنهاء**.



10. تحت **تشكيل > جدار حماية > قواعد سياسة الخدمة**، سترى سياسة الخدمة التي تم تكوينها حديثا **خارج--cisco** **policy** (لفحص HTTP) مع سياسة الخدمة الافتراضية الموجودة بالفعل على الجهاز. طقطقة **يطبق** in order to طبقت التشكيل إلى ال cisco ASA.



معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- مدير أجهزة حلول الأمان المعدلة من Cisco
- طلبات التعليقات (RFCs)
- تطبيق فحص بروتوكول طبقة التطبيق
- 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).