ASA/PIX 7.x: تعطيل الفحص العام الافتراضي وتمكين فحص التطبيق غير الافتراضي باستخدام ASDM

المحتويات

المقدمة

يوضح هذا المستند كيفية إزالة الفحص الافتراضي من السياسة العامة لتطبيق ما وكيفية تمكين الفحص لتطبيق غير افتراضي.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان القابل للتكيف (ASA) من Cisco الذي يشغل صورة برنامج x.7.

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز أمان PIX الذي يشغل صورة البرنامج x.7.

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.)

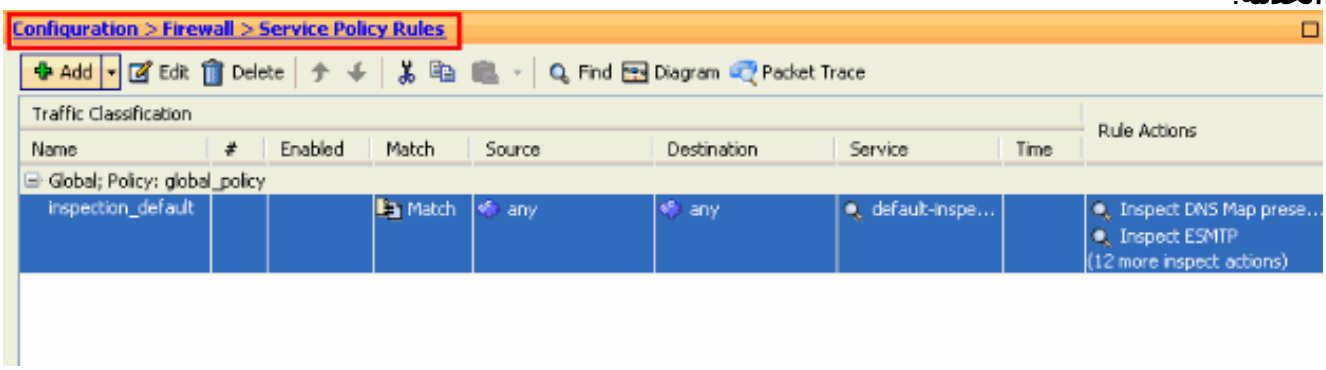
يتضمن تكوين النهج الافتراضي الأوامر التالية:

```
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
```

تمكين فحص التطبيق غير الافتراضي

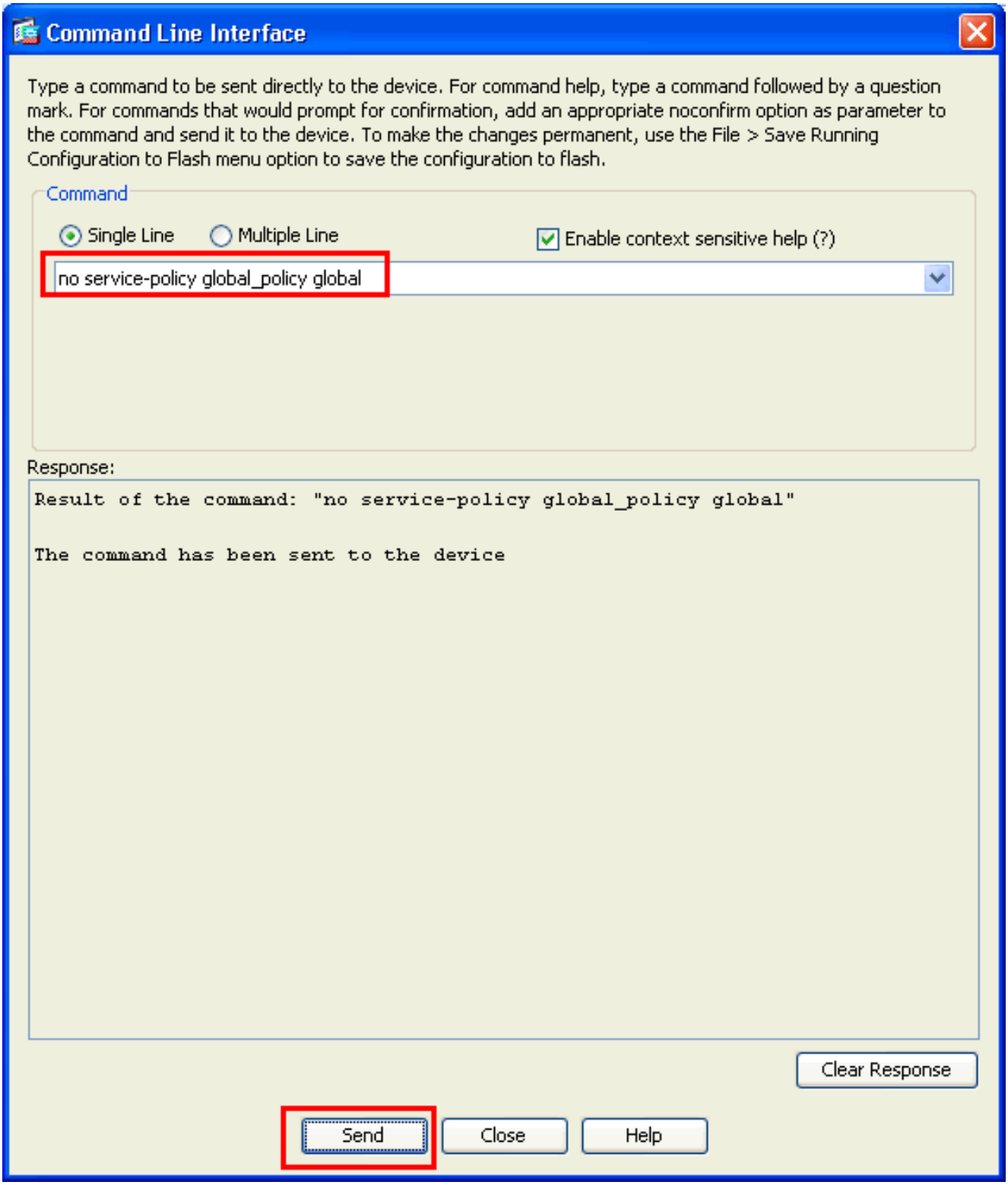
أكمل هذا الإجراء لتمكين فحص التطبيق غير الافتراضي على Cisco ASA:

1. تسجيل الدخول إلى **ASDM**. انتقل إلى **التكوين > جدار الحماية > قواعد سياسة الخدمة**.



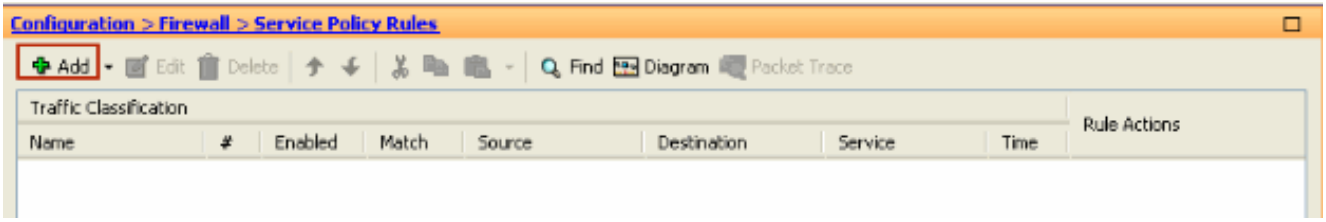
2. إذا كنت ترغب في الاحتفاظ بالتكوين للنهج العام الذي يتضمن خريطة الفئة الافتراضية وخريطة السياسة الافتراضية، ولكن تريد إزالة السياسة بشكل عام، فانتقل إلى **أدوات > واجهة سطر الأوامر** واستخدم الأمر **no**

service-policy global-policy العام لإزالة السياسة بشكل عام. بعد ذلك، انقر فوق **إرسال** حتى يتم تطبيق الأمر على
.ASA

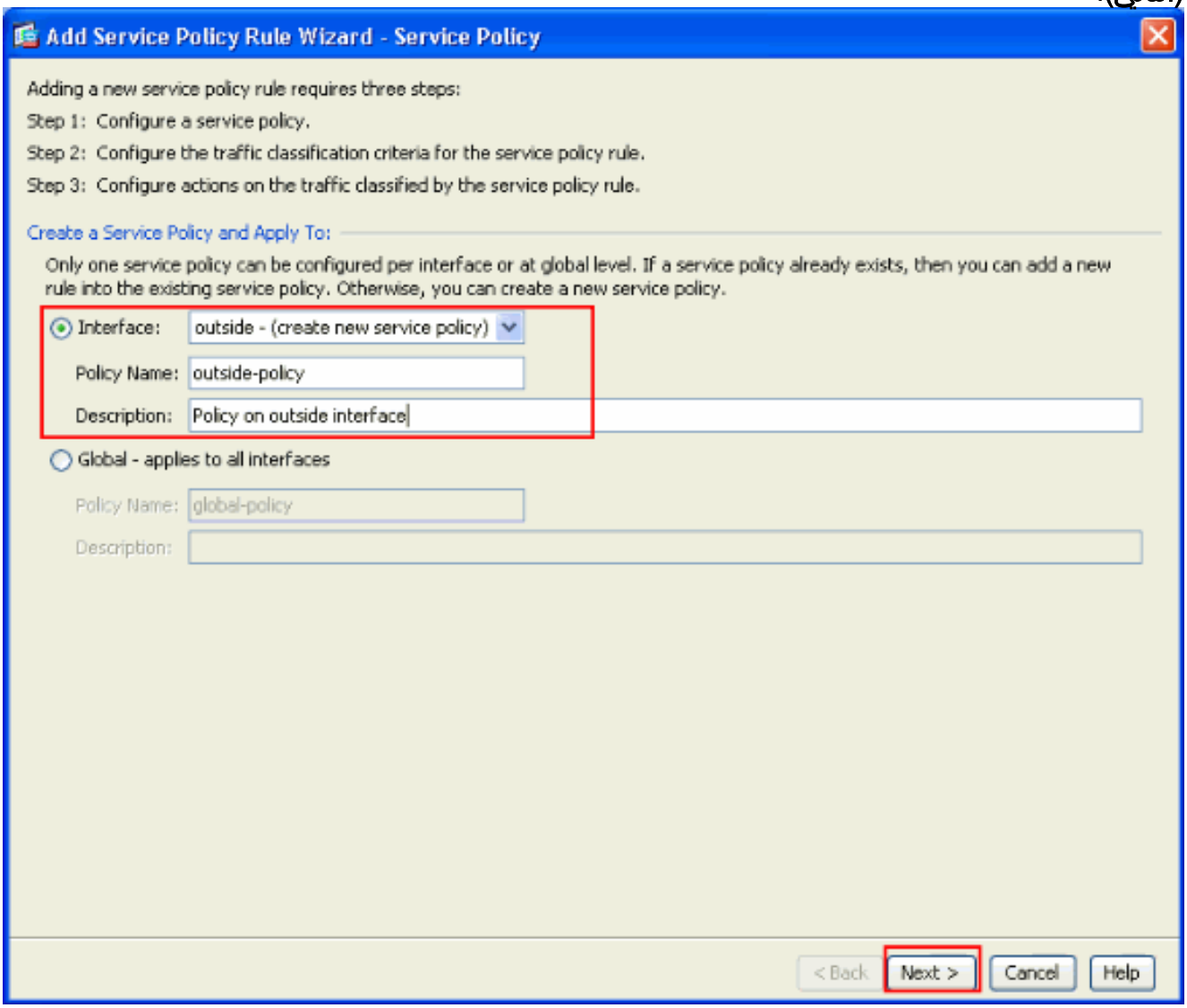


ملاحظة: مع هذه الخطوة، يصبح النهج العام غير مرئي في مدير أجهزة الأمان المعدلة (ASDM)، ولكنه يظهر في واجهة سطر الأوامر (CLI).

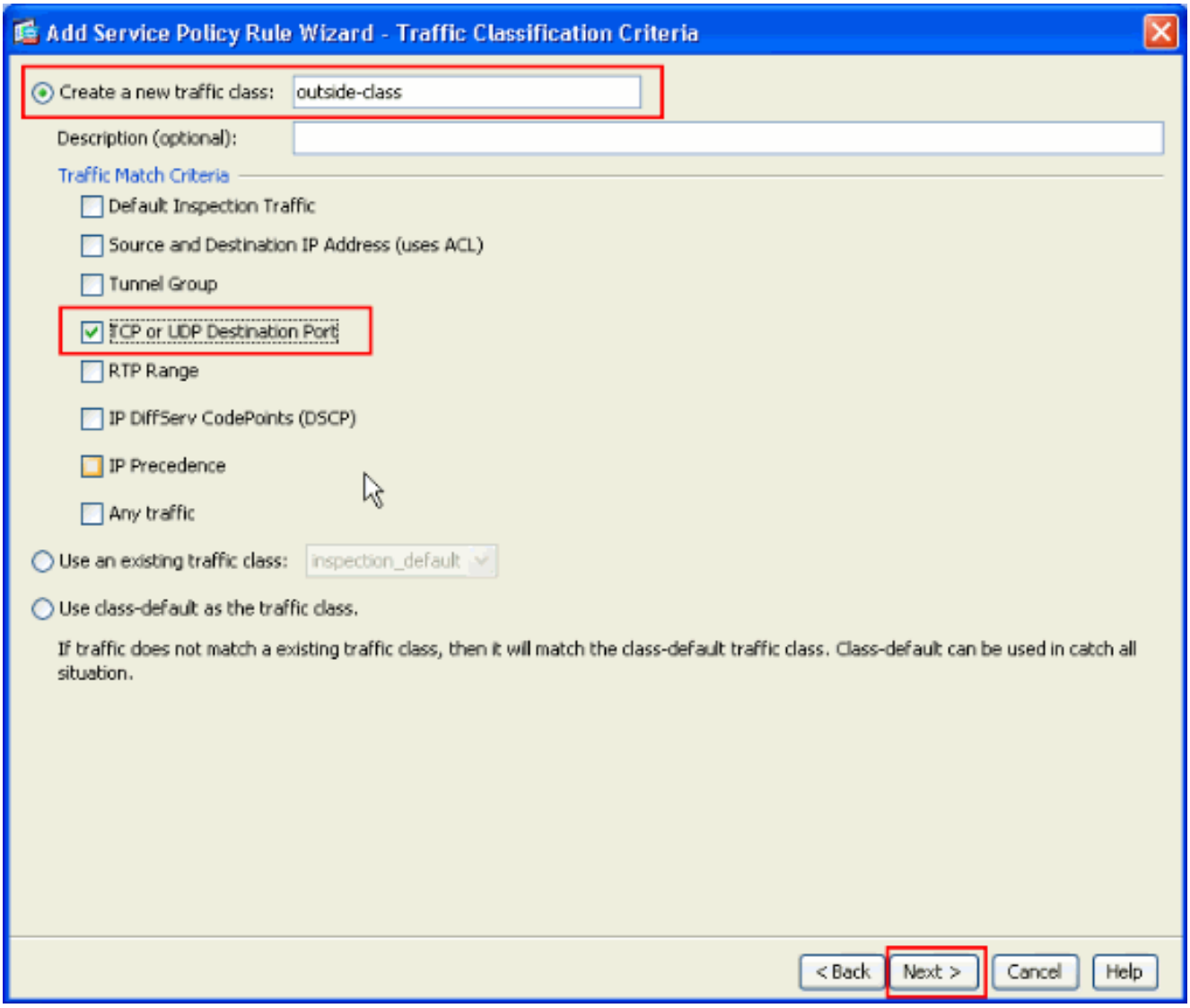
3. انقر فوق **إضافة** لإضافة سياسة جديدة كما هو موضح هنا:



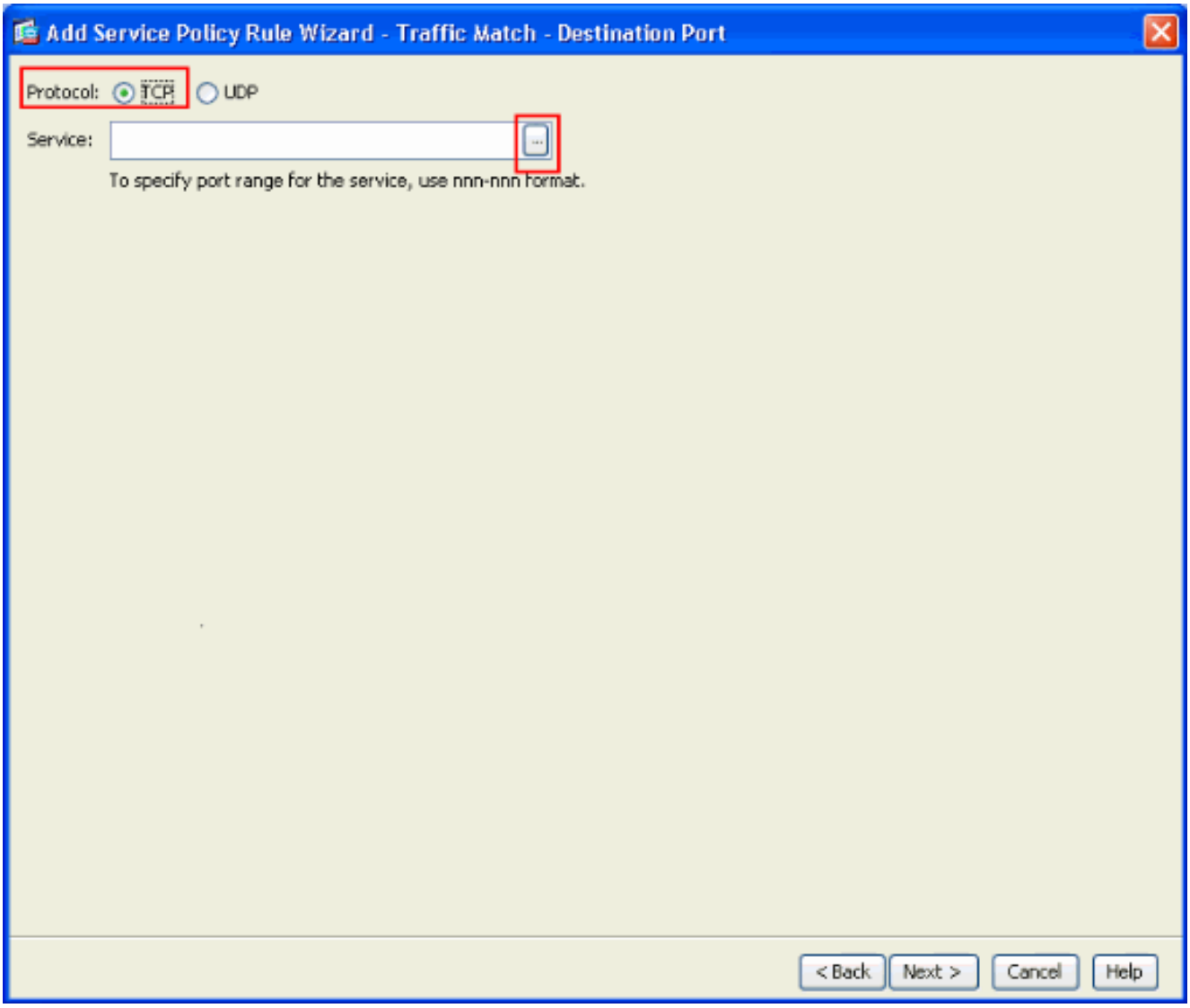
4. تأكد من تحديد زر الخيار المجاور **للواجهة** واختر الواجهة التي تريد تطبيق النهج من القائمة المنسدلة. بعد ذلك، قم بتوفير **اسم النهج** و**الوصف**. انقر فوق **Next** (التالي).



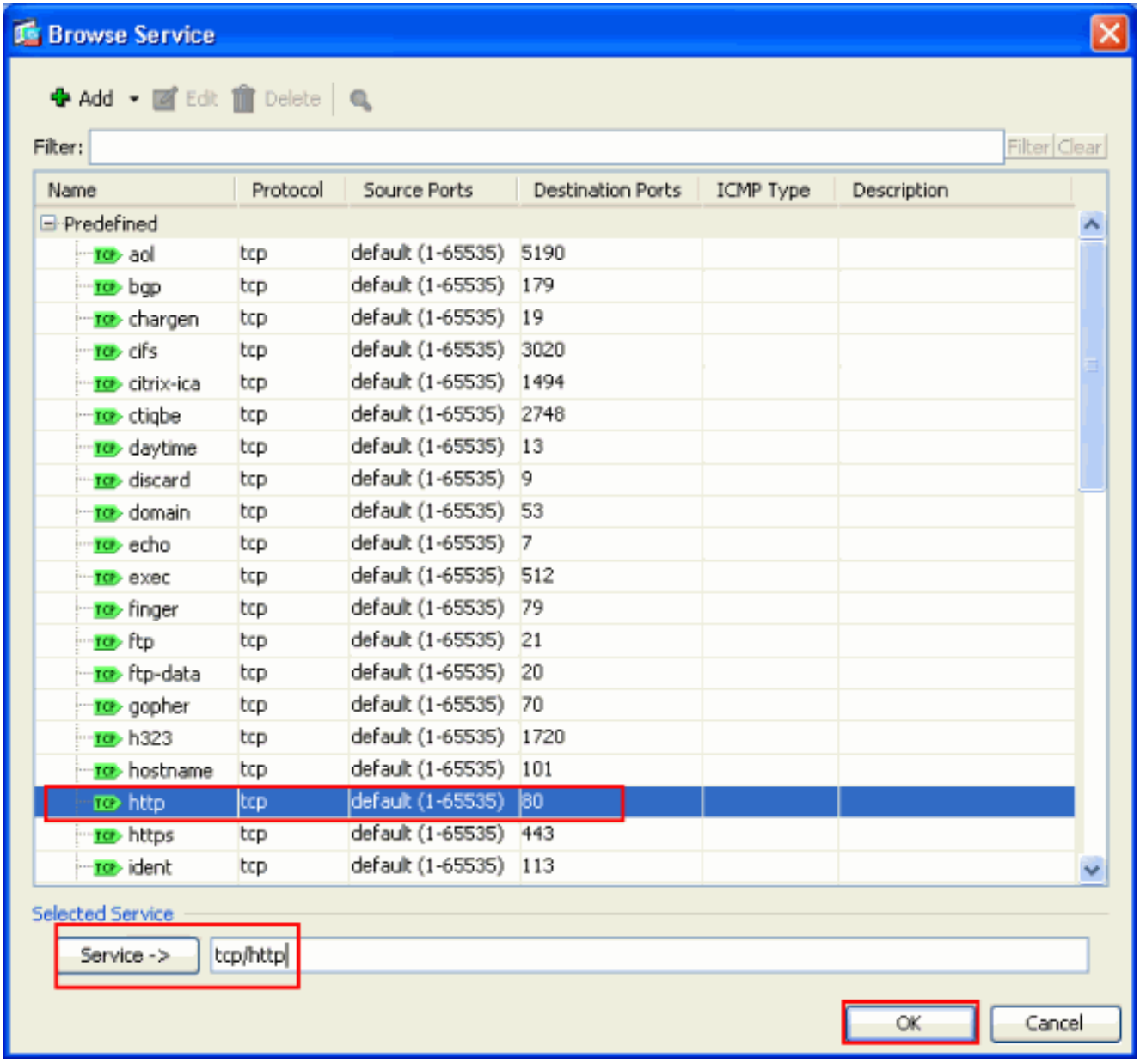
5. قم بإنشاء خريطة فئة جديدة لمطابقة حركة مرور **TCP** نظرا لأن **HTTP** يقع تحت بروتوكول TCP. انقر فوق **Next** (التالي).



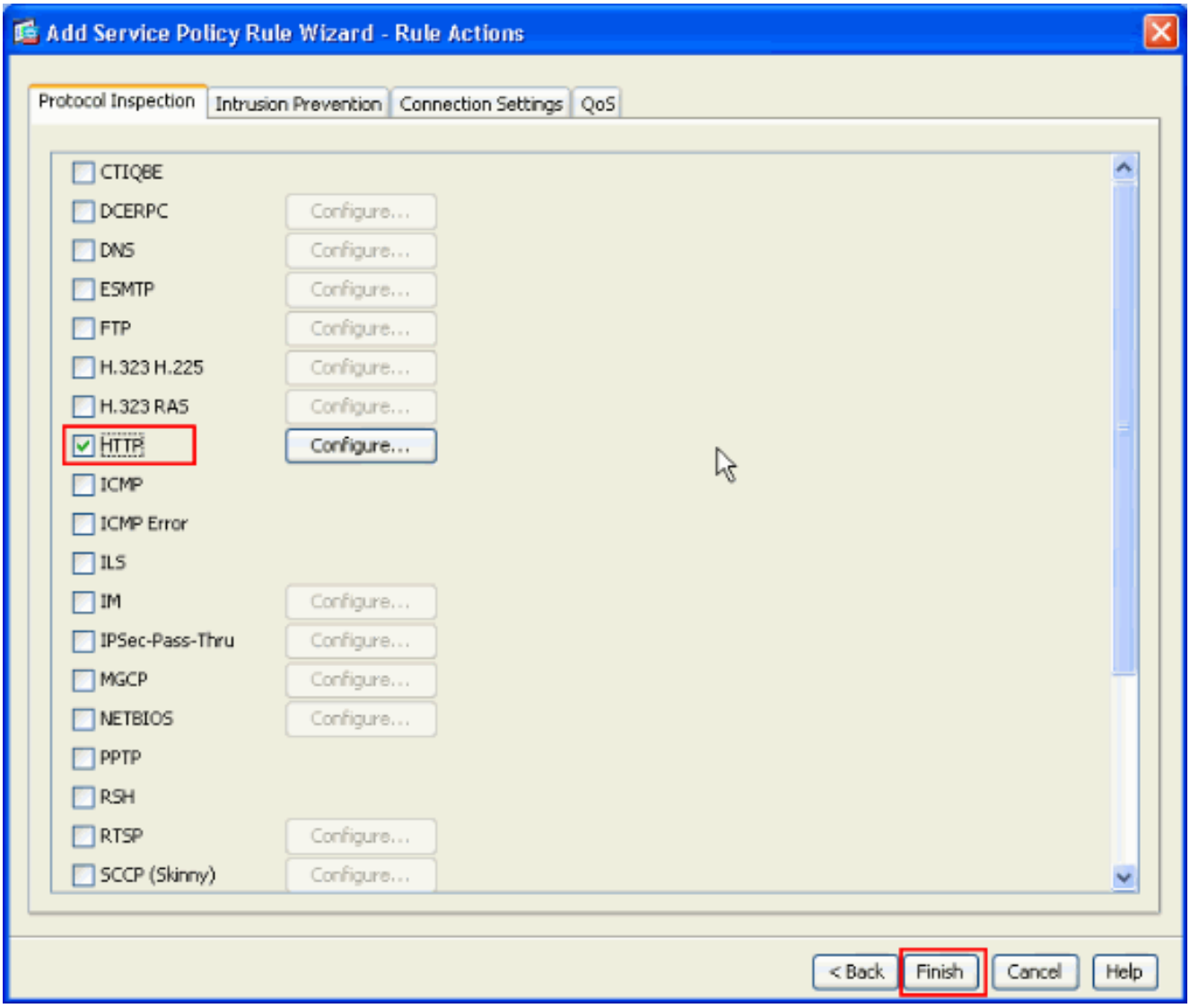
6. أختر **TCP** كبروتوكول.



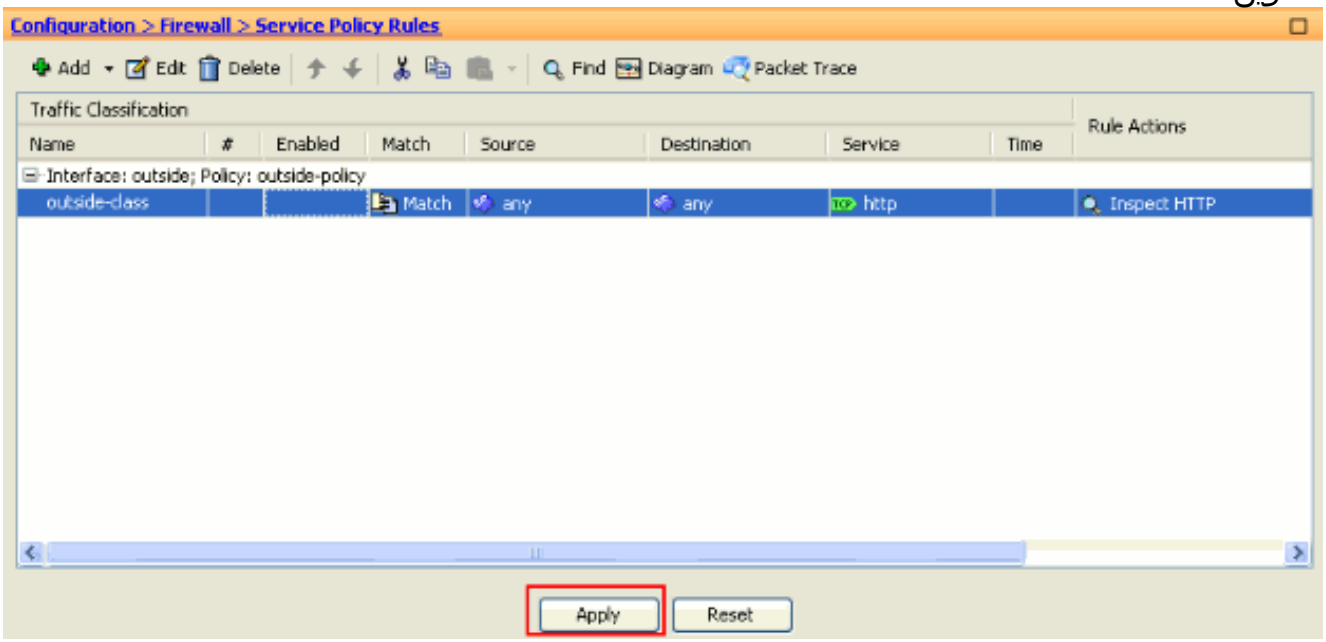
أخترت HTTP **ميناء** 80 كخدمة وطقطقة **ok**.



7. أخترت **http** وطقطقة **إنجاز**.



8. انقر فوق **تطبيق** لإرسال تغييرات التكوين هذه إلى ASA من ASDM. يؤدي هذا إلى اكتمال التكوين.



التحقق من الصحة

استعملت هذا **عرض** أمر أن يدقق التشكيل:

- أستخدم الأمر **show run class-map** لعرض خرائط الفئة التي تم تكوينها.

```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class
match port tcp eq www
!
```

- أستخدم الأمر **show run policy-map** لعرض خرائط السياسة التي تم تكوينها.

```
ciscoasa# sh run policy-map
!
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
policy-map outside-policy
description Policy on outside interface
class outside-class
inspect http
!
```

- أستخدم الأمر **show run service-policy** لعرض سياسات الخدمة التي تم تكوينها.

```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- مراجع أوامر سلسلة ASA 5500 من Cisco
- صفحة دعم مدير أجهزة حلول الأمان المعدلة (ASDM) من Cisco
- برنامج جدار حماية Cisco PIX
- طلبات التعليقات (RFCs)
- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- تطبيق فحص بروتوكول طبقة التطبيق
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- 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).