

م اعل ا ص ح ف ل ا ل ي ط ع ت : ASA/PIX 7.x ر ي غ ق ي ب ط ت ل ا ص ح ف ن ي ك م ت و ي ض ا ر ت ف ا ل ا A S D M م ا د خ ت س ا ب ي ض ا ر ت ف ا ل ا

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [المنتجات ذات الصلة](#)
- [الاصطلاحات](#)
- [السياسة العمومية الافتراضية](#)
- [تمكين فحص التطبيق غير الافتراضي](#)
- [التحقق من الصحة](#)
- [معلومات ذات صلة](#)

[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 استخدام هذا التكوين مع جهاز أمان PIX الذي يشغل صورة البرنامج x.7.

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.)

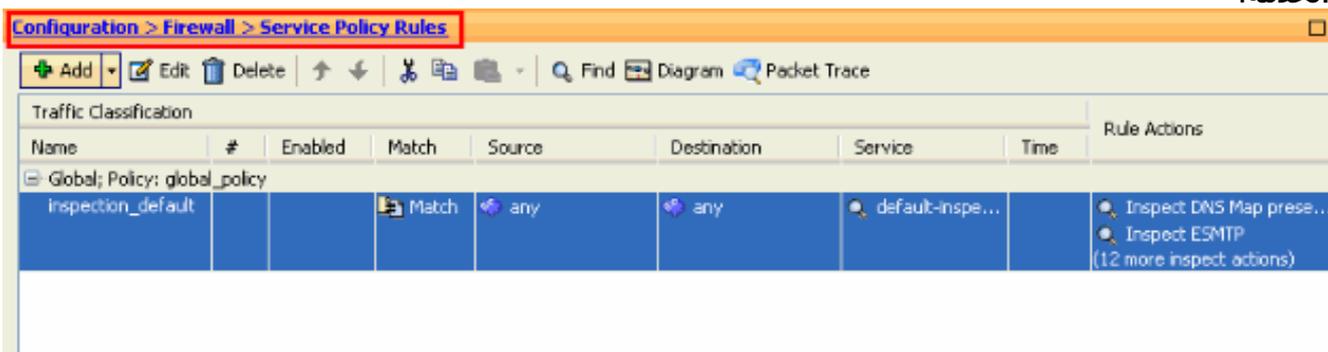
يتضمن تكوين النهج الافتراضي الأوامر التالية:

```
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

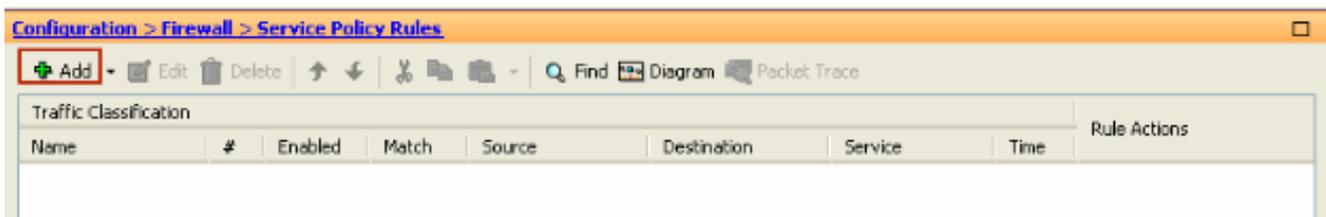
.ASA

The screenshot shows a window titled "Command Line Interface" with a close button in the top right corner. Below the title bar, there is a text area with instructions: "Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash." Below the instructions, there is a "Command" section with two radio buttons: "Single Line" (selected) and "Multiple Line". To the right of these buttons is a checked checkbox labeled "Enable context sensitive help (?)". Below the radio buttons is a text input field containing the command "no service-policy global_policy global". Below the input field is a "Response:" section with a text area containing the output: "Result of the command: 'no service-policy global_policy global'" and "The command has been sent to the device". At the bottom right of the window is a "Clear Response" button. At the bottom center of the window are three buttons: "Send", "Close", and "Help". The "Send" button is highlighted with a red box.

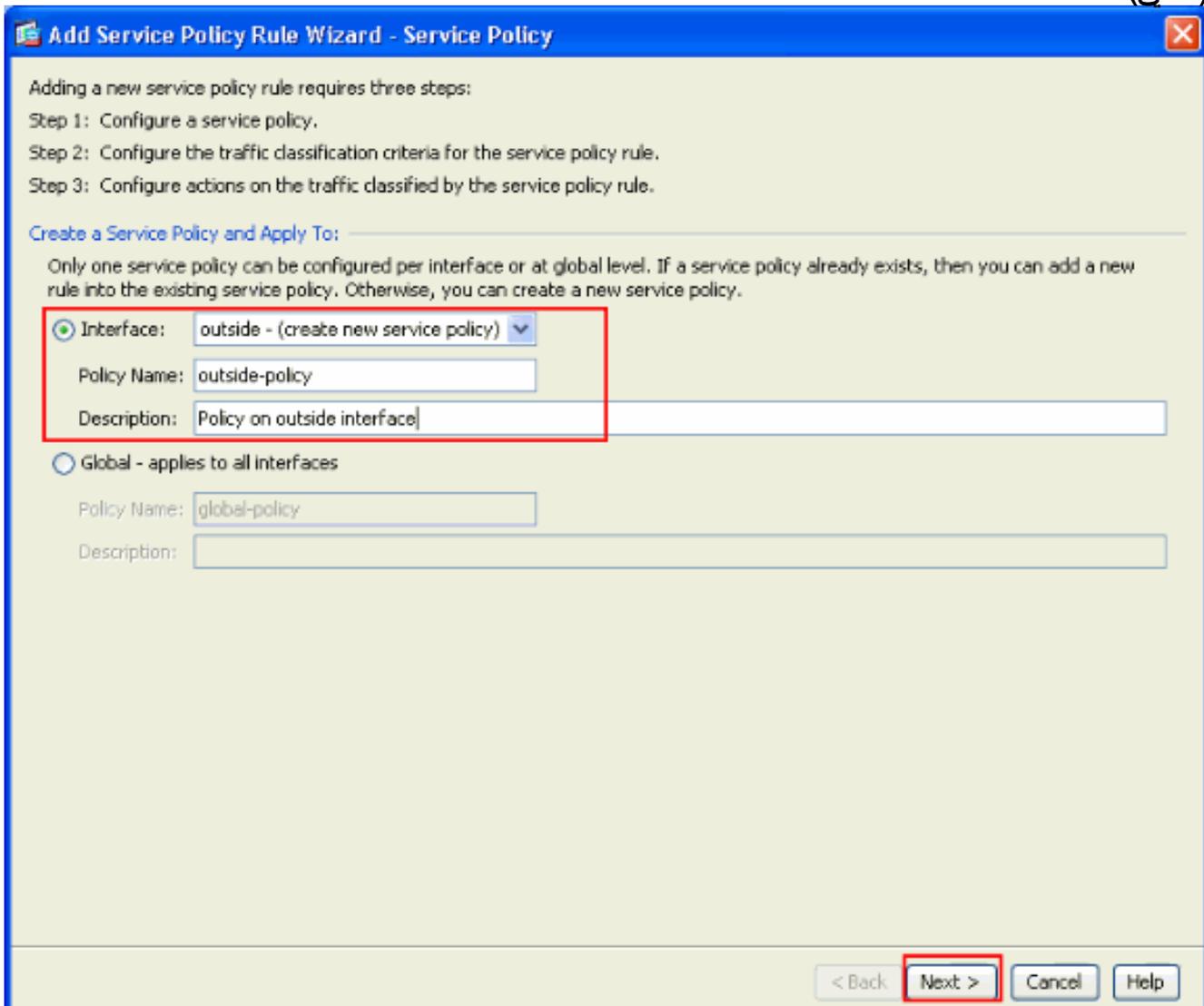
ملاحظة: مع هذه الخطوة، يصبح النهج العام غير مرئي في مدير أجهزة الأمان المعدلة (ASDM)، ولكنه يظهر في واجهة سطر الأوامر (CLI).

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 والوصف. 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).

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

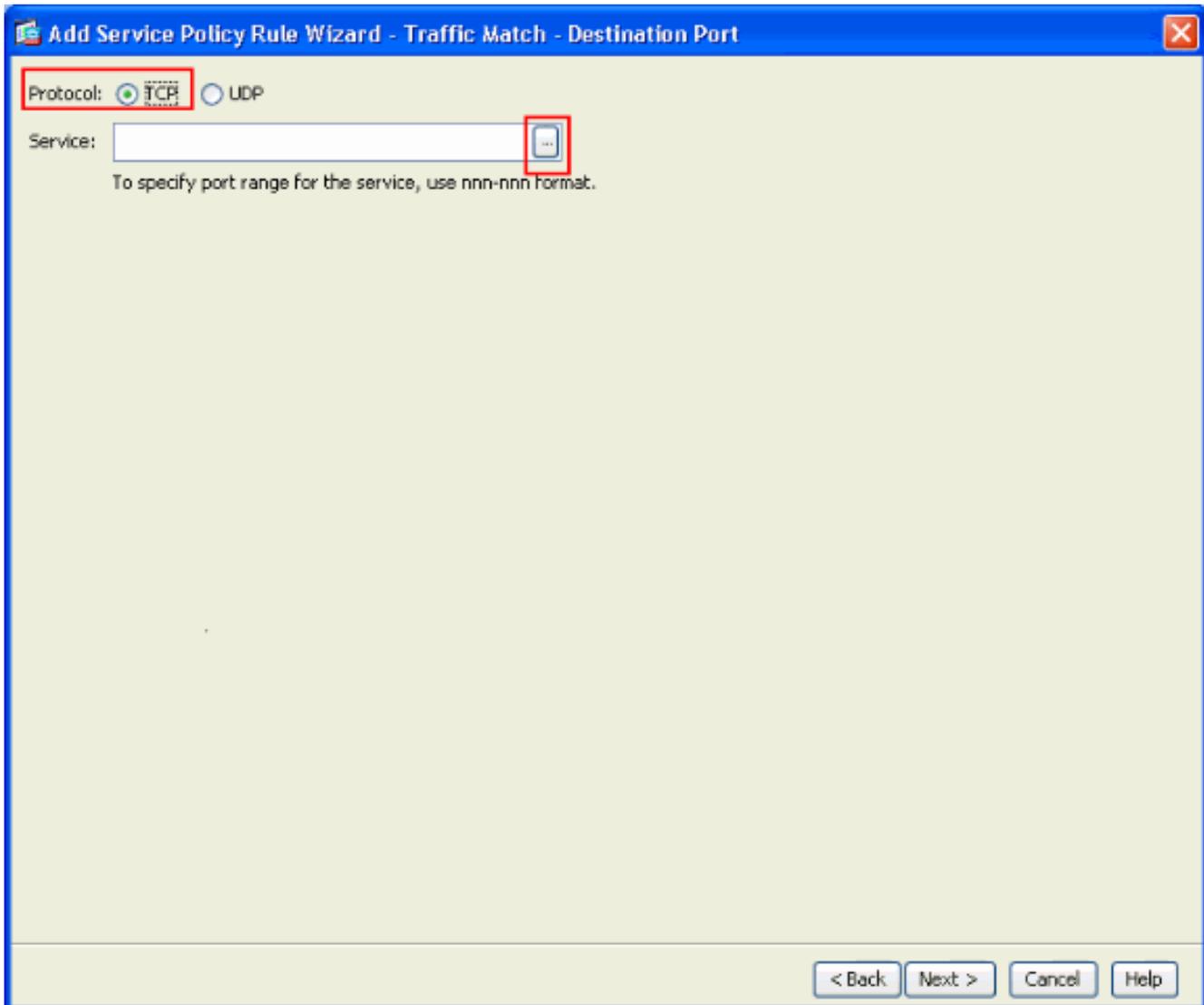
Use an existing traffic class:

Use class-default as the traffic class.

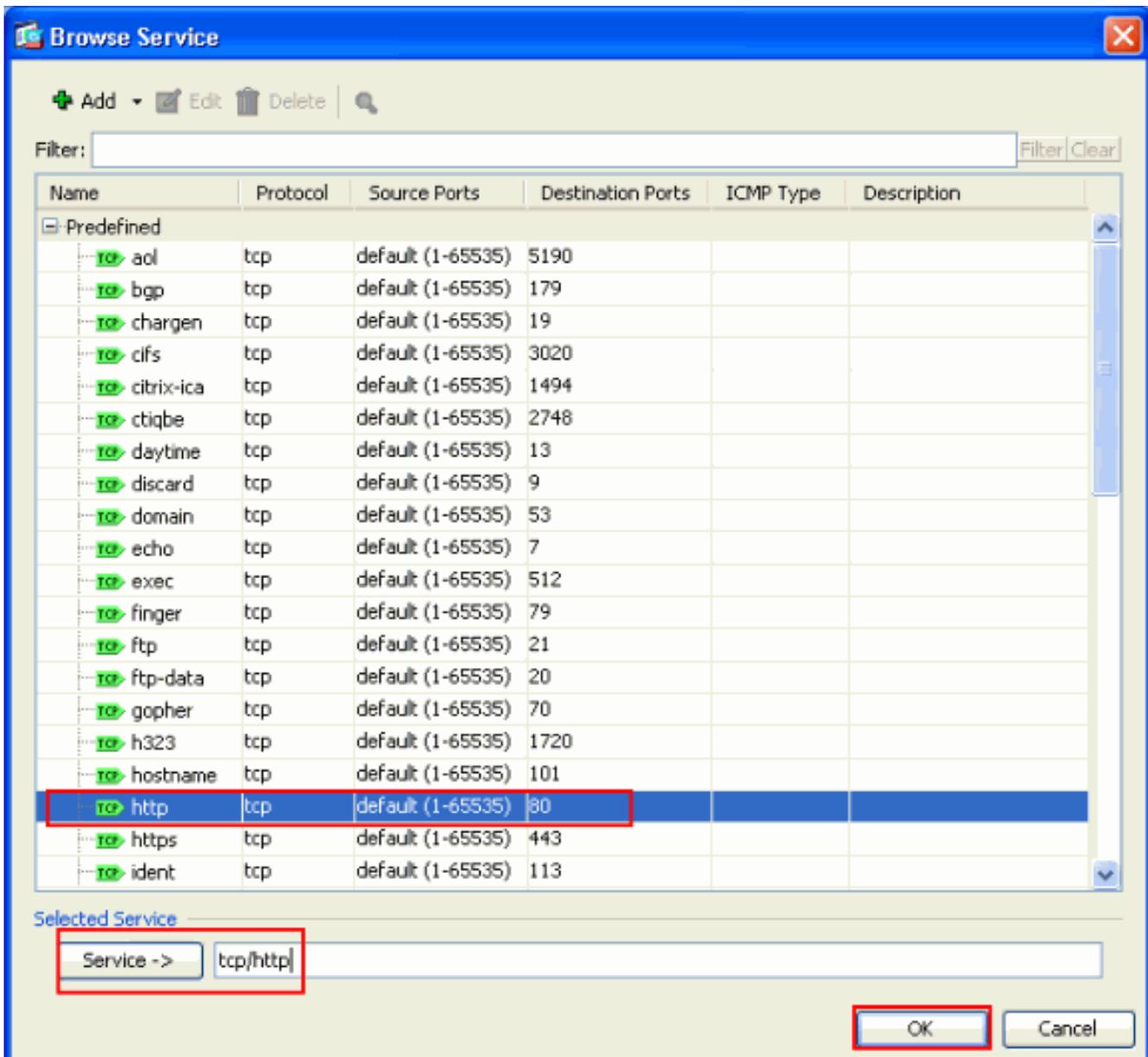
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

< Back **Next >** Cancel Help

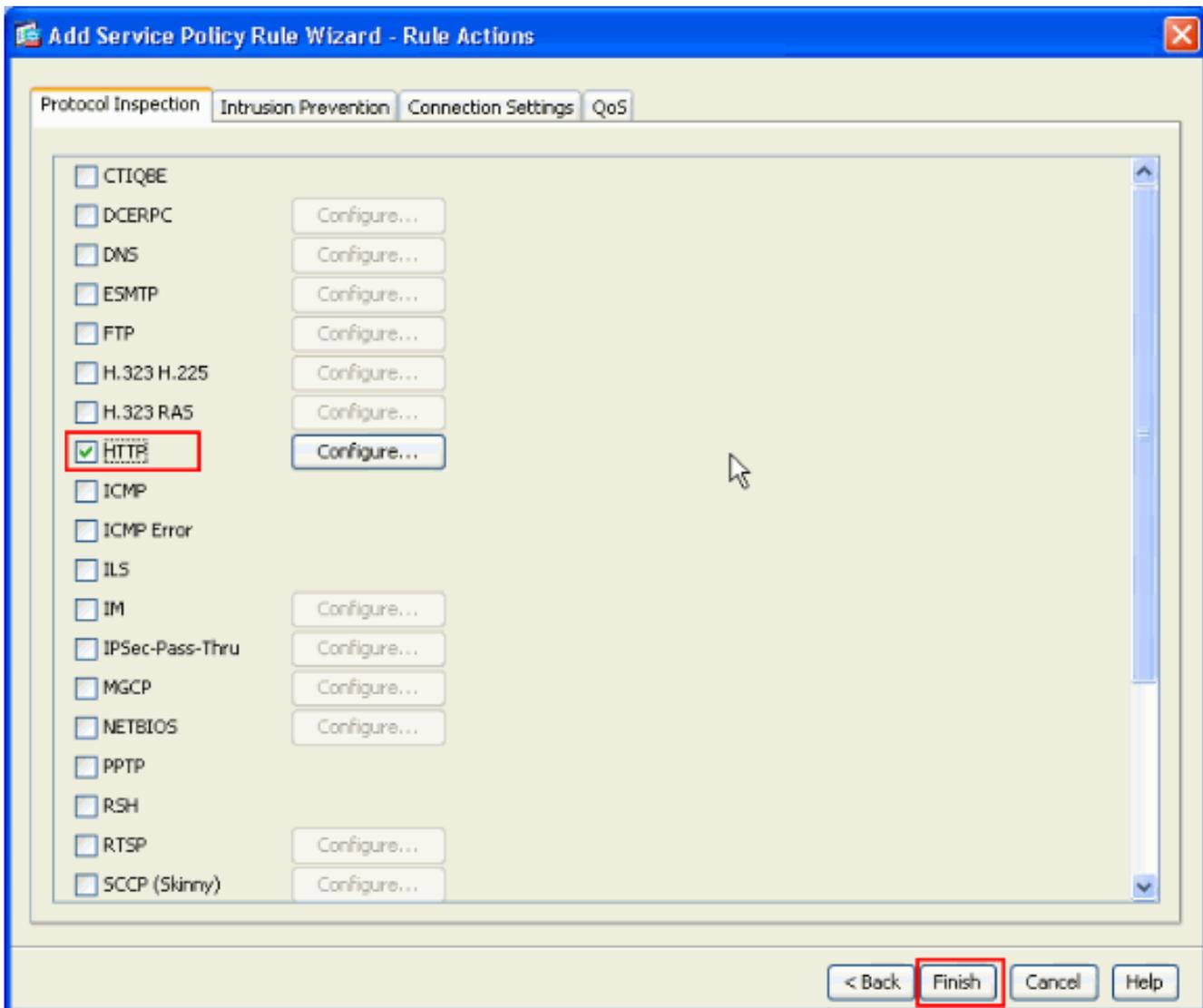
6. اختر TCP
کبروتوکول.



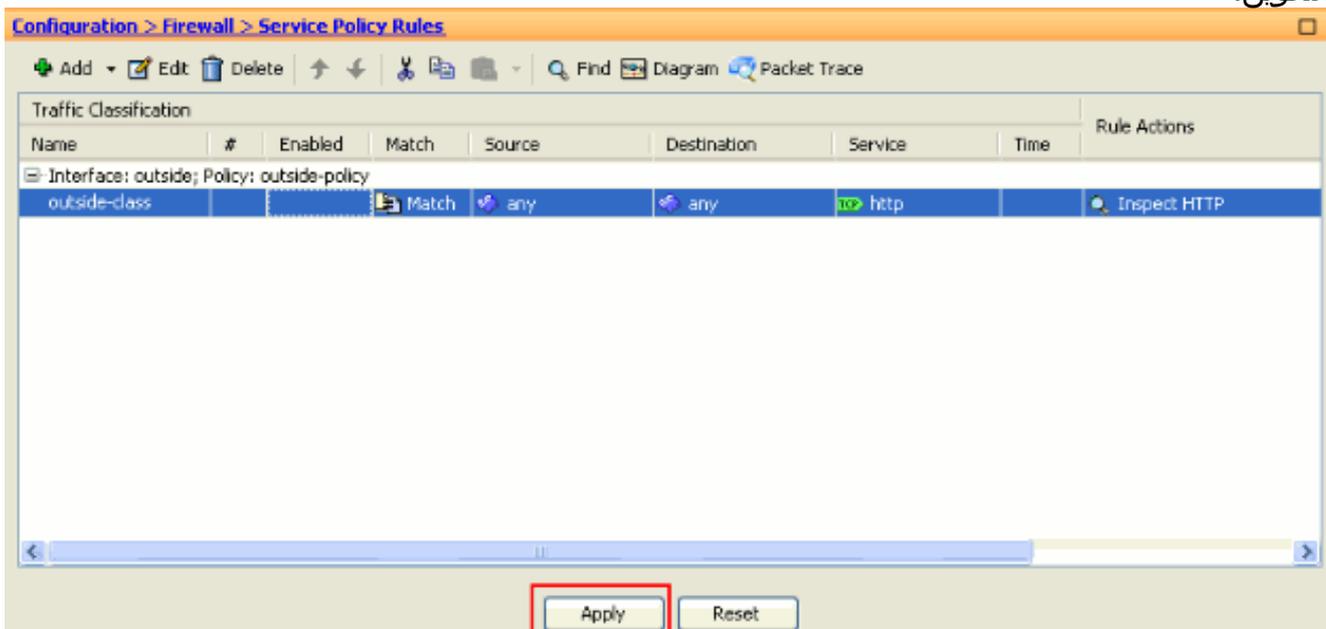
أخترت HTTP ميناء 80 كخدمة وطققة
.ok



7. اخترت http وطفقة
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](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت
ملاعلاء انء مچ م ن م دخت تسمل معد و ت م م دقت ل ة يرش ب ل و
امك ة ق ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م چ ر ة . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل چ ن ا ل ا دن تسمل ا