ASA/PIX 8.x: حظر بعض مواقع الويب (URLs) باستخدام تعبيرات منتظمة مع مثال تكوين MPF

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين أجهزة الأمان Cisco ASA/PIX 8.x التي تستخدم تعبيرات عادية مع إطار عمل السياسة النمطية (MPF) لحظر مواقع الويب المحددة (URLs).

ملاحظة: لا يمنع هذا التكوين جميع تنزيلات التطبيق. بالنسبة لحظر الملفات الذي يمكن الاعتماد عليه، يجب إستخدام جهاز مخصص مثل وحدة IronPort S Series أو وحدة مثل وحدة CSC Module ل ASA.

ملاحظة: تصفية HTTPS غير مدعومة على ASA. يتعذر على ASA إجراء فحص أو فحص متعمق للحزم استنادا إلى التعبير العادي لحركة مرور HTTPS، لأنه في HTTPS، يتم تشفير محتوى الحزمة (SSL).

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند تكوين جهاز أمان Cisco وأنه يعمل بشكل صحيح.

المكونات المستخدمة

- جهاز الأمان القابل للتكيف (ASA) من Cisco 5500 Series الذي يشغل الإصدار 8.0(x) من البرنامج والإصدارات الأحدث
- Cisco Adaptive Security Device Manager (ASDM)، الإصدار 6.x ل ASA 8.x

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

هذا تشكيل يستطيع أيضا كنت استعملت مع ال cisco 500 sery PIX أن يركض البرمجية صيغة 8.0(x) وفيما بعد.

الاصطلاحات

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

معلومات أساسية

نظرة عامة على إطار عمل السياسة النمطية

توفر ميزة "حماية مستوى الإدارة (MPF)" طريقة متناسقة ومرنة لتكوين ميزات جهاز الأمان. على سبيل المثال، يمكنك إستخدام ميزة "حماية مستوى الإدارة (MPF)" لإنشاء تكوين مهلة محدد لتطبيق TCP معين، بدلا من واحد ينطبق على جميع تطبيقات TCP.

تدعم ميزة "حماية مستوى الإدارة (MPF)" الميزات التالية:

- تطبيع TCP، وحدود اتصال TCP و UDP، وحالات انتهاء المهلة، وترقيم رقم تسلسل TCP عشوائيا
- CSC
- فحص التطبيق
- IPS
- وضع سياسات إدخال جودة الخدمة
- وضع سياسات إخراج جودة الخدمة
- قائمة انتظار أولوية جودة الخدمة

يتكون تكوين ميزة "حماية مستوى الإدارة (MPF)" من أربع مهام:

1. قم بتعريف حركة مرور الطبقة 3 و 4 التي تريد تطبيق العمليات عليها. راجع تحديد حركة المرور باستخدام خريطة فئة الطبقة 4/3 للحصول على مزيد من المعلومات.
2. (فحص التطبيق فقط) حدد الإجراءات الخاصة لحركة مرور فحص التطبيق. راجع تكوين الإجراءات الخاصة لتفتيش التطبيقات للحصول على مزيد من المعلومات.
3. تطبيق إجراءات على حركة مرور الطبقة 3 و 4. راجع تحديد الإجراءات باستخدام خريطة سياسة الطبقة 4/3 للحصول على مزيد من المعلومات.
4. قم بتنشيط الإجراءات على واجهة. راجع تطبيق سياسة الطبقة 4/3 على واجهة تستخدم سياسة الخدمة للحصول على مزيد من المعلومات.

تعبير نمطي

يطابق التعبير النمطي سلاسل النص إما حرفيا كسلسلة دقيقة، أو باستخدام الحروف الأولية بحيث يمكنك مطابقة متغيرات متعددة من سلسلة نص. يمكنك إستخدام تعبير عادي لمطابقة محتوى حركة مرور تطبيق معينة؛ على سبيل المثال، يمكنك مطابقة سلسلة URL داخل حزمة HTTP.

ملاحظة: أستخدم **Ctrl+V** للهروب من كل الحروف الخاصة في CLI، مثل علامة السؤال (؟) أو علامة التبويب. على سبيل المثال، اكتب **g؟d[Ctrl+V]** لإدخال **g؟d** في التكوين.

لإنشاء تعبير عادي، أستخدم الأمر **regex**، والذي يمكن إستخدامه للميزات المختلفة التي تتطلب مطابقة النص. على سبيل المثال، يمكنك تكوين إجراءات خاصة لفحص التطبيق باستخدام إطار عمل سياسة نمطي يستخدم خريطة سياسة فحص. راجع الأمر **فحص نوع خريطة السياسة** للحصول على مزيد من المعلومات. في خريطة سياسة التفتيش، يمكنك تعريف حركة المرور التي تريد العمل عليها إذا قمت بإنشاء خريطة فئة تفتيش تحتوي على واحد أو أكثر من أوامر **مطابقة** أو يمكنك إستخدام أوامر **مطابقة** مباشرة في خريطة سياسة التفتيش. تتيح لك بعض أوامر **التطابق** تعريف النص في الحزمة باستخدام تعبير عادي؛ على سبيل المثال، يمكنك مطابقة سلاسل عنوان URL داخل حزم HTTP. يمكنك تجميع التعبيرات العادية في خريطة فئة تعبير نمطي. راجع الأمر **class-map type regex** للحصول على مزيد من المعلومات.

يسرد هذا الجدول الحروف الأولية التي لها معان خاصة.

الحرف	الوصف	ملاحظات
.	نقطة	مطابقة أي حرف واحد. على سبيل المثال، **D.G** يطابق الكلب، dag، dtg، وأي كلمة تحتوي على تلك الحروف، مثل doggonit.
(exp)	ضغط جزئي	يفصل التعبير الجزئي الحروف

		عن الحروف المحيطة، بحيث يمكنك إستخدام حروف أولية أخرى على التعبير الجزئي. على سبيل المثال، تطابق d(o|a)g(مع الكلب والداغ، ولكن do|ag تطابق do and.ag. يمكن أيضا إستخدام التعبير الجزئي مع كميه التكرار لتمييز الحروف المقصودة للتكرار.

على سبيل المثال ، **ab(xy){3}z** يطابق abxyxyxyxyz.		
يطابق أيا من التعبيرين اللذين يفصلهما. على سبيل المثال ، يطابق **الكلب|القط** الكلب أو القط.	تناوب	|
قيمة كمية تشير إلى وجود 0 أو 1 من التعبير السابق. على سبيل المثال ، إما **أن** تتطابق مع **قيمة** العرض أو أن	علامة الاستفهام	؟

		تخسر . **ملاحظة:** يجب إدخال **Ctrl+V** ثم علامة الاستفهام وإلا سيتم إستدعاء دالة المساعدة.
*	نجمية	قيمة كمية تشير إلى وجود 0 أو 1 أو أي عدد من التعبير السابق. على سبيل المثال، يطابق **لو*se**lse، يخسر، يخسر، يخسر، وهكذا دواليك.
{x}	تكرار القياس	تكرار x مرات

		بالضبط. على سبيل المثال، **ab(xy){3}z** يطابق abxyxyxyz.
{x،}	الحد الأدنى لمكبر التكرار	تكرار x مرة على الأقل. على سبيل المثال، **ab(xy){2،}z** يطابق abxyxyz، abxyxyz، وهكذا دواليك.
[أي بي سي]	فئة الحرف	مطابقة أي حرف في الأقواس. على سبيل المثال، **[abc]** يطابق أ، ب، أو ج.
[abc^]	فئة الحرف	مطابقة

	الضار	حرف واحد غير موجود داخل الأقواس. على سبيل المثال، **[^ab]** يطابق أي حرف غير a، b، أو c. **[^a-z]** يطابق أي حرف مفرد ليس حرف كبير.
[ألف-جيم]	فئة نطاق الحروف	مطابقة أي حرف في النطاق. **[a-z]** يطابق أي حرف صغير. يمكنك مزج الحروف والنطاقات: **[abcq-z]** تطابق a، b، c،

		q، r، s، t، u، v، w، x، y، z، وهكذا **[a-cq-z]**. حرف شرطة (-) حرفي فقط إذا كان هو الحرف الأخير أو الأول داخل الأقواس: **[-abc]** أو **[abc-]**.
""	علامات الاقتباس	يحافظ على المسافات الخلفية أو المسافات البادئة في السلسلة. على سبيل المثال، يحتفظ **الاختبار** بمسافة المسا

		فة البادئة عندما يبحث عن تطابق.
٨	علامة الإقحام	يحدد بداية السطر
\	حرف الهروب	عند إستخدامه مع حرف أولي، يطابق حرف حرفي. على سبيل المثال، \[يطابق القوس المربع الأيسر.
فحم	الحرف	عندما لا يكون الحرف الأولي، يطابق الحرف الحرفي.
r\	إعادة النقل	مطابقة إرجاع النقل 0x0d

\n	نيولاين	مطابقة سطر جديد 0x0a
\t	علامة تبويب	مطابقة علامة تبويب 0x09
\f	فورم فييد	مطابقة موجز نموذج 0x0c
\xNN	الرقم السداسي العشري الفار	مطابقة حرف ASCII يستخدم قاعدة بيانات سداسية عشرية مكونة من رقمين بالضبط
\NNN	عدد ثماني منفر	مطابقة حرف ASCII على هيئة ثمانية تكون ثلاثة أرقام بالضبط. على سبيل المثال ،

		يمثل الحرف 040 مسافة.

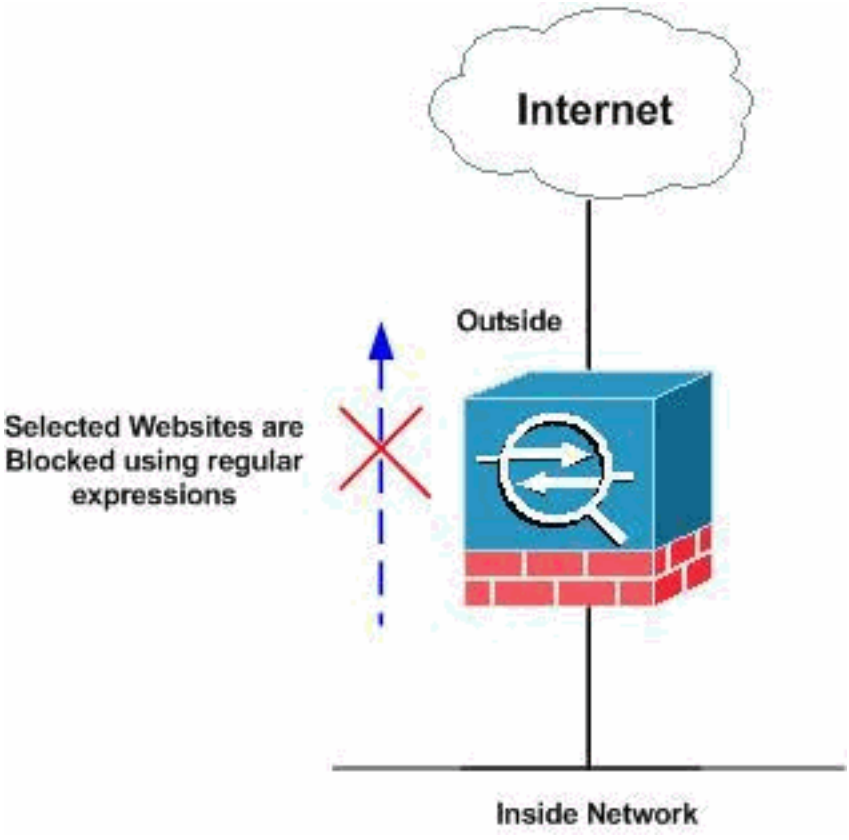
التكوين

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.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين ASA CLI
- تشكيل ASA x.8 مع ASDM 6.x

تكوين ASA CLI

تكوين ASA CLI

```
ciscoasa#show running-config
Saved :
:
(ASA Version 8.0(2
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
nameif outside
security-level 0
ip address 192.168.1.5 255.255.255.0
!
interface Ethernet0/2
nameif DMZ
security-level 90
ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted

regex urllist1
".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt])
"[HTTP/1.[01

 Extensions such as .exe, .com, .bat to be captured ---!
    and !--- provided the http version being used by web
        browser must be either 1.0 or 1.1 regex urllist2
".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh])
"[HTTP/1.[01
 Extensions such as .pif, .vbs, .wsh to be captured ---!
    !--- and provided the http version being used by web
      browser must be either !--- 1.0 or 1.1 regex urllist3
".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt])
"[HTTP/1.[01

Extensions such as .doc(word), .xls(ms-excel), .ppt ---!
 to be captured and provided !--- the http version being
     used by web browser must be either 1.0 or 1.1 regex
 urllist4 ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz])
"[HTTP/1.[01

 Extensions such as .zip, .tar, .tgz to be captured ---!
```

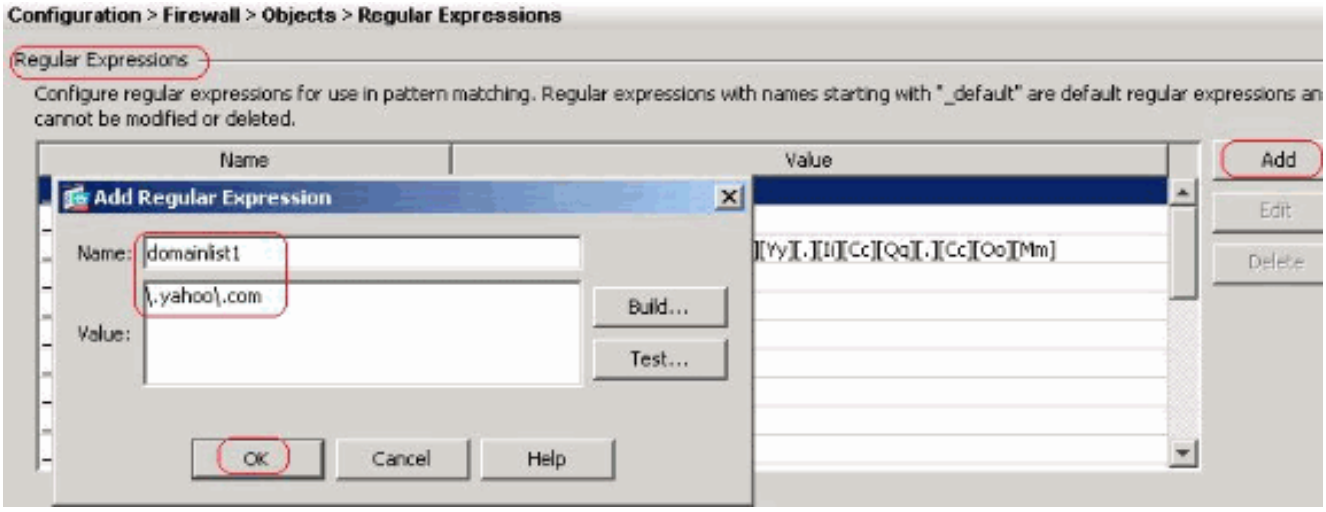
```
and provided !--- the http version being used by web
browser must be either 1.0 or 1.1 regex domainlist1
                                        ""\.yahoo\.com
                    "regex domainlist2 "\.myspace\.com
                    "regex domainlist3 "\.youtube\.com

Captures the URLs with domain name like yahoo.com, ---!
    !--- youtube.com and myspace.com regex contenttype
                                        ""Content-Type
              "*./regex applicationheader "application

  Captures the application header and type of !--- ---!
content in order for analysis boot system disk0:/asa802-
    k8.bin ftp mode passive dns server-group DefaultDNS
         domain-name default.domain.invalid access-list
          inside_mpc extended permit tcp any any eq www

  access-list inside_mpc extended permit tcp any any eq
                                                  8080

    Filters the http and port 8080 !--- traffic in ---!
  order to block the specific traffic with regular !---
  expressions pager lines 24 mtu inside 1500 mtu outside
   1500 mtu DMZ 1500 no failover icmp unreachable rate-
  limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no
 asdm history enable arp timeout 14400 route DMZ 0.0.0.0
   0.0.0.0 10.77.241.129 1 timeout xlate 3:00:00 timeout
      conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
      mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
    sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
  0:02:00 timeout uauth 0:05:00 absolute dynamic-access-
  policy-record DfltAccessPolicy http server enable http
   0.0.0.0 0.0.0.0 DMZ no snmp-server location no snmp-
           server contact snmp-server enable traps snmp
     authentication linkup linkdown coldstart no crypto
    isakmp nat-traversal telnet timeout 5 ssh timeout 5
 console timeout 0 threat-detection basic-threat threat-
 detection statistics access-list ! class-map type regex
                                  match-any DomainBlockList
                                   match regex domainlist1
                                   match regex domainlist2
                                   match regex domainlist3

    Class map created in order to match the domain ---!
   names !--- to be blocked class-map type inspect http
                                 match-all BlockDomainsClass
 match request header host regex class DomainBlockList

      Inspect the identified traffic by class !--- ---!
      "DomainBlockList". class-map type regex match-any
                                                URLBlockList
                                      match regex urllist1
                                      match regex urllist2
                                      match regex urllist3
                                      match regex urllist4

  Class map created in order to match the URLs !--- ---!
       to be blocked class-map inspection_default match
 default-inspection-traffic class-map type inspect http
                                    match-all AppHeaderClass
          match response header regex contenttype regex
                                             applicationheader
```

```
Inspect the captured traffic by regular !--- ---!
expressions "content-type" and "applicationheader".
                                    class-map httptraffic
                                  match access-list inside_mpc

Class map created in order to match the !--- ---!
filtered traffic by ACL class-map type inspect http
                                  match-all BlockURLsClass
                          match request uri regex class URLBlockList
                                                              !
Inspect the identified traffic by class !--- ---!
    "URLBlockList". ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map type inspect http http_inspection_policy
                                                  parameters
                          protocol-violation action drop-connection
                                    class AppHeaderClass
                                    drop-connection log
                                match request method connect
                                    drop-connection log
                                class BlockDomainsClass
                                              reset log
                                   class BlockURLsClass
                                              reset log

Define the actions such as drop, reset or log !--- ---!
in the inspection policy map. policy-map global_policy
   class inspection_default inspect dns preset_dns_map
 inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
             sip inspect xdmcp policy-map inside-policy
                                    class httptraffic
                        inspect http http_inspection_policy

Map the inspection policy map to the class !--- ---!
"httptraffic" under the policy map created for the !---
inside network traffic. ! service-policy global_policy
   global service-policy inside-policy interface inside

Apply the policy to the interface inside where the ---!
          websites are blocked. prompt hostname context
Cryptochecksum:e629251a7c37af205c289cf78629fc11 : end
                                                #ciscoasa
```

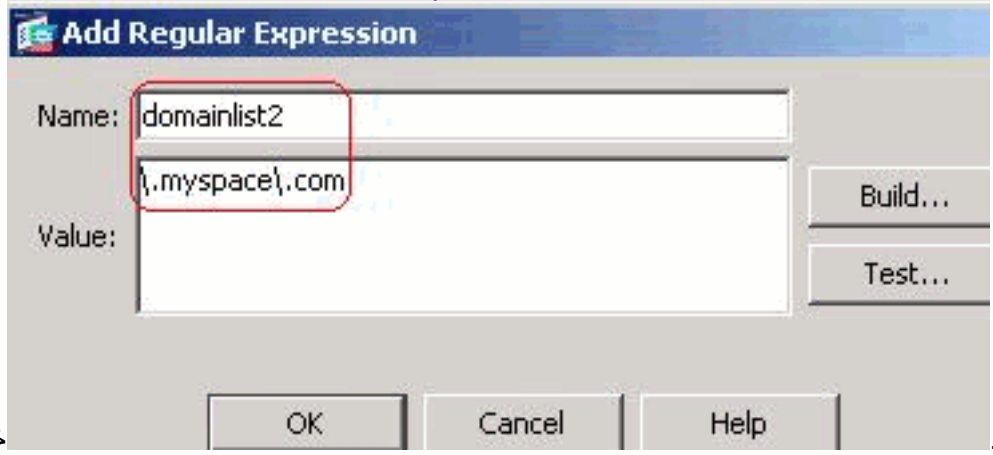
ASA تشكيل x.8 مع ASDM 6.x

أكمل هذه الخطوات لتكوين التعبيرات العادية وتطبيقها في MPF لحظر مواقع الويب المحددة كما هو موضح.

1. **إنشاء تعبيرات عادية**أخترت **تشكيل > جدار حماية> كائن > تعابير عادية** وطقطقة **يضيف** تحت علامة التبويب **تعبير عادي** in order to خلقت تعابير عادي كما هو موضح.خلقت تعبير عادي in order to **domainList1** على قبض ال **yahoo.com** domain name. وانقر فوق **OK**.

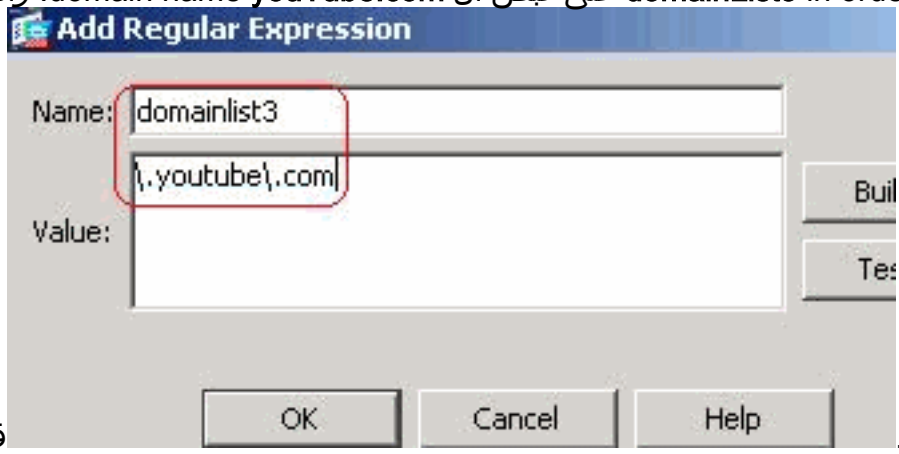


قم بإنشاء **مجال** تعبير عادي **2** من أجل التقاط اسم المجال **myspace.com**. وانقر فوق

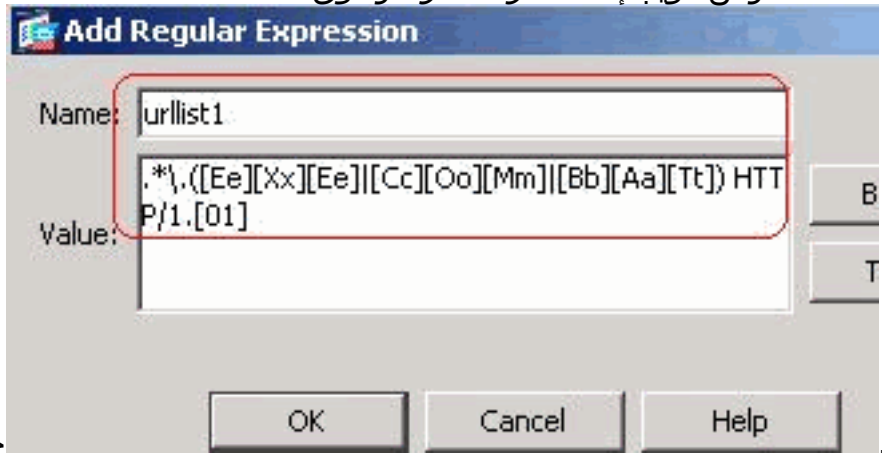


خلقت تعبير عادي **OK**.

in order to **domainList3** على قبض ال domain name **youTube.com**. وانقر فوق

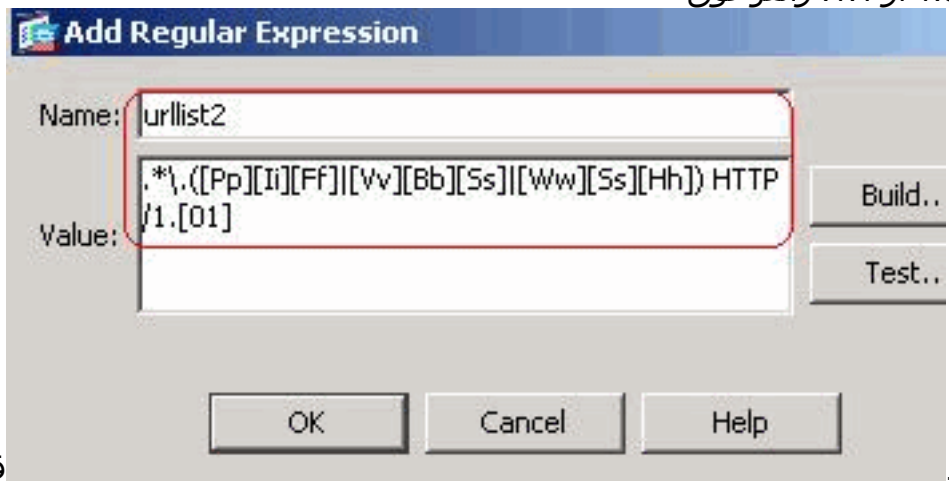


قم بإنشاء **قائمة** مرور **تعبير** عادية من أجل التقاط امتدادات الملفات مثل **exe** و**com** و**bat**، شريطة أن يكون إصدار http الذي يتم إستخدامه بواسطة مستعرض الويب إما 1.0 أو 1.1. وانقر فوق

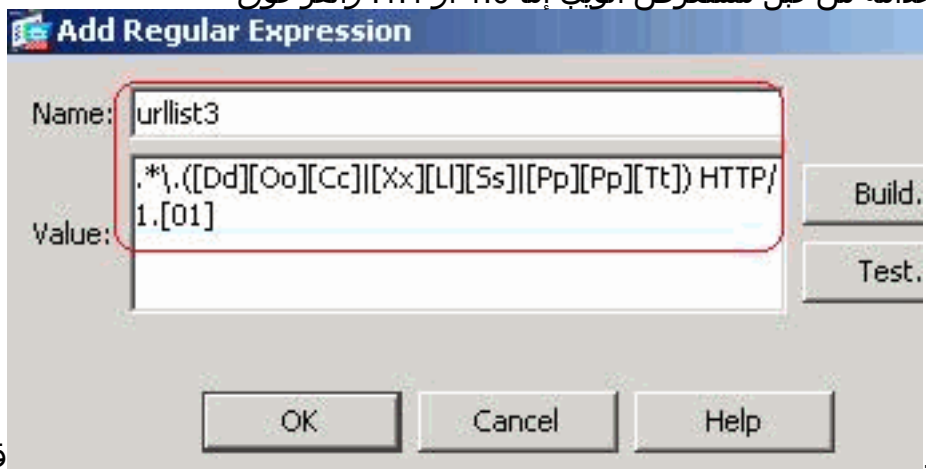


خلقت تعبير عادي in **urllist2** **OK**.

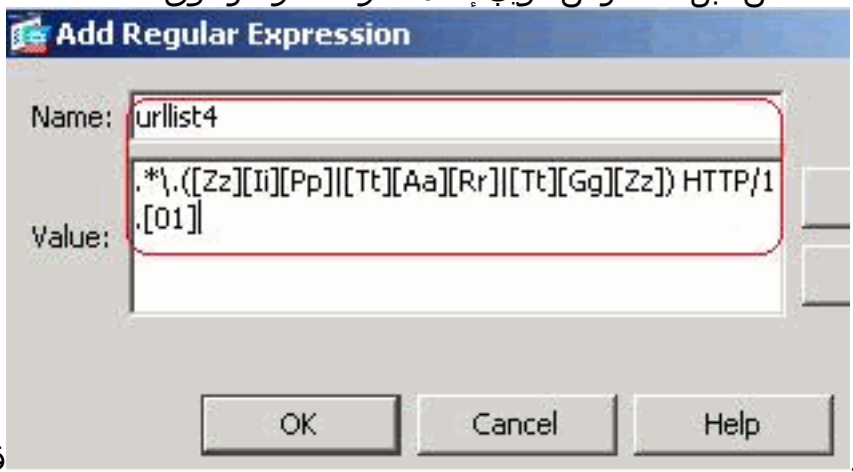
order to على قبض الملف امتدادات مثل **vbs**، **pif** و**wsh** أن ال http صيغة أن يكون استعملت بمتصفح ويب إما 1.0 أو 1.1. وانقر فوق



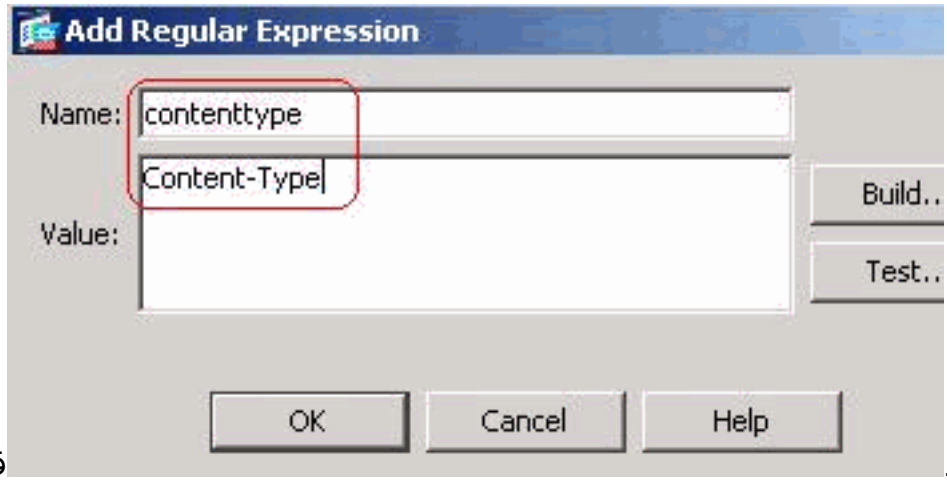
OK. قم بإنشاء **قائمة** مرور **تعبير** عادية 3 من أجل التقاط ملحقات الملفات مثل **doc** و**xls** و**ppt**، شريطة أن يكون إصدار http الذي يتم إستخدامه من قبل مستعرض الويب إما 1.0 أو 1.1. وانقر فوق



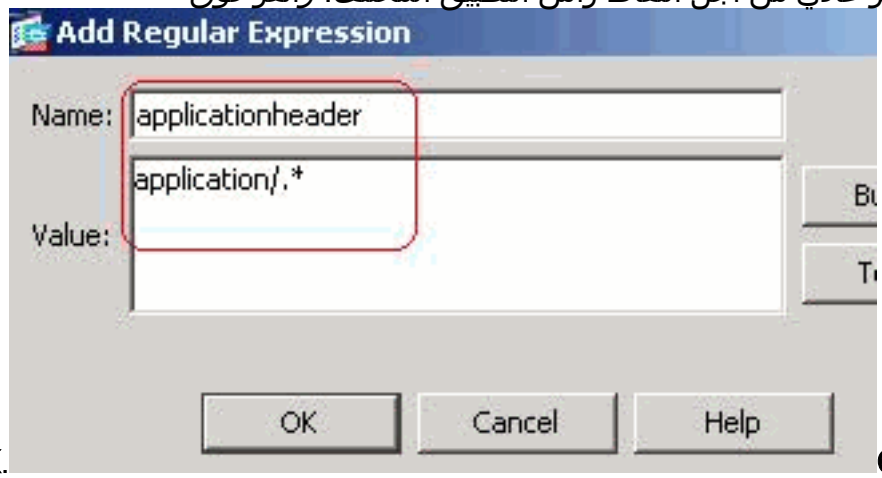
OK. قم بإنشاء **قائمة** معارف لتعبير منتظم من أجل التقاط امتدادات الملفات مثل **zip** و**tar** و**tgz**، شريطة أن يكون إصدار http الذي يتم إستخدامه من قبل مستعرض الويب إما 1.0 أو 1.1. وانقر فوق



OK. قم بإنشاء **نوع محتوى** تعبير عادي لالتقاط نوع المحتوى. وانقر فوق

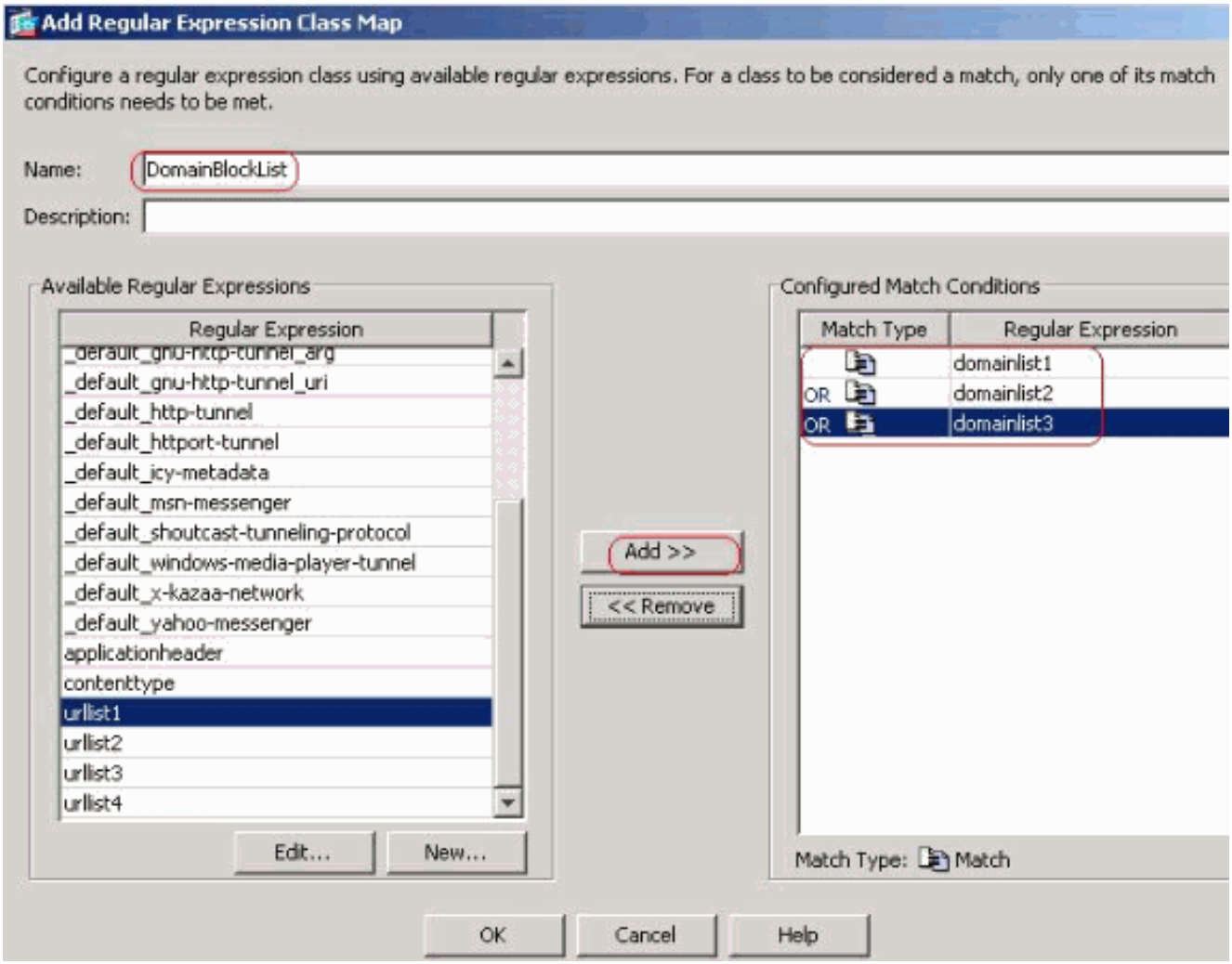


قم بإنشاء **عنوان تطبيق** تعبير عادي من أجل التقاط رأس التطبيق المختلف. وانقر فوق **OK**.

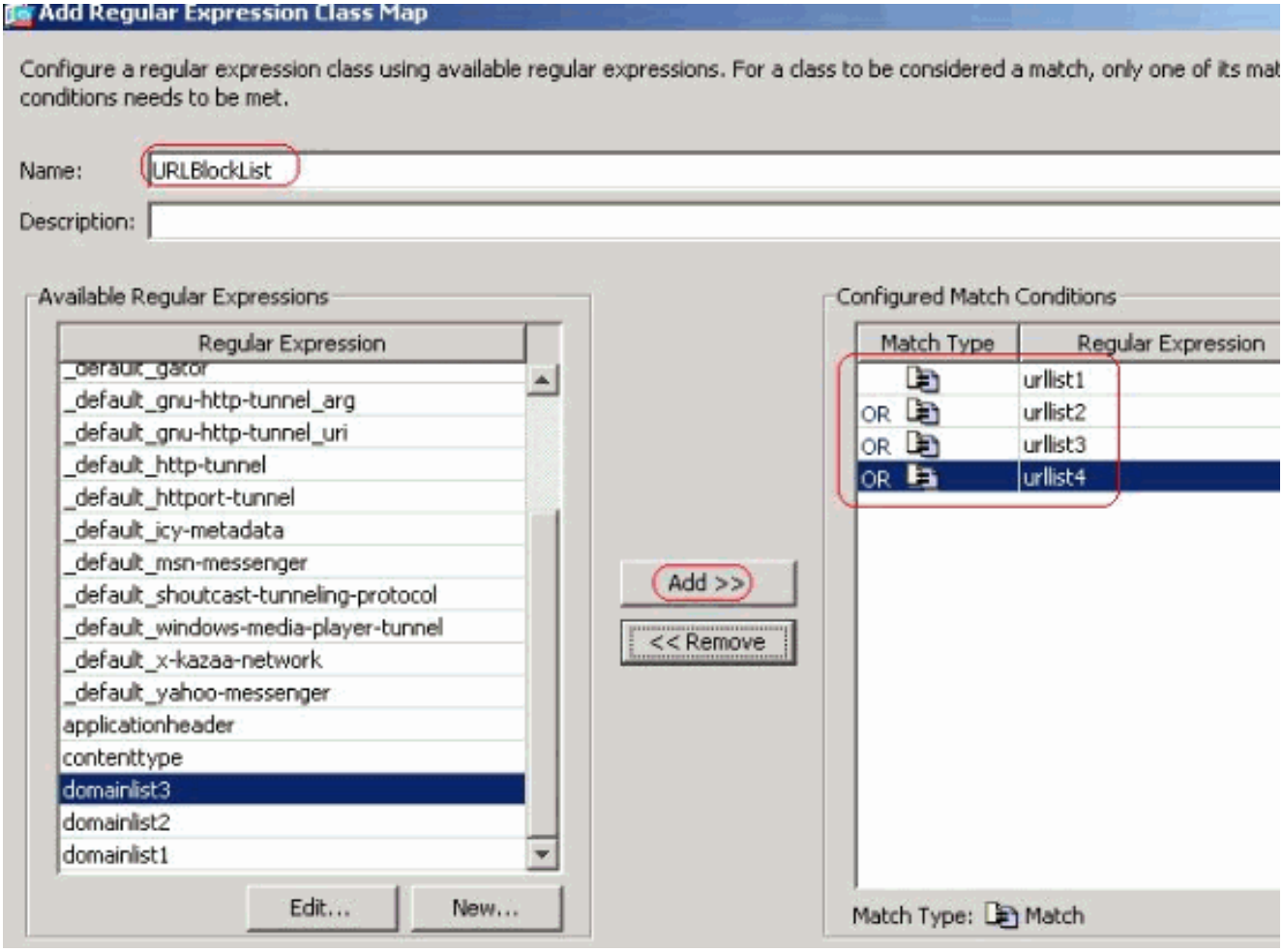


تشكيل مكافئ CLI

2. **إنشاء فئات التعبير العادي**أخترت **تشكيل > جدار حماية > كائنات > تعابير عادية** وطقطقة **يضيف** تحت علامة التبويب **فئات التعبير العادية** in order to خلقت مختلف فئات كما هو موضح.قم بإنشاء فئة تعبير عادي **DomainBlockList** لمطابقة أي من التعبيرات العادية domainList2، domainList1 و domainList3. وانقر فوق **OK**.

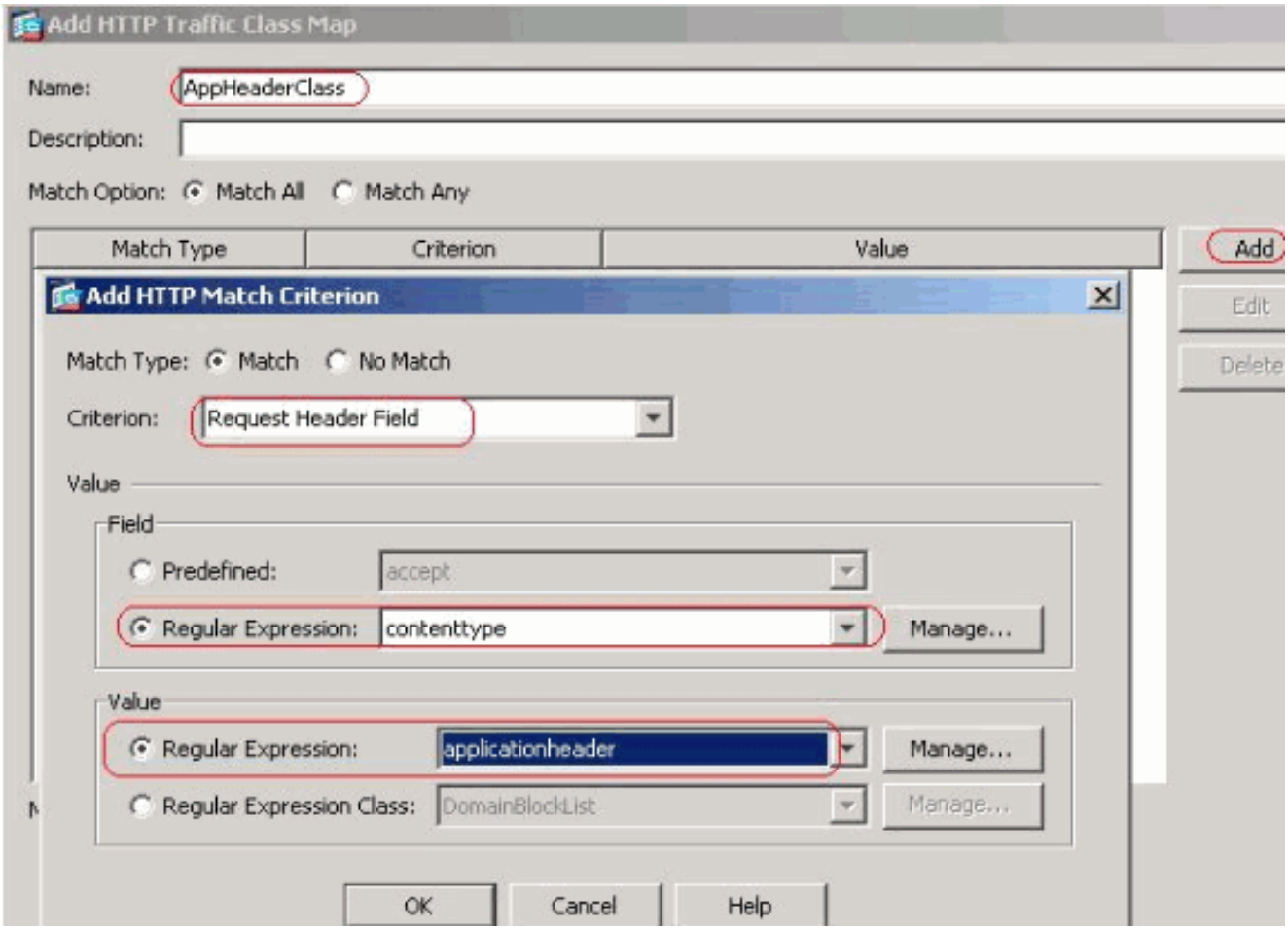


قم بإنشاء فئة تعبير عادي **URLBlockList** لمطابقة أي من التعبيرات العادية urllist3، urllist2، urllist1 و urllist4. وانقر فوق **OK**.

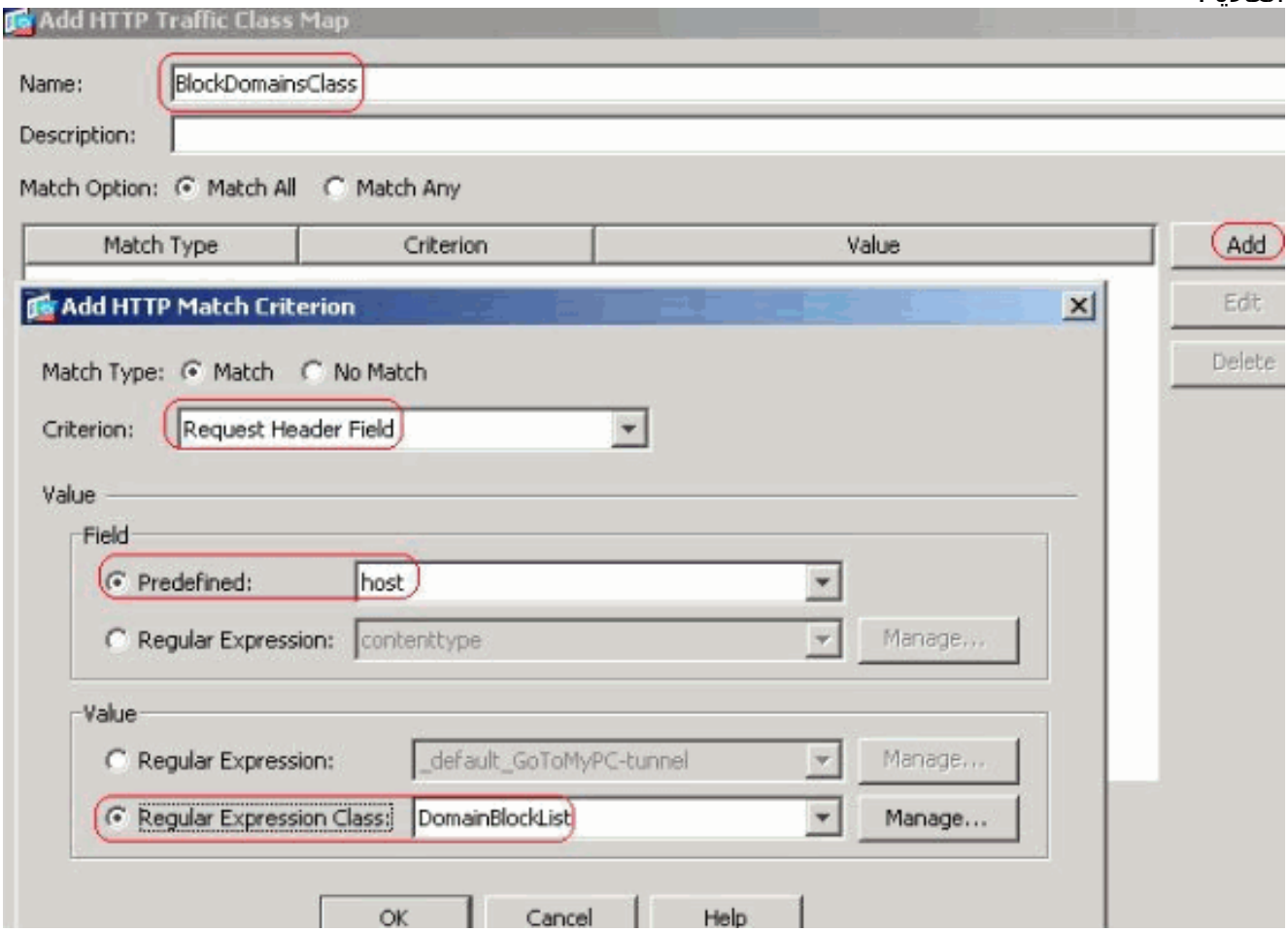


CLI تشكيل مكافئ

3. **فحص حركة المرور المحددة باستخدام خرائط الفئة**أخترت **تشكيل>جدار حماية>كائن>فئة خرائط>HTTP>إضافة** in order to خلقت صنف خريطة أن يفحص ال http حركة مرور يعين ب مختلف تعابير نظامية كما هو موضح.قم بإنشاء مخطط فئة **AppHeaderClass** لمطابقة رأس الاستجابة مع التقاط التعبيرات العادية.

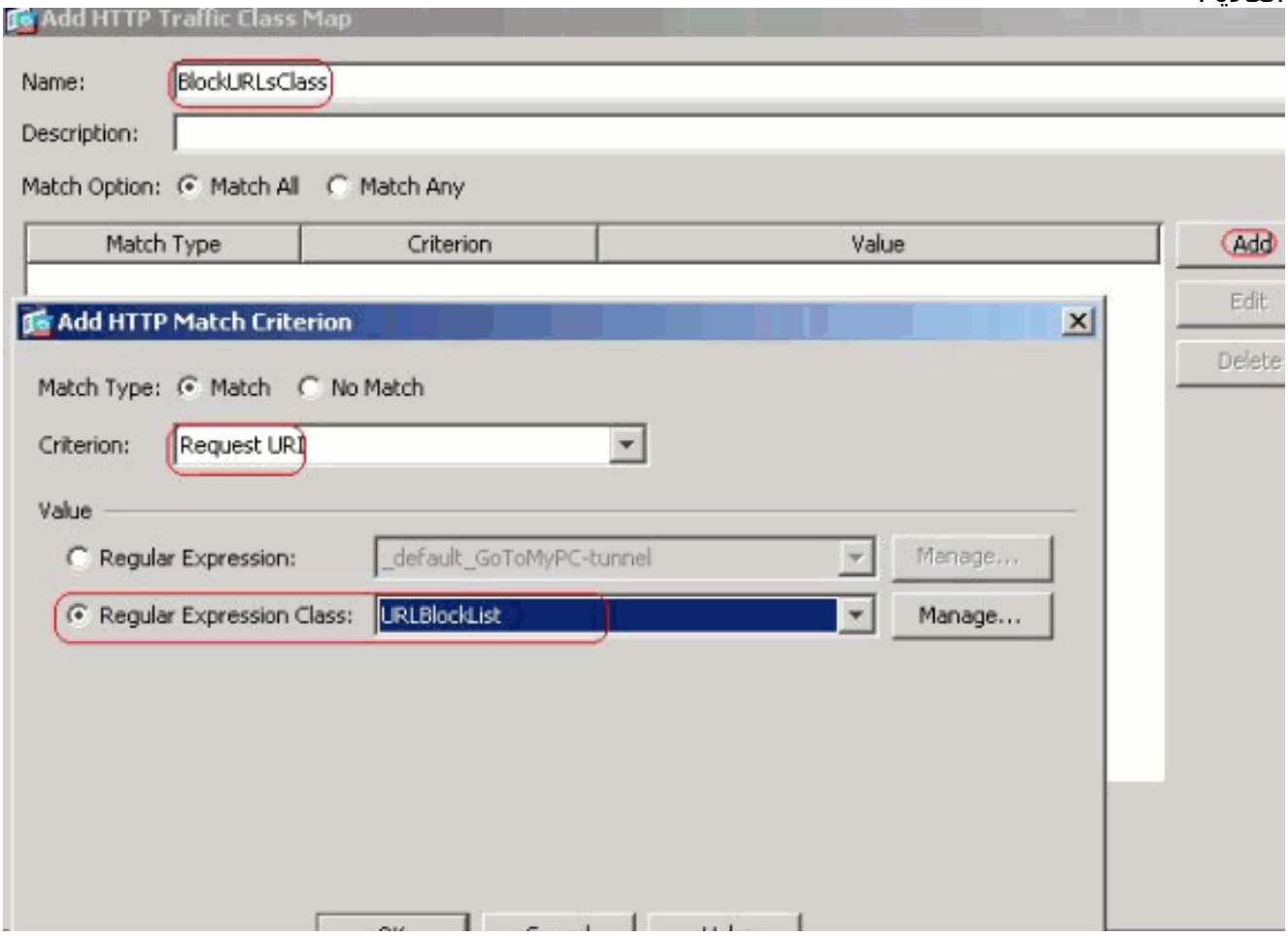


ثم انقر فوق موافققم بإنشاء **BlockDomainsClass** لمطابقة رأس الطلب مع التقاط التعبيرات العادية.



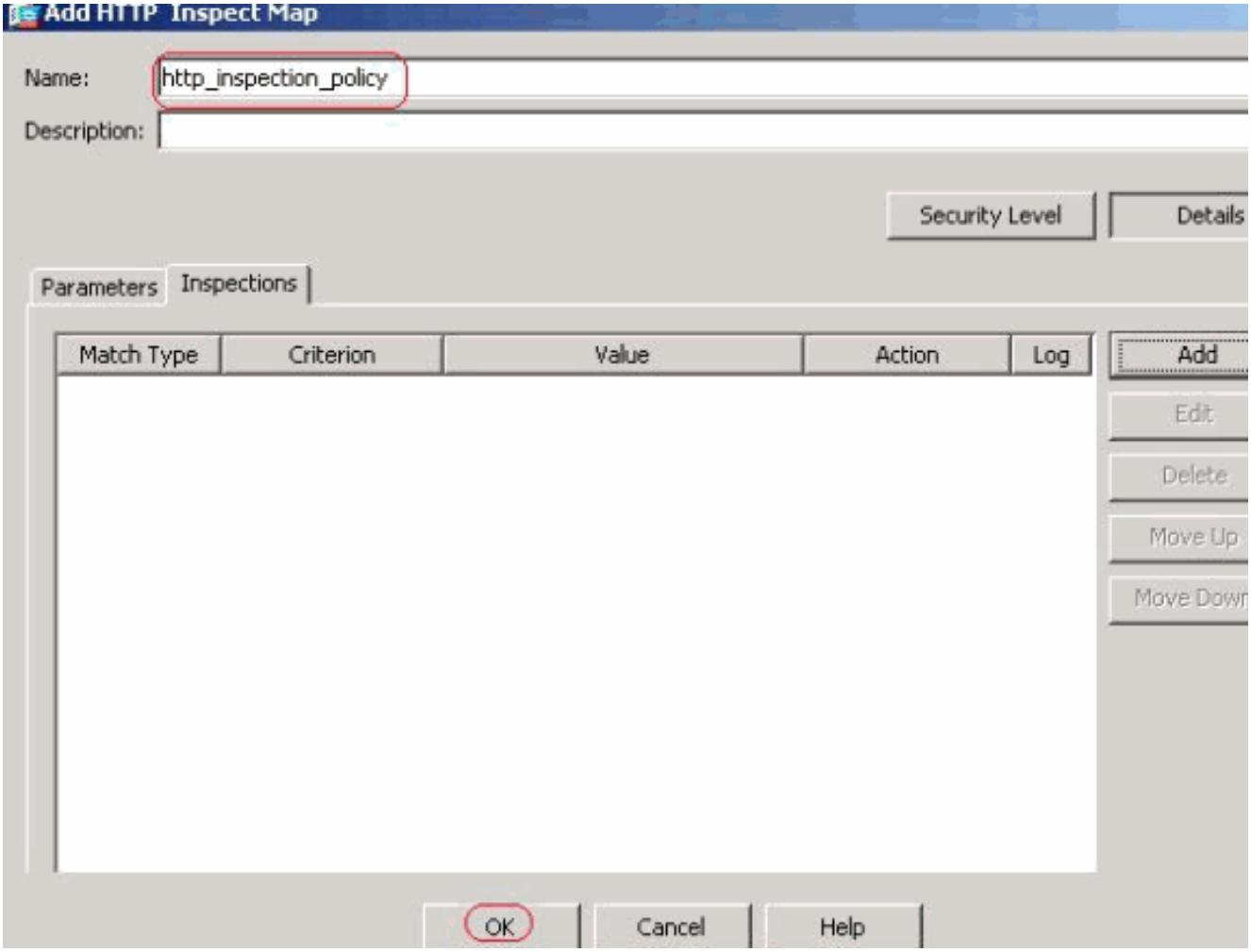
وانقر فوق **OK**.قم بإنشاء **BlockURLsClass** لتعيين الفئة لمطابقة معرف uri للطلب مع التقاط التعبيرات

العادية.

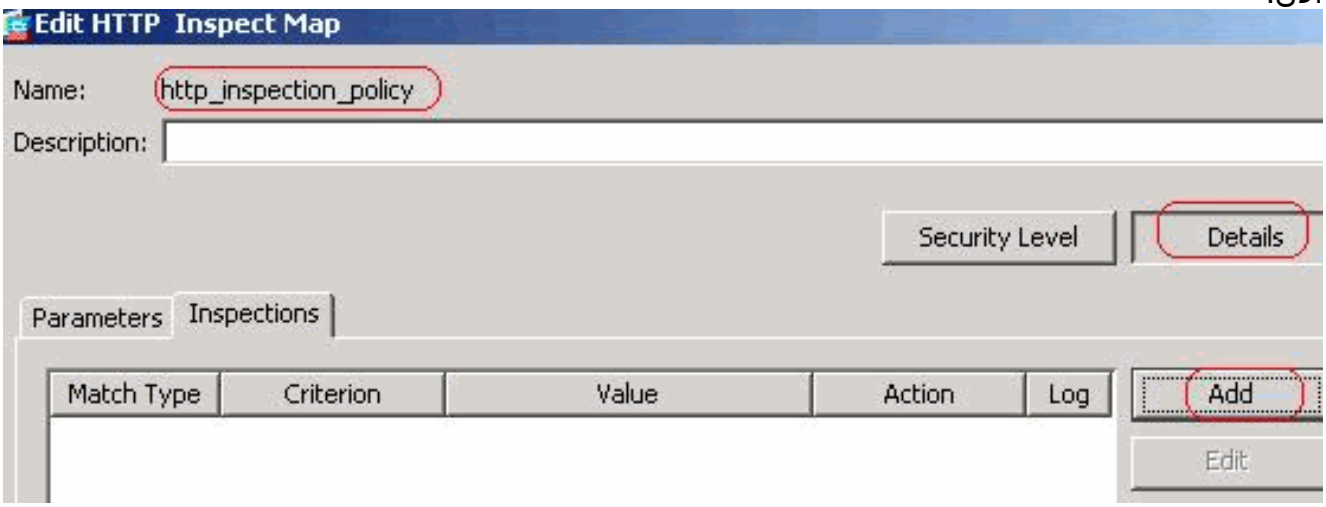


وانقر فوق OK.CLI تشكيل مكافئ:

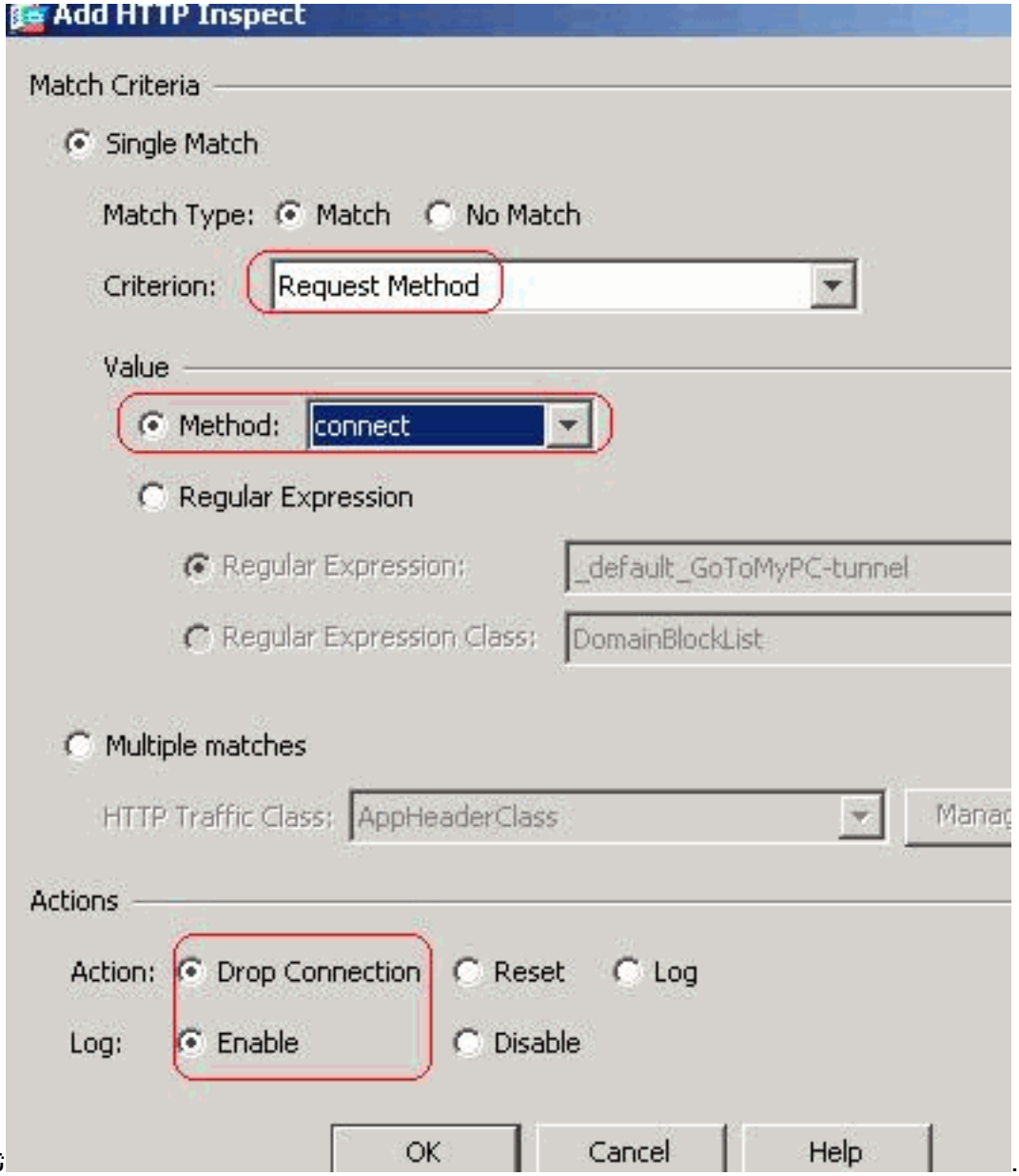
4. **تعيين الإجراءات لحركة المرور المطابقة في سياسة التفتيش**أخترت **تشكيل>جدار حماية>كائن>يفحص خرائط >** in order to HTTP خلقت **http_inspection_policy** أن يثبت الإجراء ل ال يماثل حركة مرور كما هو موضح.
وانقر فوق
.**OK**



أخترت **تشكيل > جدار حماية > كائنات > فحص الخرائط > HTTP_INSPECTION_POLICY > HTTP** **(نقرة مزدوجة)** وطقطقة **تفاصيل > إضافة** in order to ثبتت الإجراء ل مختلف الفئات يخلق حتى الآن.

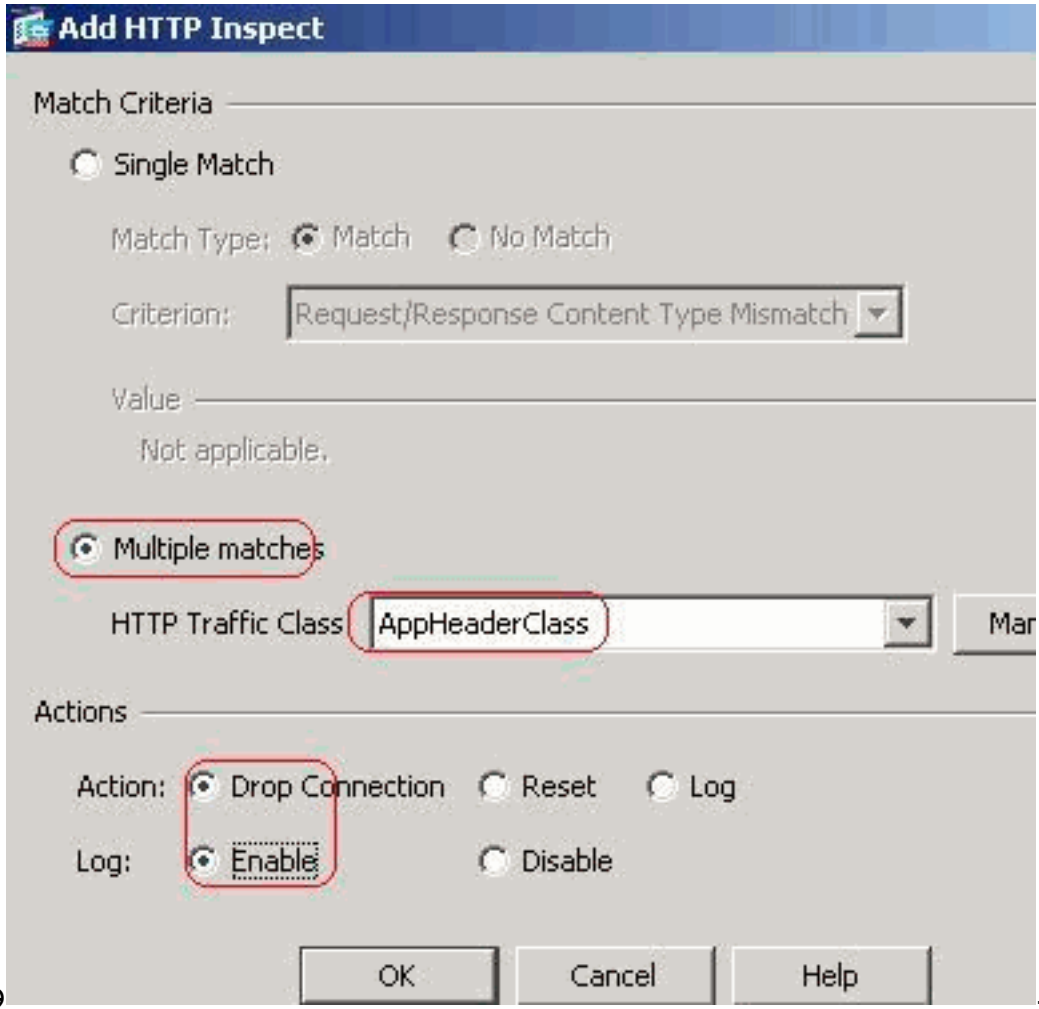


قم بتعيين الإجراء ك **اتصال إسقاط** **وقم** بتمكين تسجيل المعيار كأسلوب طلب وقيمة



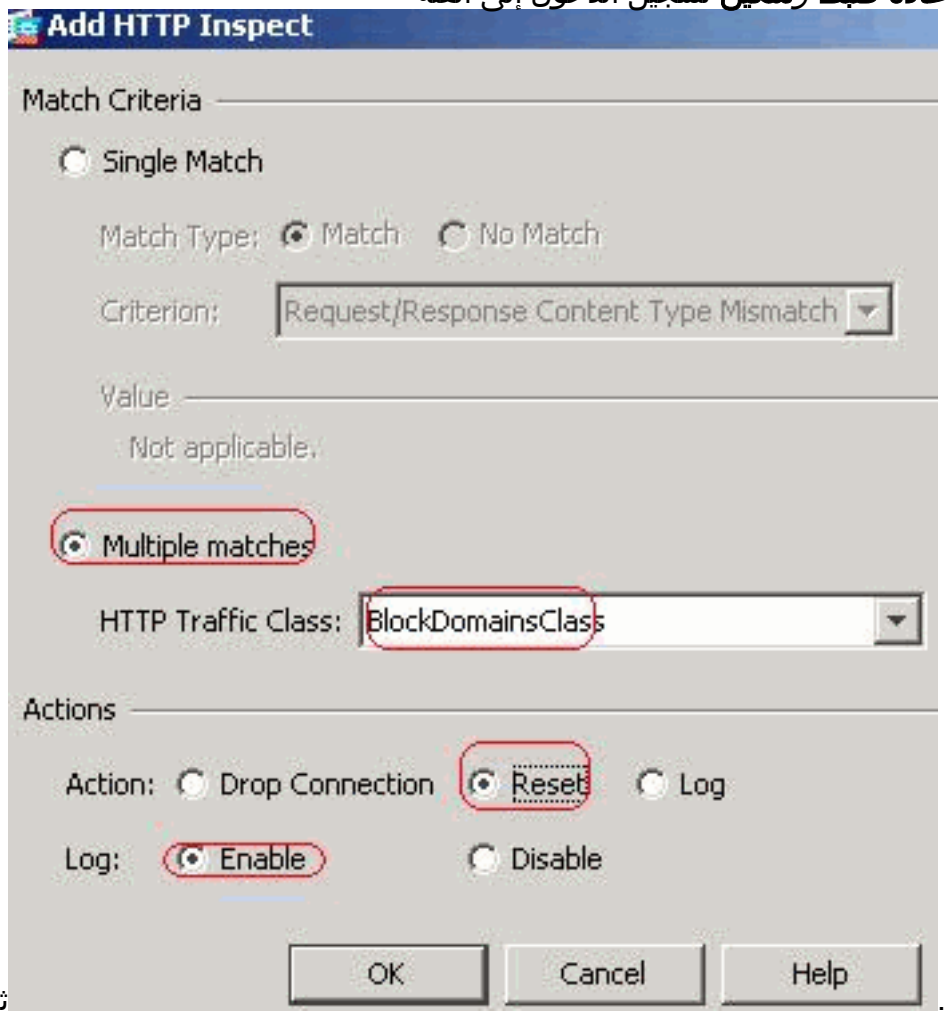
ثم انقر فوق كاتصال.

موافققم بتعيين الإجراء ك **اتصال إسقاط** و**تمكين** التسجيل للفئة **AppHeaderClass**



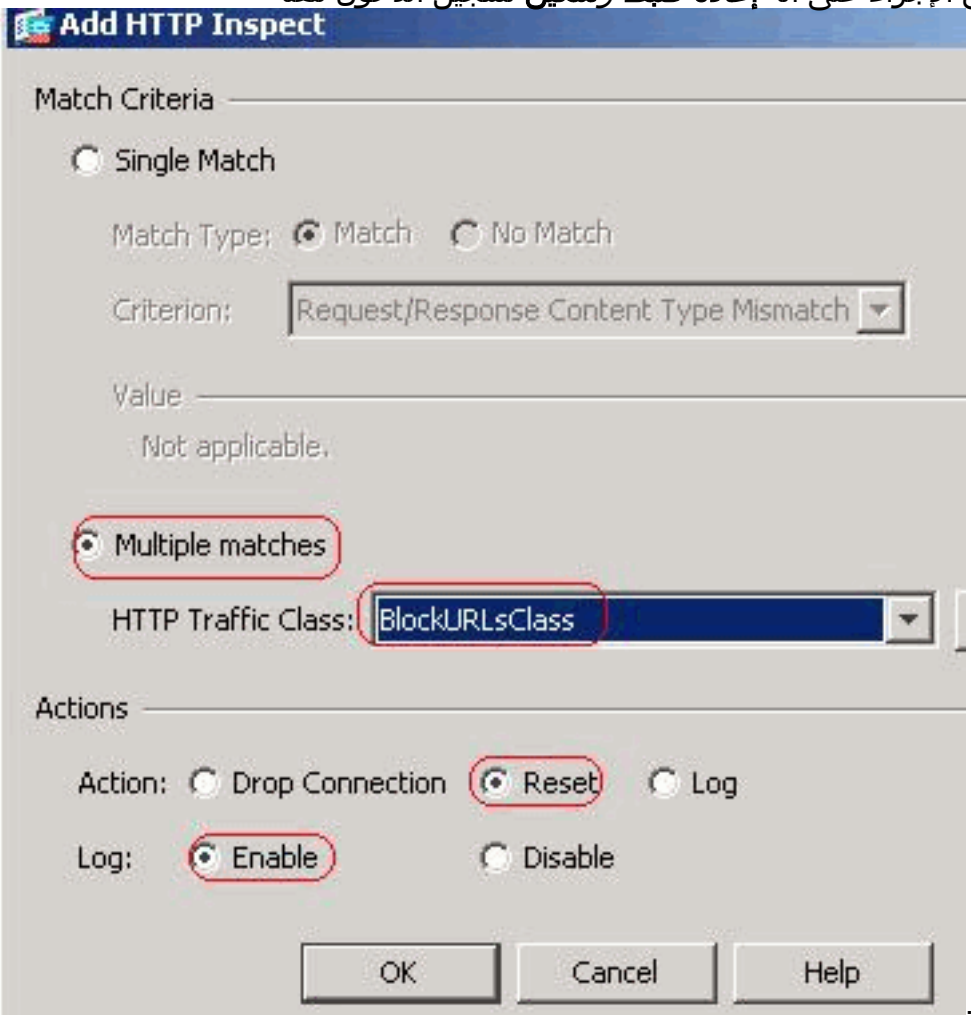
وانقر فوق **OK**.قم

بتعيين الإجراء على أنه **إعادة ضبط** و**تمكين** تسجيل الدخول إلى الفئة



ثم انقر **BlockDomainsClass**.

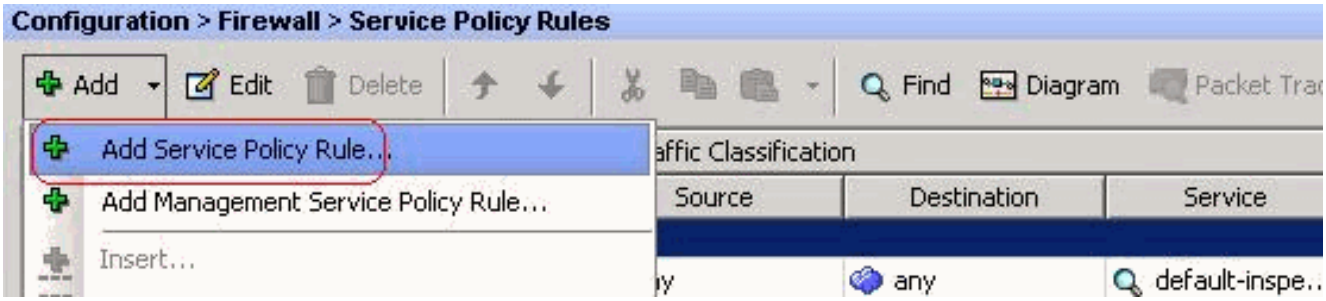
فوق موافققم بتعيين الإجراء على أنه **إعادة ضبط** و**تمكين** تسجيل الدخول للفئة



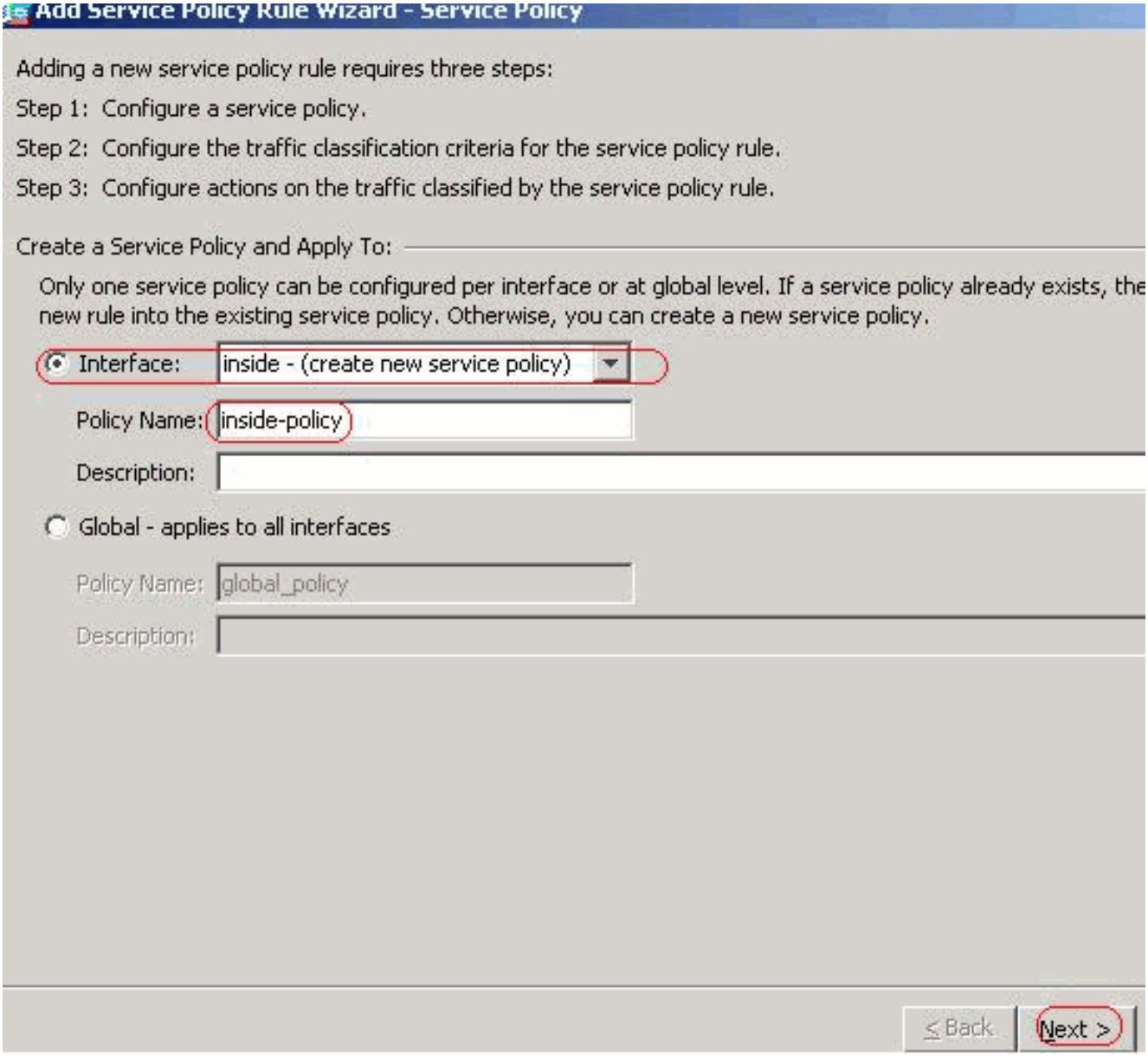
وانقر **BlockURLsClass**.

فوق OK.طقطقة **يطبق**.CLI **تشكيل مكافئ**

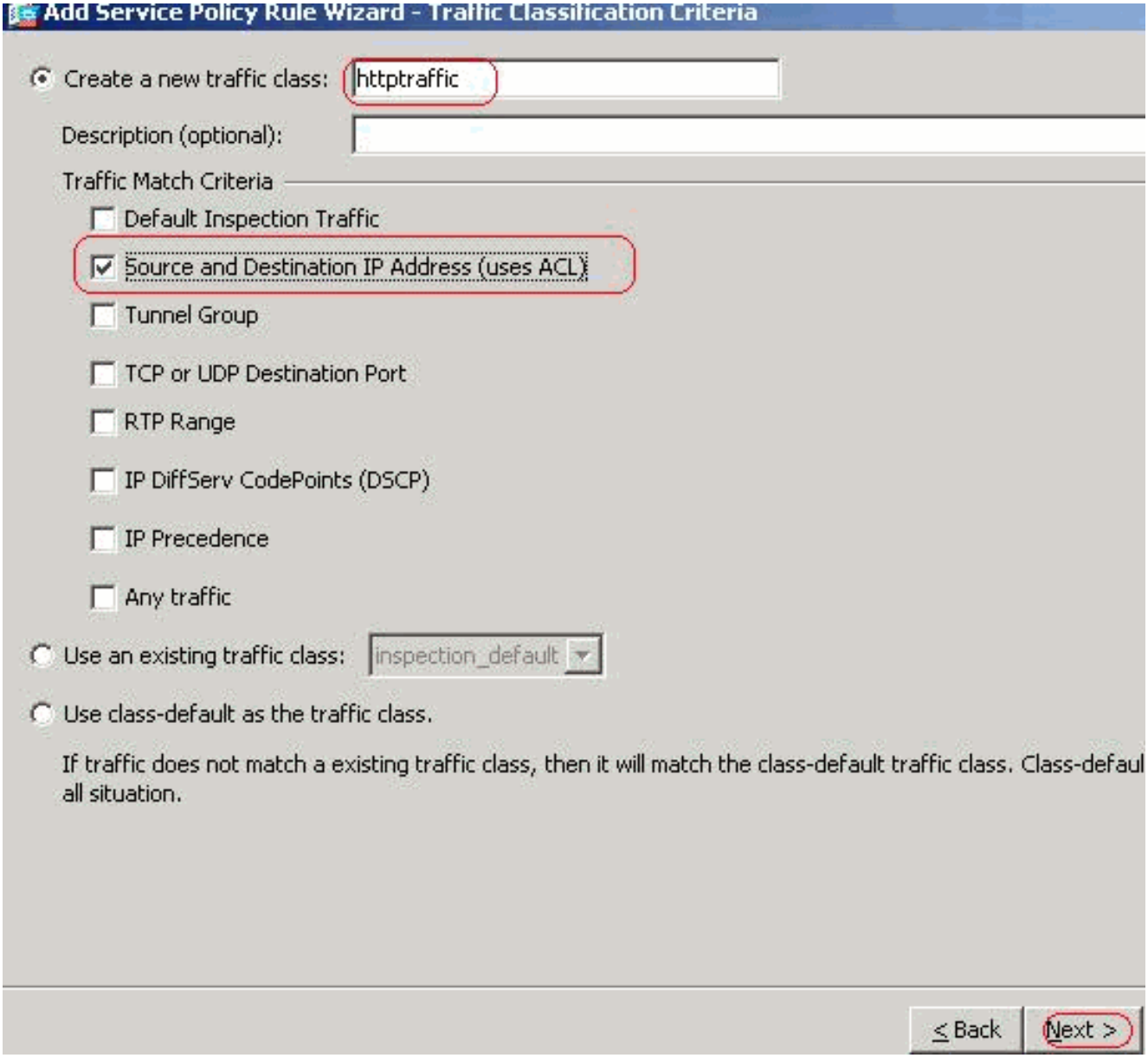
5. **تطبيق سياسة HTTP للتفتيش على الواجهة**أختر **التكوين > جدار الحماية > قواعد سياسة الخدمة > إضافة > قاعدة سياسة الخدمة**.



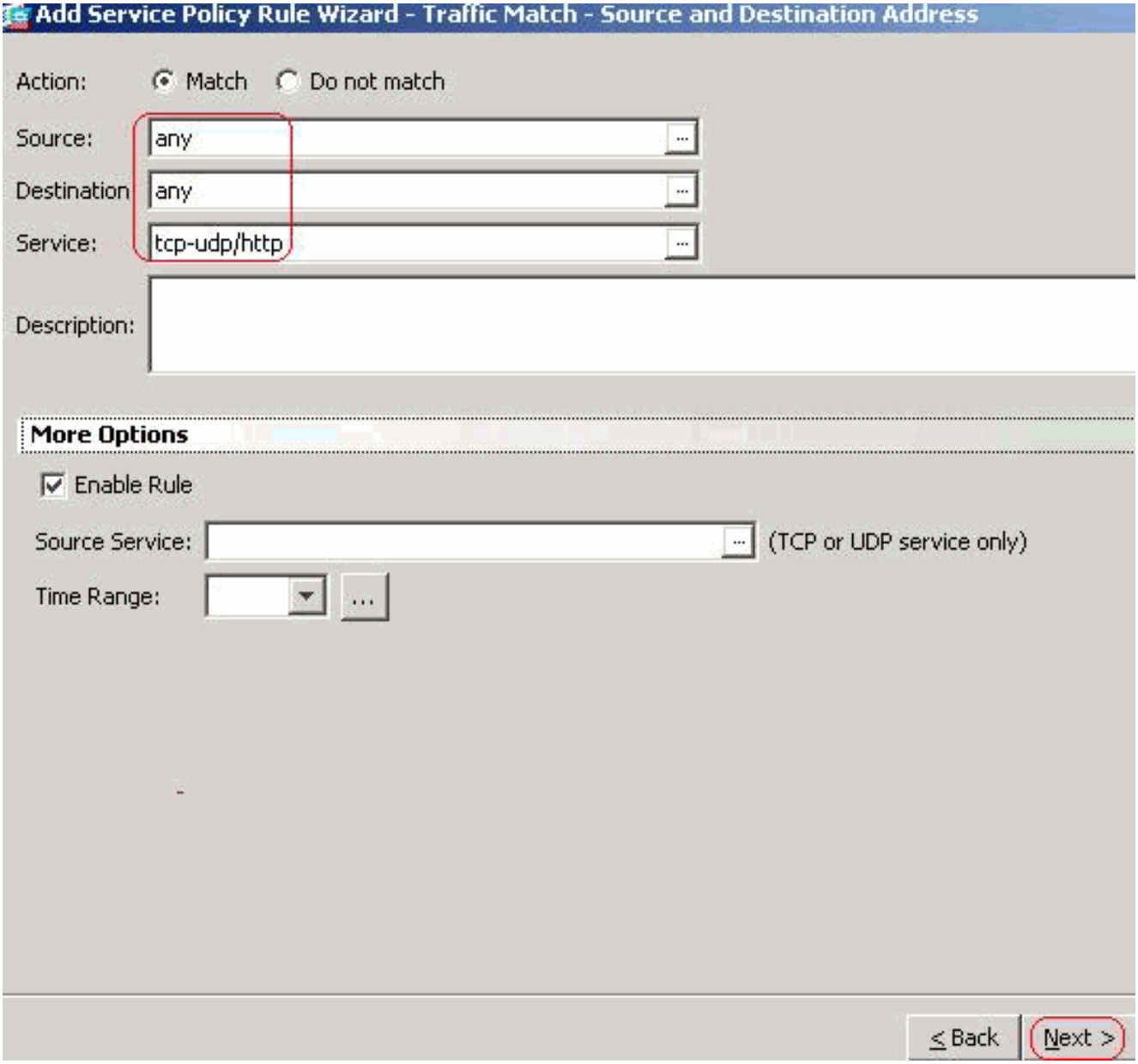
حركة مرور بيانات HTTPأخترت **القارن** لاسلكي زر مع قارن داخلي من القائمة المنسدلة ونهج إسم ك **داخلي سياسة**. انقر فوق **Next (التالي)**.

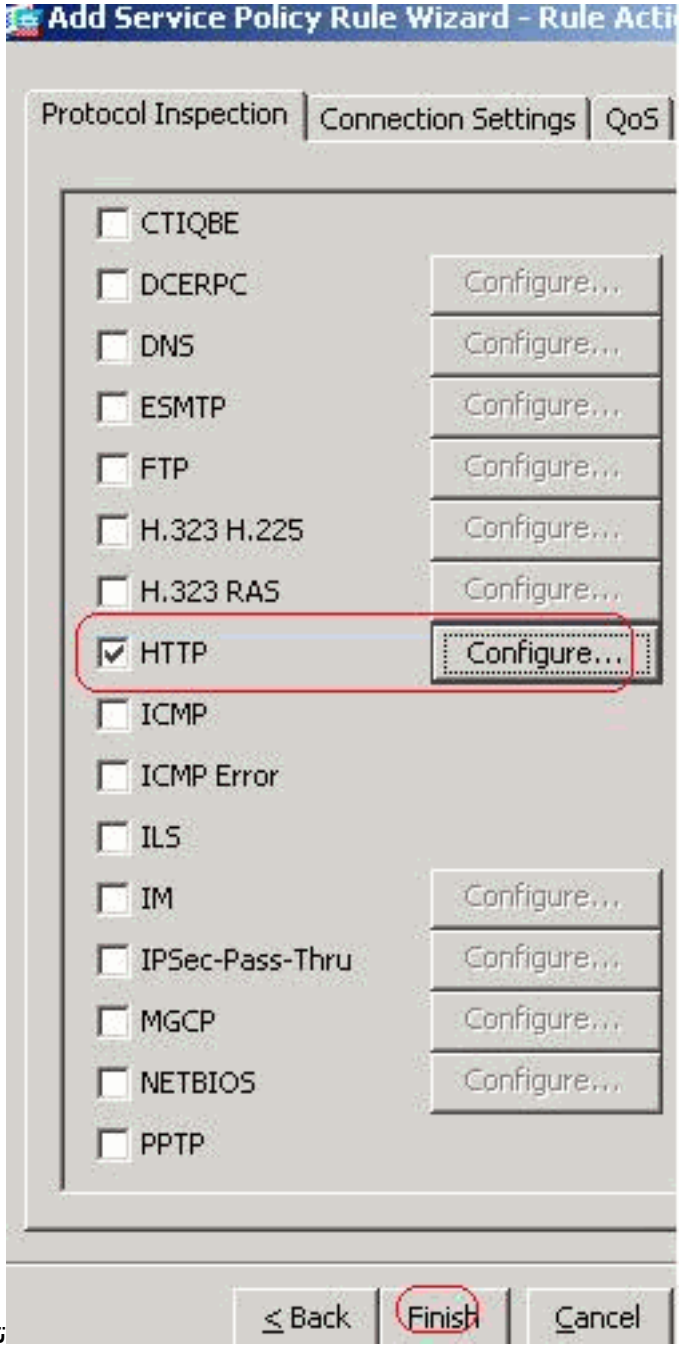


قم بإنشاء حركة مرور **http** لمخطط الفئة وحدد **عنوان IP للمصدر** والوجهة (يستخدم قائمة التحكم في الوصول). انقر فوق **Next (التالي)**.



أخترت المصدر والوجهة بما أن أي مع خدمة بما أن **tcp-udp/http**. انقر فوق **Next (التالي)**.


Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address
Action:
Match
Do not match
Source:
any
Destination
any
Service:
tcp-udp/http
Description:
More Options
Enable Rule
Source Service:
(TCP or UDP service only)
Time Range:
...
< Back
Next >

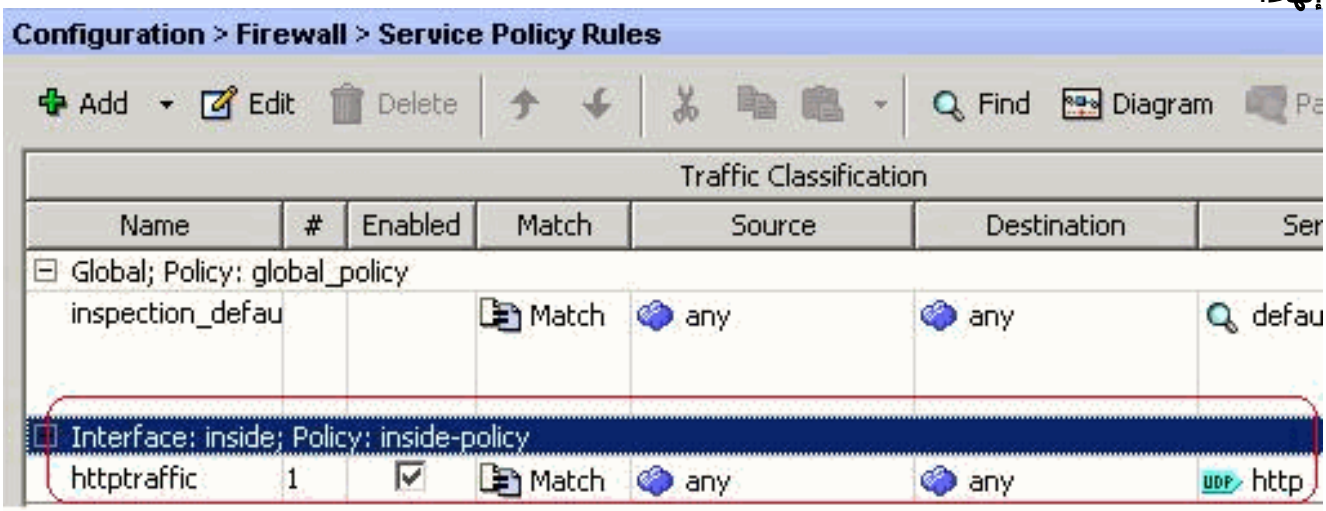


تحقق من تدقيق ال HTTP لاسلكي زر وطقطقة **يشكل**.

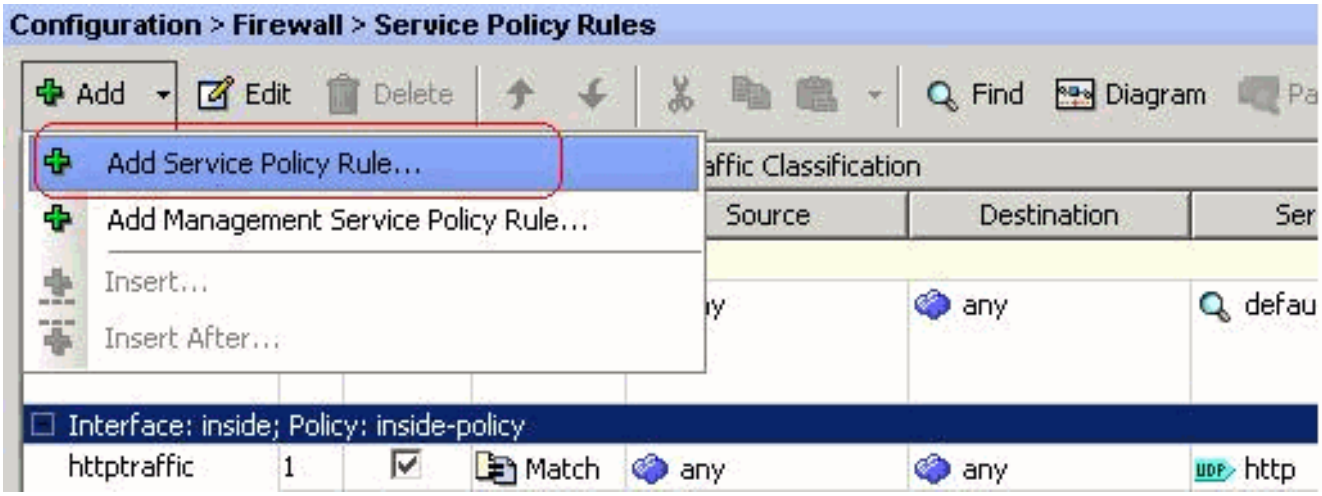
من زر الخيار **حدد خريطة فحص HTTP لعنصر التحكم في الفحص** كما هو موضح. وانقر فوق

انقر فوق **OK**.

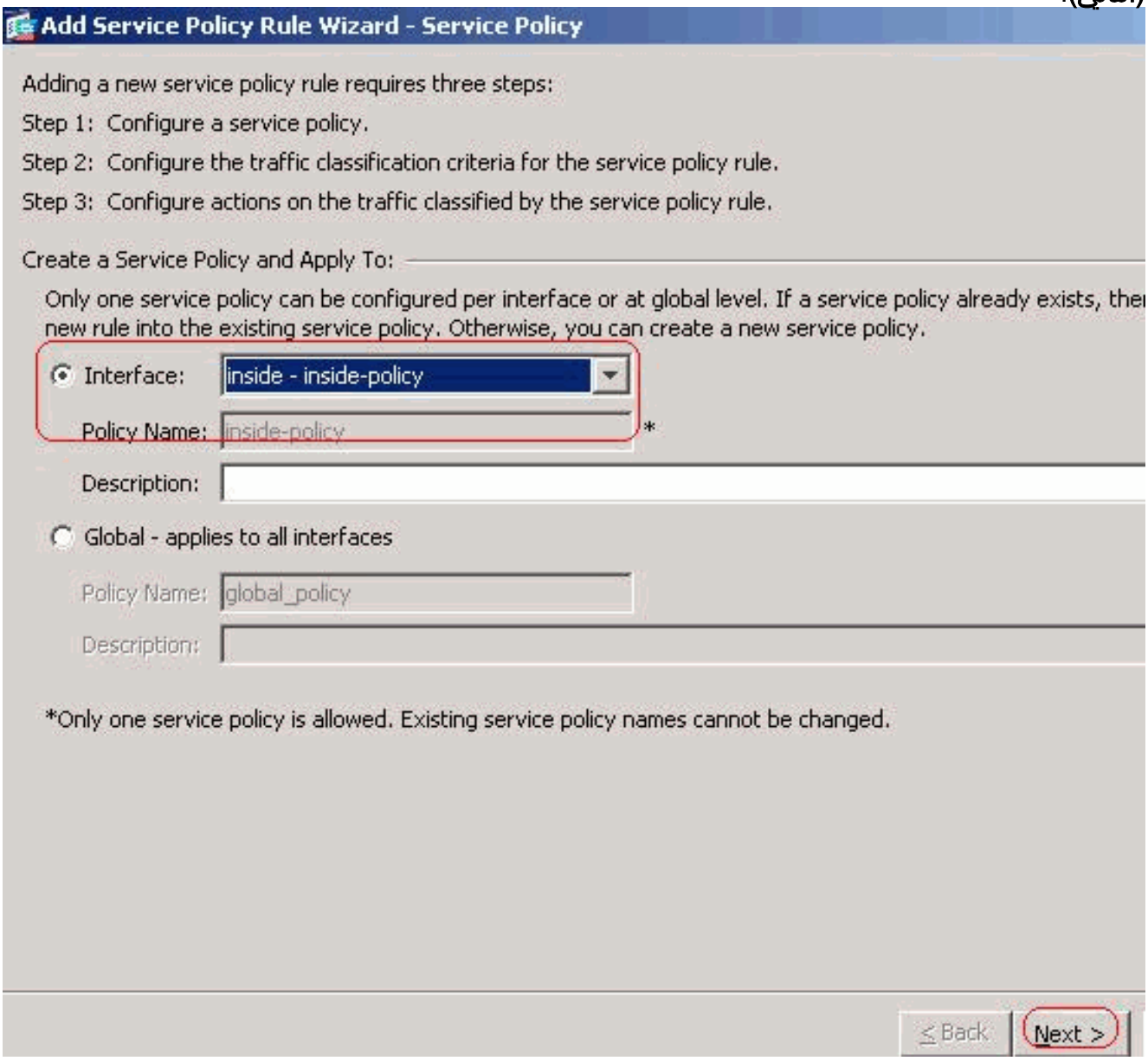
إنهاء.



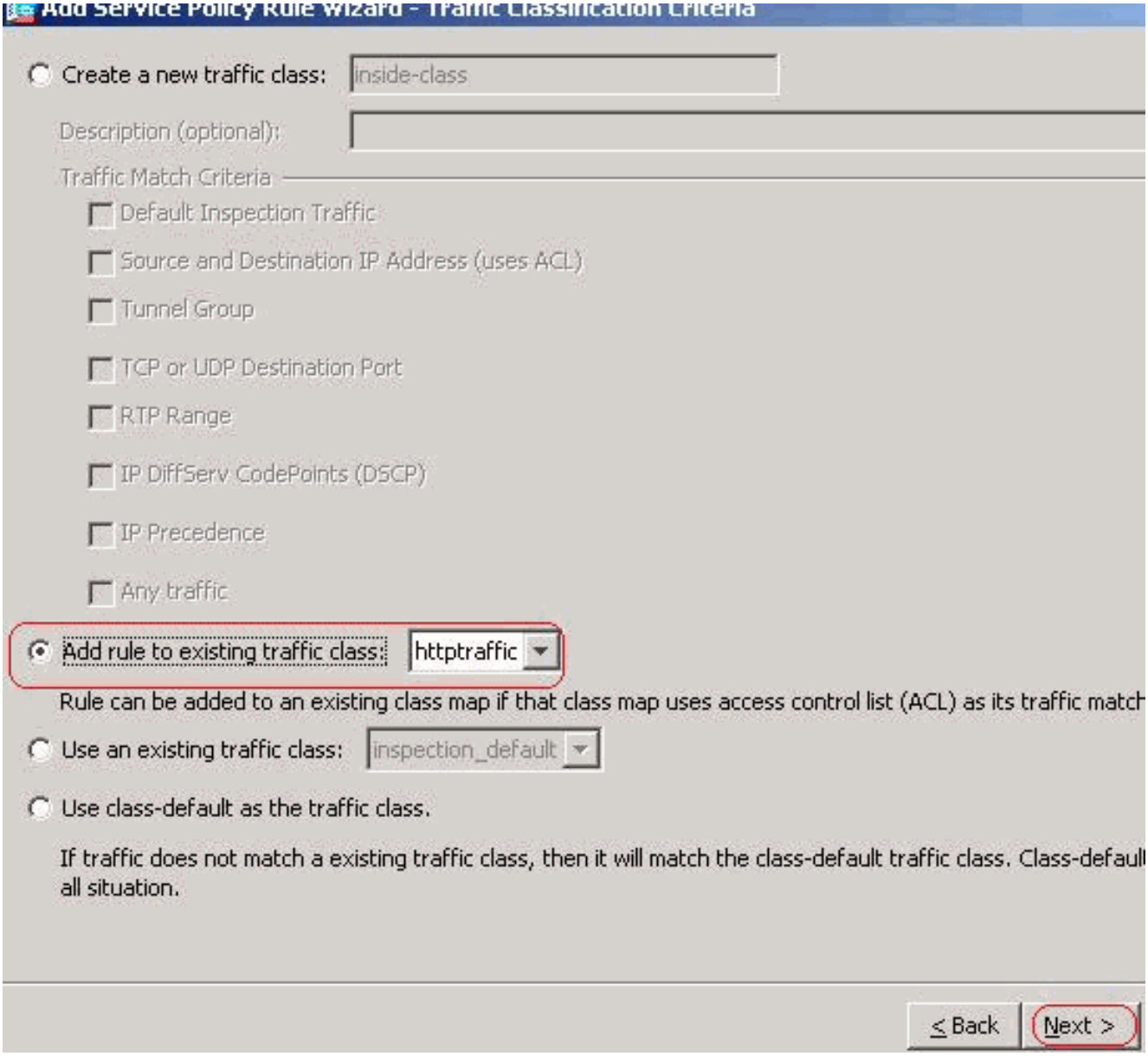
منفذ 8080 حركة مرورمرة أخرى، أختر **إضافة > قاعدة نهج الخدمة**.



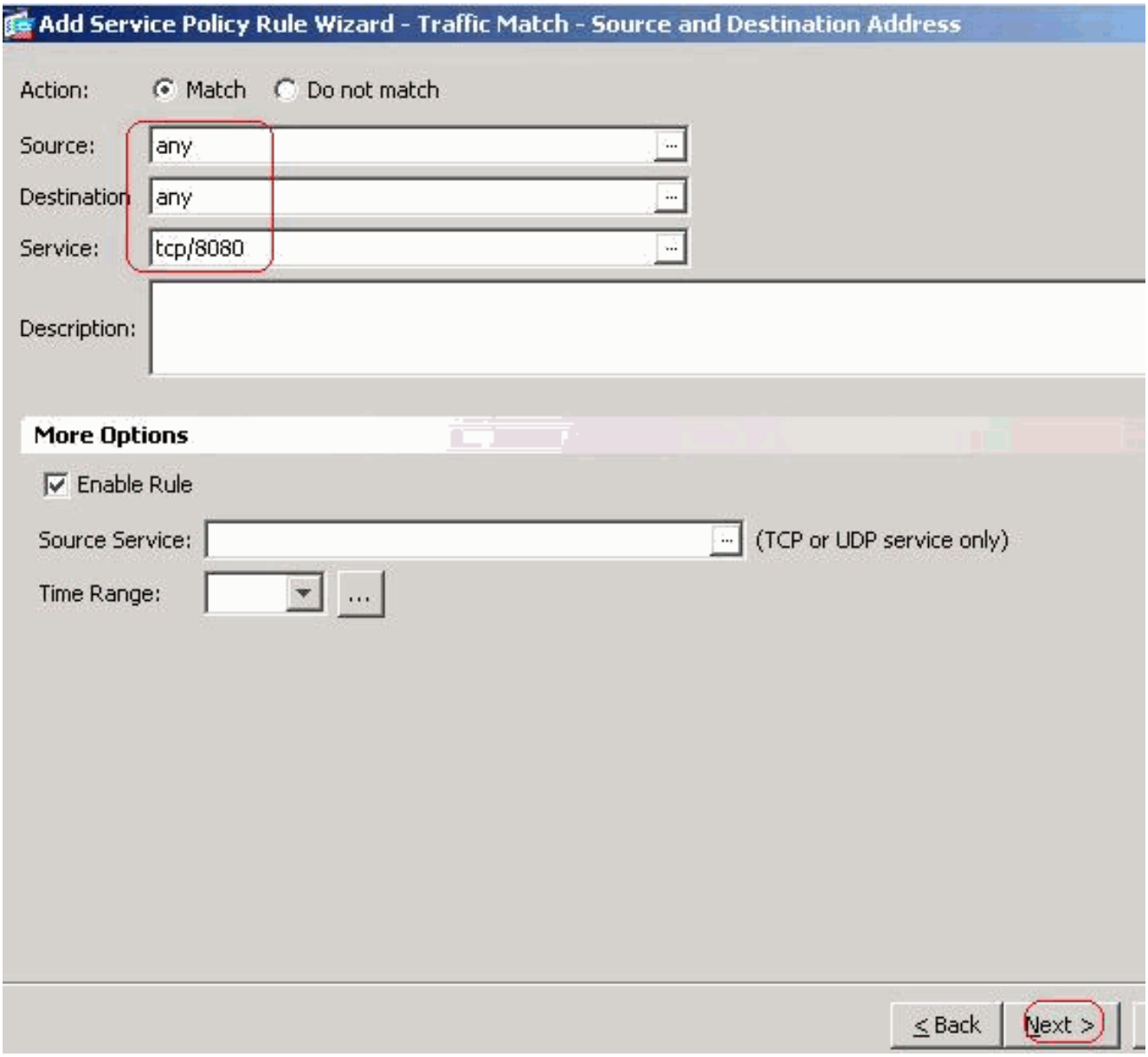
انقر فوق **Next (التالي)**.



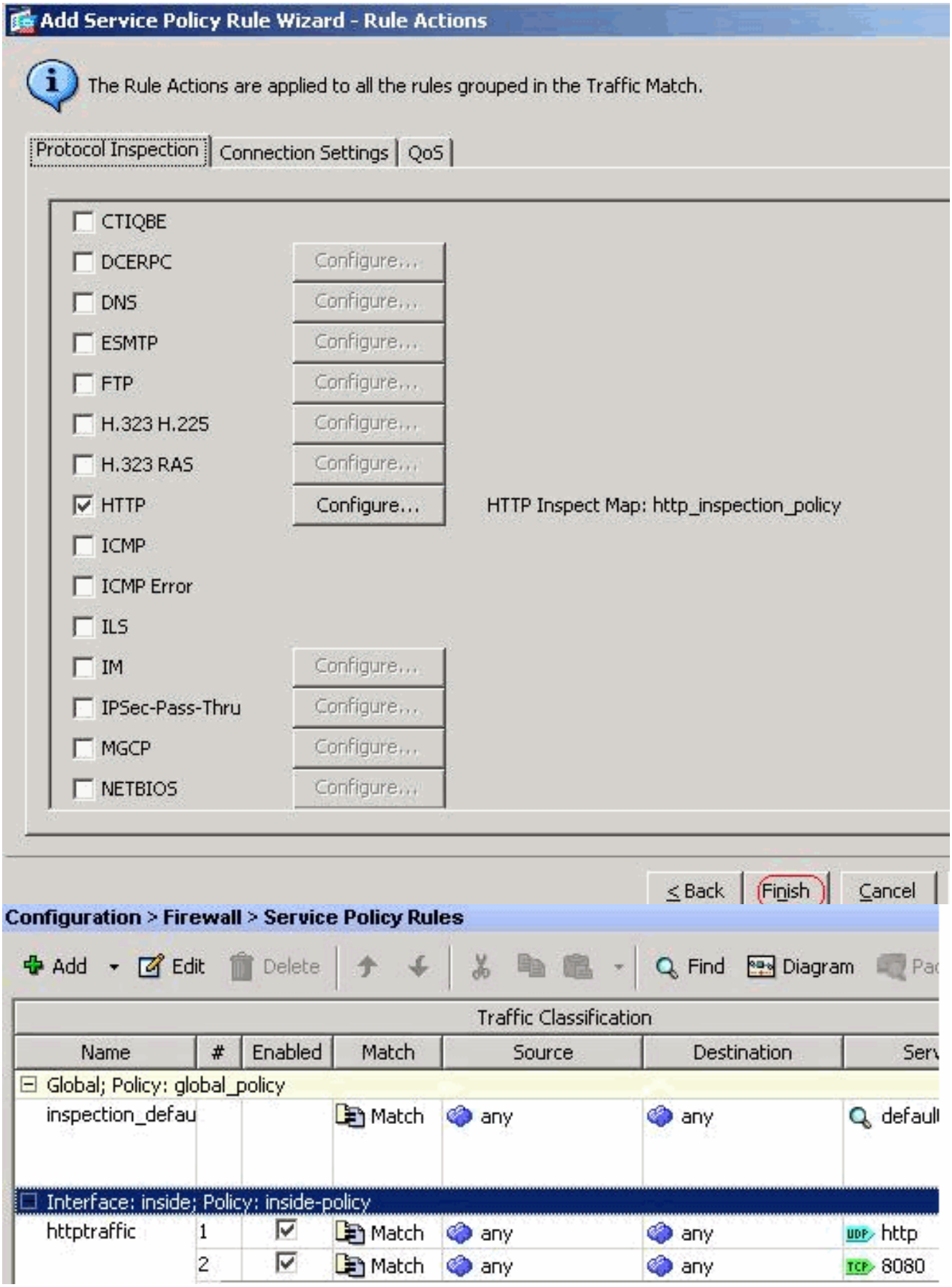
أختر زر الخيار **إضافة قاعدة إلى فئة حركة المرور الموجودة** وإختر **httpTraffic** من القائمة المنسدلة. انقر فوق **Next (التالي)**.



أخترت المصدر والوجهة أي مع TCP/8080. انقر فوق **Next (التالي)**.



انقر فوق
إنهاء.



طقطقة **يطبق**.**CLI تشكيل مكافئ**

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 running-config regex— يعرض العبارات العادية التي تم تكوينها

```
ciscoasa#show running-config regex
"[regex urllist1 ".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt]) HTTP/1.[01
"[regex urllist2 ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh]) HTTP/1.[01
"[regex urllist3 ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt]) HTTP/1.[01
"[regex urllist4 ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz]) HTTP/1.[01
                                    "regex domainlist1 "\.yahoo\.com
                                  "regex domainlist2 "\.myspace\.com
                                  "regex domainlist3 "\.youtube\.com
                                    "regex contenttype "Content-Type
                              "*./regex applicationheader "application
                                                          #ciscoasa
```

- show running-config class-map— يعرض خرائط الفئة التي تم تكوينها

```
ciscoasa#show running-config class-map
                                                                  !
                        class-map type regex match-any DomainBlockList
                                              match regex domainlist1
                                              match regex domainlist2
                                              match regex domainlist3
                    class-map type inspect http match-all BlockDomainsClass
                     match request header host regex class DomainBlockList
                              class-map type regex match-any URLBlockList
                                                 match regex urllist1
                                                 match regex urllist2
                                                 match regex urllist3
                                                 match regex urllist4
                                          class-map inspection_default
                                       match default-inspection-traffic
                          class-map type inspect http match-all AppHeaderClass
                match response header regex contenttype regex applicationheader
                                                    class-map httptraffic
                                           match access-list inside_mpc
                          class-map type inspect http match-all BlockURLsClass
                                  match request uri regex class URLBlockList
                                                                  !
                                                          #ciscoasa
```

- show running-config policy-map type فحص http—يعرض خرائط السياسة التي تفحص حركة مرور HTTP التي تم تكوينها

```
ciscoasa#show running-config policy-map type inspect http
                                                                  !
                        policy-map type inspect http http_inspection_policy
                                                       parameters
                              protocol-violation action drop-connection
                                                 class AppHeaderClass
                                                 drop-connection log
                                           match request method connect
                                                 drop-connection log
                                        class BlockDomainsClass
                                                       reset log
                                          class BlockURLsClass
                                                       reset log
                                                                  !
                                                          #ciscoasa
```

- show running-config policy-map— يعرض جميع تكوينات خريطة السياسة بالإضافة إلى تكوين خريطة السياسة الافتراضي

```
ciscoasa#show running-config policy-map
                                                                  !
                        policy-map type inspect dns preset_dns_map
```

```
                                        parameters
                                   message-length maximum 512
                          policy-map type inspect http http_inspection_policy
                                        parameters
                               protocol-violation action drop-connection
                                          class AppHeaderClass
                                          drop-connection log
                                     match request method connect
                                          drop-connection log
                                      class BlockDomainsClass
                                                reset log
                                        class BlockURLsClass
                                                reset log
                                    policy-map global_policy
                                   class inspection_default
                                 inspect dns preset_dns_map
                                              inspect ftp
                                        inspect h323 h225
                                         inspect h323 ras
                                          inspect netbios
                                              inspect rsh
                                            inspect rtsp
                                           inspect skinny
                                            inspect esmtp
                                           inspect sqlnet
                                           inspect sunrpc
                                             inspect tftp
                                              inspect sip
                                            inspect xdmcp
                                    policy-map inside-policy
                                         class httptraffic
                                inspect http http_inspection_policy
                                                        !
                                                #ciscoasa
```

- **show running-config service-policy**—يعرض جميع تكوينات نهج الخدمة الجاري تشغيلها حاليا

```
ciscoasa#show running-config service-policy
                service-policy global_policy global
           service-policy inside-policy interface inside
```

- **show running-config access-list**— يعرض تكوين قائمة الوصول التي يتم تشغيلها على جهاز الأمان

```
ciscoasa#show running-config access-list
access-list inside_mpc extended permit tcp any any eq www

access-list inside_mpc extended permit tcp any any eq 8080
                                                #ciscoasa
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug http**— يعرض رسائل تصحيح الأخطاء لحركة مرور HTTP

معلومات ذات صلة

- دعم أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- دعم مدير أجهزة حلول الأمان المعدلة (ASDM) من Cisco

- دعم أجهزة الأمان Cisco PIX 500 Series Security Appliances
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- 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).