ASA/PIX 8.x: السماح/حظر مواقع FTP باستخدام تعبيرات عادية مع مثال تكوين MPF

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين أجهزة الأمان Cisco ASA/PIX 8.x التي تستخدم تعبيرات منتظمة مع إطار عمل السياسة النمطية (MPF) لحظر مواقع FTP معينة أو السماح بها حسب اسم الخادم.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن جهاز أمان Cisco تم تكوينه ويعمل بشكل صحيح.

المكونات المستخدمة

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

- 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.

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 والطبقة 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.) تحديد الإجراءات الخاصة لحركة مرور فحص التطبيق. راجع تكوين الإجراءات الخاصة لتفتيش التطبيقات للحصول على مزيد من المعلومات.
3. تطبيق عمليات على حركة مرور الطبقة 3 والطبقة 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 النص. 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 علامات السؤال (؟) أو علامات التبويب. على سبيل المثال، اكتب g**Ctrl+V]**d لإدخال **g؟d** في التكوين.

in order to خلقت تعبير عادي، استعملت **ال regex** أمر. بالإضافة إلى أن أمر **regex** يمكن إستخدامه للميزات المختلفة التي تتطلب مطابقة النص. على سبيل المثال، يمكنك تكوين الإجراءات الخاصة لفحص التطبيق باستخدام

ميزة "حالة إدارة الأجهزة (MPF)" التي تستخدم خريطة سياسة فحص. راجع أمر **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 أمر **مطابقة** أو أكثر، أو يمكنك إستخدام أوامر **المطابقة** 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 dogg onit.
(exp)	ضغط جزئي	يفصل التعبير الجزئي الحروف عن الحروف المحيطة، بحيث يمكن

		ك إستخدام حروف أولية أخرى على التعبير الجزئي. على سبيل المثال، تطابق d(o|ag(مع الكلب والدا غ، 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 abxyxyxyz.
|	تناوب	يطابق أيا من التعبيرين اللذين يفصلهما. على سبيل المثال، يطابق **الكلب|القط** الكلب أو القط.
؟	علامة الاستفهام	قيمة كمية تشير إلى وجود 0 أو 1 من التعبير السابق. على سبيل المثال، إما **أن** تتطابق مع **قيمة** العرض أو أن تخسر. **ملاحظة:** يجب إدخال **Ctrl+**

		V ثم علامة الاستفهام وإلا سيتم إستدعاء دالة المساعدة.
*	نجمية	كمي يشير إلى أن هناك 0، 1، أو أي رقم 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 الضار	مطابقة حرف واحد غير موجود داخل الأقواس.

		على سبيل المثال، **[^abc]** 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 شرط ة (-) حرف ي فقط إذا كان هو الحر ف الأخير أو الأول داخل الأقوا س: **[abc-]** أو **[-abc]**.
""	علامات الاقتبا س	يحافظ على المسا فات الخلفي ة أو المسا فات البادئة في السل سلة. على سبيل المثال ، **الاختبا ر"** يحتفظ بمسا فة المسا فة بين السط ور عند البحث عن تطابـ

		ق.
^	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.

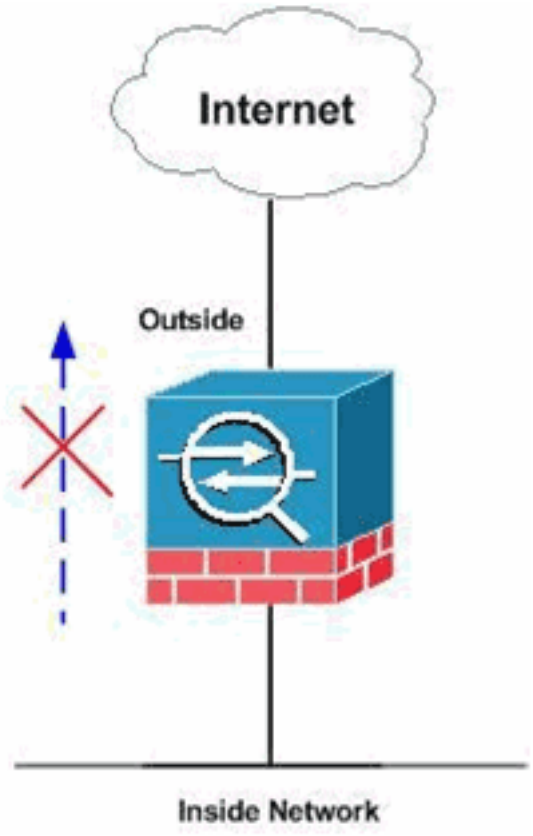
التكوين

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:



ملاحظة: يسمح بمواقع FTP المحددة أو يتم حظرها باستخدام تعبيرات عادية.

التكوينات

يستخدم هذا المستند التكوينات التالية:

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

تكوين ASA CLI

تكوين ASA CLI

```
ciscoasa#show run
Saved :
:
(ASA Version 8.0(4
!
hostname ciscoasa
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.66.79.86 255.255.255.224
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.238.26.129 255.255.255.248
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
Write regular expression (regex) to match the FTP ---!
site you want !--- to access. NOTE: The regular
expression written below must match !--- the response
220 received from the server. This can be different !---
than the URL entered into the browser. For example, !---
FTP Response: 220 g1u0103c.austin.hp.com


"[regex FTP_SITE1 "([0-9A-Za-z])*[Hh][Pp]\.[Cc][Oo][Mm
regex FTP_SITE2 "([0-9A-Za-z])* CISCO SYSTEMS ([0-9A-Za-
"*([z


NOTE: The regular expression will be checked ---!
against every line !--- in the Response 220 statement
(which means if the FTP server !--- responds with
multiple lines, the connection will be denied if !---
.(there is no match on any one line


boot system disk0:/asa804-k8.bin
ftp mode passive
pager lines 24
logging enable
logging timestamp
logging buffered debugging
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-61557.bin
no asdm history enable
arp timeout 14400

global (outside) 1 interface
```

```
                                nat (inside) 1 0.0.0.0 0.0.0.0
                    route outside 0.0.0.0 0.0.0.0 10.66.79.65 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 sip-provisional-media 0:02:00 uauth 0:05:00
                                                    absolute
              dynamic-access-policy-record DfltAccessPolicy

                                         http server enable
                                  http 0.0.0.0 0.0.0.0 inside
                                 http 0.0.0.0 0.0.0.0 outside
                                      no snmp-server location
                                      no snmp-server contact
         snmp-server enable traps snmp authentication linkup
                                        linkdown coldstart

                                           telnet timeout 5
                                           ssh scopy enable
                                              ssh timeout 5
                                         console timeout 0
                                    management-access inside
                                threat-detection basic-threat
                    threat-detection statistics access-list
                no threat-detection statistics tcp-intercept


                    class-map type regex match-any FTP_SITES
                                         match regex FTP_SITE1
                                         match regex FTP_SITE2

    Class map created in order to match the server names ! !
         of FTP sites to be blocked by regex. class-map type
                           inspect ftp match-all FTP_class_map
                      match not server regex class FTP_SITES

        Write an FTP inspect class map and match based on !
      server !--- names, user name, FTP commands, and so on.
      Note that this !--- example allows the sites specified
     with the regex command !--- since it uses the match not
      command. If you need to block !--- specific FTP sites,
             .use the match command without the  not  option


                                 class-map inspection_default
                           match default-inspection-traffic

                    policy-map type inspect dns preset_dns_map
                                                 parameters
                                 message-length maximum 512

              policy-map type inspect ftp FTP_INSPECT_POLICY
                                                 parameters
                                       class FTP_class_map
                                                 reset log

    Policy map created in order to define the actions !--- !
       such as drop, reset, or log. policy-map global_policy
         class inspection_default inspect dns preset_dns_map
```

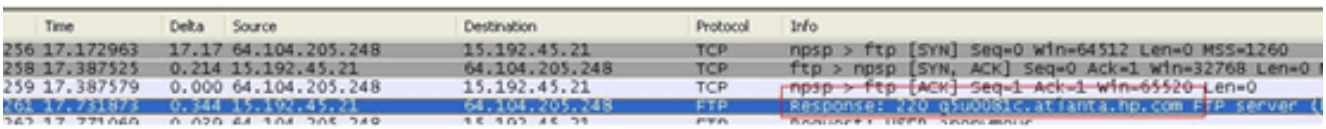
```
    inspect h323 h225 inspect h323 ras inspect netbios
  inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
        inspect xdmcp inspect icmp inspect ftp strict
                                        FTP_INSPECT_POLICY

 The FTP inspection is specified with strict option ---!
    !--- followed by the name of policy. service-policy
          global_policy global prompt hostname context
 Cryptochecksum:40cefb1189e8c9492ed7129c7577c477 : end
```

ASA تشكيل x.8 مع ASDM 6.x

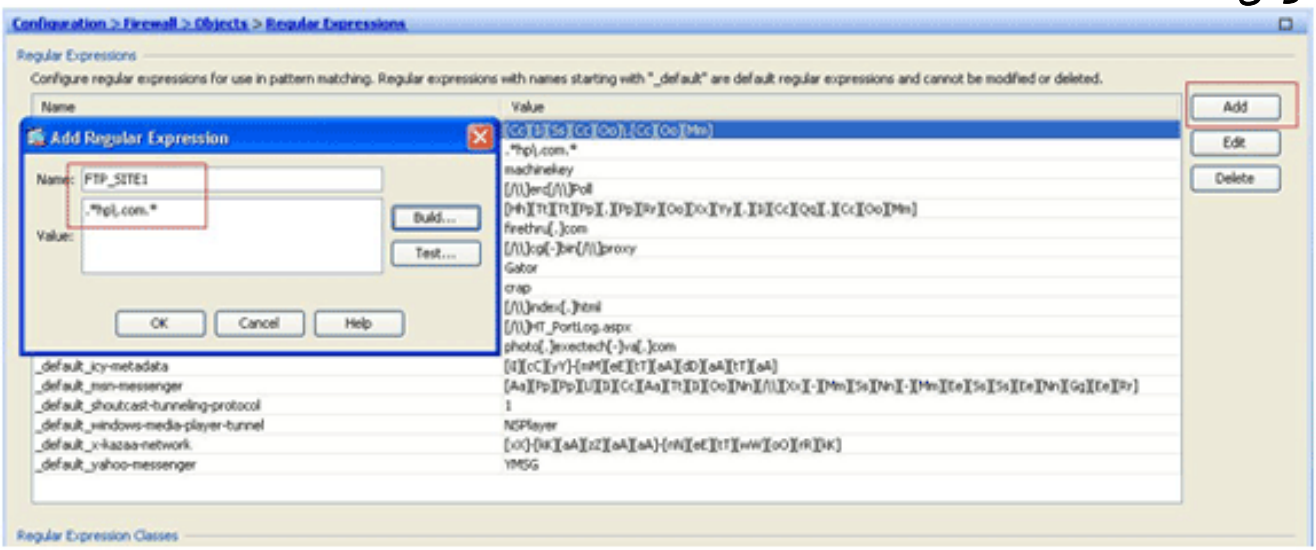
أكمل هذه الخطوات لتكوين التعبيرات العادية وتطبيقها على MPF لحظر مواقع FTP المحددة:

1. **حدد اسم خادم FTP.**يمكن أن يوفر محرك فحص FTP الفحص باستخدام معيار مختلف، مثل الأمر واسم الملف ونوع الملف والخادم واسم المستخدم. يستخدم هذا الإجراء الخادم كمعيار. يستخدم محرك فحص FTP إستجابة الخادم 220 المرسلة من موقع FTP كقيمة للخادم. يمكن أن تكون هذه القيمة مختلفة عن اسم المجال المستخدم من قبل الموقع. يستخدم هذا المثال Wireshark لالتقاط حزم FTP إلى الموقع الذي يتم فحصه للحصول على قيمة الاستجابة 220 للاستخدام في التعبير العادي الخاص بنا في الخطوة 2.

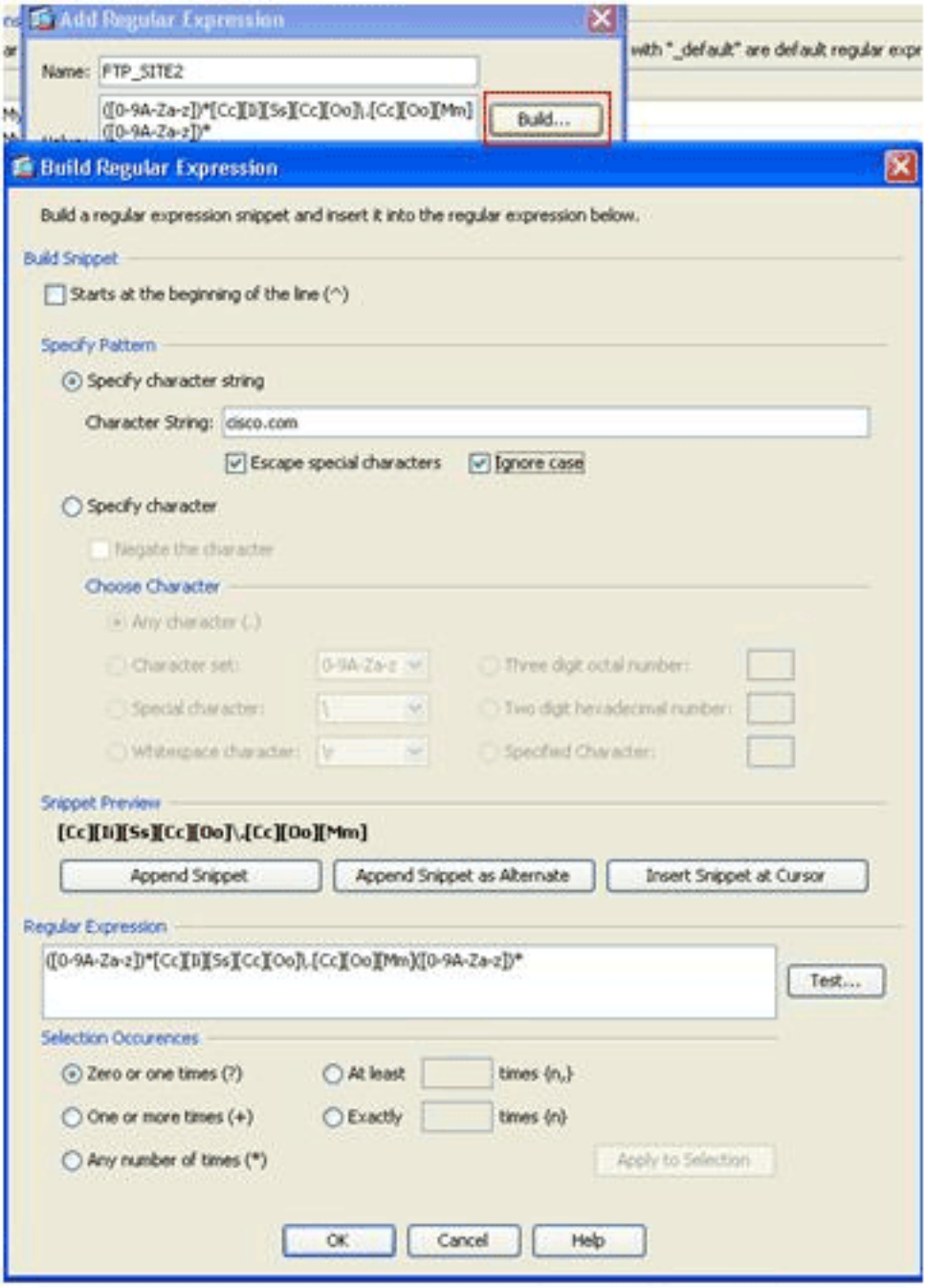


استنادا إلى التقاط قيمة الاستجابة 220 ل ftp://hp.com هي (على سبيل المثال) *q5u0081c.atlanta.hp.com*.

2. **قم بإنشاء تعبيرات عادية.**أخترت **تشكيل > جدار حماية > كائنات > تعابير عادية**، وطقطقة **يضيف** تحت ال عادي تعبير صفحة in order to خلقت تعابير عادية كما هو موضح في هذا الإجراء:قم بإنشاء تعبير عادي، *FTP_SITE1*، لمطابقة الاستجابة 220 (كما هو موضح في التقاط الحزمة في Wireshark أو أي أداة أخرى مستخدمة) التي تم تلقيها من موقع FTP (على سبيل المثال، ".*hp\.com.*")، وانقر **موافق**.

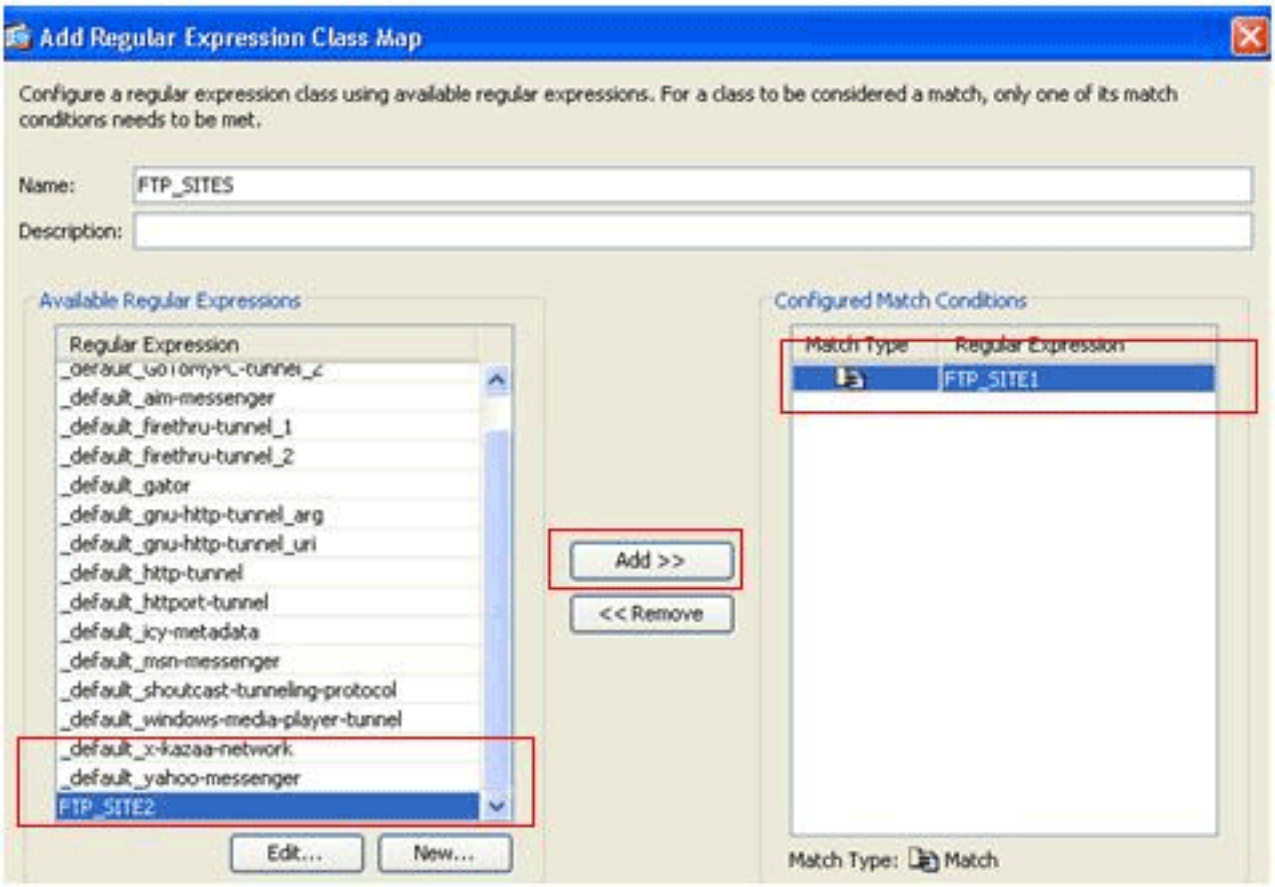


ملاحظة: يمكنك النقر فوق **بناء** للحصول على تعليمات حول كيفية إنشاء تعبيرات عادية أكثر



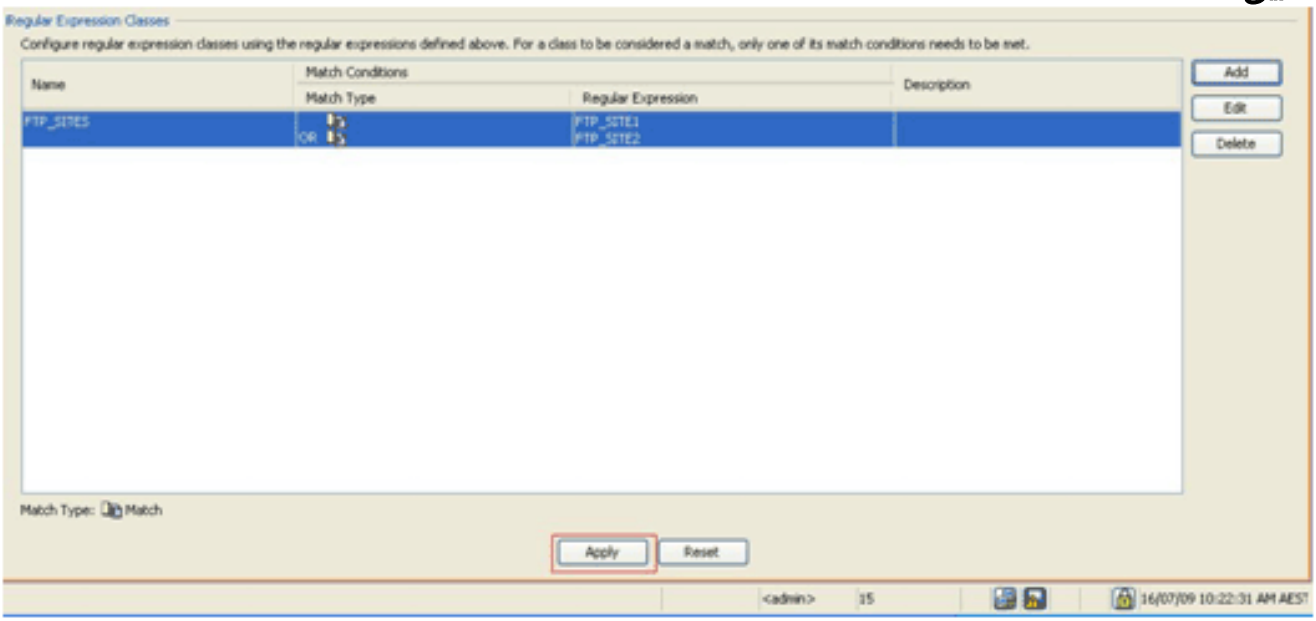
تقدما. بمجرد إنشاء التعبير العادي، انقر فوق **تطبيق**.

3. **قم بإنشاء فئات تعبير نمطي.**أخترت **تشكيل > جدار حماية > كائنات > تعابير عادية**، وطقطقة **يضيف** تحت ال عادي تعبير صنف قسم in order to خلقت الصنف كما هو موضح في هذا الإجراء:قم بإنشاء فئة تعبير عادية، *FTP_SITES*، لمطابقة أي من التعبيرات العادية *FTP_SITE1* و*FTP_SITE2*، وانقر فوق **موافق**.

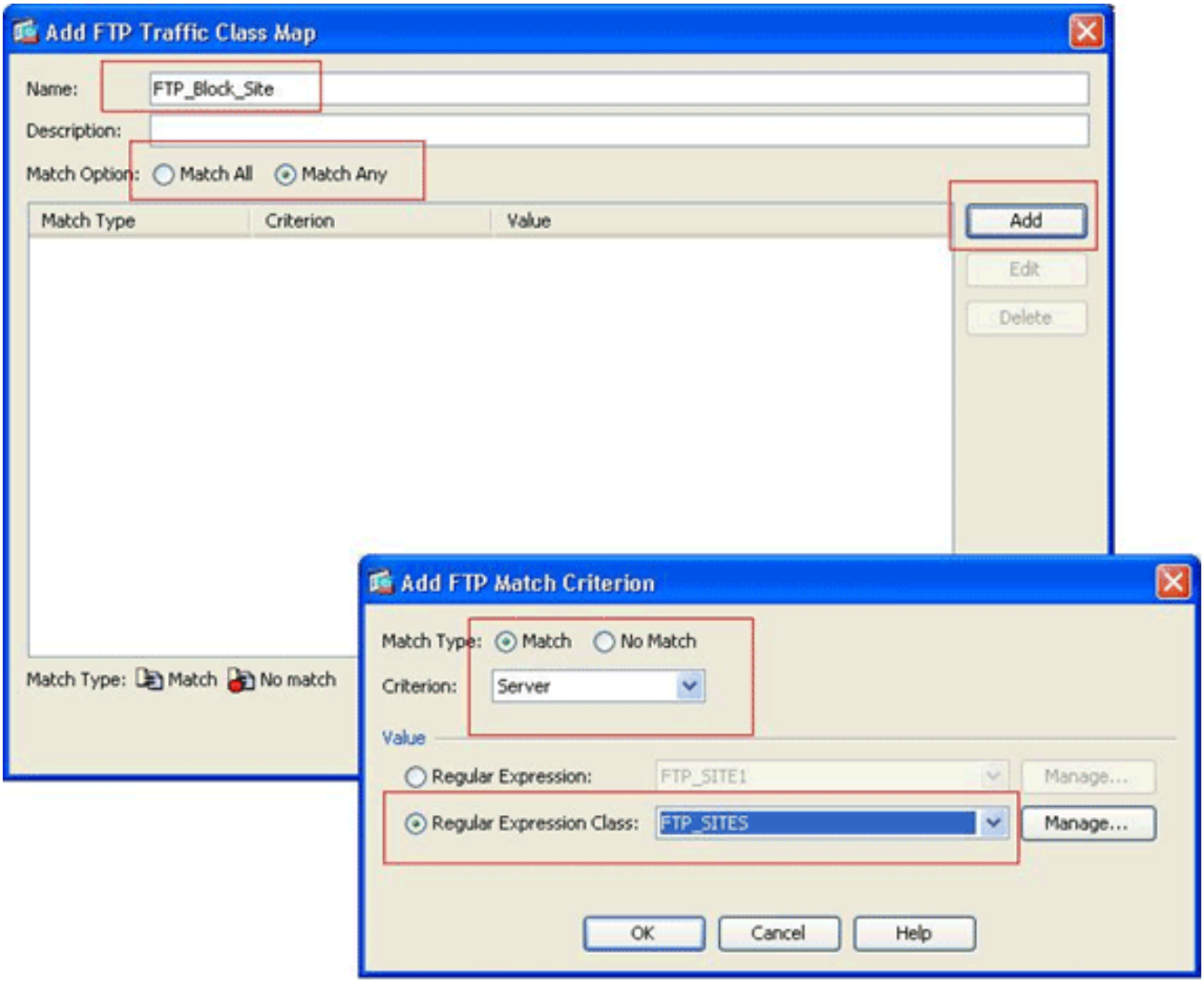


بم

جرد إنشاء خريطة الفئة، انقر فوق
تطبيق.

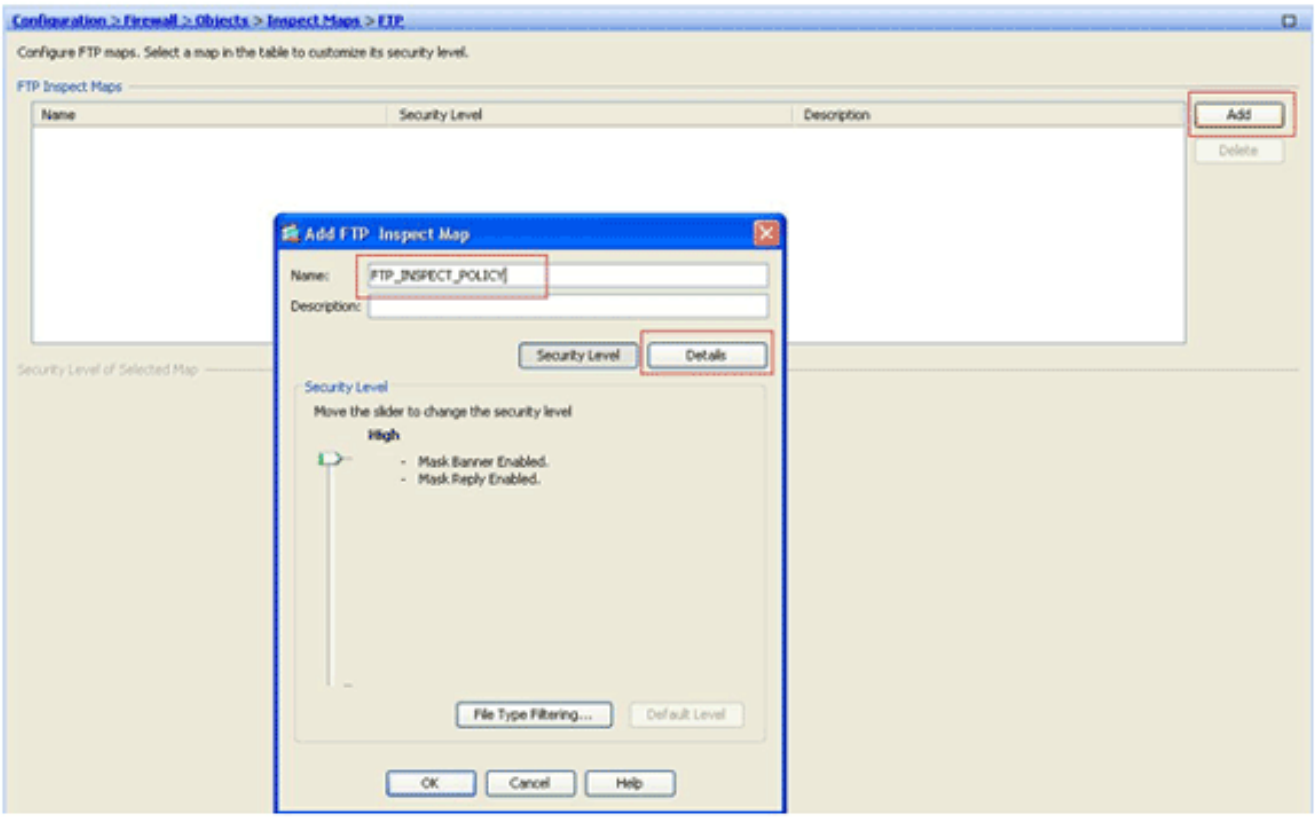


4. **قم بفحص حركة المرور المحددة باستخدام خرائط الفئة.**أختر **تكوين > جدار الحماية > كائنات > خرائط الفئة > FTP > إضافة**، انقر بزر الماوس الأيمن، واختر **إضافة** لإنشاء خريطة فئة لفحص حركة مرور FTP المحددة بواسطة تعبيرات عادية مختلفة كما هو موضح في هذا الإجراء:قم بإنشاء خريطة فئة، *FTP_BLOCK_SITE*، لمطابقة إستجابة FTP 220 مع التعبيرات العادية التي قمت بإنشائها.

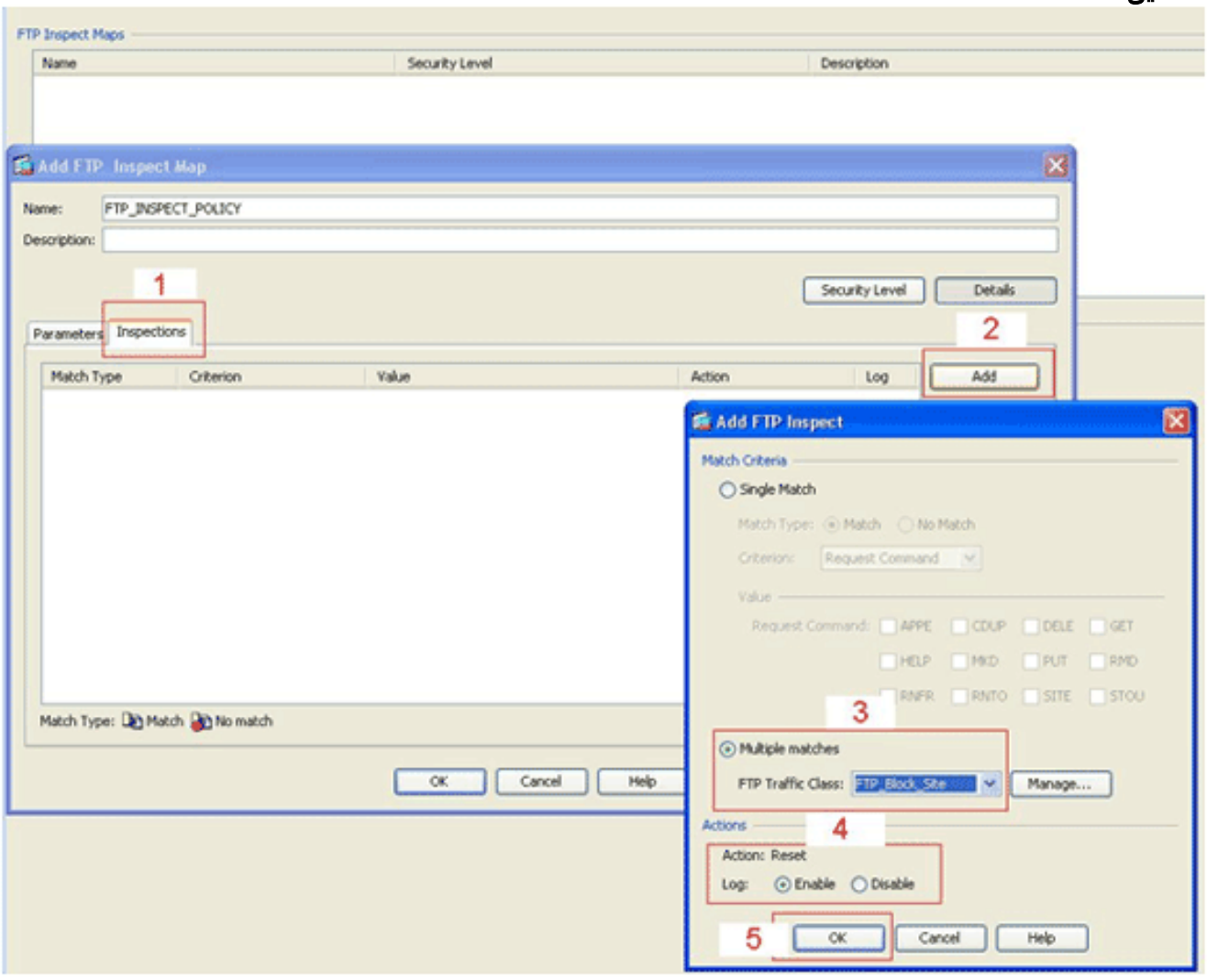


إذا كنت تريد إستبعاد المواقع المحددة في التعبير العادي، انقر فوق زر الخيار **لا تطابق**.في قسم القيمة، أختر إما تعبير عادي أو فئة تعبير عادية. لهذا الإجراء، أختر الفئة التي تم إنشاؤها مسبقا.طقطقة **يطبق**.

5. **قم بتعيين الإجراءات لحركة المرور المطابقة في سياسة التفتيش.**أخترت **تشكيل > جدار حماية > كائنات > فحص الخرائط > FTP> يضيف** in order to خلقت تفتيش سياسة، وعينت الإجراء لحركة المرور المطابقة كما هو
مطلوب.



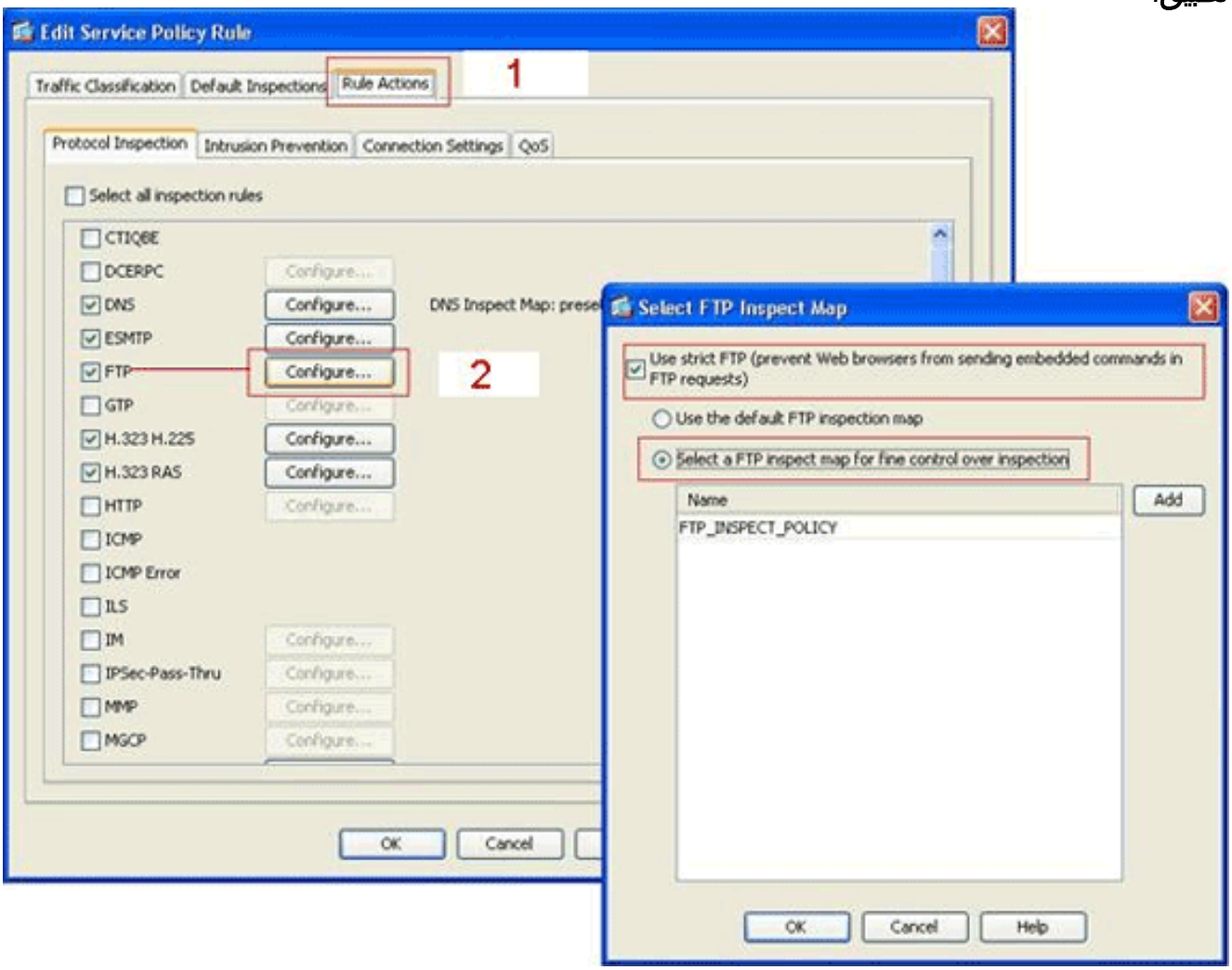
أدخل الاسم والوصف لنهج التفتيش. (على سبيل المثال، *FTP_INSPECTION_POLICY*.)انقر فوق **تفاصيل**.



انقر فوق علامة التبويب **عمليات التفتيش**. (1)انقر فوق **إضافة** (2) .(**Add**)انقر فوق زر **تطابق متعدد** الراديو،

واختر فئة حركة المرور من القائمة المنسدلة. (3)أختر إجراء إعادة الضبط المطلوب للتمكين أو التعطيل. يتيح هذا المثال إمكانية إعادة تعيين اتصال FTP لجميع مواقع FTP *التي لا تطابق* مواقعنا المحددة. (4)انقر فوق **موافق**، ثم انقر فوق **موافق**، ثم انقر فوق **تطبيق**. (5)

6. **تطبيق سياسة FTP للتفتيش على قائمة التفتيش العالمية.**أختر **تكوين > جدار الحماية > قواعد سياسة الخدمة**.على الجانب الأيمن، حدد نهج **inspection_default**، وانقر فوق **تحرير**.تحت علامة التبويب إجراءات القاعدة (1)، انقر فوق الزر **تكوين** ل 2) .FTP)في شاشة تحديد خريطة فحص FTP، حدد خانة الاختيار **إستخدام FTP صارم**، ثم انقر فوق **خريطة فحص FTP للتحكم الدقيق في** زر راديو **الفحص**.يجب أن تكون سياسة فحص FTP الجديدة، *FTP_INSPECTION_POLICY*، مرئية في القائمة.انقر فوق **موافق**، ثم انقر فوق **موافق**، ثم انقر فوق **تطبيق**.



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 التعبيرات العادية التي تم تكوينها.

```
ciscoasa#show running-configregex
"[regex FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm
"*.regex FTP_SITE2 ".*hp\.com
```

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

```
ciscoasa#show running-config class-map
class-map type regex match-any FTP_SITES
```

```
                                        match regex FTP_SITE1
                                        match regex FTP_SITE2
                        class-map type inspect ftp match-all FTP_Block_Site
                                  match not server regex class FTP_SITES
                                      class-map inspection_default
                                match default-inspection-traffic
                                                                        !
```

- **show running-config policy-map type فحص http**—يعرض خرائط السياسة التي تقوم بفحص حركة مرور HTTP التي تم تكوينها.

```
ciscoasa#show running-config policy-map type inspect ftp
                                                                        !
                        policy-map type inspect ftp FTP_INSPECT_POLICY
                                                          parameters
                                                        mask-banner
                                                    mask-syst-reply
                                                class FTP_Block_Site
                                                          reset log
                                                                  !
```

- **show running-config policy-map**— يعرض جميع تكوينات خريطة السياسة، بالإضافة إلى تكوين خريطة السياسة الافتراضية.

```
                                                ciscoasa#show running-config policy-map
                                                                        !
                            policy-map type inspect dns preset_dns_map
                                                          parameters
                                               message-length maximum 512
                        policy-map type inspect ftp FTP_INSPECT_POLICY
                                                          parameters
                                                        mask-banner
                                                    mask-syst-reply
                                                class FTP_Block_Site
                                                          reset log
                                            policy-map global_policy
                                       class inspection_default
                                  inspect dns preset_dns_map
                                          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
                            inspect ftp strict FTP_INSPECT_POLICY
                                                                        !
```

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

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

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

يمكنك إستخدام الأمر **show service-policy** للتحقق من أن محرك الفحص يقوم بفحص حركة المرور ويسمح لها أو إسقاطها بشكل صحيح.

```
ciscoasa#show service-policy

                                                    :Global policy
                                          Service-policy: global_policy
                                        Class-map: inspection_default
                Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
           Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
            Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
                           Inspect: netbios, packet 0, drop 0, reset-drop 0
                               Inspect: rsh, packet 0, drop 0, reset-drop 0
                              Inspect: rtsp, packet 0, drop 0, reset-drop 0
                            Inspect: skinny , packet 0, drop 0, reset-drop 0
              Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
                            Inspect: sqlnet, packet 0, drop 0, reset-drop 0
                            Inspect: sunrpc, packet 0, drop 0, reset-drop 0
                              Inspect: tftp, packet 0, drop 0, reset-drop 0
                              Inspect: sip , packet 0, drop 0, reset-drop 0
                             Inspect: xdmcp, packet 0, drop 0, reset-drop 0
Inspect: ftp strict FTP_INSPECT_POLICY, packet 40, drop 0, reset-drop 2
```

معلومات ذات صلة

- ASA/PIX 8.x: حظر بعض مواقع الويب (URLs) باستخدام تعبيرات منتظمة مع مثال تكوين MPF
- PIX/ASA 7.x والإصدارات الأحدث: منع حركة مرور البيانات من نظير إلى نظير (P2P) والمراسلة الفورية (IM) باستخدام مثال تكوين MPF
- PIX/ASA 7.x: تمكين مثال تكوين خدمات FTP/TFTP
- تطبيق فحص بروتوكول طبقة التطبيق
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances - الدعم
- مدير أجهزة حلول الأمان المعدلة (ASDM) من Cisco
- أجهزة الأمان Cisco PIX 500 Series Security Appliances - الدعم
- برنامج جدار حماية Cisco PIX - الدعم
- مراجع أوامر برنامج جدار حماية PIX من Cisco

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).