

ASA/PIX 7.2: بيولاء عقاوم ضع ب رضح ةلثم أ عم ةمظاتم نم تاري بعت مادختساب MPF نيوكت

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [المنتجات ذات الصلة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [نظرة عامة على إطار عمل السياسة النمطية](#)
- [تعبير نمطي](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [تكوين ASA CLI](#)
- [تكوين ASA 7.2\(x\) مع ASDM 5.2](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يصف هذا المستند كيفية تكوين أجهزة الأمان Cisco ASA/PIX 7.2 باستخدام التعبيرات العادية مع إطار عمل السياسة النمطية (MPF) لحظر مواقع ويب معينة (URLs).

ملاحظة: لا يمنع هذا التكوين جميع تنزيلات التطبيق. بالنسبة لحزم الملفات الموثوقة، يجب استخدام جهاز مخصص، مثل WebSense، وما إلى ذلك، أو وحدة، مثل وحدة CSC النمطية ل ASA.

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 7.2(2) من البرنامج
 - Cisco Adaptive Security Device Manager (ASDM)، الإصدار 5.2(2) ل ASA 7.2(2)
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين مسموح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

كما يمكن استخدام هذا التكوين مع Cisco 500 Series PIX الذي يشغل الإصدار 7.2(2) من البرنامج.

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 استخدام 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:

- تطبيق 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 بالحروف الأولية، بحيث يمكنك مطابقة متغيرات

متعددة من سلسلة نصية. يمكنك استخدام تعبير عادي لمطابقة محتوى حركة مرور تطبيق معينة؛ على سبيل المثال، يمكنك مطابقة سلسلة URL داخل حزمة HTTP.

ملاحظة: استخدم **Ctrl+V** للهروب من كل الحروف الخاصة في CLI، مثل علامة إستفهام (?) أو علامة تبويب. على سبيل المثال، اكتب **d[Ctrl+V]g** لإدخال **gd** في التكوين.

لإنشاء تعبير عادي، استخدم الأمر **regex**، والذي يمكن استخدامه لميزات مختلفة تتطلب مطابقة النص. على سبيل المثال، يمكنك تكوين إجراءات خاصة لفحص التطبيق باستخدام "إطار عمل سياسة نمطي" باستخدام خريطة سياسة التفتيش (راجع الأمر [فحص نوع خريطة السياسة](#)). 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 استخدام أوامر **المطابقة** مباشرة في خريطة سياسة التفتيش. تتيح لك بعض أوامر **التطابق** تعريف النص في حزمة ذات تعبير عادي؛ على سبيل المثال، يمكنك مطابقة سلاسل عنوان URL داخل حزم HTTP. يمكنك تجميع التعبيرات العادية في خريطة فئة تعبير نمطي (راجع الأمر [regex نوع خريطة الفئة](#)).

[الجدول 1](#) يحدد الحروف الأولية التي لها معنى خاص.

الحرف	الوصف	ملاحظات
.	نقطة	مطابقة أي حرف واحد على سبيل المثال 'D.G يطابق الكلب' 'dag, dtg واي كلمة تحتوي على تلك الحروف، مثل dogg.onit
(exp)	ضغط جزئي	يفصل التعبير الجزئي عن الحروف

ف
المحي
طة،
بحيث
يمكن
ك
إستخ
دام
حرو
ف
أولية
أخرى
على
التعبير
الجزء
ي.
على
سبيل
المثال
'
تطاب
ق
d(ola
g) مع
الكلب
والدا
غ،
ولكن
doja
g
تطاب
ق do
and
.ag
يمكن
أيضا
إستخ
دام
التعبير
الجزء
بي مع
كميه
التكرا
ر
لتمييز
الحرو
ف
المق
صودة
للتكرا
ر
على
سبيل

المثال ، $ab(x$ $y)\{3\}$ z يطا ، ق $abxy$ $xyxy$.z		
يطا ، ق أيا من التعبير ين الذين يفصلها ما . على سبيل المثال ، يطا ، ق الكلب القط الكلب أو القط .	تناوب	
قيمة كمية تشير إلى وجود 0 أو 1 من التعبير السا ، ق . على سبيل المثال ، إما أن تتطا ، ق مع قيمة العر ض أو أن تخسر .	علامة الاستفهام ام	?

<p>ملاحظة: يجب إدخال Ctrl+V ثم علامة الاستفهام وإلا سيتم إساءة دالة المسا عدة.</p>		
<p>قيمة كمية تشير إلى وجود 0 أو 1 أي عدد من التعبير السابق. ق. على سبيل المثال ، يطابق $lo*se$ ، lse ، فقد ، غير محكم ، وهكذا .</p>	<p>نجمية</p>	<p>*</p>
<p>تكرار x مرات بالضبط. ط. على سبيل المثال ،</p>	<p>تكرار القياس</p>	<p>{x}</p>

<p>ab(x y){3} z يطا ق abxy xyxy .z</p>		
<p>تكرار x مرة على الأقل. على سبيل المثال ' ab(x y){2، }z يطا ق abxy xyz، abxy xyxy ،z وهكذا .</p>	<p>الحد الأدنى لمكبر التكرار</p>	<p>{،x}</p>
<p>مطابقة ة أي حرف في الأقوا س. على سبيل المثال ' [abc] يطا ق أ، ب، أو ج.</p>	<p>فئة الحرف</p>	<p>[أي بي سي]</p>
<p>مطابقة ة حرف واحد غير موجود د داخل الأقوا</p>	<p>فئة الحرف الضار</p>	<p>[abc^]</p>

<p>س. على سبيل المثال</p> <p>ab[^] [c يطا ق أي حرف غير ،a، b أو c. [[^]a- [z يطا ق أي حرف مفرد ليس حرف كبير.</p>		
<p>مطابقة ة أي حرف في النطا ق. [a-z] يطا ق أي حرف صغير . يمكن ك مزج الحرو ف والنطا قات: [abcq [-z تطا ق، a، b، c، q، r، s، t، u، v، w، x، ،y، z وهكذا a-] ا</p>	<p>فئة نطاق الحرو ف</p>	<p>[ألف-جيم]</p>

<p> cq- .z حرف شرط ة (-) حرف ب فقط إذا كان هو الحر ف الأخير أو الأول داخل الأقوا س: -abc] أو [-] .abc </p>		
<p> يحاف ظ على المسا فات الخليفي ة أو المسا فات البادئة في السا سلة. على سبيل المثال ، يحتف ظ الاختبا ر بمسا فة المسا فة البادئة عندما يبحث عن تطاب ق. </p>	<p> علامات الاقتبا س </p>	<p> ''' </p>

يحدد بداية السطر . ر	علامة الإفحام	٨
عند إستخ دame مع حرف أولي، يطاء ق حرف حرف	حرف الهروب	١
عندما لا يكون الحر ف الحر ف الأوا ي، قانه يطاء ق الحر ف الحرف ب.	الحرف	فحم
مطابقة ة إرجاع النقل 0x0d .	إعادة النقل	r\
مطابقة ة سطر	نيولايين	n\

جديد 0x0a		
مطابقة علامة تبويب 0x09	علامة تبويب	t\
مطابقة موجز نموذج 0x0c	فورم فييد	f\
مطابقة حرف ASC II باستخ دام سداس ي عشر (رقما ن بالضبط (ط.)	الرقم السداس ي العشر ي الفار	xNN\
مطابقة حرف ASC II على هيئة ثمانية (ثلاثة أرقام بالضبط (ط.) على سبيل المثال ' يمثل حرف 040 مسافة .	عدد ثمانية منفر	NNN\

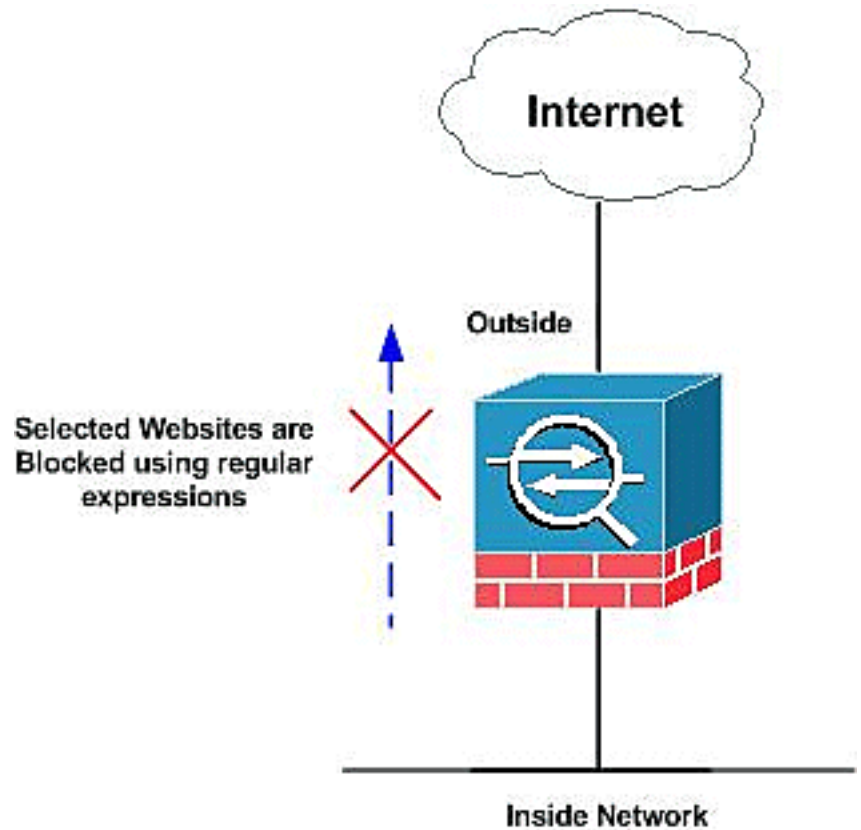
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعلماء 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](#)
- [تكوين ASA 7.2\(x\) مع ASDM 5.2](#)

تكوين ASA CLI

```
ASA CLI تكوين
ciscoasa#show running-config
Saved :
:
(ASA Version 7.2(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/1.0]

```

*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/1.0]

```

*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/1.0]

```

*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/1.0]

```

*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

```

```

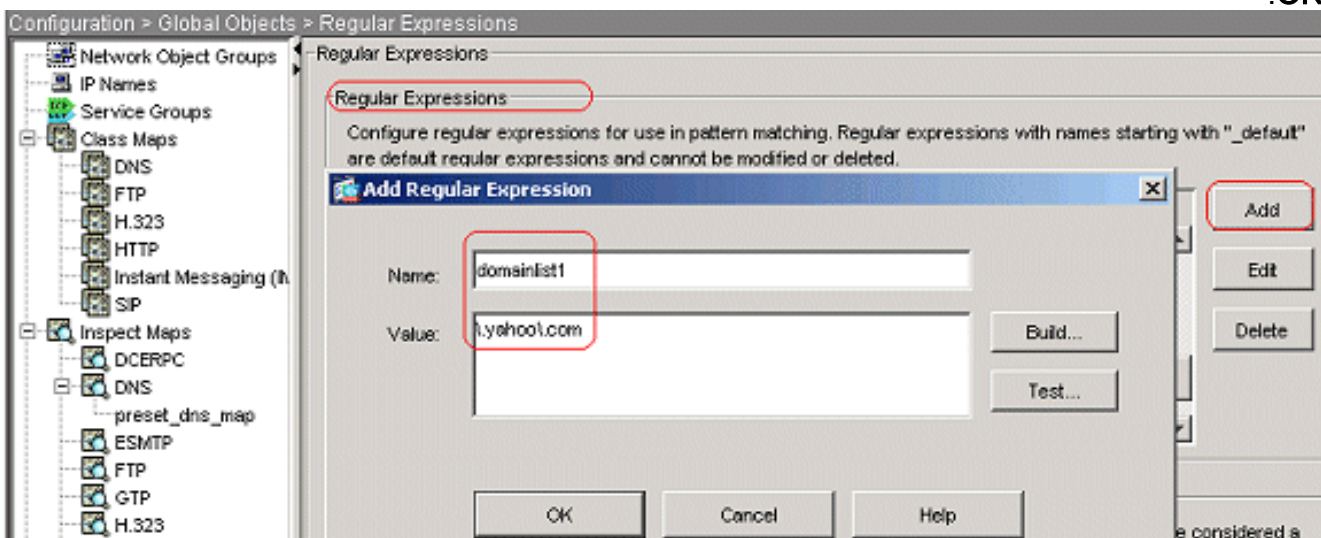
Apply the policy to the interface inside where the ---!
websites will be blocked prompt hostname context
Cryptochecksum:e629251a7c37af205c289cf78629fc11 : end
#ciscoa

```

تكوين ASA 7.2(x) مع ASDM 5.2

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

1. إنشاء تعبيرات عادية أخترت تشكيل < كائن شامل > تعابير عادية وطققة يضيف تحت ال عادي تعبير صفحة in order to خلقت تعابير عادي. خلقت تعبير عادي in order to domainList1 على قبض ال domain name yahoo.com وانقر فوق OK.



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

Add Regular Expression

Name: domainlist2

Value: \.myspace\.com

Build... Test...

OK Cancel Help

OK
 قمت بتعبير عادي في order to domainList3 على قبض ال domain name YouTube.com. وانقر فوق

Add Regular Expression

Name: domainlist3

Value: \.youtube\.com

Build... Test...

OK Cancel Help

OK
 م بإنشاء قائمة مرور تعبير عادية من أجل التقاط ملحقات الملف مثل exe و com و bat، شريطة أن يكون إصدار http المستخدم من قبل مستعرض الويب إما 1.0 أو 1.1. وانقر فوق

Add Regular Expression

Name: urllist1

Value: .*\.(?=[Ee][Xx][Ee][Cc][Oo][Mm][Bb][Aa][Tt]) HTTP/1.[01]

Build... Test...

OK Cancel Help

OK
 خلقت تعبير عادي في order to urllist2 على قبض المبرد امتدادات، مثل vbs، pif، و wsh، أن ال HTTP صيغة أن يكون استعملت ب متصفح ويب إما 1.0 أو 1.1. وانقر فوق

Add Regular Expression

Name:

Value:

Build...
Test...

OK Cancel Help

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

Add Regular Expression

Name:

Value:

Build...
Test...

OK Cancel Help

قم بإنشاء قائمة معارف التعبير العادي من أجل التقاط امتدادات الملف، مثل **tar**، **zip**، و **tgz**، شريطة أن يكون إصدار HTTP الذي يتم استخدامه من قبل مستعرض الويب إما 1.0 أو 1.1. وانقر فوق

Add Regular Expression

Name:

Value:

Build...
Test...

OK Cancel Help

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

Add Regular Expression

Name: contenttype

Value: Content-Type

Build

Test

OK Cancel Help

قم بإنشاء

.OK

عنوان تطبيق تعبير عادي من أجل التقاط رأس التطبيق المختلف. وانقر فوق

Add Regular Expression

Name: applicationheade

Value: application/*

Build

Test

OK Cancel Help

OK. تشكيل

CLI

مكافئ

2. إنشاء فئات التعبير العادية اخترت تشكيل < كائن عام > تعبير عادي، وطققة يضيف تحت ال عادي تعبير صنف طقطقة in order to خلقت مختلف صنف. قم بإنشاء فئة تعبير عادي DomainBlockList لمطابقة أي من التعبيرات العادية: domainList1، domainList2، و domainList3. وانقر فوق .OK

Add Regular Expression Class Map

Configure a regular expression class using available regular expressions. For a class to be considered a match, only one of its match conditions needs to be met.

Name:

Description:

Available Regular Expressions

Regular Expression
_default_jcy-metadata
_default_msn-messenger
_default_shoutcast-tunneling-prot...
_default_windows-media-player-t...
_default_x-kazaa-network
_default_yahoo-messenger
applicationheader
contenttype
urllist1
urllist2
urllist3
urllist4




Edit...


New...

Add >>

<< Remove

Configured Match Conditions

Match Type	Regular Expression
	domainlist1
OR 	domainlist2
OR 	domainlist3

Match Type:  Match

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

Add Regular Expression Class Map

Configure a regular expression class using available regular expressions. For a class to be considered a match, only one of its match conditions needs to be met.

Name:

URLBlockList

Description:





Available Regular Expressions


Regular Expression
_default_ntpport-tunnel
_default_jcy-metadata
_default_msn-messenger
_default_shoutcast-tunneling-prot...
_default_windows-media-player-t...
_default_x-kazaa-network
_default_yahoo-messenger
applicationheader
contenttype
domainlist1
domainlist2
domainlist3

Add >>

<< Remove

Configured Match Conditions

Match Type	Regular Expression
	urllist1
OR 	urllist2
OR 	urllist3
OR 	urllist4

Match Type:  Match

CLI تشكيل مكافئ

3. فحص حركة المرور المحددة باستخدام خرائط الفئة اخترت تشكيل شامل كائن <صنف خرائط<HTTP> إضافة
in order to خلقت صنف خريطة أن يفحص ال HTTP حركة مرور يعين ب مختلف تعابير نظامية. قم بإنشاء
مخطط فئة AppHeaderClass لمطابقة رأس الاستجابة مع لقطات التعبير
العادية.

Add HTTP Traffic Class Map

Name:

Description:

Match All

Match Type	Criterion	Value	Add
			<input type="button" value="Add"/>

Add HTTP Match Criterion

Match Type: Match No Match

Criterion:

Value

Field

Predefined:

Regular Expression:

Value

Regular Expression:

Regular Expression Class:

وانقر فوق OK. قم بإنشاء **BlockDomainsClass** لتعيين الفئة لمطابقة رأس الطلب مع لقطات التعبير العادية.

Add HTTP Traffic Class Map

Name:

Description:

Match All

Match Type	Criterion	Value	Add
------------	-----------	-------	-----

Add HTTP Match Criterion

Match Type: Match No Match

Criterion:

Value

Field

Predefined:

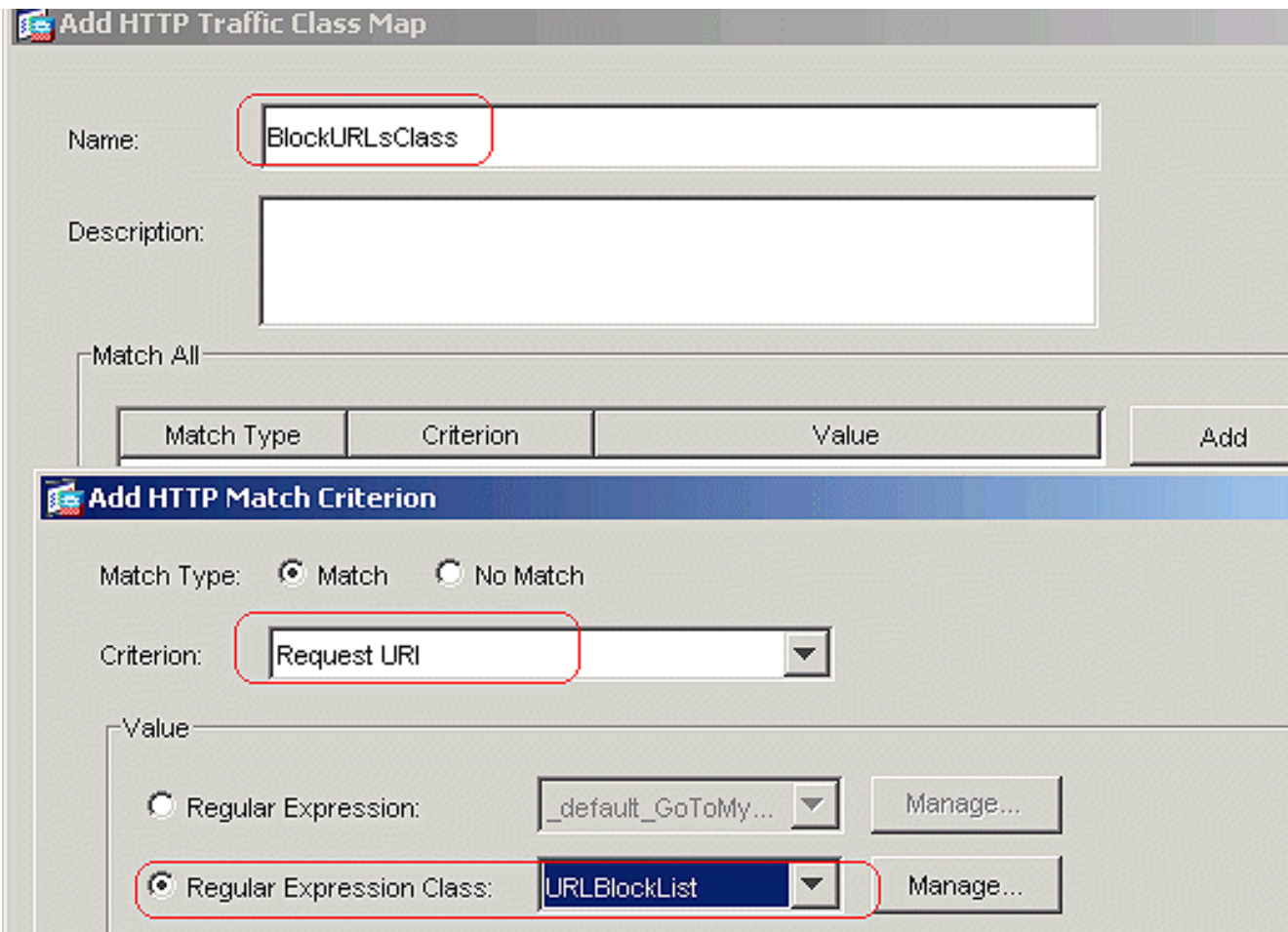
Regular Expression:

Value

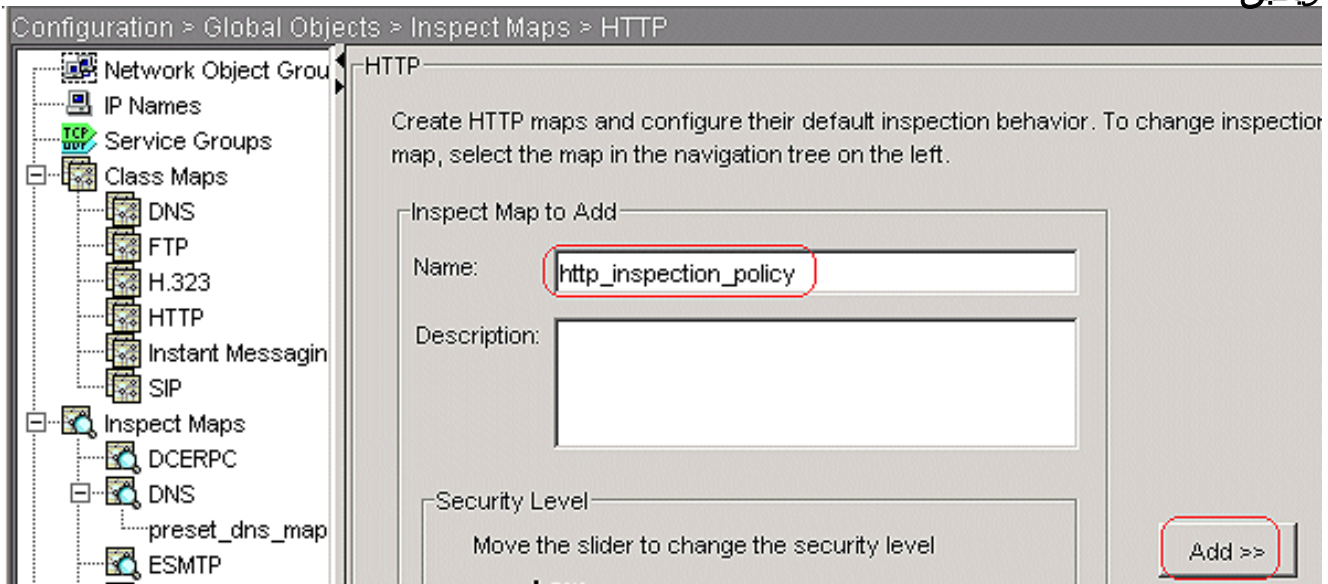
Regular Expression:

Regular Expression Class:

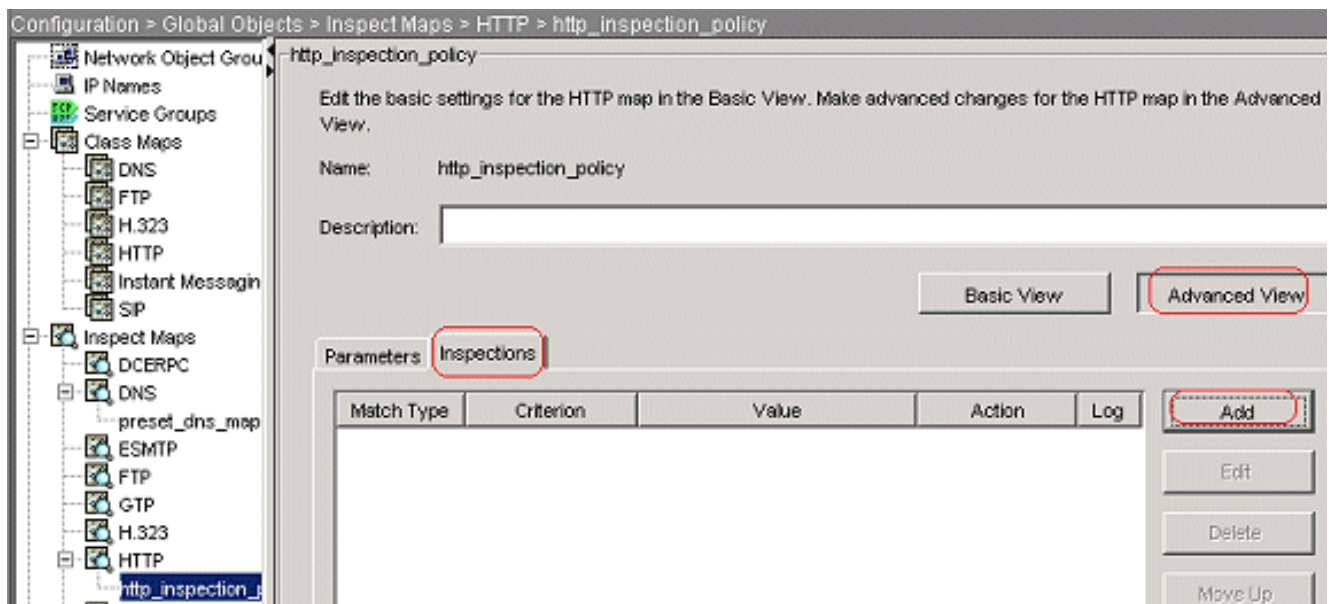
وانقر فوق OK. قم بإنشاء **BlockURLsClass** لتعيين الفئة لمطابقة URI للطلب مع التقاط التعبير العادي.



وانقر فوق OK.CLI تشكيل مكافئ
 4. تعيين الإجراءات لحركة المرور المطابقة في سياسة التفتيش اخترت تشكيل <شامل كائن> يفحص خرائط <HTTP
 in order to خلقت http_inspection_policy أن يثبت الإجراء ل ال يماثل حركة مرور. قطعة يضيف
 ويطبق.



أخترت تشكيل <كائن شامل> فحص خرائط <http_inspection_policy> HTTP و قطعة متقدم
 عرض <تفتيش> إضافة in order to يثبت الإجراء ل مختلف فئات يخلق حتى
 الآن.



وانقر فوق OK. قم بتعيين الإجراءات كاتصال إسقاط؛ قم بتمكين تسجيل المعيار كطريقة طلب وقيمة

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion:

Value

Method:

Regular Expression

Regular Expression:

Regular Expression Class:

Multiple matches

HTTP Traffic Class:

Actions

Action: Drop Connection Reset Log

Log: Enable Disable

وانقر فوق

كاتصال.

OK. قم بتعيين الإجراء ك اتصال إسقاط، وقم بتمكين التسجيل للفتة

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request/Response Content Type Mismatch

Value: Not applicable.

Multiple matches

HTTP Traffic Class: AppHeaderClass

Actions

Action: Drop Connection Reset Log

Log: Enable Disable

9

AppHeaderClass
نقر فوق OK. قم بتعيين الإجراء على أنه إعادة ضبط، وقم بتمكين تسجيل الفئة
BlockDomainsClass

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request/Response Content Type Mismatch

Value: Not applicable.

Multiple matches

HTTP Traffic Class: BlockDomainsClass

Actions

Action: Drop Connection Reset Log

Log: Enable Disable

وانقر فوق OK. قم

بتعيين الإجراء على أنه إعادة تعيين، وقم بتمكين تسجيل الفئة

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request/Response Content Type Mismatch

Value: Not applicable.

Multiple matches

HTTP Traffic Class: BlockURLsClass

Actions

Action: Drop Connection Reset Log

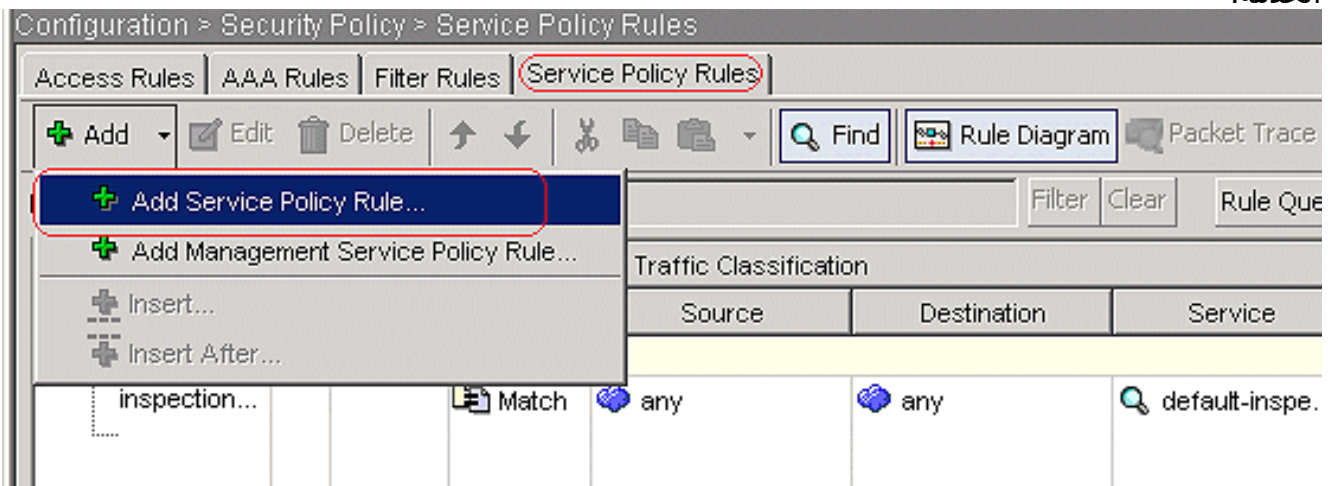
Log: Enable Disable

وانقر

.BlockURLsClass

فوق OK. قطعة يطبق CLI تشكيل مكافئ

5. تطبيق سياسة HTTP للتفتيش على الواجهة أختار تكوين < سياسة التأمين < قواعد سياسة الخدمة < إضافة < قاعدة سياسة الخدمة ضمن علامة التوجيه قواعد سياسة



حركة مرور بيانات HTTP اخترت القارن لاسلكي مع القارن داخلي من القائمة المنسدلة والنهج إسم بما أن
داخلي سياسة. انقر فوق **Next**
(التالي).

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: inside - (create new service policy)

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

قم بإنشاء حركة مرور http لخريطة الفئة، وفحص عنوان IP للمصدر والوجهة (يستخدم قائمة التحكم في الوصول (ACL). انقر فوق **Next**
(التالي).

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

httptraffic

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

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.

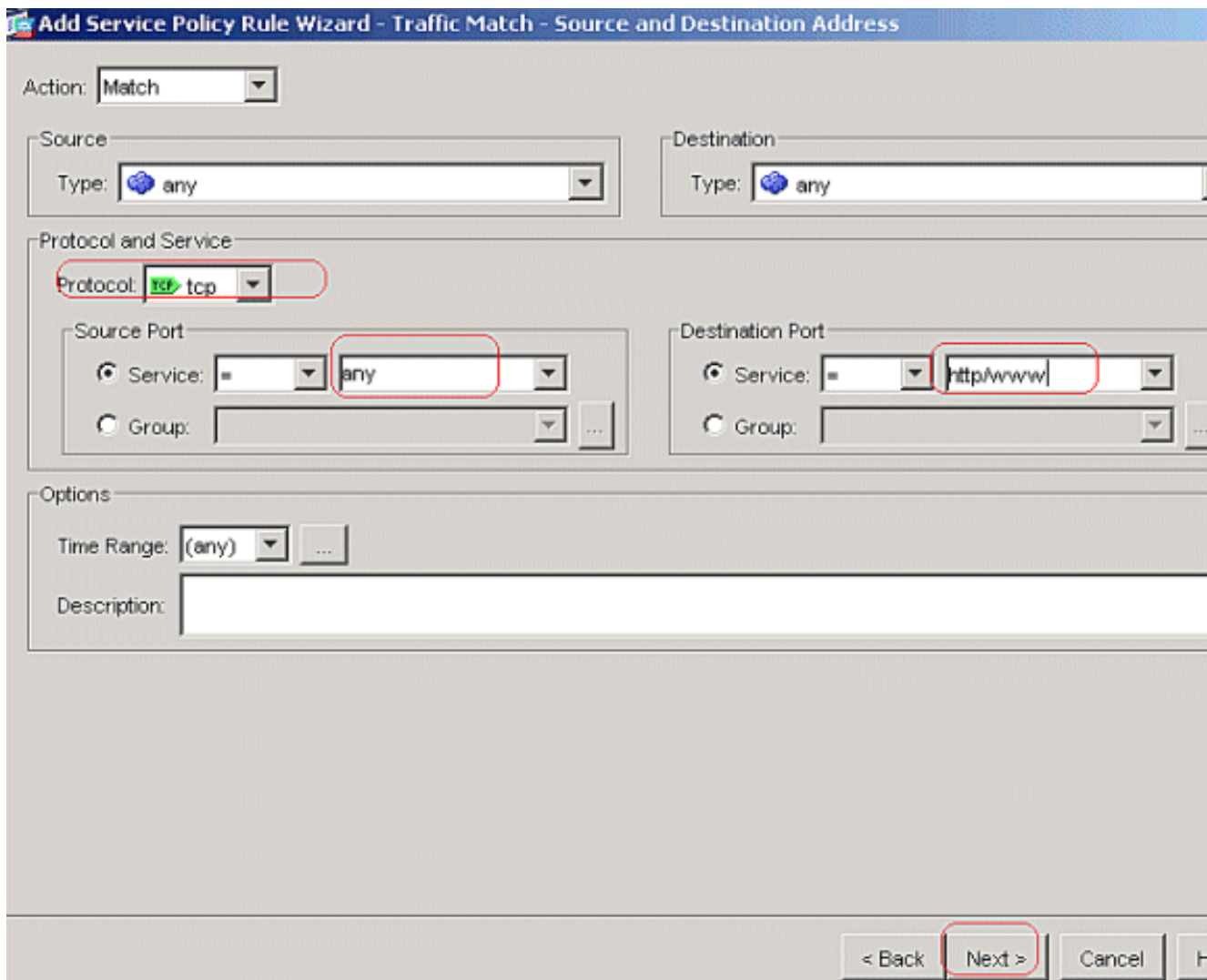
Use class-default as the traffic class.

< Back

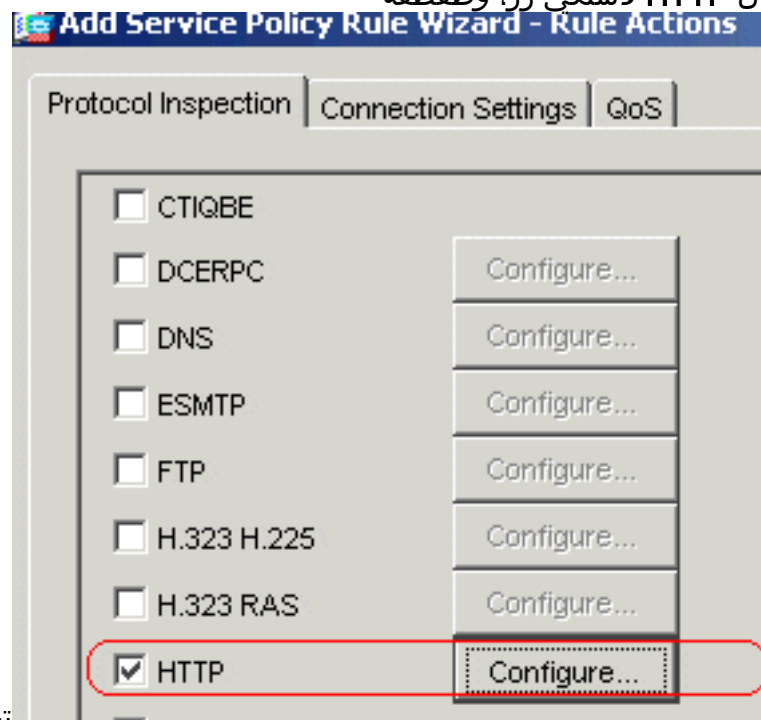
Next >

Cancel

أخترت المصدر والوجهة أي مع ال TCP ميناء ك HTTP. انقر فوق Next (التالي).



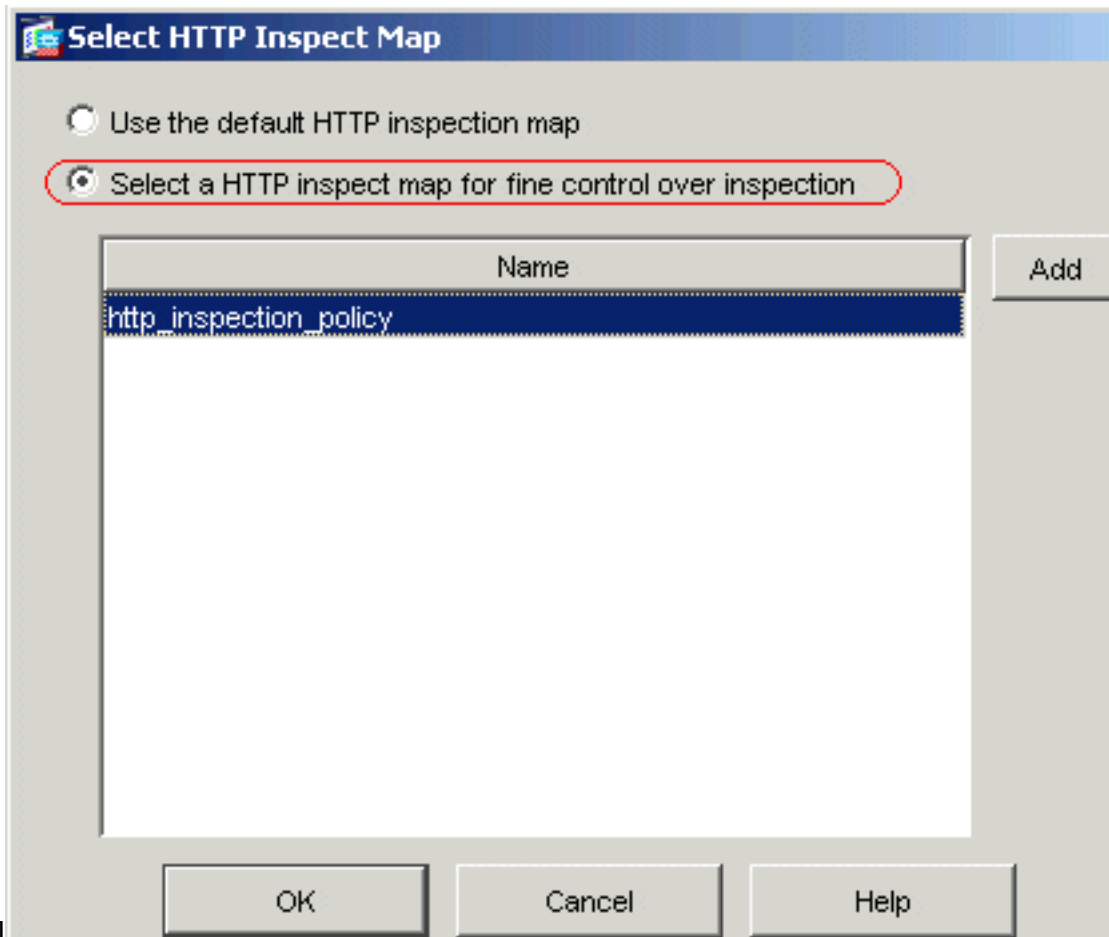
تدقيق ال HTTP لاسلكي زر، وطققة



تحقق من زر الخيار حدد خريطة فحص

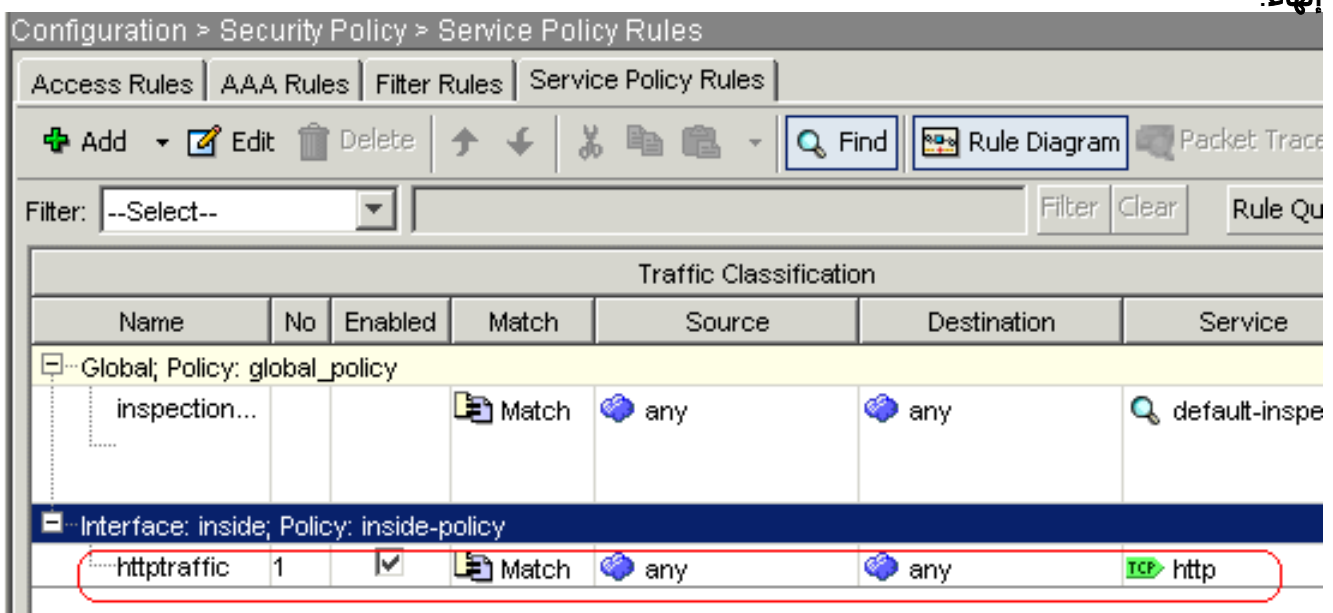
يشكل.

HTTP لعنصر التحكم في الفحص. وانقر فوق



انقر فوق

.OK
إنهاء.



منفذ 8080 حركة مرور مرورية أخرى، انقر فوق إضافة < قاعدة نهج الخدمة.

Configuration > Security Policy > Service Policy Rules

Access Rules | AAA Rules | Filter Rules | Service Policy Rules

+ Add Edit Delete ↑ ↓ ✂ 📄 📄 Find Rule Diagram Packet Tr

+ Add Service Policy Rule... Filter Clear Rule

+ Add Management Service Policy Rule...

Insert... Traffic Classification

Insert After...

Source	Destination	Service
inspection...	Match any	any default-ins
Interface: inside; Policy: inside-policy		
httptraffic	1 Match any	any tcp http

انقر فوق Next
(التالي).

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

Only one service policy can be configured per interface or at global level. If a service policy already exists on the selected interface, you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface:

Policy Name: *

Description:

أخترت

ال add قاعدة إلى موجود حركة مرور صنف لاسلكي، واخترت httpTraffic من القائمة المنسدلة. انقر فوق
Next
(التالي).

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

inside-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

Rule can be added to existing class map if that class map uses access control list (ACL) as traffic match criteria.
Following class maps use ACL as traffic match criteria

Add rule to existing traffic class:

httptraffic

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.

Use class-default as the traffic class.

< Back

Next >

Cancel

أخترت المصدر والوجهة أي مع ال TCP ميناء ك 8080. انقر فوق Next (التالي).

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match

Source

Type: any

Destination

Type: any

Protocol and Service

Protocol: tcp

Source Port

Service: = any

Group: ...

Destination Port

Service: = 8080

Group: ...

Options

Time Range: (any) ...

Description:

< Back | Next > | Cancel

انقر فوق
إنهاء.

Add Service Policy Rule Wizard - Rule Actions

Protocol Inspection | Connection Settings | QoS

- CTIQBE
- DCERPC Configure...
- DNS Configure...
- ESMTMP Configure...
- FTP Configure...
- H.323 H.225 Configure...
- H.323 RAS Configure...
- HTTP Configure... HTTP Inspect Map: http_inspection_policy
- ICMP
- ICMP Error
- ILS
- IM Configure...
- IPSec-Pass-Thru Configure...
- MGCP Configure...
- NETBIOS Configure...
- PPTP

< Back

Finish

Configuration > Security Policy > Service Policy Rules

Access Rules | AAA Rules | Filter Rules | Service Policy Rules

+ Add | Edit | Delete | Find | Rule Diagram | Packet T

Filter: --Select-- | Filter | Clear | Rule

Traffic Classification

Name	No	Enabled	Match	Source	Destination	Service
Global; Policy: global_policy						
inspection...			Match	any	any	default-ir
Interface: inside; Policy: inside-policy						
httptraffic	1	<input checked="" type="checkbox"/>	Match	any	any	TCP http
	2	<input checked="" type="checkbox"/>	Match	any	any	TCP 8080

طقطقة يطبق. CLI تشكيل مكافئ

[التحقق من الصحة](#)

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج 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 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 استخدام أوامر `debug`.

• **debug http** — يعرض رسائل تصحيح الأخطاء لحركة مرور HTTP.

معلومات ذات صلة

• [صفحة دعم أجهزة الأمان المعدلة من Cisco](#)

- [صفحة دعم مدير أجهزة حلول الأمان المعدلة \(ASDM\) من Cisco](#)
- [صفحة دعم PIX لسلسلة Cisco 500](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج 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 ج ن ا ل ا دن ت س م ل ا