مثال تكوين تصفية PIX/ASA URL

المحتويات

المقدمة

يشرح هذا المستند كيفية تكوين تصفية URL على جهاز أمان.

لتصفية حركة المرور هذه الميزات:

- فهو يساعد على تقليل مخاطر الأمان ومنع الاستخدام غير المناسب.
- ويمكن أن يوفر قدرا أكبر من التحكم في حركة المرور التي تمر عبر جهاز الأمان.

ملاحظة: نظرا لأن تصفية URL تستخدم وحدة المعالجة المركزية (CPU) بشكل مكثف، فإن إستخدام خادم تصفية خارجي يضمن عدم تأثر إخراج حركة المرور الأخرى. ومع ذلك، استنادا إلى سرعة شبكتك وسعة خادم تصفية URL، يمكن أن يكون الوقت المطلوب للاتصال الأولي أبطأ بشكل ملحوظ عندما تتم تصفية حركة المرور باستخدام خادم تصفية خارجي.

ملاحظة: لا يتم دعم تنفيذ التصفية من مستوى أمان أقل إلى مستوى أعلى. تعمل تصفية URL فقط لحركة المرور الصادرة، على سبيل المثال، حركة المرور التي تنشأ على واجهة أمان عالية موجهة لخادم على واجهة أمان منخفضة.

المتطلبات الأساسية

المكونات المستخدمة

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

- جهاز الأمان PIX 500 Series مع الإصدار 6.2 والإصدارات الأحدث
- جهاز الأمان ASA 5500 Series Security Appliance مع الإصدار x.7 والإصدارات الأحدث
- مدير أجهزة حلول الأمان المعدلة (ASDM)، الإصدار 6.0

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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

يمكنك تصفية طلبات الاتصال التي تنشأ من شبكة أكثر أمانا إلى شبكة أقل أمانا. على الرغم من أنه يمكنك إستخدام قوائم التحكم في الوصول (ACL) لمنع الوصول الصادر إلى خوادم المحتوى المحددة، إلا أنه من الصعب إدارة الاستخدام بهذه الطريقة بسبب حجم الإنترنت وطبيعتها الديناميكية. يمكنك تبسيط التهيئة وتحسين أداء أجهزة الأمان باستخدام خادم منفصل يشغل أحد منتجات تصفية الإنترنت التالية:

- WebSense Enterprise — تصفية HTTP و HTTPS و FTP. يتم دعمه بواسطة جدار حماية PIX الإصدار 5.3 والإصدارات الأحدث.
- يعمل SmartFilter للحوسبة الآمنة، المعروف سابقا باسم N2H2—على تصفية HTTP و HTTPS و FTP وتصفية URL الطويلة. يتم دعمه بواسطة جدار حماية PIX الإصدار 6.2 والإصدارات الأحدث.

ومقارنة باستخدام قوائم التحكم في الوصول، فإن ذلك يقلل من المهمة الإدارية ويحسن من فعالية التصفية. أيضا، لأن تصفية URL تتم معالجتها على نظام أساسي منفصل، فإن أداء جدار حماية PIX يكون أقل تأثرا. ومع ذلك، يمكن للمستخدمين ملاحظة أوقات وصول أطول إلى مواقع الويب أو خوادم FTP عندما يكون خادم التصفية بعيدا عن جهاز الأمان.

يتحقق جدار حماية PIX من طلبات URL الصادرة باستخدام النهج المحدد على خادم تصفية URL. يسمح جدار حماية PIX بالاتصال أو يرفضه، استنادا إلى الاستجابة من خادم التصفية.

عند تمكين التصفية وتوجيه طلب للمحتوى عبر جهاز الأمان، يتم إرسال الطلب إلى خادم المحتوى وإلى خادم التصفية في نفس الوقت. إذا كان خادم التصفية يسمح بالاتصال، يقوم جهاز الأمان بإعادة توجيه الاستجابة من خادم المحتوى إلى العميل الذي قام بإنشاء الطلب. إذا رفض خادم التصفية الاتصال، يقوم جهاز الأمان بإسقاط الاستجابة وإرسال رسالة أو رمز إرجاع يشير إلى عدم نجاح الاتصال.

في حالة تمكين مصادقة المستخدم على جهاز الأمان، يرسل جهاز الأمان أيضا اسم المستخدم إلى خادم التصفية. يمكن لخادم التصفية إستخدام إعدادات التصفية الخاصة بالمستخدم أو توفير تقارير محسنة فيما يتعلق بالاستخدام.

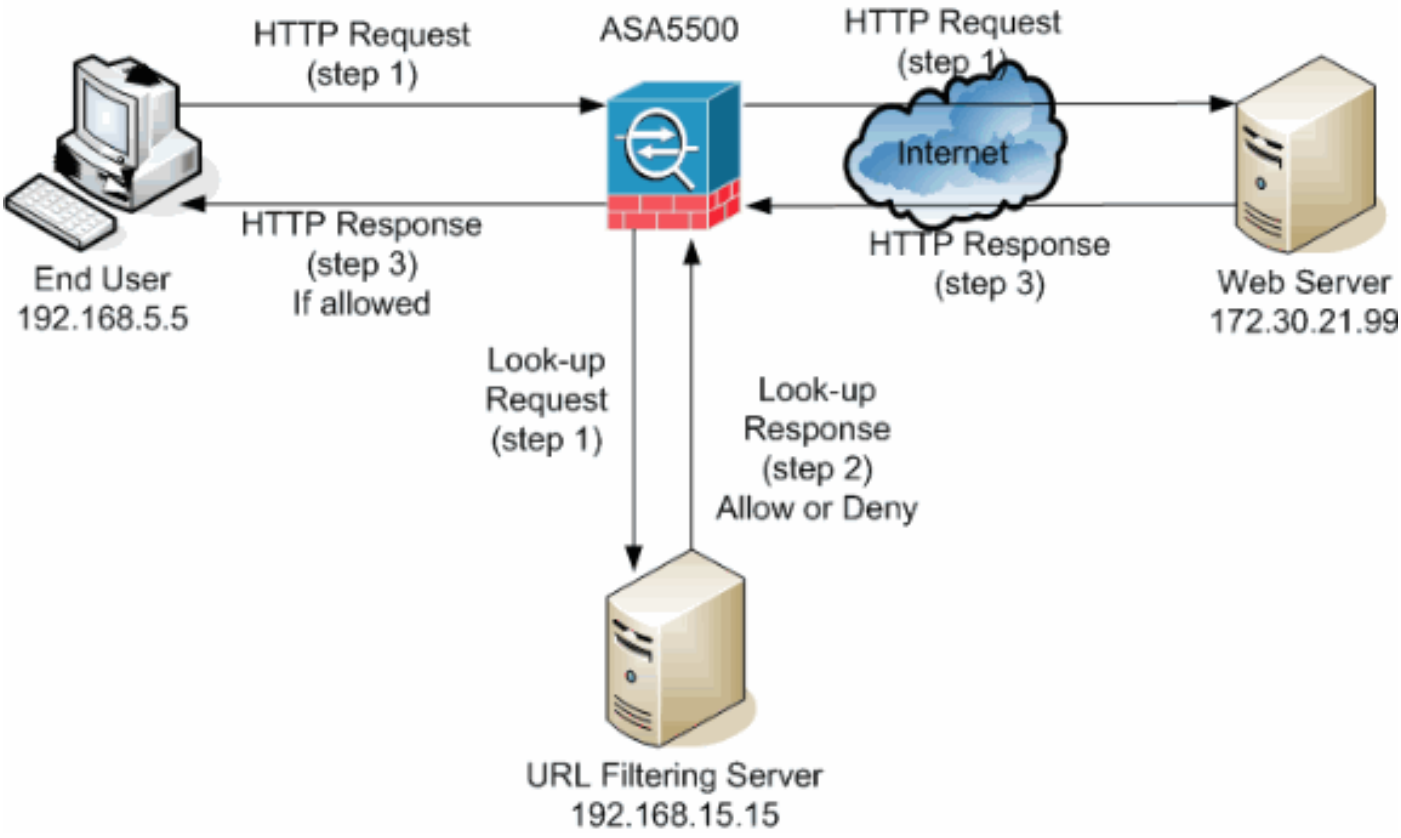
تكوين ASA/PIX باستخدام CLI

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:



في هذا المثال، يقع خادم تصفية URL في شبكة DMZ. يحاول المستخدمون النهائيون الموجودون داخل الشبكة الوصول إلى خادم الويب الموجود خارج الشبكة عبر الإنترنت.

يتم إكمال هذه الخطوات أثناء طلب المستخدم لخادم ويب:

1. يقوم المستخدم النهائي بالتصفح إلى صفحة على خادم ويب، ويقوم المستعرض بإرسال طلب HTTP.
2. بعد أن يتلقى جهاز الأمان هذا الطلب، فإنه يعيد توجيه الطلب إلى خادم ويب ويستخرج في نفس الوقت عنوان الربط ويرسل طلب بحث إلى خادم تصفية URL.
3. بعد أن يتلقى خادم تصفية URL طلب البحث، يتحقق من قاعدة بياناته لتحديد ما إذا كان سيتم السماح بعنوان URL أو رفضه. وهو يرجع حالة السماح أو الرفض باستخدام إستجابة البحث إلى جدار حماية Cisco IOS®.
4. يتلقى جهاز الأمان إستجابة البحث هذه ويقوم بتنفيذ إحدى هذه الوظائف:إذا سمحت إستجابة البحث بعنوان URL، فإنها ترسل إستجابة HTTP إلى المستخدم النهائي.إذا رفضت إستجابة البحث عنوان URL، يقوم خادم تصفية عنوان URL بإعادة توجيه المستخدم إلى خادم ويب الداخلي الخاص به، والذي يعرض رسالة تصف الفئة التي تم حظر عنوان URL تحتها. وبعد ذلك، تتم إعادة تعيين الاتصال على كلا الغرضين.

التعرف على خادم التصفية

يجب تعريف عنوان خادم التصفية باستخدام الأمر **url-server**. يجب إستخدام النموذج المناسب لهذا الأمر استنادا إلى نوع خادم التصفية الذي تستخدمه.

ملاحظة: بالنسبة لإصدار البرنامج x.7 والإصدارات الأحدث، يمكنك تحديد ما يصل إلى أربعة خوادم تصفية لكل سياق. يستخدم جهاز الأمان الخوادم بالترتيب حتى يستجيب الخادم. يمكنك تكوين نوع واحد فقط من الخادم، إما WebSense أو N2H2، في التكوين الخاص بك.

WebSense

WebSense هو برنامج تصفية من جهة خارجية يمكنه تصفية طلبات HTTP على أساس هذه السياسات:

- اسم المضيف الوجهة
- غاية عنوان IP
- الكلمات الأساسية
- اسم المستخدم

ويحتفظ البرنامج بقاعدة بيانات لعنوان URL تتألف من أكثر من 20 مليون موقع منظمة في أكثر من 60 فئة وفئة فرعية.

- إصدار البرنامج 6.2:

```
url-server [(if_name)] vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP}
[version
```

يعين الأمر **url-server** الخادم الذي يشغل تطبيق تصفية N2H2 أو WebSense URL. الحد هو 16 خادم عنوان URL. ومع ذلك، يمكنك إستخدام تطبيق واحد فقط في كل مرة، إما N2H2 أو WebSense. وبالإضافة إلى ذلك، إذا قمت بتغيير التكوين الخاص بك على جدار حماية PIX، فلن يقوم بتحديث التكوين على خادم التطبيق. ويجب أن يتم ذلك بشكل منفصل، استنادا إلى تعليمات المورد الفردي.

- الإصدار x.7 من البرنامج والإصدارات الأحدث:

```
pix(config)# url-server (if_name) host local_ip [timeout seconds] [protocol TCP | UDP
version 1|4
[ [connections num_conns]
```

استبدل `if_name` باسم واجهة جهاز الأمان المتصلة بخادم التصفية. الإعداد الافتراضي موجود بالداخل. استبدلت `local_ip` مع العنوان من التصفية نادل. استبدل بعدد الثواني التي يجب أن يستمر فيها جهاز الأمان في محاولة الاتصال بخادم التصفية.

أستخدم خيار لتحديد ما إذا كنت تريد إستخدام TCP أو UDP. باستخدام خادم WebSense، يمكنك أيضا تحديد TCP الذي تريد إستخدامه. الإصدار 1 من TCP هو الإعداد الافتراضي. يسمح الإصدار 4 من TCP لجدار حماية PIX بإرسال أسماء المستخدمين المصدق عليها ومعلومات تسجيل URL إلى خادم WebSense إذا كان جدار حماية PIX قد قام بمصادقة المستخدم بالفعل.

على سبيل المثال، لتحديد خادم تصفية WebSense واحد، قم بإصدار هذا الأمر:

```
hostname(config)#url-server (DMZ) vendor websense host 192.168.15.15 protocol TCP version 4
```

تقنية SmartFilter للحوسبة الآمنة

- الإصدار PIX 6.2:

```
pix(config)#url-server [(if_name)] vendor n2h2 host local_ip[:port number] [timeout
```

- إصدارات البرامج 7.0 و 7.1:

```
hostname(config)#url-server (if_name) vendor n2h2 host local_ip[:port number] [timeout
```

```
[seconds
[[protocol TCP connections number | UDP [connections num_conns]]
```

- الإصدار 7.2 من البرنامج والإصدارات الأحدث:

```
hostname(config)#url-server (if_name) vendor {secure-computing | n2h2} host
```

بالنسبة {secure-computing | n2h2}، يمكنك إستخدام كسلسلة مورد. ومع ذلك، يعد n2h2 مقبولا للتوافق مع الإصدارات السابقة. عند إنشاء إدخالات التكوين، يتم حفظ كسلسلة المورد.

استبدل if_name باسم واجهة جهاز الأمان المتصلة بخادم التصفية. الإعداد الافتراضي موجود بالداخل. استبدلت _ip مع العنوان من التصفية نادل <number> مع ال مرغوب ميناء رقم.

ملاحظة: المنفذ الافتراضي المستخدم من قبل خادم Secure Computing SmartFilter للاتصال بجهاز الأمان مع TCP أو UDP هو المنفذ 4005.

استبدل بعدد الثواني التي يجب أن يستمر فيها جهاز الأمان في محاولة الاتصال بخادم التصفية. أستخدم خيار لتحديد ما إذا كنت تريد إستخدام TCP أو UDP.

يقصد ب <number> Connections> عدد المرات التي تحاول فيها إجراء اتصال بين المضيف والخادم.

مثلا، أصدرت in order to عينت وحيد N2H2 ييصفي نادل، هذا أمر:

```
hostname(config)#url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol
                                                                                tcp connections 10
```

أو، إذا كنت تريد إستخدام القيم الافتراضية، قم بإصدار هذا الأمر:

```
hostname(config)#url-server (DMZ) vendor n2h2 host 192.168.15.15
```

تكوين نهج التصفية

ملاحظة: يجب تحديد خادم تصفية URL وتمكينه قبل تمكين تصفية URL.

تمكين تصفية URL

عندما يوافق خادم التصفية على طلب اتصال HTTP، يسمح جهاز الأمان بالرد من خادم الويب للوصول إلى العميل الذي قام بإنشاء الطلب. إذا رفض خادم التصفية الطلب، فإن جهاز الأمان يقوم بإعادة توجيه المستخدم إلى صفحة الحظر التي تشير إلى رفض الوصول.

قم بإصدار الأمر **filter url** لتكوين السياسة المستخدمة في تصفية عناوين URL:

- PIX الإصدار 6.2:

```
filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-
                                                                                [block
[longurl-truncate | longurl-deny] [cgi-truncate]
```

- الإصدار x.7 من البرنامج والإصدارات الأحدث:

```
filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-
                                                                                    [block
[longurl-truncate | longurl-deny] [cgi-truncate]
```

استبدلت مع الميناء رقم على أي أن مرشح حركة مرور HTTP إن يكون مختلف ميناء من التقصير ميناء ل HTTP 80)) استعملت. لتحديد نطاق من أرقام المنافذ، أدخل بداية ونهاية النطاق مفصولة بواصلة.

مع تمكين التصفية، يقوم جهاز الأمان بإيقاف حركة مرور HTTP الصادرة حتى يسمح خادم التصفية بالاتصال. في حالة عدم إستجابة خادم التصفية الأساسي، يقوم جهاز الأمان بتوجيه طلب التصفية إلى خادم التصفية الثانوي. يتسبب خيار في قيام جهاز الأمان بإعادة توجيه حركة مرور HTTP دون التصفية عندما يكون خادم التصفية الأساسي غير متوفر.

قم بإصدار الأمر **proxy-block** لإسقاط جميع الطلبات على الخوادم الوكيل.

ملاحظة: يتم إستخدام باقي المعلمات لاقتطاع عناوين URL الطويلة.

اقتطاع عناوين HTTP الطويلة

يتسبب خيار `longurl-trunate` في أن يرسل جهاز الأمان فقط اسم المضيف أو جزء عنوان IP من عنوان URL للتقييم إلى خادم التصفية عندما يكون عنوان URL أطول من الحد الأقصى للطول المسموح به.

أستخدم خيار `longurl-deny` لرفض حركة مرور URL الصادرة إذا كان عنوان URL أطول من الحد الأقصى المسموح به.

أستخدم خيار `cgi-trunate` لاقتطاع عناوين CGI URLs لتضمين موقع برنامج CGI النصي فقط واسم البرنامج النصي بدون أي معلمات.

هذا مثال لتكوين عامل التصفية العام:

```
hostname(config)#filter url http 192.168.5.0 255.255.255.0 172.30.21.99 255.255.255.255 allow
                                proxy-block longurl-truncate cgi-truncate
```

إعفاء حركة المرور من التصفية

إذا كنت تريد إجراء إستثناء لنهج التصفية العامة، قم بإصدار هذا الأمر:

```
[filter url except local_ip local_mask foreign_ip foreign_mask
```

استبدلت `local_ip` و`local_mask` مع عنوان IP وقناع الشبكة الفرعية لمستخدم أو شبكة فرعية تريد أن تستثنيها من قيود التصفية.

استبدلت `foreign_ip` و`foreign_mask` مع عنوان IP وقناع الشبكة الفرعية لخادم أو شبكة فرعية تريد أن تستثنيها من قيود التصفية.

على سبيل المثال، يتسبب هذا الأمر في إعادة توجيه جميع طلبات HTTP إلى 172.30.21.99، من الأجهزة المضيفة

الداخلية، إلى خادم التصفية باستثناء الطلبات من المضيف 192.168.5.5:

هذا مثال تكوين للاستثناء:

```
hostname(config)#filter url except 192.168.5.5 255.255.255.255 172.30.21.99 255.255.255.255
```

تصفية URL المتقدمة

يوفر هذا القسم معلومات حول معلمات التصفية المتقدمة، والتي تتضمن الموضوعات التالية:

- تخزين مؤقت
- تخزين مؤقت
- دعم عنوان URL طويل

تخزين استجابات خادم الويب مؤقتا

عندما يصدر المستخدم طلبا للاتصال بخادم محتوى، يرسل جهاز الأمان الطلب إلى خادم المحتوى وخادم التصفية في نفس الوقت. إذا لم يستجب خادم التصفية قبل خادم المحتوى، سيتم إسقاط إستجابة الخادم. يؤدي هذا إلى تأخير إستجابة خادم الويب من وجهة نظر عميل ويب لأنه يجب على العميل إعادة إصدار الطلب.

إذا قمت بتمكين المخزن المؤقت لاستجابات HTTP، سيتم تخزين الردود من خوادم محتوى الويب مؤقتا وإعادة توجيه الاستجابات إلى العميل الذي يقوم بإجراء الطلب إذا كان خادم التصفية يسمح بالاتصال. وهذا يؤدي إلى منع التأخير الذي يمكن أن يحدث خلاف ذلك.

لتخزين الاستجابات مؤقتا لطلبات HTTP، أكمل الخطوات التالية:

1. لتمكين التخزين المؤقت للاستجابات لطلبات HTTP التي تنتظر إستجابة من خادم التصفية، قم بإصدار هذا الأمر:
   ```
   hostname(config)#url-block block block-buffer-limit
   ```
   استبدلت `block-buffer-limit` مع العدد الأقصى من كتل أن يكون المخزن مؤقتا.
2. لتكوين الحد الأقصى للذاكرة المتوفرة لمخزن URLs المعلق مؤقتا، ولتخزين URLs الطويلة مؤقتا باستخدام WebSense، قم بإصدار هذا الأمر:
   ```
   hostname(config)#url-block url-mempool memory-pool-size
   ```
   استبدل بقيمة من 2 إلى 10240 لتخصيص ذاكرة بحد أقصى من 2 كيلوبايت إلى 10 ميغابايت.

عناوين خادم التخزين المؤقت

بعد وصول المستخدم إلى موقع ما، يمكن لخادم التصفية أن يسمح لجهاز الأمان بتخزين عنوان الخادم مؤقتا لفترة معينة من الوقت، طالما كان كل موقع تتم إستضافته على العنوان ضمن فئة مسموح بها في جميع الأوقات. بعد ذلك، عندما يقوم المستخدم بالوصول إلى الخادم مرة أخرى، أو إذا قام مستخدم آخر بالوصول إلى الخادم، فلن يحتاج جهاز الأمان إلى مراجعة خادم التصفية مرة أخرى.

قم بإصدار الأمر **url-cache** إذا لزم الأمر لتحسين الإنتاجية:

```
hostname(config)#url-cache dst | src_dst size
```

إستبدال بقيمة لحجم ذاكرة التخزين المؤقت ضمن النطاق من 1 إلى 128 (كيلوبايت).

أستخدم الكلمة الأساسية dst لتخزين إدخالات التخزين المؤقت استنادا إلى عنوان وجهة عنوان URL. حدد هذا الوضع إذا قام جميع المستخدمين بمشاركة نفس نهج تصفية URL على خادم WebSense.

أستخدم الكلمة الأساسية src_dst لذاكرة التخزين المؤقت للإدخالات استنادا إلى كل من عنوان المصدر الذي يبدأ طلب URL وكذلك عنوان وجهة URL. حدد هذا الوضع إذا لم يشارك المستخدمون نفس نهج تصفية URL على خادم WebSense.

تمكين تصفية عناوين URL الطويلة

بشكل افتراضي، يعتبر جهاز الأمان عنوان URL ل HTTP عنوان URL طويل إذا كان أكبر من 1159 حرفا. يمكنك زيادة الحد الأقصى للطول المسموح به لعنوان URL واحد باستخدام هذا الأمر:

```
hostname(config)#url-block url-size long-url-size
```

استبدلت url-size- مع الحد الأقصى للحجم بالكيلوبايت لكل URL طويل يتم تخزينه مؤقتا.

على سبيل المثال، تقوم هذه الأوامر بتكوين جهاز الأمان لتصفية URL المتقدمة:

```
hostname(config)#url-block block 10
hostname(config)#url-block url-mempool 2
hostname(config)#url-cache dst 100
hostname(config)#url-block url-size 2
```

التكوين

يتضمن هذا التكوين الأوامر الموضحة في هذا المستند:

تكوين ASA 8.0

```
ciscoasa#show running-config
Saved :
:
(ASA Version 8.0(2
!
hostname ciscoasa
domain-name Security.lab.com
enable password 2kxsYuz/BehvglCF encrypted
no names
dns-guard
!
interface GigabitEthernet0/0
speed 100
duplex full
nameif outside
security-level 0
ip address 172.30.21.222 255.255.255.0
!
interface GigabitEthernet0/1
description INSIDE
nameif inside
security-level 100
ip address 192.168.5.11 255.255.255.0
!
interface GigabitEthernet0/2
```

```
                description LAN/STATE Failover Interface
                                                shutdown
                                                       !
                                interface GigabitEthernet0/3
                                            description DMZ
                                                 nameif DMZ
                                           security-level 50
                     ip address 192.168.15.1 255.255.255.0
                                                       !
                                        interface Management0/0
                                                    no nameif
                                               no security-level
                                                   no ip address
                                                       !
                                passwd 2KFQnbNIdI.2KYOU encrypted
                                 boot system disk0:/asa802-k8.bin
                                                ftp mode passive
                                            clock timezone CST -6
                                clock summer-time CDT recurring
                                    dns server-group DefaultDNS
                                  domain-name Security.lab.com
                          same-security-traffic permit intra-interface




                                             pager lines 20
                                             logging enable
                                   logging buffer-size 40000
                                logging asdm-buffer-size 200
                                   logging monitor debugging
                               logging buffered informational
                                        logging trap warnings
                                   logging asdm informational
                                       logging mail debugging
                             logging from-address aaa@cisco.com
                                                mtu outside 1500
                                                 mtu inside 1500
                                                    mtu DMZ 1500
                                                  no failover
                                   failover lan unit primary
     failover lan interface interface GigabitEthernet0/2
              failover link interface GigabitEthernet0/2
                                no monitor-interface outside
              icmp unreachable rate-limit 1 burst-size 1

                                asdm image disk0:/asdm-602.bin
                                           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 0.0.0.0 172.30.21.244 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
                                   ldap attribute-map tomtom
           dynamic-access-policy-record DfltAccessPolicy

     url-server (DMZ) vendor websense host 192.168.15.15
```

```
timeout 30 protocol TCP version 1 connections 5

url-cache dst 100
aaa authentication ssh console LOCAL
aaa authentication enable console LOCAL
aaa authentication telnet console LOCAL

filter url except 192.168.5.5 255.255.255.255
172.30.21.99 255.255.255.255

filter url http 192.168.5.0 255.255.255.0 172.30.21.99
255.255.255.255 allow
proxy-block longurl-truncate cgi-truncate
http server enable
http 172.30.0.0 255.255.0.0 outside

no snmp-server location
no snmp-server contact
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 60
console timeout 0
management-access inside
dhcpd address 192.168.5.12-192.168.5.20 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
!
service-policy global_policy global
url-block url-mempool 2
url-block url-size 2
url-block block 10
username fwadmin password aDRVKThrSs46pTjG encrypted
privilege 15
prompt hostname context
Cryptochecksum:db208a243faa71f9b3e92491a6ed2105
end :
```

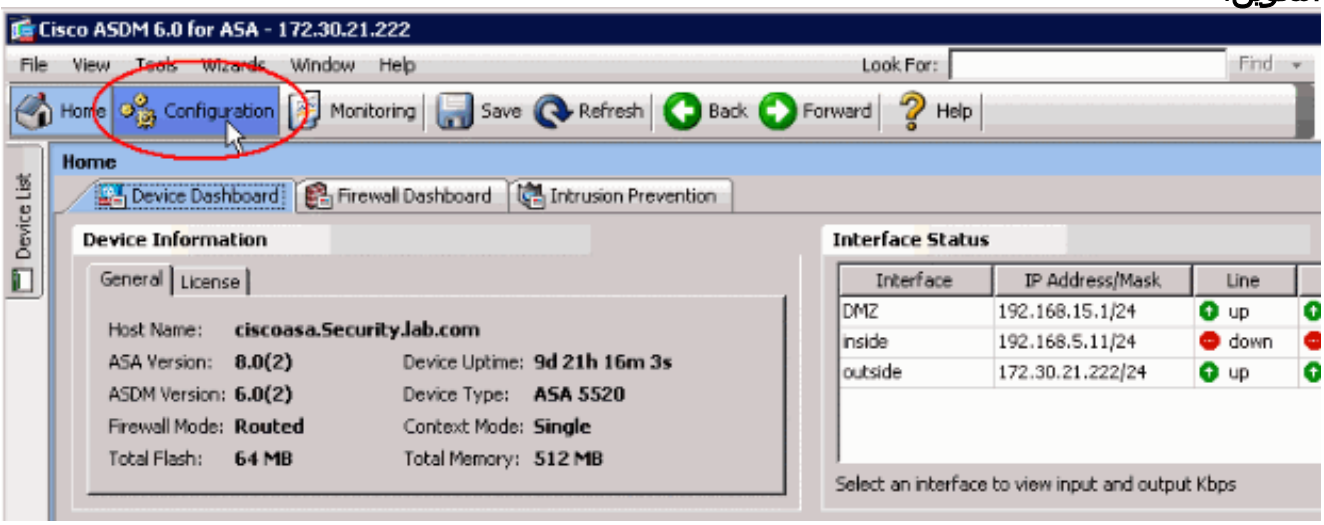
تكوين ASA/PIX باستخدام ASDM

يوضح هذا القسم كيفية تكوين تصفية URL لجهاز الأمان باستخدام Adaptive Security Device Manager

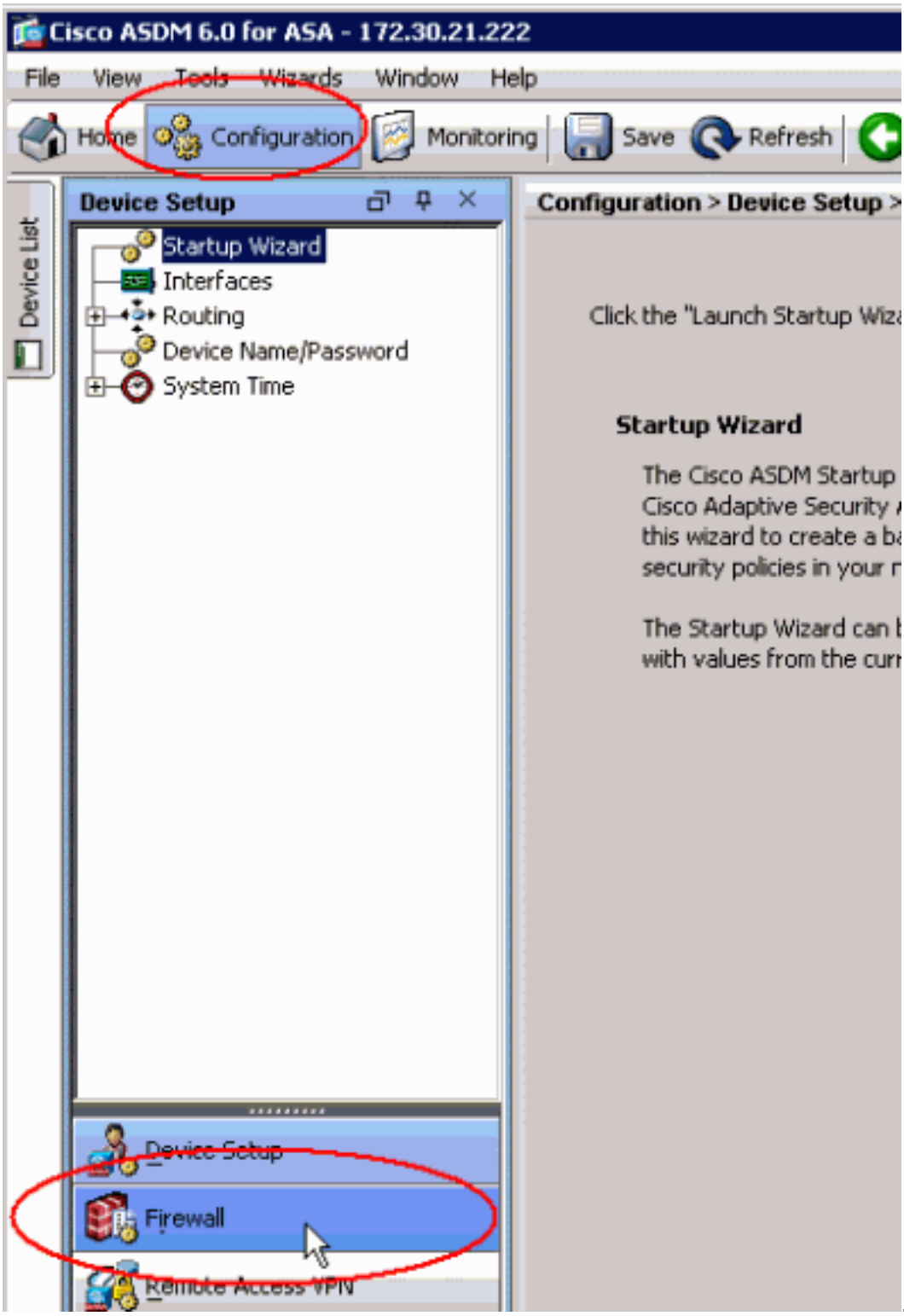
.((ASDM

بعد تشغيل ASDM، أكمل الخطوات التالية:

1. أختر جزء **التكوين**.

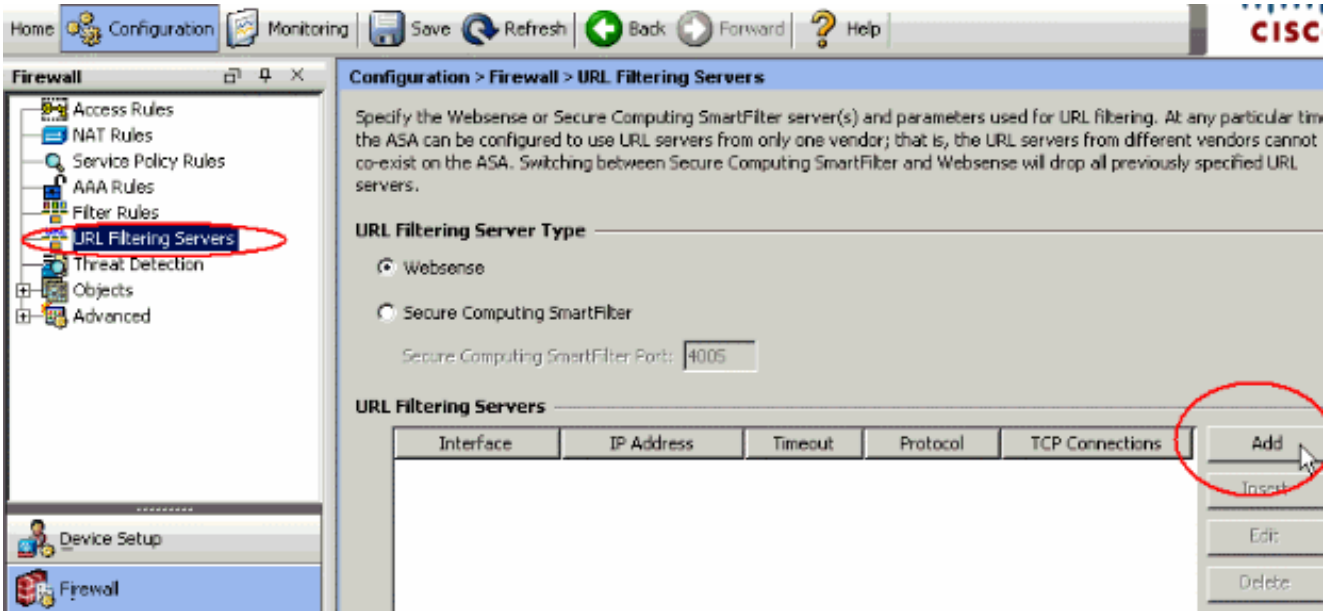


2. انقر فوق **جدار الحماية** في القائمة الموضحة في جزء

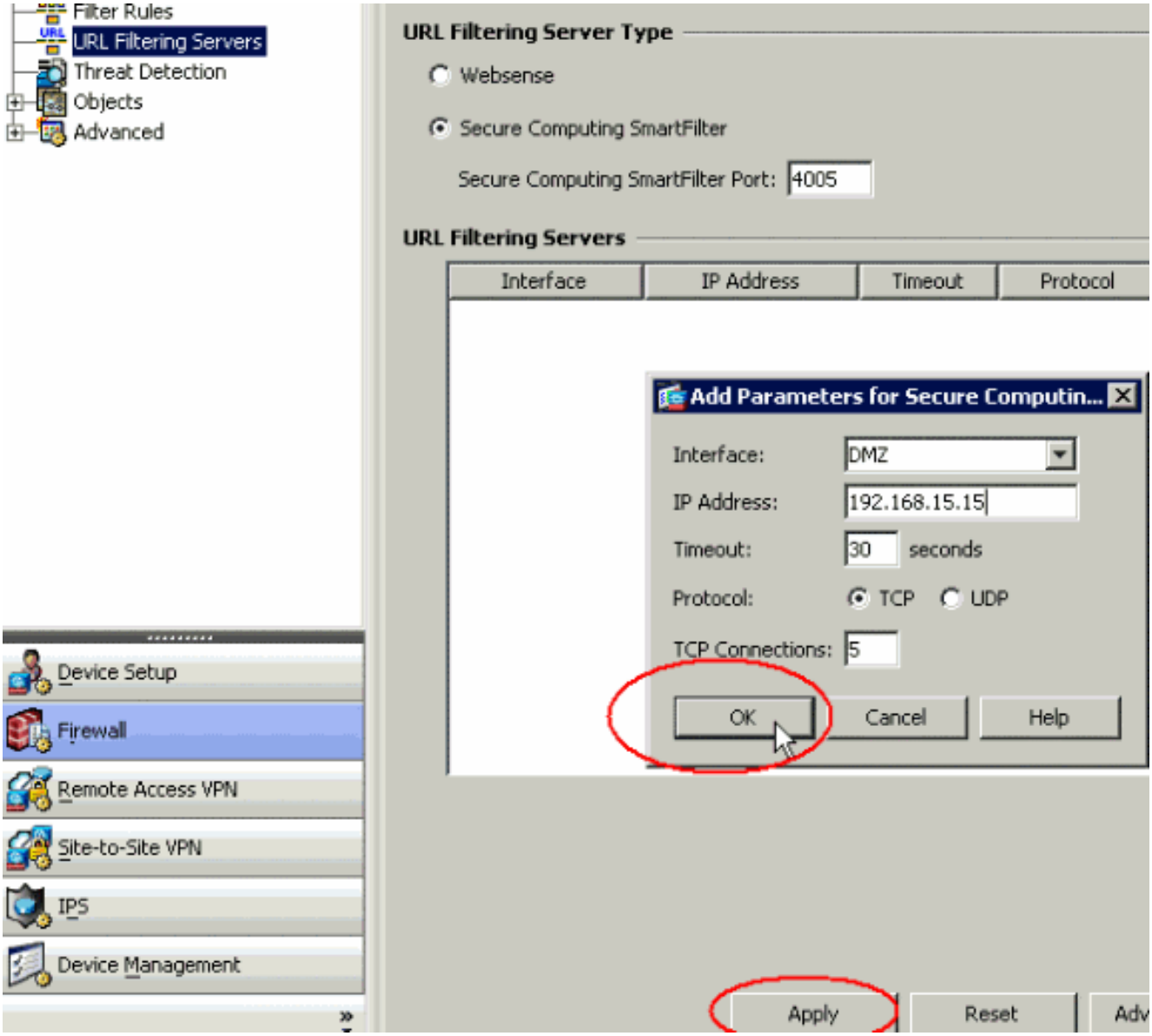


التكوين.

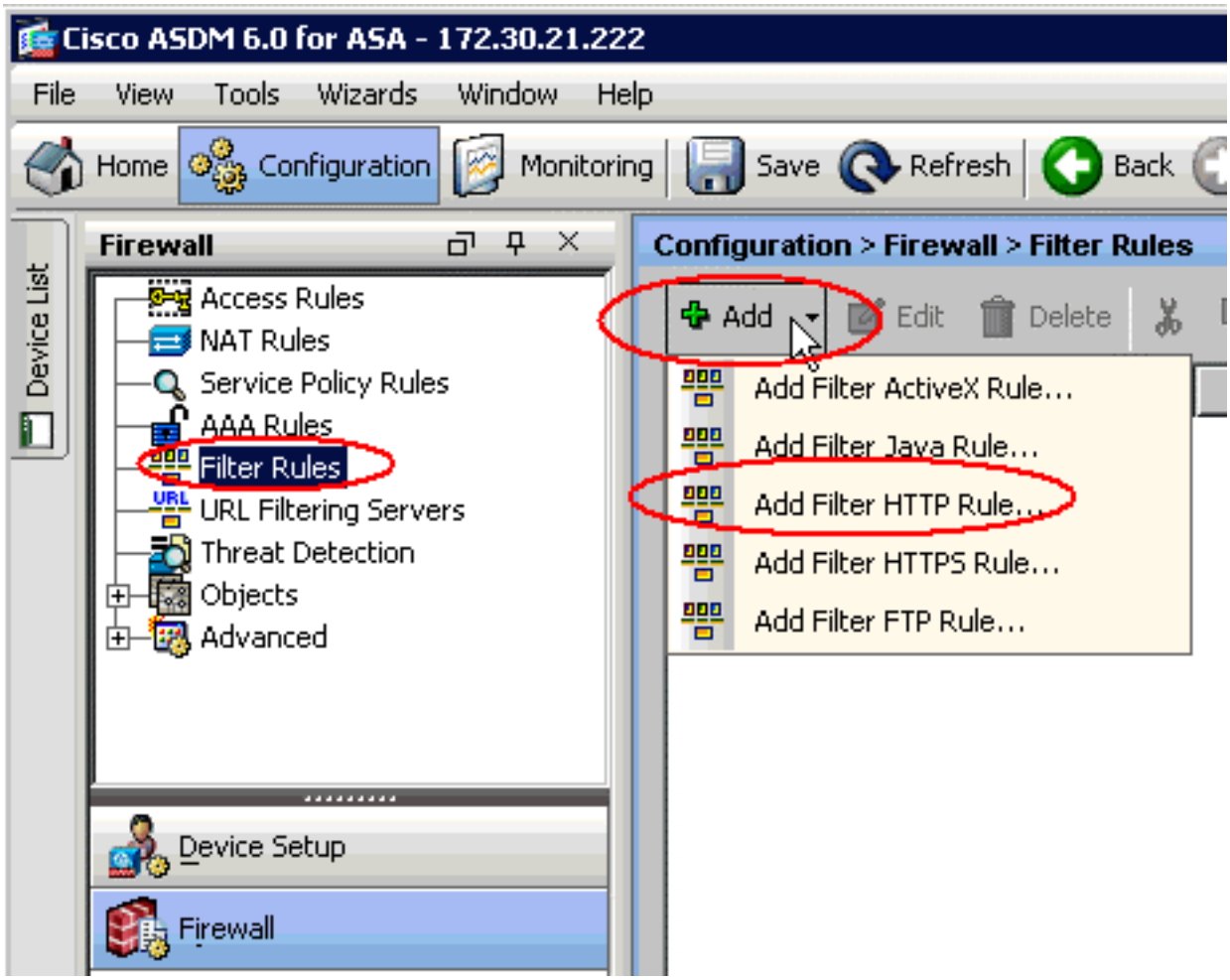
3. من القائمة المنسدلة **جدار الحماية**، أختر **خوادم تصفية URL**. أختر نوع خادم تصفية URL الذي تريد إستخدامه، ثم انقر فوق **إضافة** لتكوين المعلمات الخاصة به.**ملاحظة:** يجب إضافة خادم التصفية قبل تكوين التصفية لقواعد تصفية HTTP أو HTTPS أو FTP.



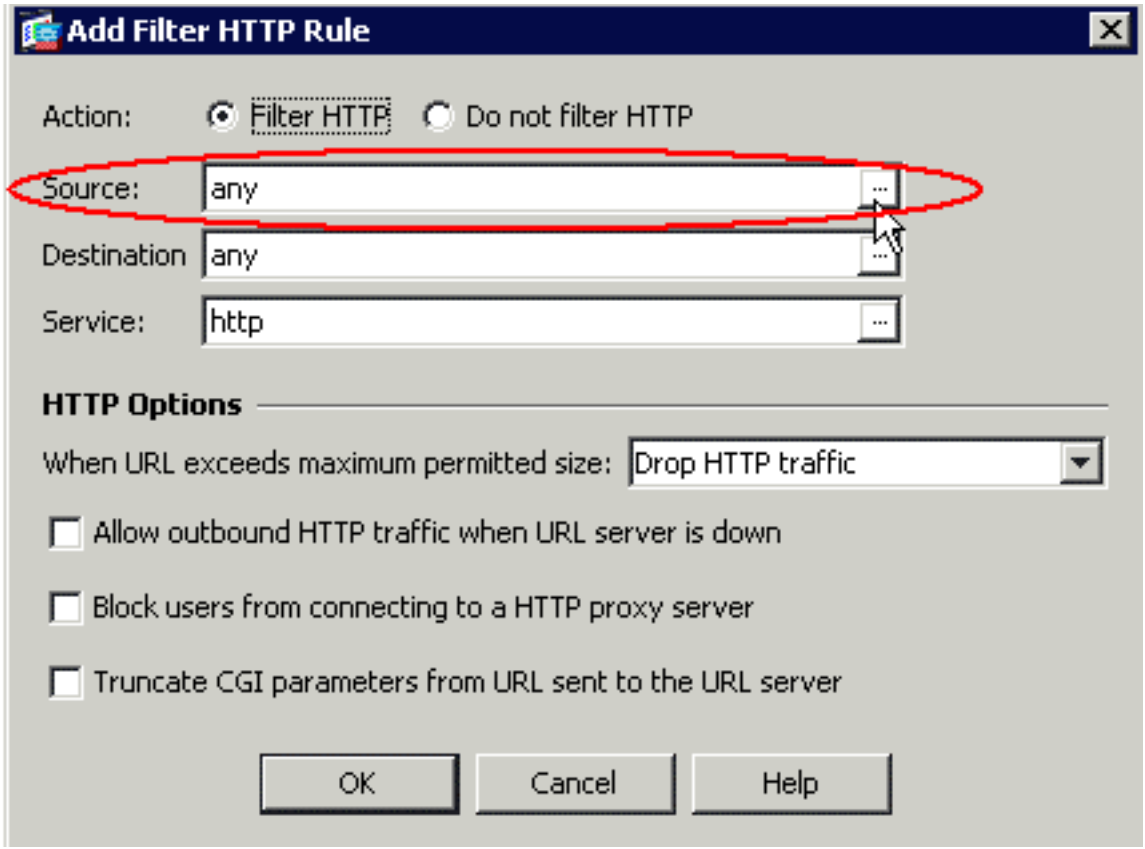
4. أختر المعلمات المناسبة في الإطار المنبثق:الواجهة—يعرض الواجهة المتصلة بخادم التصفيةعنوان IP—يعرض عنوان IP الخاص بخادم التصفيةالمهلة—يعرض عدد الثواني التي انتهت بعدها مهلة الطلب إلى خادم التصفيةالبروتوكول—يعرض البروتوكول المستخدم للاتصال بخادم التصفية. الإصدار 1 من TCP هو الإعداد الافتراضي. يسمح الإصدار 4 من TCP لجدار حماية PIX بإرسال أسماء المستخدمين المصدق عليها ومعلومات تسجيل URL إلى خادم WebSense، إذا كان جدار حماية PIX قد قام بالفعل بمصادقة المستخدمإتصالات TCP—يعرض الحد الأقصى لعدد إتصالات TCP المسموح بها للاتصال بخادم تصفية URLبعد إدخال المعلمات، انقر فوق **موافق** في الإطار المنبثق **وقم بتطبيق** في الإطار الرئيسي.



5. من القائمة المنسدلة **جدار الحماية**، أختر **قواعد التصفية**. انقر فوق الزر **إضافة** في الإطار الرئيسي، واختر نوع القاعدة التي تريد إضافتها. في هذا المثال، يتم إختيار **قاعدة إضافة عامل تصفية HTTP**.

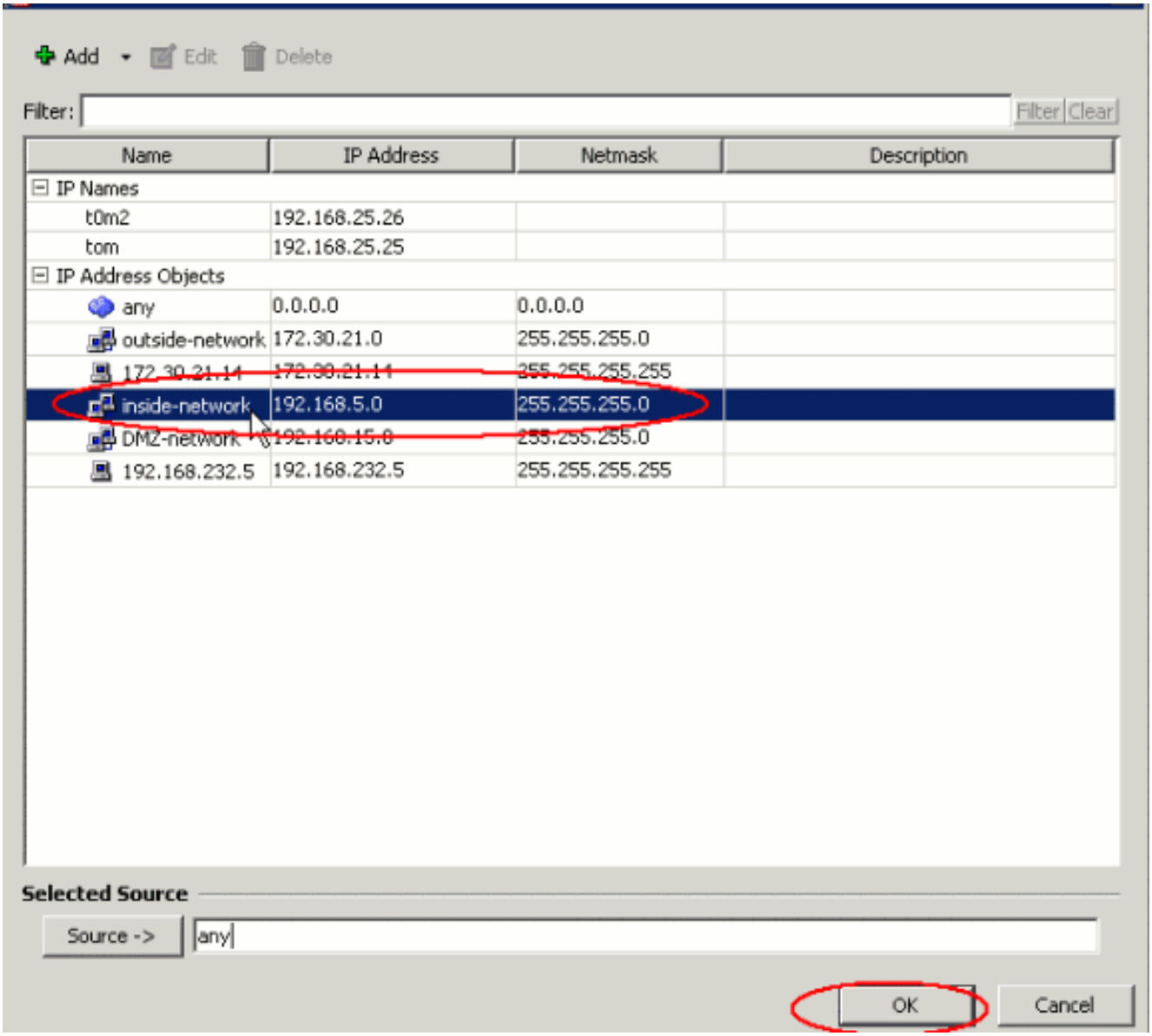


6. بمجرد أن تظهر النافذة المنبثقة، يمكنك النقر فوق أزرار الاستعراض لخيارات **المصدر** و**الوجهة** و**الخدمة** لاختيار المعلمات

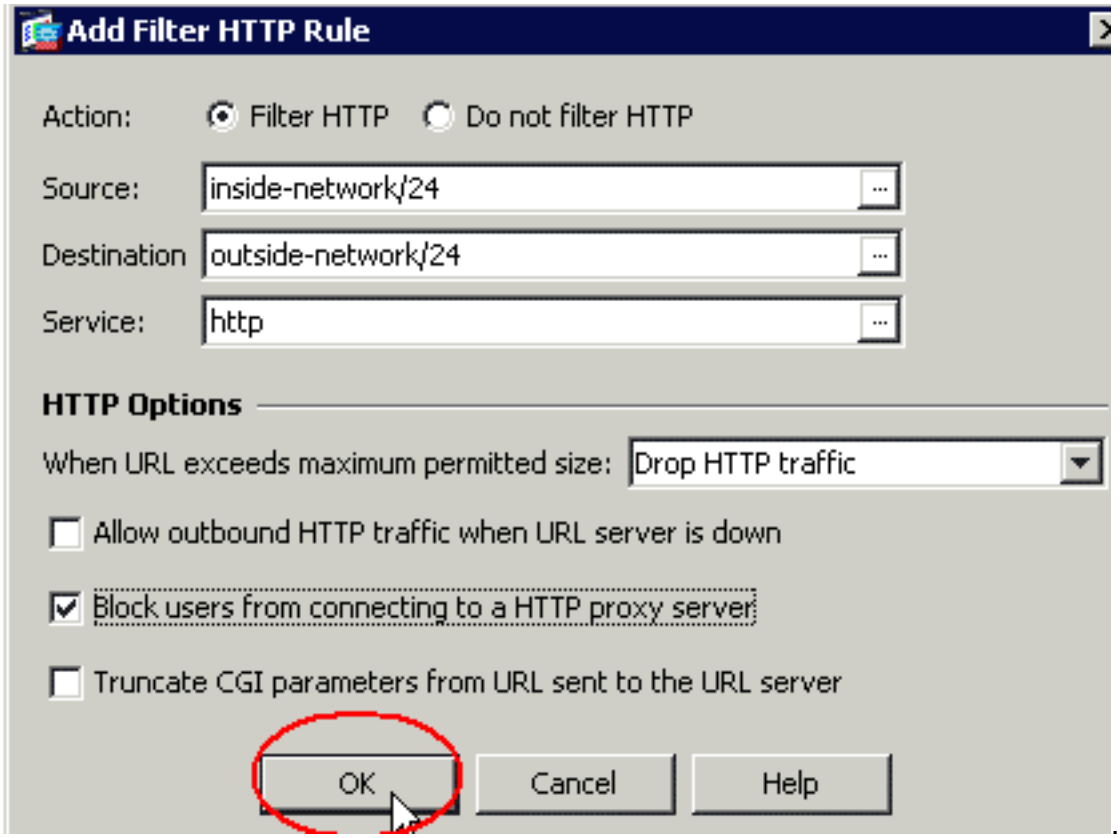


المناسبة.

7. يظهر هذا نافذة الاستعراض لخيار **المصدر**. قم بالتحديد وانقر فوق **OK**.

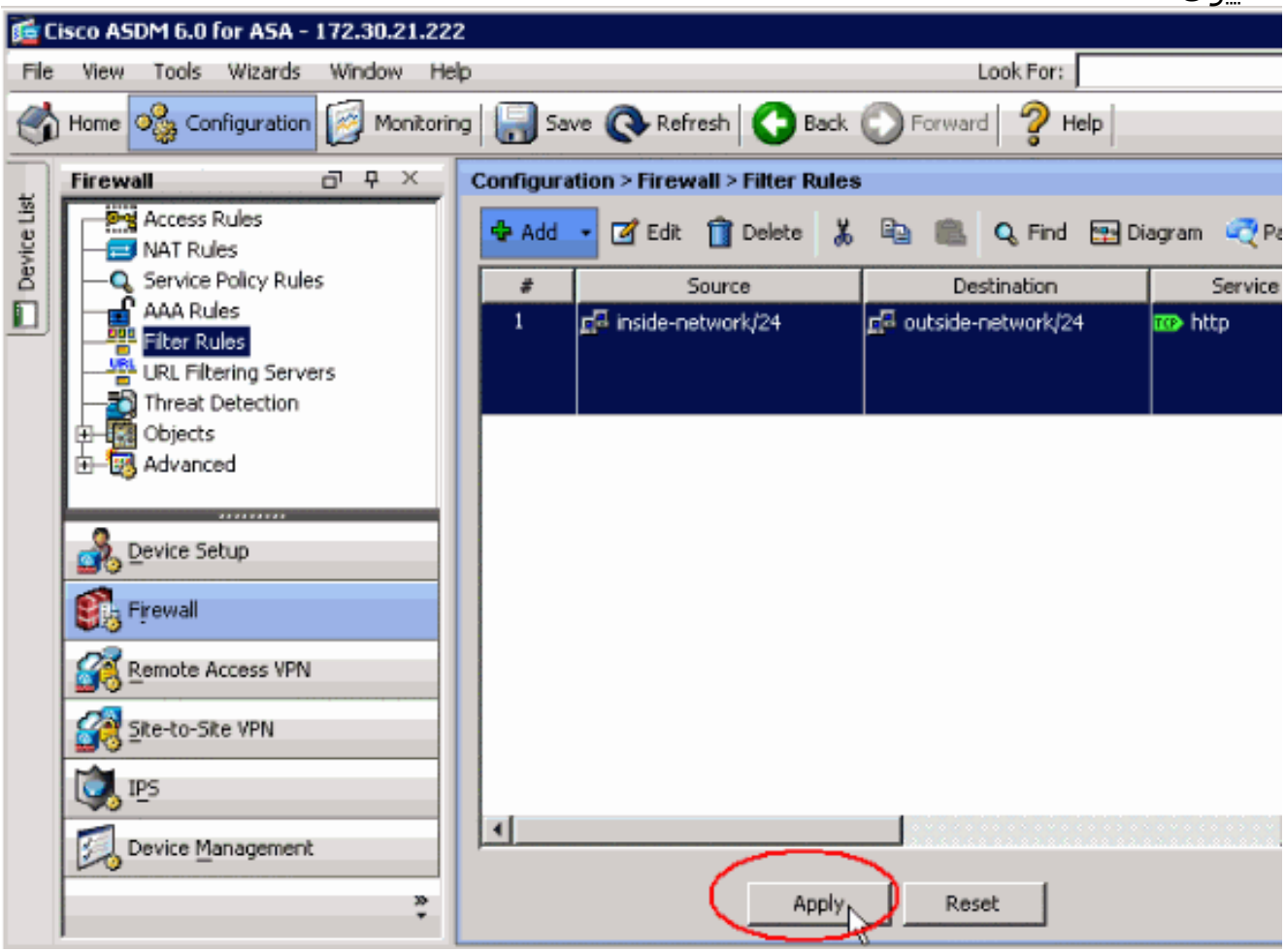


8. بعد إكمال التحديد لكافة المعلمات، انقر فوق **موافق**

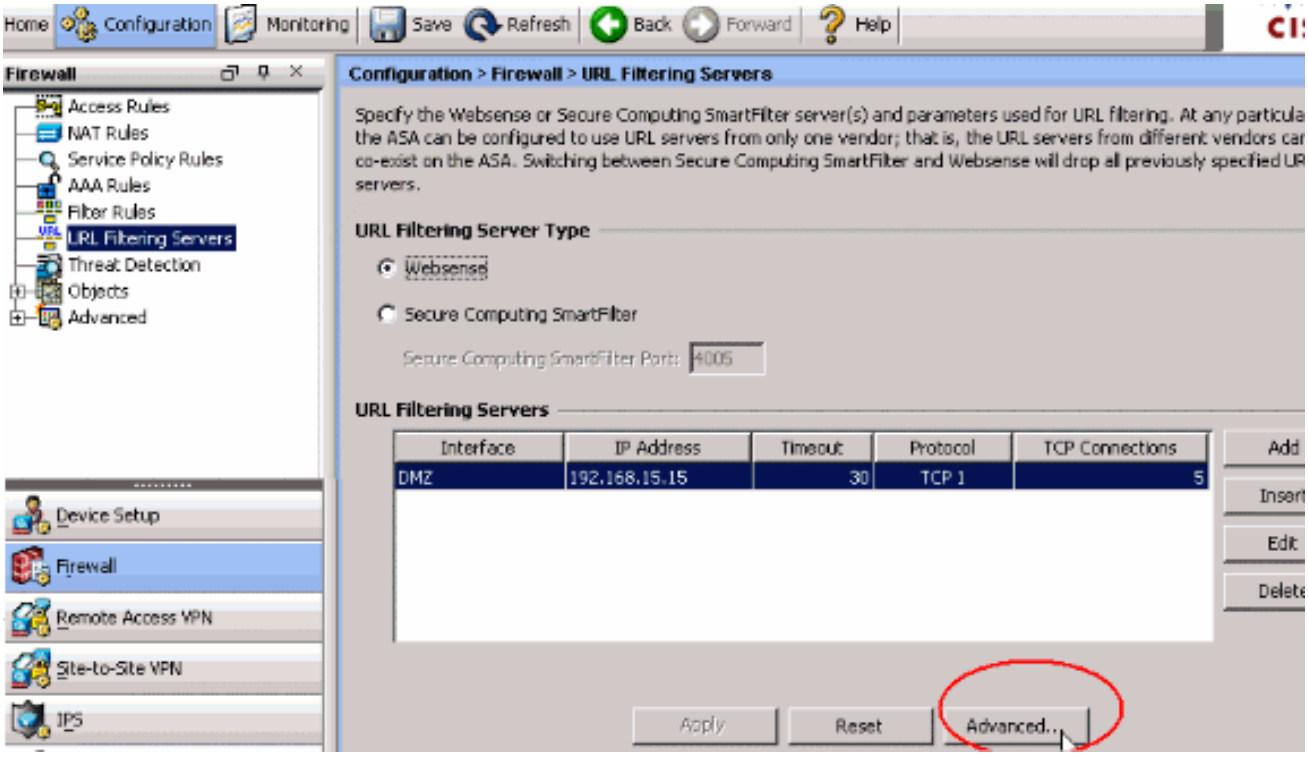


للمتابعة.

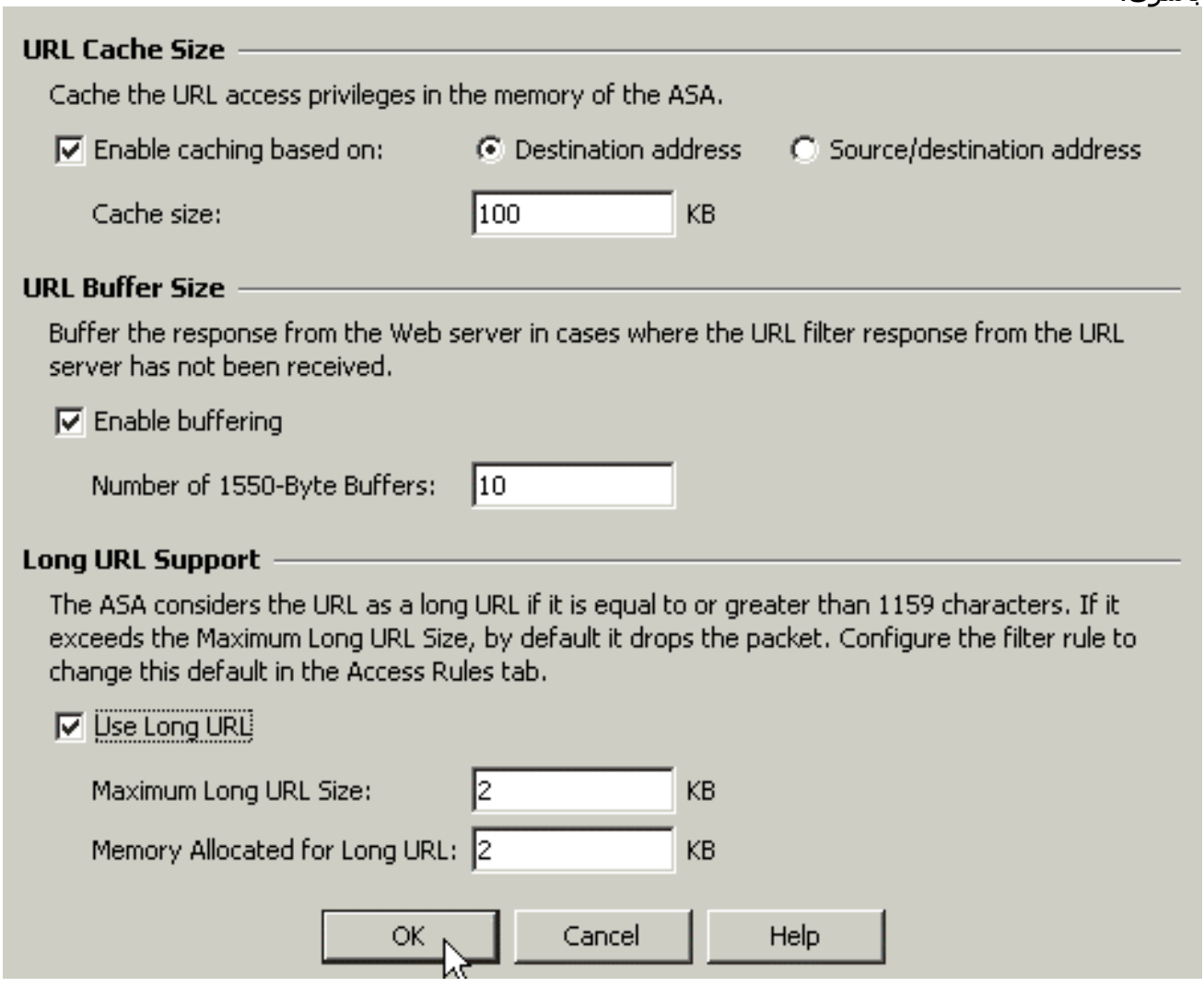
9. بمجرد تكوين المعلمات المناسبة، انقر فوق **تطبيق** لإرسال التغييرات.



10. لخيارات تصفية URL المتقدمة، أختر **خوادم تصفية URL** مرة أخرى من القائمة المنسدلة **جدار الحماية**، وانقر فوق الزر **خيارات متقدمة** في الإطار الرئيسي.



11. قم بتكوين المعلمات، مثل حجم ذاكرة التخزين المؤقت لعنوان URL وحجم المخزن المؤقت لعنوان URL ودعم عنوان URL الطويل، في النافذة المنبثقة. طقطقة **ok** في النافذة منبثقة، وطقطقة **يطبق** في النافذة رئيسي in order to
باشرت.



12. أخيرا، تأكد من حفظ التغييرات التي تقوم بها قبل إنهاء جلسة ASDM.

التحقق من الصحة

استعملت الأمر في هذا قسم in order to شاهدت url يبصفي معلومة. يمكنك إستخدام هذه الأوامر للتحقق من التكوين الخاص بك.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

- **show url-server**—يعرض معلومات حول خادم التصفيةعلى سبيل المثال:

```
hostname#show url-server
url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp
                                                                connections 10
```

في الإصدار 7.2 من البرنامج والإصدارات الأحدث، قم بإصدار نموذج **show running-config url-server** لهذا الأمر.

- **إظهار إحصائيات خادم url**—يعرض المعلومات والإحصائيات حول خادم التصفيةبالنسبة لإصدار البرنامج 7.2، قم بإصدار نموذج **إحصائيات show running-config url-server** لهذا الأمر.في الإصدار 8.0 من البرنامج والإصدارات الأحدث، قم بإصدار نموذج **إحصائيات show url-server** لهذا الأمر.على سبيل المثال:

```
hostname#show url-server statistics

                                    :Global Statistics
                                  --------------------
                  URLs total/allowed/denied         13/3/10
                      URLs allowed by cache/server      0/3
                     URLs denied by cache/server       0/10
                HTTPSs total/allowed/denied       138/137/1
                    HTTPSs allowed by cache/server    0/137
                      HTTPSs denied by cache/server     0/1
                    FTPs total/allowed/denied         0/0/0
                      FTPs allowed by cache/server      0/0
                      FTPs denied by cache/server       0/0
                        Requests dropped                  0
                      Server timeouts/retries           0/0
Processed rate average 60s/300s   0/0 requests/second
Denied rate average 60s/300s      0/0 requests/second
Dropped rate average 60s/300s     0/0 requests/second

                                    :Server Statistics
                                  --------------------
                           UP                     192.168.15.15
                  Vendor                             websense
                     Port                               15868
               Requests total/allowed/denied   151/140/11
                     Server timeouts/retries          0/0
                     Responses received               151
                     Response time average 60s/300s  0/0

                      :URL Packets Sent and Received Stats
                      ------------------------------------
                 Message                 Sent    Received
                     STATUS_REQUEST          1609    1601
                     LOOKUP_REQUEST          1526    1526
                       LOG_REQUEST             0       NA

                                                 :Errors
                                                 -------
                        RFC noncompliant GET method     0
                        URL buffer update failure       0
```

- **show url-block**—يعرض تكوين المخزن المؤقت لكتلة عنوان URLعلى سبيل المثال:

```
hostname#show url-block
url-block url-mempool 128
     url-block url-size 4
      url-block block 128
```

في الإصدار 7.2 من البرنامج والإصدارات الأحدث، قم بإصدار نموذج **show running-config url-block** لهذا الأمر.

- **إظهار إحصائيات كتلة عنوان URL**—يعرض إحصائيات كتلة عنوان URLعلى سبيل المثال:

```
hostname#show url-block block statistics

  URL Pending Packet Buffer Stats with max block  128
-----------------------------------------------------
  Cumulative number of packets held:              896
    Maximum number of packets held (per URL):       3
   Current number of packets held (global):        38
                                Packets dropped due to
 exceeding url-block buffer limit:        7546
   HTTP server retransmission:              10
    Number of packets released back to client:      0
```

بالنسبة لإصدار البرنامج 7.2، قم بإصدار نموذج **إحصائيات كتل كتل** show running-config **url** لهذا الأمر.

- **إظهار إحصائيات ذاكرة التخزين المؤقت لعنوان url**—يعرض كيفية إستخدام ذاكرة التخزين المؤقتعلى سبيل المثال:

```
hostname#show url-cache stats

        URL Filter Cache Stats
        ----------------------
          Size :     128KB
          Entries :      1724
          In Use :       456
          Lookups :        45
          Hits :         8
```

في إصدار البرنامج 8.0، قم بإصدار نموذج **إحصائيات show url-cache** لهذا الأمر.

- **إظهار Perfmon**—يعرض إحصائيات أداء تصفية URL، بالإضافة إلى إحصائيات الأداء الأخرى. يتم عرض إحصائيات التصفية في صفوف Req الخاصة ب URL للوصول و URL Server.على سبيل المثال:

```
hostname#show perfmon

PERFMON STATS:    Current       Average
 Xlates               0/s           0/s
 Connections          0/s           2/s
 TCP Conns            0/s           2/s
 UDP Conns            0/s           0/s
 URL Access           0/s           2/s
 URL Server Req       0/s           3/s
 TCP Fixup            0/s           0/s
 TCPIntercept         0/s           0/s
 HTTP Fixup           0/s           3/s
 FTP Fixup            0/s           0/s
 AAA Authen           0/s           0/s
 AAA Author           0/s           0/s
 AAA Account          0/s           0/s
```

- **show filter** — يعرض تكوين التصفيةعلى سبيل المثال:

```
hostname#show filter
```

```
filter url http 192.168.5.5 255.255.255.255 172.30.21.99 255.255.255.255 allow proxy-block
longurl-truncate cgi-truncate
```

في الإصدار 7.2 من البرنامج والإصدارات الأحدث، قم بإصدار نموذج **عامل تصفية show running-config** لهذا الأمر.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات حول كيفية أستكشاف أخطاء التكوين وإصلاحها.

خطأ: "ASA-3-304009: نفدت كتل المخزن المؤقت المحددة بواسطة أمر كتلة url"

ينفذ جدار الحماية من ذاكرة التخزين المؤقت لعنوان URL التي يقصد بها الاحتفاظ بردود الخادم عندما ينتظر جدار الحماية الحصول على تأكيد من خادم URL.

الحل

تتعلق المشكلة بشكل أساسي بزمن انتقال بين ASA وخادم WebSense. لحل هذه المشكلة، جرب هذه الحلول البديلة.

- حاول تغيير البروتوكول الذي يتم إستخدامه على ASA إلى UDP للاتصال ب WebSense.توجد مشكلة تتعلق بزمن الوصول بين خادم WebSense وجدار الحماية، حيث تستغرق الردود من خادم WebSense وقتا طويلا للعودة إلى جدار الحماية، وبالتالي يتسبب هذا في امتلاء مخزن URL المؤقت أثناء انتظار الاستجابة.يمكنك إستخدام UDP بدلا من TCP للاتصال بين خادم WebSense وجدار الحماية. وذلك لأنك عند إستخدام بروتوكول TCP لتصفية عنوان URL، لكل طلب عنوان URL جديد، يحتاج ASA إلى إنشاء اتصال TCP بخادم WebSense. بما أن UDP هو بروتوكول لا اتصال، فلا يتم فرض إنشاء الاتصال على ASA لتلقي إستجابة الخادم. يجب أن يؤدي ذلك إلى تحسين أداء الخادم.
```
ASA(config)#url-server (inside) vendor websense host  X.X.X.X timeout 30
protocol UDP version 4 connections 5
```
- تأكد من زيادة كتلة عنوان URL إلى أعلى قيمة ممكنة، وهي 128. يمكن التحقق من هذا باستخدام الأمر **show url-block**.إن يبدي هو 128، يأخذ cisco بق CSCta27415 id (يسجل **زبون فقط**) تحسين بعين الاعتبار.

معلومات ذات صلة

- دعم منتجات أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco
- دعم منتجات أمان سلسلة PIX 500 من Cisco
- دعم منتجات مدير أجهزة حلول الأمان المعدلة من Cisco
- PIX/ASA: إنشاء الاتصال واستكشاف أخطائه وإصلاحها من خلال جهاز الأمان من Cisco
- أستكشاف أخطاء الاتصالات وإصلاحها من خلال PIX و ASA
- 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).