SDM: تصفية عنوان URL على مثال تكوين موجه Cisco IOS

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين تصفية URL على موجه Cisco IOS. توفر تصفية URL قدرا أكبر من التحكم في حركة المرور التي تمر عبر موجه Cisco IOS. يتم دعم تصفية عنوان URL في إصدارات Cisco IOS في الإصدار 12.2(11)YU والإصدارات الأحدث.

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

المتطلبات الأساسية

قيود تصفية URL الخاص بإستشعار WebSENSE لجدار الحماية

متطلبات خادم WebSense: لتمكين هذه الميزة، يجب أن يكون لديك خادم WebSense واحد على الأقل، ولكن يفضل خادمين أو أكثر من خوادم WebSense. على الرغم من عدم وجود حد لعدد خوادم WebSense التي يمكنك الحصول عليها، ويمكنك تكوين العديد من الخوادم كما تريد، يمكن لخادم واحد فقط أن يكون نشطا في أي وقت - وهو الخادم الأساسي. يتم إرسال طلبات البحث عن عنوان URL إلى الخادم الأساسي فقط.

قيد دعم تصفية URL: تدعم هذه الميزة نظام تصفية URL نشط واحد فقط في كل مرة. (قبل تمكين تصفية URL الخاص ب WebSense، يجب دائما التأكد من عدم تكوين مخطط تصفية URL آخر، مثل N2H2.)

تقييد اسم المستخدم: لا تقوم هذه الميزة بتمرير معلومات اسم المستخدم والمجموعة إلى خادم WebSense، ولكن يمكن لخادم WebSense العمل للسياسات المستندة إلى المستخدم لأنه يحتوي على آلية أخرى لتمكين اسم المستخدم ليتوافق مع عنوان IP.

المكونات المستخدمة

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

- cisco 2801 مسحاج تخديد مع cisco ios ® برمجية إطلاق T(15)12.4
- Cisco Security Device Manager (SDM)، الإصدار 2.5

ملاحظة: ارجع إلى تكوين الموجه الأساسي باستخدام SDM للسماح بتكوين الموجه بواسطة SDM.

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

تتيح ميزة تصفية عنوان URL الخاص بإستشعار الويب لجدار حماية Cisco IOS (المعروف أيضا باسم برنامج Cisco [Secure Integrated Software CSIS]) التفاعل مع برنامج تصفية عنوان URL الخاص بميزة WebSense. يسمح لك هذا بمنع وصول المستخدم إلى مواقع ويب محددة على أساس بعض النهج. يعمل جدار حماية Cisco IOS مع خادم WebSense لمعرفة ما إذا كان يمكن السماح بعنوان URL معين أو رفضه (حظره).

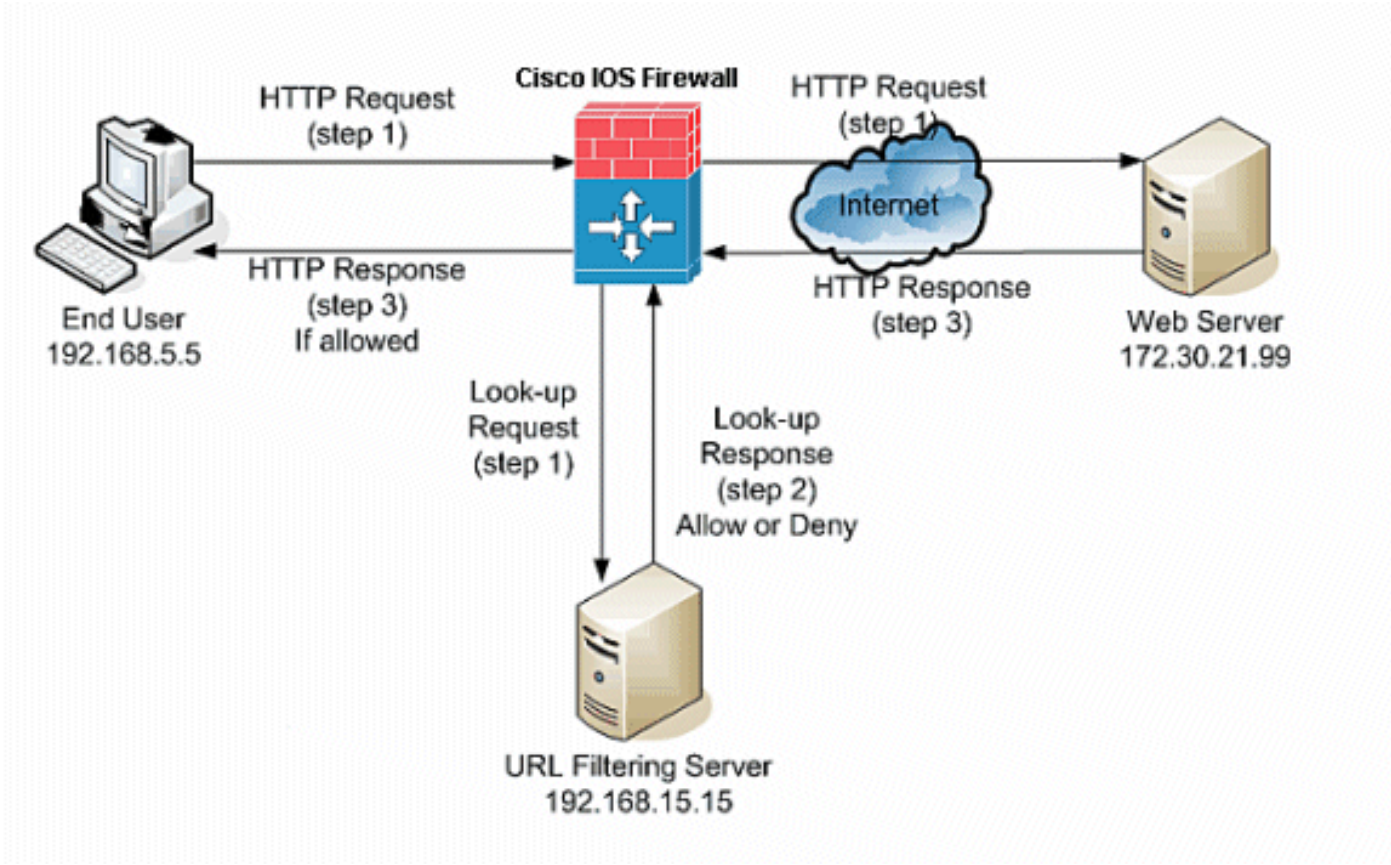
تكوين الموجه باستخدام CLI (واجهة سطر الأوامر)

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، يوجد خادم تصفية URL في الشبكة الداخلية. يحاول المستخدمون النهائيون الموجودون داخل الشبكة الوصول إلى خادم الويب الموجود خارج الشبكة عبر الإنترنت.

يتم إكمال هذه الخطوات بناء على طلب المستخدم لخادم ويب:

1. يقوم المستخدم النهائي بالتصفح إلى صفحة على خادم ويب، ويقوم المستعرض بإرسال طلب HTTP.
2. بعد أن يستقبل جدار حماية Cisco IOS هذا الطلب، فإنه يعيد توجيه الطلب إلى خادم الويب. يستخرج في نفس الوقت عنوان الربط ويرسل طلب بحث إلى خادم تصفية عنوان 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 جدار حماية Cisco IOS® إستجابة البحث هذه ويقوم بتنفيذ إحدى الوظائف التالية: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

تحتاج إلى تعريف عنوان خادم التصفية باستخدام الأمر **ip urlFilter server vendor**. يجب إستخدام النموذج المناسب لهذا الأمر استنادا إلى نوع خادم التصفية الذي تستخدمه.

ملاحظة: 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.

يعين أمر **ip urlFilter server vendor** الخادم الذي يشغل تطبيق تصفية N2H2 أو WebSense URL. لتكوين خادم مورد لتصفية URL، أستخدم الأمر **ip urlFilter server vendor** في وضع التكوين العام. لإزالة خادم من التكوين الخاص بك، أستخدم الصيغة no من هذا الأمر. هذه هي الصياغة الخاصة بالأمر **ip urlFilter server vendor**:

```
hostname(config)# ip urlfilter server vendor
[websense | n2h2} ip-address [port port-number}
[timeout seconds] [retransmit number] [outside] [vrf vrf-name]
```

استبدلت مع العنوان من WebSense نادل. استبدل بعدد الثواني التي يجب أن يستمر فيها جدار حماية IOS في محاولة الاتصال بخادم التصفية.

على سبيل المثال، لتكوين خادم تصفية WebSense واحد لتصفية URL، قم بإصدار هذا الأمر:

```
#(hostname(config
ip urlfilter server vendor websense 192.168.15.15
```

تكوين نهج التصفية

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

اقتطاع عناوين HTTP الطويلة

للسماح لعامل تصفية عنوان URL باقتطاع عناوين URL طويلة إلى الخادم، أستخدم الأمر ip urlfilter trunate في وضع التكوين العام. لتعطيل خيار الاقتطاع، أستخدم الصيغة no من هذا الأمر. يتم دعم هذا الأمر في الإصدار T(6)12.4 من Cisco IOS والإصدارات الأحدث.

`{ip urlFilter trunate {script-parameters | hostname` هي صياغة هذا الأمر.

معلمات البرنامج النصي: يتم إرسال عنوان URL حتى خيارات البرنامج النصي فقط. على سبيل المثال، إذا كان عنوان URL بأكمله هو `http://www.cisco.com/dev/xxx.cgi?when=now`، فإنه يتم إرسال عنوان URL فقط عبر `http://www.cisco.com/dev/xxx.cgi` (إذا لم يتم تجاوز الحد الأقصى لطول عنوان URL المعتمد).

hostname: يتم إرسال اسم المضيف فقط. على سبيل المثال، إذا كان عنوان URL بأكمله هو `http://www.cisco.com/dev/xxx.cgi?when=now`، فإنه يتم إرسال `http://www.cisco.com` فقط.

إذا تم تكوين كل من معلمات البرنامج النصي وكلمات Hostname للكلمات الأساسية، فالكلمة الأساسية script-parameters تكون لها الأولوية على الكلمة الأساسية hostname. إذا تم تكوين كلا الكلمتين الأساسيتين وتم اقتطاع عنوان URL لمعلمات البرنامج النصي وتجاوز الحد الأقصى لطول عنوان URL المعتمد، يتم اقتطاع عنوان URL حتى اسم المضيف.

ملاحظة: إذا تم تكوين كل من معلمات البرنامج النصي للكلمات الأساسية واسم المضيف، فيجب أن يكونا على أسطر منفصلة كما هو موضح أدناه. لا يمكن تجميعها في سطر واحد.

ملاحظة: `ip urlfilter trunate script-parameters`

ملاحظة: IP URLFILTER

تكوين الموجه الذي يشغل برنامج Cisco IOS، الإصدار 12.4

يتضمن هذا التكوين الأوامر الموضحة في هذا المستند:

تكوين الموجه الذي يشغل برنامج Cisco IOS، الإصدار 12.4

```
R3#show running-config
Saved :
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
!
username cisco123 privilege 15 password 7 ---!
104D000A061843595F
!
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
ip ips sdf location flash://128MB.sdf
ip ips notify SDEE
ip ips po max-events 100

use the ip inspect name command in global ---!
configuration mode to define a set of inspection rules.
This Turns on HTTP inspection. The urlfilter keyword
.associates URL filtering with HTTP inspection

ip inspect name test http urlfilter


use the ip urlfilter allow-mode command in global ---!
configuration mode to turn on the default mode (allow
.mode) of the filtering algorithm

ip urlfilter allow-mode on


use the ip urlfilter exclusive-domain command in ---!
global configuration mode to add or remove a domain name
to or from the exclusive domain list so that the
firewall does not have to send lookup requests to the
vendor server. Here we have configured the IOS firewall
to permit the URL www.cisco.com without sending any
.lookup requests to the vendor server

ip urlfilter exclusive-domain permit www.cisco.com


use the ip urlfilter audit-trail command in global ---!
configuration mode to log messages into the syslog
.server or router
```

```
                                        ip urlfilter audit-trail


    use the ip urlfilter urlf-server-log command in ---!
      global configuration mode to enable the logging of
            .system messages on the URL filtering server

                                      ip urlfilter urlf-server-log


       use the ip urlfilter server vendor command in ---!
     global configuration mode to configure a vendor server
      for URL filtering. Here we have configured a websense
       server for URL filtering ip urlfilter server vendor
                                          websense 192.168.15.15
                                    no ftp-server write-enable
                                                             !
                                                             !
     Below is the basic interface configuration on the ---!
     router interface FastEthernet0 ip address 192.168.5.10
        255.255.255.0 ip virtual-reassembly !--- use the ip
    inspect command in interface configuration mode to apply
       a set of inspection rules to an interface. Here the
          inspection name TEST is applied to the interface
                          FastEthernet0. ip inspect test in
                                                 duplex auto
                                                  speed auto
                                                             !
                                       interface FastEthernet1
                     ip address 192.168.15.1 255.255.255.0
                                        ip virtual-reassembly
                                                 duplex auto
                                                  speed auto
                                                             !
                                       interface FastEthernet2
                   ip address 10.77.241.109 255.255.255.192
                                        ip virtual-reassembly
                                                 duplex auto
                                                  speed auto
                                                             !
                                       interface FastEthernet2
                                                no ip address
                                                             !


                                                interface Vlan1
                   ip address 10.77.241.111 255.255.255.192
                                        ip virtual-reassembly
                                                             !
                                                  ip classless
                ip route 10.10.10.0 255.255.255.0 172.17.1.2
                 ip route 10.77.0.0 255.255.0.0 10.77.241.65
                                                             !
                                                             !
     Configure the below commands to enable SDM access ---!
                          to the cisco routers ip http server
                                  ip http authentication local
                                      no ip http secure-server
                                                             !
                                                             !
                                                   line con 0
                                                   line aux 0
                                                 line vty 0 4
                                          privilege level 15
```

```
 transport input telnet ssh
 !
end
```

تكوين الموجه باستخدام SDM

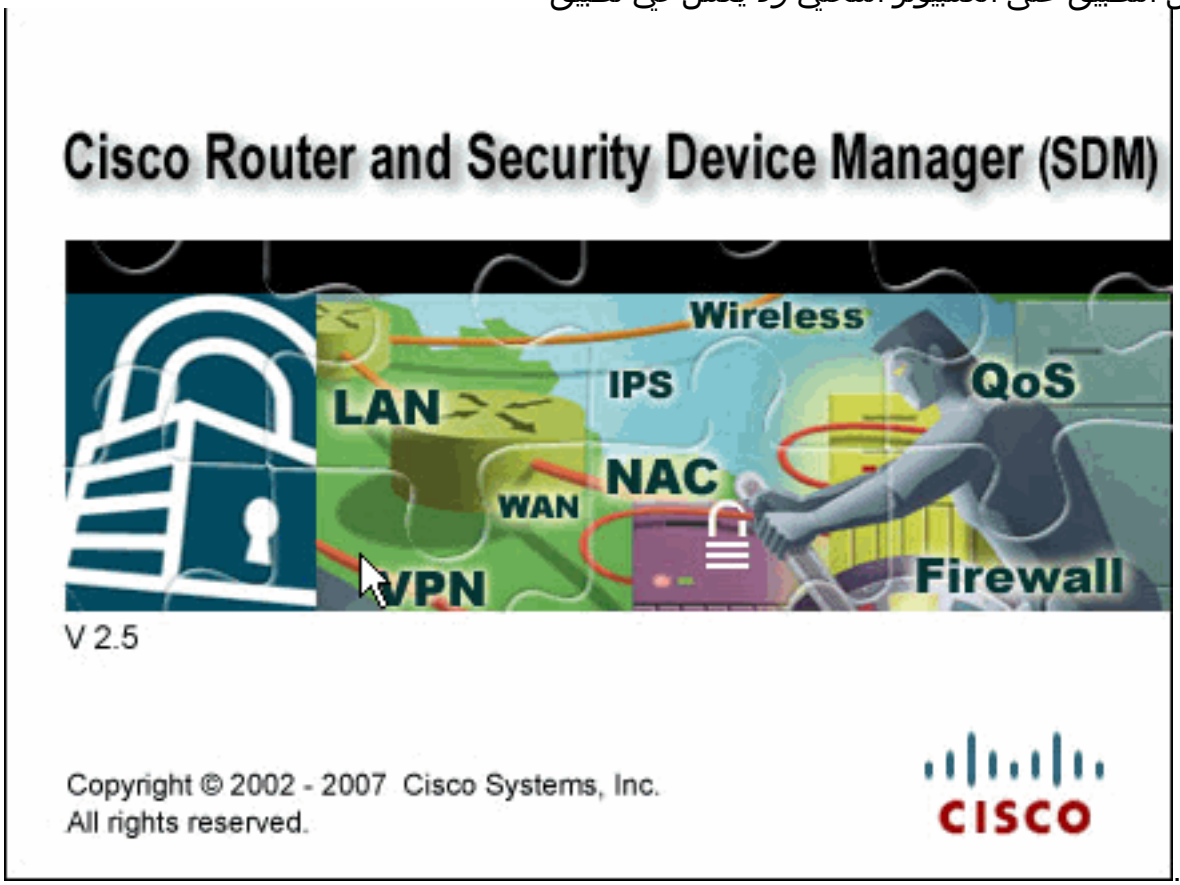
تكوين SDM للموجه

أتمت هذا steps in order to شكلت URL بيصفي على ال cisco ios مسحاج تخديد:

ملاحظة: لتكوين تصفية URL باستخدام إدارة قاعدة بيانات المحول (SDM)، أستخدم الأمر **ip inspection name** في وضع التكوين العام لتحديد مجموعة من قواعد الفحص. يشغل هذا فحص HTTP. تقترن الكلمة الأساسية url تصفية URL باستخدام فحص HTTP. ثم يمكن تعيين اسم التفتيش الذي تم تكوينه على الواجهة التي سيتم إجراء التصفية عليها، على سبيل المثال:

```
hostname(config)#ip inspect
name test http urlfilter
```

1. افتح المستعرض وأدخل **https://<IP_Address الخاص بواجهة الموجه الذي تم تكوينه للوصول إلى إدارة قاعدة بيانات المحول (SDM)>** للوصول إلى إدارة قاعدة بيانات المحول (SDM) على الموجه.تأكد من تخويل أية تحذيرات يعطيك المستعرض لها علاقة بموثوقية شهادة SSL. التقصير username وكلمة على حد سواء فارغ.يعرض الموجه هذه النافذة للسماح بتنزيل تطبيق إدارة قاعدة بيانات المحول (SDM). يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي ولا يعمل في تطبيق

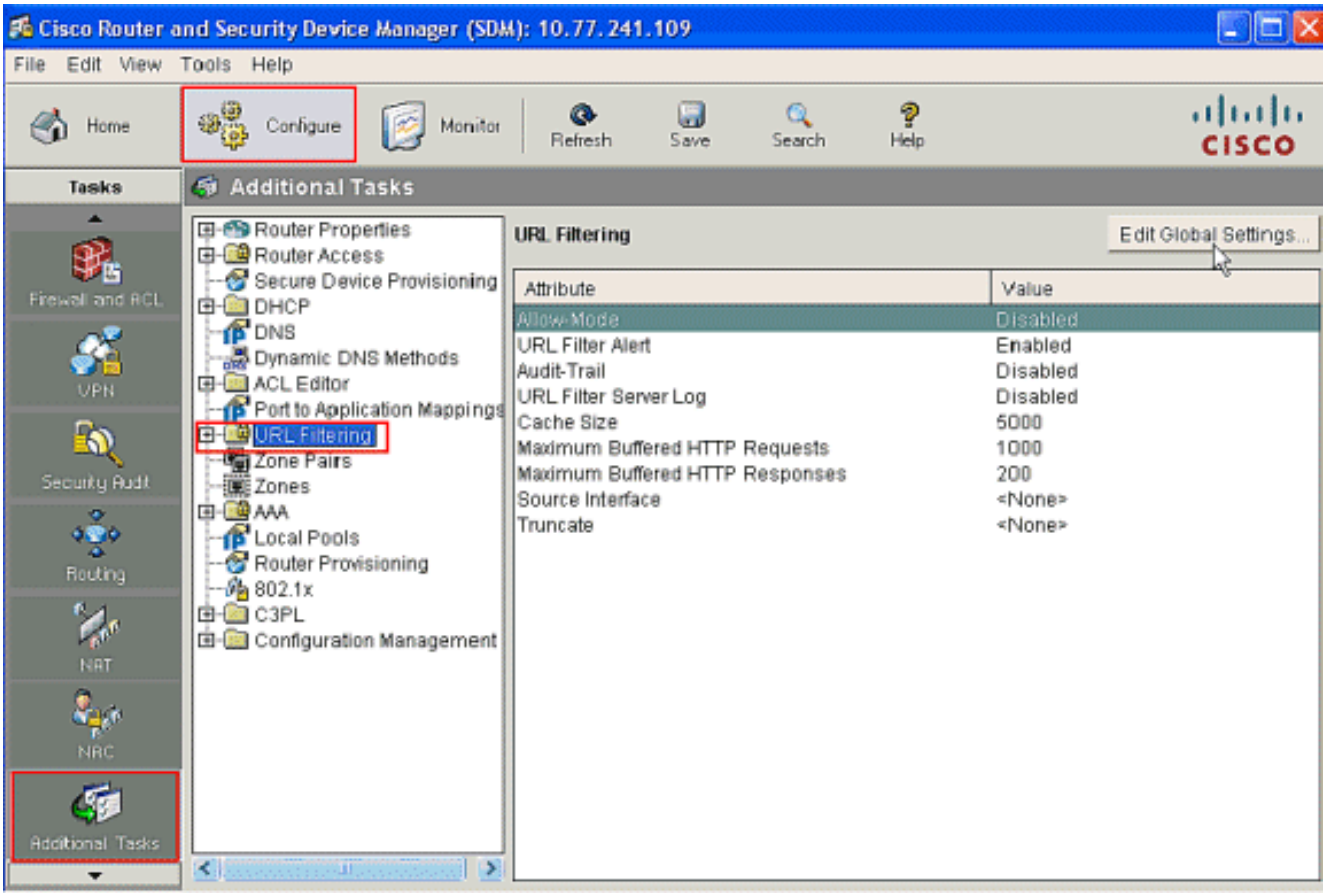


Java.

2. يبدأ تنزيل إدارة قاعدة بيانات المحول (SDM) الآن. بمجرد تنزيل مشغل إدارة قاعدة بيانات المحول (SDM)، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل إدارة قاعدة بيانات المحول (SDM) من Cisco.
3. دخلت **ال username** و **كلمة**، إن يعين أنت واحد، وطقطقة **ok**.يستخدم هذا المثال **Cisco123** لاسم المستخدم و**Cisco123** ككلمة

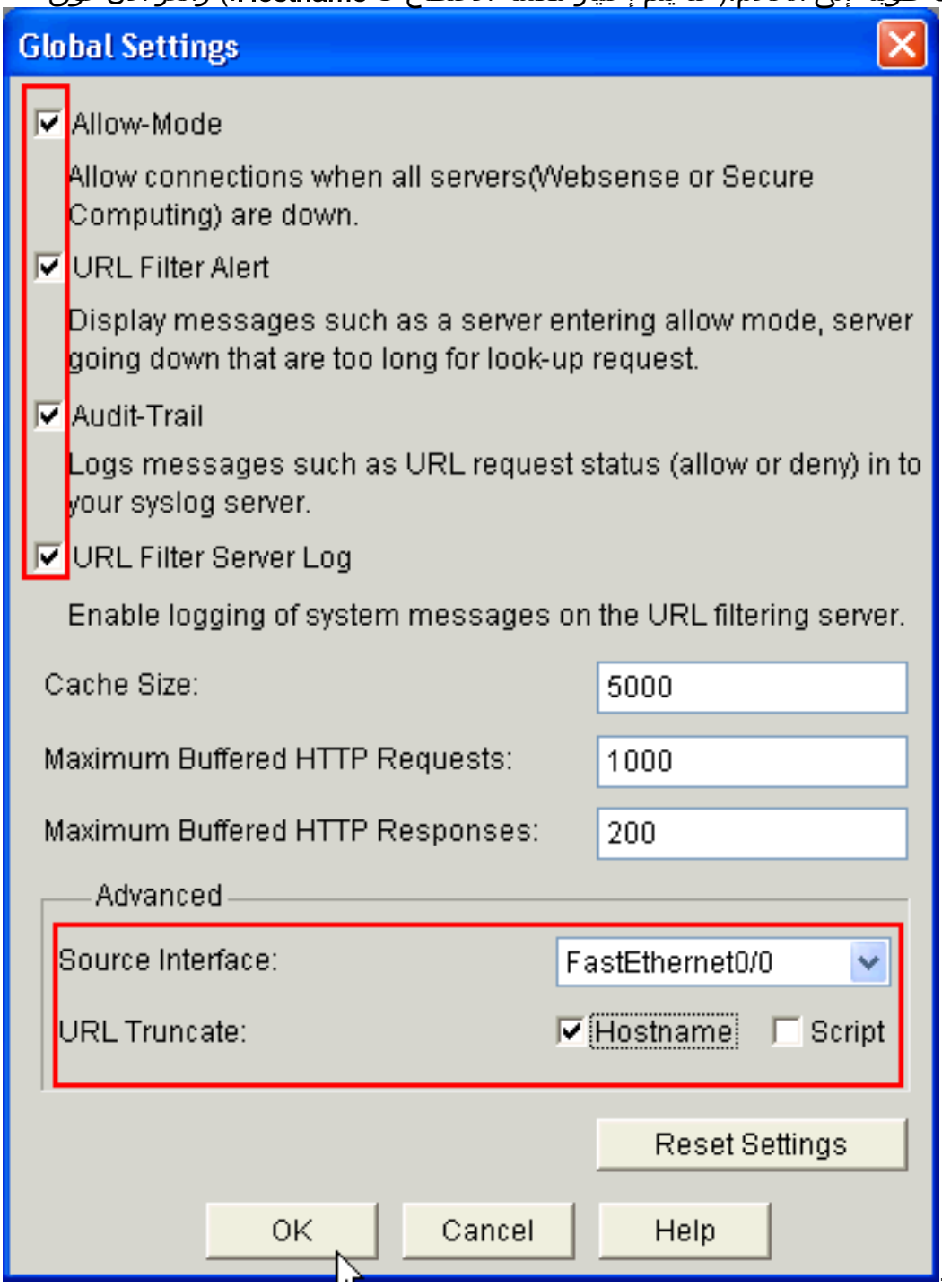
المرور.

4. أختر **تكوين->مهام إضافية** وانقر فوق **تصفية URL** على الصفحة الرئيسية لإدارة قاعدة بيانات المحول (SDM). ثم انقر على **تحرير الإعدادات العامة**، كما هو موضح هنا:



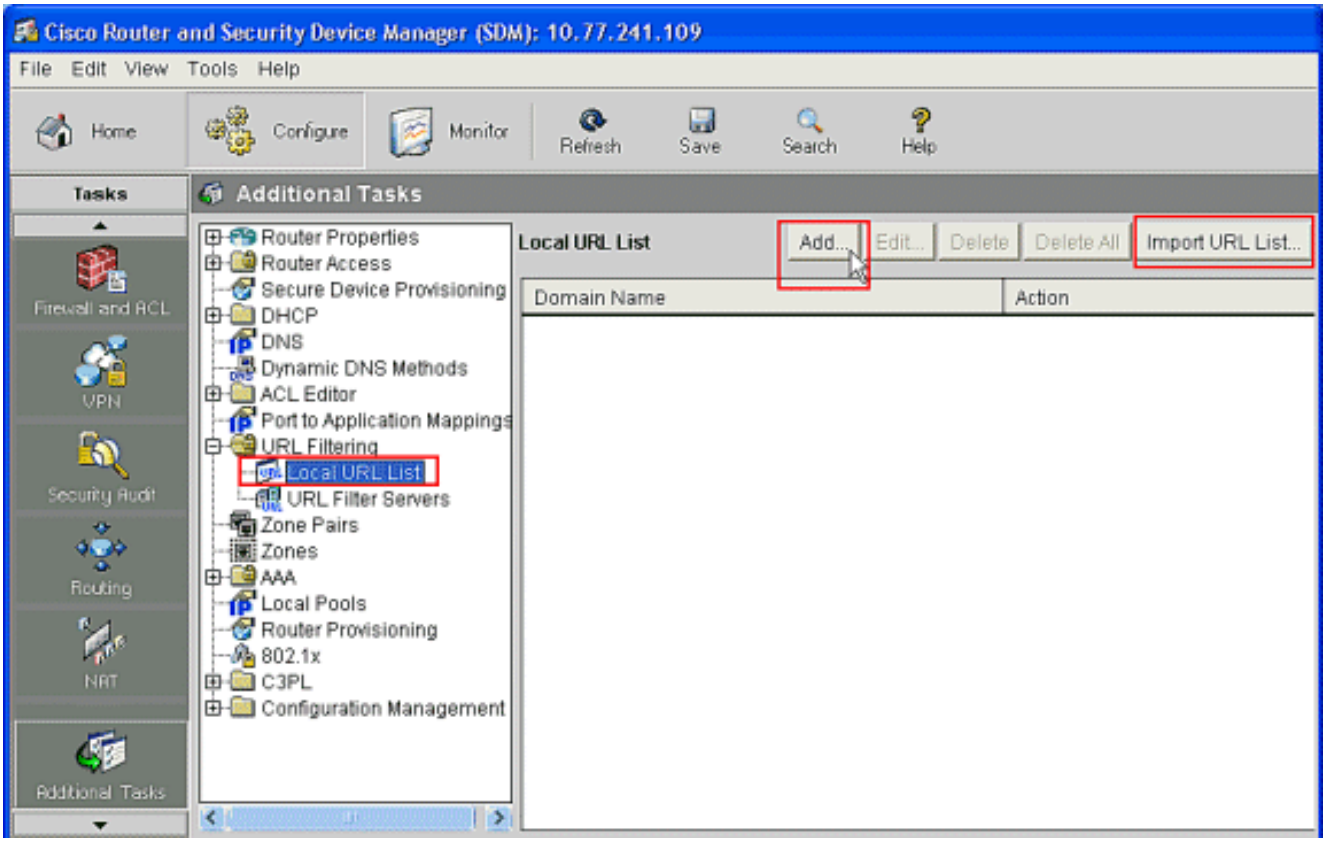
5. في النافذة الجديدة التي تظهر، قم بتمكين المعلمات المطلوبة لتصفية URL، مثل **Allow-Mode**، **و URL Filter**، **Alert**، **و Audit-Trail** و**URL Filtering Server Log**. حدد خانات الاختيار المجاورة لكل معلمة كما هو موضح. الآن قم بتوفير معلومات **حجم ذاكرة التخزين المؤقت** و**مخزن HTTP المؤقت**. قم أيضا بتوفير طريقة **واجهة**

المصدر و**اقتطاع URL** ضمن قسم **خيارات متقدمة** كما هو موضح للسماح لعامل تصفية URL باقتطاع عناوين URL طويلة إلى الخادم.(هنا يتم إختيار معلمة الاقتطاع ك **Hostname**.) وانقر الآن فوق

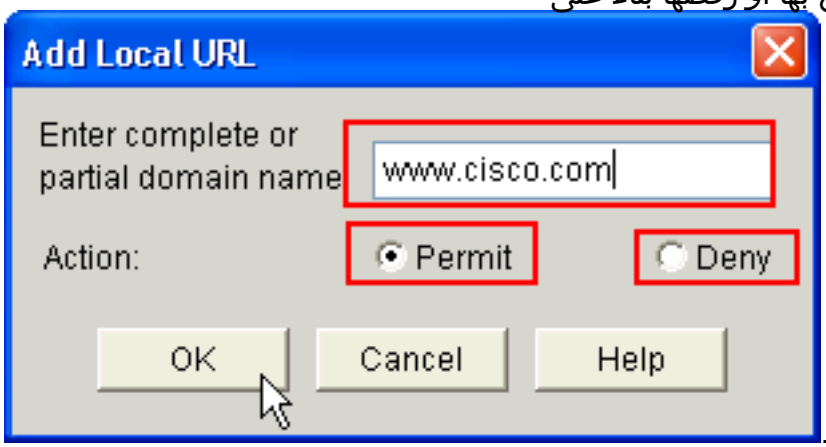


OK.

6. أختر الآن خيار **قائمة URL المحلية** الموجود ضمن علامة التبويب **تصفية URL**. انقر فوق **إضافة** لإضافة اسم المجال وتكوين جدار الحماية للسماح باسم المجال الذي تمت إضافته أو رفضه. يمكنك أيضا إختيار خيار **إدراج قائمة URL** إذا كانت قائمة URLs المطلوبة موجودة كملف. أنت أخترت أن يختار إما **إضافة url** أو **إستيراد قائمة url** خيار يؤسس على متطلب وتوافر قائمة .url

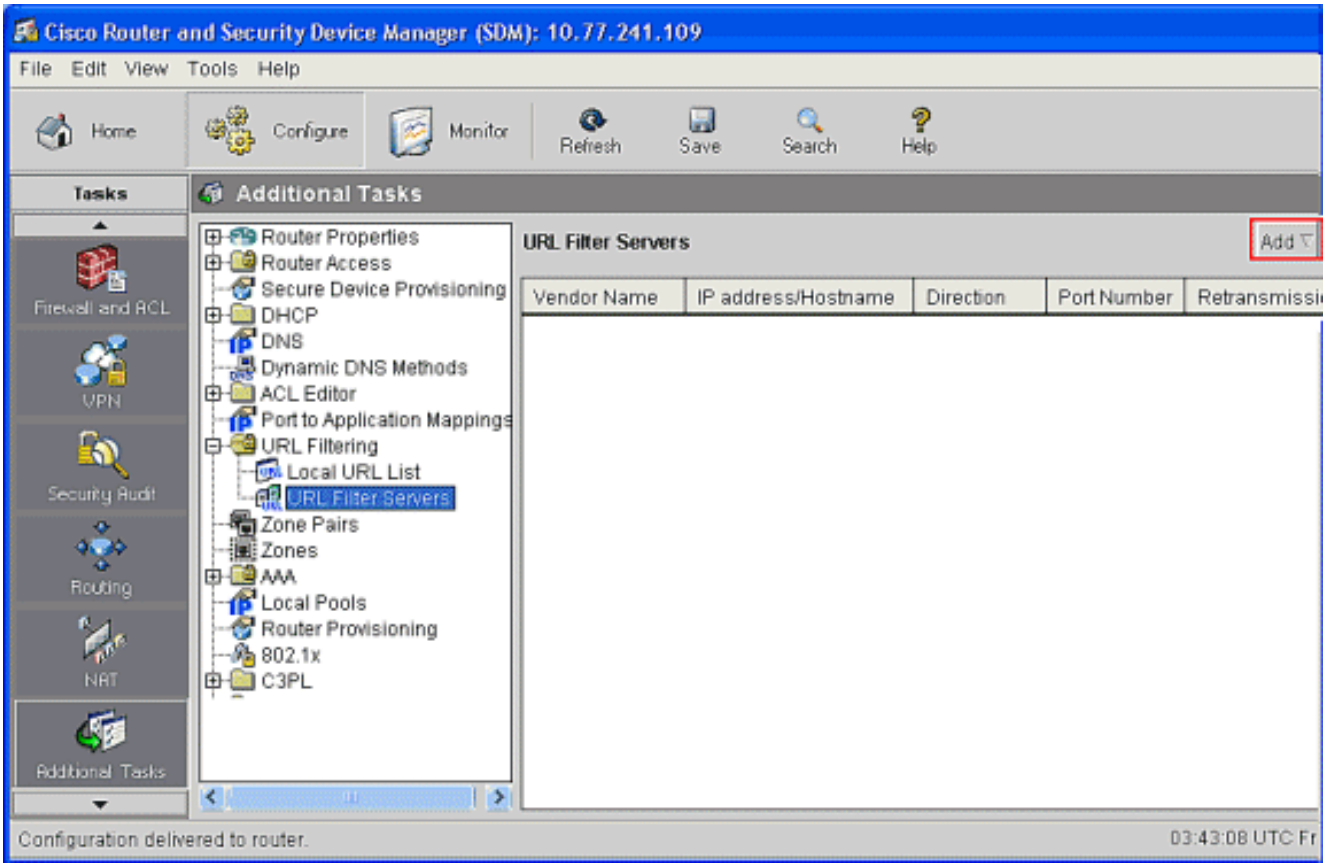


7. في هذا المثال، انقر فوق **إضافة** لإضافة عنوان URL وتكوين جدار حماية IOS للسماح بعنوان URL أو رفضه حسب الحاجة. يفتح الآن نافذة جديدة بعنوان **إضافة عنوان URL محلي** حيث يجب على المستخدم توفير اسم المجال وتقرير ما إذا كان سيسمح أو يرفض عنوان URL. انقر فوق زر الاختيار المجاور لخيار السماح أو الرفض كما هو موضح. هنا ال **www.cisco.com** domain name ، والمستخدم **يسمح** ال **url www.cisco.com**.
بنفس الطريقة، يمكنك النقر فوق **إضافة**، وإضافة العديد من عناوين URL حسب الحاجة، وتكوين جدار الحماية إما للسماح بها أو رفضها بناء على

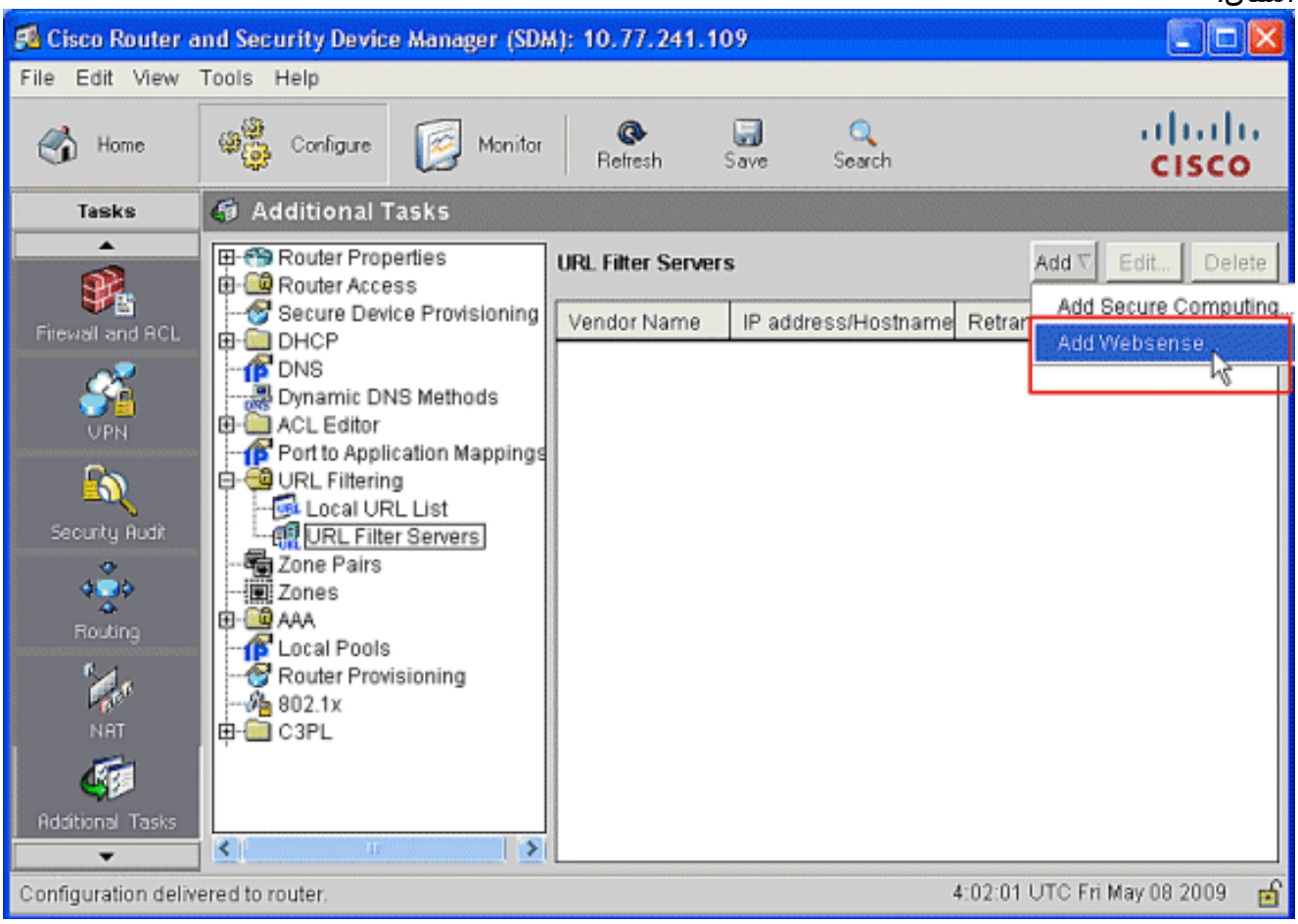


المتطلبات.

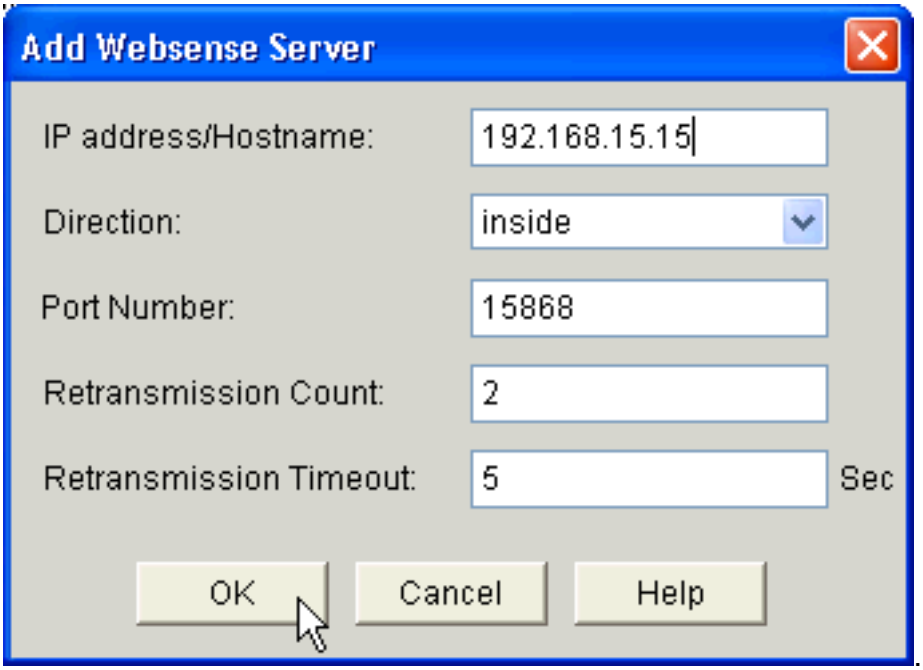
8. أختر خيار **خوادم مرشح عنوان URL** الموجودة ضمن علامة التبويب **تصفية عنوان URL**، كما هو موضح. انقر فوق **إضافة** لإضافة اسم خادم تصفية URL الذي يقوم بتنفيذ وظيفة تصفية URL.



9. بعد النقر فوق **إضافة**، أختر خادم التصفية ك **WebSense** كما هو موضح أدناه منذ إستخدام خادم تصفية WebSense في هذا المثال.



10. في نافذة Add WebSense Server هذه، قم بتوفير **عنوان IP** الخاص بخادم WebSense مع **الإتجاه** الذي يعمل فيه عامل التصفية و**رقم المنفذ**،(رقم المنفذ الافتراضي لخادم WebSense هو **15868**). توفر أيضا قيم **عدد مرات إعادة الإرسال** و**مهلة إعادة الإرسال**، كما هو موضح. طقطقت **ok**، وهذا يتم **ال url يصفي**



تشكيل.

التحقق من الصحة

استعملت الأمر في هذا قسم in order to شاهدت url بيصفي 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 ip urlFilter statistics — يعرض المعلومات والإحصائيات حول خادم التصفيةعلى سبيل المثال:

```
Router# show ip urlfilter statistics
                URL filtering statistics
                ================
              Current requests count:25
Current packet buffer count(in use):40
         Current cache entry count:3100
              Maxever request count:526
Maxever packet buffer count:120
Maxever cache entry count:5000
                 Total requests sent to
    URL Filter Server: 44765
  Total responses received from
    URL Filter Server: 44550
  Total requests allowed: 44320
    Total requests blocked: 224
```

- show ip urlFilter cache — يعرض الحد الأقصى لعدد الإدخالات التي يمكن تخزينها مؤقتا في جدول ذاكرة التخزين المؤقت، وعدد الإدخالات، وعناوين IP للوجهة التي يتم تخزينها مؤقتا في جدول ذاكرة التخزين المؤقت عند إستخدام الأمر show ip urlFilter cache في وضع EXEC ذي الامتيازات
- show ip urlFilter filter filter config — يعرض تكوين التصفيةعلى سبيل المثال:

```
hostname#show ip urlfilter config

                URL filter is ENABLED
  Primary Websense server configurations
  ======================================
:Websense server IP address Or Host Name
                    192.168.15.15
  Websense server port: 15868
```

```
                                :Websense retransmission time out
                                      (in seconds) 6
                            Websense number of retransmission: 2

                        Secondary Websense servers configurations
                        =========================================
                                                            None

                                                 Other configurations
                                                =====================
                                                       Allow Mode: ON
                                                System Alert: ENABLED
                                                 Audit Trail: ENABLED
                                  Log message on Websense server: ENABLED
                                    Maximum number of cache entries: 5000
                                    Maximum number of packet buffers: 200
                                       Maximum outstanding requests: 1000
```

استكشاف الأخطاء وإصلاحها

رسائل الخطأ

URLF-3-SERVER_DOWN: URL 10.92.0.9 — يعرض هذا المستوى الثالث من نوع رسالة LOG_ERR عند تعطل نظام UFS الذي تم تكوينه. عند حدوث ذلك، سيقوم جدار الحماية بوضع علامة ثانوية على الخادم الذي تم تكوينه ومحاولة جلب أحد الخوادم الثانوية الأخرى ووضع علامة على هذا الخادم كخادم أساسي. في حالة عدم تكوين خادم آخر، سيقوم جدار الحماية بإدخال وضع السماح وعرض رسالة URLF-3-ALLOW_MODE.

URLF-3-ALLOW_MODE: URL " — تظهر رسالة نوع LOG_ERR هذه عندما تكون جميع UFS معطلة، ويدخل النظام وضع السماح.

ملاحظة: عند دخول النظام إلى وضع السماح (تكون جميع خوادم التصفية معطلة)، يتم تشغيل مؤقت حفظ نشط دوري يحاول فتح اتصال TCP وعرض خادم.

URLF-5-SERVER_UP: URL 10.92.0.9 — تظهر هذه الرسالة من نوع LOG_NOTICE عندما يتم اكتشاف UFS كقيمة أعلى ويعود النظام من وضع السماح.

URLF-4-URL_TOO_LONG:URL (3072) — تظهر هذه الرسالة LOG_WARNING-type عندما يكون عنوان URL في طلب البحث طويل جدا، ويتم إسقاط أي عنوان URL أطول من 3K.

URLF-4-MAX_REQ: <1000> – يتم عرض رسالة نوع LOG_WARNING هذه عندما يتجاوز عدد الطلبات المعلقة في النظام الحد الأقصى، ويتم إسقاط كافة الطلبات الأخرى.

معلومات ذات صلة

- جدار حماية Cisco IOS
- تصفية عنوان URL الخاص بجدار الحماية WebSense
- دليل تكوين أمان Cisco IOS، الإصدار 12.4-support
- 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).