SDM: Konfigurationsbeispiel für die URL-Filterung auf dem Cisco IOS Router

Inhalt

Einführung

In diesem Dokument wird veranschaulicht, wie die URL-Filterung auf einem Cisco IOS-Router konfiguriert wird. Die URL-Filterung bietet eine bessere Kontrolle über den Datenverkehr, der über den Cisco IOS-Router geleitet wird. URL-Filterung wird in Cisco IOS-Versionen ab Version 12.2(11)YU unterstützt.

Hinweis: Da die URL-Filterung CPU-intensiv ist, stellt die Verwendung eines externen Filterservers sicher, dass der Durchsatz des anderen Datenverkehrs nicht beeinträchtigt wird. Je nach Geschwindigkeit Ihres Netzwerks und der Kapazität Ihres URL-Filterservers kann die für die Erstverbindung erforderliche Zeit deutlich langsamer werden, wenn der Datenverkehr mit einem externen Filterserver gefiltert wird.

Voraussetzungen

Einschränkungen für die Websense-URL-Filterung der Firewall

Websense-Serveranforderung: Um diese Funktion zu aktivieren, muss mindestens ein Websense-Server vorhanden sein, jedoch werden mindestens zwei Websense-Server bevorzugt. Auch wenn

die Anzahl der Websense Server, die Sie nutzen können, nicht begrenzt ist und Sie so viele Server konfigurieren können, wie Sie möchten, kann immer nur ein Server aktiv sein - der primäre Server. Anfragen zur URL-Suche werden nur an den primären Server gesendet.

Einschränkung der URL-Filterunterstützung: Diese Funktion unterstützt jeweils nur ein aktives URL-Filterschema. (Bevor Sie die Websense URL-Filterung aktivieren, müssen Sie immer sicherstellen, dass kein anderes URL-Filterungsschema konfiguriert ist, z. B. N2H2.)

Einschränkung des Benutzernamens: Diese Funktion übergibt den Benutzernamen und die Gruppeninformationen nicht an den Websense-Server. Der Websense-Server kann jedoch für benutzerbasierte Richtlinien verwendet werden, da er über einen anderen Mechanismus verfügt, mit dem der Benutzername einer IP-Adresse entspricht.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco 2801 Router mit Cisco IOS® Software, Version 12.4(15)T
- Cisco Security Device Manager (SDM) Version 2.5

Hinweis: Informationen zur Konfiguration des Routers mithilfe von SDM finden Sie unter Basic Router Configuration (Basiskonfiguration des Routers).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Die URL-Filterungsfunktion von Firewall Websense ermöglicht es Ihrer Cisco IOS-Firewall (auch bekannt als Cisco Secure Integrated Software [CSIS]), mit der Websense URL-Filtersoftware zu interagieren. Auf diese Weise können Sie den Benutzerzugriff auf bestimmte Websites aufgrund bestimmter Richtlinien verhindern. Die Cisco IOS-Firewall erkennt gemeinsam mit dem Websense-Server, ob eine bestimmte URL zugelassen oder abgelehnt (blockiert) werden kann.

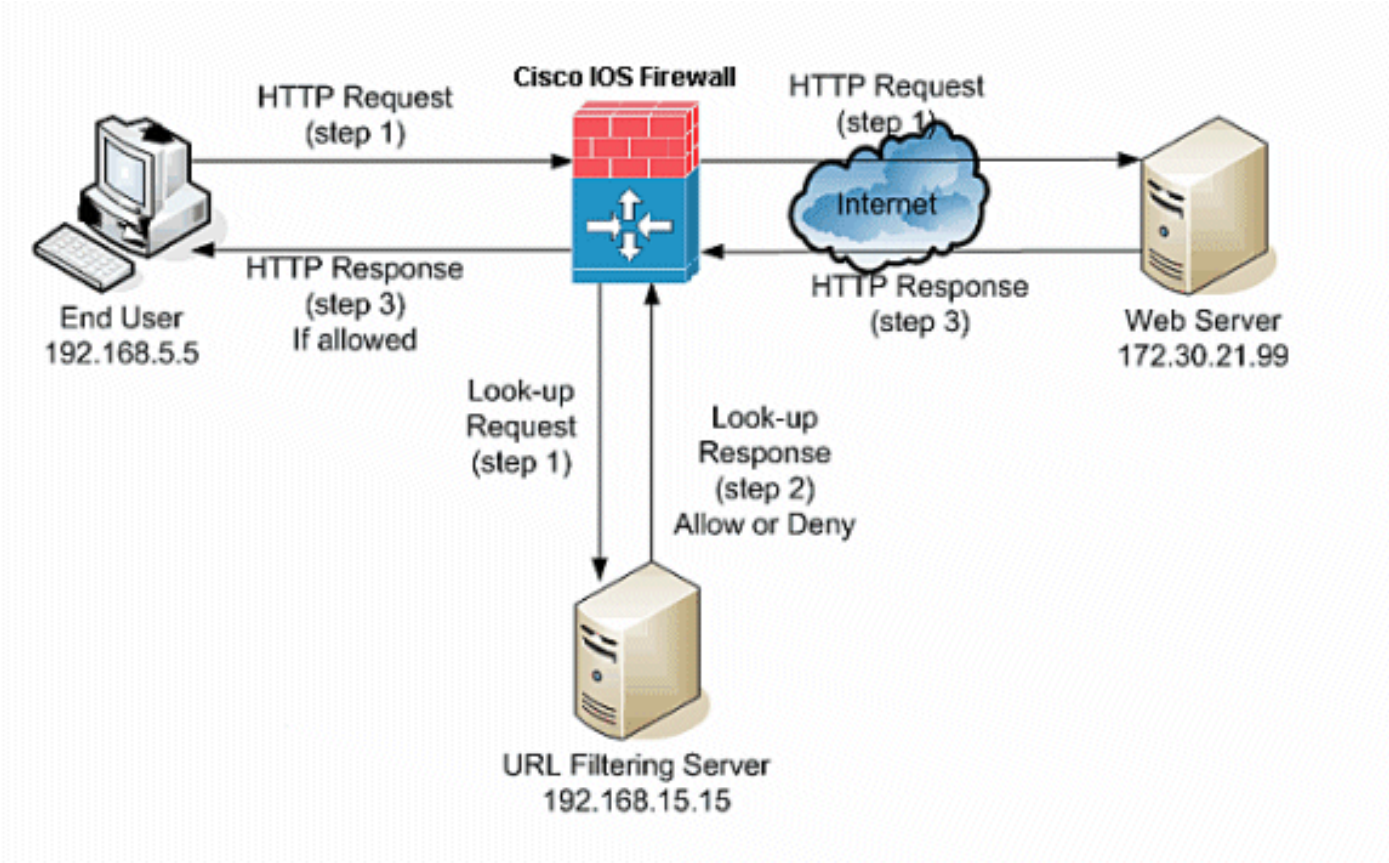
Konfigurieren des Routers mit der CLI

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Beispiel befindet sich der URL-Filterserver im internen Netzwerk. Endbenutzer im Netzwerk versuchen, über das Internet auf den Webserver außerhalb des Netzwerks zuzugreifen.

Diese Schritte werden auf Anforderung des Benutzers für den Webserver ausgeführt:

1. Der Endbenutzer ruft eine Seite auf dem Webserver auf, und der Browser sendet eine HTTP-Anfrage.
2. Nachdem die Cisco IOS Firewall diese Anforderung erhält, leitet sie die Anforderung an den Webserver weiter. Gleichzeitig wird die URL extrahiert und eine Suchanfrage an den URL-Filterserver gesendet.
3. Nachdem der URL-Filterserver die Suchanfrage empfängt, überprüft er seine Datenbank, um festzustellen, ob die URL zugelassen oder verweigert werden soll. Sie gibt den Status "Zulassen" oder "Ablehnen" mit einer Nachfrageantwort auf die Cisco IOS® Firewall zurück.
4. Die Cisco IOS® Firewall erhält diese Nachschlageantwort und führt eine der folgenden Funktionen aus:Wenn die Nachschlageantwort die URL zulässt, sendet sie die HTTP-Antwort an den Endbenutzer.Wenn die Nachschlageantwort die URL verweigert, leitet der URL-Filterserver den Benutzer zu seinem eigenen internen Webserver um, der eine Meldung anzeigt, in der die Kategorie beschrieben wird, unter der die URL blockiert wird. Anschließend wird die Verbindung an beiden Enden zurückgesetzt.

Identifizieren des Filterservers

Sie müssen die Adresse des Filterservers mit dem Befehl **ip urlfilter server vendor** identifizieren.

Sie müssen die entsprechende Form dieses Befehls basierend auf dem verwendeten Filterservertyp verwenden.

Hinweis: Sie können in Ihrer Konfiguration nur einen Servertyp konfigurieren, entweder Websense oder N2H2.

Websense

Websense ist eine Filtersoftware eines Drittanbieters, mit der HTTP-Anfragen anhand der folgenden Richtlinien gefiltert werden können:

- Zielhostname
- Ziel-IP-Adresse
- Schlüsselwörter
- Benutzername

Die Software unterhält eine URL-Datenbank mit mehr als 20 Millionen Websites, die in mehr als 60 Kategorien und Unterkategorien unterteilt sind.

Der Befehl **ip urlfilter server** gibt den Server an, auf dem die N2H2- oder Websense URL-Filteranwendung ausgeführt wird. Um einen Anbieterserver für die URL-Filterung zu konfigurieren, verwenden Sie den Befehl **ip urlfilter server vendor** im globalen Konfigurationsmodus. Um einen Server aus Ihrer Konfiguration zu entfernen, verwenden Sie die no-Form dieses Befehls. Dies ist die Syntax des Befehls **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]
```

Ersetzen Sie `ip-address` durch die IP-Adresse des Websense-Servers. Tauschen Sie `Sekunden` durch die Anzahl der Sekunden aus, die die IOS Firewall weiterhin versuchen muss, eine Verbindung zum Filterserver herzustellen.

Führen Sie zum Beispiel den folgenden Befehl aus, um einen Websense-Filterserver für die URL-Filterung zu konfigurieren:

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

Konfigurieren der Filterrichtlinie

Hinweis: Sie müssen den URL-Filterserver identifizieren und aktivieren, bevor Sie die URL-Filterung aktivieren.

Kürzung langer HTTP-URLs

Damit der URL-Filter lange URLs zum Server abschneiden kann, verwenden Sie den **Befehl ip urlfilter truncate** (ip urlfilter abschneiden) im globalen Konfigurationsmodus. Um die Abschneiden-Option zu deaktivieren, verwenden Sie die no-Form dieses Befehls. Dieser Befehl wird in Cisco IOS, Version 12.4(6)T und höher, unterstützt.

`ip urlfilter truncate {script-parameter} | hostname}` ist die Syntax dieses Befehls.

Skriptparameter: Nur die URL bis zu den Skriptoptionen wird gesendet. Wenn beispielsweise die gesamte URL `http://www.cisco.com/dev/xxx.cgi?when=now` ist, wird nur die URL über `http://www.cisco.com/dev/xxx.cgi` gesendet (wenn die maximal unterstützte URL-Länge nicht überschritten wird).

Hostname: Nur der Hostname wird gesendet. Wenn z. B. die gesamte URL `http://www.cisco.com/dev/xxx.cgi?when=now` ist, `wird` nur `http://www.cisco.com` gesendet.

Wenn sowohl die Skript-Parameter als auch die Schlüsselwörter für den Hostnamen konfiguriert sind, hat das script-parameters-Schlüsselwort Vorrang vor dem Schlüsselwort hostname. Wenn beide Schlüsselwörter konfiguriert und die URL der Skriptparameter gekürzt wird und die maximal unterstützte URL-Länge überschritten wird, wird die URL bis zum Hostnamen gekürzt.

Hinweis: Wenn beide Schlüsselwortskript-Parameter und der Hostname konfiguriert sind, müssen sie sich in separaten Zeilen befinden, wie unten gezeigt. Sie können nicht in einer Zeile kombiniert werden.

Hinweis: `ip urlfilter spaltet Skriptparameter ab`

Hinweis: `ip urlfilter spaltet Hostname ab`

Konfiguration für Router mit Cisco IOS-Version 12.4

Diese Konfiguration enthält die in diesem Dokument beschriebenen Befehle:

Konfiguration für Router mit Cisco IOS Version 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
```

Konfigurieren des Routers mit SDM

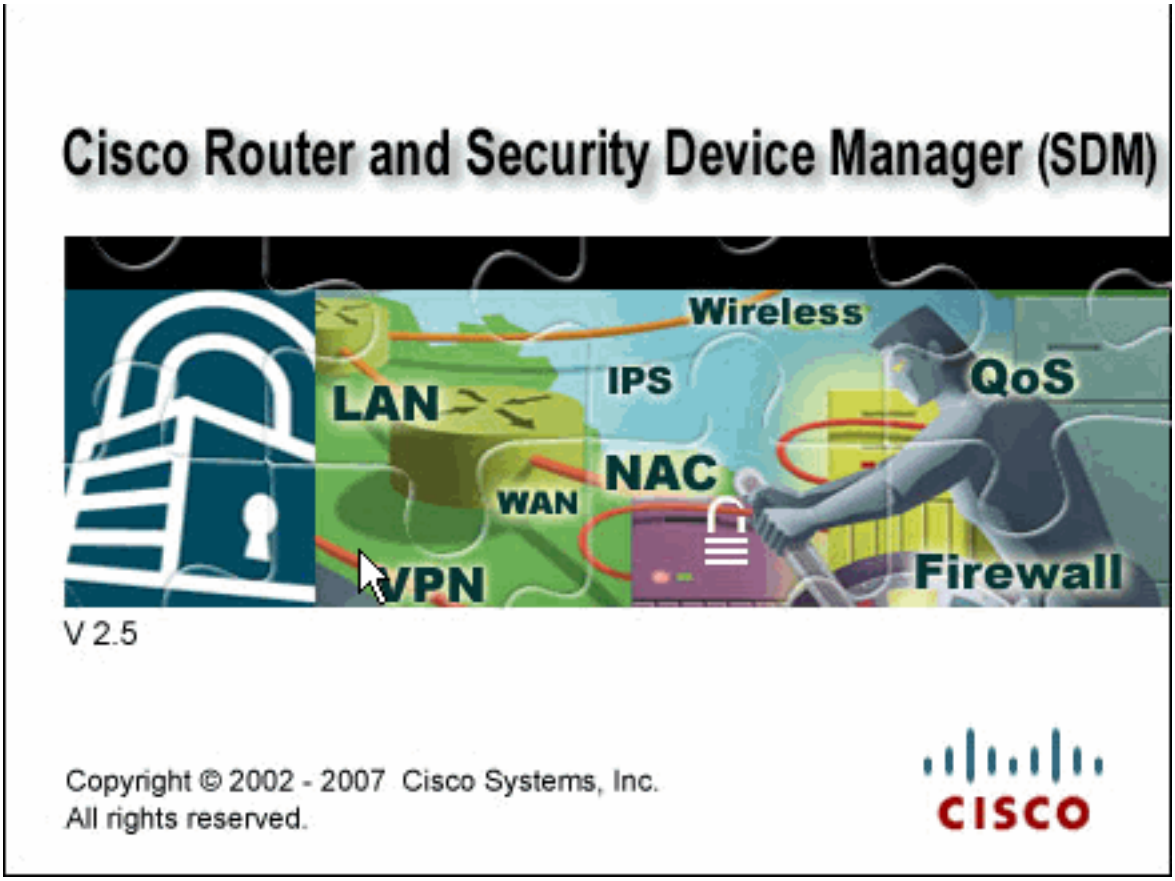
Router-SDM-Konfiguration

Gehen Sie wie folgt vor, um die URL-Filterung auf dem Cisco IOS-Router zu konfigurieren:

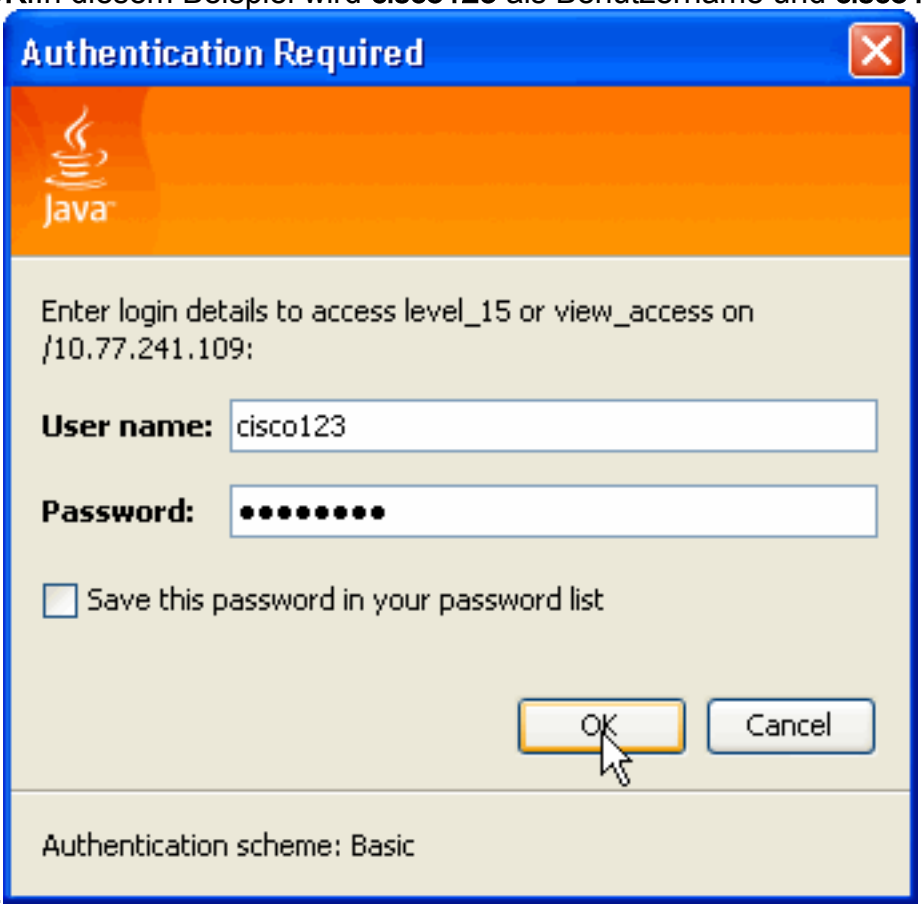
Hinweis: Um die URL-Filterung mit SDM zu konfigurieren, verwenden Sie den Befehl **ip inspect name** im globalen Konfigurationsmodus, um einen Satz von Prüfungsregeln zu definieren. Dadurch wird die HTTP-Prüfung aktiviert. Das urlfilter-Schlüsselwort ordnet URL-Filterung HTTP-Prüfung zu. Anschließend kann der konfigurierte Prüfname der Schnittstelle zugeordnet werden, auf der die Filterung durchgeführt werden soll, z. B.:

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

1. Öffnen Sie Ihren Browser, und geben Sie **https://<IP_Address der Schnittstelle des Routers ein, der für SDM Access konfiguriert wurde>**, um auf das SDM auf dem Router zuzugreifen.Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität des SSL-Zertifikats ausgibt. Standardmäßig sind Benutzername und Kennwort leer.Der Router zeigt dieses Fenster an, um das Herunterladen der SDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet ausgeführt.

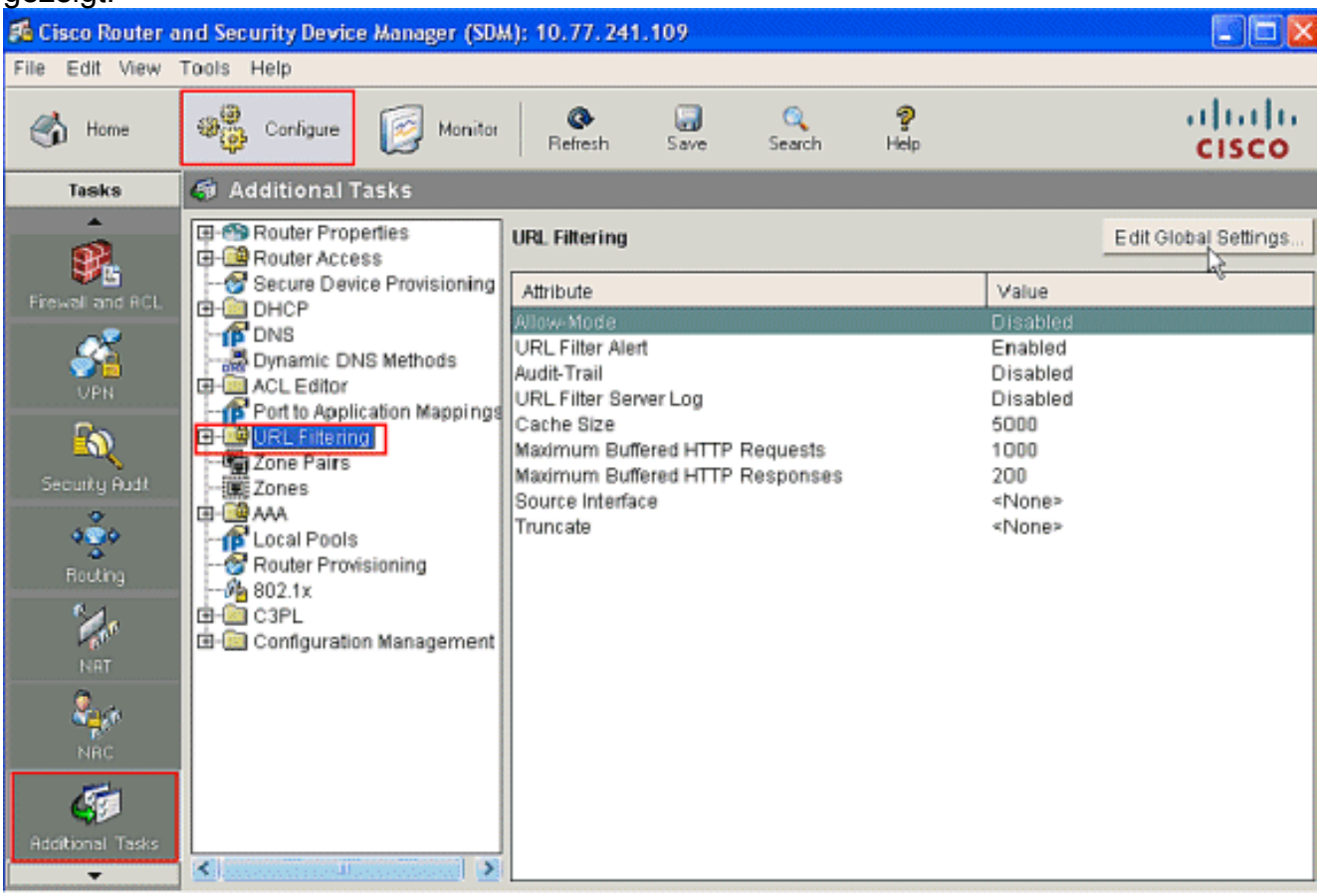


2. Der SDM-Download beginnt jetzt. Wenn der SDM-Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen angewiesen werden, um die Software zu installieren und den Cisco SDM Launcher auszuführen.
3. Geben Sie den **Benutzernamen** und das **Kennwort ein**, wenn Sie diesen angegeben haben, und klicken Sie auf **OK**.In diesem Beispiel wird **cisco123** als Benutzername und **cisco123** als Kennwort verwendet.

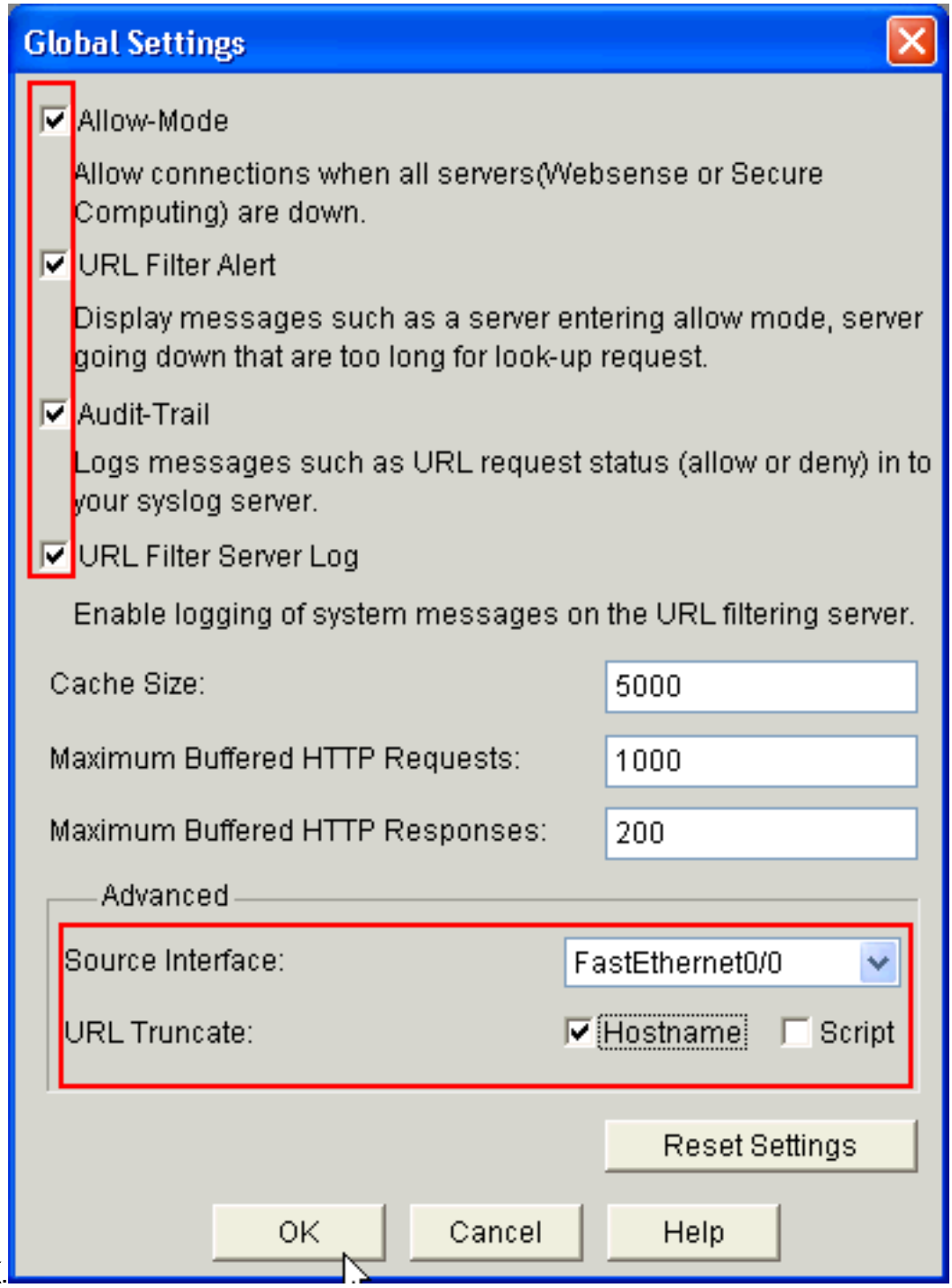


4. Wählen Sie **Konfiguration > Zusätzliche Aufgaben** aus, und klicken Sie auf der SDM-

Startseite auf **URL-Filterung**. Klicken Sie anschließend auf **Globale Einstellungen bearbeiten**, wie hier
gezeigt:

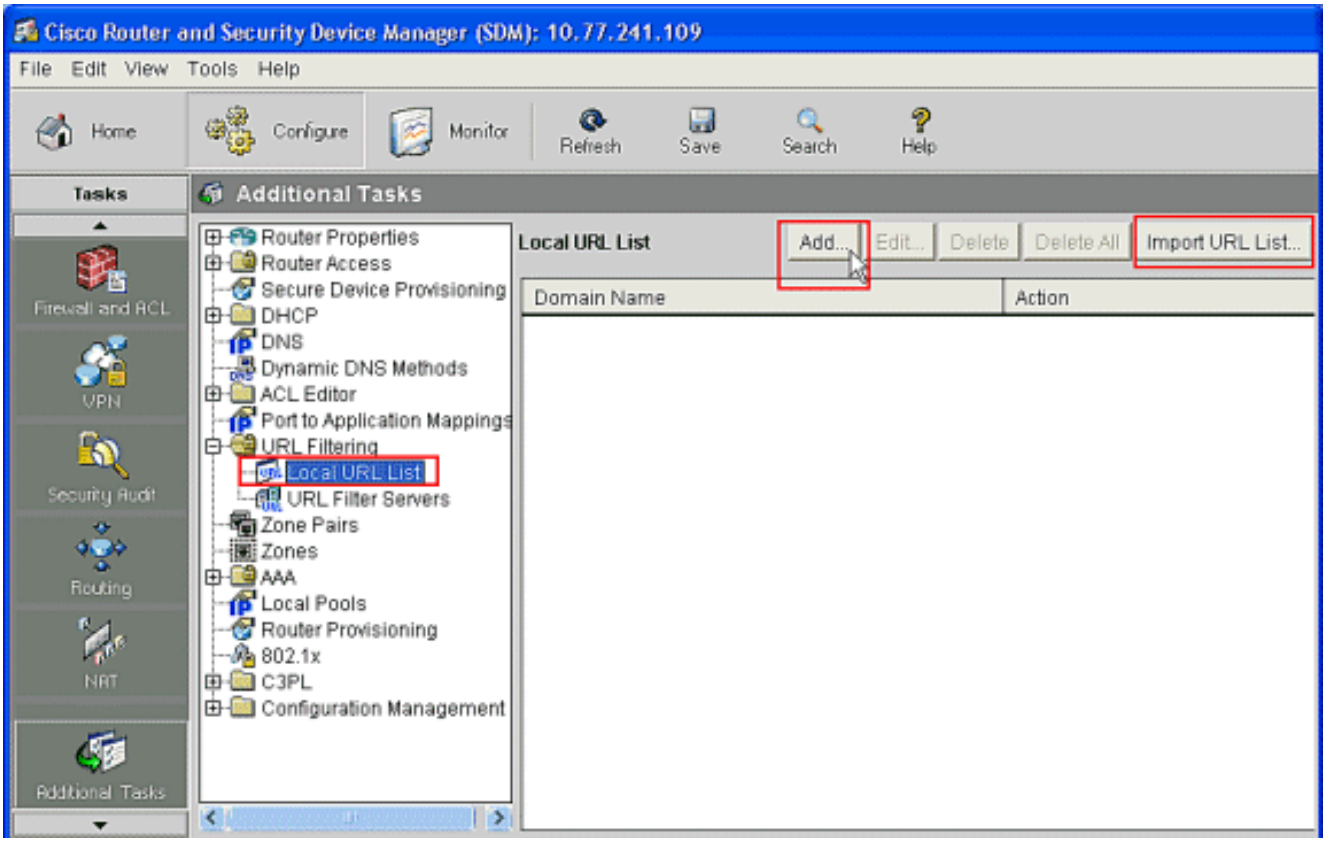


5. Aktivieren Sie im neuen sich öffnenden Fenster die für die URL-Filterung erforderlichen Parameter, z. B. **Zulassungsmodus, URL-Filterwarnung, Audit-Test** und **URL-Filterungsprotokoll**. Aktivieren Sie die Kontrollkästchen neben den einzelnen Parametern wie gezeigt. Geben Sie nun die Informationen **Cache Size** und **HTTP Buffer** an. Stellen Sie außerdem die **Quellschnittstelle** und die URL-Truncate-**Methode** im **erweiterten** Abschnitt bereit, wie gezeigt, damit der URL-Filter lange URLs zum Server abspalten kann. (Hier wird der Truncation-Parameter als **Hostname** ausgewählt.) Klicken Sie jetzt auf

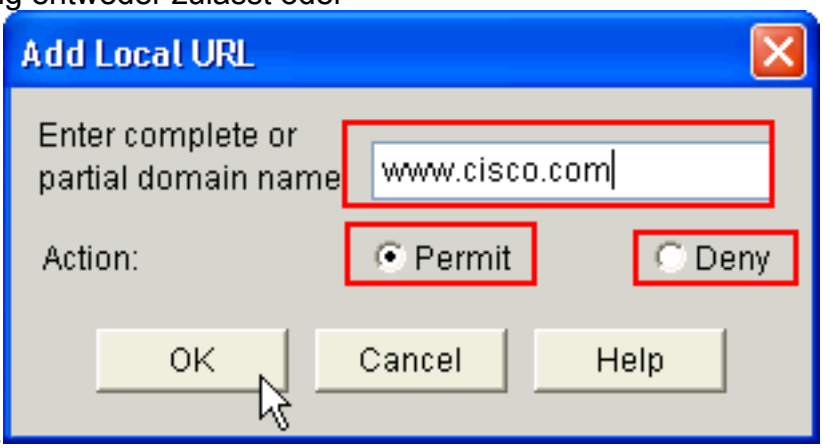


OK.

6. Wählen Sie jetzt die Option **Lokale URL-Liste** unter der Registerkarte **URL-Filterung aus**. Klicken Sie auf **Hinzufügen**, um den Domänennamen hinzuzufügen und die Firewall so zu konfigurieren, dass der hinzugefügte Domänenname zugelassen oder abgelehnt wird. Sie können auch die Option **URL-Liste importieren** auswählen, wenn die Liste der erforderlichen URLs als Datei vorhanden ist. Sie haben die Wahl zwischen den Optionen **URL hinzufügen** oder **URL-Liste importieren**, abhängig von der Anforderung und Verfügbarkeit der URL-Liste.

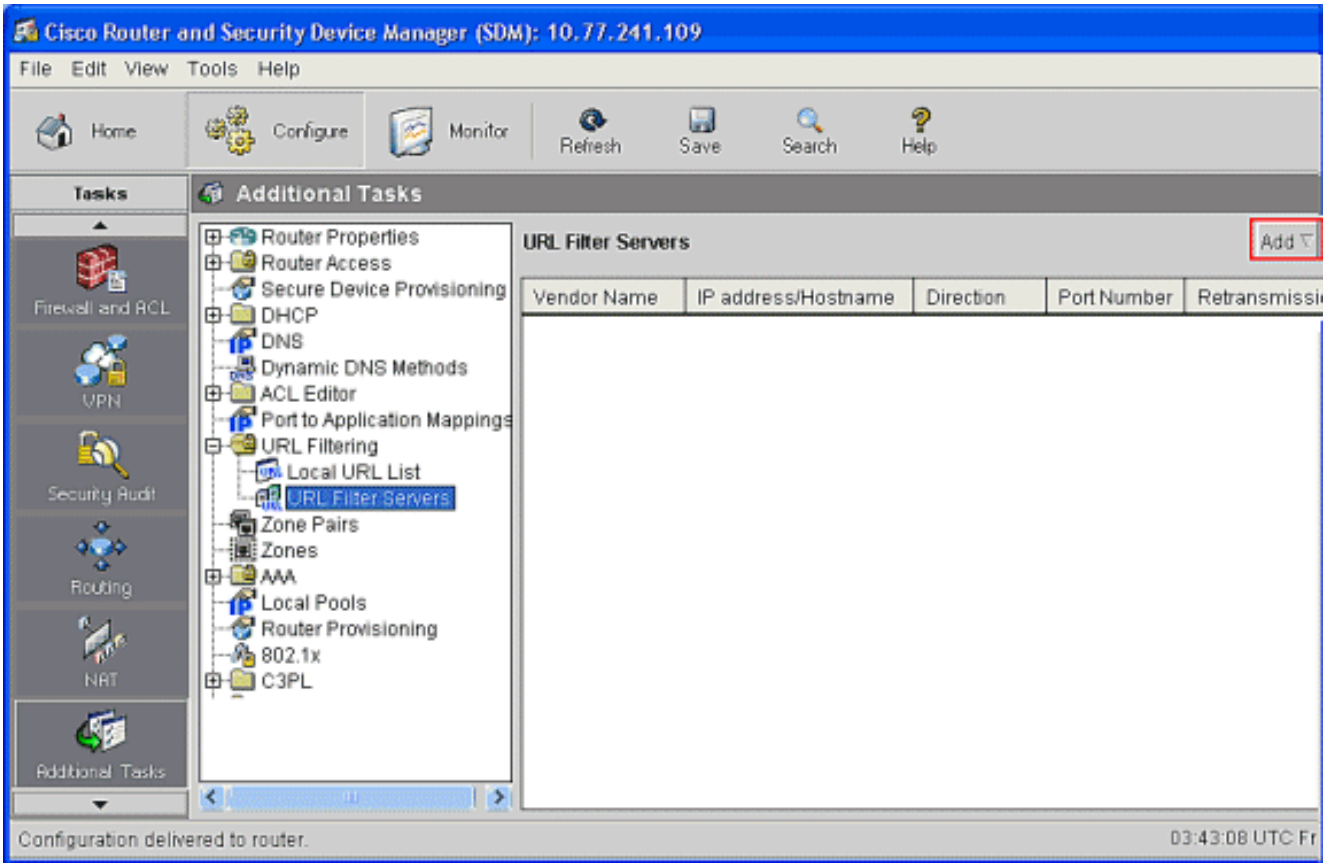


7. Klicken Sie in diesem Beispiel auf **Hinzufügen**, um die URL hinzuzufügen, und konfigurieren Sie die IOS-Firewall so, dass die URL bei Bedarf zugelassen oder verweigert wird. Nun wird ein neues Fenster mit dem Titel **ADD Local URL** geöffnet, in dem der Benutzer den Domänennamen angeben und entscheiden muss, ob er die URL zulassen oder verweigern soll. Klicken Sie auf das Optionsfeld neben der Option Zulassen oder Verweigern, wie gezeigt. Hier lautet der Domänenname **www.cisco.com**, und der Benutzer **lässt** die **URL www.cisco.com zu**. Auf die gleiche Weise können Sie auf **Hinzufügen** klicken, so viele URLs wie erforderlich hinzufügen und die Firewall so konfigurieren, dass sie diese je nach Anforderung entweder zulässt oder

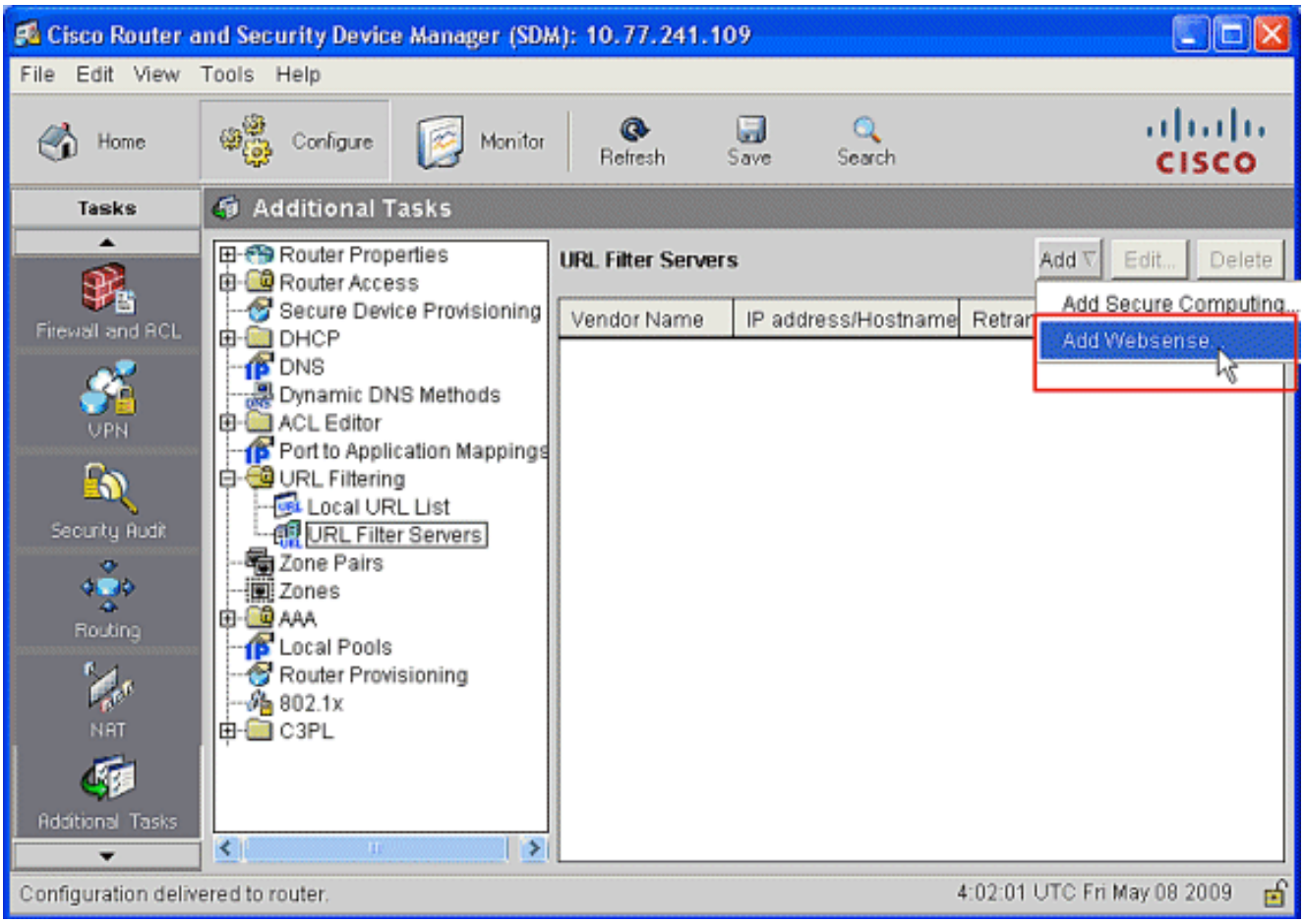


verweigert.

8. Wählen Sie die Option **URL-Filter-Server** unter der Registerkarte **URL-Filterung** aus, wie dargestellt. Klicken Sie auf **Hinzufügen**, um den Namen des URL-Filterungsservers hinzuzufügen, der die URL-Filterfunktion ausführt.

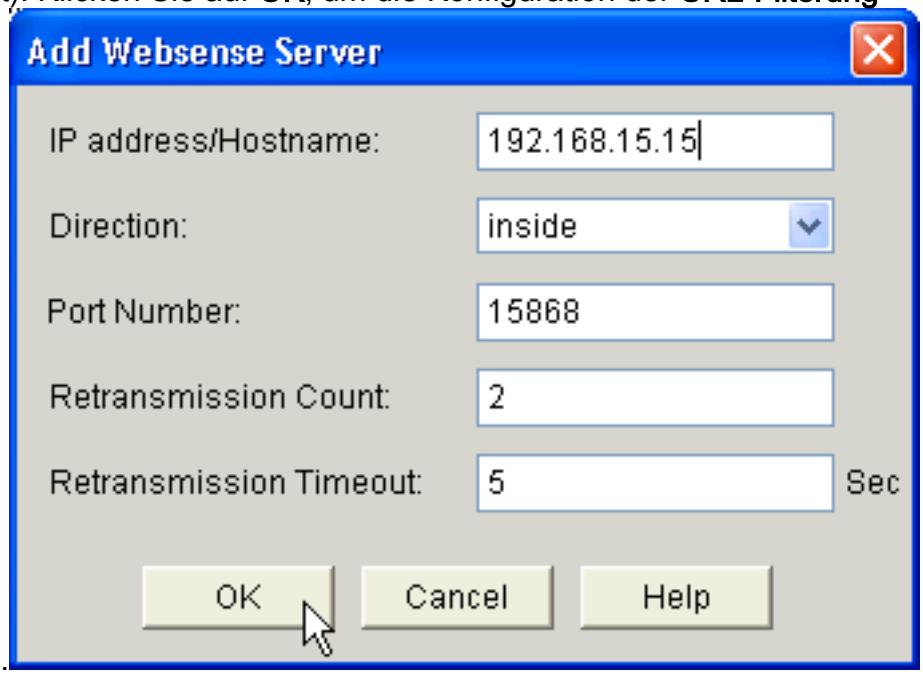


9. Nachdem Sie auf **Hinzufügen** geklickt haben, wählen Sie den Filterserver als **Websense** aus, wie unten dargestellt, da der Websense-Filterserver in diesem Beispiel verwendet wird.



10. Geben Sie in diesem Fenster **Websense-Server hinzufügen** die **IP-Adresse** des Websense-Servers sowie die **Richtung**, in der der Filter funktioniert, und **Portnummer an** (die Standard-Portnummer für den Websense-Server ist **15868).** Geben Sie außerdem die Werte **für die**

Anzahl der **wiederholten Übertragungen** und **für das Timeout** für die erneute Übertragung an (wie gezeigt). Klicken Sie auf **OK**, um die Konfiguration der **URL-Filterung** abzuschließen.



Überprüfen

Verwenden Sie die Befehle in diesem Abschnitt, um Informationen zur URL-Filterung anzuzeigen. Sie können diese Befehle verwenden, um Ihre Konfiguration zu überprüfen.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

- **show ip urlfilter statistics statistics** - Zeigt Informationen und Statistiken über den Filterserver anBeispiel:

```
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** - Zeigt die maximale Anzahl der Einträge an, die in die Cachetabelle zwischengespeichert werden können, die Anzahl der Einträge und die Ziel-IP-Adressen, die in der Cachetabelle zwischengespeichert werden, wenn Sie den Befehl show ip urlfilter cache im privilegierten EXEC-Modus verwenden
- **show ip urlfilter filter filter config** - Zeigt die Filterkonfiguration anBeispiel:

```
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:
   6 (in seconds)
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
```

Fehlerbehebung

Fehlermeldungen

`%URLF-3-SERVER_DOWN: Verbindung zum URL-Filterserver 10.92.0.9 ist unterbrochen` — Diese Stufe drei LOG_ERR-Meldung wird angezeigt, wenn ein konfiguriertes UFS ausfällt. In diesem Fall markiert die Firewall den konfigurierten Server als sekundär und versucht, einen der anderen sekundären Server aufzurufen und diesen Server als primären Server zu markieren. Wenn kein anderer Server konfiguriert ist, wechselt die Firewall in den Zulassungsmodus und zeigt die Meldung `URLF-3-ALLOW_MODE` an.

`%URLF-3-ALLOW_MODE: Die Verbindung zu allen URL-Filterservern ist unterbrochen, und der ZULASSUNGSMODUS ist AUS` — Diese LOG_ERR-Typmeldung wird angezeigt, wenn alle UFS ausgefallen sind, und das System wechselt in den Zulassungsmodus.

Hinweis: Wenn das System in den Genehmigungsmodus wechselt (alle Filterserver sind ausgefallen), wird ein periodischer Keep-Alive-Timer ausgelöst, der versucht, eine TCP-Verbindung zu öffnen und einen Server zu starten.

`%URLF-5-SERVER_UP: Verbindung mit einem URL-Filterserver 10.92.0.9 hergestellt wird; das System kehrt vom ALLOW MODE zurück` — Diese LOG_NOTICE-Meldung wird angezeigt, wenn die UFS als aktiv erkannt werden und das System aus dem Zulassungsmodus zurückkehrt.

`%URLF-4-URL_TOO_LONG:URL zu lang (über 3072 Byte), möglicherweise ein falsches Paket?` — Diese LOG_WARNING-Meldung wird angezeigt, wenn die URL in einer Suchanfrage zu lang ist. Jede URL, die länger als 3K ist, wird gelöscht.

`%URLF-4-MAX_REQ: Die Anzahl der ausstehenden Anfragen überschreitet die Höchstgrenze <1000>` — Diese Nachricht vom Typ LOG_WARNING wird angezeigt, wenn die Anzahl der ausstehenden Anfragen im System die Höchstgrenze überschreitet und alle weiteren Anfragen verworfen

werden.

Zugehörige Informationen

- Cisco IOS-Firewall
- URL-Filterung für Firewall Websense
- Cisco IOS Security Configuration Guide, Release 12.4-Support
- Technischer Support und Dokumentation - Cisco Systems