dm: URL-filtering op Cisco IOS-routerconfiguratie, voorbeeld

Inhoud

Inleiding

Dit document toont aan hoe u URL Filtering op een Cisco IOS router kunt configureren. URL-filtering biedt meer controle over het verkeer dat door de Cisco IOS-router gaat. URL-filtering wordt ondersteund in Cisco IOS-versies in versie 12.2(11)YU en hoger.

Opmerking: Omdat URL-filtering CPU-intensief is, zorgt het gebruik van een externe filterserver ervoor dat de doorvoersnelheid van ander verkeer niet wordt beïnvloed. Op basis van de snelheid van uw netwerk en de capaciteit van uw URL-filterserver kan de tijd die nodig is voor de eerste verbinding aanzienlijk trager zijn wanneer het verkeer wordt gefilterd met een externe filterserver.

Voorwaarden

Beperkingen voor URL-filtering van firewall

Vereiste voor webzineserver: Om deze optie in te schakelen moet u minimaal één Websessserver hebben, maar twee of meer Websone-servers hebben de voorkeur. Hoewel er geen limiet is aan het aantal webzineservers dat u kunt hebben en u kunt zoveel servers configureren als u wilt, kan slechts één server op elk gewenst moment actief zijn — de primaire server. URL opriep-verzoeken

worden alleen naar de primaire server verzonden.

Beperking van URL-filtering Deze optie ondersteunt slechts één actief URL-filterschema tegelijk. (Voordat u URL-filtering inschakelen, moet u er altijd voor zorgen dat er geen ander URL-filterschema is ingesteld, zoals N2H2.)

Beperking van gebruikersnaam: Deze optie geeft de gebruikersnaam en groepsinformatie niet door aan de WebBetleersserver, maar de Webzineserver kan werken voor op gebruikers gebaseerd beleid omdat het een ander mechanisme heeft om de gebruikersnaam om aan een IP-adres te corresponderen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 2801 router met Cisco IOS® softwarerelease 12.4(15)T
- Cisco Security apparaat Manager (DSM) versie 2.5

Opmerking: Raadpleeg de basisrouterconfiguratie met behulp van een dm om de router door een dm te laten configureren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Met de functie Firewall Websin URL Filtering kan uw Cisco IOS-firewall (ook bekend als Cisco Secure Integrated Software [CSIS]) communiceren met de websonde URL-filtersoftware. Hiermee kunt u op basis van een bepaald beleid de toegang van gebruikers tot bepaalde websites beletten. De Cisco IOS firewall werkt met de server van het WebReader om te weten of een bepaalde URL kan worden toegestaan of ontkend (geblokkeerd).

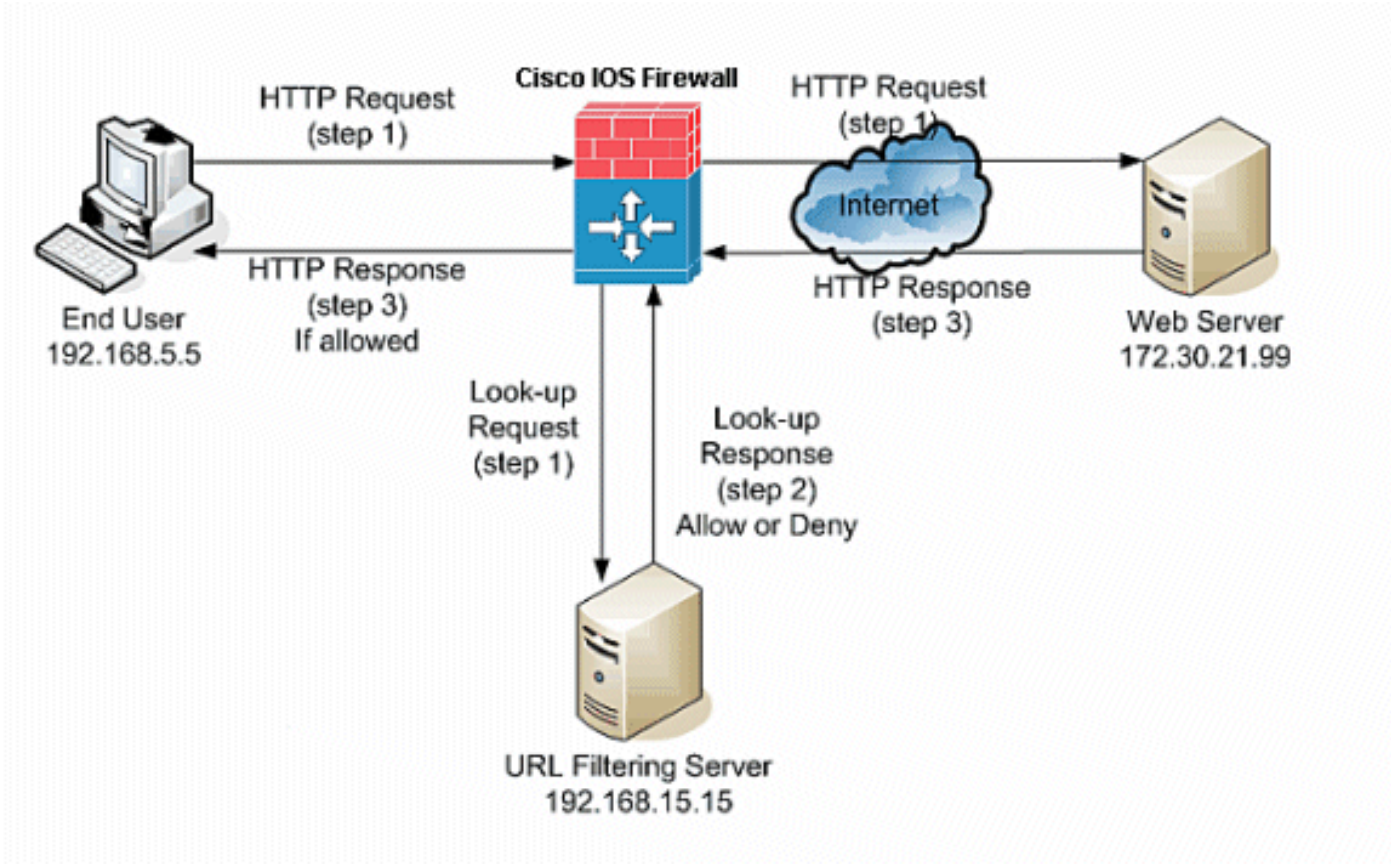
De router met CLI configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



In dit voorbeeld, wordt de URL filterserver gevestigd in het binnennetwerk. Eindgebruikers in het netwerk proberen toegang te krijgen tot de webserver buiten het netwerk via het internet.

Deze stappen worden op verzoek van de gebruiker op de webserver voltooid:

1. De eindgebruiker bladert naar een pagina op de webserver en de browser stuurt een HTTP aanvraag.
2. Nadat de Cisco IOS Firewall dit verzoek ontvangt, stuurt het het verzoek naar de webserver door. Het haalt tegelijkertijd de URL uit en stuurt een opzoek verzoek naar de URL-filterserver.
3. Nadat de URL-filterserver het look-up-verzoek ontvangt, controleert het zijn database om te bepalen of de URL al dan niet moet worden toegestaan. Het geeft een vergunning terug of ontkent status met een kijk-up reactie op de Cisco IOS® firewall.
4. De Cisco IOS® firewall ontvangt deze raadpleging en voert een van deze functies uit:Als de look-up-reactie de URL toestaat, stuurt het de HTTP-reactie naar de eindgebruiker.Als de raadpleging-reactie de URL ontkent, wijst de URL-filterserver de gebruiker terug naar zijn eigen interne webserver, die een bericht toont dat de categorie beschrijft waaronder de URL wordt geblokkeerd. Vervolgens wordt de verbinding aan beide uiteinden hersteld.

Identificeer de filtering server

U dient het adres van de filterserver te identificeren met de opdracht **van de** verkoper van de **IP-**filterserver. U moet de juiste vorm van deze opdracht gebruiken, gebaseerd op het type filterserver dat u gebruikt.

Opmerking: U kunt slechts één type server configureren, ofwel Webzin ofwel N2H2, in uw configuratie.

webzucht

WebecSony is een software van derden die HTTP-aanvragen kan filteren op basis van dit beleid:

- doelhostname
- IP-adres van bestemming
- sleutelwoorden
- gebruikersnaam

De software onderhoudt een URL-database van meer dan 20 miljoen sites die zijn georganiseerd in meer dan 60 categorieën en subcategorieën.

De **ip urlfilter server** opdracht wijst de server aan die de N2H2 of Webslin URL-filtertoepassing runt. Om een verkoper server voor URL-filtering te configureren gebruikt u de opdracht van een **ip-**filterserververkoper in de mondiale configuratie. Gebruik de no-vorm van deze opdracht om een server uit de configuratie te verwijderen. Dit is de syntaxis van de **ip urlfilter server**-opdracht:

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

Vervang `ip-adres` door het IP-adres van de webzineserver. Vervang `seconden` met het aantal seconden dat de IOS Firewall moet proberen verbinding te maken met de filterserver.

Bijvoorbeeld, om één enkele Websone filterserver voor URL filtratie te vormen, geef deze opdracht uit:

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

Het filterbeleid configureren

N.B.: U moet de URL-filterserver identificeren en inschakelen voordat u URL-filtering toestaat.

Truncate Long HTTP URL's

Om het URL-filter in staat te stellen lange URL's op de server te inkorten, gebruikt u de **opdracht IP-urlfilter** in de mondiale configuratie-modus. Gebruik de no-formulier van deze opdracht om de optie ingedrukt te houden. Deze opdracht wordt ondersteund in Cisco IOS versie 12.4(6)T en hoger.

`IP-filterfunctie {script-parameters | hostname}` is de syntaxis van deze opdracht.

script-parameters: Alleen de URL tot de script opties wordt verzonden. Als de gehele URL bijvoorbeeld `http://www.cisco.com/dev/xxx.cgi?when=now` is, `wordt` alleen de URL via `http://www.cisco.com/dev/xxx.cgi` verzonden (als de maximale ondersteunde URL-lengte niet wordt overschreden).

Hostname: Alleen de hostname wordt verstuurd. Als de gehele URL bijvoorbeeld `http://www.cisco.com/dev/xxx.cgi?when=now` is, `wordt` alleen `http://www.cisco.com` verzonden.

Als de script-parameters en de hostname sleutelwoorden beide zijn ingesteld, heeft het script-parameters sleutelwoord voorrang op het hostname sleutelwoord. Als beide zoekwoorden worden geconfigureerd en de URL van de script parameters wordt ingekort en de maximum ondersteunde URL length wordt overschreden, wordt de URL ingekort tot de hostname.

Opmerking: Als zowel trefwoorden script-parameters als hostname zijn ingesteld, moeten ze op aparte regels staan zoals hieronder wordt weergegeven. Ze kunnen niet op één lijn worden gecombineerd.

Opmerking: `IP-filterfunctie voor script-parameters`

Opmerking: `IP-hostnaam, filter truncate`

Configuratie voor router die Cisco IOS versie 12.4 uitvoert

Deze configuratie omvat de opdrachten die in dit document worden beschreven:

Configuratie voor router die Cisco IOS versie 12.4 uitvoert

```
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
```

Configureer de router met DSM

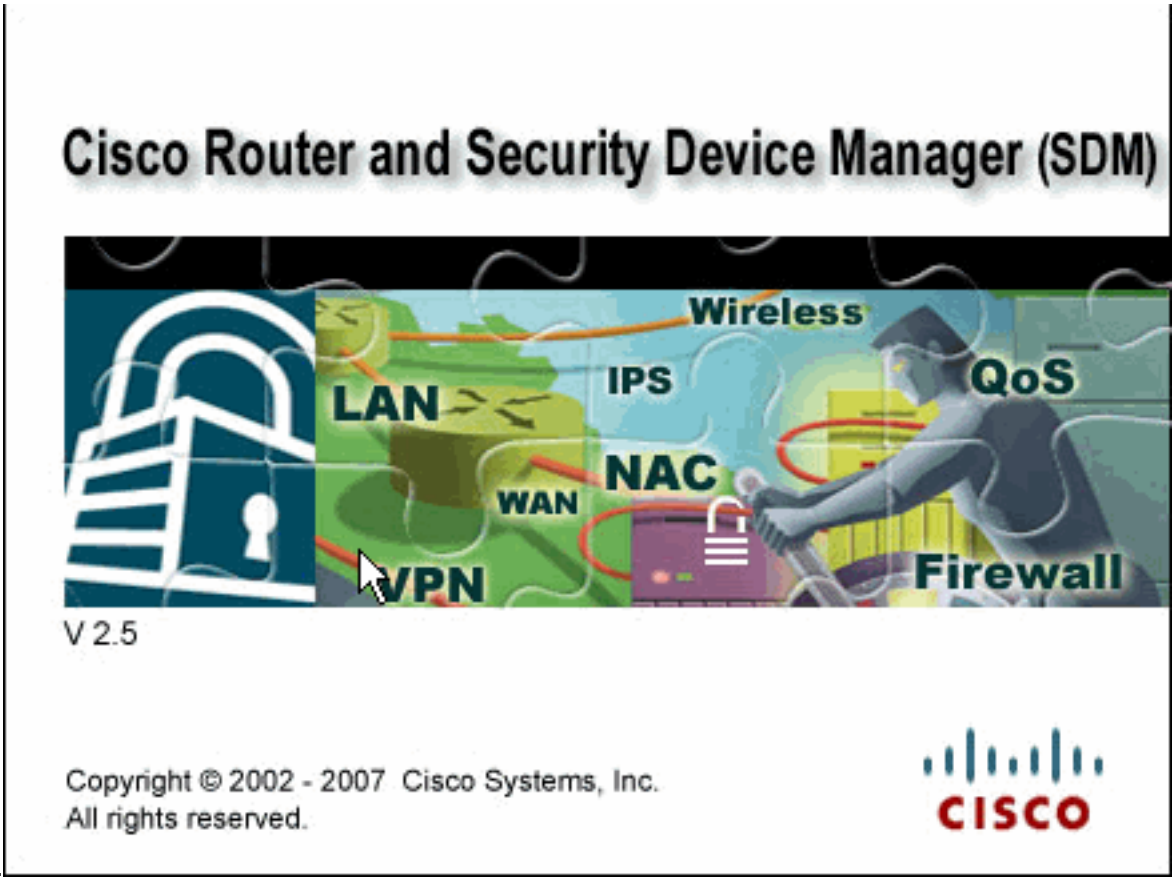
Configuratie van routerdm

Voltooi deze stappen om URL-filtering op de Cisco IOS-router te configureren:

Opmerking: Om het URL filteren met het middel te configureren gebruikt u de **ip-inspectie naam** opdracht in globale configuratiemodus om een verzameling inspectieregels te definiëren. Dit schakelt HTTP-inspectie in. Het urlfilter sleutelwoord associeert URL filteren met HTTP inspectie. Vervolgens kan de ingestelde controlenaam worden gekoppeld aan de interface waarop het filteren moet worden uitgevoerd, bijvoorbeeld:

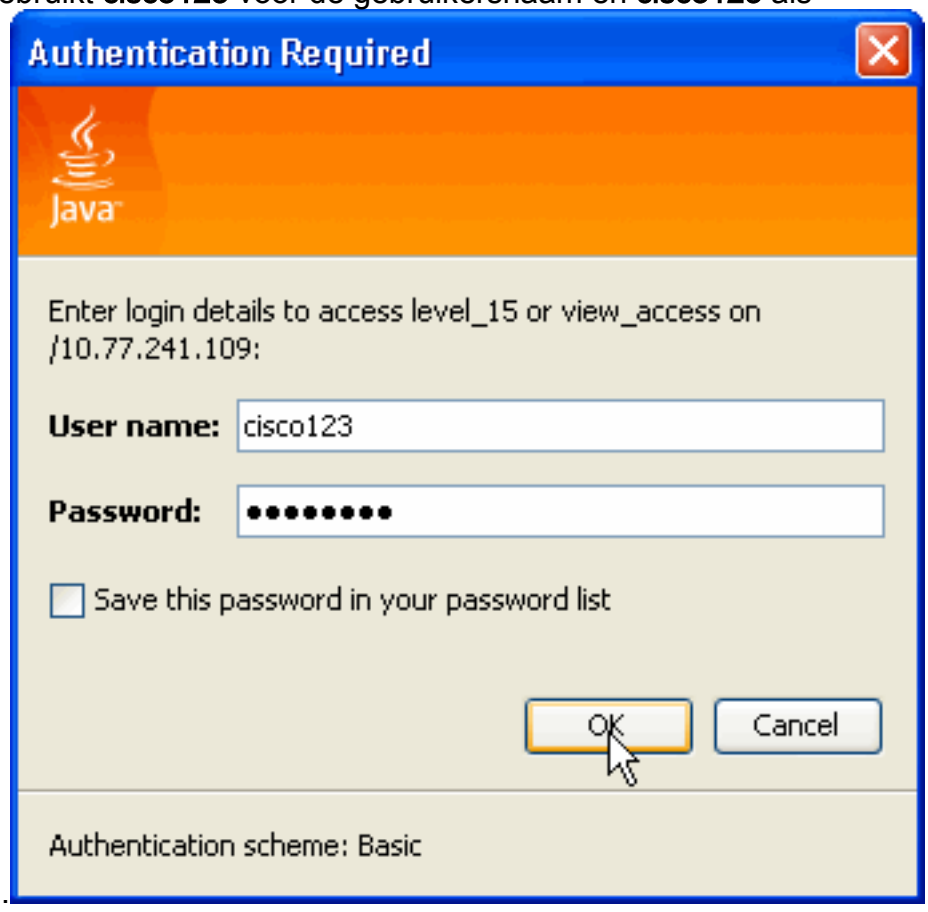
```
hostname(config)#ip inspect
   name test http urlfilter
```

1. Open uw browser en voer **https://<IP_Address van de interface van de router** in **die voor** de **Toegang** van **het** Sdm op de router **is gevormd**.Controleer of alle waarschuwingen die uw browser u geeft, geldig zijn voor de SSL-certificatie. De standaard gebruikersnaam en wachtwoord zijn beide leeg.De router stelt dit venster voor om de download van de toepassing te toestaan. Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Java-



applet.

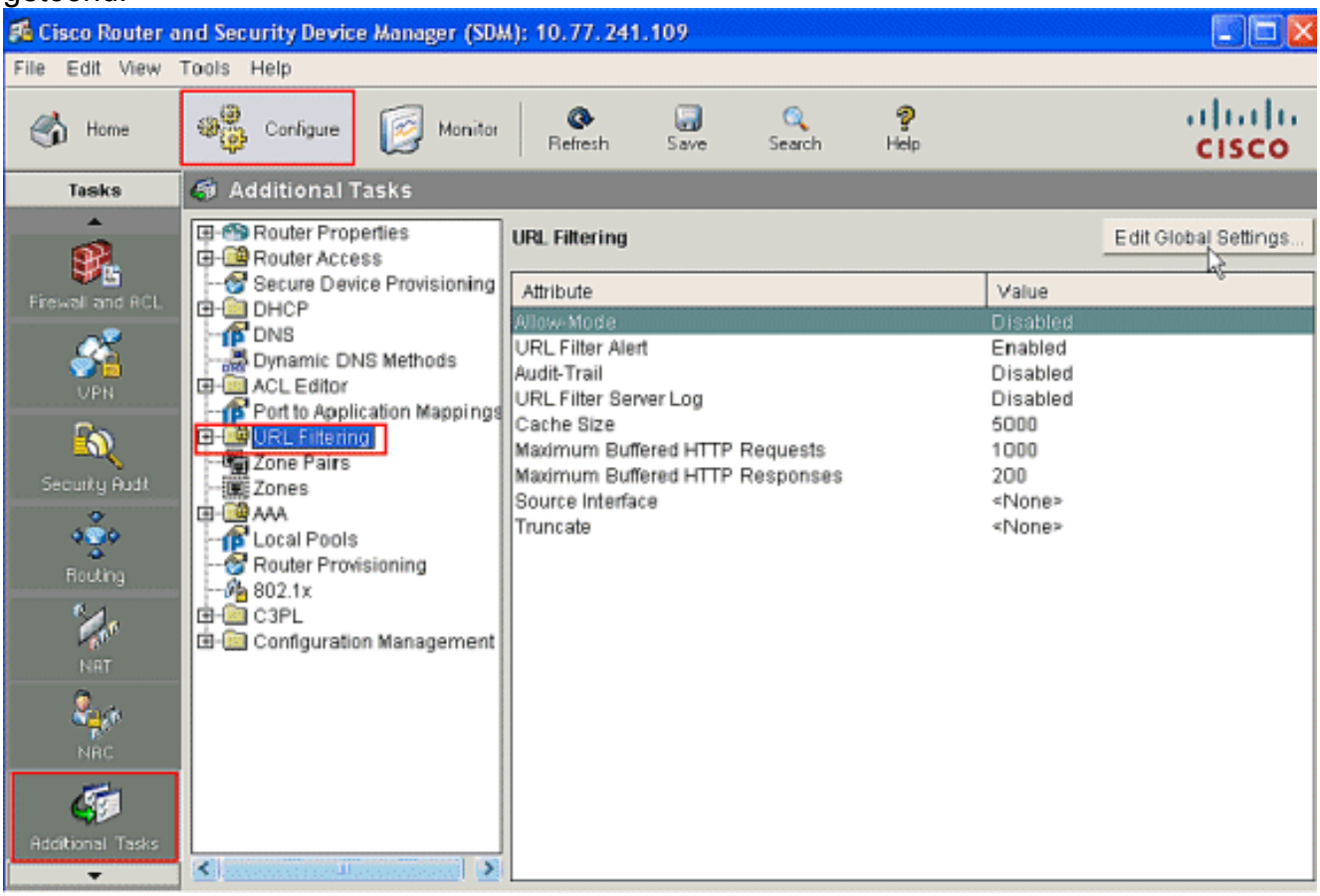
2. De download van het dm begint nu. Zodra de lantaarn van het Sdm wordt gedownload, voltooien de stappen die door de herinnering worden geregisseerd om de software te installeren en de Launcher van Cisco Sdm in werking te stellen.
3. Voer de **gebruikersnaam** en het **wachtwoord in** als u deze hebt ingesteld en klik op **OK**.Dit voorbeeld gebruikt **cisco123** voor de gebruikersnaam en **cisco123** als



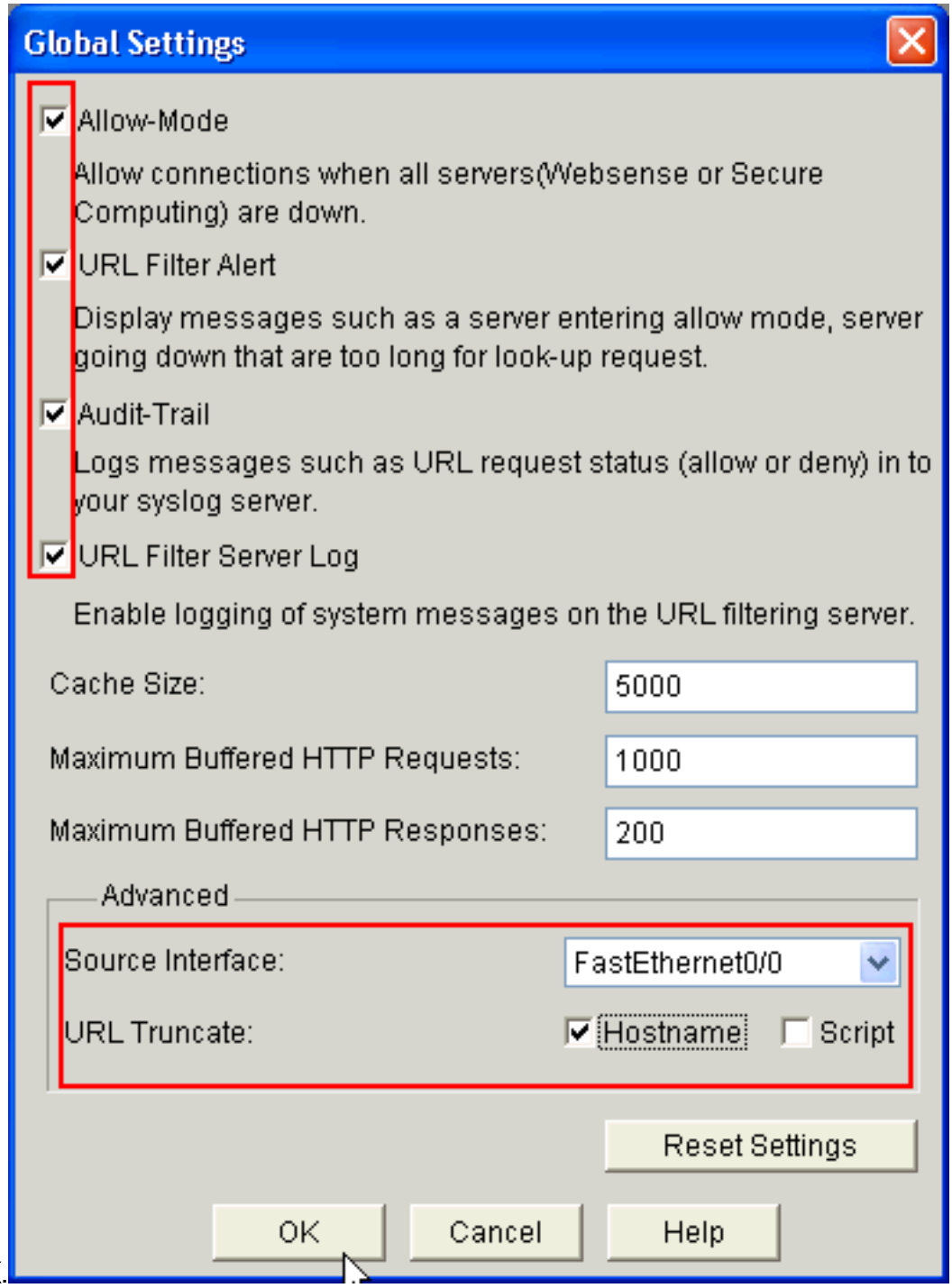
wachtwoord.

4. Kies **Configuration->**Aanvullende taken en klik op **URL Filtering** op de vanaf **het** begin

ingestelde herkenningspagina. Klik vervolgens op **Global Settings**, zoals hier wordt getoond:

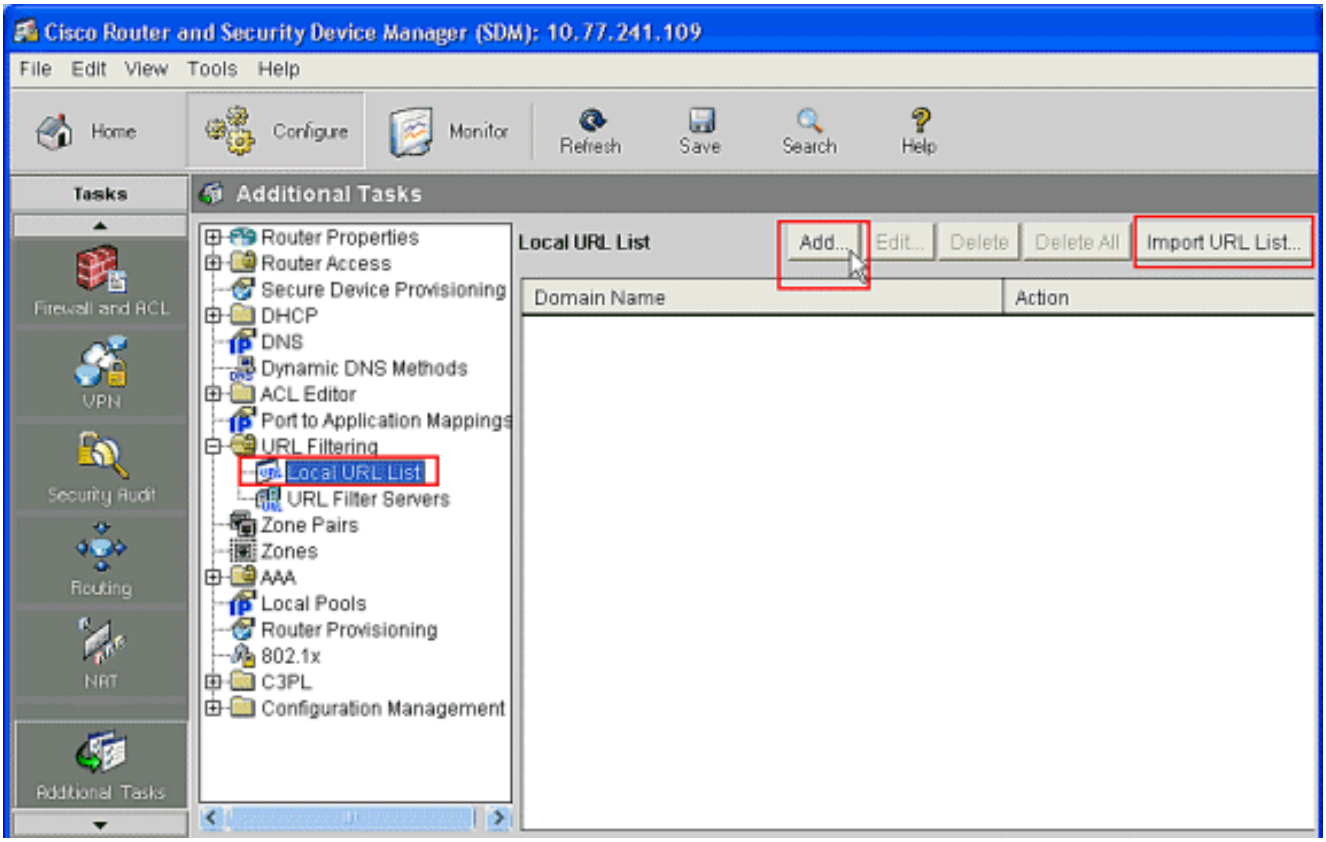


5. In het nieuwe venster dat nu wordt weergegeven, stelt u de parameters in die vereist zijn voor URL-filtering, zoals **toestaan, URL-filterwaarschuwing, Audit-Trial** en **URL-filtering van serverlogboek**. Controleer de aankruisvakjes naast elke parameters zoals aangegeven. Typ nu de informatie **Cache Size** en **HTTP Buffer**. Verstrek ook de **Bron-interface** en de **URL-truncate-methode onder de geavanceerde** sectie zoals getoond om het URL-filter in staat te stellen lange URL's naar de server te inkorten.(Hier wordt de truncatie-parameter gekozen als **Hostname.)** Klik nu op

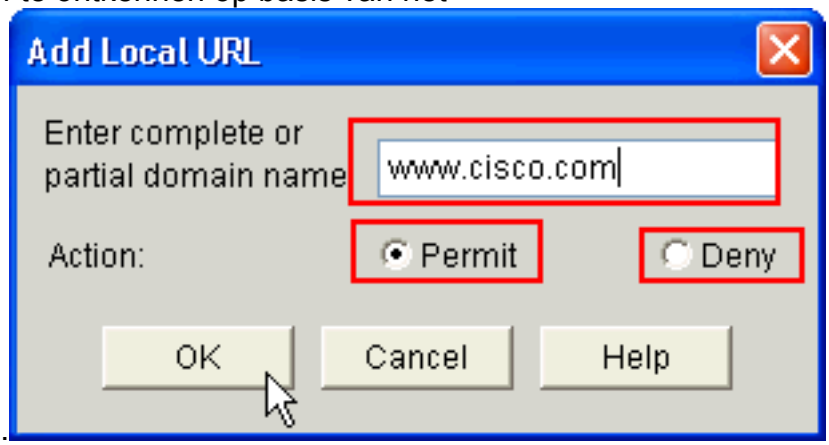


OK.

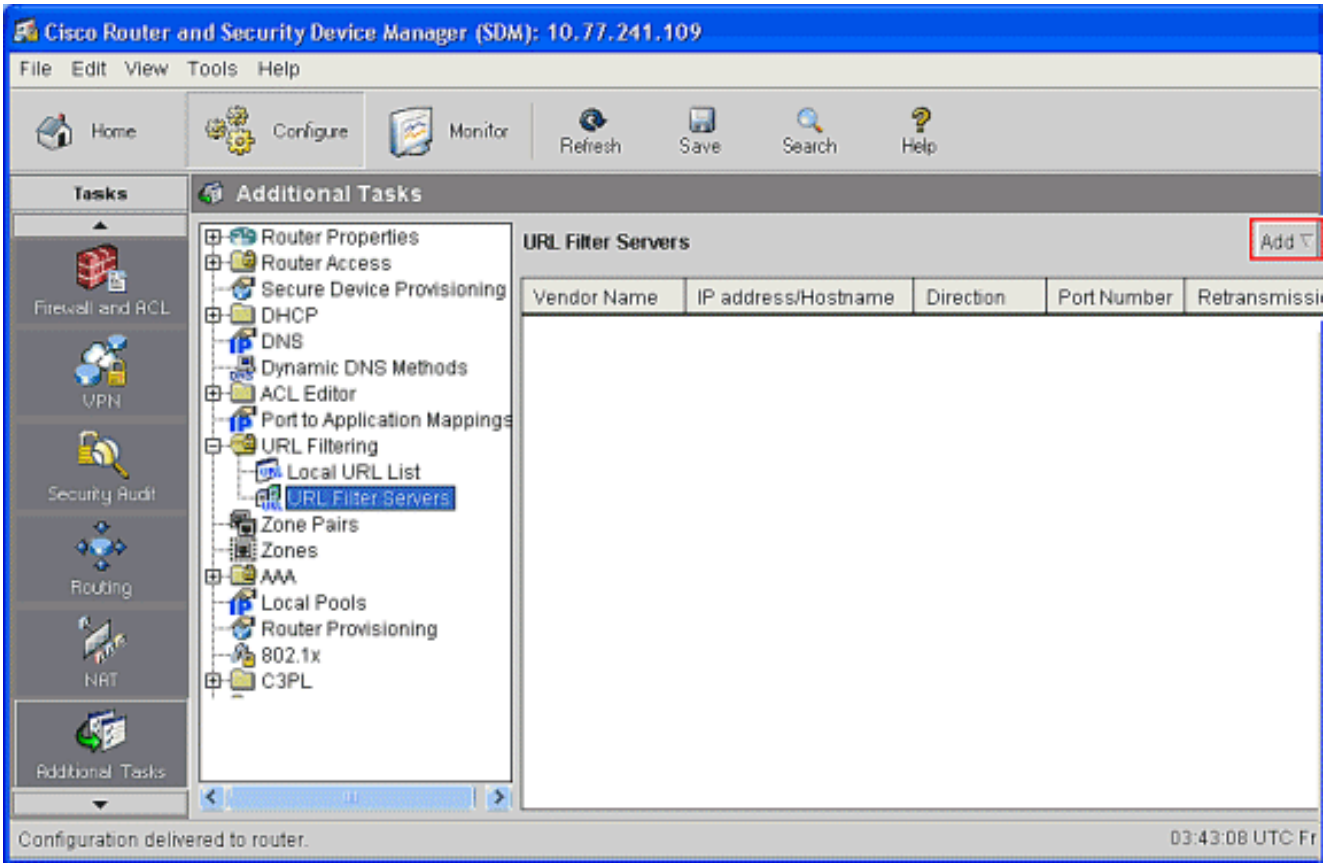
6. Kies nu de optie **Local URL List** onder het tabblad **URL Filtering**. Klik op **Add** om de domeinnaam toe te voegen en de firewall te configureren om de toegevoegde domeinnaam toe te staan of te ontkennen. U kunt ook de optie **URL-lijst importeren** kiezen als de gewenste lijst met URL's in een bestand voorkomt. U kunt kiezen uit de opties **URL** of **URL-lijst importeren** op basis van de eis en beschikbaarheid van de URL-lijst.



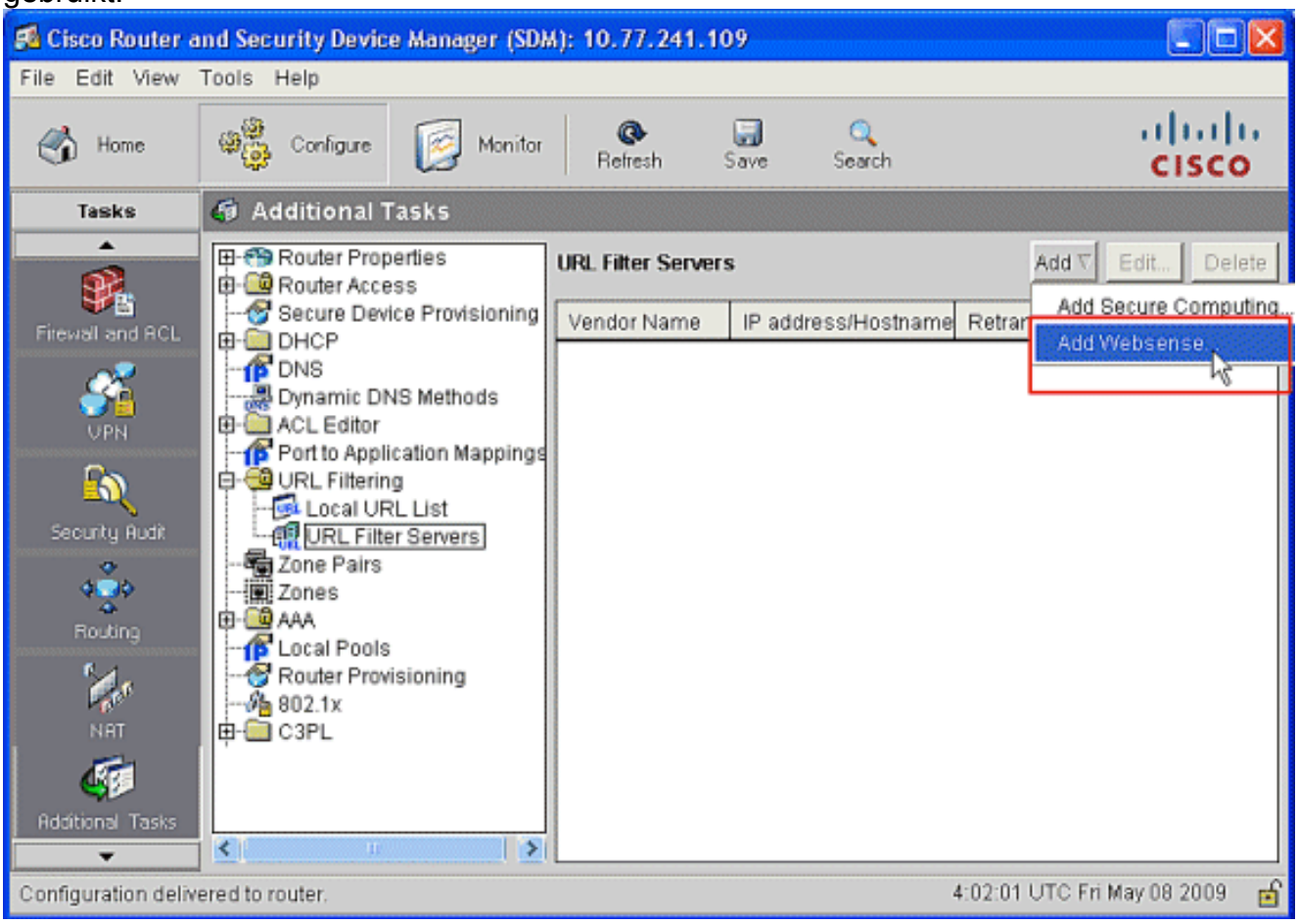
7. In dit voorbeeld, klik op **Add** om de URL toe te voegen en de IOS Firewall te configureren om de URL zoals vereist toe te staan of te ontkennen. Nu wordt een nieuw venster met de naam **ADD Local URL** geopend, waarin de gebruiker de domeinnaam moet opgeven en moet beslissen of hij de URL al dan niet toestaat of ontkent. Klik op de radioknop naast de optie Vergunning of Jeans zoals weergegeven. Hier is de domeinnaam **www.cisco.com** en de gebruiker **geeft** de **URL www.cisco.com toestemming**. Op dezelfde manier kunt u op **Add** klikken, zoveel URL's toevoegen als nodig is en de firewall configureren om een licentie te geven of te ontkennen op basis van het vereiste.



8. Kies de optie **URL Filter servers** onder het **URL Filtering** tabblad, zoals getoond. Klik op **Add** om de naam van de URL Filtering Server toe te voegen die de functie URL Filtering uitvoert.

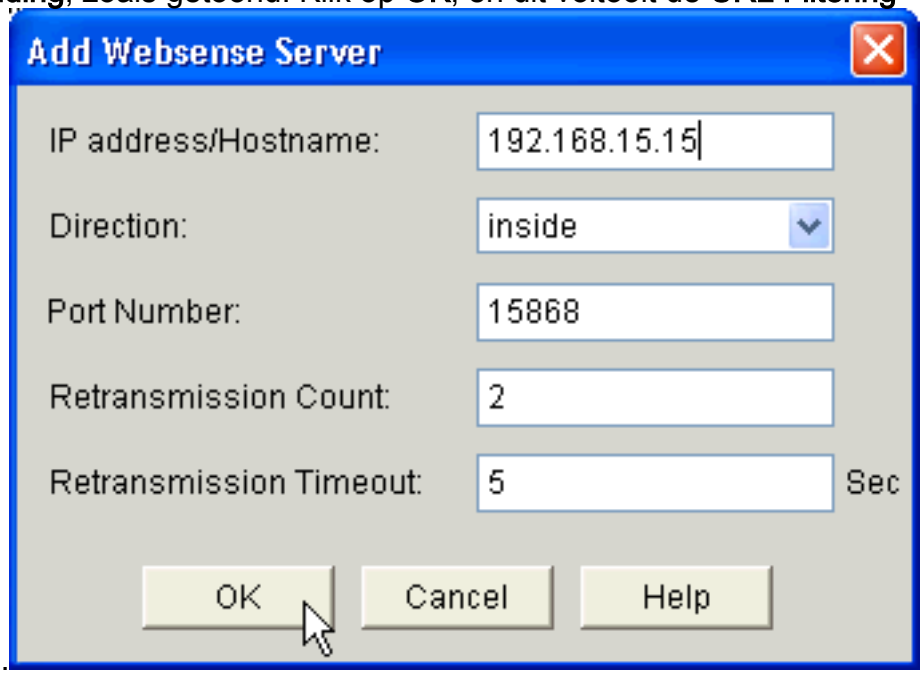


9. Nadat u op **Toevoegen** klikt, kiest u de filterserver als **Webzin** zoals hieronder wordt weergegeven, aangezien de Webzin Filtering Server in dit voorbeeld wordt gebruikt.



10. In dit venster **Add Websence Server**, typt u het **IP-adres** van de server van het **Webex** samen met **Richting** waarin het filter werkt en **Port Number,** (het standaard poortnummer voor de server van het Spark **15868).** Verstrek ook de waarden **voor** de **Time-outdoorgifte**

en **terugzending**, zoals getoond. Klik op **OK**, en dit voltooit de **URL Filtering** configuratie.



Verifiëren

Gebruik de opdrachten in deze sectie om URL-filterinformatie te bekijken. U kunt deze opdrachten gebruiken om de configuratie van het apparaat te controleren.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

- **ip urlfilter statistieken tonen** - Toont informatie en statistieken over de filterserverBijvoorbeeld:

```
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
```

- **ip urlfilter cache**-Hiermee wordt het maximale aantal items weergegeven dat in de cache-tabel kan worden gecached, het aantal items en de bestemming IP-adressen weergegeven die in de cache-tabel worden gecached wanneer u de opdracht van het topofilter in een bevoorrechte EXEC-modus gebruikt
- **Toon ip het filter. filter configuratie**-toont de filterconfiguratieBijvoorbeeld:

```
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
```

Problemen oplossen

Foutberichten

`%URLF-3-SERVER_DOWN: De verbinding met de URL filterserver 10.92.0.9 is omlaag` — Dit niveau drie LOG_ERR-type bericht wordt weergegeven wanneer een geconfigureerde UFS daalt. Wanneer dit gebeurt, zal de firewall de geconfigureerde server als secundair markeren en proberen een van de andere secundaire servers op te halen en die server als primaire server te markeren. Als er geen andere server is geconfigureerd zal de firewall de modus toelaten en het bericht `URLF-3-ALLOW_MODE` weergeven.

`%URLF-3-ALLOW_MODE: De verbinding met alle URL filter servers is gezakt en de MODUS UIT is` — Dit LOG_ERR type bericht wordt weergegeven als alle UFS zijn ingedrukt en het systeem schakelt de modus in.

Opmerking: Wanneer het systeem naar de toegestane modus gaat (alle filterservers zijn ingedrukt) wordt er een periodieke bewaarde timer geactiveerd om een TCP-verbinding te openen en een server op te halen.

`%URLF-5-SERVER_UP: Er wordt een verbinding gemaakt met een URL-filterserver 10.92.0.9. het systeem keert terug van ALLOW MODE` — Dit LOG_NOTICE-type bericht toont wanneer de UFS als omhoog worden gedetecteerd en het systeem terugkeert uit de tolerante modus.

`%URLF-4-URL_TOO_LONG:URL te lang (meer dan 3072 bytes), mogelijk een nep-pakket?` — Dit bericht van het LOG_WARNING-type toont wanneer de URL in een opzoek te lang is; Een URL die langer is dan 3K wordt ingetrokken.

`%URLF-4-MAX_REQ: Het aantal hangende aanvragen overschrijdt de maximumgrens <1000>`— Dit bericht LOG_WARNING-type wordt weergegeven wanneer het aantal hangende aanvragen in het systeem de maximumgrens overschrijdt en alle verdere verzoeken worden ingetrokken.

Gerelateerde informatie

- Cisco IOS Firewall
- FirewallURL-filtering
- Cisco IOS-beveiligingsgids, release 12.4-ondersteuning
- Technische ondersteuning en documentatie – Cisco Systems