SDM: Filtragem URL no exemplo da configuração de roteador do Cisco IOS

Índice

Introdução

Este documento demonstra como configurar a filtragem de URL em um roteador do Cisco IOS. A filtragem de URL propicia maior controle sobre o tráfego que passa pelo roteador do Cisco IOS. A Filtragem URL é apoiada nas versões do Cisco IOS na versão 12.2(11)YU e mais recente.

Nota: Porque a Filtragem URL é processo intensivo de cpu, o uso de um servidor de filtragem externo assegura-se de que a taxa de transferência do outro tráfego não seja afetada. Baseado na velocidade de sua rede e na capacidade de seu server da Filtragem URL, o tempo exigido para a conexão inicial pode ser visivelmente mais lento quando o tráfego é filtrado com um servidor de filtragem externo.

Pré-requisitos

Limitações para a Filtragem URL de Websense do Firewall

Exigência do servidor websense: A fim permitir esta característica, você deve ter pelo menos um servidor websense; , mas dois ou mais servidores websense são preferidos. Embora não haja nenhum limite ao número de servidores websense que você pode ter, e você pode configurar

tantos como server como você deseja, simplesmente um server pode ser ativo a um momento determinado — o servidor primário. Os pedidos da consulta URL são enviados somente ao servidor primário.

Limitação do apoio da Filtragem URL: Este suportes de recurso somente um esquema ativo da Filtragem URL de cada vez. (Antes que você permitir a Filtragem URL de Websense, você deve sempre se assegurar de que não haja um outro esquema da Filtragem URL configurado, como o N2H2.)

Limitação username: Esta característica não passa o username e a informação do grupo ao servidor websense, mas o servidor websense pode trabalhar para políticas USER-baseadas porque tem um outro mecanismo para permitir o username de corresponder a um endereço IP de Um ou Mais Servidores Cisco ICM NT.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2801 Router com Software Release 12.4(15)T de Cisco IOS®
- Versão 2.5 do gerenciador do dispositivo de segurança da Cisco (SDM)

Nota: Refira a configuração de roteador básico usando o SDM a fim permitir que o roteador seja configurado pelo SDM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

A característica da Filtragem URL de Websense do Firewall permite seu Cisco IOS Firewall (igualmente conhecido como o [CSIS] do Cisco Secure Integrated Software) de interagir com o software da Filtragem URL de Websense. Isto permite que você impeça o acesso de usuário aos Web site especificados com base em alguma política. O Cisco IOS Firewall trabalha com o servidor websense para saber se uma URL particular pode ser permitida ou negado (obstruído).

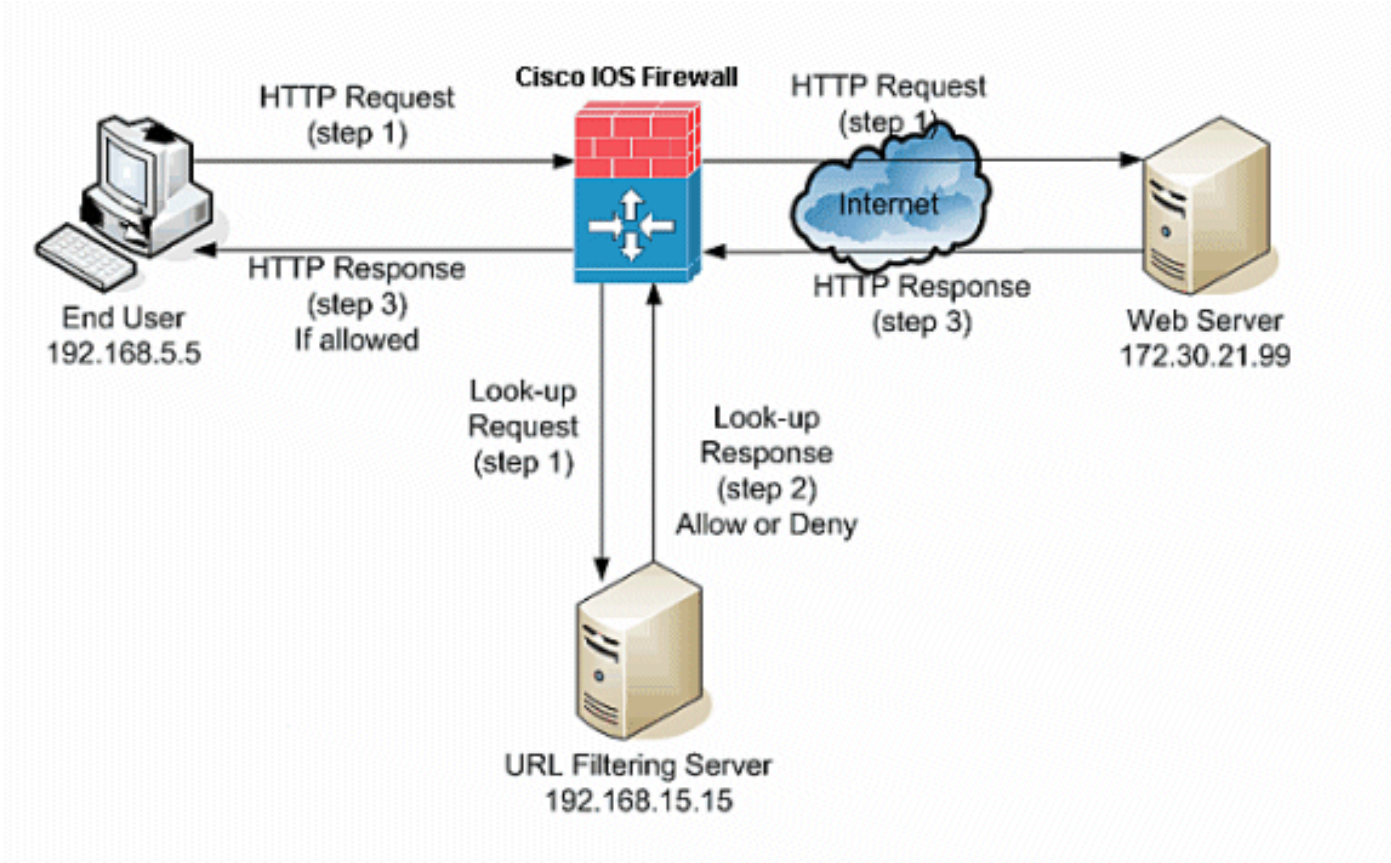
Configurar o roteador com o CLI

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Neste exemplo, o server da Filtragem URL é ficado situado na rede interna. Os utilizadores finais situados dentro da rede tentam alcançar o servidor de Web situado fora da rede sobre o Internet.

Estas etapas são terminadas na requisição de usuário para o servidor de Web:

1. O utilizador final consulta a uma página no servidor de Web, e o navegador envia um pedido do HTTP.
2. Depois que o Cisco IOS Firewall recebe este pedido, ele para a frente o pedido ao servidor de Web. Extrai simultaneamente a URL e envia um pedido da consulta ao server da Filtragem URL.
3. Depois que o server da Filtragem URL recebe o pedido da consulta, verifica seu base de dados a fim determinar se ao permit or deny a URL. Retorna um estado do permit or deny com uma resposta da consulta ao Firewall de Cisco IOS®.
4. O Firewall de Cisco IOS® recebe esta resposta da consulta e executa uma destas funções:Se a resposta da consulta permite a URL, envia a resposta HTTP ao utilizador final.Se a resposta da consulta nega a URL, o server da Filtragem URL reorienta o usuário a seu próprio servidor de Web interno, que indica uma mensagem que descreva a categoria sob que a URL é obstruída. Depois disso, a conexão é restaurada no ambas as extremidades.

Identifique o servidor de filtragem

Você precisa de identificar o endereço do servidor de filtragem com o comando do **fornecedor de**

servidor do urlfilter IP. Você deve usar o formulário apropriado deste comando baseado no tipo de servidor de filtragem que você se usa.

Nota: Você pode somente configurar um único tipo de server, Websense ou N2H2, em sua configuração.

Websense

Websense é um software de filtração da terceira que possa filtrar pedidos do HTTP com base nestas políticas:

- nome de host de destino
- endereço IP de destino
- palavras-chaves
- nome de usuário

O software mantém um base de dados URL de mais de 20 milhão locais organizados em mais de 60 categorias e subcategorias.

O comando do **fornecedor de servidor do urlfilter IP** designa o server que executa o aplicativo da Filtragem URL N2H2 ou de Websense. A fim configurar um server do vendedor para a Filtragem URL, use o comando do **fornecedor de servidor do urlfilter IP no** modo de configuração global. A fim remover um server de sua configuração, não use nenhum formulário deste comando. Esta é a sintaxe do comando do **fornecedor de servidor do urlfilter IP**:

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

Substitua o `IP address` com o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor websense. Substitua `segundos` com o número de segundos que o firewall de IOS deve continuar a tentar conectar ao servidor de filtragem.

Por exemplo, a fim configurar um único servidor de filtragem de Websense para a Filtragem URL, emita este comando:

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

Configurar a política de filtragem

Nota: Você deve identificar e permitir o server da Filtragem URL antes que você permita a Filtragem URL.

URL do HTTP longos truncados

A fim permitir que o filtro URL trunque URL longas ao server, use o comando **truncado do urlfilter IP no** modo de configuração global. A fim desabilitar a opção de truncagem, não use nenhum formulário deste comando. Este comando é apoiado na versão do Cisco IOS 12.4(6)T e mais tarde.

`urlfilter IP truncado {script-parâmetros | o hostname}` é a sintaxe deste comando.

script-parâmetros: Somente a URL até as opções do script é enviada. Por exemplo, se a URL inteira é `http://www.cisco.com/dev/xxx.cgi?when=now`, simplesmente a URL com `http://www.cisco.com/dev/xxx.cgi` está enviada (se o comprimento apoiado máximo URL não é excedido).

Hostname: Somente o hostname é enviado. Por exemplo, se a URL inteira é `http://www.cisco.com/dev/xxx.cgi?when=now`, simplesmente `http://www.cisco.com` está enviado.

Se os script-parâmetros e as palavras-chaves ambas do hostname são configurados, a palavra-chave dos script-parâmetros toma a precedência sobre a palavra-chave do hostname. Se o ambas as palavras-chave está configurado e os parâmetros URL do script estão truncados e o comprimento apoiado máximo URL está excedido, a URL está truncada até o hostname.

Nota: Se os script-parâmetros e o hostname do ambas as palavras-chave são configurados, devem estar em linhas separadas como mostrado abaixo. Não podem ser combinados em uma linha.

Nota: `script-parâmetros truncados do urlfilter IP`

Nota: `hostname truncado do urlfilter IP`

Configuração para roteador que executa a versão do Cisco IOS 12.4

Esta configuração inclui os comandos descritos neste documento:

Configuração para roteador que executa a versão do Cisco IOS 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
```

Configurar o roteador com SDM

Configuração de SDM do roteador

Termine estas etapas a fim configurar a Filtragem URL no roteador do Cisco IOS:

Nota: A fim configurar a Filtragem URL com SDM, use o **comando ip inspect name no** modo de configuração global definir um grupo de regras da inspeção. Isto gerencie sobre a inspeção HTTP. A palavra-chave do urlfilter associa a Filtragem URL com a inspeção HTTP. Então o nome da inspeção configurado pode ser traçado à relação em que a filtração deve ser feita, por exemplo:

```
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**

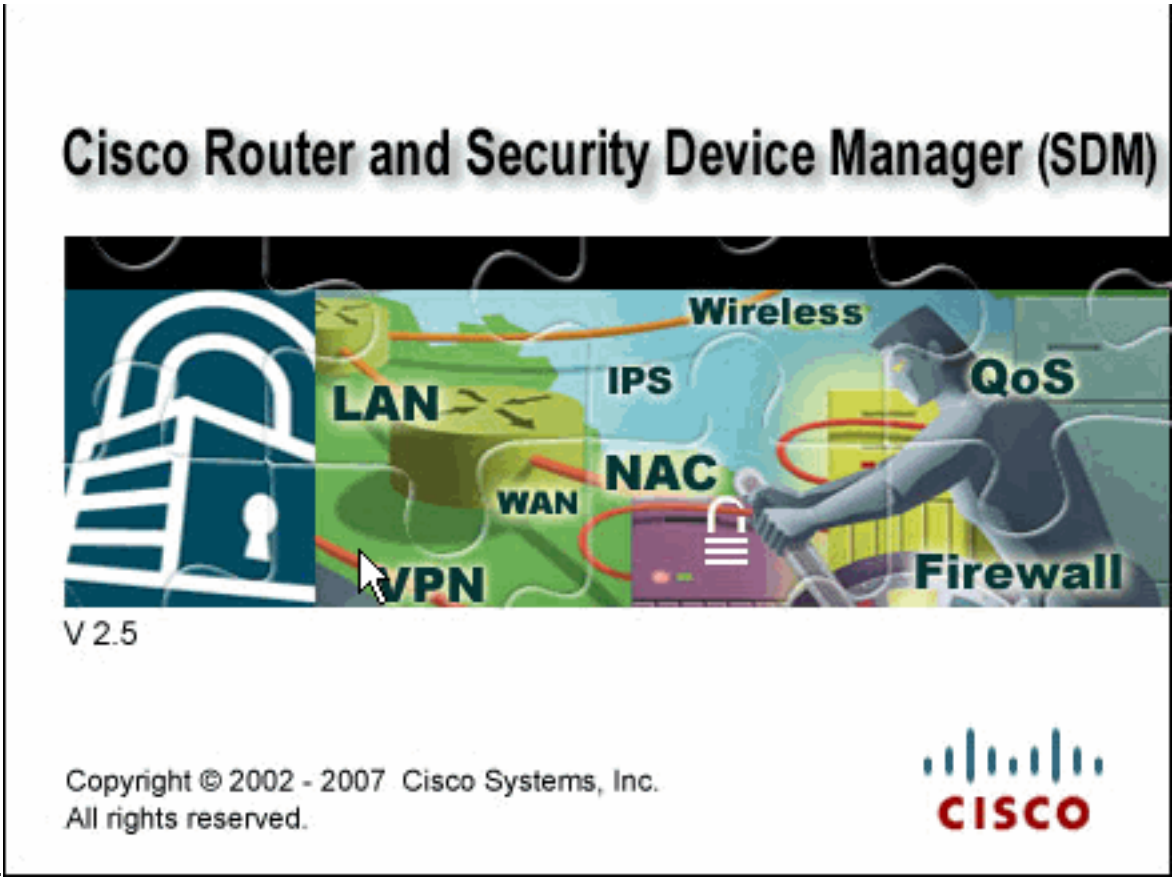
```
no ftp-server write-enable
!
!
```

!--- 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
```

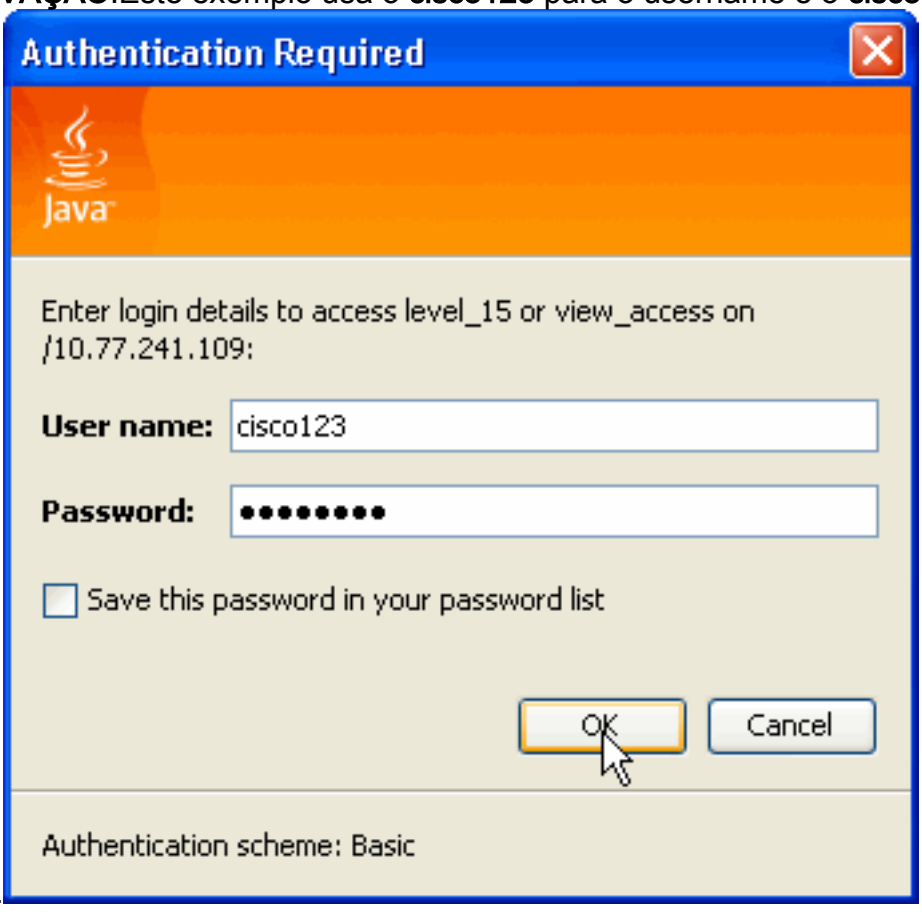
```
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!

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
```

1. Abra seu navegador e incorpore **<IP_Address de https:// da relação do roteador que foi configurado para SDM Access>** para alcançar o SDM no roteador.Certifique-se autorizar todos os avisos que seu navegador o der relativo à autenticidade de certificado de SSL. O nome de usuário padrão e a senha são ambos placa.O roteador apresenta este indicador para permitir a transferência do aplicativo SDM. Este exemplo carrega o aplicativo no computador local e não o é executado em um Java



applet.

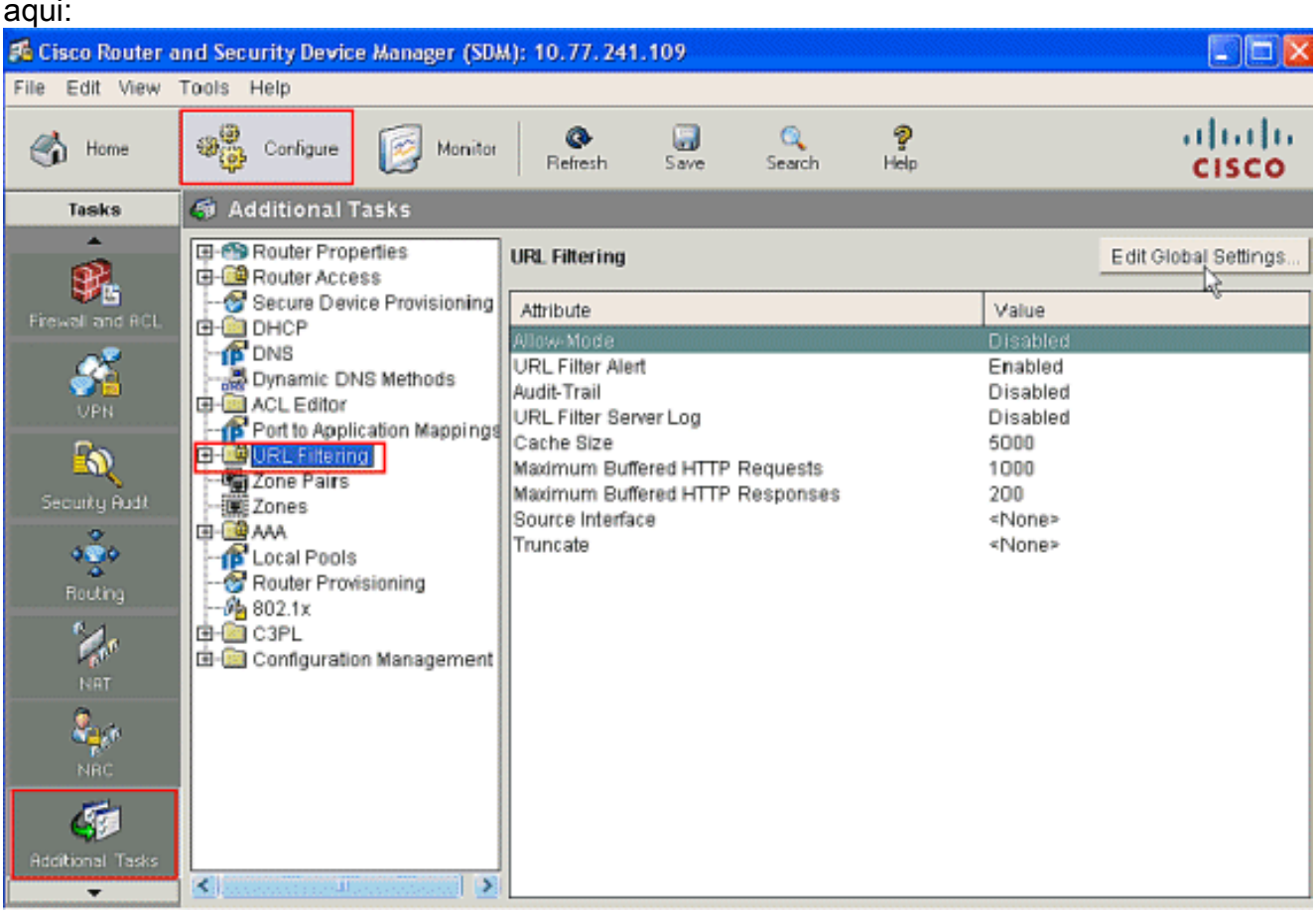
2. A transferência SDM começa agora. Uma vez as transferências do lançador SDM, terminam as etapas dirigidas pelas alertas a fim instalar o software e executar o lançador de Cisco SDM.
3. Incorpore o **nome de usuário e senha**, se você especificou um, e clique a **APROVAÇÃO**.Este exemplo usa o **cisco123** para o username e o **cisco123** como a



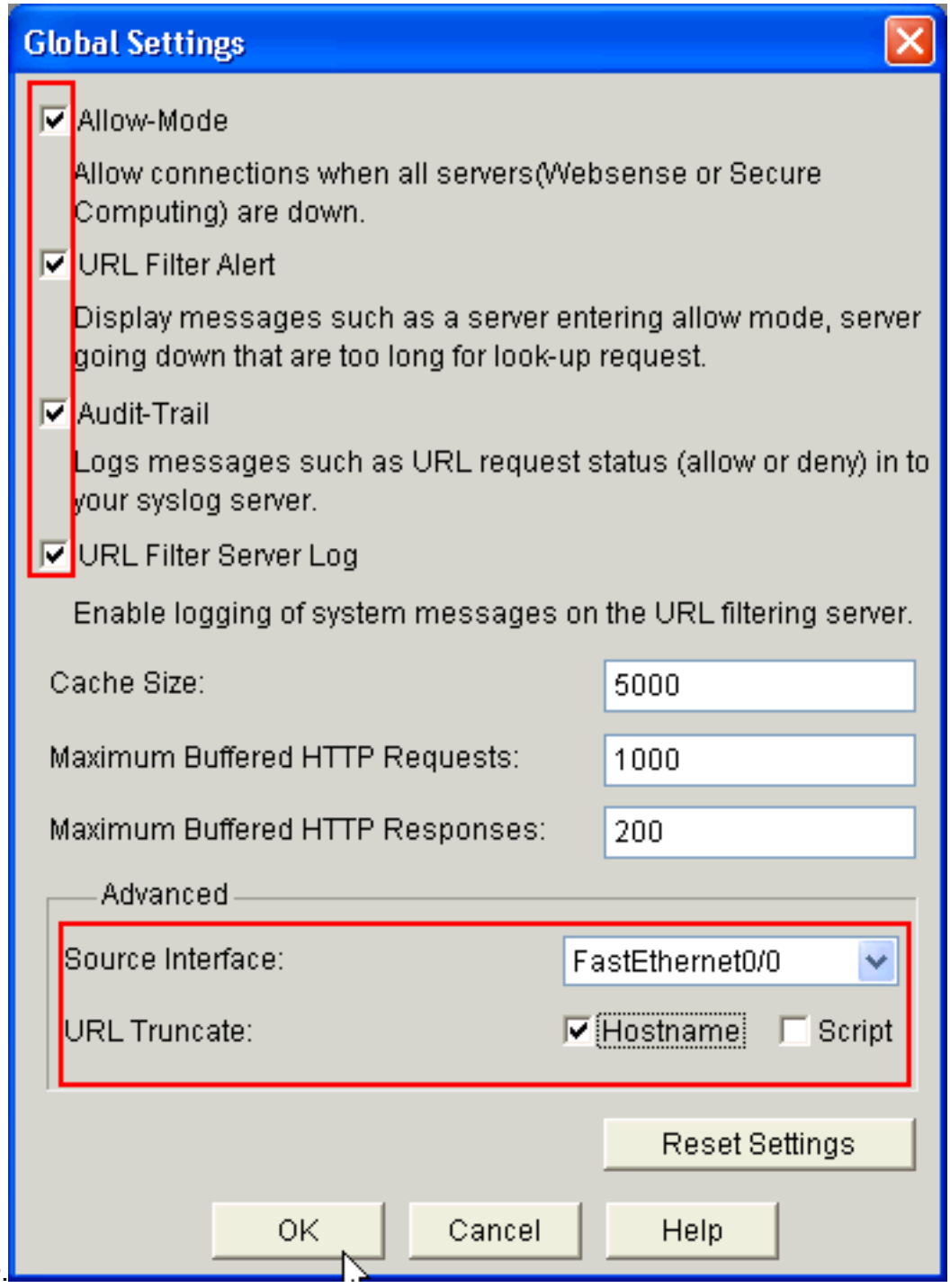
senha.

4. Escolha **tarefas de Configuration->Additional** e clique a **Filtragem URL no** Home Page SDM.

Clique então **editam configurações globais**, como mostrado aqui:

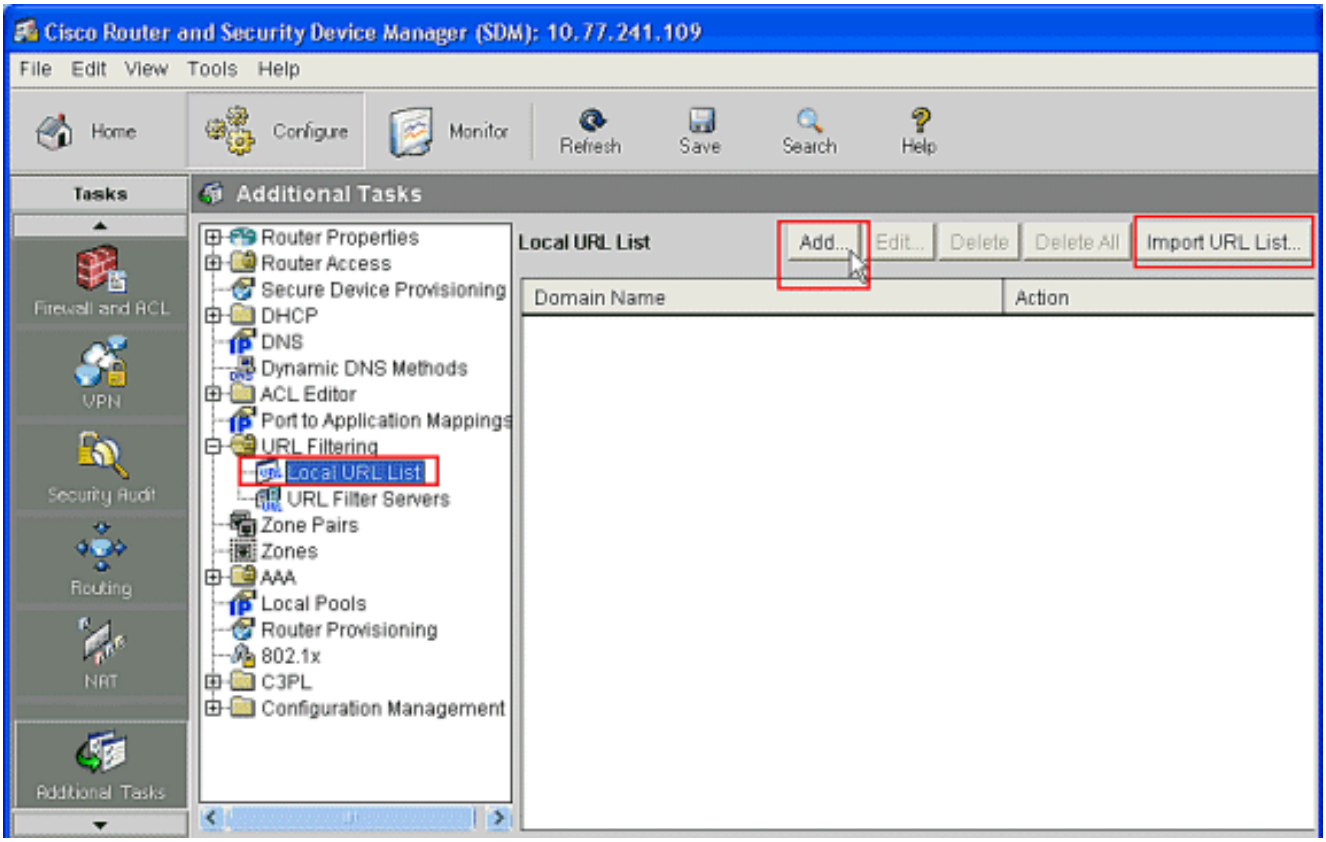


5. Na nova janela que aparece, permita os parâmetros exigidos para a Filtragem URL, tal como o **alerta Permitir-MODE, de filtro URL, a Auditoria-experimentação** e o **log de servidor da Filtragem URL**. Verifique as caixas de seleção ao lado do cada parâmetros como mostrado. Forneça agora a informação do **tamanho de cache** e do **buffer HTTP**. Igualmente forneça a **interface de origem** e o método truncado URL sob a seção **avançada** como mostrado para permitir que o filtro URL trunque URL longas ao server. (O parâmetro do truncamento é escolhido aqui como o **hostname**.) Clique agora a

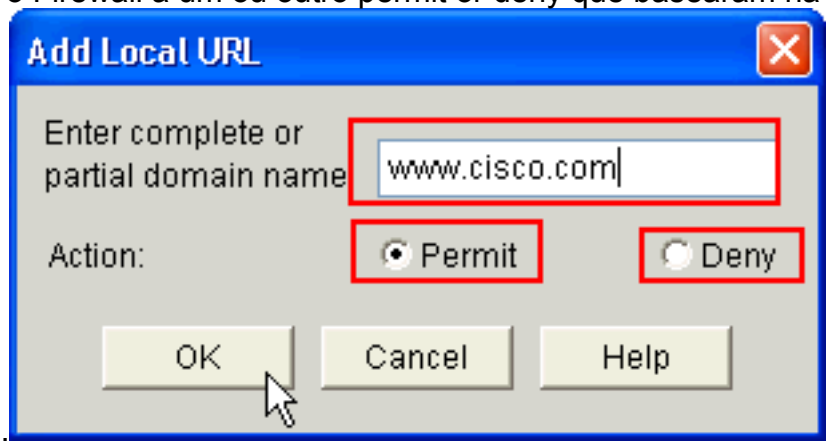


APROVAÇÃO.

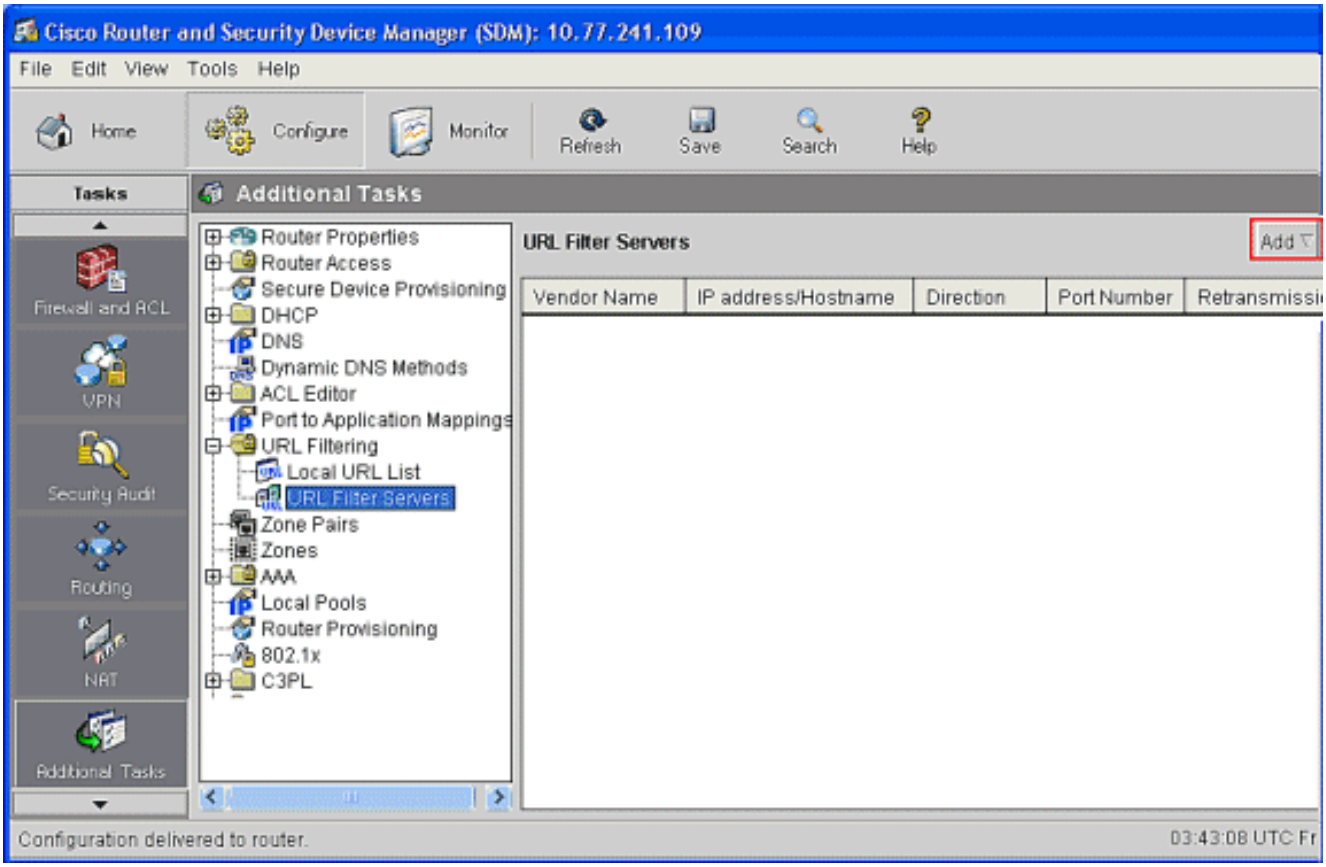
6. Escolha agora a opção **local da lista URL** situada sob a aba da **Filtragem URL**. O clique **adiciona** a fim adicionar o Domain Name e para configurar o Firewall ao permit or deny que o Domain Name adicionou. Você pode igualmente escolher a **lista URL de importação da** opção se a lista de URL necessárias esta presente como um arquivo. A escolha é a vossa para escolher **adicionar URL** ou as opções da **lista URL da importação** baseadas na exigência e na Disponibilidade da lista
URL.



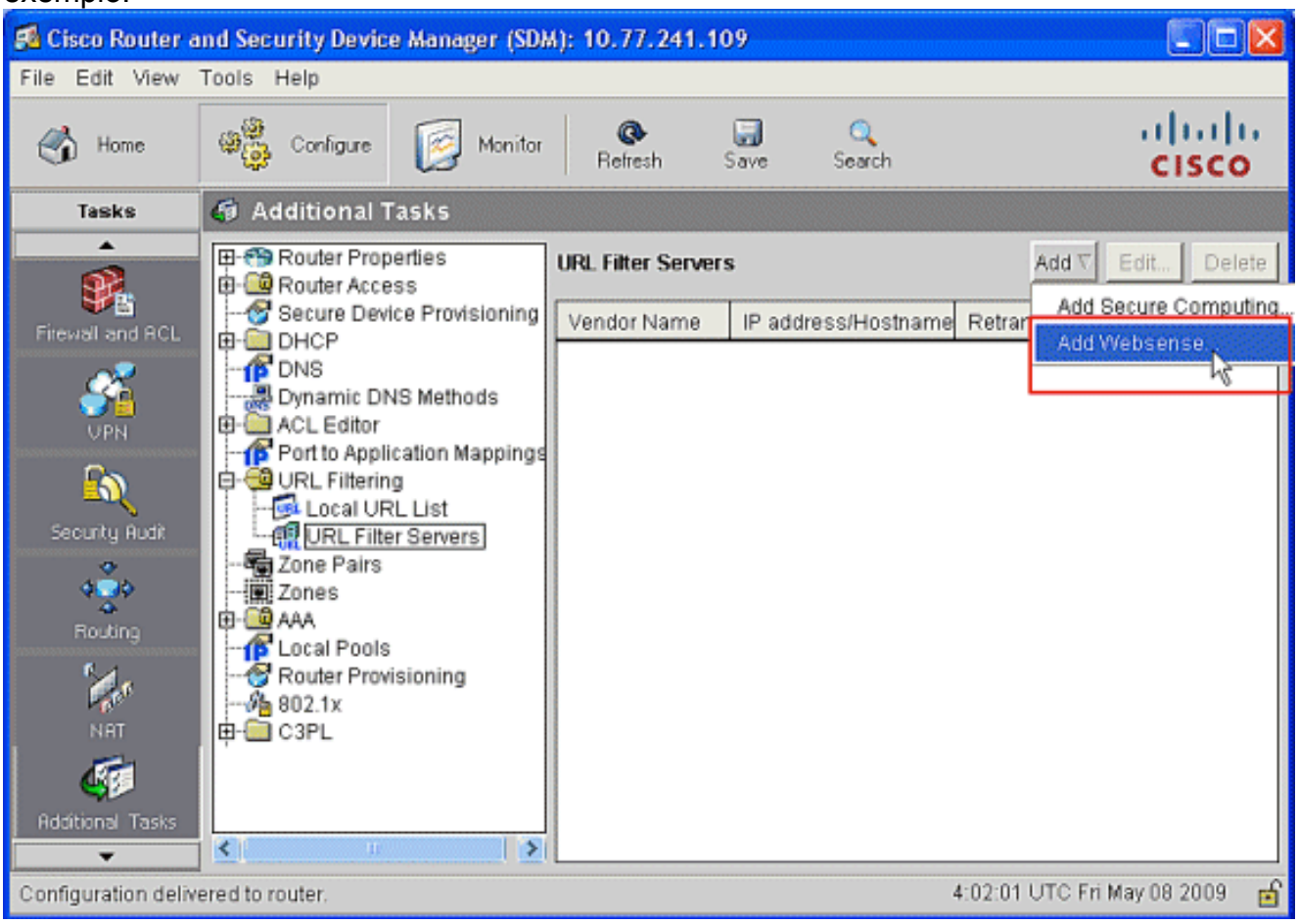
7. Neste exemplo, o clique **adiciona** para adicionar a URL e para configurar como necessário o firewall de IOS ao permit or deny a URL. Agora uma nova janela autorizada **ADICIONA A URL local** abre em qual o usuário tem que fornecer o Domain Name e decidir se ao permit or deny a URL. Clique o botão de rádio ao lado da opção do permit or deny como mostrado. Aqui o Domain Name é **www.cisco.com**, e o usuário **permite a URL www.cisco.com**. Da mesma forma, você pode clicar **adiciona**, adiciona tantas como URL como necessárias, e configura o Firewall a um ou outro permit or deny que basearam na exigência.



8. Escolha a **opção Servidores do filtro URL** situada sob a aba da **Filtragem URL**, como mostrado. O clique **adiciona** a fim adicionar o nome do servidor da Filtragem URL que executa a função da Filtragem
URL.

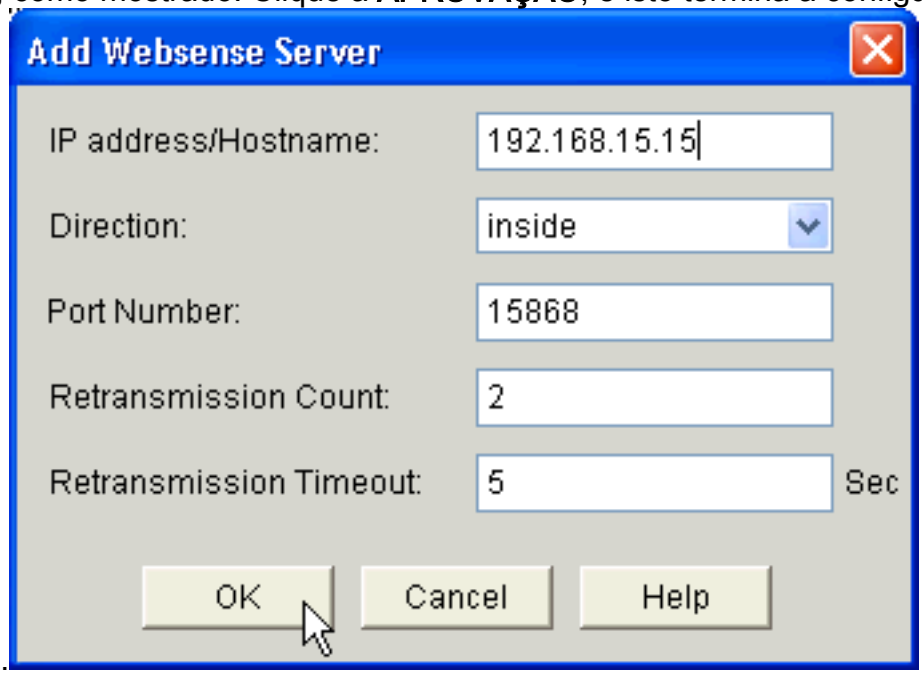


9. Depois que você clique **adiciona**, escolha o servidor de filtragem como **Websense** como mostrado abaixo desde que o servidor de filtragem de Websense é usado neste exemplo.



10. Nisto **adicionar o** indicador do **servidor websense**, forneça o **endereço IP de Um ou Mais Servidores Cisco ICM NT do** servidor websense junto com o **sentido em** que o filtro funciona e **número de porta,** (o número de porta padrão para o servidor websense é

15868). Igualmente forneça a **contagem da retransmissão** e os **valores de timeout da retransmissão**, como mostrado. Clique a **APROVAÇÃO**, e isto termina a configuração da Filtragem URL.



Verificar

Use os comandos nesta seção a fim ver a informação da Filtragem URL. Você pode usar estes comandos a fim verificar sua configuração.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

- mostre estatísticas do urlfilter IP — Mostras informação e estatísticas sobre o servidor de filtragemPor exemplo:

```
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
```

- mostre o esconderijo do urlfilter IP — Indica o número máximo de entradas que podem ser postas em esconderijo na tabela de cache, no número de entradas, e nos endereços IP de destino que estão postos em esconderijo na tabela de cache quando você usa o comando cache do urlfilter da mostra IP no modo de exec privilegiado
- mostre a configuração do filtro do urlfilter IP — Mostra a configuração de filtraçãoPor exemplo:

```
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
```

Troubleshooting

Mensagens de erro

`%URLF-3-SERVER_DOWN: A conexão ao server 10.92.0.9 do filtro URL é para baixo` — exibições de mensagem deste LOG_ERR-type do nível três quando um UFS configurado vai para baixo. Quando isto acontece, o Firewall marcará o servidor configurado como secundário e tentá-lo-á trazer acima um dos outros servidores secundários e marcar esse server como o servidor primário. Se não há nenhum outro server configurado, o Firewall entrará permite o modo e indica a mensagem `URLF-3-ALLOW_MODE`.

`%URLF-3-ALLOW_MODE: A conexão a todos os server do filtro URL está para baixo e PERMITE O MODE está` — este tipo exibições de mensagem LOG_ERR quando todos os UFS estão para baixo, e o sistema entram permitem o modo.

Nota: Sempre que o sistema entra em permita o modo (todos os server do filtro estão para baixo), um temporizador periódico da manutenção de atividade é provocado que tente abrir uma conexão de TCP e trazer acima um server.

`%URLF-5-SERVER_UP: A conexão a um server 10.92.0.9 do filtro URL é feita; o sistema está retornando de PERMITE O MODE` — exibições de mensagem deste LOG_NOTICE-type quando os UFS são detectados enquanto acima de e os retornos do sistema do modo reservar.

`%URLF-4-URL_TOO_LONG:URL demasiado por muito tempo (mais de 3072 bytes), possivelmente um pacote falsificado?` — Exibições de mensagem deste LOG_WARNING-type quando a URL em um pedido da consulta for demasiado longa; toda a URL do que 3K é deixada cair mais por muito tempo.

`%URLF-4-MAX_REQ: O número de pedido pendente excede o limite máximo <1000>` — as exibições de

mensagem deste LOG_WARNING-type quando o número de pedidos pendentes no sistema excede o limite máximo, e tudo pedem mais são deixados cair.

Informações Relacionadas

- Cisco IOS Firewall
- Filtragem URL de Websense do Firewall
- Manual de configuração do Cisco IOS Security, liberação 12.4-Support
- Suporte Técnico e Documentação - Cisco Systems