SDM Esempio di configurazione del filtro URL sul router Cisco IOS

Sommario

Introduzione

In questo documento viene spiegato come configurare il filtro URL su un router Cisco IOS. Il filtro URL offre un controllo maggiore sul traffico che attraversa il router Cisco IOS. Il filtro URL è supportato nelle versioni di Cisco IOS a partire dalla 12.2(11)YU.

Nota: poiché il filtro URL richiede un elevato utilizzo della CPU, l'uso di un server di filtro esterno assicura che il throughput di altro traffico non venga influenzato. In base alla velocità della rete e alla capacità del server di filtro URL, il tempo richiesto per la connessione iniziale può essere sensibilmente più lento quando il traffico viene filtrato con un server di filtro esterno.

Prerequisiti

Restrizioni per il filtro URL di Firewall Websense

Requisiti del server Websense: Per abilitare questa funzionalità, è necessario disporre di almeno un server Websense;, ma sono preferiti due o più server Websense. Sebbene non vi siano limiti al numero di server Websense che è possibile avere e sia possibile configurare tutti i server che si desidera, solo un server può essere attivo alla volta: il server principale. Le richieste di ricerca

URL vengono inviate solo al server principale.

Restrizione di supporto del filtro URL: Questa funzionalità supporta solo uno schema di filtro URL attivo alla volta. Prima di abilitare il filtro URL di Websense, è necessario verificare che non sia configurato un altro schema di filtro URL, ad esempio N2H2.

Restrizione nome utente: Questa funzionalità non consente di passare le informazioni sul nome utente e sul gruppo al server Websense, ma il server Websense può funzionare per i criteri basati sull'utente perché dispone di un altro meccanismo che consente al nome utente di corrispondere a un indirizzo IP.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 2801 router con software Cisco IOS® versione 12.4(15)T
- Cisco Security Device Manager (SDM) versione 2.5

Nota: per consentire al router di essere configurato dal modello SDM, consultare il documento sulla configurazione base del router utilizzando l'SDM.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

La funzionalità di filtro URL di Firewall Websense consente al firewall Cisco IOS (noto anche come Cisco Secure Integrated Software [CSIS]) di interagire con il software di filtro URL di Websense. In questo modo è possibile impedire l'accesso degli utenti a siti Web specifici in base a determinati criteri. Il firewall Cisco IOS interagisce con il server Websense per sapere se un particolare URL può essere autorizzato o rifiutato (bloccato).

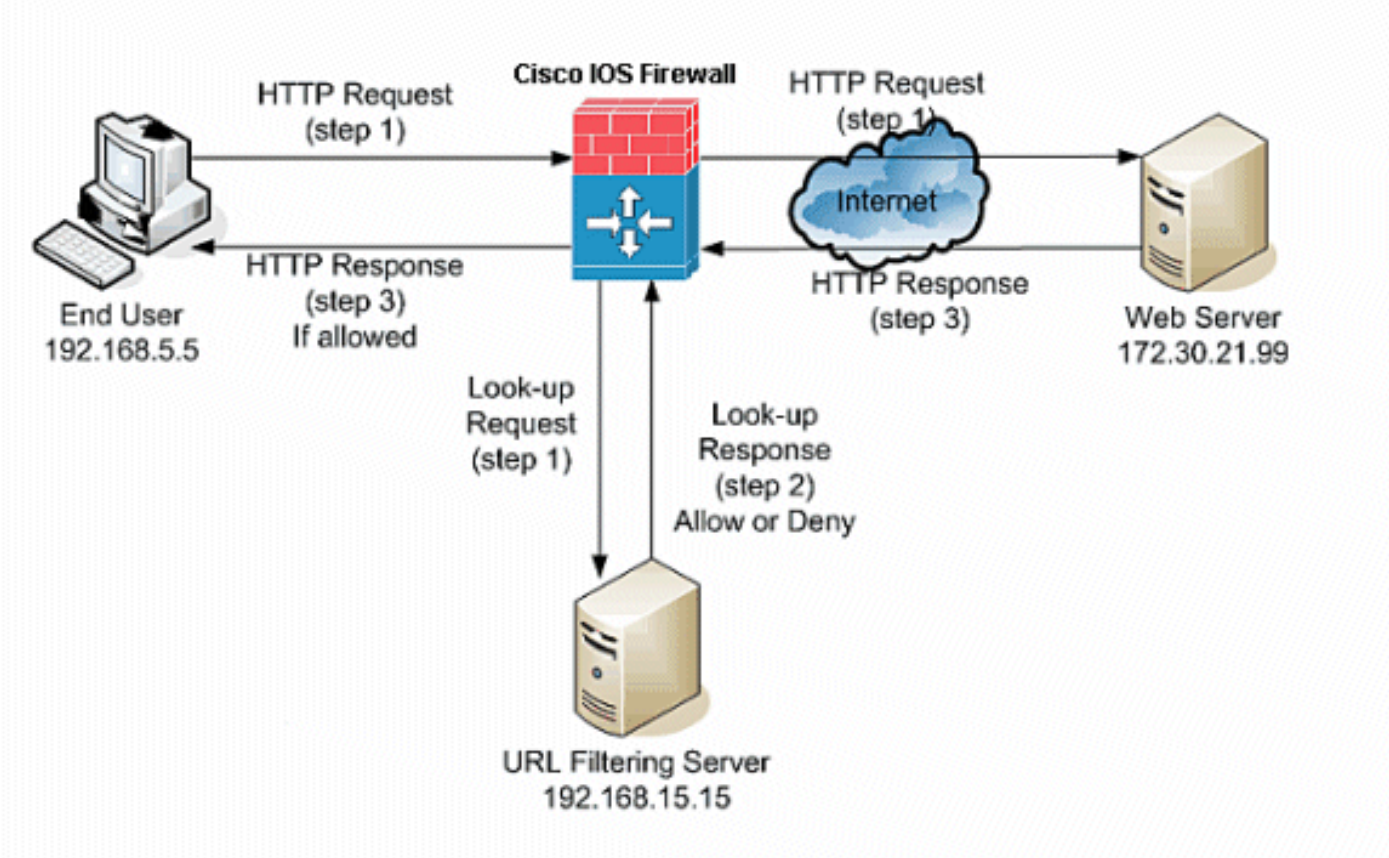
Configurazione del router con la CLI

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nell'esempio, il server del filtro URL si trova nella rete interna. Gli utenti finali che si trovano all'interno della rete tentano di accedere tramite Internet al server Web che si trova all'esterno della rete.

Questi passaggi vengono completati su richiesta dell'utente per il server Web:

1. L'utente finale accede a una pagina sul server Web e il browser invia una richiesta HTTP.
2. Dopo aver ricevuto la richiesta, Cisco IOS Firewall la inoltra al server Web. Estrae contemporaneamente l'URL e invia una richiesta di ricerca al server di filtro URL.
3. Dopo aver ricevuto la richiesta di ricerca, il server filtro URL controlla il database per stabilire se autorizzare o negare l'URL. Restituisce lo stato di autorizzazione o rifiuto con una risposta di ricerca al firewall Cisco IOS®.
4. Il firewall Cisco IOS® riceve questa risposta alla ricerca ed esegue una delle seguenti funzioni:Se la risposta di ricerca consente l'URL, invia la risposta HTTP all'utente finale.Se la risposta di ricerca nega l'URL, il server filtro URL reindirizza l'utente al proprio server Web interno, in cui viene visualizzato un messaggio in cui viene descritta la categoria in cui l'URL è bloccato. In seguito, la connessione viene ripristinata su entrambe le estremità.

Identificare il server di filtro

Ènecessario identificare l'indirizzo del server di filtro con il comando **ip urlfilter server vendor**. È necessario utilizzare la forma appropriata di questo comando in base al tipo di server di filtro utilizzato.

Nota: nella configurazione è possibile configurare un solo tipo di server, Websense o N2H2.

Websense

Websense è un software di filtraggio di terze parti in grado di filtrare le richieste HTTP sulla base di questi criteri:

- hostname di destinazione
- indirizzo IP di destinazione
- parole chiave
- nome utente

Il software gestisce un database di URL di oltre 20 milioni di siti organizzati in più di 60 categorie e sottocategorie.

Il comando **ip urlfilter server vendor** designa il server che esegue l'applicazione di filtro URL N2H2 o Websense. Per configurare un server fornitore per il filtro URL, usare il comando **ip urlfilter server vendor** in modalità di configurazione globale. Per rimuovere un server dalla configurazione, utilizzare la forma no di questo comando. Questa è la sintassi del comando **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]
```

Sostituire `ip-address` con l'indirizzo IP del server websense. Sostituire `secondi` con il numero di secondi durante i quali il firewall IOS deve continuare a tentare di connettersi al server di filtro.

Ad esempio, per configurare un singolo server di filtro Websense per il filtro URL, usare questo comando:

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

Configurare i criteri di filtro

Nota: prima di abilitare il filtro URL, è necessario identificare e abilitare il server filtro URL.

Tronca URL HTTP lunghi

Per consentire al filtro URL di troncare URL lunghi sul server, utilizzare il comando ip urlfilter truncate in modalità di configurazione globale. Per disabilitare l'opzione di troncamento, utilizzare la forma no di questo comando. Questo comando è supportato in Cisco IOS versione 12.4(6)T e successive.

`ip urlfilter tronca {parametri-script | nomehost}` è la sintassi del comando.

parametri script: Viene inviato solo l'URL fino alle opzioni script. Ad esempio, se l'intero URL è `http://www.cisco.com/dev/xxx.cgi?when=now`, viene inviato solo l'URL da `http://www.cisco.com/dev/xxx.cgi` (se la lunghezza massima supportata dell'URL non viene superata).

Hostname:viene inviato solo il nome host. Ad esempio, se l'intero URL è

`http://www.cisco.com/dev/xxx.cgi?when=now`, viene inviato solo `http://www.cisco.com`.

Se sono configurati entrambi i parametri script e le parole chiave hostname, la parola chiave script-parameters ha la precedenza sulla parola chiave hostname. Se entrambe le parole chiave sono configurate e l'URL dei parametri dello script viene troncato e viene superata la lunghezza massima supportata dell'URL, l'URL viene troncato fino al nome host.

Nota: se sono configurati sia le parole chiave script-parameters che hostname, devono trovarsi su righe separate, come mostrato di seguito. Non possono essere combinati in un'unica riga.

Nota: `parametri-script troncati ip urlfilter`

Nota: `ip urlfilter troncamento nome host`

Configurazione per il router con Cisco IOS versione 12.4

Questa configurazione include i comandi descritti nel presente documento:

Configurazione per il router con Cisco IOS versione 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
```

Configurazione del router con SDM

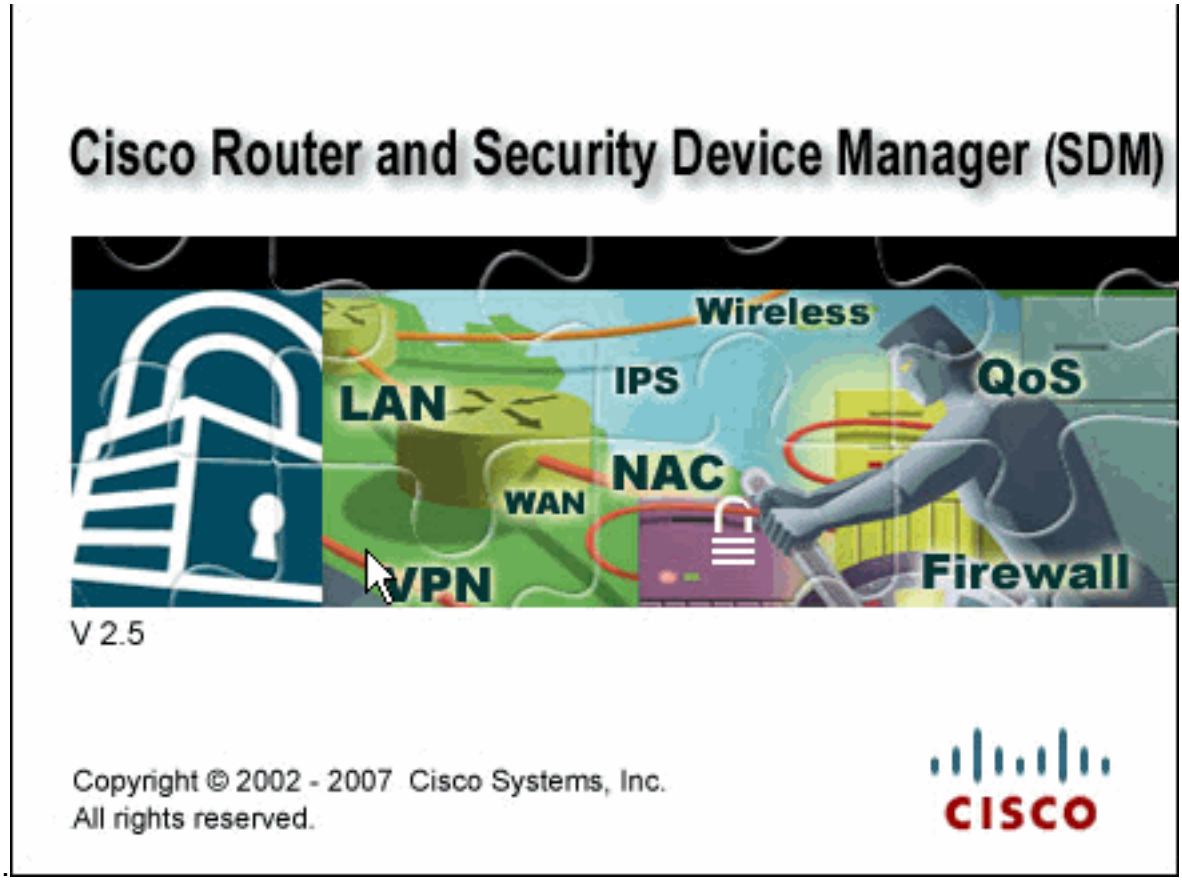
Configurazione SDM router

Completare questa procedura per configurare il filtro URL sul router Cisco IOS:

Nota: per configurare il filtro URL con il modello SDM, usare il comando **ip inspect name** in modalità di configurazione globale per definire una serie di regole di ispezione. Questa opzione attiva l'ispezione HTTP. La parola chiave urlfilter associa il filtro URL all'ispezione HTTP. Il nome di ispezione configurato può quindi essere mappato all'interfaccia su cui deve essere eseguito il filtro, ad esempio:

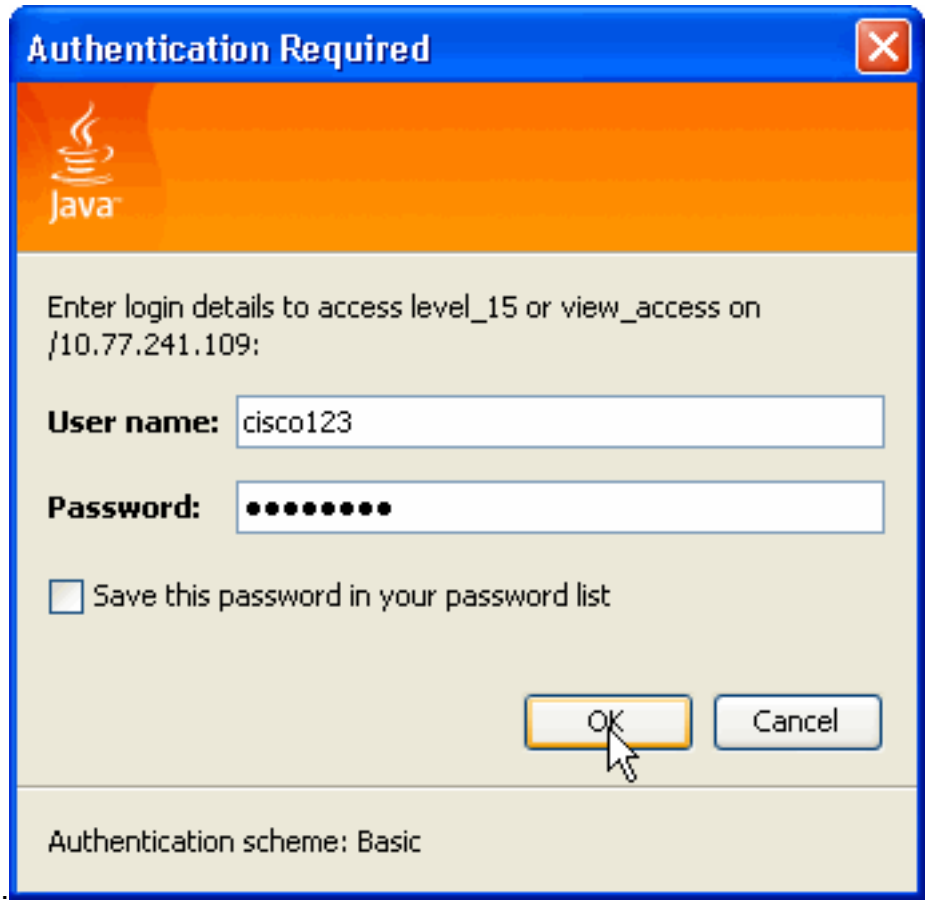
```
hostname(config)#ip inspect
   name test http urlfilter
```

1. Aprire il browser e immettere **https://<Indirizzo_IP dell'interfaccia del router configurata per l'accesso SDM>** per accedere al modulo SDM sul router.Accertarsi di autorizzare gli avvisi che il browser visualizza relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.Il router visualizza questa finestra per consentire il download dell'applicazione SDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet



Java.

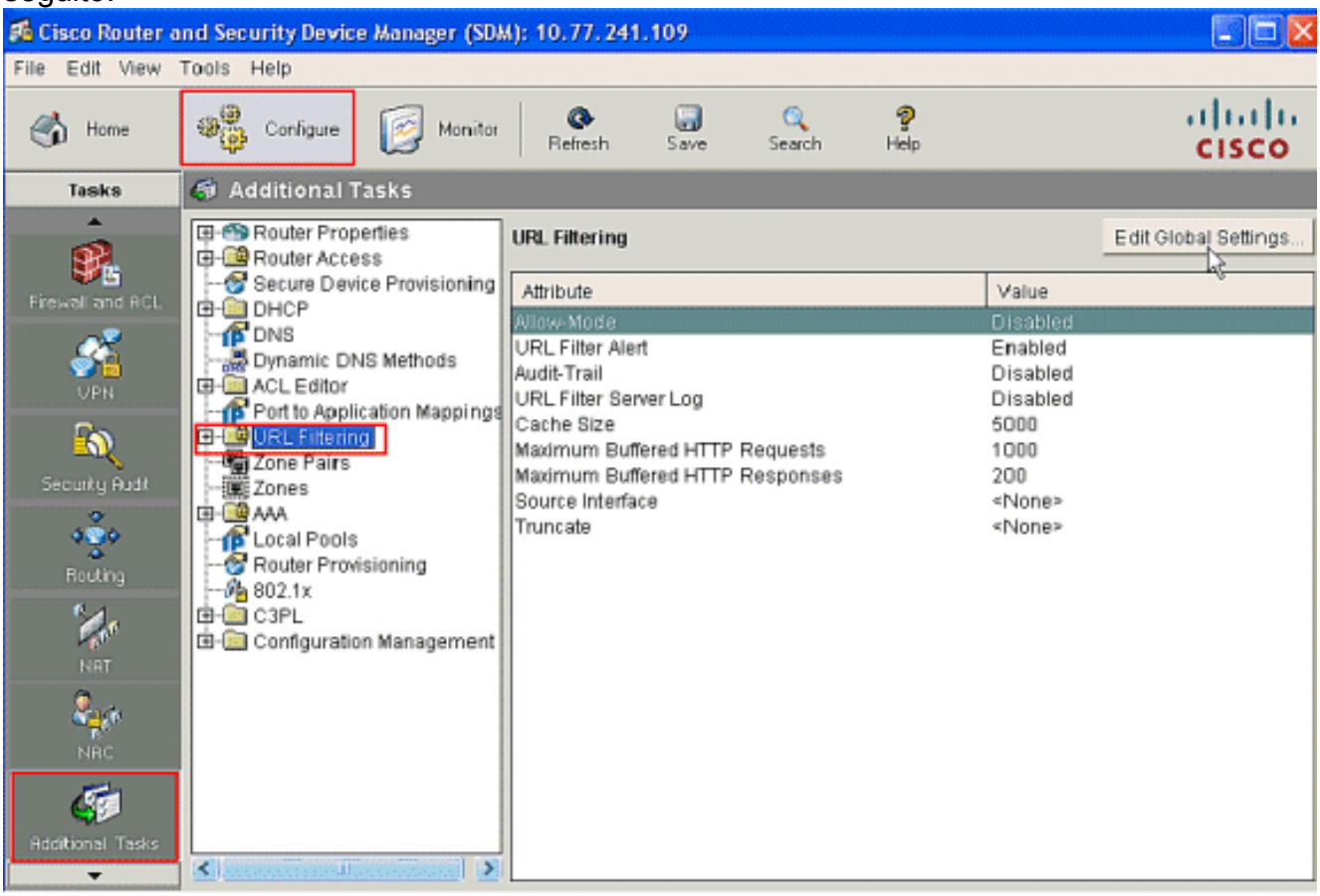
2. Il download dell'SDM ha inizio ora. Una volta scaricato l'utilità di avvio SDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio SDM di Cisco.
3. Immettere il **Nome utente** e la **Password**, se specificati, e fare clic su **OK**.In questo esempio viene utilizzato **cisco123** come nome utente e **cisco123** come



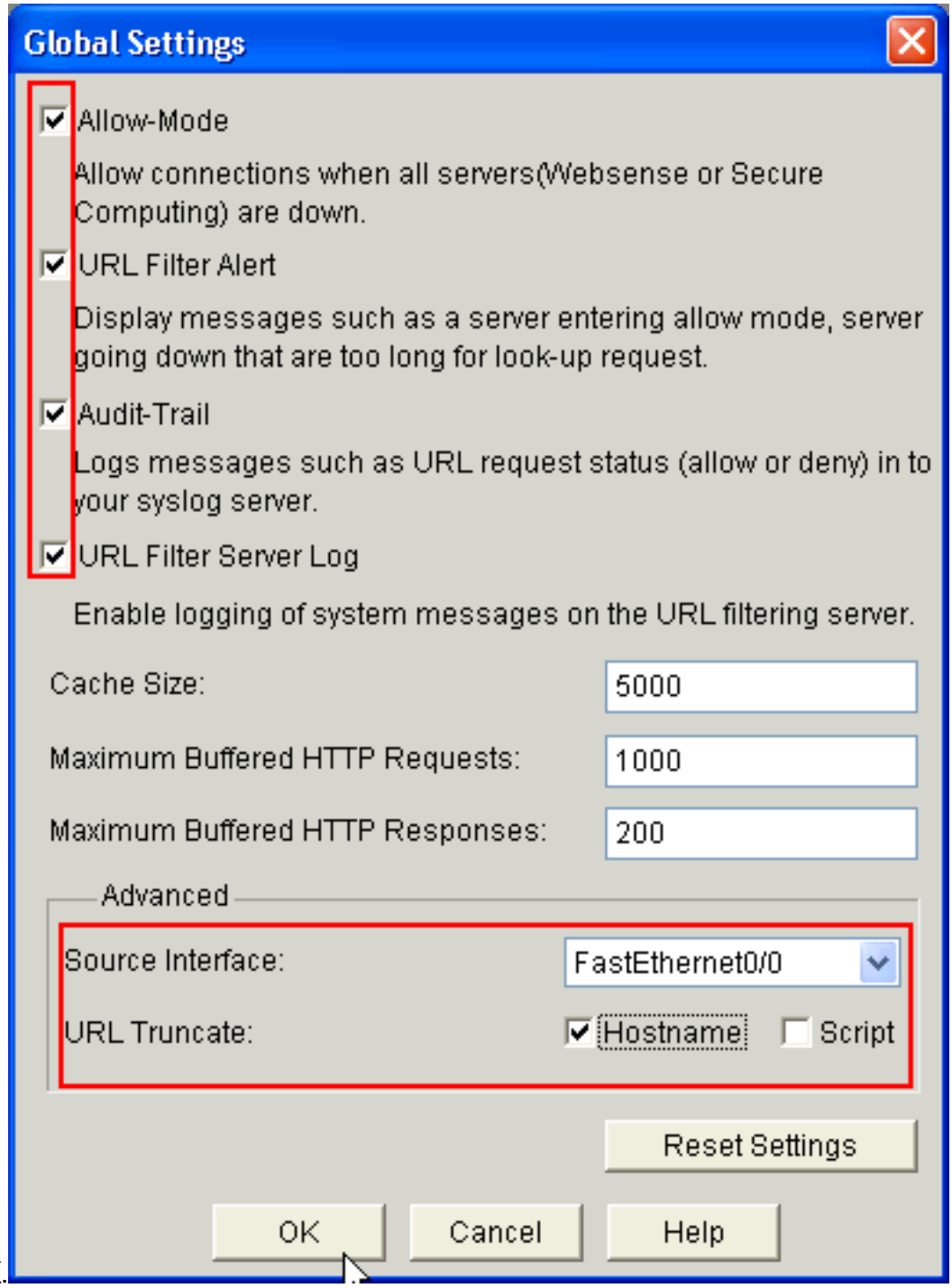
password.

4. Selezionare **Configurazione->Altre attività**, quindi fare clic su **Filtro URL** nella home page

SDM. Quindi fare clic su **Modifica impostazioni globali**, come mostrato di seguito:

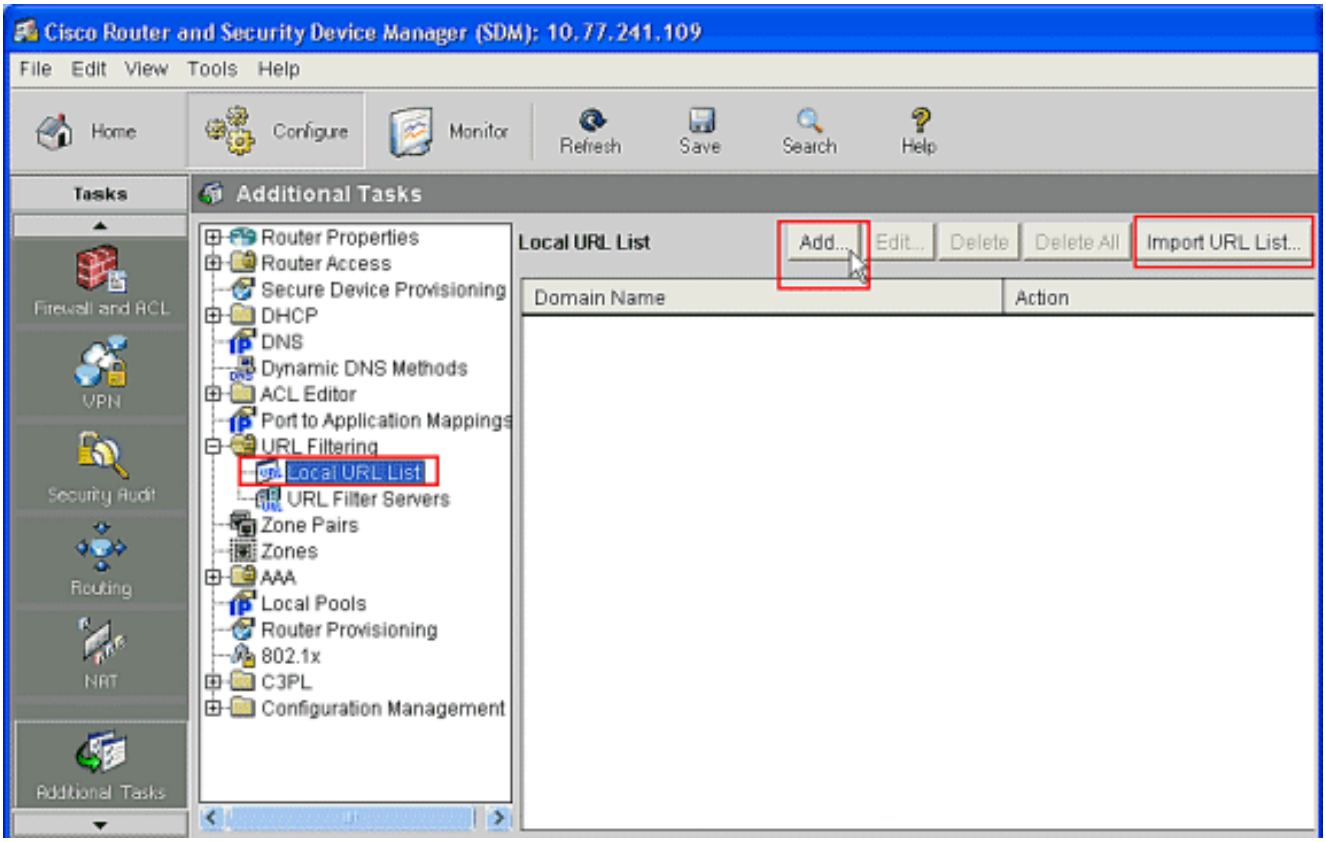


5. Nella nuova finestra che viene visualizzata, abilitare i parametri richiesti per il filtro URL, ad esempio **Allow-Mode, URL Filter Alert, Audit-Trial** e **URL Filtering Server Log**. Selezionate le caselle di controllo accanto a ciascun parametro come mostrato nella figura. Fornire ora le informazioni **Dimensione cache** e **Buffer HTTP**. Specificare inoltre l'interfaccia di origine e il metodo URL Truncate nella sezione **Advanced** come illustrato per consentire al filtro URL di troncare URL lunghi sul server. In questo caso, il parametro Truncation è impostato su **Hostname**. Fare clic su

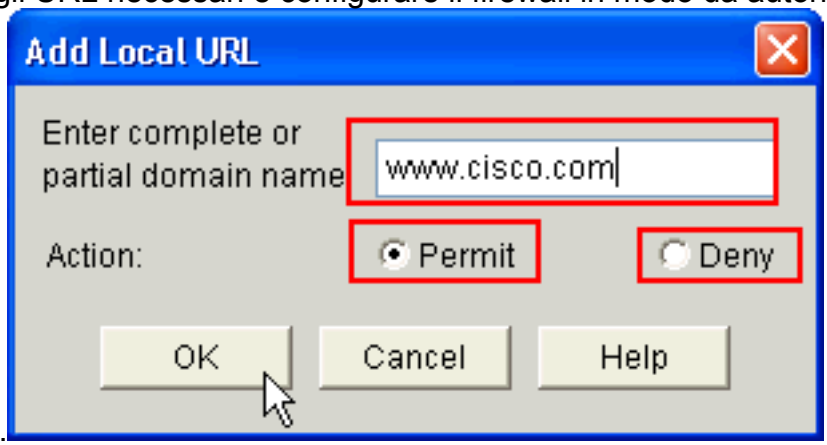


OK.

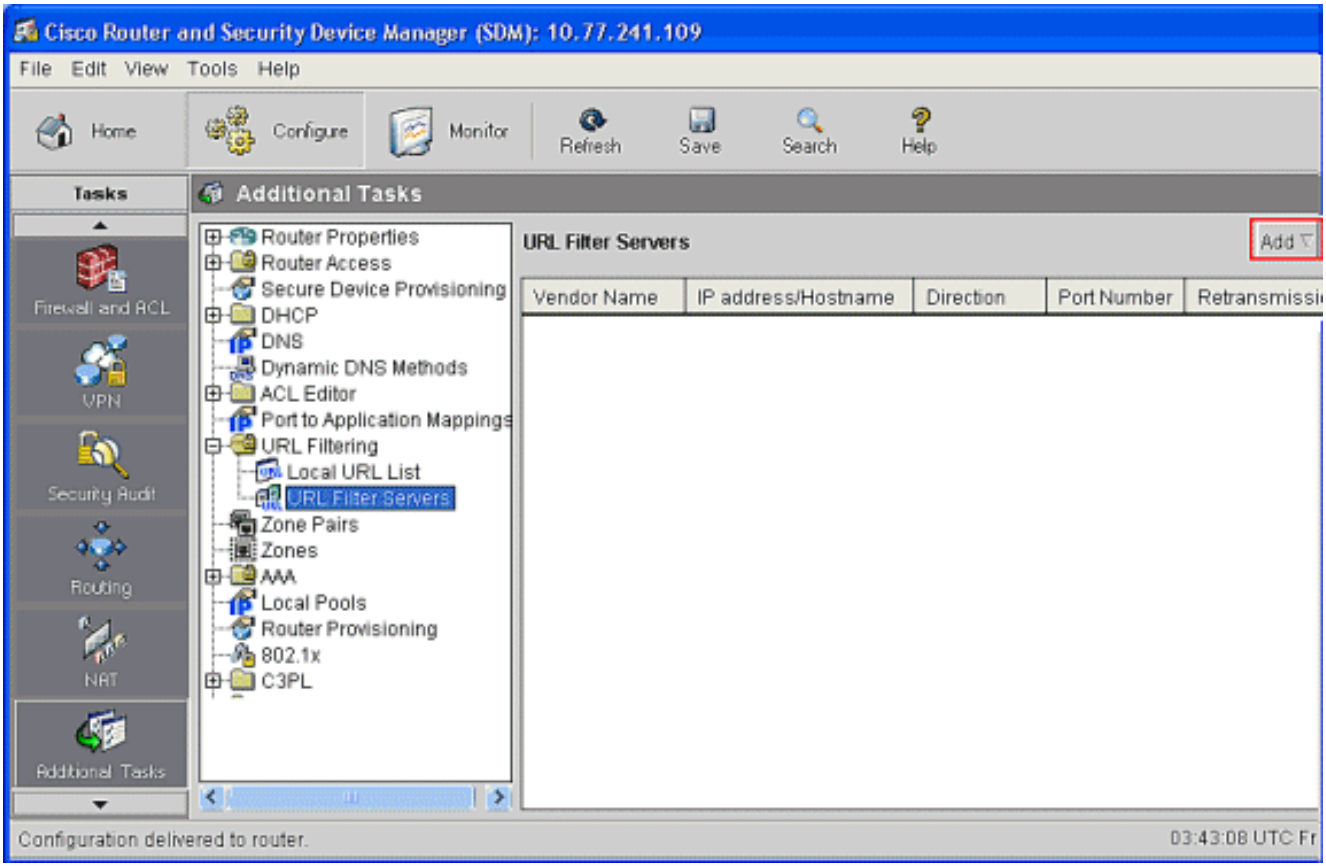
6. A questo punto, selezionare l'opzione **Local URL List** (Elenco URL locali) nella scheda **URL Filtering** (Filtro URL). Fare clic su **Add** (Aggiungi) per aggiungere il nome di dominio e configurare il firewall in modo che consenta o neghi l'aggiunta del nome di dominio. È inoltre possibile scegliere l'opzione **Importa elenco URL** se l'elenco degli URL necessari è presente come file. È possibile scegliere tra le opzioni **Add URL** (Aggiungi URL) o **Import URL List** (Importa elenco URL) in base ai requisiti e alla disponibilità dell'elenco URL.



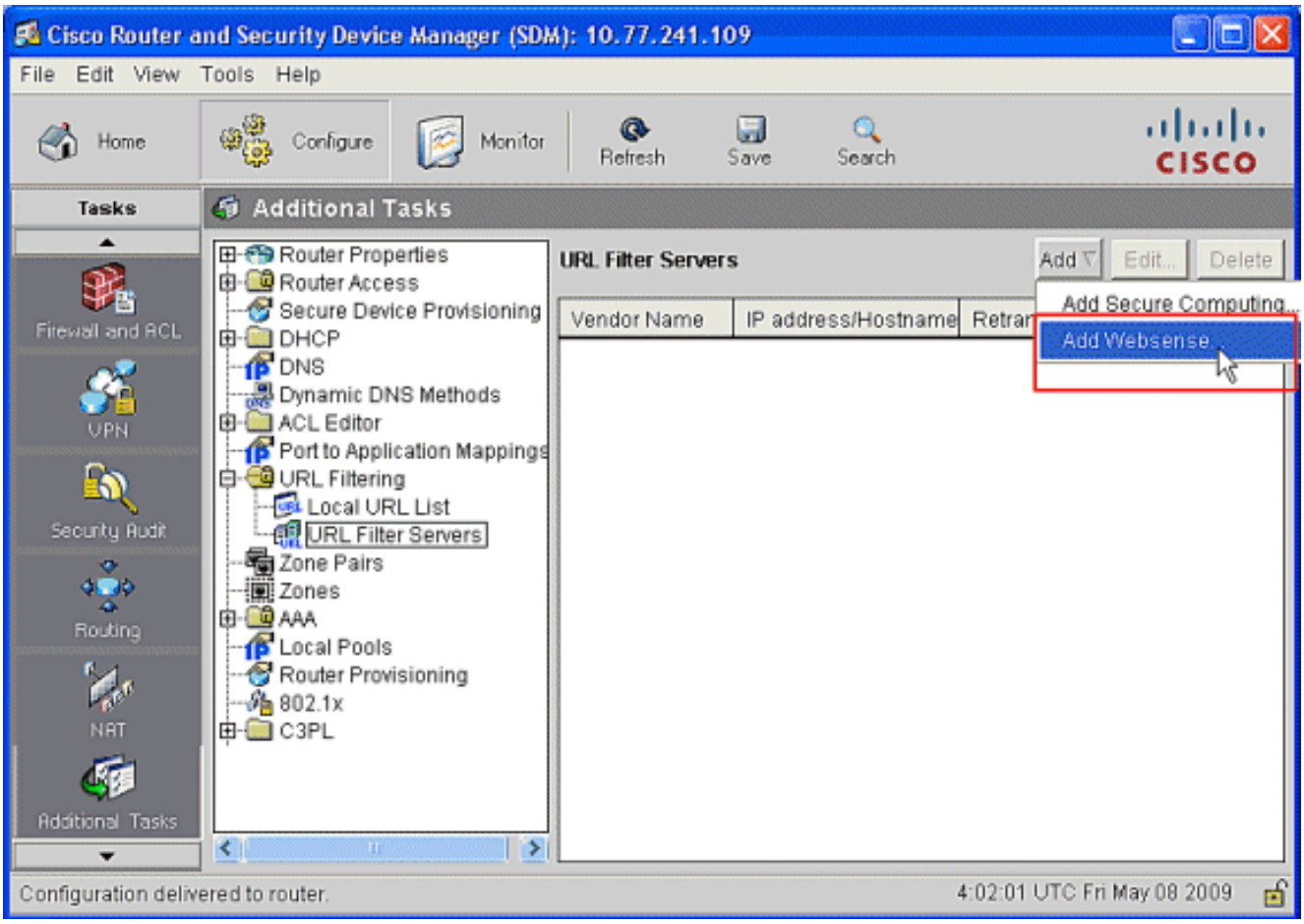
7. In questo esempio, fare clic su **Add** per aggiungere l'URL e configurare IOS Firewall in modo da autorizzare o negare l'URL come richiesto. A questo punto, viene visualizzata una nuova finestra chiamata **ADD Local URL** (AGGIUNGI URL locale) in cui l'utente deve fornire il nome di dominio e decidere se autorizzare o negare l'URL. Fare clic sul pulsante di opzione accanto all'opzione Autorizza o Nega come illustrato. Il nome del dominio è **www.cisco.com**, e l'utente **autorizza** l'**URL www.cisco.com**. Analogamente, è possibile fare clic su **Add** (Aggiungi), aggiungere tutti gli URL necessari e configurare il firewall in modo da autorizzarli o negarli in base al requisito.



8. Scegliere l'opzione **Server filtro URL** nella scheda **Filtro URL**, come mostrato. Per aggiungere il nome del server del filtro URL che esegue la funzione, fare clic su **Add** (Aggiungi).

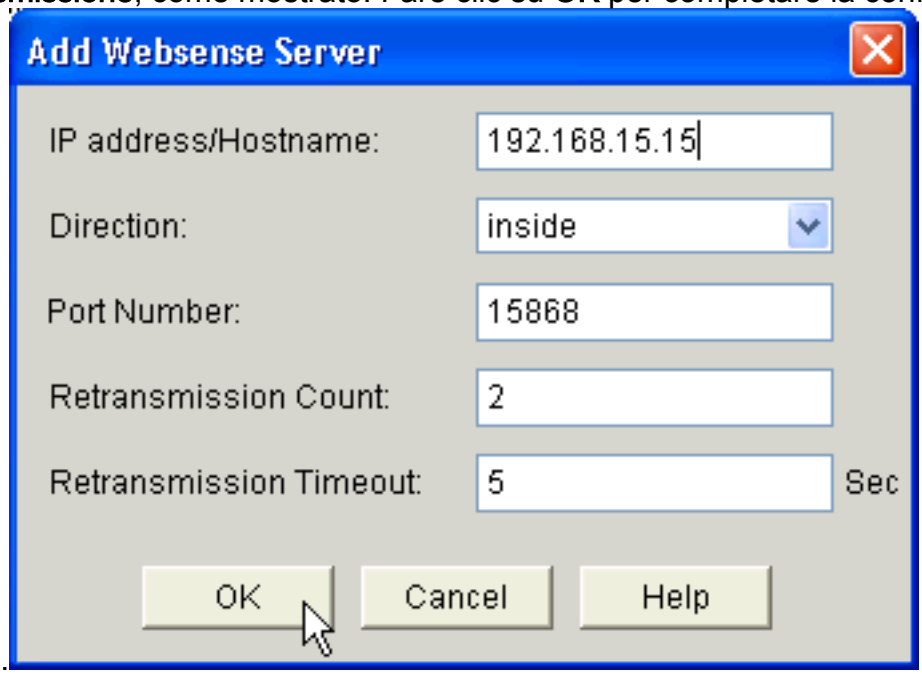


9. Dopo aver fatto clic su **Aggiungi**, scegliere il server di filtro come **Websense** come illustrato di seguito, poiché in questo esempio viene utilizzato il server di filtro Websense.



10. In questa finestra Aggiungi server Websense, fornire l'**indirizzo IP** del server Websense insieme a **Direzione** in cui funziona il filtro e **Numero porta,**(Il numero di porta predefinito per il server Websense è **15868**). Fornire anche i valori **Conteggio ritrasmissioni** e **Timeout**

ritrasmissione, come mostrato. Fare clic su **OK** per completare la configurazione del **filtro URL**.



Verifica

Per visualizzare le informazioni sul filtro URL, usare i comandi di questa sezione. È possibile utilizzare questi comandi per verificare la configurazione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show ip urlfilter statistics**: visualizza le informazioni e le statistiche sul server filtroAd esempio:

```
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**: visualizza il numero massimo di voci che possono essere memorizzate nella tabella della cache, il numero di voci e gli indirizzi IP di destinazione che vengono memorizzati nella tabella della cache quando si utilizza il comando show ip urlfilter cache in modalità di esecuzione privilegiata.
- **show ip urlfilter config**: visualizza la configurazione del filtro.Ad esempio:

```
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
```

Risoluzione dei problemi

Messaggi di errore

`%URLF-3-SERVER_DOWN: La connessione al server filtro URL 10.92.0.9 non è attiva` — Questo messaggio di livello tre di tipo LOG_ERR viene visualizzato quando un UFS configurato non è attivo. In questo caso, il firewall contrassegnerà il server configurato come server secondario e tenterà di attivare uno degli altri server secondari e contrassegnarlo come server primario. Se non sono configurati altri server, il firewall entra in modalità di autorizzazione e visualizza il messaggio `URLF-3-ALLOW_MODE`.

`%URLF-3-ALLOW_MODE: La connessione a tutti i server filtro URL è disattivata e ALLOW MODE è disattivato` — Questo messaggio di tipo LOG_ERR viene visualizzato quando tutti gli UFS sono disattivati e il sistema entra in modalità di autorizzazione.

Nota: ogni volta che il sistema entra in modalità di abilitazione (tutti i server di filtro sono inattivi), viene attivato un timer keep-alive periodico che tenta di aprire una connessione TCP e attivare un server.

`%URLF-5-SERVER_UP: Viene effettuata la connessione a un server filtro URL 10.92.0.9; il sistema sta tornando da ALLOW MODE` — Questo messaggio di tipo LOG_NOTICE viene visualizzato quando gli UFS vengono rilevati come attivi e il sistema torna dalla modalità di autorizzazione.

`%URLF-4-URL_TOO_LONG:URL troppo lungo (più di 3072 byte). Probabilmente è un pacchetto falso?` — Questo messaggio di tipo LOG_WARNING viene visualizzato quando l'URL in una richiesta di ricerca è troppo lungo; qualsiasi URL più lungo di 3K viene eliminato.

`%URLF-4-MAX_REQ: Il numero di richieste in sospeso supera il limite massimo <1000>` — Questo messaggio di tipo LOG_WARNING viene visualizzato quando il numero di richieste in sospeso nel sistema supera il limite massimo e tutte le ulteriori richieste vengono eliminate.

Informazioni correlate

- Cisco IOS Firewall
- Filtro URL di Firewall Websense
- Guida alla configurazione della sicurezza di Cisco IOS, supporto versione 12.4
- Documentazione e supporto tecnico – Cisco Systems