Esempio di configurazione del filtro URL PIX/ASA

Sommario

Introduzione

In questo documento viene spiegato come configurare il filtro URL su un accessorio di sicurezza.

Per filtrare il traffico, è possibile:

- Consente di ridurre i rischi per la sicurezza e di prevenire un utilizzo non appropriato.
- Offre un maggiore controllo sul traffico che attraversa l'appliance di sicurezza.

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. Tuttavia, in base alla velocità della rete e alla capacità del server di filtro URL, il tempo necessario per la connessione iniziale può essere sensibilmente più lento quando il traffico viene filtrato con un server di filtro esterno.

Nota: l'implementazione di un filtro dal livello di protezione inferiore a quello superiore non è supportata. Il filtro URL funziona solo per il traffico in uscita, ad esempio il traffico che ha origine su un'interfaccia ad alta sicurezza destinata a un server su un'interfaccia a bassa sicurezza.

Prerequisiti

Componenti usati

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

- PIX serie 500 Security Appliance con versione 6.2 e successive
- ASA serie 5500 Security Appliance con versione 7.x e successive
- Adaptive Security Device Manager (ASDM) 6.0

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

Èpossibile filtrare le richieste di connessione provenienti da una rete più protetta in una rete meno protetta. Sebbene sia possibile utilizzare gli elenchi di controllo di accesso (ACL, Access Control List) per impedire l'accesso in uscita a specifici server di contenuti, è difficile gestire l'utilizzo in questo modo a causa delle dimensioni e della natura dinamica di Internet. È possibile semplificare la configurazione e migliorare le prestazioni delle appliance di sicurezza utilizzando un server separato che esegue uno dei seguenti prodotti di filtro Internet:

- Websense Enterprise: filtra HTTP, HTTPS e FTP. È supportato da PIX firewall versione 5.3 e successive.
- Secure Computing SmartFilter, precedentemente noto come N2H2, filtra HTTP, HTTPS, FTP e filtro URL lunghi. È supportato da PIX firewall versione 6.2 e successive.

Rispetto all'utilizzo degli elenchi di controllo di accesso, questo consente di ridurre le attività amministrative e di migliorare l'efficacia dei filtri. Inoltre, poiché il filtro URL viene gestito su una piattaforma separata, le prestazioni del firewall PIX ne risentono notevolmente. Tuttavia, quando il server di filtraggio è remoto rispetto all'accessorio di sicurezza, gli utenti possono notare tempi di accesso più lunghi ai siti Web o ai server FTP.

Il firewall PIX controlla le richieste URL in uscita con i criteri definiti sul server filtro URL. Il firewall PIX consente o nega la connessione, in base alla risposta del server di filtro.

Quando il filtro è attivato e una richiesta di contenuto viene indirizzata attraverso l'appliance di sicurezza, la richiesta viene inviata contemporaneamente al server del contenuto e al server del filtro. Se il server di filtro consente la connessione, l'appliance di sicurezza inoltra la risposta dal server del contenuto al client che ha originato la richiesta. Se il server di filtro nega la connessione, l'accessorio di protezione ignora la risposta e invia un messaggio o un codice restituito indicante che la connessione non è riuscita.

Se l'autenticazione dell'utente è attivata sull'accessorio di protezione, quest'ultimo invierà anche il nome utente al server di filtro. Il server di filtro può utilizzare impostazioni di filtro specifiche dell'utente o fornire report avanzati relativi all'utilizzo.

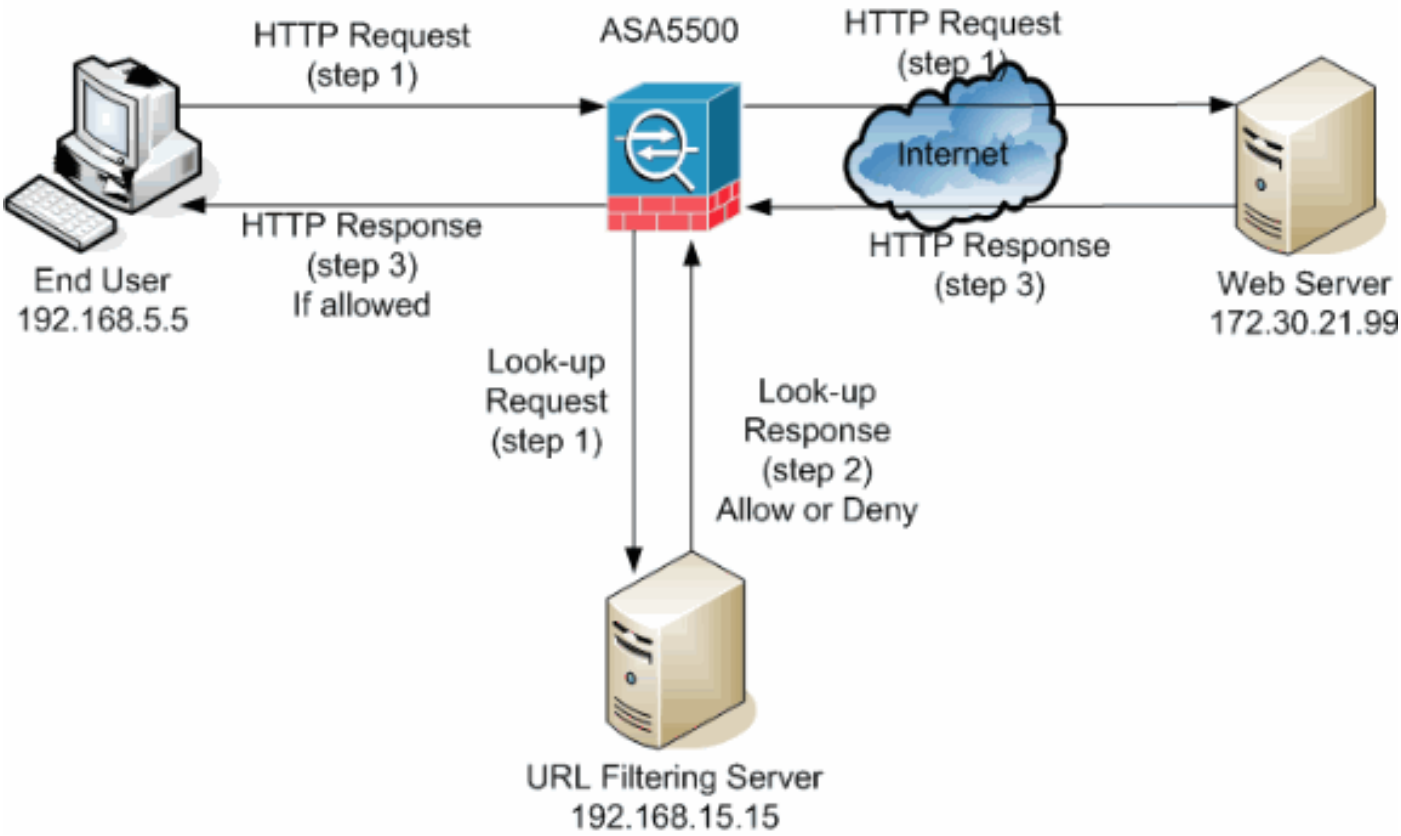
Configurazione di ASA/PIX con la CLI

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 filtro URL si trova in una rete DMZ. 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 durante la 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, l'appliance di sicurezza la inoltra al server Web, estrae contemporaneamente l'URL e invia una richiesta di ricerca al server 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. L'appliance di sicurezza riceve la risposta di 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

Identificare l'indirizzo del server di filtro con il comando **url-server**. È necessario utilizzare la forma appropriata di questo comando in base al tipo di server di filtro utilizzato.

Nota: per il software versione 7.x e successive, è possibile identificare fino a quattro server di filtraggio per ogni contesto. L'accessorio di protezione utilizza i server nell'ordine corretto fino a quando un server non risponde. 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.

- Software versione 6.2:

  ```
  url-server [(if_name)] vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP}
  version]
  ```

  Il comando **url-server** designa il server che esegue l'applicazione di filtro URL N2H2 o Websense. Il limite è 16 server URL. Tuttavia, è possibile utilizzare una sola applicazione alla volta, N2H2 o Websense. Inoltre, se si modifica la configurazione sul firewall PIX, la configurazione sul server applicazioni non viene aggiornata. Questo deve essere fatto separatamente, in base alle istruzioni del singolo fornitore.
- Software versione 7.x e successive:

  ```
  pix(config)# url-server (if_name) host local_ip [timeout seconds] [protocol TCP | UDP
  version 1|4
  [connections num_conns] ]
  ```

Sostituire `if_name` con il nome dell'interfaccia dell'appliance di sicurezza collegata al server di filtraggio. Il valore predefinito è inside. Sostituire `local_ip` con l'indirizzo IP del server di filtro. Sostituire `secondi` con il numero di secondi durante i quali l'appliance di sicurezza deve continuare a tentare di connettersi al server di filtro.

Per specificare se si desidera utilizzare il protocollo TCP o UDP, usare l'opzione `protocol`. Con un server Websense è inoltre possibile specificare la `versione` di TCP che si desidera utilizzare. TCP versione 1 è l'impostazione predefinita. TCP versione 4 consente al firewall PIX di inviare nomi utente autenticati e informazioni di registrazione URL al server Websense se il firewall PIX ha già autenticato l'utente.

Ad esempio, per identificare un singolo server di filtro Websense, eseguire questo comando:

```
hostname(config)#url-server (DMZ) vendor websense host 192.168.15.15 protocol TCP version 4
```

SmartFilter Secure Computing

- PIX versione 6.2:
  ```
  pix(config)#url-server [(if_name)] vendor n2h2 host local_ip[:port number] [timeout
  ```

- Software versioni 7.0 e 7.1:
  ```
  hostname(config)#url-server (if_name) vendor n2h2 host local_ip[:port number] [timeout
  seconds]
  [protocol TCP connections number | UDP [connections num_conns]]
  ```

- Software versione 7.2 e successive:
  ```
  hostname(config)#url-server (if_name) vendor {secure-computing | n2h2} host
  ```

  Per il `fornitore {secure-computing | n2h2}`, è possibile utilizzare l'`elaborazione sicura` come stringa del fornitore. Tuttavia, `n2h2` è accettabile per la compatibilità con le versioni precedenti. Quando vengono generate le voci di configurazione, l'`elaborazione sicura` viene salvata come stringa del fornitore.

Sostituire `if_name` con il nome dell'interfaccia dell'appliance di sicurezza collegata al server di filtraggio. Il valore predefinito è inside. Sostituire `local_ip` con l'indirizzo IP del server di filtraggio e `la porta <number>` con il numero di porta desiderato.

Nota: la porta predefinita utilizzata dal server Secure Computing SmartFilter per comunicare con l'appliance di sicurezza tramite TCP o UDP è la porta 4005.

Sostituire `secondi` con il numero di secondi durante i quali l'appliance di sicurezza deve continuare a tentare di connettersi al server di filtro. Per specificare se si desidera utilizzare il protocollo TCP o UDP, usare l'opzione `protocol`.

Il `numero di connessioni <number>` indica il numero di tentativi di connessione tra l'host e il server.

Ad esempio, per identificare un singolo server di filtro N2H2, usare questo comando:

```
hostname(config)#url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol
 tcp connections 10
```

Oppure, se si desidera utilizzare i valori predefiniti, utilizzare questo comando:

```
hostname(config)#url-server (DMZ) vendor n2h2 host 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.

Abilitazione del filtro URL

Quando il server di filtro approva una richiesta di connessione HTTP, l'appliance di sicurezza consente alla risposta dal server Web di raggiungere il client da cui proviene la richiesta. Se il server di filtro rifiuta la richiesta, l'accessorio di protezione reindirizza l'utente a una pagina bloccata che indica che l'accesso è negato.

Usare il comando **filter url** per configurare i criteri usati per filtrare gli URL:

- PIX versione 6.2:

```
filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-
block]
[longurl-truncate | longurl-deny] [cgi-truncate]
```

- Software versione 7.x e successive:

```
filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-
block]
[longurl-truncate | longurl-deny] [cgi-truncate]
```

Sostituire `port` con il numero della porta su cui filtrare il traffico HTTP se si utilizza una porta diversa da quella predefinita per HTTP (80). Per identificare un intervallo di numeri di porta, immettere l'inizio e la fine dell'intervallo separati da un trattino.

Se il filtro è attivato, l'appliance di sicurezza interrompe il traffico HTTP in uscita finché un server di filtro non consente la connessione. Se il server di filtro primario non risponde, l'accessorio di protezione indirizzerà la richiesta di filtro al server di filtro secondario. L'opzione `allow` (Consenti) consente all'appliance di sicurezza di inoltrare il traffico HTTP senza filtraggio quando il server di filtro primario non è disponibile.

Usare il comando **proxy-block** per eliminare tutte le richieste dai server proxy.

Nota: per troncare URL lunghi, vengono utilizzati i parametri restanti.

Tronca URL HTTP lunghi

Se l'opzione `longurl-truncate` (troncamento URL lungo) è selezionata, l'appliance di sicurezza invierà solo la parte dell'URL relativa al nome host o all'indirizzo IP per la valutazione al server di filtro quando l'URL supera la lunghezza massima consentita.

Per rifiutare il traffico URL in uscita se la lunghezza dell'URL supera il valore massimo consentito, usare l'opzione `longurl-deny`.

Utilizzare l'opzione `cgi-truncate` per troncare gli URL CGI in modo da includere solo la posizione

dello script CGI e il nome dello script senza parametri.

Questo è un esempio di configurazione generale del filtro:

```
hostname(config)#filter url http 192.168.5.0 255.255.255.0 172.30.21.99 255.255.255.255 allow
proxy-block longurl-truncate cgi-truncate
```

Esenzione del traffico dai filtri

Per creare un'eccezione al criterio di filtro generale, eseguire questo comando:

```
filter url except local_ip local_mask foreign_ip foreign_mask]
```

Sostituire `local_ip` e `local_mask` con l'indirizzo IP e la subnet mask di un utente o di una sottorete che si desidera esentare dalle restrizioni dei filtri.

Sostituire `foreign_ip` e `foreign_mask` con l'indirizzo IP e la subnet mask di un server o di una subnet che si desidera esentare dalle restrizioni di filtro.

Ad esempio, questo comando determina l'inoltro di tutte le richieste HTTP dagli host interni all'host 172.30.21.99 al server di filtro, ad eccezione delle richieste provenienti dall'host 192.168.5.5:

Questo è un esempio di configurazione per un'eccezione:

```
hostname(config)#filter url except 192.168.5.5 255.255.255.255 172.30.21.99 255.255.255.255
```

Filtro URL avanzato

In questa sezione vengono fornite informazioni sui parametri di filtro avanzati, che includono gli argomenti seguenti:

- buffering
- memorizzazione nella cache
- supporto di URL lunghi

Memorizza nel buffer le risposte del server Web

Quando un utente invia una richiesta di connessione a un server del contenuto, l'accessorio di protezione la invia contemporaneamente al server del contenuto e al server di filtro. Se il server di filtro non risponde prima del server di contenuti multimediali, la risposta del server verrà ignorata. In questo modo la risposta del server Web viene ritardata dal punto di vista del client Web, in quanto il client deve riemettere la richiesta.

Se si abilita il buffer di risposta HTTP, le risposte dei server del contenuto Web vengono memorizzate nel buffer e le risposte vengono inoltrate al client che effettua la richiesta se il server filtro consente la connessione. In questo modo si evita il ritardo che potrebbe verificarsi in altro modo.

Per inserire nel buffer le risposte alle richieste HTTP, attenersi alla seguente procedura:

1. Per abilitare il buffering delle risposte per le richieste HTTP in attesa di risposta dal server di filtro, eseguire questo comando:
   `hostname(config)#url-block block block-buffer-limit`

   Sostituire `block-buffer-limit` con il numero massimo di blocchi da inserire nel buffer.
2. Per configurare la memoria massima disponibile per inserire nel buffer gli URL in sospeso e gli URL lunghi con Websense, eseguire questo comando:
   `hostname(config)#url-block url-mempool memory-pool-size`

   Sostituire `memory-pool-size` con un valore da 2 a 10240 per un'allocazione di memoria massima da 2 KB a 10 MB.

Indirizzi server cache

Dopo che un utente ha eseguito l'accesso a un sito, il server di filtro può consentire all'appliance di sicurezza di memorizzare nella cache l'indirizzo del server per un determinato periodo di tempo, a condizione che ogni sito ospitato all'indirizzo sia incluso in una categoria sempre consentita. Quando l'utente accede nuovamente al server o un altro utente accede al server, l'appliance di sicurezza non deve consultare nuovamente il server di filtraggio.

Utilizzare il comando **url-cache** se necessario per migliorare la velocità effettiva:

```
hostname(config)#url-cache dst | src_dst size
```

Sostituire `size` con un valore per la dimensione della cache compreso tra 1 e 128 (KB).

Usare la parola chiave `dst` per memorizzare nella cache le voci in base all'indirizzo di destinazione dell'URL. Selezionare questa modalità se tutti gli utenti condividono lo stesso criterio di filtro URL sul server Websense.

Utilizzare la parola chiave `src_dst` per memorizzare nella cache le voci in base sia all'indirizzo di origine che avvia la richiesta URL sia all'indirizzo di destinazione URL. Selezionare questa modalità se gli utenti non condividono lo stesso criterio di filtro URL sul server Websense.

Abilitazione del filtro degli URL lunghi

Per impostazione predefinita, un URL HTTP viene considerato come URL lungo se supera i 1159 caratteri. È possibile aumentare la lunghezza massima consentita per un singolo URL con questo comando:

```
hostname(config)#url-block url-size long-url-size
```

Sostituire `long-url-size` con le dimensioni massime in KB per ogni URL lungo da inserire nel buffer.

Ad esempio, questi comandi configurano l'appliance di sicurezza per il filtro URL avanzato:

```
hostname(config)#url-block block 10
hostname(config)#url-block url-mempool 2
hostname(config)#url-cache dst 100
hostname(config)#url-block url-size 2
```

Configurazione

Questa configurazione include i comandi descritti nel presente documento:

Configurazione ASA 8.0

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name Security.lab.com
enable password 2kxsYuz/BehvglCF encrypted
no names
dns-guard
!
interface GigabitEthernet0/0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 172.30.21.222 255.255.255.0
!
interface GigabitEthernet0/1
 description INSIDE
 nameif inside
 security-level 100
 ip address 192.168.5.11 255.255.255.0
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
 shutdown
!
interface GigabitEthernet0/3
 description DMZ
 nameif DMZ
 security-level 50
 ip address 192.168.15.1 255.255.255.0
!
interface Management0/0
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone CST -6
clock summer-time CDT recurring
dns server-group DefaultDNS
domain-name Security.lab.com
same-security-traffic permit intra-interface
```

```
pager lines 20
logging enable
logging buffer-size 40000
logging asdm-buffer-size 200
logging monitor debugging
logging buffered informational
logging trap warnings
logging asdm informational
logging mail debugging
logging from-address aaa@cisco.com
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
no failover
failover lan unit primary
failover lan interface interface GigabitEthernet0/2
failover link interface GigabitEthernet0/2
no monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1

asdm image disk0:/asdm-602.bin
asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0

route outside 0.0.0.0 0.0.0.0 172.30.21.244 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
ldap attribute-map tomtom
dynamic-access-policy-record DfltAccessPolicy

url-server (DMZ) vendor websense host 192.168.15.15
timeout 30 protocol TCP version 1 connections 5

url-cache dst 100
aaa authentication ssh console LOCAL
aaa authentication enable console LOCAL
aaa authentication telnet console LOCAL

filter url except 192.168.5.5 255.255.255.255
172.30.21.99 255.255.255.255

filter url http 192.168.5.0 255.255.255.0 172.30.21.99
255.255.255.255 allow
       proxy-block longurl-truncate cgi-truncate
http server enable
http 172.30.0.0 255.255.0.0 outside

no snmp-server location
no snmp-server contact
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 60
console timeout 0
management-access inside
```

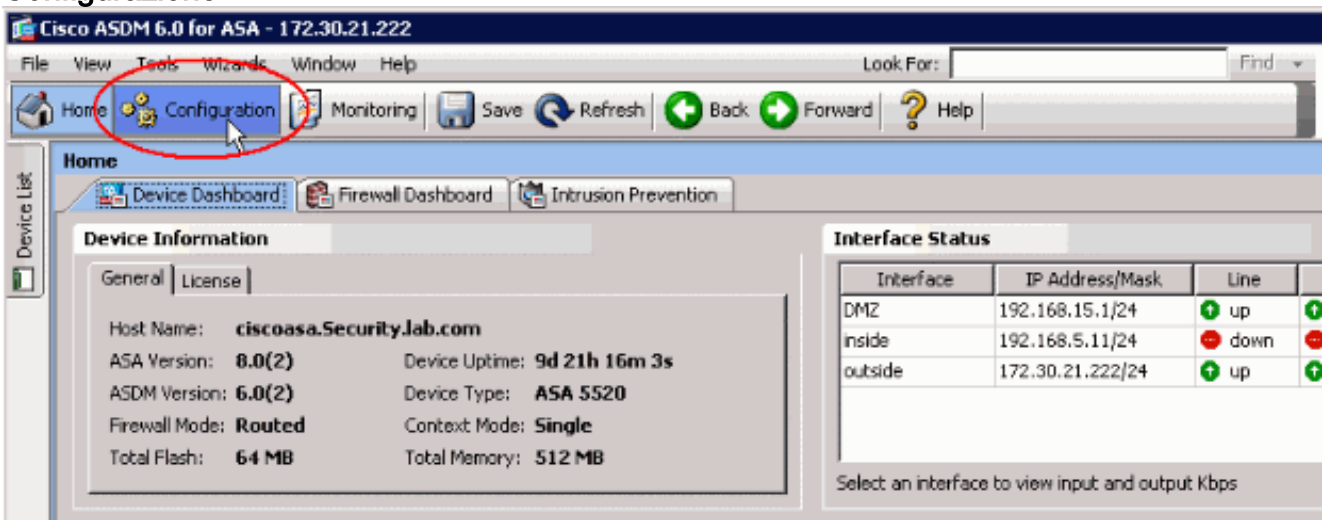
```
dhcpd address 192.168.5.12-192.168.5.20 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
!
service-policy global_policy global
url-block url-mempool 2
url-block url-size 2
url-block block 10
username fwadmin password aDRVKThrSs46pTjG encrypted
privilege 15
prompt hostname context
Cryptochecksum:db208a243faa71f9b3e92491a6ed2105
: end
```

Configurazione di ASA/PIX con ASDM

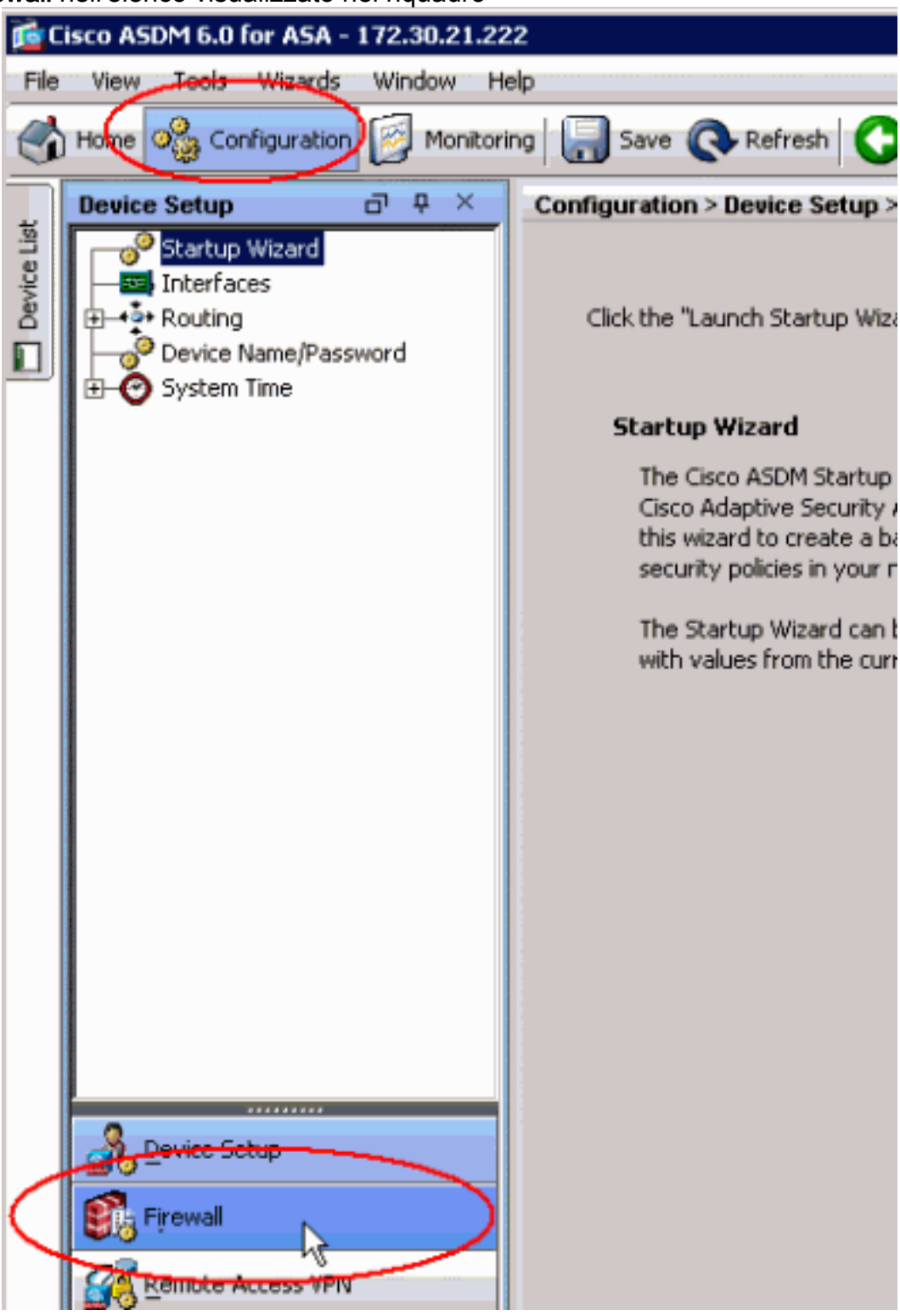
In questa sezione viene illustrato come configurare il filtro URL per l'appliance di sicurezza con Adaptive Security Device Manager (ASDM).

Dopo aver avviato ASDM, attenersi alla seguente procedura:

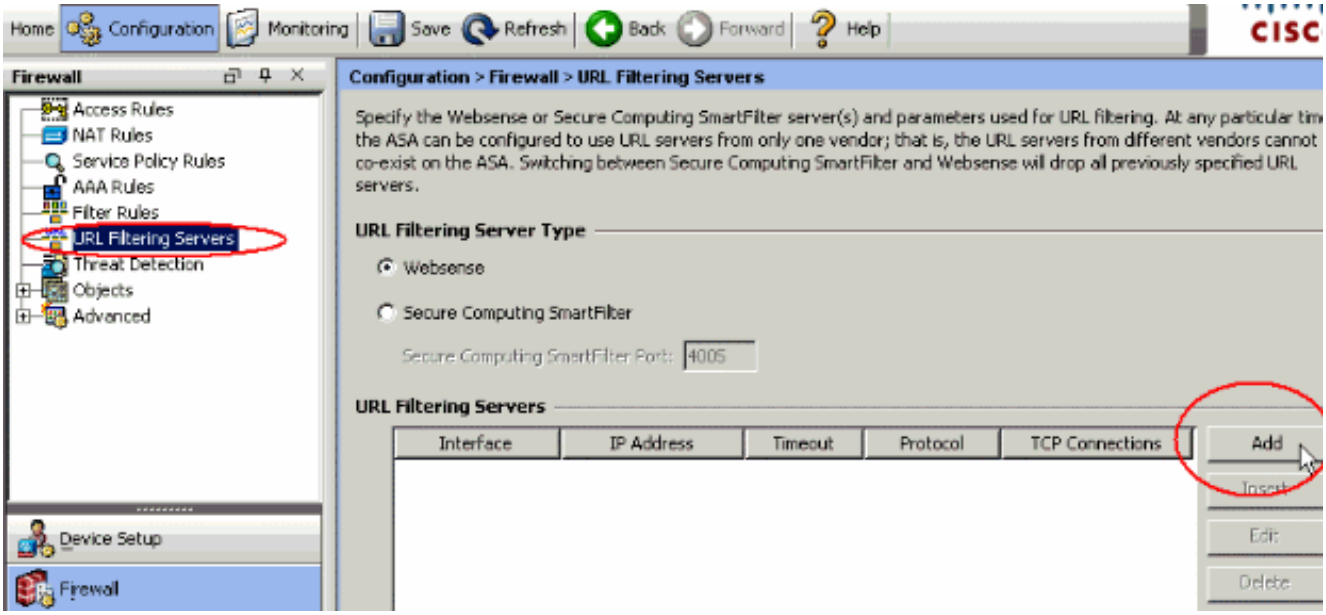
1. Scegliere il riquadro **Configurazione**.



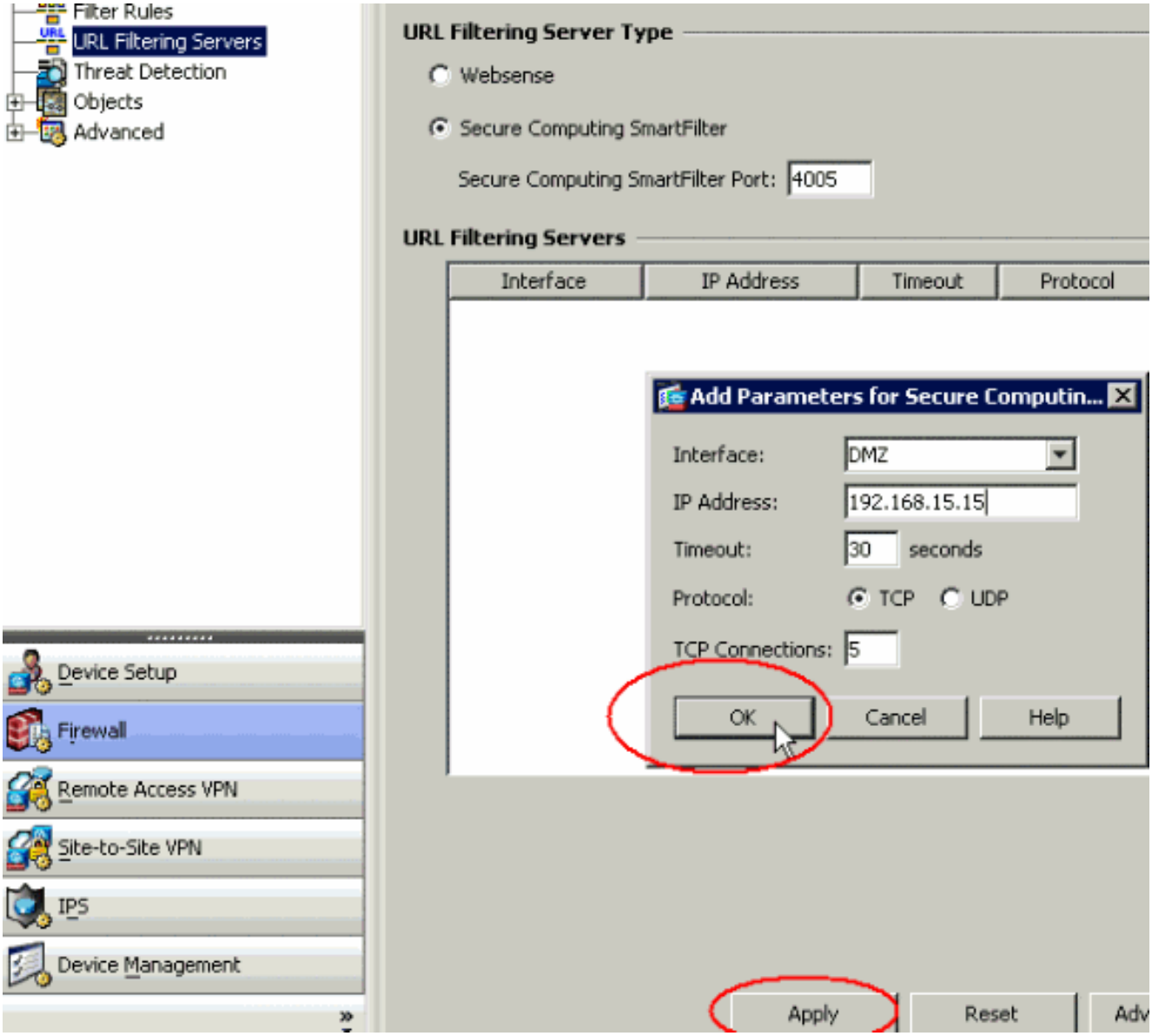
2. Fare clic su **Firewall** nell'elenco visualizzato nel riquadro **Configurazione**.



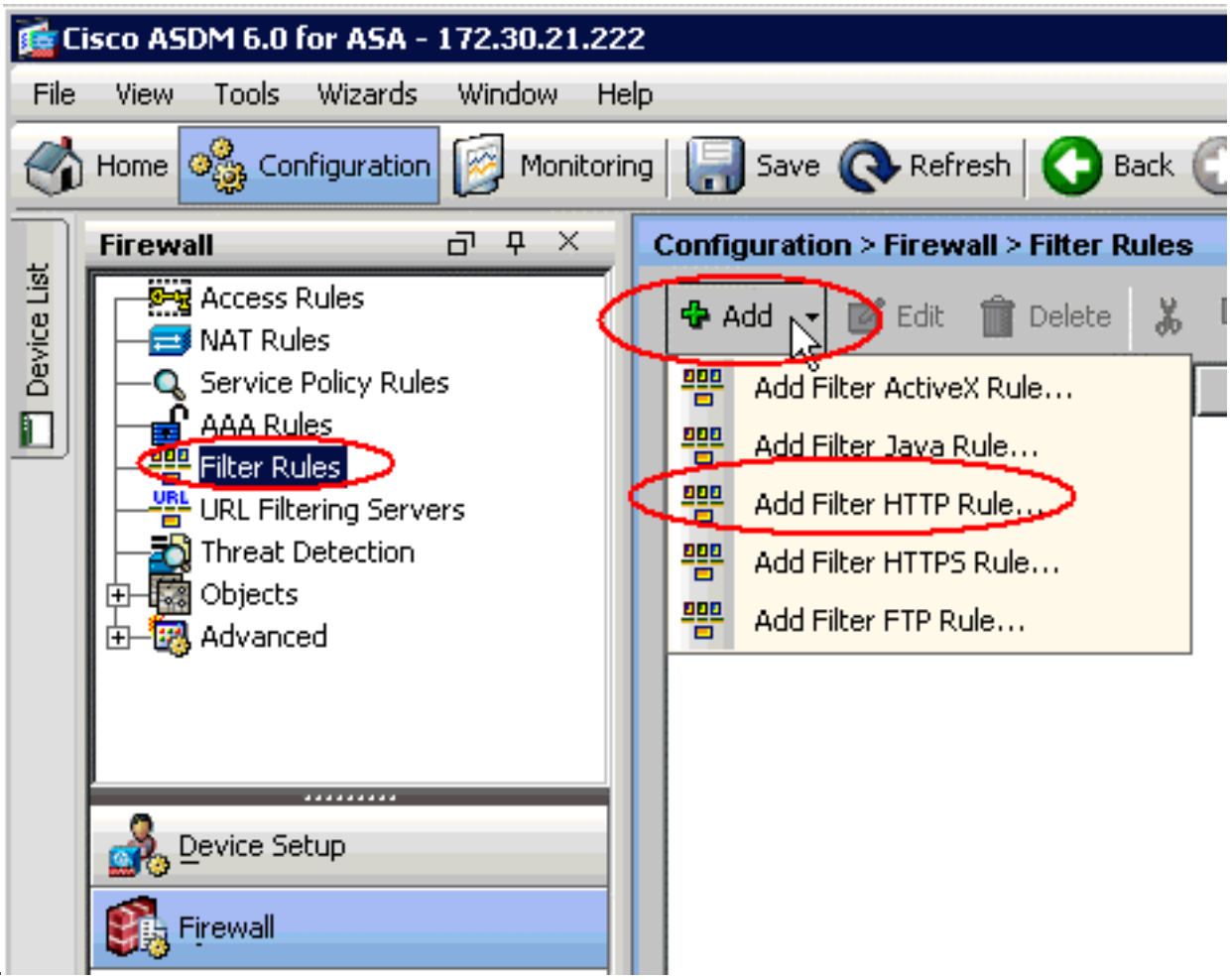
3. Dall'elenco a discesa **Firewall** (Firewall), selezionare **URL Filtering Server** (Server filtro URL). Selezionare il tipo di server filtro URL da utilizzare e fare clic su **Add** (Aggiungi) per configurarne i parametri.**Nota:** è necessario aggiungere il server di filtro prima di poter configurare il filtro per le regole HTTP, HTTPS o FTP.



4. Scegliere i parametri appropriati nella finestra popup:Interfaccia: visualizza l'interfaccia connessa al server di filtraggio.Indirizzo IP: visualizza l'indirizzo IP del server di filtraggio.Timeout: visualizza il numero di secondi trascorsi i quali si verifica il timeout della richiesta al server di filtro.Protocollo: visualizza il protocollo utilizzato per comunicare con il server di filtraggio. TCP versione 1 è l'impostazione predefinita. TCP versione 4 consente al firewall PIX di inviare nomi utente autenticati e informazioni di registrazione URL al server Websense, se il firewall PIX ha già autenticato l'utenteConnessioni TCP: visualizza il numero massimo di connessioni TCP consentite per comunicare con il server di filtro URL.Dopo aver immesso i parametri, fare clic su **OK** nella finestra popup e su **Applica** nella finestra principale.

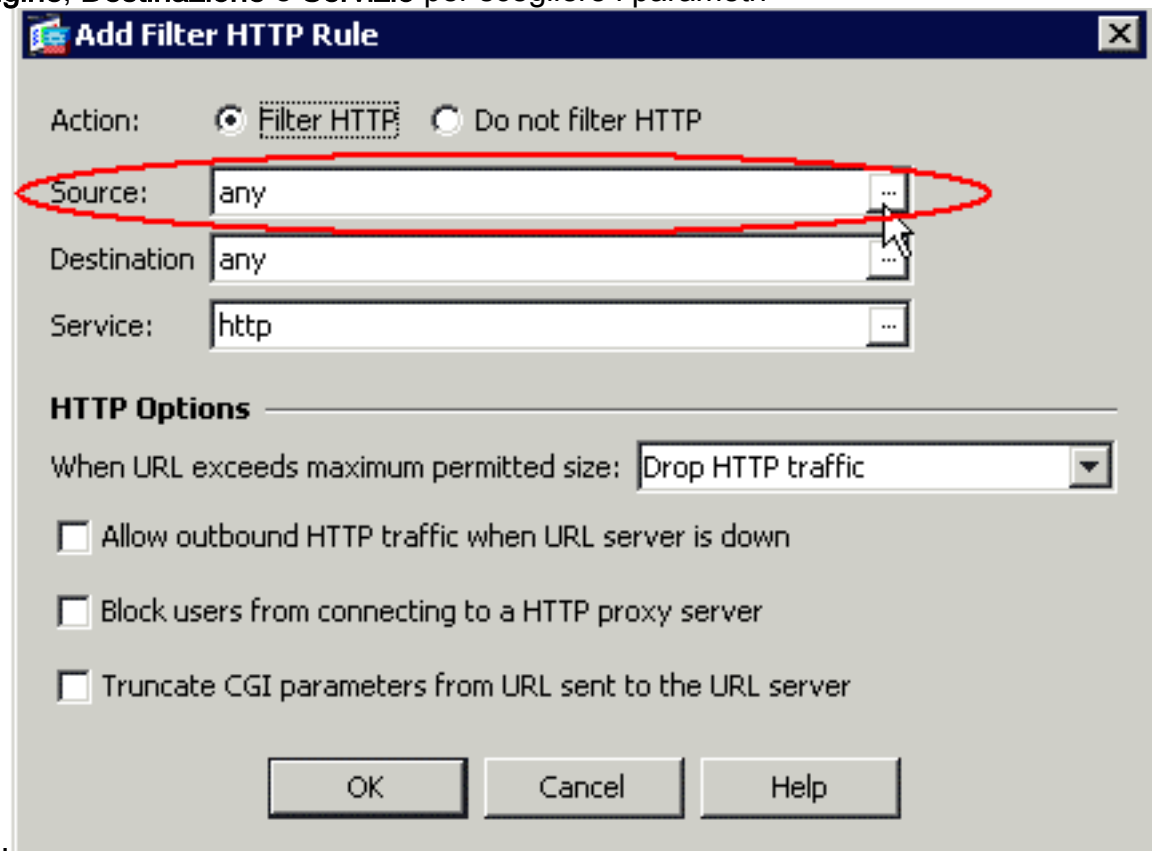


5. Dall'elenco a discesa **Firewall** (Firewall), scegliere **Regole filtro**. Fare clic sul pulsante **Aggiungi** nella finestra principale e scegliere il tipo di regola da aggiungere. In questo esempio viene scelta **Aggiungi regola HTTP**



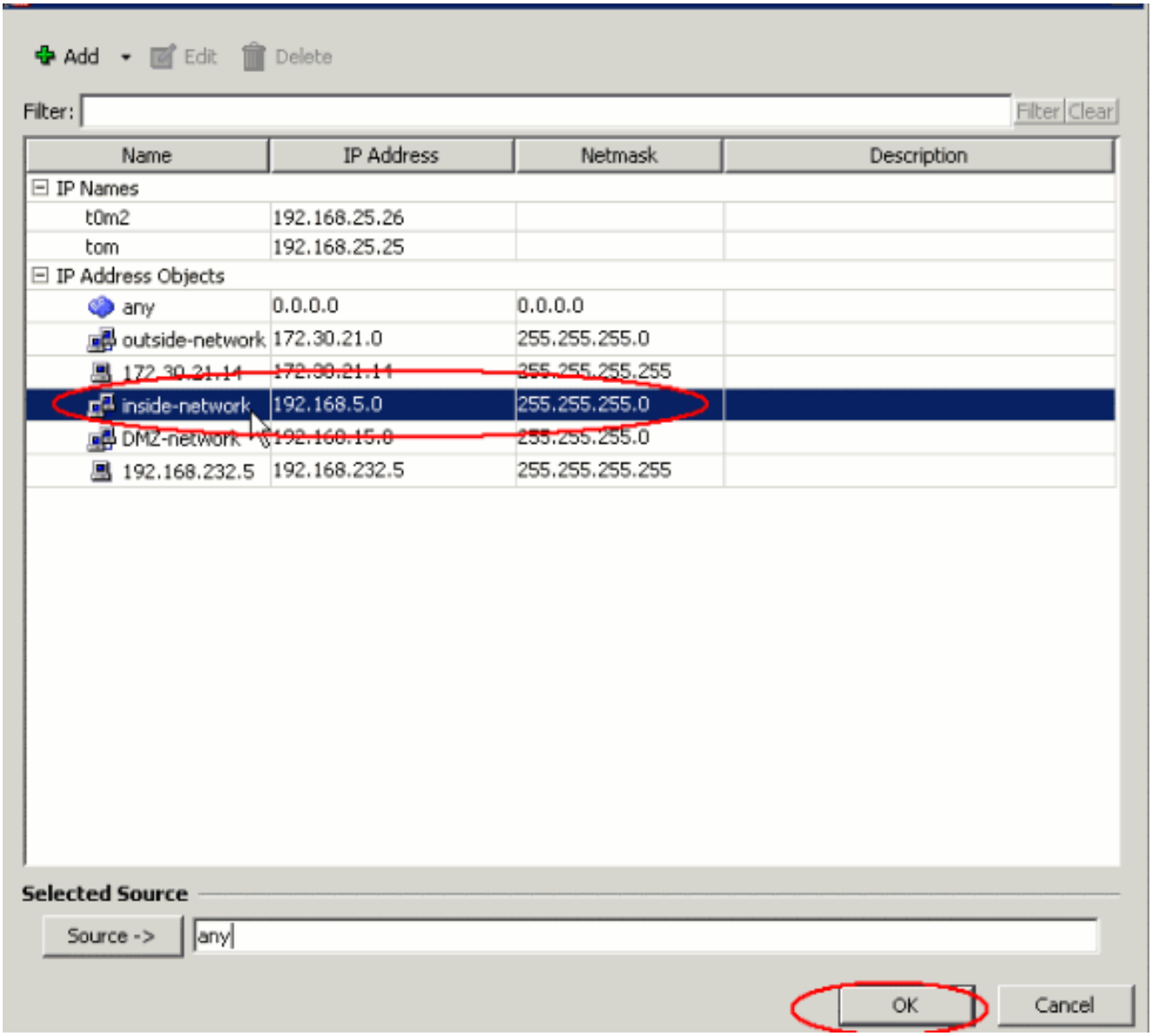
filtro.

6. Una volta visualizzata la finestra pop-up, è possibile fare clic sui pulsanti Sfoglia per le opzioni **Origine**, **Destinazione** e **Servizio** per scegliere i parametri

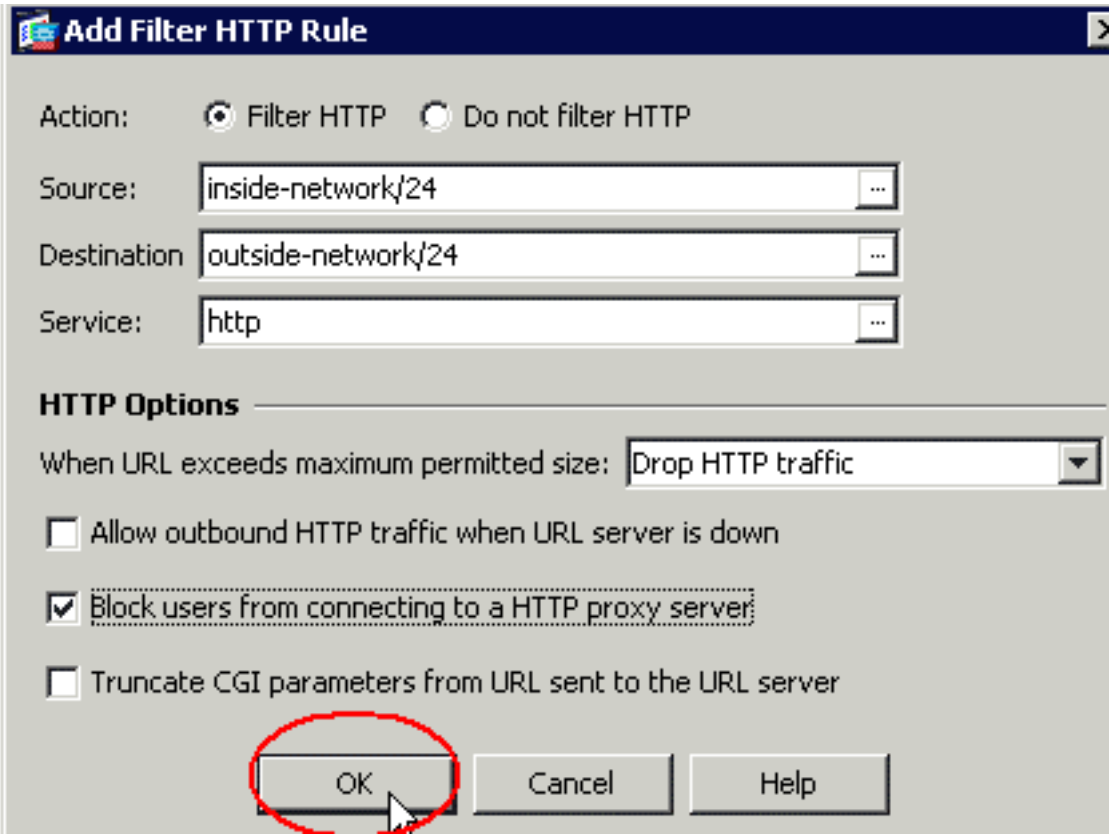


appropriati.

7. Viene visualizzata la finestra Sfoglia per l'opzione **Origine**. Effettuare la selezione e fare clic su
OK.

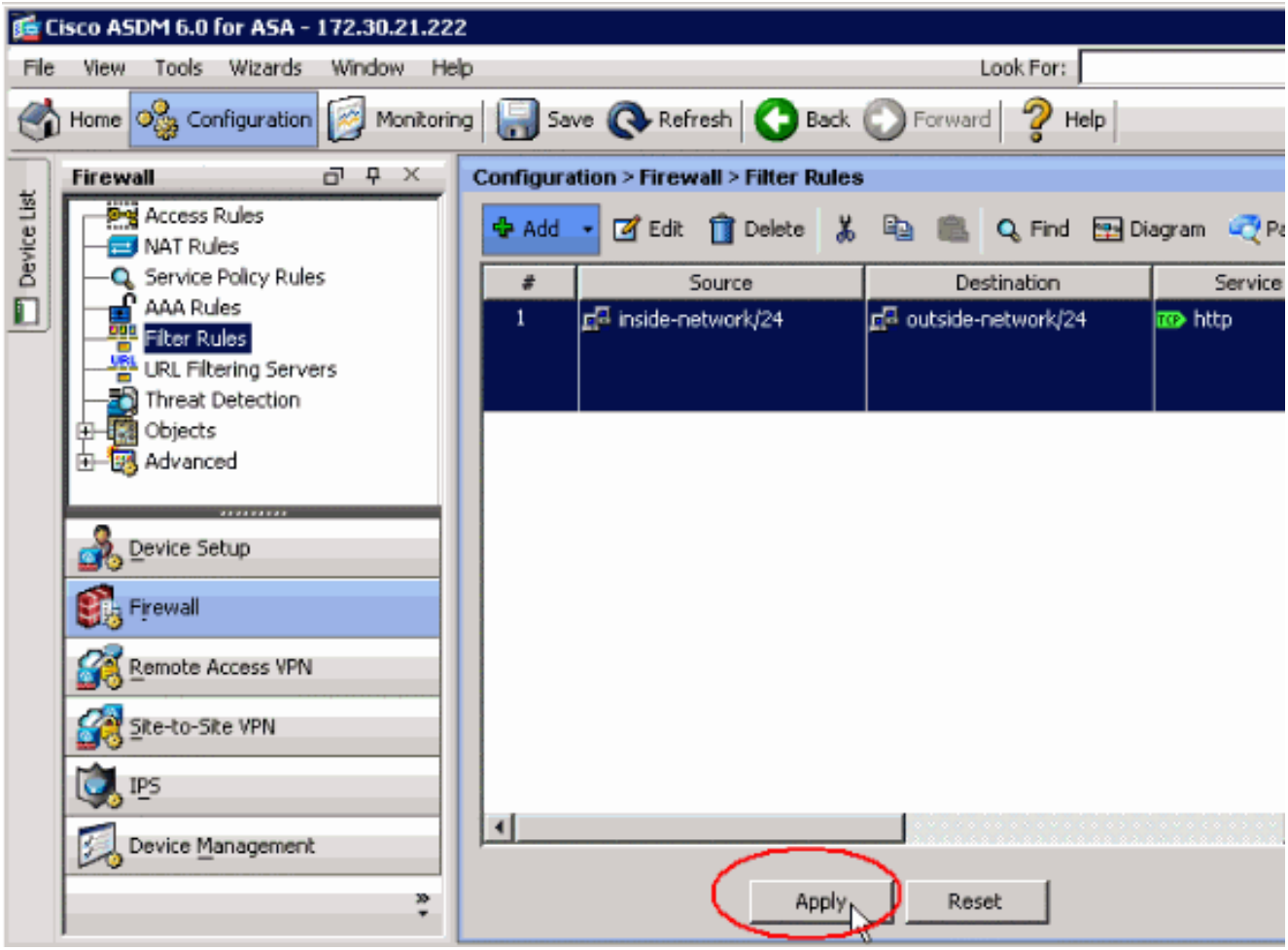


8. Dopo aver selezionato tutti i parametri, fare clic su **OK** per



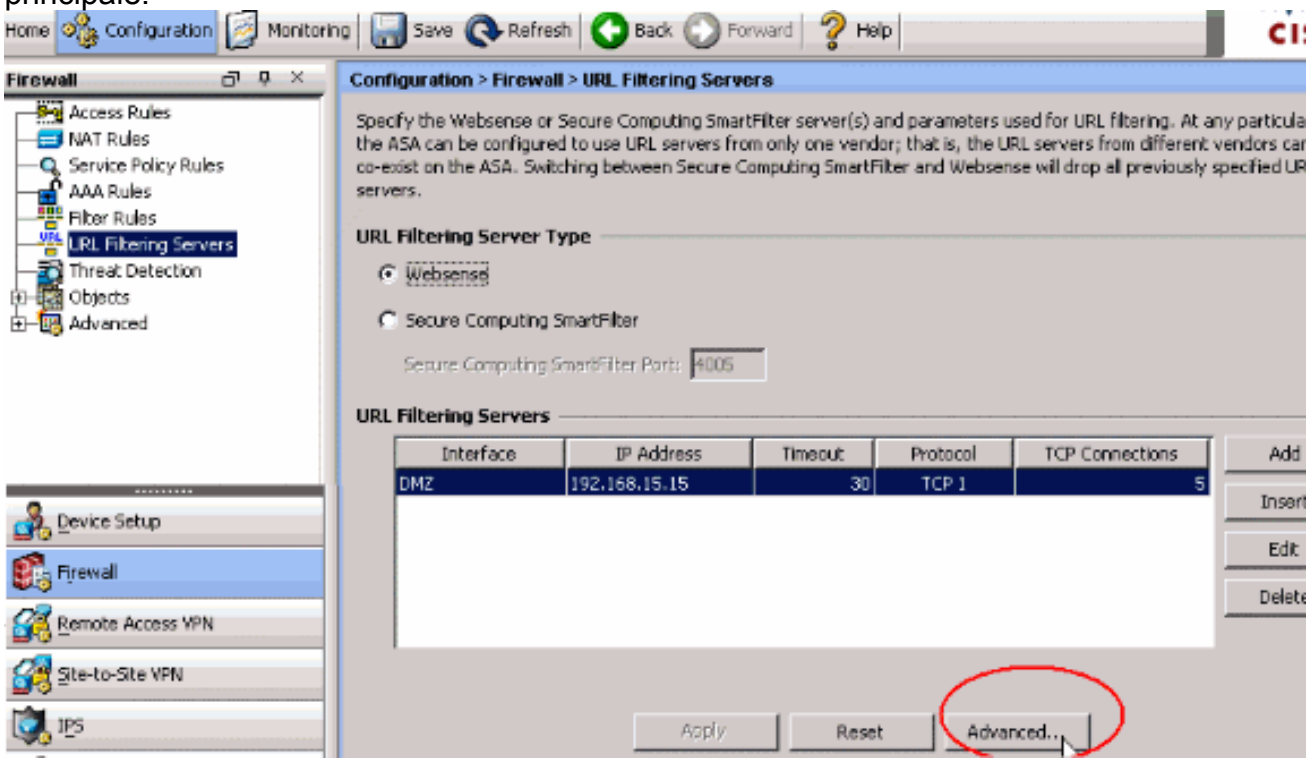
continuare.

9. Una volta configurati i parametri appropriati, fare clic su **Apply** (Applica) per inviare le modifiche.

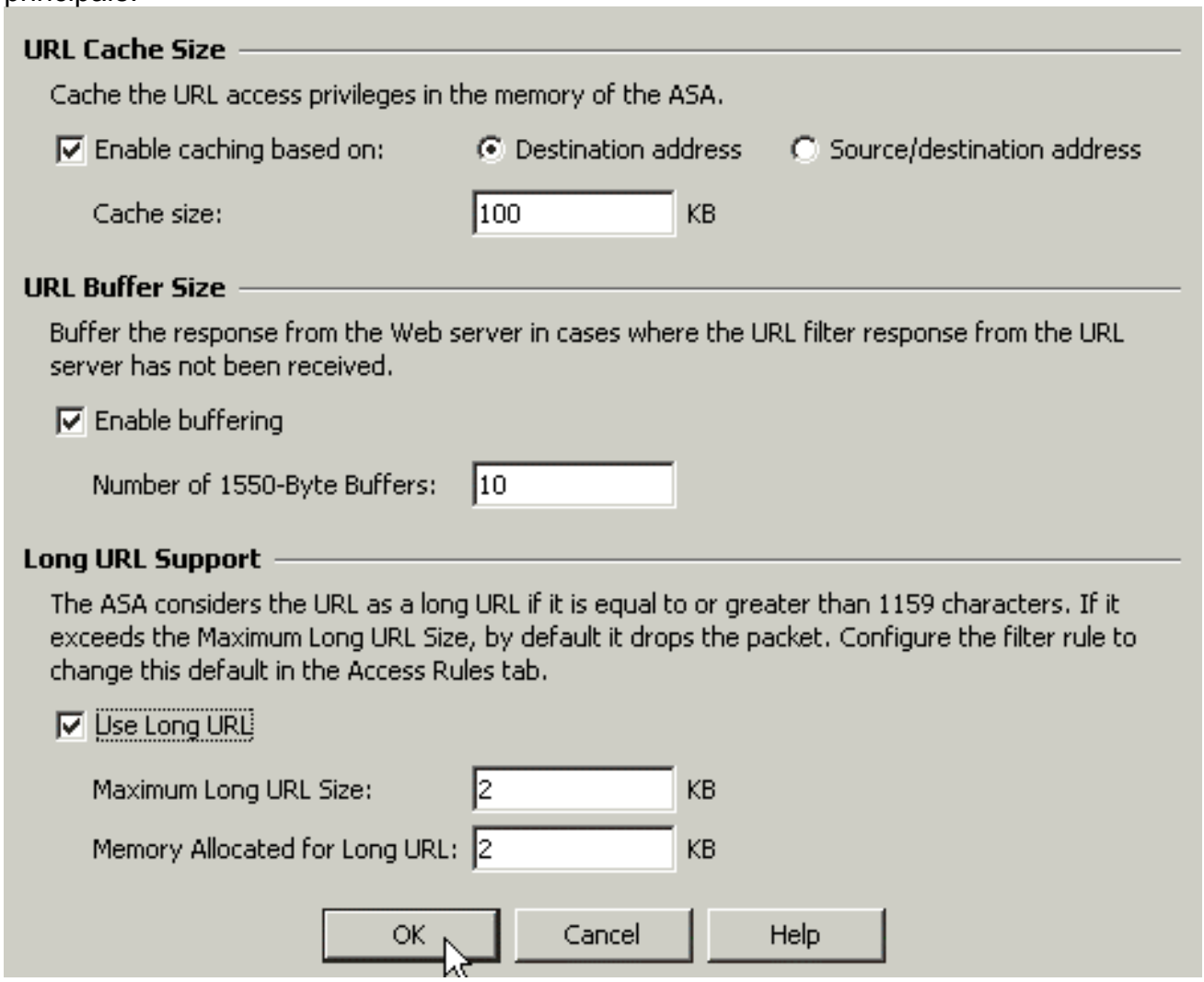


10. Per le opzioni avanzate del filtro URL, selezionare nuovamente **URL Filtering Server (Server filtro URL)** dall'elenco a discesa **Firewall**, quindi fare clic sul pulsante **Advanced** (Avanzate) nella finestra

principale.



11. Configurare i parametri, ad esempio la dimensione della cache dell'URL, la dimensione del buffer dell'URL e il supporto dell'URL lungo, nella finestra popup. Per continuare, fare clic su **OK** nella finestra popup e su **Applica** nella finestra principale.



12. Infine, accertarsi di salvare le modifiche apportate prima di terminare la sessione ASDM.

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 url-server**: visualizza le informazioni sul server di filtraggio.Ad esempio:
  ```
  hostname#show url-server
  url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp
  connections 10
  ```

  Nel software versione 7.2 e successive, usare il formato **show running-config url-server** di questo comando.
- **show url-server stats**: visualizza le informazioni e le statistiche sul server di filtro.Per il software versione 7.2, usare il modulo **show running-config url-server statistics** di questo comando.Nel software versione 8.0 e successive, usare il modulo **show url-server statistics** per questo comando.Ad esempio:
  ```
  hostname#show url-server statistics

  Global Statistics:
  --------------------
  URLs total/allowed/denied         13/3/10
  URLs allowed by cache/server      0/3
  URLs denied by cache/server       0/10
  HTTPSs total/allowed/denied       138/137/1
  HTTPSs allowed by cache/server    0/137
  HTTPSs denied by cache/server     0/1
  FTPs total/allowed/denied         0/0/0
  FTPs allowed by cache/server      0/0
  FTPs denied by cache/server       0/0
  Requests dropped                  0
  Server timeouts/retries           0/0
  Processed rate average 60s/300s   0/0 requests/second
  Denied rate average 60s/300s      0/0 requests/second
  Dropped rate average 60s/300s     0/0 requests/second

  Server Statistics:
  --------------------
  192.168.15.15                     UP
    Vendor                          websense
    Port                            15868
    Requests total/allowed/denied   151/140/11
    Server timeouts/retries         0/0
    Responses received              151
    Response time average 60s/300s  0/0

  URL Packets Sent and Received Stats:
  ------------------------------------
  Message                 Sent    Received
  STATUS_REQUEST          1609    1601
  LOOKUP_REQUEST          1526    1526
  LOG_REQUEST             0       NA

  Errors:
  ```

```
-------
RFC noncompliant GET method     0
URL buffer update failure       0
```

- **show url-block**: visualizza la configurazione del buffer del blocco URLAd esempio:

```
hostname#show url-block
    url-block url-mempool 128
    url-block url-size 4
    url-block block 128
```

Nel software versione 7.2 e successive, usare il comando **show running-config url-block** in forma di blocco.

- **show url-block statistics**: visualizza le statistiche del blocco URLAd esempio:

```
hostname#show url-block block statistics

URL Pending Packet Buffer Stats with max block  128
-----------------------------------------------------
Cumulative number of packets held:              896
Maximum number of packets held (per URL):       3
Current number of packets held (global):        38
Packets dropped due to
       exceeding url-block buffer limit:        7546
       HTTP server retransmission:              10
Number of packets released back to client:      0
```

Per il software versione 7.2, usare il modulo **show running-config url-block statistics** di questo comando.

- **show url-cache stats**: visualizza la modalità di utilizzo della cacheAd esempio:

```
hostname#show url-cache stats

URL Filter Cache Stats
----------------------
    Size :     128KB
 Entries :      1724
  In Use :       456
 Lookups :        45
    Hits :         8
```

Nel software versione 8.0, usare il modulo **show url-cache statistics** per questo comando.

- **show perfmon**: visualizza le statistiche sulle prestazioni del filtro URL e altre statistiche. Le statistiche di filtro vengono visualizzate nelle righe URL Access (Accesso URL) e URL Server Req (Richiesta server URL).Ad esempio:

```
hostname#show perfmon

PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          2/s
TCP Conns            0/s          2/s
UDP Conns            0/s          0/s
URL Access           0/s          2/s
URL Server Req       0/s          3/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          3/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

- **show filter**: visualizza la configurazione del filtro.Ad esempio:
```
hostname#show filter

filter url http 192.168.5.5 255.255.255.255 172.30.21.99 255.255.255.255 allow proxy-block
longurl-truncate cgi-truncate
```

  Nel software versione 7.2 e successive, usare il formato **show running-config filter** di questo comando.

Risoluzione dei problemi

In questa sezione vengono fornite informazioni su come risolvere i problemi relativi alla configurazione.

Errore: "%ASA-3-304009: Blocchi buffer esauriti specificati dal comando url-block"

La cache dell'URL del firewall si esaurisce per contenere le risposte del server quando il firewall attende di ricevere conferma dal server URL.

Soluzione

Il problema è essenzialmente correlato a una latenza tra l'ASA e il server Websense. Per risolvere il problema, provare le soluzioni indicate.

- Per comunicare con Websense, provare a modificare il protocollo usato sull'appliance ASA in UDP.Esiste un problema di latenza tra il server Websense e il firewall, in cui le risposte del server Websense impiegano molto tempo per tornare al firewall, in modo che il buffer URL si riempia mentre attende una risposta.Èpossibile utilizzare UDP anziché TCP per la comunicazione tra il server Websense e il firewall. Infatti, quando si usa il protocollo TCP per il filtro URL, per ogni nuova richiesta URL l'ASA deve stabilire una connessione TCP con il server Websense. Poiché UDP è un protocollo senza connessione, l'ASA non è costretta a stabilire la connessione per ricevere la risposta del server. Ciò dovrebbe migliorare le prestazioni del server.
```
ASA(config)#url-server (inside) vendor websense host  X.X.X.X timeout 30
protocol UDP version 4 connections 5
```
- Accertarsi di aumentare il blocco url al valore più alto possibile, ossia 128. Per controllare questa condizione, usare il comando **show url-block**.Se il numero è 128, prendere in considerazione l'miglioramento dell'ID bug Cisco CSCta27415 (solo utenti registrati).

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance - Supporto dei prodotti
- Cisco PIX serie 500 Security Appliance - Supporto dei prodotti
- Supporto dei prodotti Cisco Adaptive Security Device Manager
- PIX/ASA Definizione e risoluzione dei problemi di connettività tramite Cisco Security Appliance
- Risoluzione dei problemi di connessione tramite PIX e ASA

- Documentazione e supporto tecnico – Cisco Systems