Configuratievoorbeeld van PIX/ASA URL-filtering

Inhoud

Inleiding

Dit document legt uit hoe u URL-filtering op een beveiligingsapparaat kunt configureren.

Het filter heeft deze voordelen:

- Het kan veiligheidsrisico's verminderen en ongepast gebruik voorkomen.
- Het kan zorgen voor een betere controle over het verkeer dat door het beveiligingsapparaat loopt.

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 echter aanzienlijk trager zijn wanneer het verkeer wordt gefilterd met een externe filterserver.

Opmerking: Het filteren van lager veiligheidsniveau naar hoger wordt niet ondersteund. URL-filtering werkt alleen voor uitgaand verkeer, bijvoorbeeld, verkeer dat afkomstig is op een hoge veiligheidsinterface en bestemd is voor een server op een lage beveiligingsinterface.

Voorwaarden

Gebruikte componenten

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

- PIX 500 Series security applicatie met versie 6.2 en hoger
- ASA 5500 Series security applicatie met versie 7.x en hoger
- Adaptieve Security Devices Manager (ASDM) 6.0

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

U kunt verbindingsverzoeken filteren die uit een veiliger netwerk aan een minder veilig netwerk voortkomen. Hoewel u toegangscontrolelijsten (ACL's) kunt gebruiken om uitgaande toegang tot specifieke contentservers te voorkomen, is het vanwege de omvang en de dynamische aard van het internet moeilijk om gebruik op deze manier te beheren. U kunt de configuratie vereenvoudigen en de prestaties van het beveiligingsapparaat verbeteren met behulp van een aparte server waarop een van deze internetfilterproducten wordt uitgevoerd:

- Webeer Enterprise-filters HTTP, HTTPS en FTP. Het wordt ondersteund door PIX-firewall versie 5.3 en hoger.
- Secure Computing SmartFilter, voorheen bekend als N2H2-filters HTTP, HTTPS, FTP en lang URL-filtering. Het wordt ondersteund door PIX-firewall versie 6.2 en hoger.

Vergeleken met het gebruik van toegangscontrolelijsten vermindert dit de administratieve taak en verbetert dit de filtereffectiviteit. Ook, omdat URL-filtering op een afzonderlijk platform wordt verwerkt, wordt de prestatie van de PIX-firewall veel minder aangetast. Gebruikers kunnen echter langere toegangsperioden naar websites of FTP-servers opmerken wanneer de filterserver niet op afstand van het beveiligingsapparaat staat.

De PIX-firewall controleert uitgaande URL-verzoeken met het beleid dat op de URL-filterserver wordt gedefinieerd. De PIX-firewall staat de verbinding toe of ontkent, op basis van de reactie van de filterserver.

Als filtering is ingeschakeld en een verzoek om inhoud via het beveiligingsapparaat is gericht, wordt het verzoek tegelijkertijd naar de contentserver en de filterserver gestuurd. Als de filterserver de verbinding toelaat, zendt het veiligheidsapparaat de reactie van de contentserver naar de client die de aanvraag heeft ingediend door. Als de filterserver de verbinding ontkent, laat het beveiligingsapparaat de respons vallen en verstuurt u een bericht- of retourcode die aangeeft dat de verbinding niet met succes is voltooid.

Als de gebruikersverificatie op het beveiligingsapparaat is ingeschakeld, stuurt het beveiligingsapparaat ook de gebruikersnaam naar de filterserver. De filterserver kan gebruikersspecifieke filterinstellingen gebruiken of uitgebreide rapporten over het gebruik verstrekken.

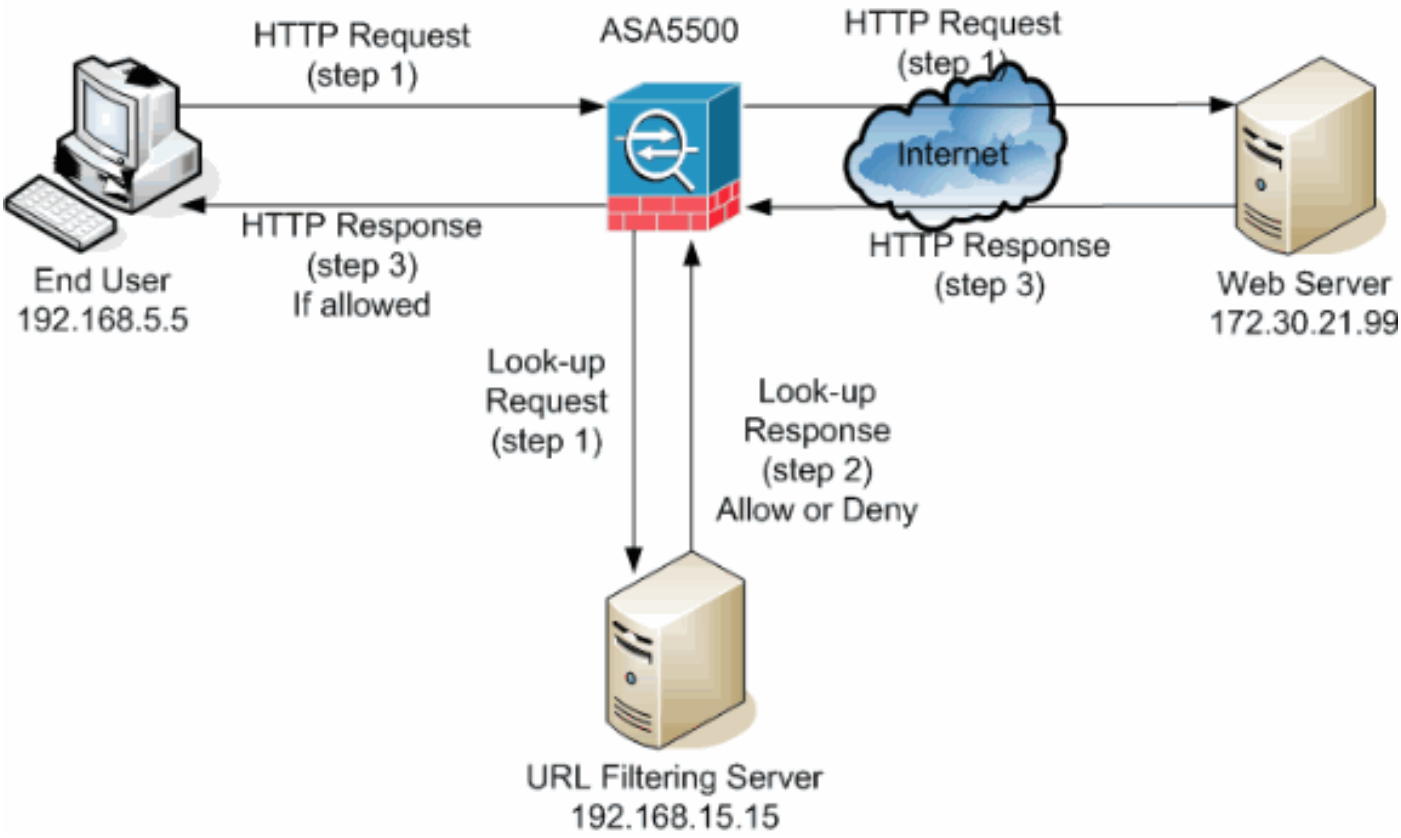
De ASA/PIX met de CLI configureren

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 bevindt de URL-filterserver zich in een DMZ-netwerk. Eindgebruikers in het netwerk proberen toegang te krijgen tot de webserver buiten het netwerk via het internet.

Deze stappen worden voltooid tijdens het gebruikersverzoek voor de webserver:

1. De eindgebruiker bladert naar een pagina op de webserver en de browser stuurt een HTTP aanvraag.
2. Nadat het beveiligingsapparaat dit verzoek heeft ontvangen, stuurt het het verzoek door naar de webserver en haalt het tegelijkertijd de URL uit en stuurt het een opzoek 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. Het beveiligingsapparaat 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 moet het adres van de filterserver identificeren met de opdracht **url-server**. U moet de juiste vorm van deze opdracht gebruiken, gebaseerd op het type filterserver dat u gebruikt.

Opmerking: Voor softwareversie 7.x en later kunt u maximaal vier filterservers voor elke context identificeren. Het beveiligingsapparaat gebruikt de servers in volgorde tot de server reageert. U kunt slechts één type server in uw configuratie configureren, ofwel Webec of N2H2.

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.

- Software, versie 6.2:

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

De opdracht **url-server** wijst de server aan die de N2H2 of Websin URL-filtertoepassing draait. De limiet is 16 URL servers. U kunt echter maar één applicatie tegelijk gebruiken: N2H2 of Websensor. Bovendien, als u uw configuratie op de PIX firewall verandert, werkt het de configuratie op de toepassingsserver niet bij. Dit moet afzonderlijk gebeuren op basis van de instructies van de afzonderlijke verkoper.

- Software, versie 7.x en hoger:

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

Vervang `if_name` door de naam van de beveiligingswasmachine-interface die is aangesloten op de filterserver. De standaard zit erin. Vervang `local_ip` met het IP-adres van de filterserver. Vervang `seconden` door het aantal seconden dat het security apparaat moet proberen aan te sluiten op de filterserver.

Gebruik de optie `protocol` om te specificeren of u TCP of UDP wilt gebruiken. Met een Webslank server kunt u ook de `versie` van TCP specificeren die u wilt gebruiken. TCP versie 1 is standaard. TCP versie 4 stelt de PIX-firewall in staat om geauthentiseerde gebruikersnamen en URL-loginformatie naar de Websfeer-server te sturen als de PIX-firewall de gebruiker al heeft geauthenticeerd.

Om bijvoorbeeld één webzinsfilterserver te identificeren, geeft u deze opdracht uit:

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

Secure Computing SmartFilter

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

- Software versie 7.0 en 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]]`

- Softwareversie 7.2 en hoger:
  `hostname(config)#url-server (if_name) vendor {secure-computing | n2h2} host`

  Voor de `verkoper/verkoper | n2h2]`, kunt u `veilig-rekenwerk` als een verkopers string gebruiken. `n2h2` is echter aanvaardbaar voor compatibiliteit met de achterzijde. Wanneer de configuratieingangen worden gegenereerd, `veilig-rekenwerk` wordt opgeslagen als de kraan van de verkoper.

Vervang `if_name` door de naam van de beveiligingswasmachine-interface die is aangesloten op de filterserver. De standaard zit erin. Vervang `local_ip` met het IP-adres van de filterserver en `poort <number>`met het gewenste poortnummer.

Opmerking: de standaardpoort die door de Secure Computing SmartFilter server wordt gebruikt om met het security apparaat met TCP of UDP te communiceren, is poort 4005.

Vervang `seconden` door het aantal seconden dat het security apparaat moet proberen aan te sluiten op de filterserver. Gebruik de optie `protocol` om te specificeren of u TCP of UDP wilt gebruiken.

De `verbindingen <number>`zijn het aantal keer dat u probeert een verbinding te maken tussen de host en de server.

Om bijvoorbeeld één N2H2-filterserver te identificeren, geeft u deze opdracht uit:

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

Of, als u standaardwaarden wilt gebruiken, geeft u deze opdracht uit:

```
hostname(config)#url-server (DMZ) vendor n2h2 host 192.168.15.15
```

Het filterbeleid configureren

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

URL-filtering inschakelen

Wanneer de filterserver een HTTP-verbindingsaanvraag goedkeurt, staat het security apparaat het antwoord van de webserver toe om de client te bereiken die de aanvraag heeft ingediend. Als de filterserver het verzoek ontkent, wijst het beveiligingsapparaat de gebruiker terug naar een blokpagina die aangeeft dat de toegang wordt geweigerd.

Geef de opdracht **filter toe** om het beleid te configureren dat wordt gebruikt om URL's te filteren:

- PIX versie 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, versie 7.x en hoger:

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

Vervang `poort` met het poortnummer waarop HTTP-verkeer moet worden gefilterd als een andere poort dan de standaardpoort voor HTTP (80) wordt gebruikt. Om een bereik van poortnummers te identificeren voert u het begin- en einde van de range in, gescheiden door een koppelteken.

Als filtering is ingeschakeld, stopt het beveiligingsapparaat het HTTP-verkeer uit totdat een filterserver de verbinding toestaat. Als de primaire filterserver niet reageert, stuurt het beveiligingsapparaat de filteraanvraag naar de secundaire filterserver. Met de optie kunt u ervoor zorgen dat het security apparaat doorspoelt van HTTP-verkeer zonder filtering, wanneer de primaire filterserver niet beschikbaar is.

Geef de **proxy-block** opdracht uit om alle verzoeken naar proxy servers te laten vallen.

Opmerking: de rest van de parameters wordt gebruikt om lange URL's te beknotten.

Truncate Long HTTP URL's

De optie met een `lange`-truncate zorgt ervoor dat het beveiligingsapparaat alleen de naam van de host of het IP-adresgedeelte van de URL voor evaluatie naar de filterserver stuurt wanneer de URL langer is dan de maximaal toegestane lengte.

Gebruik de optie `longurl-ontkennen` om uitgaande URL verkeer te ontkennen als de URL langer is dan het maximum toegestaan.

Gebruik de optie `cgi-truncate` om CGI URLs te inkorten om alleen de CGI script locatie en de script naam zonder enige parameters op te nemen.

Dit is een algemeen voorbeeld van de filterconfiguratie:

```
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
```

Vrijgesteld verkeer door filtering

Als u een uitzondering wilt maken op het algemene filterbeleid, geeft u deze opdracht uit:

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

Vervang `local_ip` en `local_mask` met het IP adres en het subnetmasker van een gebruiker of subnetwerk die u van filterbeperkingen wilt vrijstellen.

Vervang `foreign_ip` en `foreign_mask` met het IP adres en het subnetmasker van een server of subnetwork die u van filterbeperkingen wilt vrijstellen.

Bijvoorbeeld, deze opdracht veroorzaakt alle HTTP verzoeken om 172.30.21.99, van de binnenhosts, om te worden doorgestuurd naar de filterserver behalve voor verzoeken van host 192.168.5.5:

Dit is een configuratievoorbeeld voor een uitzondering:

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

Geavanceerde URL-filtering

Deze sectie verschaft informatie over geavanceerde filterparameters, die deze onderwerpen bevatten:

- buffering
- castreren
- lange URL-ondersteuning

Buffer de reacties van de webserver

Wanneer een gebruiker een verzoek indient om verbinding te maken met een contentserver, stuurt het beveiligingsapparaat tegelijkertijd het verzoek naar de contentserver en de filterserver. Als de filterserver niet reageert vóór de contentserver, wordt de serverrespons verminderd. Dit vertraagt de reactie van de webserver vanuit het oogpunt van de webclient omdat de client het verzoek opnieuw moet indienen.

Als u de HTTP-responsbuffer activeert, worden de antwoorden van webcontentservers gebufferd en worden de reacties doorgestuurd naar de client die het verzoek indient als de filterserver de

verbinding toestaat. Dit voorkomt de vertraging die anders kan optreden.

Voltooi de volgende stappen om reacties op HTTP-aanvragen te bufferen:

1. Om het bufferen van reacties voor HTTP verzoeken mogelijk te maken die in afwachting zijn van een antwoord van de filterserver, geef deze opdracht uit:
   `hostname(config)#url-block block block-buffer-limit`

   Plaats `de limiet van de buffer-buffer terug` met het maximale aantal blokken dat moet worden gebufferd.
2. Om het maximale geheugen aan te passen dat beschikbaar is om hangende URL's te bufferen en lange URL's met Websensor te bufferen, geeft u deze opdracht uit:
   `hostname(config)#url-block url-mempool memory-pool-size`

   Plaats `het geheugen-pool-formaat` met een waarde van 2 tot 10240 voor een maximale geheugentoewijzing van 2 KB tot 10 MB.

Cache Server-adressen

Nadat een gebruiker toegang heeft tot een site, kan de filterserver het beveiligingsapparaat toestaan om het serveradres gedurende een bepaalde tijd in te houden, zolang elke locatie op het adres is opgeslagen in een categorie die te allen tijde is toegestaan. Als de gebruiker de server opnieuw benadert of als een andere gebruiker toegang heeft tot de server, hoeft het beveiligingsapparaat de filterserver niet opnieuw te raadplegen.

Geef de **url-cache** opdracht af indien nodig om de doorvoersnelheid te verbeteren:

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

Vervang `grootte` met een waarde voor de cachegrootte binnen bereik 1 tot 128 (KB).

Gebruik het trefwoord om indelingen op basis van het URL-doeladres in te delen. Selecteer deze modus als alle gebruikers hetzelfde URL-filterbeleid op de weblogserver hebben.

Gebruik het sleutelwoord `src_dst` om ingangen in het voorgeheugen te plaatsen gebaseerd op zowel het bronadres dat het URL verzoek zowel als het URL doeladres initieert. Selecteer deze modus als de gebruikers niet hetzelfde URL-filterbeleid op de weblogserver hebben.

Filtering van lange URL's inschakelen

Standaard beschouwt het security apparaat een HTTP URL als een lange URL als deze groter is dan 1159 tekens. U kunt de maximaal toegestane lengte voor één URL met deze opdracht verhogen:

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

Plaats `lang url-size` terug in KB voor elke lange URL die moet worden gebufferd.

Met deze opdrachten kunt u bijvoorbeeld het beveiligingsapparaat configureren voor

geavanceerde URL-filtering:

```
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
```

Configuratie

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

ASA 8.0-configuratie

```
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
```

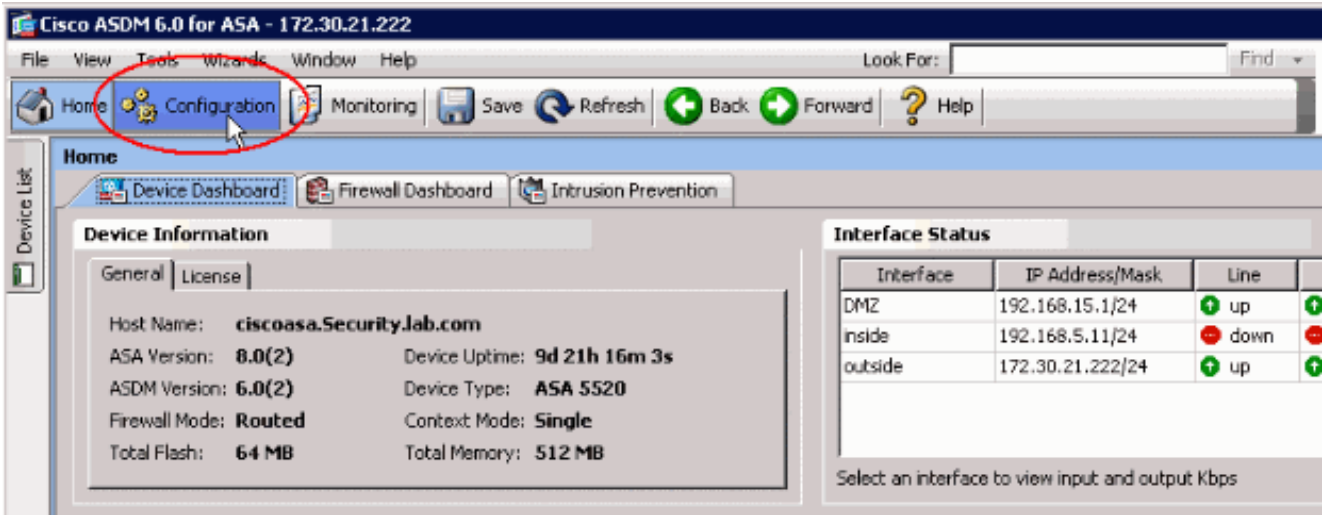
```
ssh timeout 60
console timeout 0
management-access inside
dhcpd address 192.168.5.12-192.168.5.20 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class 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
```

ASA/PIX configureren met ASDM

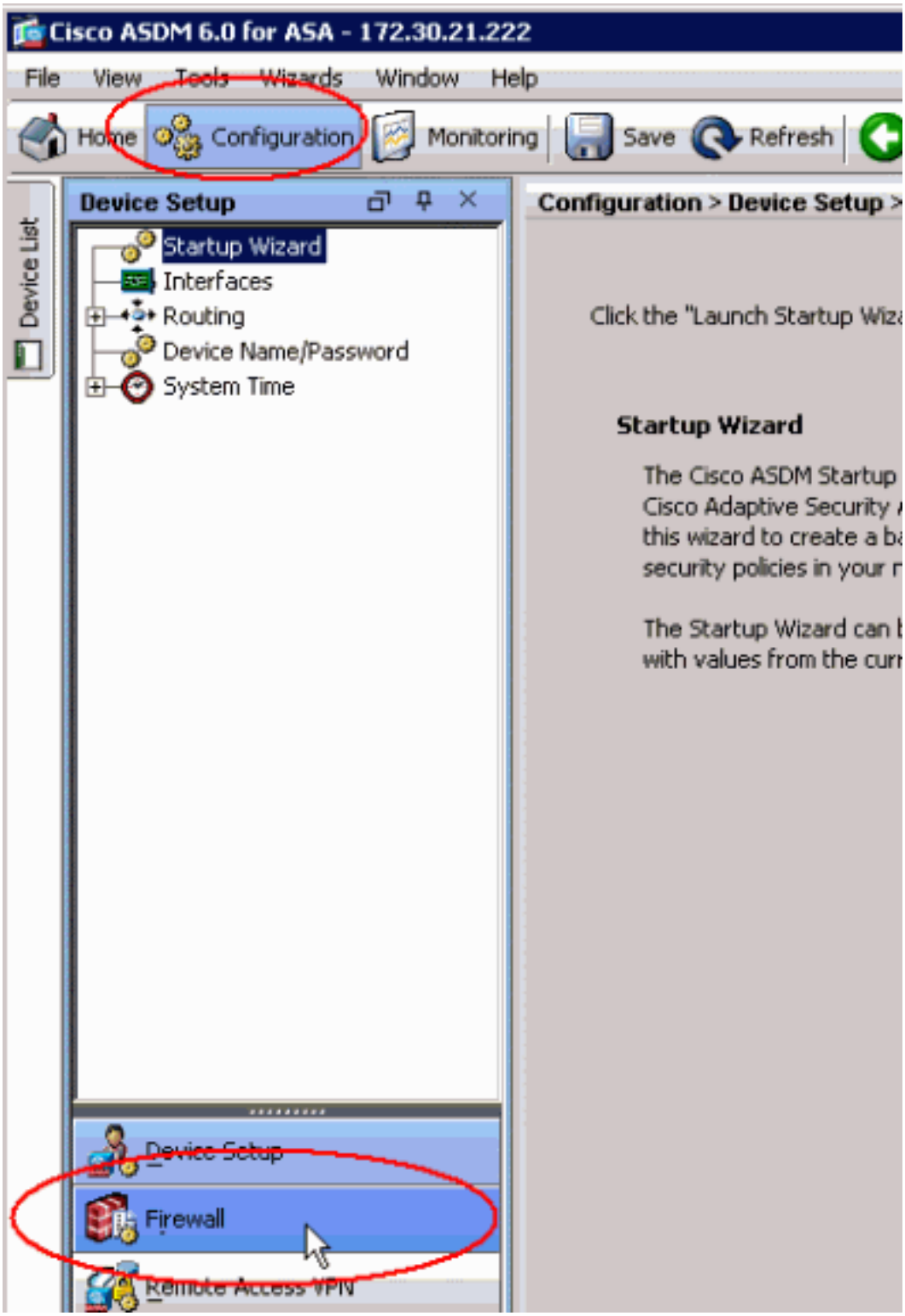
Deze sectie laat zien hoe u URL-filtering voor het security apparaat kunt configureren met de Adaptieve Security Apparatuur Manager (ASDM).

Nadat u ASDM start, dient u deze stappen te voltooien:

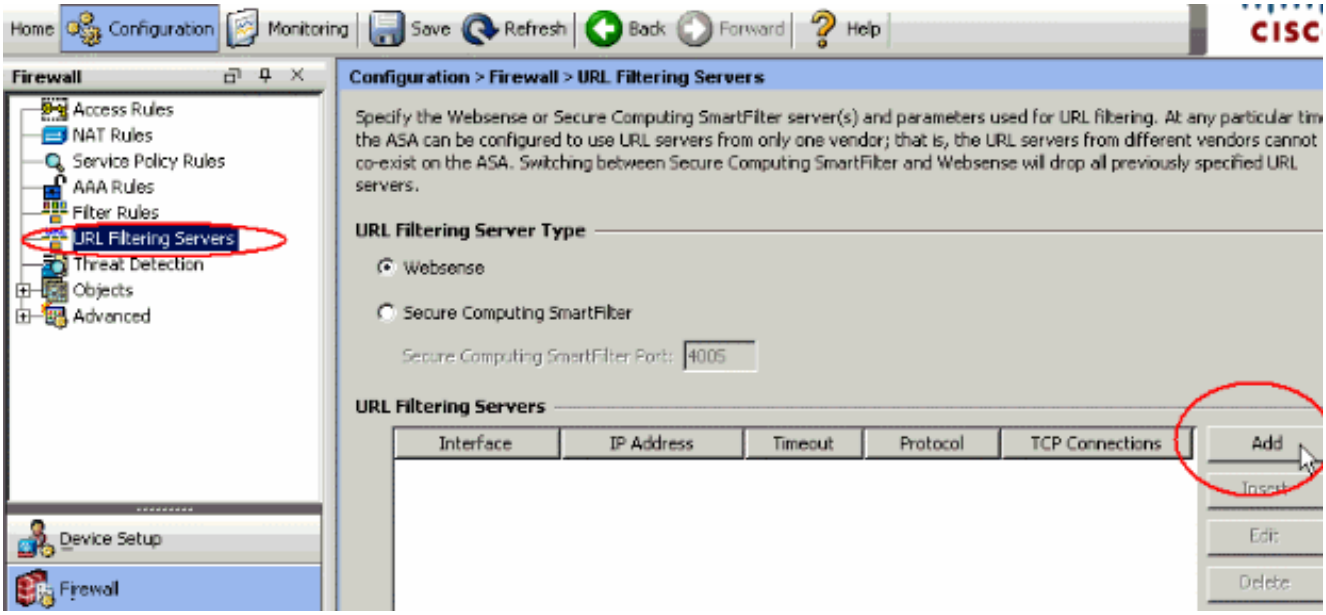
1. Kies het venster **Configuration**.



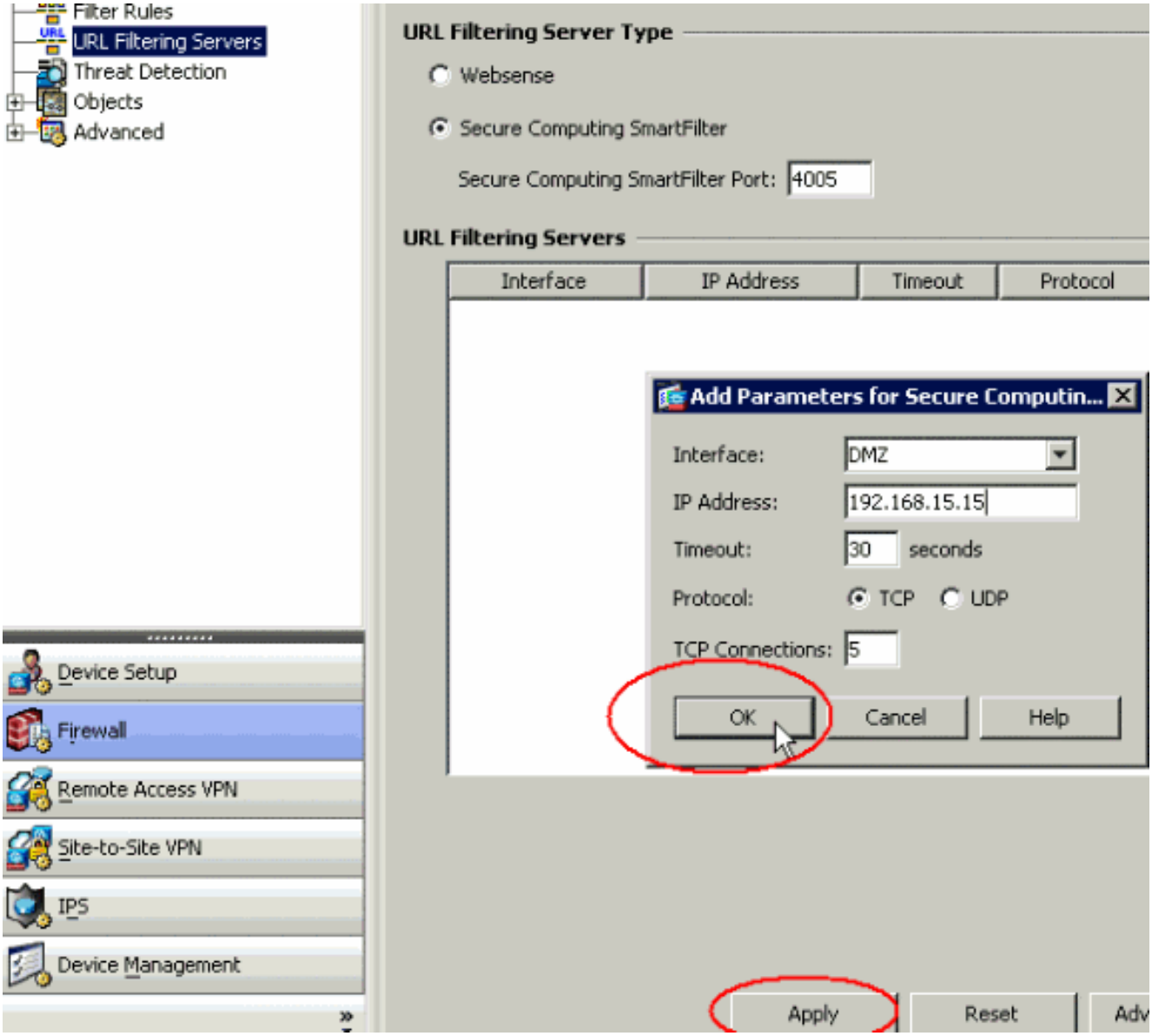
2. Klik op **Firewall** in de lijst in het **Configuratiescherm**.



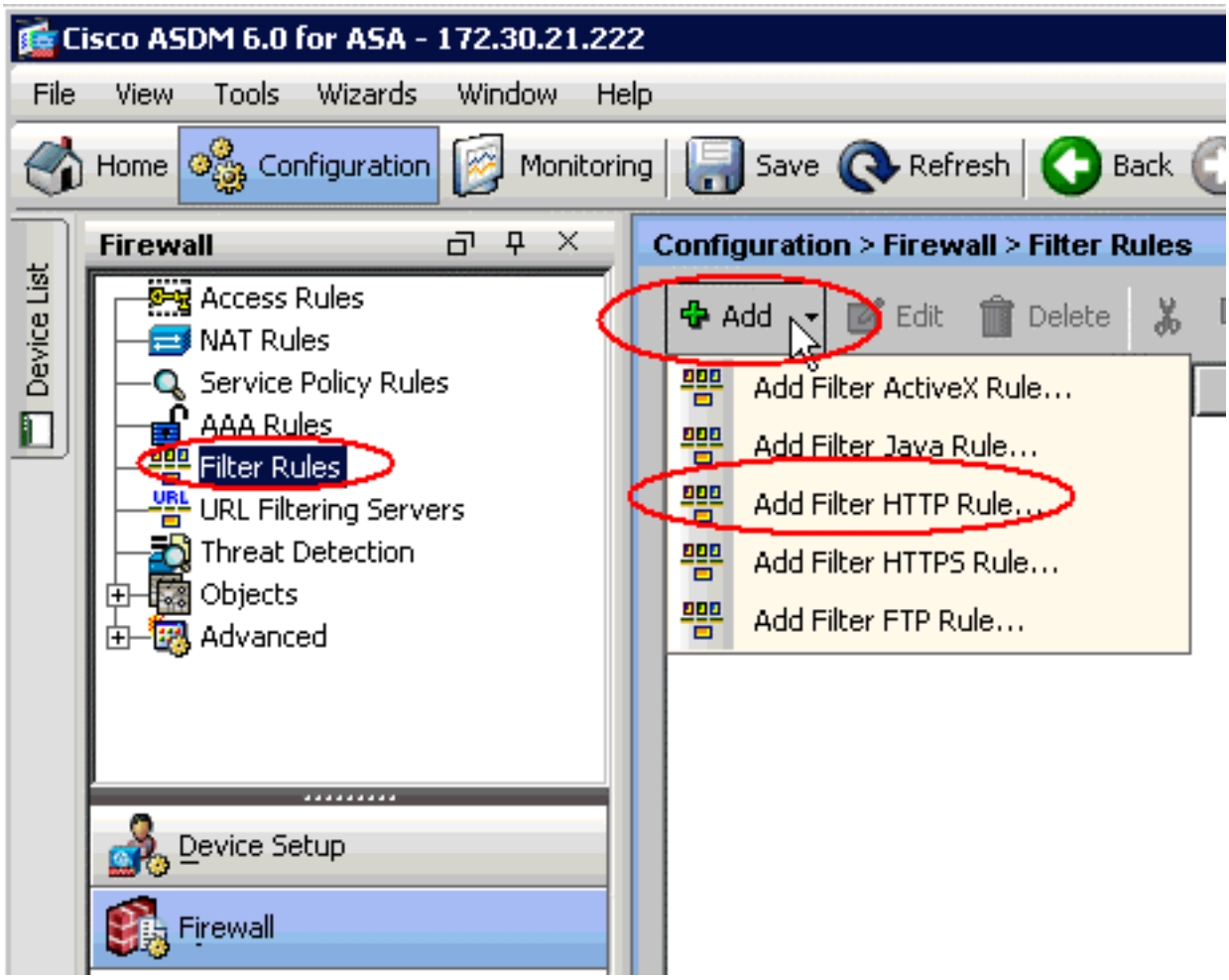
3. Kies in de vervolgkeuzelijst **Firewall** de **URL-filtering servers**. Kies het type URL Filtering Server dat u wilt gebruiken en klik op **Add** om zijn parameters te configureren.**Opmerking:** U moet de filterserver toevoegen voordat u filtering kunt instellen voor HTTP, HTTPS of FTP-filterregels.



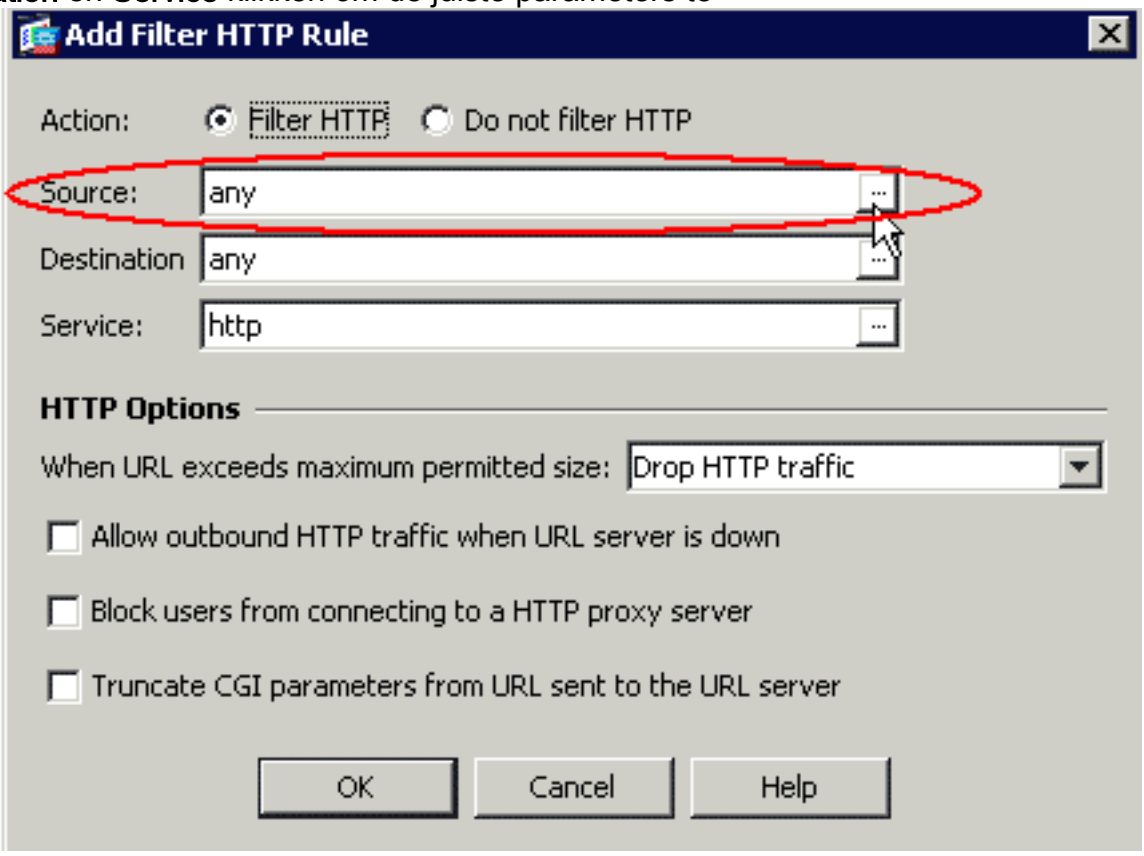
4. Kies de gewenste parameters in het pop-upvenster:Interface - Hiermee wordt de interface weergegeven die is aangesloten op de filterserverIP-adres—Hier wordt het IP-adres van de filterserver weergegevenTime-out: Hiermee wordt het aantal seconden weergegeven waarna het verzoek wordt gericht aan de filterserver tijdenProtocol-Toont het protocol dat wordt gebruikt om met de filterserver te communiceren. TCP versie 1 is standaard. TCP versie 4 stelt de PIX-firewall in staat om geauthentiseerde gebruikersnamen en URL-loginformatie naar de weblogserver te verzenden, als de PIX-firewall de gebruiker al echt heeft verklaardTCP-verbindingen—hiermee wordt het maximale aantal TCP-verbindingen weergegeven dat mag communiceren met de URL-filterserverNadat u de parameters hebt ingevoerd, klikt u op **OK** in het pop-upvenster en **Toepassen** in het hoofdvenster.



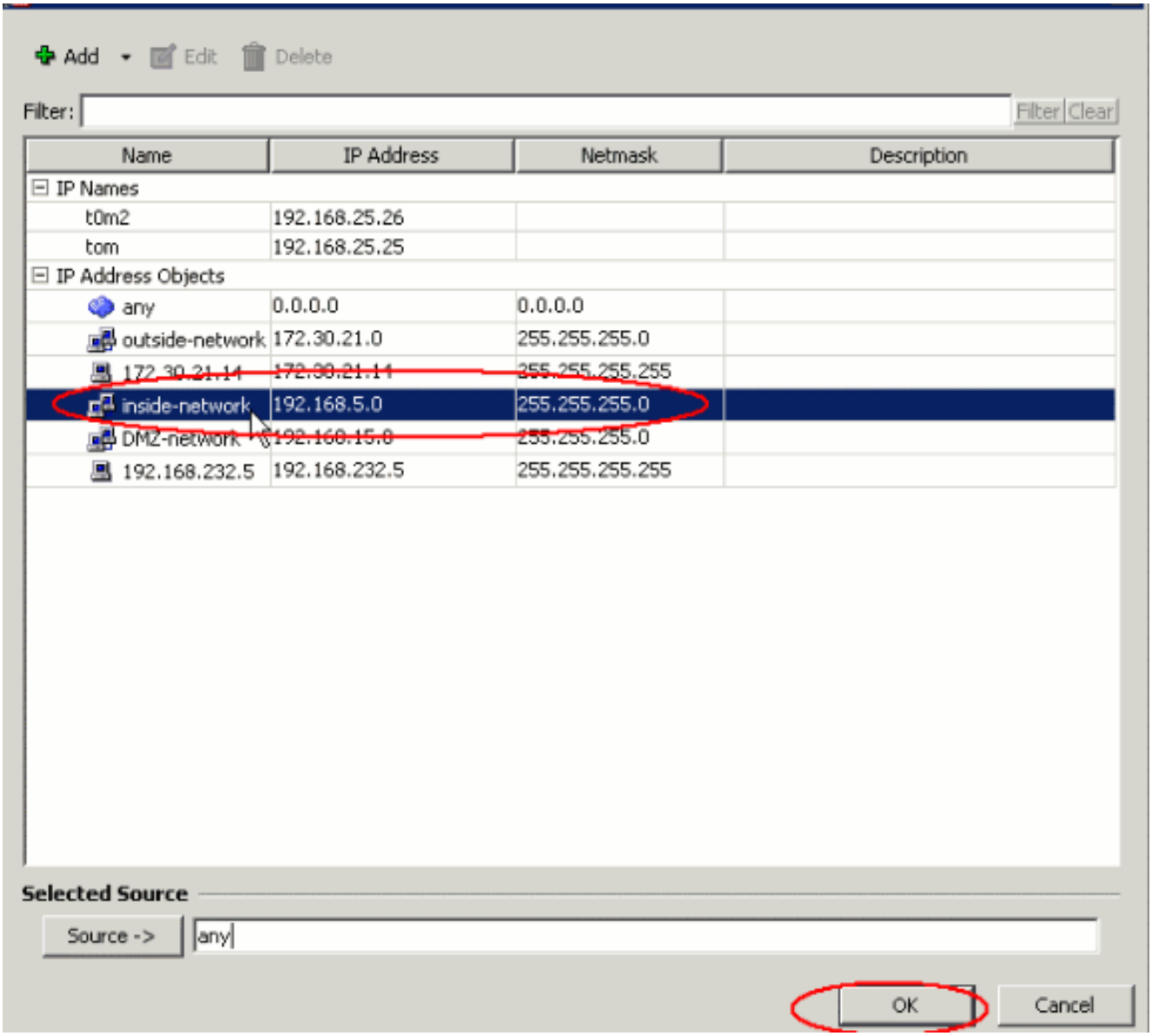
5. Kies in de vervolgkeuzelijst **Firewall** de **regels voor het filter**. Klik op de knop **Toevoegen** in het hoofdvenster en kies het type regel dat u wilt toevoegen. In dit voorbeeld wordt de **HTTP-regel voor filter toevoegen**
geselecteerd.



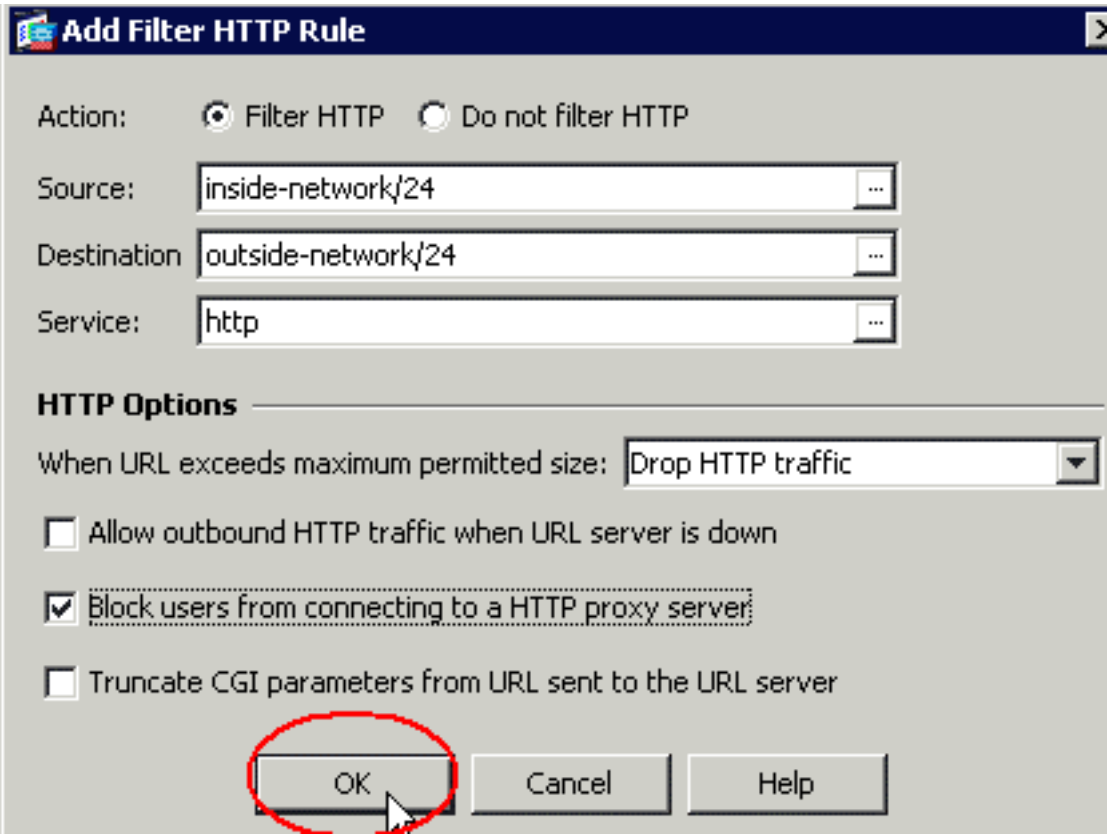
6. Nadat het pop-upvenster verschijnt, kunt u op de browse-knoppen voor de opties **Bron**, **Destination** en **Service** klikken om de juiste parameters te kiezen.



7. Dit toont het venster van het browse venster voor de optie **Bron**. Maak uw selectie en klik op **OK**.

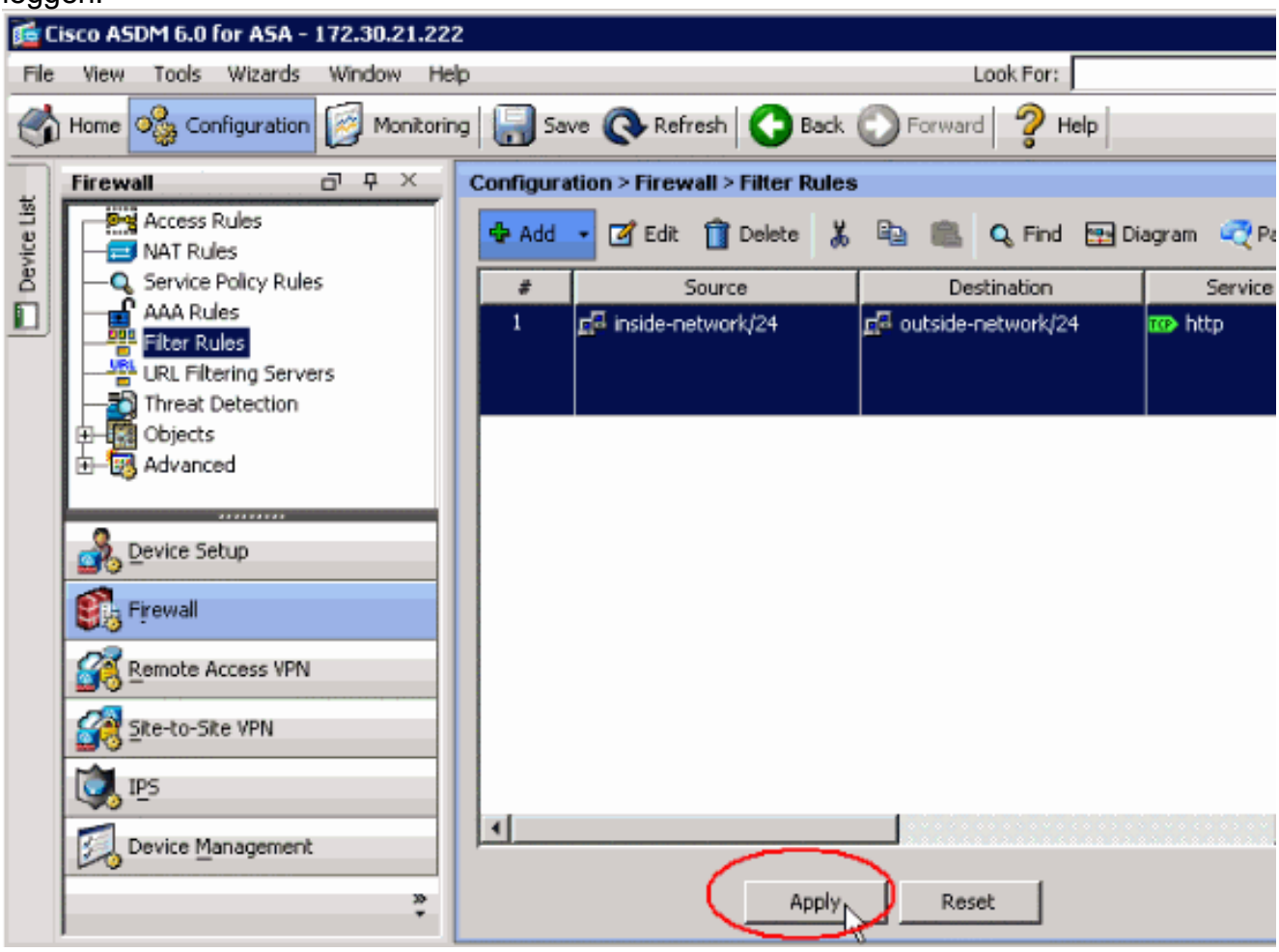


8. Nadat u de selectie voor alle parameters hebt voltooid, klikt u op **OK** om door te

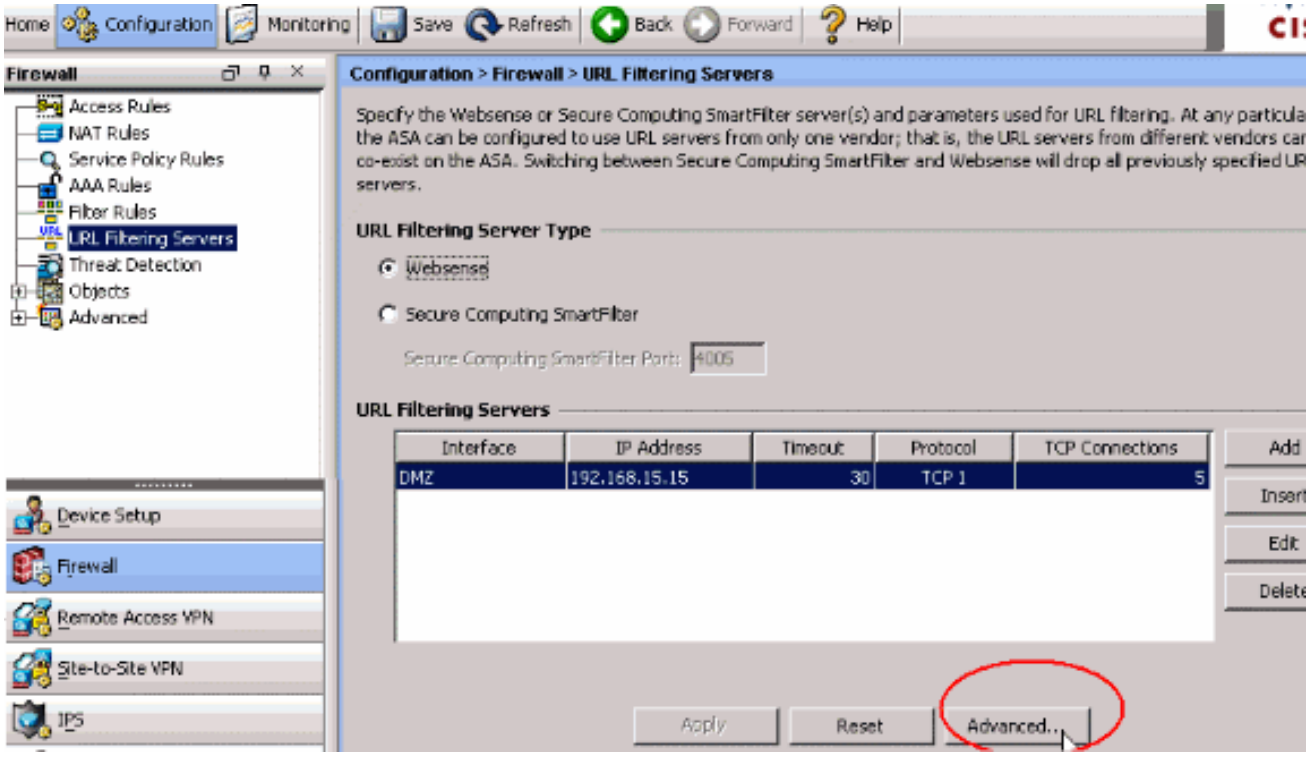


gaan.

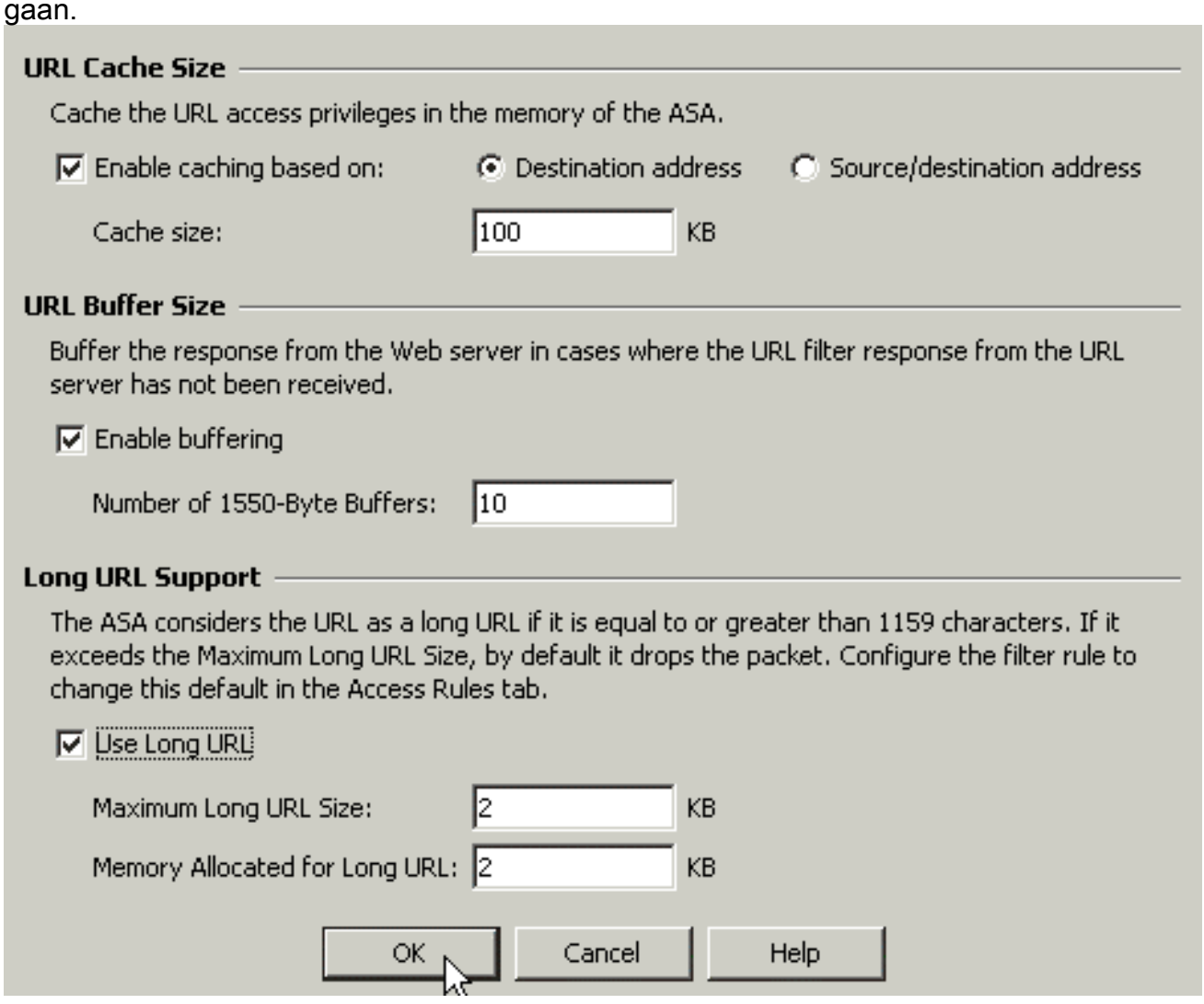
9. Zodra de juiste parameters zijn ingesteld, klikt u op **Toepassen** om de wijzigingen voor te leggen.



10. Voor geavanceerde URL-filteropties kiest u opnieuw **URL Filtering Server** uit de vervolgkeuzelijst **Firewall** en klikt u op de knop **Geavanceerd** in het hoofdvenster.



11. Configureer de parameters, zoals de URL cache-grootte, de URL-buffergrootte en de lange URL-ondersteuning in het pop-upvenster. Klik op **OK** in het popupvenster en klik **op** Toepassen in het hoofdvenster om verder te gaan.



12. Tenslotte, zorg ervoor dat u de veranderingen opslaat die u aanbrengt voordat u de ASDM-

sessie beëindigt.

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.

- **toont url-server**—Toont informatie over de filterserverBijvoorbeeld:
```
hostname#show url-server
url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp
connections 10
```

  In softwareversie 7.2 en later, geef de **show in werking stellen-in werking stellen-configuratie url-server** vorm van deze opdracht uit.
- **De status van de url-server tonen** —Toont informatie en statistieken over de filterserverVoor softwareversie 7.2, geef de **show in werking stellen-configuratie url-server statistieken** vorm van deze opdracht uit.In softwareversie 8.0 en later geeft u de vorm **van** deze opdracht de **stookoxistentiestatistieken** weer.Bijvoorbeeld:
```
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
```

- **toon url-block**-Geeft de configuratie van de URL blok-buffer weerBijvoorbeeld:
```
hostname#show url-block
    url-block url-mempool 128
    url-block url-size 4
    url-block block 128
```

  In softwareversie 7.2 en later, geef de **show in werking stellen-configuratie url-block** vorm van deze opdracht uit.
- **Statistieken van blok-blok tonen** - toont de URL-blokstatistiekenBijvoorbeeld:
```
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
```

  Voor softwareversie 7.2 geeft u de **show in werking stellen-configuratie url-block statistieken** van deze opdracht uit.
- **tonen de status van het url-cache** - toont hoe het cache wordt gebruiktBijvoorbeeld:
```
hostname#show url-cache stats

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

  In softwareversie 8.0 geeft u de **show url-cache statistiek** vorm van deze opdracht af.
- **tonen perfmon**-toont URL het filteren van prestatiestatistieken, samen met andere prestatiestatistieken. De filterstatistieken worden weergegeven in de rijen Req van de URL Access en URL Server.Bijvoorbeeld:
```
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
```

- **Het filter tonen** —Toont de filterconfiguratieBijvoorbeeld:
```
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
```

  In softwareversie 7.2 en later, geef de **show in werking stellen-configuratiefiltervorm** van deze opdracht uit.

Problemen oplossen

Deze sectie verschaft informatie over het oplossen van problemen in uw configuratie.

Fout: "%ASA-3-30409: Uitschakelen van bufferblokken gespecificeerd door middel van URL-block opdracht"

Firewall loopt zonder URL cache dat bedoeld is om serverantwoorden te bevatten wanneer de firewall bevestiging van de URL server wacht.

Oplossing

De kwestie houdt verband met een latentie tussen de ASA en de Websleser. Probeer deze tijdelijke oplossing voor dit probleem aan de hand van de volgende stappen.

- Probeer het protocol dat op de ASA wordt gebruikt in UDP te veranderen om met de Websensor te communiceren.Er is een probleem met latentie tussen de Websone-server en de firewall, waarbij de antwoorden van de Websone-server lang duren om terug te keren naar de firewall, waardoor de URL-buffer opvult terwijl hij op een reactie wacht.U kunt UDP in plaats van TCP gebruiken voor de communicatie tussen de webzineserver en de Firewall. Dit komt doordat wanneer u TCP voor URL-filtering gebruikt, voor elk nieuw URL-verzoek, de ASA een TCP-verbinding met de Webslaansserver moet opzetten. Aangezien UDP een protocol zonder verbindingen is, is de ASA niet gedwongen om de verbinding in te stellen om de reactie van de server te ontvangen. Dit zou de prestaties van de server moeten verbeteren.
```
ASA(config)#url-server (inside) vendor websense host  X.X.X.X timeout 30
protocol UDP version 4 connections 5
```
- Zorg ervoor dat u het blok-blok verhoogt naar de hoogste waarde mogelijk, die 128 is. Dit kan worden gecontroleerd met de opdracht **url-block**.Als deze functie 128 toont, houdt u rekening met de verbetering van Cisco bug-ID CSCta27415 (**alleen** geregistreerde **klanten**).

Gerelateerde informatie

- Cisco ASA 5500 Series productondersteuning voor adaptieve security applicaties
- Cisco PIX 500 Series security applicaties - productondersteuning
- Productondersteuning voor Cisco Adaptieve Security Apparatuur Manager
- PIX/ASA: Connectiviteit met Cisco security applicatie vaststellen en oplossen
- Probleemoplossing met verbindingen via PIX en ASA

- Technische ondersteuning en documentatie – Cisco Systems