Ejemplo de configuración del Filtrado de URL del PIX/ASA

Contenido

Introducción

Este documento explica cómo configurar el Filtrado de URL en un dispositivo de seguridad.

Al filtrar tráfico tiene estas ventajas:

- Puede ayudar a reducir los riesgos de seguridad y a prevenir el uso inadecuado.
- Puede proporcionar el mayor control sobre el tráfico que pasa a través del dispositivo de seguridad.

Nota: Porque el Filtrado de URL es Uso intensivo de la CPU, el uso de un servidor de filtrado externo se asegura de que la producción del otro tráfico no sea afectada. Sin embargo, sobre la base de la velocidad de su red y de la capacidad de su servidor del Filtrado de URL, el tiempo requerido para la conexión inicial puede ser perceptiblemente más lento cuando el tráfico se filtra con un servidor de filtrado externo.

Nota: Implement que filtra de un nivel de seguridad más bajo a más arriba no se soporta. El Filtrado de URL trabaja solamente para el tráfico saliente, por ejemplo, el tráfico que origina en una interfaz de la gran seguridad destinada para un servidor en una interfaz de seguridad baja.

prerrequisitos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad de la serie PIX 500 con la versión 6.2 y posterior
- Dispositivo de seguridad de las 5500 Series ASA con la versión 7.x y posterior
- Administrador de dispositivos de seguridad adaptante (ASDM) 6.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Usted puede filtrar los pedidos de conexión que originan de una red más segura a una red menos segura. Aunque usted pueda utilizar el Listas de control de acceso (ACL) para prevenir el acceso de salida a los servidores del contenido del específico, es difícil manejar el uso esta manera debido al tamaño y la naturaleza dinámica de Internet. Usted puede simplificar la configuración y mejorar el funcionamiento del dispositivo de seguridad con el uso de un servidor separado que funcione con uno de estos Productos de filtración de Internet:

- Empresa del Websense — filtros HTTP, HTTPS, y FTP. Es soportada por la versión 5.3 y posterior del firewall PIX.
- Asegure SmartFilter computacional, conocido antes como N2H2 — los filtros HTTP, HTTPS, FTP, y Filtrado de URL largo. Es soportado por la versión 6.2 y posterior del firewall PIX.

Comparado al uso de las listas de control de acceso, esto reduce la tarea administrativa y mejora la eficacia de filtración. También, porque el Filtrado de URL se maneja en una plataforma separada, el funcionamiento del firewall PIX es mucho menos afectado. Sin embargo, los usuarios pueden notar horas de acceso más largas a los sitios web o a los servidores FTP cuando el servidor de filtrado es remoto del dispositivo de seguridad.

El firewall PIX marca las peticiones salientes URL con la directiva definida en el servidor del Filtrado de URL. El firewall PIX permite o niega la conexión, sobre la base de la respuesta del servidor de filtrado.

Cuando se habilita la filtración y un pedido el contenido se dirige a través del dispositivo de seguridad, la petición se envía al servidor contento y al servidor de filtrado al mismo tiempo. Si el servidor de filtrado permite la conexión, el dispositivo de seguridad adelante la respuesta del servidor contento al cliente que originó la petición. Si el servidor de filtrado niega la conexión, el dispositivo de seguridad cae la respuesta y envía un mensaje o un código de retorno que indique que la conexión no es acertada.

Si la autenticación de usuario se habilita en el dispositivo de seguridad, el dispositivo de seguridad también envía el Nombre de usuario al servidor de filtrado. El servidor de filtrado puede utilizar las configuraciones de filtración específicas del usuario o proporcionar los informes aumentados con respecto al uso.

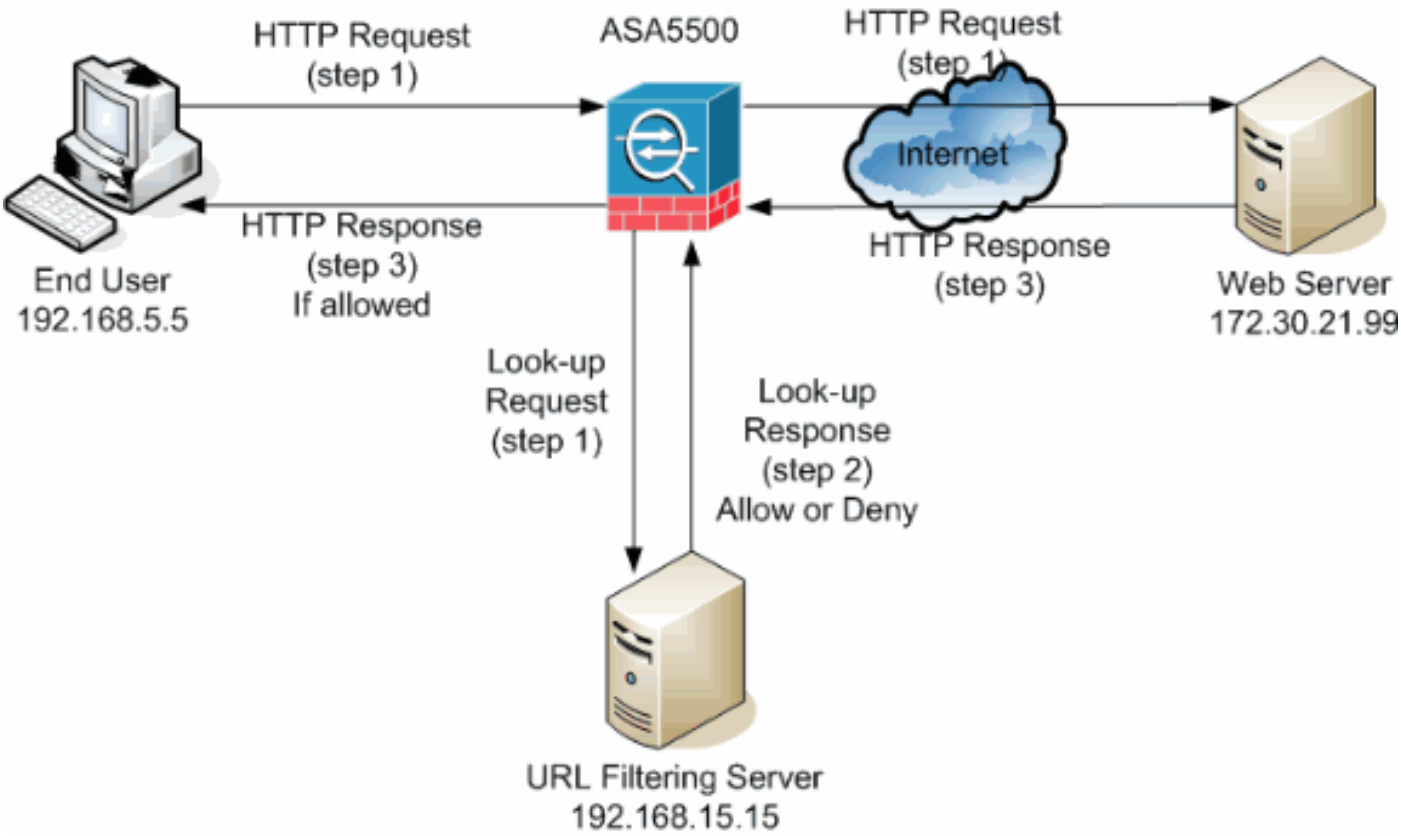
Configure ASA/PIX con el CLI

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



En este ejemplo, el servidor del Filtrado de URL está situado en una red DMZ. Los usuarios finales situados dentro de la red intentan acceder al servidor Web situado fuera de la red sobre Internet.

Estos pasos se completan durante la petición del usuario para el servidor Web:

1. El usuario final hojea a una página en el servidor Web, y el navegador envía un pedido de HTTP.
2. Después de que el dispositivo de seguridad reciba esta petición, adelante la petición al servidor Web y extrae simultáneamente el URL y envía una petición de las operaciones de búsqueda al servidor del Filtrado de URL.

3. Después de que el servidor del Filtrado de URL reciba la petición de las operaciones de búsqueda, marca su base de datos para determinar si al permit or deny el URL. Vuelve un estatus del permit or deny con una respuesta de las operaciones de búsqueda al Firewall de Cisco IOS®.
4. El dispositivo de seguridad recibe esta respuesta de las operaciones de búsqueda y realiza una de estas funciones:Si la respuesta de las operaciones de búsqueda permite el URL, envía el HTTP de respuesta al usuario final.Si la respuesta de las operaciones de búsqueda niega el URL, el servidor del Filtrado de URL reorienta al usuario a su propio servidor Web interno, que visualiza un mensaje que describa la categoría bajo la cual se bloquea el URL. Después de eso, la conexión se reajusta en los ambos extremos.

Identifique al servidor de filtrado

Usted necesita identificar el direccionamiento del servidor de filtrado con el comando del URL-**servidor**. Usted debe utilizar la forma apropiada de este comando basado en el tipo de servidor de filtrado que usted utiliza.

Nota: Para la versión de software 7.x y posterior, usted puede identificar a hasta cuatro servidores de filtrado para cada contexto. El dispositivo de seguridad utiliza los servidores en la orden hasta que responda un servidor. Usted puede configurar solamente un tipo único de servidor, Websense o N2H2, en su configuración.

Websense

El Websense es un software de filtración de tercera persona que puede filtrar los pedidos de HTTP en base de estas directivas:

- nombre del host de destino
- IP Address de destino
- palabras claves
- Nombre de usuario

El software mantiene una base de datos URL de más de 20 millones de sitios ordenados en más de 60 categorías y subcategorías.

- Versión de software 6.2:
  `url-server [(if_name)] vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP} version]` El comando del URL-**servidor** señala el servidor que ejecuta la aplicación del Filtrado de URL N2H2 o del Websense. El límite es 16 servidores URL. Sin embargo, usted puede utilizar solamente un en un momento de la aplicación, N2H2 o Websense. Además, si usted cambia su configuración en el firewall PIX, no pone al día la configuración en el servidor de aplicaciones. Esto se debe hacer por separado, sobre la base de las instrucciones del vendedor individual.
- Versión de software 7.x y posterior:
  `pix(config)# url-server (if_name) host local_ip [timeout seconds] [protocol TCP | UDP version 1|4 [connections num_conns] ]`

`If_name del` reemplace con el nombre de la interfaz del dispositivo de seguridad que está conectada con el servidor de filtrado. El valor por defecto está dentro. Substituya el `local_ip` por la dirección IP del servidor de filtrado. `Segundos del` reemplace con el número de segundos que el dispositivo de seguridad debe continuar para intentar para conectar con el servidor de filtrado.

Utilice la opción del `protocolo` para especificar si usted quiere utilizar el TCP o el UDP. Con un servidor Websense, usted puede también especificar la `versión del` TCP que usted quiere utilizar. La versión de TCP 1 es el valor por defecto. La versión de TCP 4 permite que el firewall PIX envíe los nombres de usuario autenticado y la información de ingreso al sistema URL al servidor Websense si el firewall PIX ha autenticado ya al usuario.

Por ejemplo, para identificar a un solo servidor de filtrado del Websense, publique este comando:

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

Asegure SmartFilter computacional

- Versión de PIX 6.2:`pix(config)#`**`url-server [(if_name)] vendor n2h2 host local_ip[:port number] [timeout <seconds>] [protocol TCP | UDP]`**
- Versiones de software 7.0 y 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]]`**
- Versión de software 7.2 y posterior:`hostname(config)#`**`url-server (if_name) vendor {secure-computing | n2h2} host <local_ip> [port <number>] [timeout <seconds>] [protocol {TCP [connections <number>]} | UDP]`** Para el `vendedor {seguro-que computa | n2h2}`, usted puede utilizar la seguro-`computación` como cadena del vendedor. Sin embargo, `n2h2` es aceptable para la compatibilidad descendente. Cuando las entradas de configuración se generan, seguro-`computando` se guarda como la cadena del vendedor.

`If_name del` reemplace con el nombre de la interfaz del dispositivo de seguridad que está conectada con el servidor de filtrado. El valor por defecto está dentro. Substituya el `local_ip` por la dirección IP del servidor de filtrado y `vire el <number> hacia el lado de babor` con el número del puerto deseado.

Nota: El puerto predeterminado usado por el servidor computacional seguro de SmartFilter para comunicar con el dispositivo de seguridad con el TCP o el UDP es el puerto 4005.

`Segundos del` reemplace con el número de segundos que el dispositivo de seguridad debe continuar para intentar para conectar con el servidor de filtrado. Utilice la opción del `protocolo` para especificar si usted quiere utilizar el TCP o el UDP.

`El <number> de las conexiones` es la cantidad de veces a intentar hacer una conexión entre el host y el servidor.

Por ejemplo, para identificar a un solo servidor de filtrado N2H2, publique este comando:

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

O, si usted quiere utilizar los valores predeterminados, publicar este comando:

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

Configure la política de filtrado

Nota: Usted debe identificar y habilitar el servidor del Filtrado de URL antes de que usted habilite el Filtrado de URL.

Filtrado de URL del permiso

Cuando el servidor de filtrado aprueba una petición de conexión HTTP, el dispositivo de seguridad permite que la contestación del servidor Web alcance al cliente que originó la petición. Si el servidor de filtrado niega la petición, el dispositivo de seguridad reorienta al usuario a una página del bloque que indique que el acceso está negado.

Publique el **comando url del filtro** para configurar la directiva usada para filtrar los URL:

- Versión de PIX 6.2:
  filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]
- Versión de software 7.x y posterior:
  filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]

`Puerto del` reemplace con el número del puerto en el cual para filtrar el tráfico HTTP si un diverso puerto que el puerto predeterminado para HTTP (80) se utiliza. Para identificar los números de un rango de puertos, ingrese el comienzo y el extremo del rango separado por un guión.

Con la filtración habilitada, el dispositivo de seguridad para el tráfico HTTP saliente hasta que un servidor de filtrado permita la conexión. Si no responde el servidor de filtrado primario, el dispositivo de seguridad dirige la petición de filtración al servidor de filtrado secundario. La opción de la `permit` hace el dispositivo de seguridad remitir el tráfico HTTP sin la filtración cuando el servidor de filtrado primario es inasequible.

Publique el comando del proxy-**bloque** para caer todas las peticiones a los servidores proxy.

Nota: El resto de los parámetros se utiliza para truncar los URL largos.

HTTP largo truncado URL

La opción longurl-`truncada` hace el dispositivo de seguridad enviar solamente el nombre del host o la porción de la dirección IP del URL para la evaluación al servidor de filtrado cuando el URL es más largo que el Largo máximo permitido.

Utilice la opción de la longurl-`negación` para negar el tráfico saliente URL si el URL es más largo que el máximo permitido.

Utilice la opción CGI-`truncada` para truncar CGI URL para incluir solamente la ubicación de la secuencia de comandos CGI y el nombre de secuencia de comandos sin ningunos parámetros.

Esto es un ejemplo general de la configuración de 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
```

Tráfico exento de la filtración

Si usted quiere hacer una excepción a la política de filtrado general, publique este comando:

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

Substituya el `local_ip` y el `local_mask` por la dirección IP y la máscara de subred de un usuario o de un red secundario que usted quiera eximir de las restricciones de filtración.

Substituya el `foreign_ip` y el `foreign_mask` por la dirección IP y la máscara de subred de un servidor

o de un red secundario que usted quiera eximir de las restricciones de filtración.

Por ejemplo, este comando causa todos los pedidos de HTTP a 172.30.21.99, de los host interiores, de ser remitido al servidor de filtrado a excepción de las peticiones del host 192.168.5.5:

Esto es un ejemplo de configuración para una excepción:

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

Filtrado de URL avanzado

Esta sección proporciona la información sobre los parámetros de filtración avanzados, que incluye estos temas:

- el mitigar
- almacenamiento en memoria inmediata
- soporte largo URL

Mitigue las respuestas del servidor Web

Cuando un usuario publica una petición de conectar con un servidor contento, el dispositivo de seguridad envía la petición al servidor contento y al servidor de filtrado al mismo tiempo. Si no responde el servidor de filtrado antes de que se caiga el servidor contento, la respuesta del servidor. Esto retrasa la respuesta del servidor Web desde el punto de vista del cliente de Web porque el cliente debe reeditar la petición.

Si usted habilita el buffer del HTTP de respuesta, las contestaciones de los servidores del contenido de la Web están mitigadas y las respuestas se remiten al cliente que hace la petición si el servidor de filtrado permite la conexión. Esto previene el retardo que puede ocurrir de otra manera.

Para mitigar las respuestas a los pedidos de HTTP, complete estos pasos:

1. Para habilitar mitigar de las respuestas para los pedidos de HTTP que están hasta que finalice una respuesta del servidor de filtrado, publique este comando:`hostname(config)#`**`url-block block block-buffer-limit`** Substituya el bloque-buffer-`límite` por el número máximo de bloques que se mitigarán.
2. Para configurar memoria máxima disponible para mitigar hasta que finalicen los URL, y para mitigar los URL largos con el Websense, publica este comando:`hostname(config)#`**`url-block url-mempool memory-pool-size`** Substituya el memoria-pool-`tamaño` por un valor a partir del 2 a 10240 para una asignación de memoria máxima de 2 KB al 10 MB.

Direccionamientos del servidor caché

Después del los accesos del usuario un sitio, el servidor de filtrado pueden permitir que el dispositivo de seguridad oculte a la dirección del servidor por una determinada cantidad de hora, mientras cada sitio recibido en el direccionamiento esté en una categoría que se permita siempre. Entonces, cuando los accesos del usuario el servidor otra vez, o si otros accesos del usuario el servidor, el dispositivo de seguridad no necesitan consultar al servidor de filtrado otra vez.

Publique el comando del URL-**caché** si es necesario de mejorar la producción:

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

Substituya el `tamaño` por un valor para el tamaño de la memoria caché dentro del rango 1 a 128 (KB).

Utilice la palabra clave del `dst` para ocultar las entradas basadas en la dirección destino URL. Seleccione este modo si todos los usuarios comparten la misma directiva del Filtrado de URL en el servidor Websense.

Utilice la palabra clave del `src_dst` para ocultar las entradas basadas en ambos la dirección de origen que inicia la petición URL así como la dirección destino URL. Seleccione este modo si los usuarios no comparten la misma directiva del Filtrado de URL en el servidor Websense.

Habilite la filtración de los URL largos

Por abandono, el dispositivo de seguridad considera HTTP URL para ser un URL largo si es mayor de 1159 caracteres. Usted puede aumentar el Largo máximo permitido para un solo URL con este comando:

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

`Largo-URL-tamaño del` reemplace con el tamaño máximo en el KB para que cada URL largo sea mitigado.

Por ejemplo, estos comandos configure el dispositivo de seguridad para el Filtrado de URL avanzado:

```
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
```

Configuración

Esta configuración incluye los comandos descritos en este documento:

Configuración 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-
```

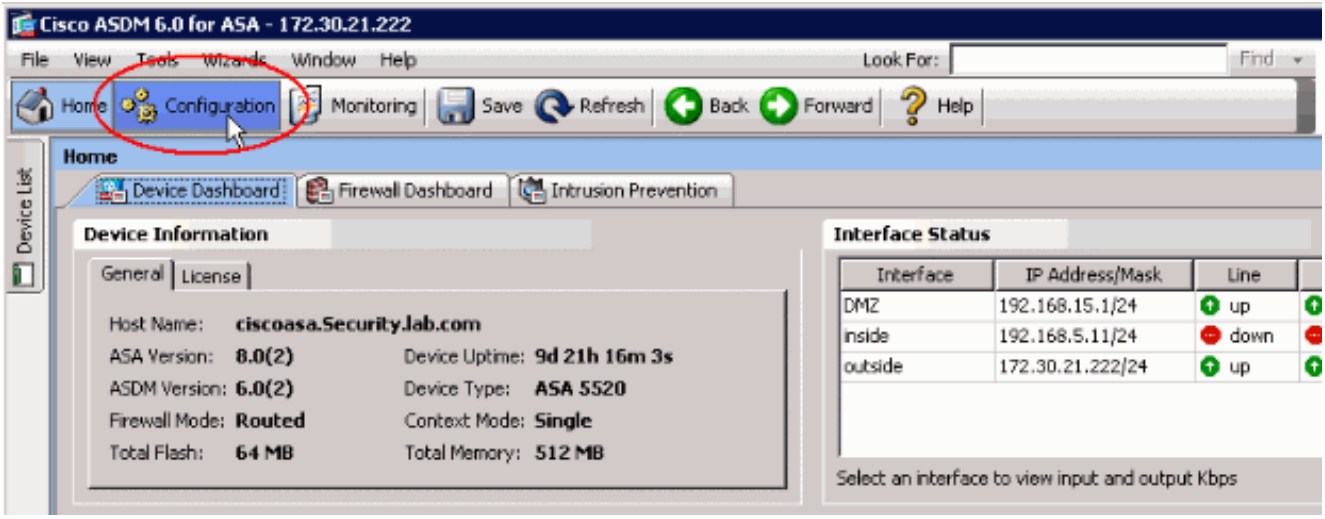
```
address aaa@cisco.com mtu outside 1500 mtu inside 1500
mtu DMZ 1500 no failover failover lan unit primary
failover lan interface interface GigabitEthernet0/2
failover link interface GigabitEthernet0/2 no monitor-
interface outside icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-602.bin 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
```

Configure ASA/PIX con el ASDM

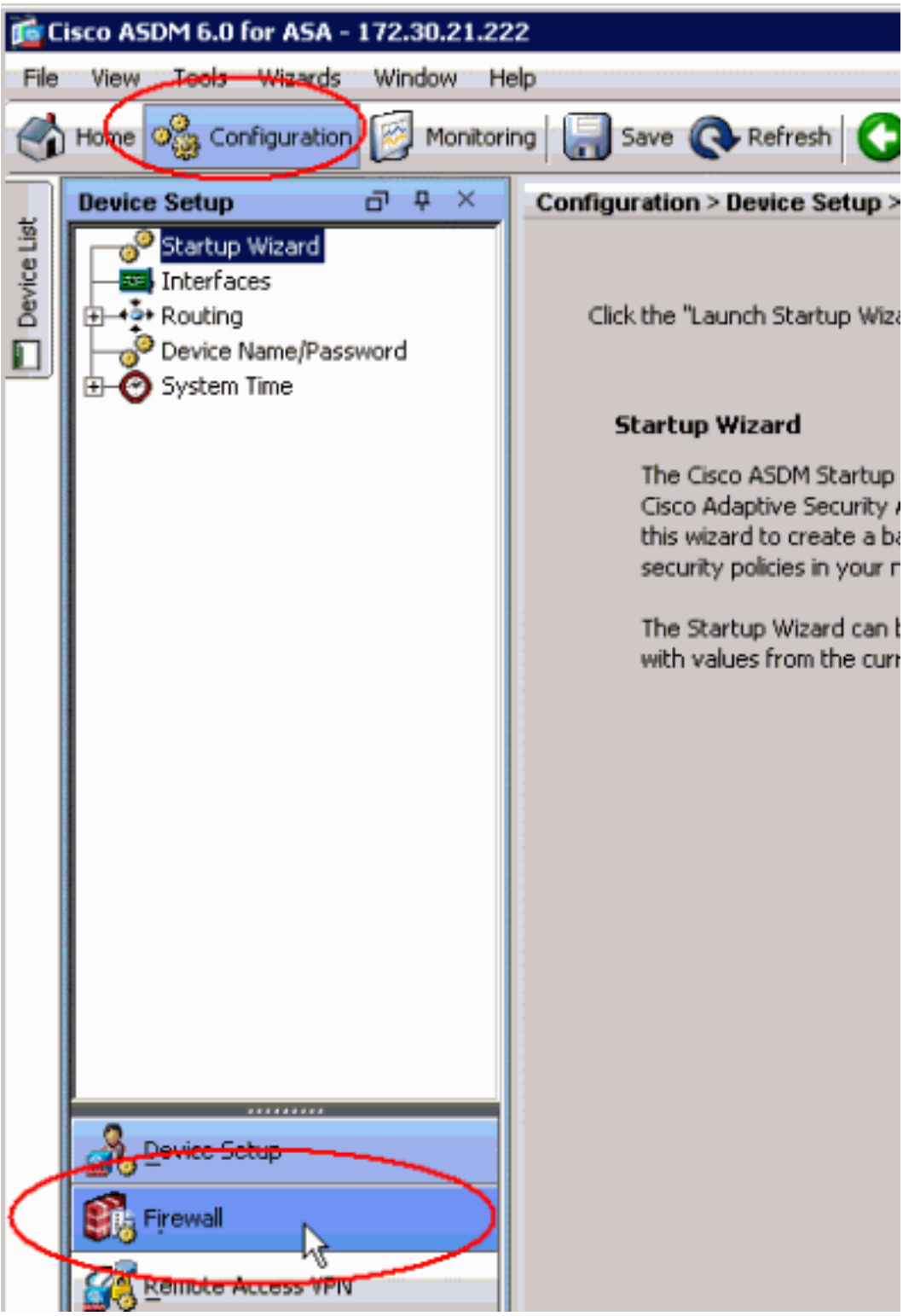
Esta sección demuestra cómo configurar el Filtrado de URL para el dispositivo de seguridad con el Administrador de dispositivos de seguridad adaptante (ASDM).

Después de que usted inicie el ASDM, complete estos pasos:

1. Elija el cristal de la **configuración**.

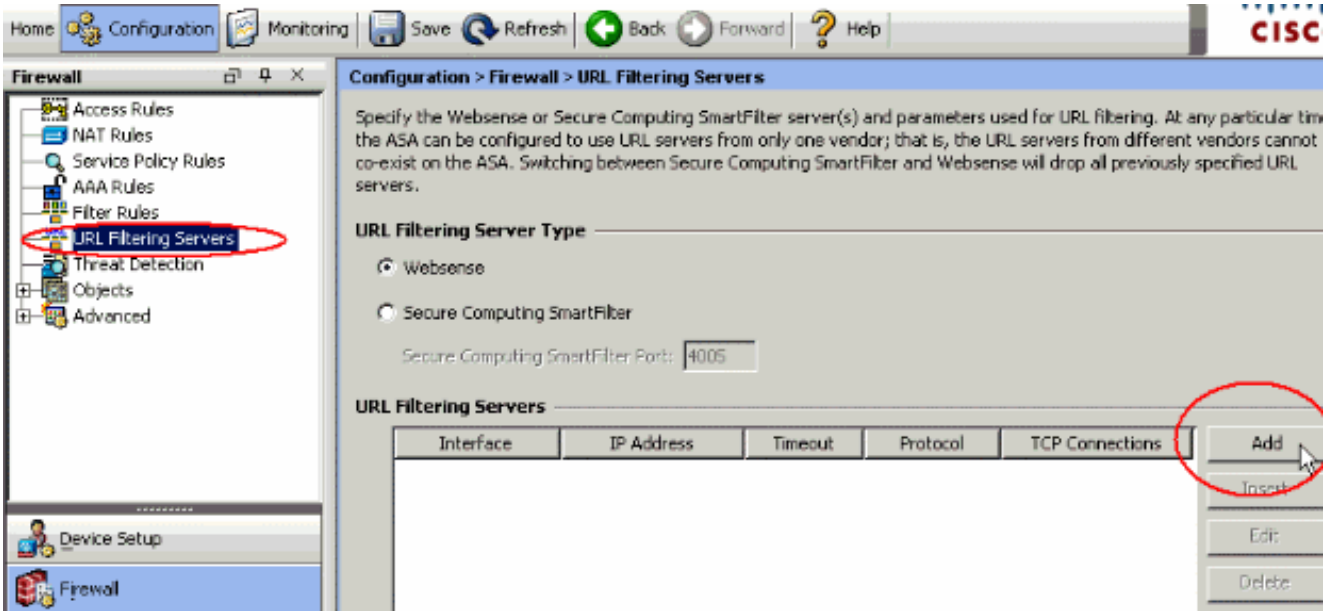


2. Haga clic el **Firewall** en la lista mostrada en el cristal de la

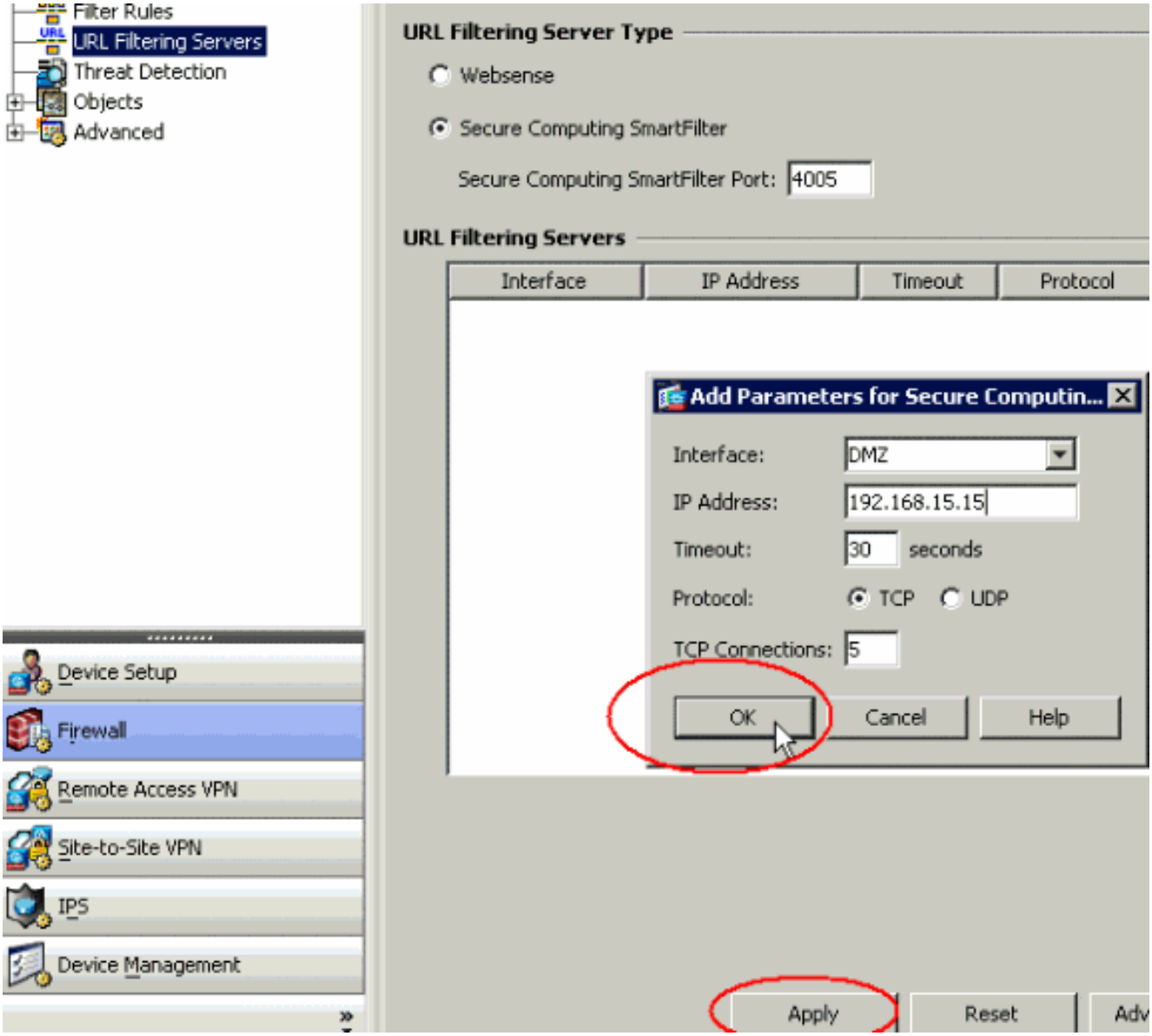


configuración.

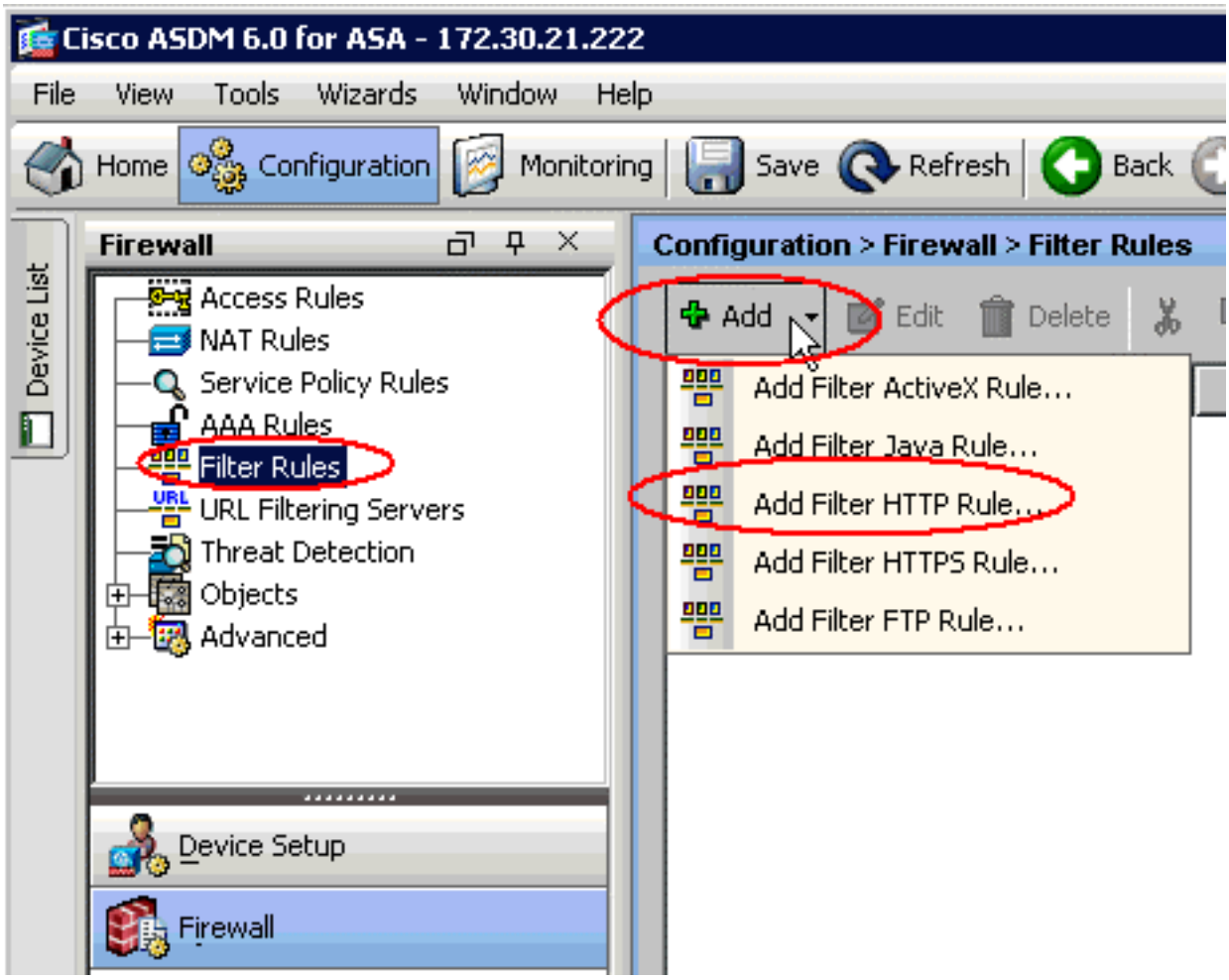
3. De la lista desplegable del **Firewall**, elija los **servidores del Filtrado de URL**. Elija el tipo de servidor del Filtrado de URL que usted quiere utilizar, y el tecleo **agrega** para configurar sus parámetros.**Nota:** Usted debe agregar al servidor de filtrado antes de que usted pueda configurar la filtración para las reglas para filtros HTTP, HTTPS, o FTP.



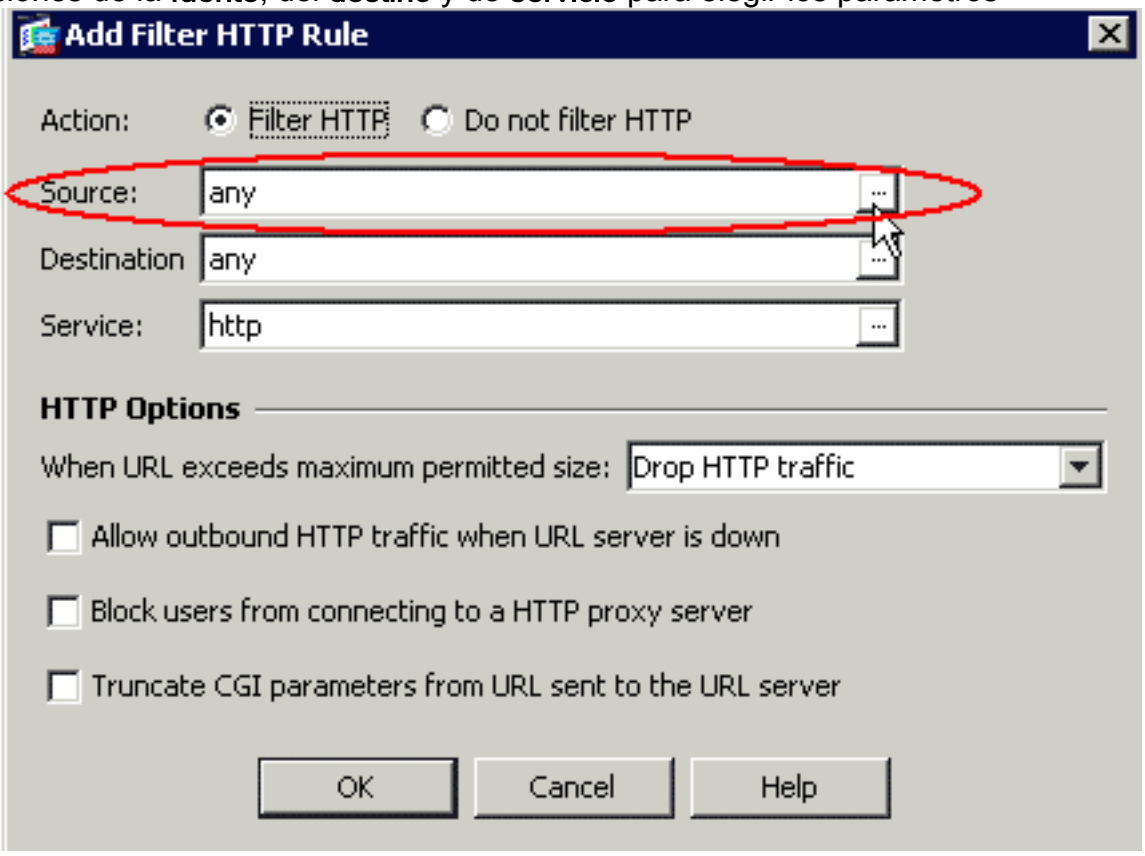
4. Elija los parámetros apropiados en la ventana emergente:Interfaz — Visualiza la interfaz conectada con el servidor de filtradoDirección IP — Visualiza la dirección IP del servidor de filtradoDescanso — Visualiza el número de segundos después de lo cual la petición a los tiempos del servidor de filtrado hacia fueraProtocolo — Visualiza el protocolo usado para comunicar con el servidor de filtrado. La versión de TCP 1 es el valor por defecto. La versión de TCP 4 permite que el firewall PIX envíe los nombres de usuario autenticado y la información de ingreso al sistema URL al servidor Websense, si el firewall PIX ha autenticado ya al usuarioConexiones TCP — Visualiza el número máximo de conexiones TCP permitidas comunicar con el servidor del Filtrado de URLDespués de que usted ingrese los parámetros, haga clic la **AUTORIZACIÓN** en la ventana emergente y **apliqúese** en la ventana
principal.



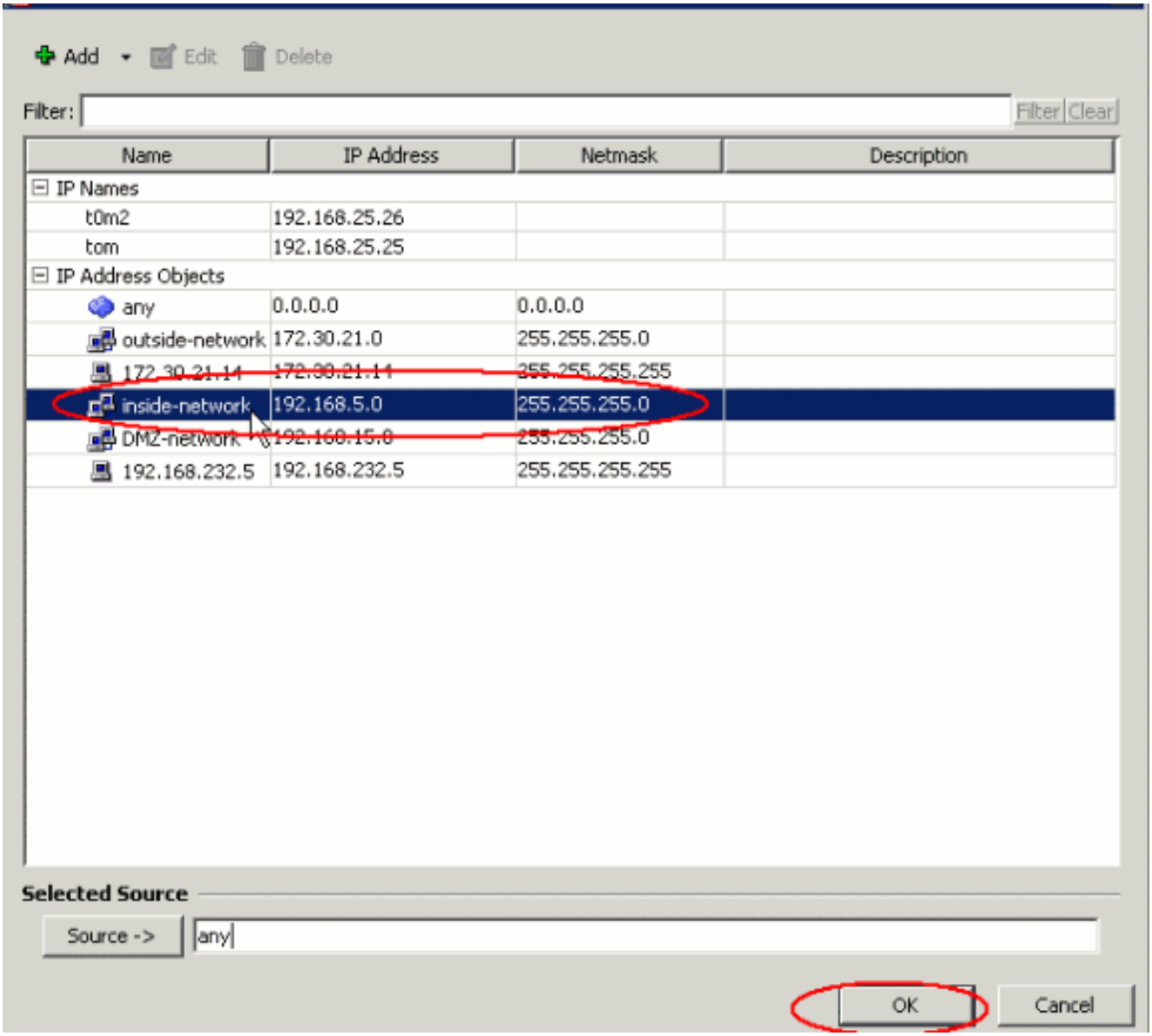
5. De la lista desplegable del **Firewall**, elija las **reglas para filtros**. Haga clic el **botón Add** en la ventana principal, y elija el tipo de regla que usted quiere agregar. En este ejemplo, se elige la **regla del filtro HTTP del agregar**.



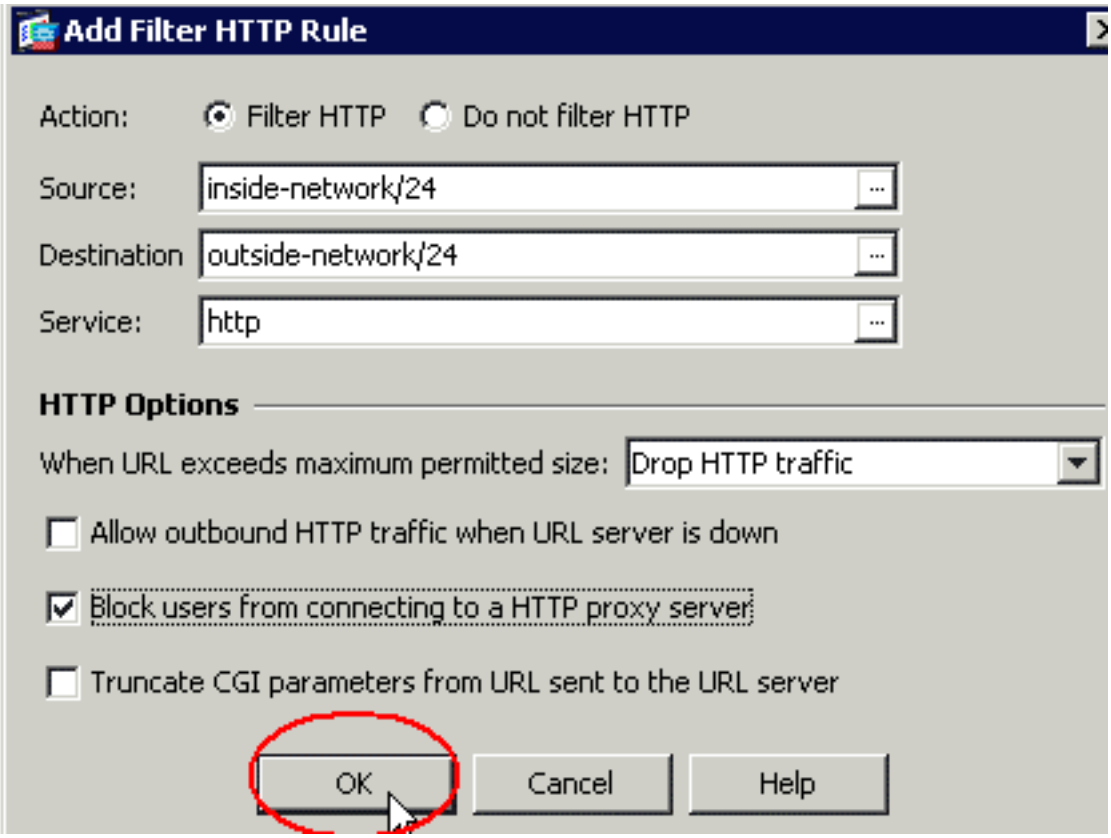
6. Una vez que aparece la ventana emergente, usted puede hacer clic en los botones Browse para las opciones de la **fuente**, del **destino** y de **servicio** para elegir los parámetros apropiados.



7. Esto muestra la ventana de la ojeada para la opción de la **fuente**. Haga su selección y haga clic la **AUTORIZACIÓN**.

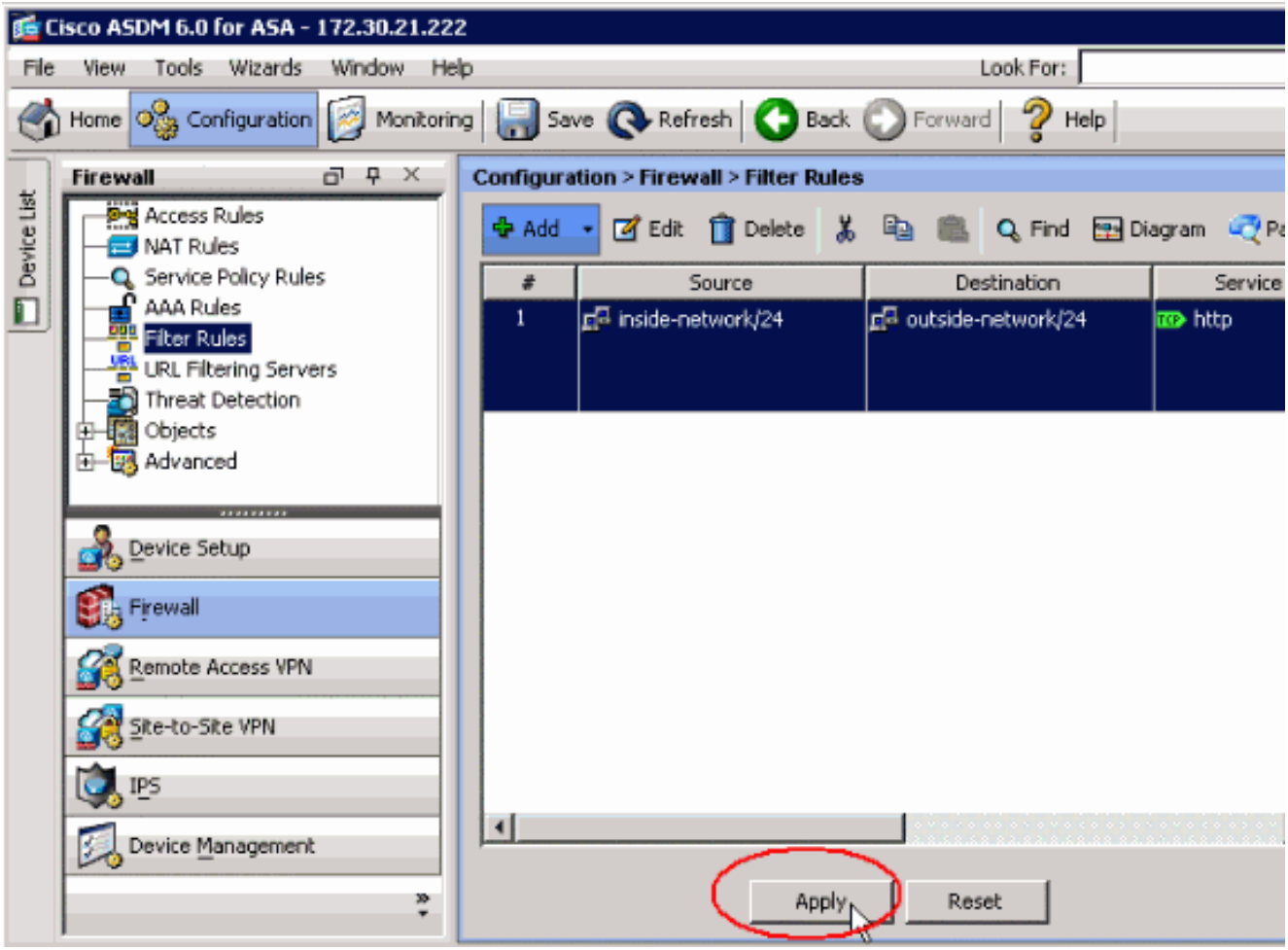


8. Después de que usted complete la selección para todos los parámetros, haga clic la **AUTORIZACIÓN** para

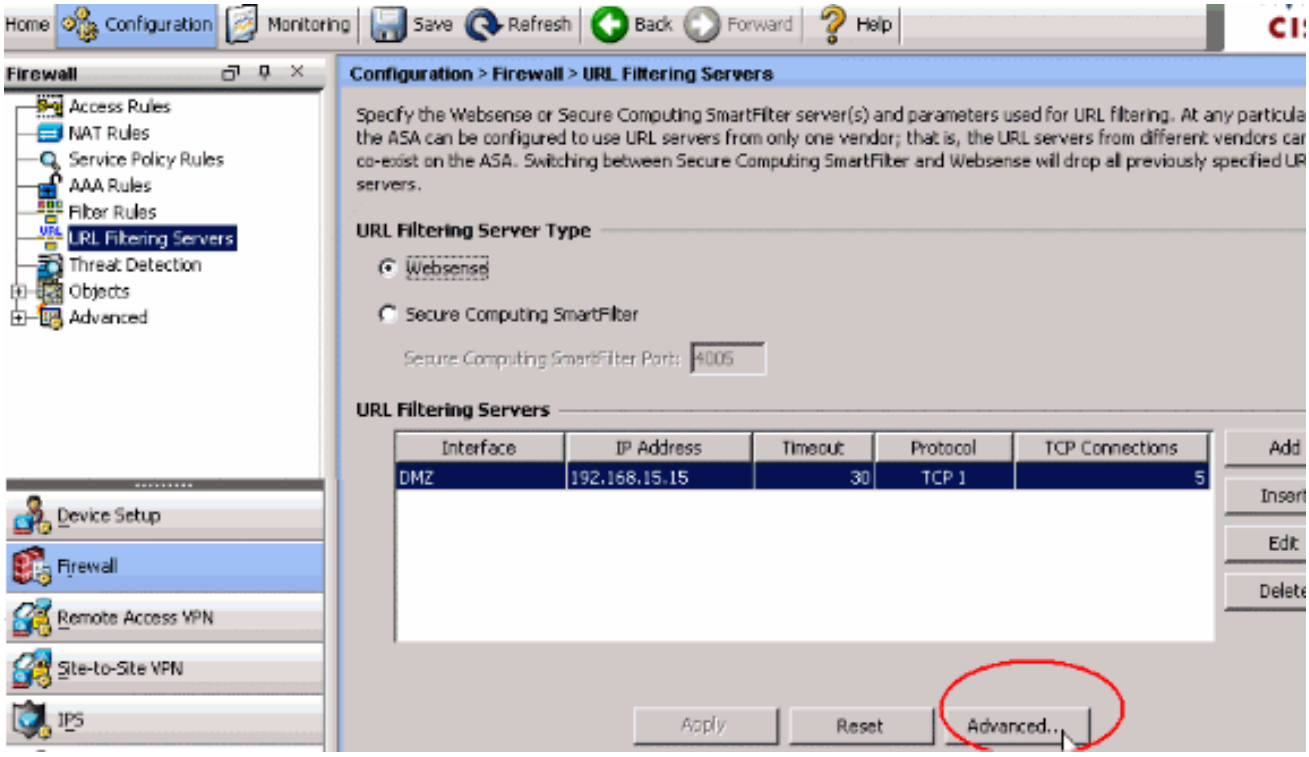


continuar.

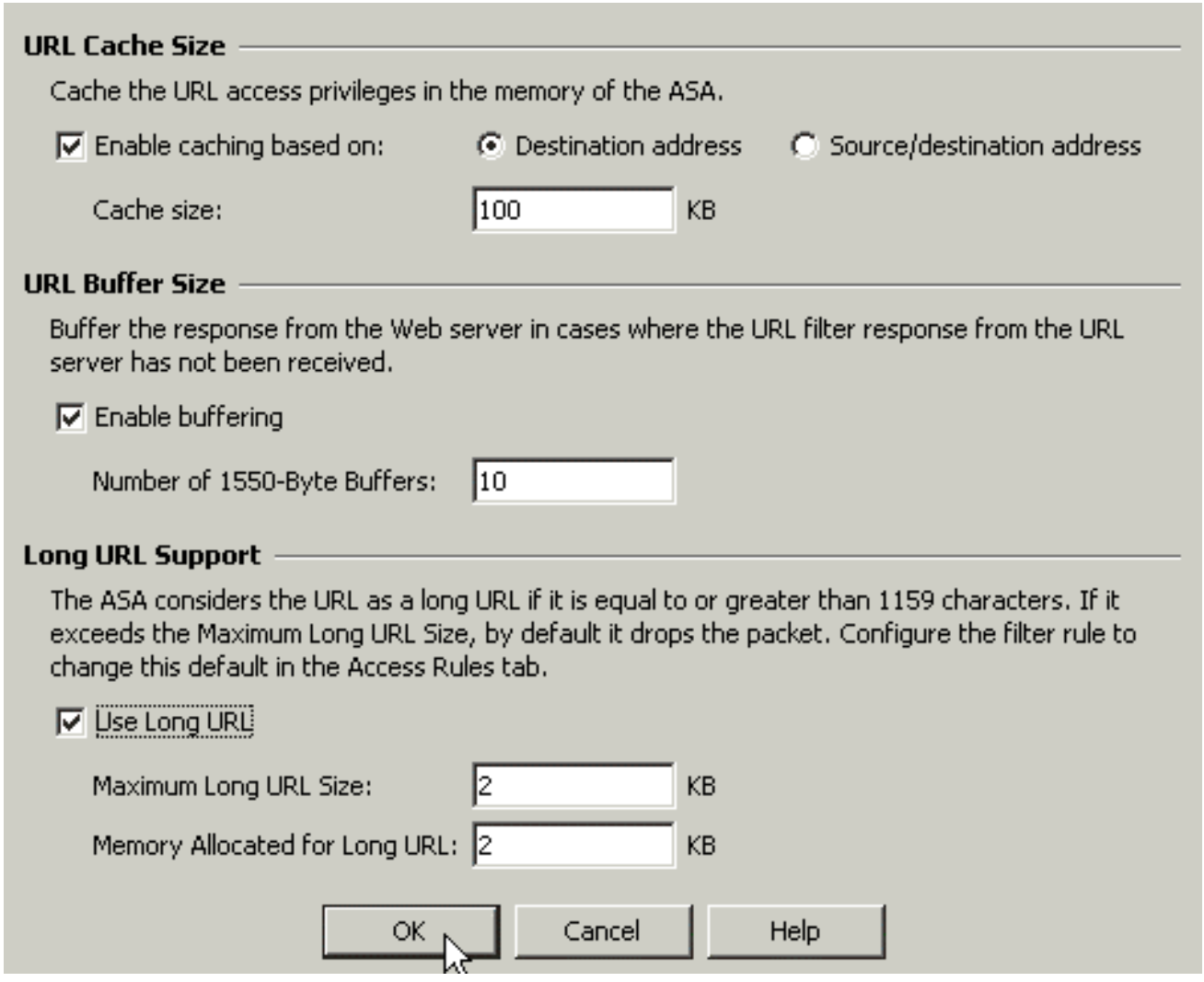
9. Una vez que se configuran los parámetros apropiados, el tecleo **se aplica** para someter los cambios.



10. Para las opciones avanzadas del Filtrado de URL, elija los **servidores del Filtrado de URL** otra vez del menú desplegable del **Firewall**, y haga clic el **botón Advanced** en la ventana principal.



11. Configure los parámetros, tales como tamaño de la memoria caché URL, tamaño de almacén intermedio URL y soporte largo URL, en la ventana emergente. El Haga Click en OK en la ventana emergente, y el tecleo **se aplican** en la ventana principal para continuar.



12. Finalmente, aseegurese que usted salva los cambios que usted realiza antes de que usted

termine a la sesión ASDM.

Verificación

Utilice los comandos en esta sección para ver la información del Filtrado de URL. Usted puede utilizar estos comandos para verificar su configuración.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

- **URL-servidor de la demostración** — Muestra la información sobre el servidor de filtradoPor ejemplo:`hostname#`**`show url-server`** `url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp connections 10` En la versión de software 7.2 y posterior, publique la forma del URL-**servidor de los ejecutar-config de la demostración de** este comando.
- **muestre el stats del URL-servidor** — Demostraciones información y estadísticas sobre el servidor de filtradoPara la versión de software 7.2, publique las **estadísticas del URL-servidor de los ejecutar-config de la demostración** forman de este comando.En la versión de software 8.0 y posterior, publique las **estadísticas del URL-servidor de la demostración** forman de este comando.Por ejemplo:`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`
- **URL-bloque de la demostración** — Muestra la configuración del buffer del bloque URLPor ejemplo:`hostname#`**`show url-block`** `url-block url-mempool 128 url-block url-size 4 url-block block 128` En la versión de software 7.2 y posterior, publique la forma del URL-**bloque de los ejecutar-config de la demostración de** este comando.
- **muestre las estadísticas del bloque del URL-bloque** — Muestra las estadísticas del bloque URLPor ejemplo:`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` Para la versión de software 7.2, publique las **estadísticas del bloque del URL-bloque de los ejecutar-config de la demostración** forman de este comando.
- **muestre el stats del URL-caché** — Muestra cómo se utiliza el cachéPor ejemplo:`hostname#`**`show url-cache stats`** `URL Filter Cache Stats ---------- Size : 128KB Entries : 1724 In Use : 456 Lookups : 45 Hits : 8` En la versión de software 8.0, publique las **estadísticas del URL-caché de la demostración** forman de este comando.
- **perfmon de la demostración** — Estadísticas de rendimiento del Filtrado de URL de las demostraciones, junto con otras estadísticas de rendimiento. Las estadísticas de filtración se muestran en las filas del req del acceso URL y del servidor URL.Por ejemplo:`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
```

- **filtro de la demostración** — Muestra la configuración de filtraciónPor ejemplo:`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` En la versión de software 7.2 y posterior, publique la forma del **filtro de los ejecutar-config de la demostración de** este comando.

Troubleshooting

Esta sección proporciona la información sobre cómo resolver problemas su configuración.

Error: "%ASA-3-304009: Se ejecutó de los bloques del buffer especificados por el comando del URL-bloque"

El Firewall se ejecuta fuera del caché URL que se significa para llevar a cabo las contestaciones del servidor cuando el Firewall espera para conseguir la confirmación del servidor URL.

Solución

El problema se relaciona básicamente con un tiempo de espera entre el ASA y el servidor Websense. Para resolver este intento del problema estas soluciones alternativas.

- Intente cambiar el protocolo que se utiliza en el ASA al UDP para comunicar con el Websense.Hay un problema con el tiempo de espera entre el servidor Websense y el Firewall, en quienes las contestaciones del servidor Websense tardan un tiempo prolongado para volver al Firewall, así ésta hace el buffer URL llenarse mientras que espera una respuesta.Usted puede utilizar el UDP en vez del TCP para la comunicación entre el servidor Websense y el Firewall. Esto es porque cuando usted utiliza el TCP para el Filtrado de URL, para cada nueva petición URL, el ASA necesita establecer una conexión TCP con el servidor Websense. Puesto que el UDP es un protocolo sin conexión, el ASA no se fuerza a establecer la conexión para recibir la respuesta del servidor. Esto debe mejorar el funcionamiento del servidor.`ASA(config)#`**`url-server (inside) vendor websense host X.X.X.X timeout 30`**` protocol UDP version 4 connections 5`
- Aseegurese aumentar el bloque del URL-bloque al valor más alto posible, que es 128. Esto se puede marcar con el comando del URL-**bloque de la demostración**.Si muestra el 128, tome la mejora del Id. de bug Cisco CSCta27415 (clientes registrados solamente) en la consideración.

Información Relacionada

- Soporte de producto para dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Soporte de productos del Dispositivos de seguridad Cisco PIX de la serie 500
- Soporte de Productos de Cisco Adaptive Security Device Manager
- PIX/ASA: Establezca y resuelva problemas la Conectividad a través del dispositivo del Cisco Security
- Resuelva problemas las conexiones con el PIX y el ASA
- Soporte Técnico y Documentación - Cisco Systems