Exemplo de configuração da Filtragem URL PIX/ASA

Índice

Introdução

Este documento explica como configurar a Filtragem URL em uma ferramenta de segurança.

Ao filtrar tráfego tem estas vantagens:

- Pode ajudar a reduzir riscos de segurança e impedir o uso impróprio.
- Pode fornecer o maior controle sobre o tráfego que passa através da ferramenta de segurança.

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

Nota: O implementar que filtra de um mais baixo nível de segurança a mais altamente não é apoiado. A Filtragem URL trabalha somente para o tráfego de saída, por exemplo, o tráfego que origina em uma relação da segurança elevada destinada para um server em uma baixa interface de segurança.

Pré-requisitos

Componentes Utilizados

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

- Ferramenta de segurança da série PIX 500 com versão 6.2 e mais recente
- Ferramenta de segurança do 5500 Series ASA com versão 7.x e mais recente
- Security Device Manager adaptável (ASDM) 6.0

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

Convenções

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

Informações de Apoio

Você pode filtrar os pedidos de conexão que originam de uma rede mais segura a uma rede menos segura. Embora você possa usar o Access Control Lists (ACLs) a fim impedir o acesso externo aos server satisfeitos específicos, é difícil controlar o uso esta maneira devido ao tamanho e à natureza dinâmica do Internet. Você pode simplificar a configuração e melhorar o desempenho da ferramenta de segurança com o uso de um servidor separado que execute um deste Produtos de filtração do Internet:

- Empresa de Websense — filtros HTTP, HTTPS, e FTP. É apoiada pela versão 5.3 e mais recente do PIX Firewall.
- Fixe SmartFilter de computação, conhecido anteriormente como o N2H2 — filtros HTTP, HTTPS, FTP, e Filtragem URL longa. É apoiado pela versão 6.2 e mais recente do PIX Firewall.

Comparado ao uso das listas de controle de acesso, isto reduz as tarefas administrativas e melhora a eficácia de filtração. Também, porque a Filtragem URL é segurada em uma plataforma separada, o desempenho do PIX Firewall é muito menos afetado. Contudo, os usuários podem observar um tempo de acesso mais longo aos Web site ou aos servidores FTP quando o servidor de filtragem é remoto da ferramenta de segurança.

O PIX Firewall verifica pedidos de partida URL com a política definida no server da Filtragem URL. O PIX Firewall permite ou nega a conexão, com base na resposta do servidor de filtragem.

Quando filtrar é permitida e um pedido para o índice está dirigido através da ferramenta de segurança, o pedido está enviado ao server satisfeito e ao servidor de filtragem ao mesmo tempo. Se o servidor de filtragem permite a conexão, a ferramenta de segurança para a frente a resposta do server satisfeito ao cliente que originou o pedido. Se o servidor de filtragem nega a conexão, a ferramenta de segurança deixa cair a resposta e envia uma mensagem ou um código de retorno que indique que a conexão não é bem sucedida.

Se a autenticação de usuário é permitida na ferramenta de segurança, a ferramenta de segurança igualmente envia o nome de usuário ao servidor de filtragem. O servidor de filtragem pode usar ajustes de filtração específicas de usuário ou fornecer relatórios aumentados no que diz respeito ao uso.

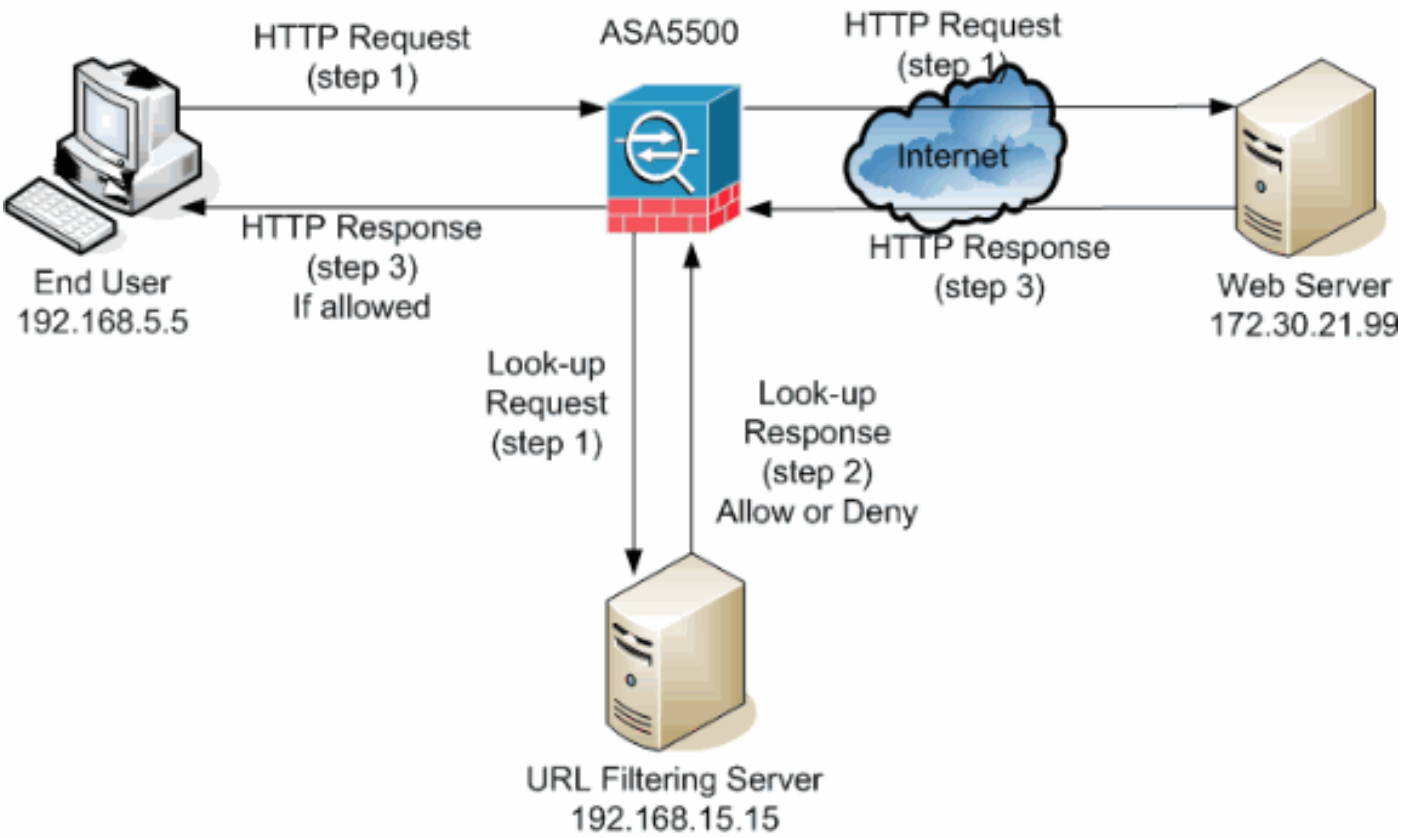
Configurar o ASA/PIX com o CLI

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

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



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

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

1. O utilizador final consulta a uma página no servidor de Web, e o navegador envia um pedido do HTTP.
2. Depois que a ferramenta de segurança recebe este pedido, para a frente o pedido ao servidor de Web e extrai simultaneamente a URL e envia um pedido da consulta ao server da Filtragem URL.

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

Identifique o servidor de filtragem

Você precisa de identificar o endereço do servidor de filtragem com o comando do URL-**server**. Você deve usar o formulário apropriado deste comando baseado no tipo de servidor de filtragem que você se usa.

Nota: Para a versão de software 7.x e mais tarde, você pode identificar até quatro servidores de filtragem para cada contexto. A ferramenta de segurança usa os server em ordem até que um server responda. Você pode somente configurar um único tipo de server, Websense ou N2H2, em sua configuração.

Websense

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

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

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

- Versão de software 6.2:
  `url-server [(if_name)] vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP} version]` O comando do URL-**server** designa o server que executa o aplicativo da Filtragem URL N2H2 ou de Websense. O limite é 16 server URL. Contudo, você pode usar somente um aplicativo de cada vez, N2H2 ou Websense. Adicionalmente, se você muda sua configuração no PIX Firewall, não atualiza a configuração no server de aplicativo. Isto deve ser feito separadamente, com base nas instruções do vendedor individual.
- Versão de software 7.x e mais tarde:
  `pix(config)# url-server (if_name) host local_ip [timeout seconds] [protocol TCP | UDP version 1|4 [connections num_conns] ]`

Substitua o `if_name` com o nome da relação da ferramenta de segurança que é conectada ao servidor de filtragem. O padrão está para dentro. Substitua o `local_ip` com o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de filtragem. Substitua `segundos` com o número de segundos onde a ferramenta de segurança deve continuar a tentar conectar ao servidor de filtragem.

Use a opção do `protocolo` a fim especificar se você quer usar o TCP ou o UDP. Com um servidor

websense, você pode igualmente especificar a `versão do` TCP que você quer se usar. A versão do TCP 1 é o padrão. A versão do TCP 4 permite que o PIX Firewall envie nomes de usuário autenticado e informação de registro URL ao servidor websense se o PIX Firewall tem autenticado já o usuário.

Por exemplo, a fim identificar um único servidor de filtragem de Websense, emita este comando:

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

Fixe SmartFilter de computação

- Versão de PIX 6.2:`pix(config)#` **`url-server [(if_name)] vendor n2h2 host local_ip[:port number] [timeout <seconds>] [protocol TCP | UDP]`**
- Versões de software 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]]`**
- Versão de software 7.2 e mais atrasado:`hostname(config)#` **`url-server (if_name) vendor {secure-computing | n2h2} host <local_ip> [port <number>] [timeout <seconds>] [protocol {TCP [connections <number>]} | UDP]`** Para o `vendedor {quecomputa | n2h2}`, você pode usar a seguro-`computação` como uma corda do vendedor. Contudo, `n2h2` é aceitável para a compatibilidade retrógrada. Quando as entradas de configuração são geradas, seguro-`computar` salvar como a corda do vendedor.

Substitua o `if_name` com o nome da relação da ferramenta de segurança que é conectada ao servidor de filtragem. O padrão está para dentro. Substitua o `local_ip` com o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de filtragem e o `<number> da porta` com o número de porta desejado.

Nota: A porta padrão usada pelo server de computação seguro de SmartFilter para comunicar-se com a ferramenta de segurança com TCP ou UDP é a porta 4005.

Substitua `segundos` com o número de segundos onde a ferramenta de segurança deve continuar a tentar conectar ao servidor de filtragem. Use a opção do `protocolo` a fim especificar se você quer usar o TCP ou o UDP.

`O <number> das conexões` é o número de vezes a tentar fazer uma conexão entre o host e o server.

Por exemplo, a fim identificar um único servidor de filtragem N2H2, emita este comando:

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

Ou, se você quer usar valores padrão, para emitir este comando:

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

Configurar a política de filtragem

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

Permita a Filtragem URL

Quando o servidor de filtragem aprova um pedido de conexão de HTTP, a ferramenta de segurança permite que a resposta do servidor de Web alcance o cliente que originou o pedido. Se

o servidor de filtragem nega o pedido, a ferramenta de segurança reorienta o usuário a uma página do bloco que indique que o acesso está negado.

Emita o **comando url do filtro** a fim configurar a política usada para filtrar URL:

- Versão 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]
- Versão de software 7.x e mais tarde:
  filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]

Substitua a `porta` com o número de porta em que para filtrar o tráfego de HTTP se uma porta diferente do que a porta padrão para HTTP (80) é usada. A fim identificar números de faixa de porta, incorporar o começo e a extremidade da escala separada por um hífen.

Com a filtração permitida, a ferramenta de segurança para o tráfego de HTTP de partida até que um servidor de filtragem permita a conexão. Se o servidor de filtragem preliminar não responde, a ferramenta de segurança dirige o pedido de filtração ao servidor de filtragem secundário. A opção `reservar` faz com que a ferramenta de segurança envie o tráfego de HTTP sem filtrar quando o servidor de filtragem preliminar é não disponível.

Emita o comando do proxy-**bloco** a fim deixar cair todos os pedidos aos servidores proxy.

Nota: O restante dos parâmetros é usado a fim truncar URL longas.

URL do HTTP longos truncados

A opção longurl-`truncada` faz com que a ferramenta de segurança envie somente o nome de host ou a parcela do endereço IP de Um ou Mais Servidores Cisco ICM NT da URL para a avaliação ao servidor de filtragem quando a URL é mais longa do que o comprimento máximo permitido.

Use a opção da longurl-`negação` a fim negar o tráfego de partida URL se a URL é mais longa do que o máximo permitido.

Use a opção CGI-`truncada` a fim truncar CGI URL para incluir somente o lugar do script CGI e o nome de script sem nenhuns parâmetros.

Este é um exemplo geral da configuração 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
```

Tráfego isento da filtração

Se você quer fazer uma exceção à política de filtragem geral, emita este comando:

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

Substitua o `local_ip` e o `local_mask` com o endereço IP de Um ou Mais Servidores Cisco ICM NT e a máscara de sub-rede de um usuário ou de uma sub-rede que você queira isentar das limitações de filtração.

Substitua o `foreign_ip` e o `foreign_mask` com o endereço IP de Um ou Mais Servidores Cisco ICM NT e a máscara de sub-rede de um server ou de uma sub-rede que você queira isentar das

limitações de filtração.

Por exemplo, este comando causa todos os pedidos do HTTP a 172.30.21.99, dos host internos, ser enviado ao servidor de filtragem à exceção dos pedidos do host 192.168.5.5:

Este é um exemplo de configuração para uma exceção:

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

Filtragem URL avançada

Esta seção fornece a informação sobre parâmetros de filtração avançados, que inclui estes assuntos:

- proteção
- pôr em esconderijo
- apoio longo URL

Proteja as respostas do servidor de Web

Quando um usuário emite um pedido conectar a um server satisfeito, a ferramenta de segurança envia o pedido ao server satisfeito e ao servidor de filtragem ao mesmo tempo. Se o servidor de filtragem não responde antes do server satisfeito, a resposta de servidor está deixada cair. Isto atrasa a resposta do servidor de Web do ponto de vista do cliente web porque o cliente deve reeditar o pedido.

Se você permite o buffer da resposta HTTP, as respostas dos server do conteúdo da Web estão protegidas e as respostas são enviadas ao cliente que faz o pedido se o servidor de filtragem permite a conexão. Isto impede o atraso que pode de outra maneira ocorrer.

A fim proteger respostas aos pedidos do HTTP, termine estas etapas:

1. A fim permitir a proteção das respostas para os pedidos do HTTP que são durante uma resposta do servidor de filtragem, emita este comando:`hostname(config)#`**`url-block block block-buffer-limit`** Substitua o bloco-buffer-`limite` com o número máximo de blocos a ser protegidos.
2. A fim configurar a memória máxima disponível para proteger durante URL, e para proteger URL longas com Websense, emite este comando:`hostname(config)#`**`url-block url-mempool memory-pool-size`** Substitua o memória-pool-`tamanho` com um valor de 2 a 10240 para uma atribuição de memória máxima de 2 KB ao 10 MB.

Endereços do servidor em cache

Após os acessos de usuário um local, o servidor de filtragem podem permitir que a ferramenta de segurança ponha em esconderijo o endereço do servidor para uma certa quantidade de tempo, enquanto cada local hospedado no endereço está em uma categoria que esteja permitida em todas as vezes. Então, quando os acessos de usuário o server outra vez, ou se uns outros acessos de usuário o server, a ferramenta de segurança não precisam de consultar outra vez o servidor de filtragem.

Emita o comando do URL-**esconderijo** se necessário para melhorar a taxa de transferência:

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

Substitua o `tamanho` com um valor para o tamanho de cache dentro da escala 1 a 128 (KB).

Use as entradas de cache da palavra-chave do `dst` baseadas no endereço de destino URL. Selecione este modo se todos os usuários compartilham da mesma política da Filtragem URL no servidor websense.

Use as entradas de cache da palavra-chave do `src_dst` baseadas em ambos o endereço de origem que inicia o pedido URL assim como o endereço de destino URL. Selecione este modo se os usuários não compartilham da mesma política da Filtragem URL no servidor websense.

Permita a filtração de URL longas

Àrevelia, a ferramenta de segurança considera um URL DO HTTP ser uma URL longa se é maior de 1159 caráteres. Você pode aumentar o comprimento máximo reservado para uma única URL com este comando:

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

Substitua o longo-URL-`tamanho` com o tamanho máximo no KB para que cada URL longa seja protegida.

Por exemplo, estes comandos configure a ferramenta de segurança para Filtragem URL avançada:

```
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
```

Configuração

Esta configuração inclui os comandos descritos neste documento:

Configuração 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
```

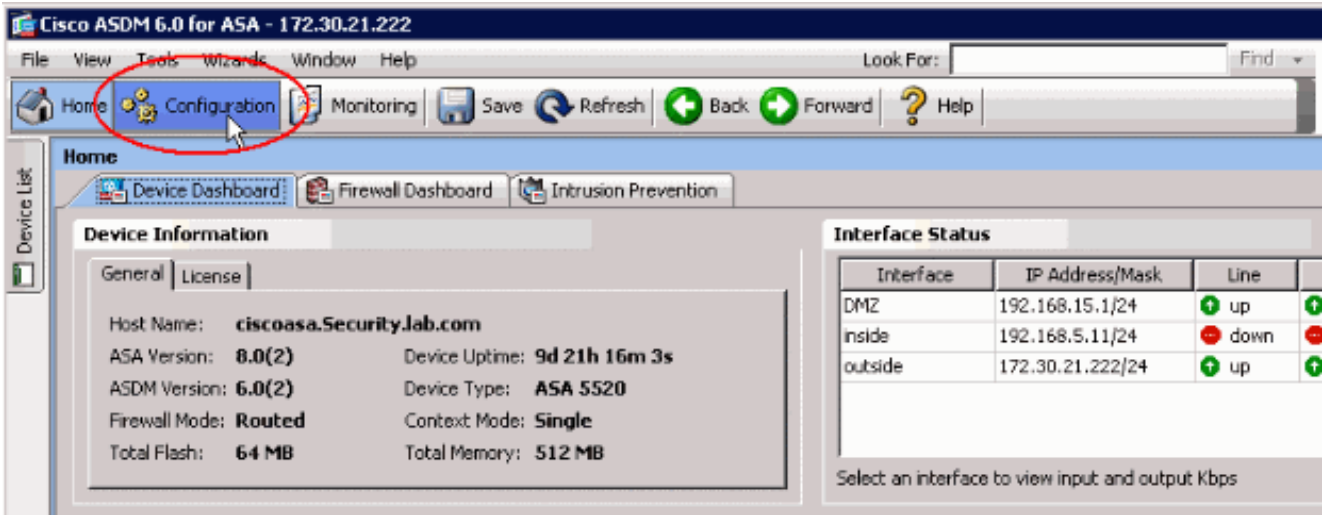
```
failover link interface GigabitEthernet0/2 no monitor-
interface outside icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-602.bin asdm history
enable arp timeout 14400 global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0
0.0.0.0 172.30.21.244 1 timeout 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
```

Configurar o ASA/PIX com ASDM

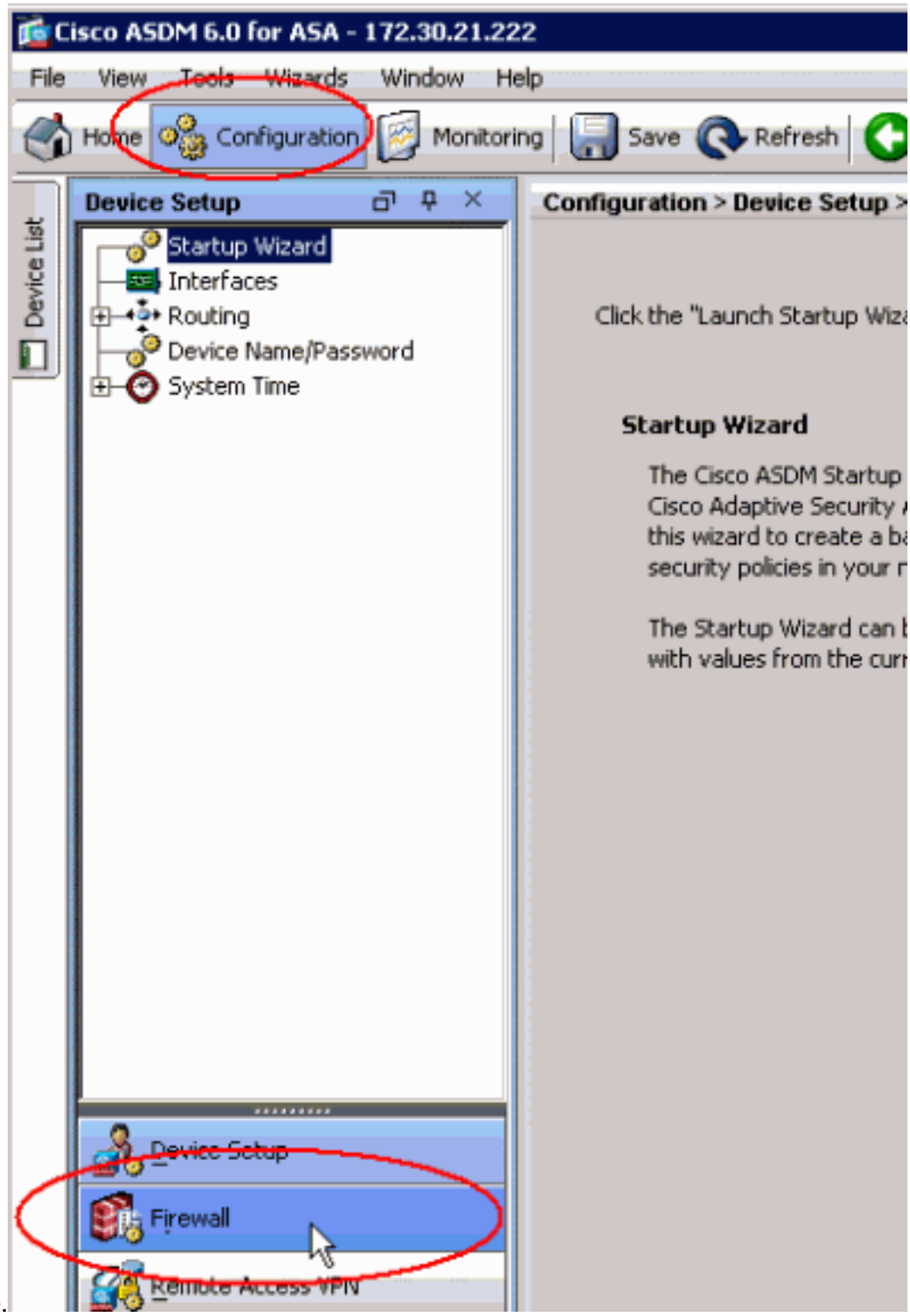
Esta seção demonstra como configurar a Filtragem URL para a ferramenta de segurança com o Security Device Manager adaptável (ASDM).

Depois que você lança o ASDM, termine estas etapas:

1. Escolha a placa da **configuração**.

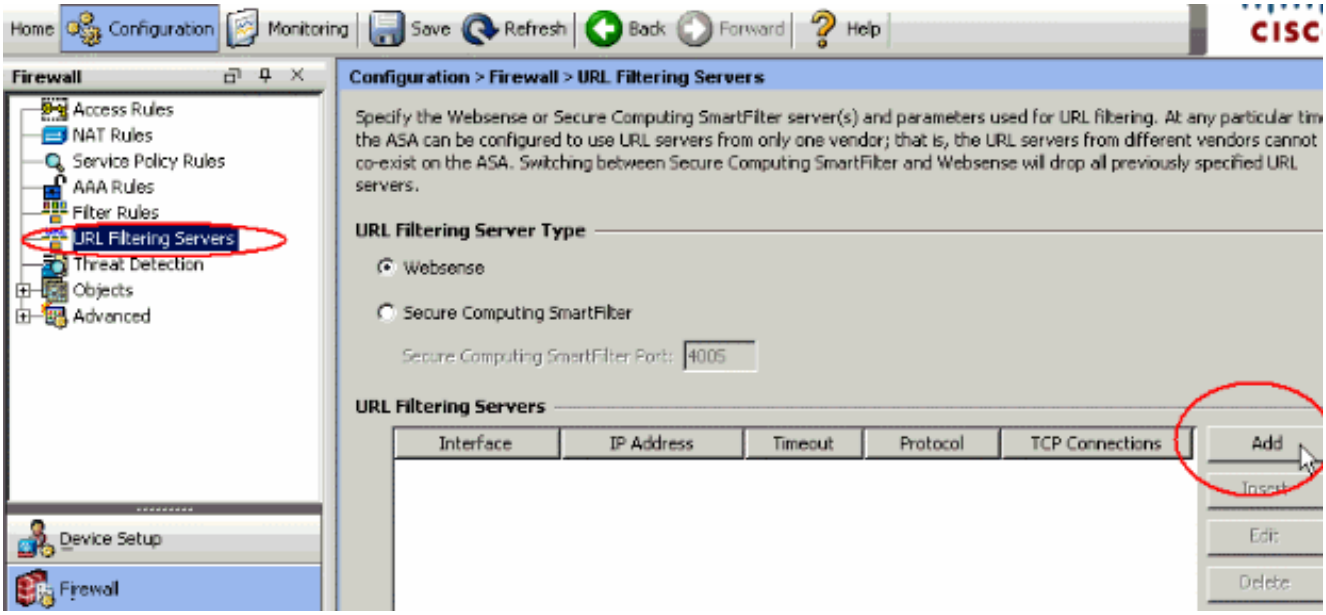


2. Clique o **Firewall na** lista mostrada na placa da

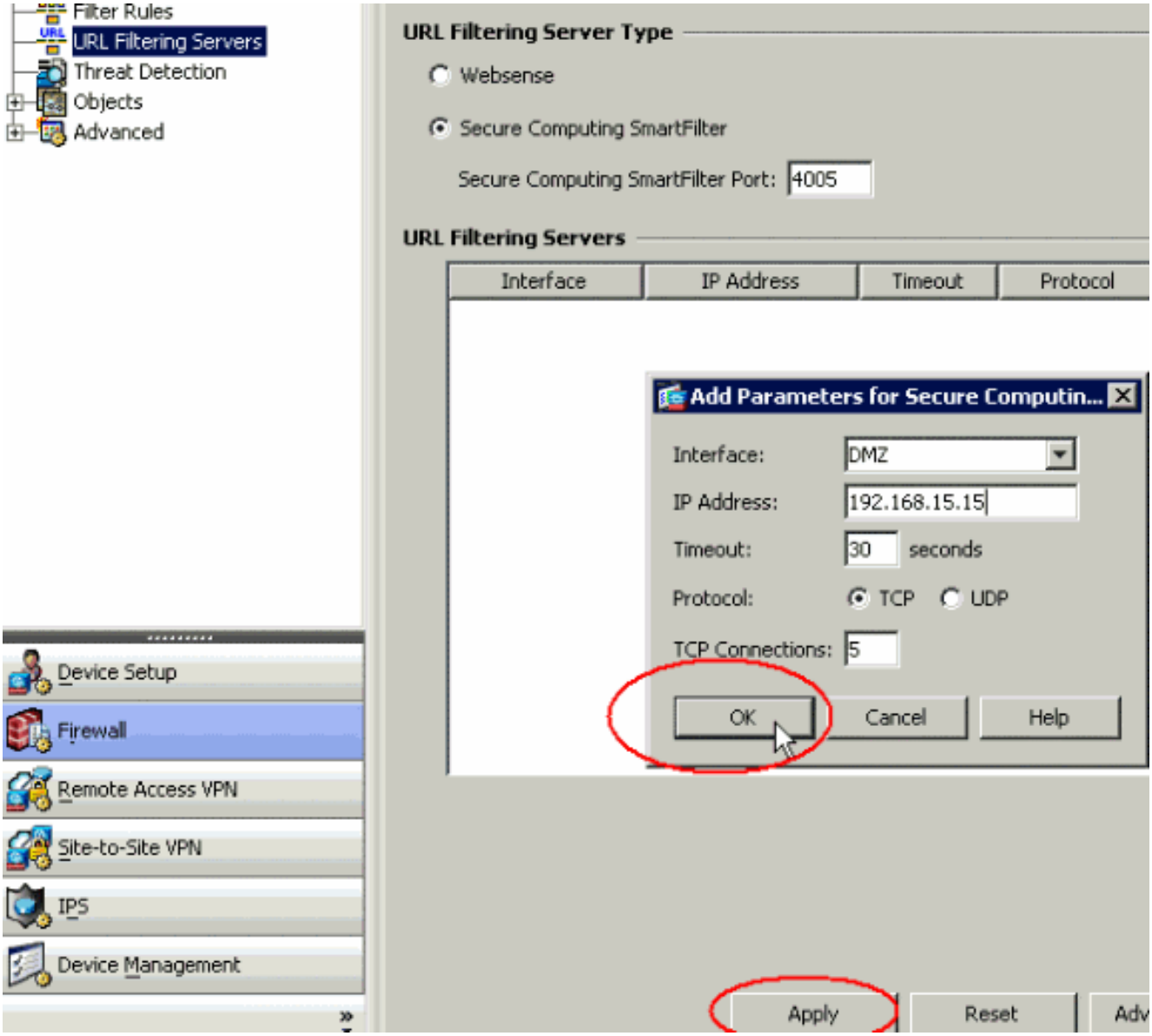


configuração.

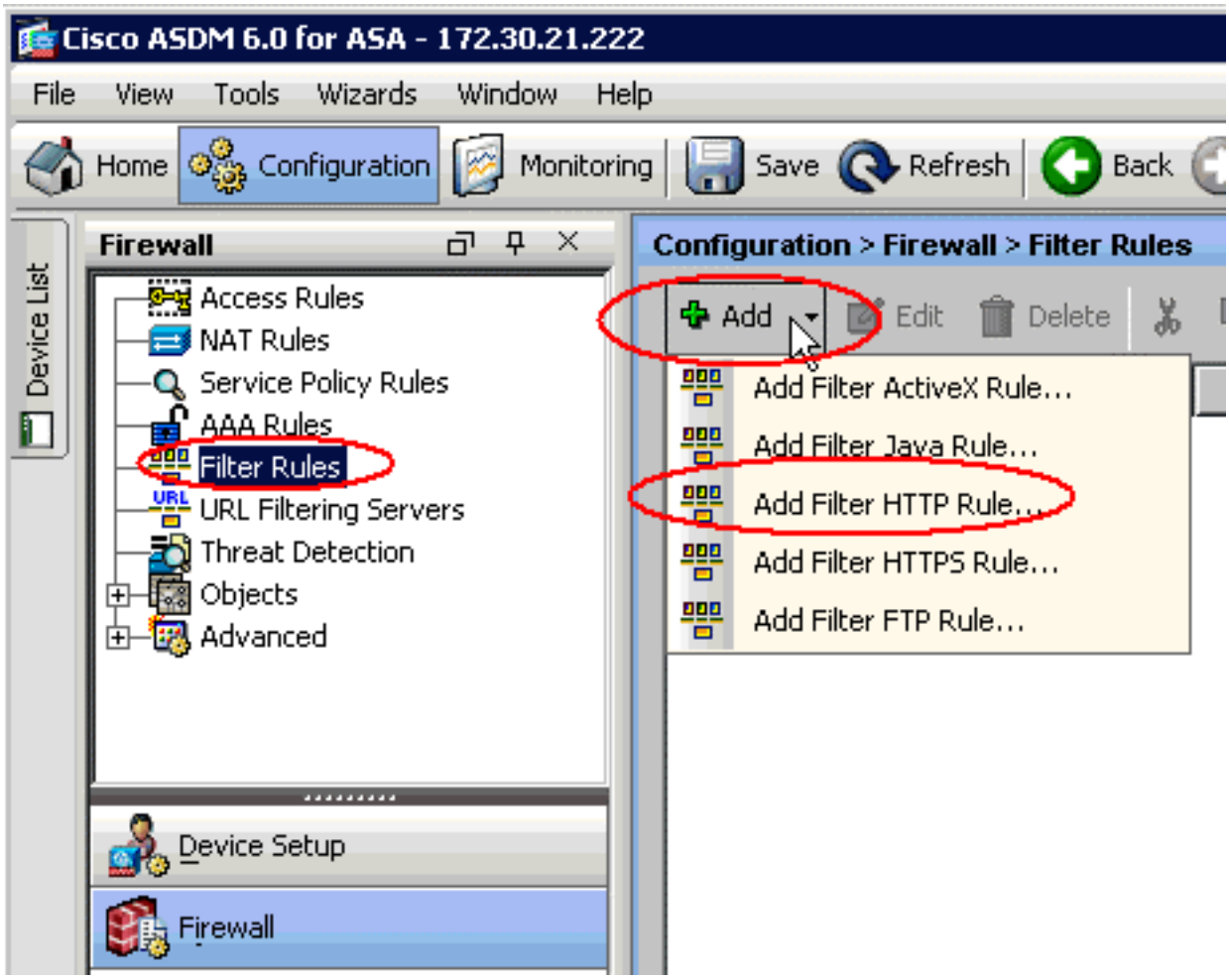
3. Da lista de drop-down do **Firewall**, escolha **server da Filtragem URL**. Escolha o tipo de servidor que da Filtragem URL você quer se usar, e o clique **adiciona** para configurar seus parâmetros.**Nota:** Você deve adicionar o servidor de filtragem antes que você possa configurar a filtração para regras de filtragem HTTP, HTTPS, ou FTP.



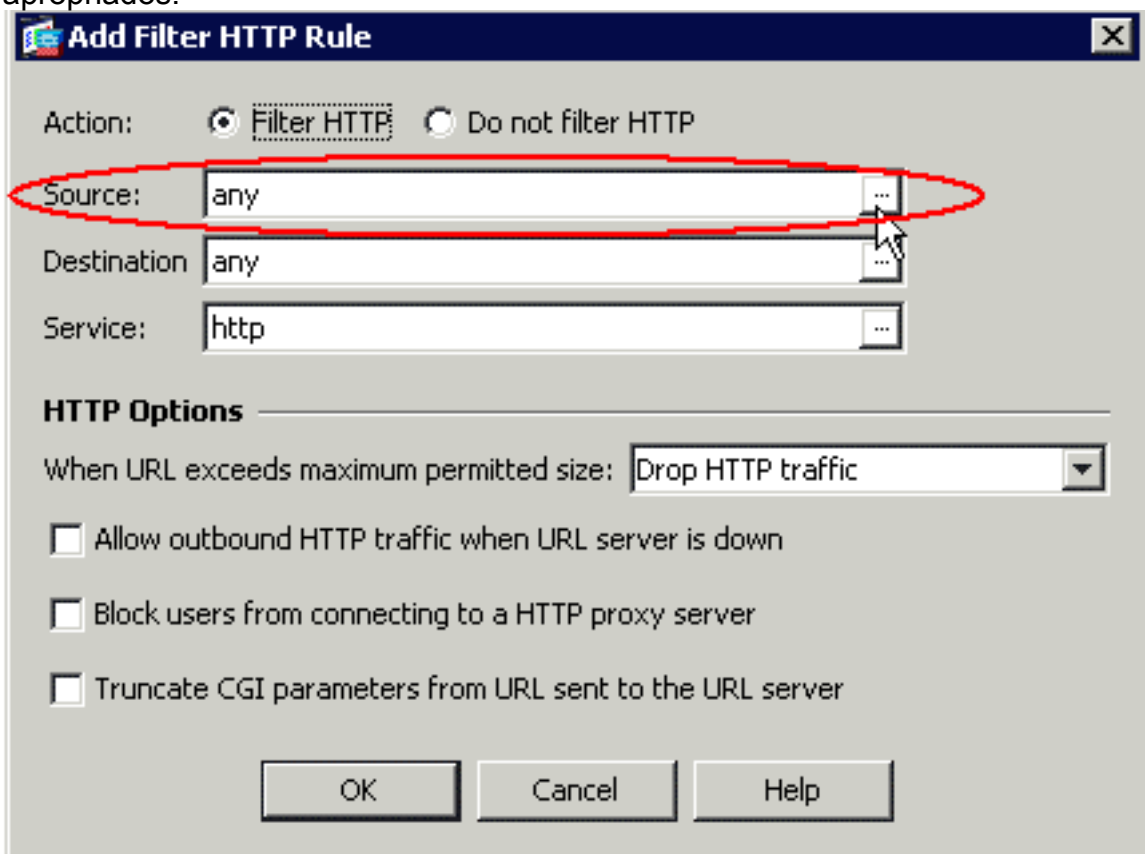
4. Escolha os parâmetros apropriados na janela pop-up:Relação — Indica a relação conectada ao servidor de filtragemEndereço IP de Um ou Mais Servidores Cisco ICM NT — Indica o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de filtragemIntervalo — Indica o número de segundos depois do qual o pedido aos tempos do servidor de filtragem para foraProtocolo — Indica o protocolo usado para comunicar-se com o servidor de filtragem. A versão do TCP 1 é o padrão. A versão do TCP 4 permite que o PIX Firewall envie nomes de usuário autenticado e informação de registro URL ao servidor websense, se o PIX Firewall tem autenticado já o usuárioConexões de TCP — Indica o número máximo de conexões de TCP permitidas comunicar-se com o server da Filtragem URLDepois que você incorpora os parâmetros, clique a **APROVAÇÃO na** janela pop-up e **aplique-a na** janela principal.



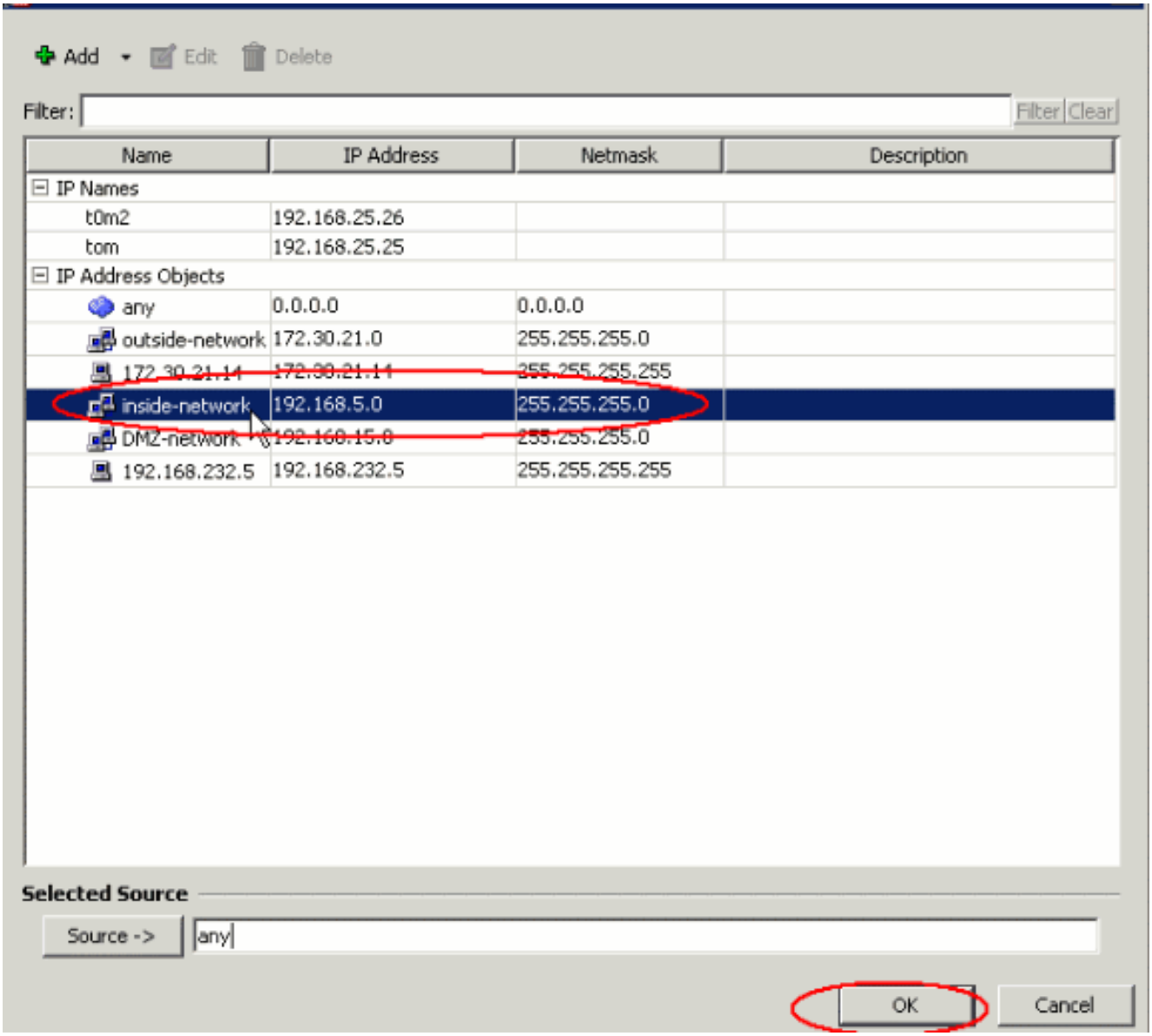
5. Da lista de drop-down do **Firewall**, escolha **regras de filtro**. Clique o **botão Add na** janela principal, e escolha o tipo de regra que você quer adicionar. Neste exemplo, a **regra do filtro HTTP adicionar** é escolhida.



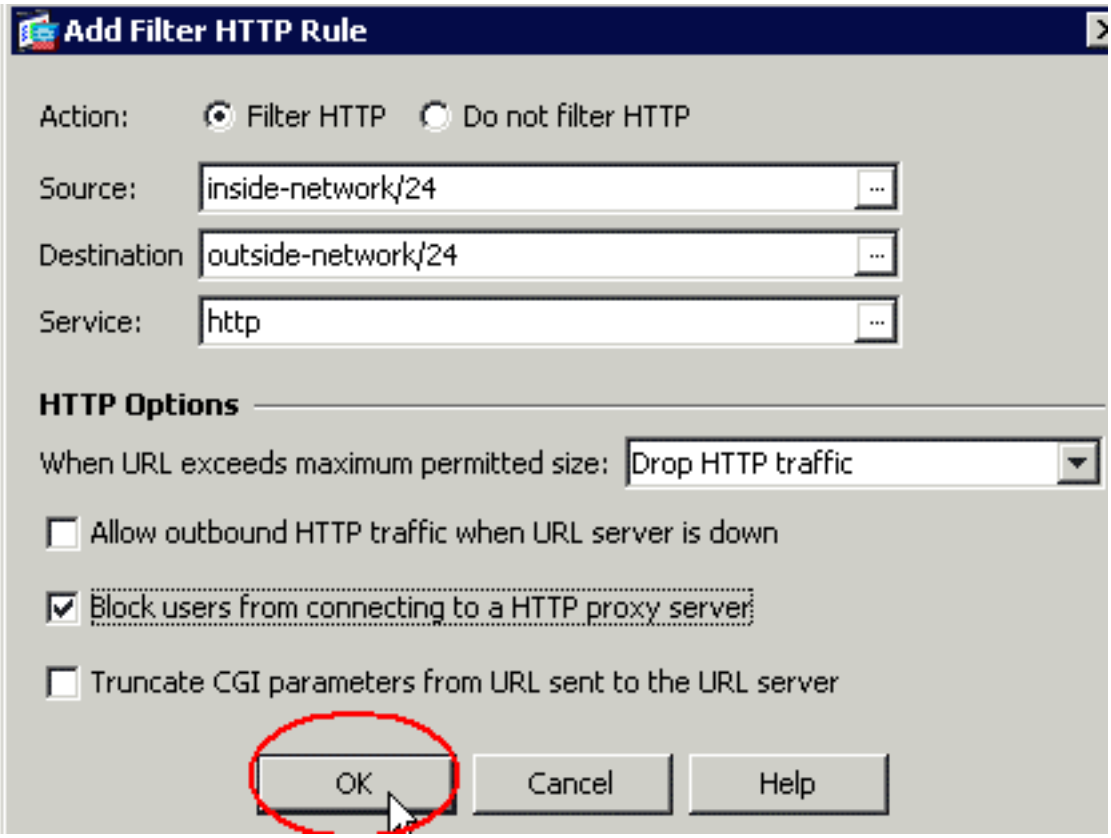
6. Uma vez que a janela pop-up aparece, você pode clicar sobre os botões Browse para opções da **fonte**, do **destino** e de **serviço** a fim escolher os parâmetros apropriados.



7. Isto mostra o indicador da consultação para a opção da **fonte**. Faça sua seleção e clique a **APROVAÇÃO**.

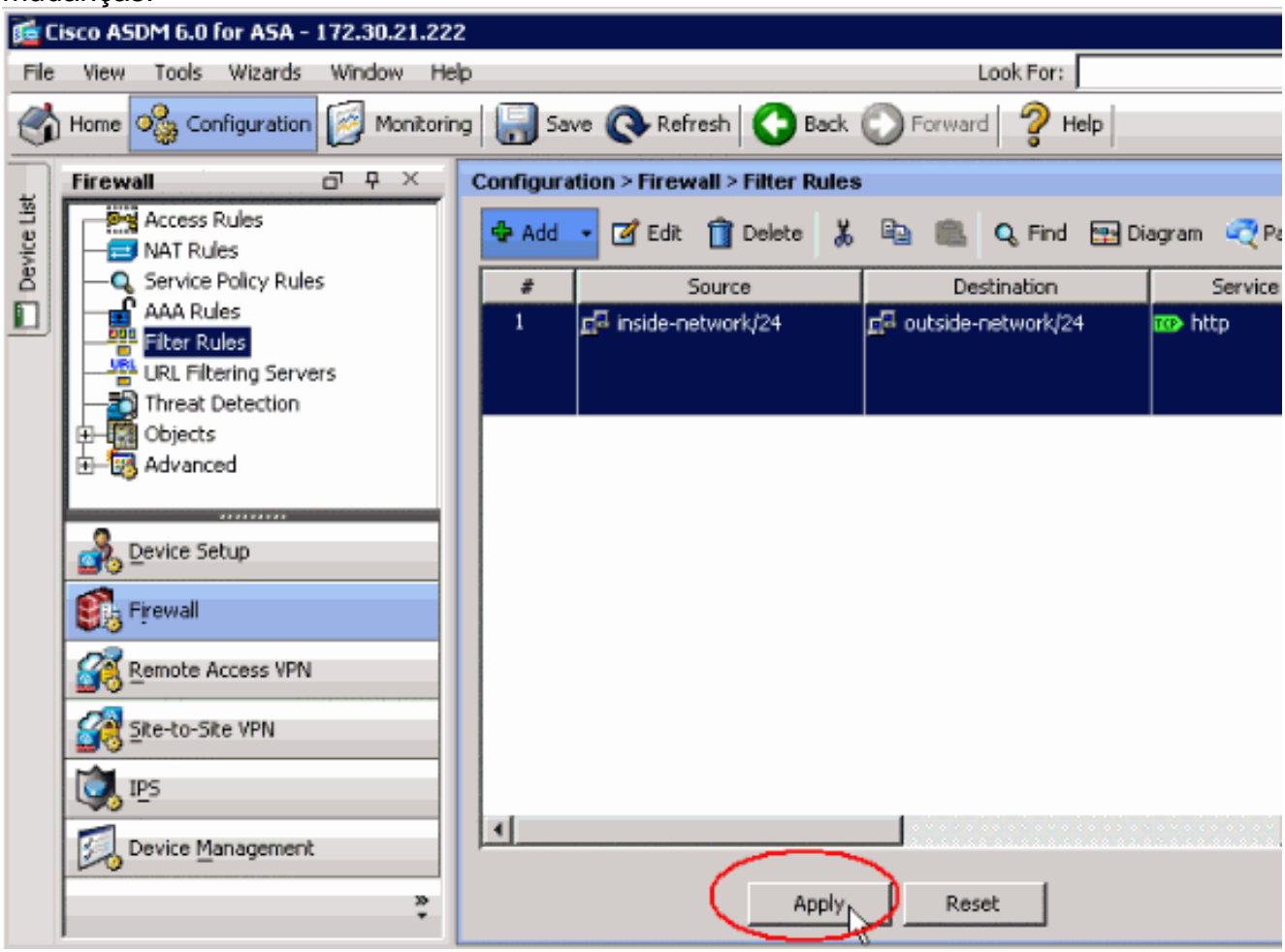


8. Depois que você termina a seleção para todos os parâmetros, clique a **APROVAÇÃO** para



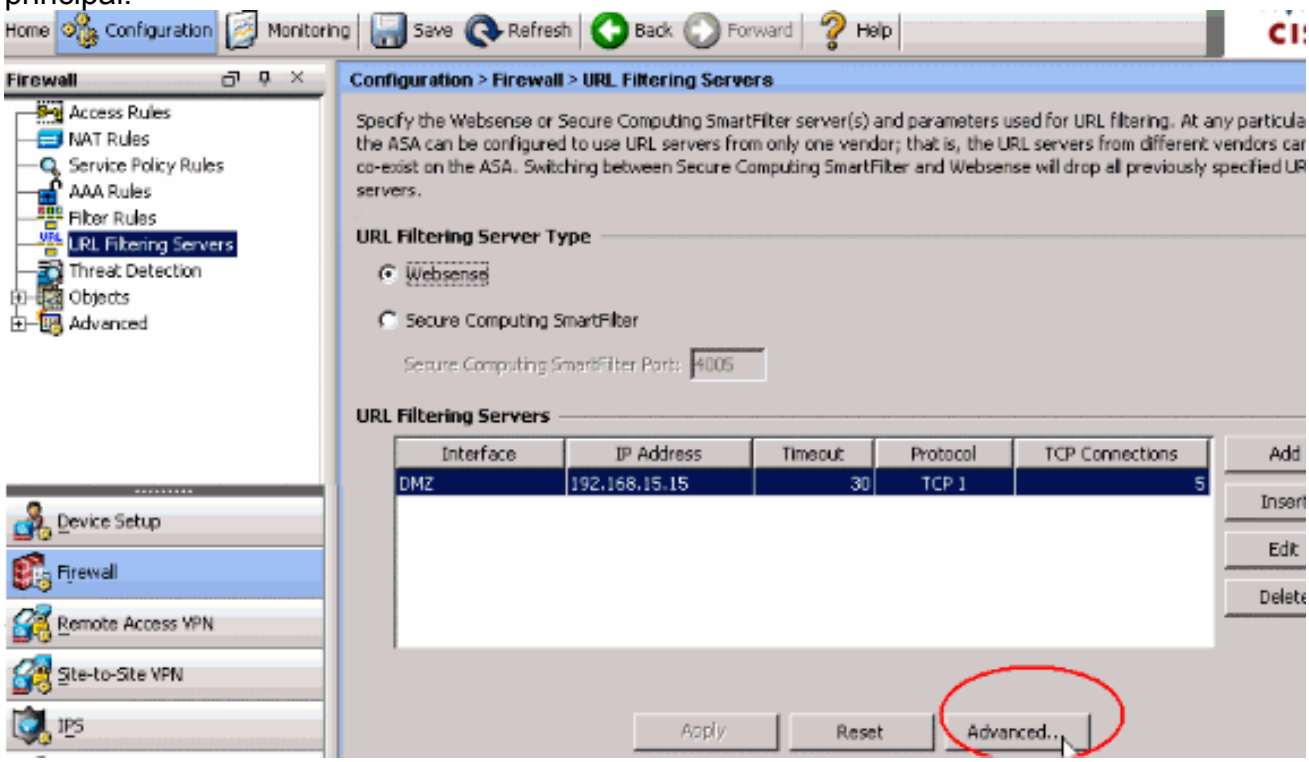
continuar.

9. Uma vez que os parâmetros apropriados são configurados, o clique **aplica-se** a fim submeter as
mudanças.

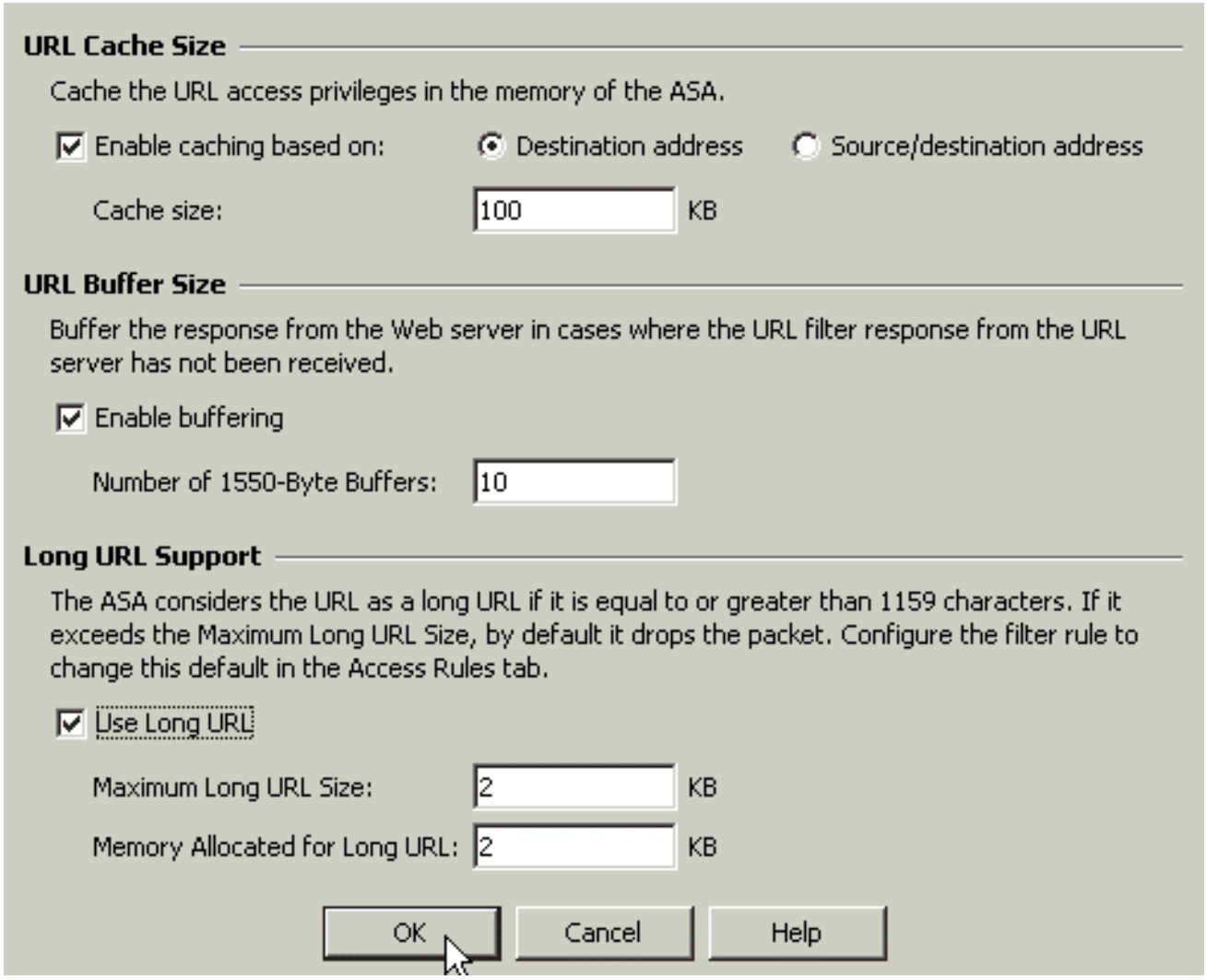


10. Para opções avançadas da Filtragem URL, escolha **server da Filtragem URL** outra vez do **Firewall** deixam cair para baixo a lista, e clicam o **botão Advanced na** janela

principal.



11. Configurar os parâmetros, tais como o tamanho de cache URL, o tamanho de buffer URL e o apoio longo URL, na janela pop-up. Clique a **APROVAÇÃO na** janela pop-up, e o clique **aplica-se na** janela principal a fim
continuar.



12. Finalmente, certifique-se de que você salvar as mudanças que você faz antes que você termine a sessão ASDM.

Verificar

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

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

- **URL-server da mostra** — Mostra a informação sobre o servidor de filtragemPor exemplo:`hostname#show url-server url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp connections 10` Na versão de software 7.2 e mais atrasado, emita o formulário do URL-**server da executar-configuração da mostra d**este comando.
- **mostre o stats do URL-server** — Mostras informação e estatísticas sobre o servidor de filtragemPara a versão de software 7.2, emita as **estatísticas do URL-server da executar-configuração da mostra** formam deste comando.Na versão de software 8.0 e mais atrasado, emita as **estatísticas do URL-server da mostra** formam deste comando.Por exemplo:`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-bloco da mostra** — Mostra a configuração do buffer do bloco URLPor exemplo:`hostname#show url-block url-block url-mempool 128 url-block url-size 4 url-block block 128` Na versão de software 7.2 e mais atrasado, emita o formulário do URL-**bloco da executar-configuração da mostra d**este comando.
- **mostre estatísticas do bloco do URL-bloco** — Mostra as estatísticas do bloco URLPor exemplo:`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 a versão de software 7.2, emita as **estatísticas do bloco do URL-bloco da executar-configuração da mostra** formam deste comando.
- **mostre o stats do URL-esconderijo** — Mostra como o esconderijo é usadoPor exemplo:`hostname#show url-cache stats URL Filter Cache Stats ---------- Size : 128KB Entries : 1724 In Use : 456 Lookups : 45 Hits : 8` Na versão de software 8.0, emita as **estatísticas do URL-esconderijo da mostra** formam deste comando.
- **perfmon da mostra** — Estatísticas de desempenho da Filtragem URL das mostras, junto com outras estatísticas de desempenho. As estatísticas de filtração são mostradas nas fileiras do req do acesso URL e do server URL.Por exemplo:`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 da mostra** — Mostra a configuração de filtraçãoPor exemplo:`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` Na versão de software 7.2 e mais atrasado, emita o formulário do **filtro da executar-configuração da mostra d**este comando.

Troubleshooting

Esta seção fornece a informação em como pesquisar defeitos sua configuração.

Erro: "%ASA-3-304009: Foi executado fora dos blocos do buffer especificados pelo comando do URL-bloco"

O Firewall é executado fora do esconderijo URL que está significado guardar respostas do server quando o Firewall espera para obter a confirmação do server URL.

Solução

A edição é relacionada basicamente a uma latência entre o ASA e o servidor websense. A fim resolver esta tentativa da edição estas ações alternativas.

- Tente mudar o protocolo que é usado no ASA ao UDP a fim se comunicar com Websense.Há uma edição com latência entre o servidor websense e o Firewall, em que as respostas do servidor websense tomam um muito tempo retornar ao Firewall, assim esta faz com que o buffer URL encha-se acima quando esperar uma resposta.Você pode usar o UDP em vez do TCP para a comunicação entre o servidor websense e o Firewall. Isto é porque quando você se usa o TCP para a Filtragem URL, para cada pedido novo URL, o ASA precisa de estabelecer uma conexão de TCP com o servidor websense. Desde que o UDP é um protocolo sem conexão, o ASA não é forçado a estabelecer a conexão para receber a resposta do server. Isto deve melhorar o desempenho do server.`ASA(config)#`**`url-server (inside) vendor websense host X.X.X.X timeout 30`** `protocol UDP version 4 connections 5`
- Certifique-se aumentar o bloco do URL-bloco ao valor o mais alto possível, que é 128. Isto pode ser verificado com o comando do URL-**bloco da mostra**.Se mostra o 128, tome o realce da identificação de bug Cisco CSCta27415 (clientes registrados somente) **na** consideração.

Informações Relacionadas

- Sustentação do produto do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Sustentação do produto do Dispositivos de segurança Cisco PIX série 500
- Sustentação do produto do Cisco Adaptive Security Device Manager
- PIX/ASA: Estabeleça e pesquise defeitos a Conectividade através do dispositivo do Cisco Security
- Troubleshooting de Conexões via PIX e ASA
- Suporte Técnico e Documentação - Cisco Systems