# Konfigurationsbeispiel für die PIX/ASA-URL-Filterung

## Inhalt



## Einführung

In diesem Dokument wird erläutert, wie Sie die URL-Filterung auf einer Sicherheits-Appliance konfigurieren.

Datenverkehr filtern hat folgende Vorteile:

- Sie trägt dazu bei, Sicherheitsrisiken zu reduzieren und eine unangemessene Nutzung zu verhindern.
- Sie bietet eine bessere Kontrolle über den Datenverkehr, der über die Sicherheits-Appliance geleitet wird.

**Hinweis:** Da die URL-Filterung CPU-intensiv ist, stellt die Verwendung eines externen Filterservers sicher, dass der Durchsatz des anderen Datenverkehrs nicht beeinträchtigt wird. Je nach Geschwindigkeit Ihres Netzwerks und der Kapazität Ihres URL-Filterservers kann die für die Erstverbindung erforderliche Zeit jedoch deutlich langsamer werden, wenn der Datenverkehr mit einem externen Filterserver gefiltert wird.

**Hinweis:** Die Implementierung einer Filterung von einer niedrigeren Sicherheitsstufe zu einer

höheren wird nicht unterstützt. URL-Filterung funktioniert nur für ausgehenden Datenverkehr, z. B. Datenverkehr, der von einer Schnittstelle mit hoher Sicherheit ausgeht und für einen Server mit niedriger Sicherheitsschnittstelle bestimmt ist.

# Voraussetzungen

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Security Appliance der Serie PIX 500 mit Version 6.2 und höher
- Security Appliance der Serie ASA 5500 mit Version 7.x und höher
- Adaptive Security Device Manager (ASDM) 6.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

# Hintergrundinformationen

Sie können Verbindungsanforderungen, die von einem sichereren Netzwerk stammen, in ein weniger sicheres Netzwerk filtern. Obwohl Sie Zugriffskontrolllisten (ACLs) verwenden können, um den ausgehenden Zugriff auf bestimmte Content-Server zu verhindern, ist es aufgrund der Größe und Dynamik des Internets schwierig, die Nutzung auf diese Weise zu verwalten. Sie können die Konfiguration vereinfachen und die Leistung von Sicherheitsgeräten verbessern, indem Sie einen separaten Server verwenden, auf dem eines dieser Internet-Filterungsprodukte ausgeführt wird:

- Websense Enterprise - filtert HTTP, HTTPS und FTP. Es wird von der PIX-Firewall ab Version 5.3 unterstützt.
- Secure Computing SmartFilter (ehemals N2H2) filtert HTTP-, HTTPS-, FTP- und lange URL-Filterung. Es wird von der PIX-Firewall ab Version 6.2 unterstützt.

Im Vergleich zur Verwendung von Zugriffskontrolllisten verringert dies den Verwaltungsaufwand und verbessert die Filtereffektivität. Da die URL-Filterung auf einer separaten Plattform erfolgt, ist auch die Leistung der PIX-Firewall weitaus weniger beeinträchtigt. Benutzer können jedoch längere Zugriffszeiten auf Websites oder FTP-Server feststellen, wenn der Filterserver von der Sicherheits-Appliance entfernt ist.

Die PIX-Firewall überprüft ausgehende URL-Anfragen mit der auf dem URL-Filterserver definierten Richtlinie. Die PIX-Firewall erlaubt oder verweigert die Verbindung basierend auf der Antwort des Filterservers.

Wenn die Filterung aktiviert ist und eine Inhaltsanfrage über die Sicherheits-Appliance gesendet wird, wird die Anforderung gleichzeitig an den Content-Server und den Filterserver gesendet.

Wenn der Filterserver die Verbindung zulässt, leitet die Sicherheits-Appliance die Antwort vom Content-Server an den Client weiter, der die Anforderung erstellt hat. Wenn der Filterserver die Verbindung verweigert, verwirft die Sicherheits-Appliance die Antwort und sendet eine Meldung oder einen Rückgabecode, die anzeigt, dass die Verbindung nicht erfolgreich ist.

Wenn die Benutzerauthentifizierung auf der Sicherheits-Appliance aktiviert ist, sendet die Sicherheits-Appliance auch den Benutzernamen an den Filterserver. Der Filterserver kann benutzerspezifische Filtereinstellungen verwenden oder erweiterte Berichte zur Verwendung bereitstellen.

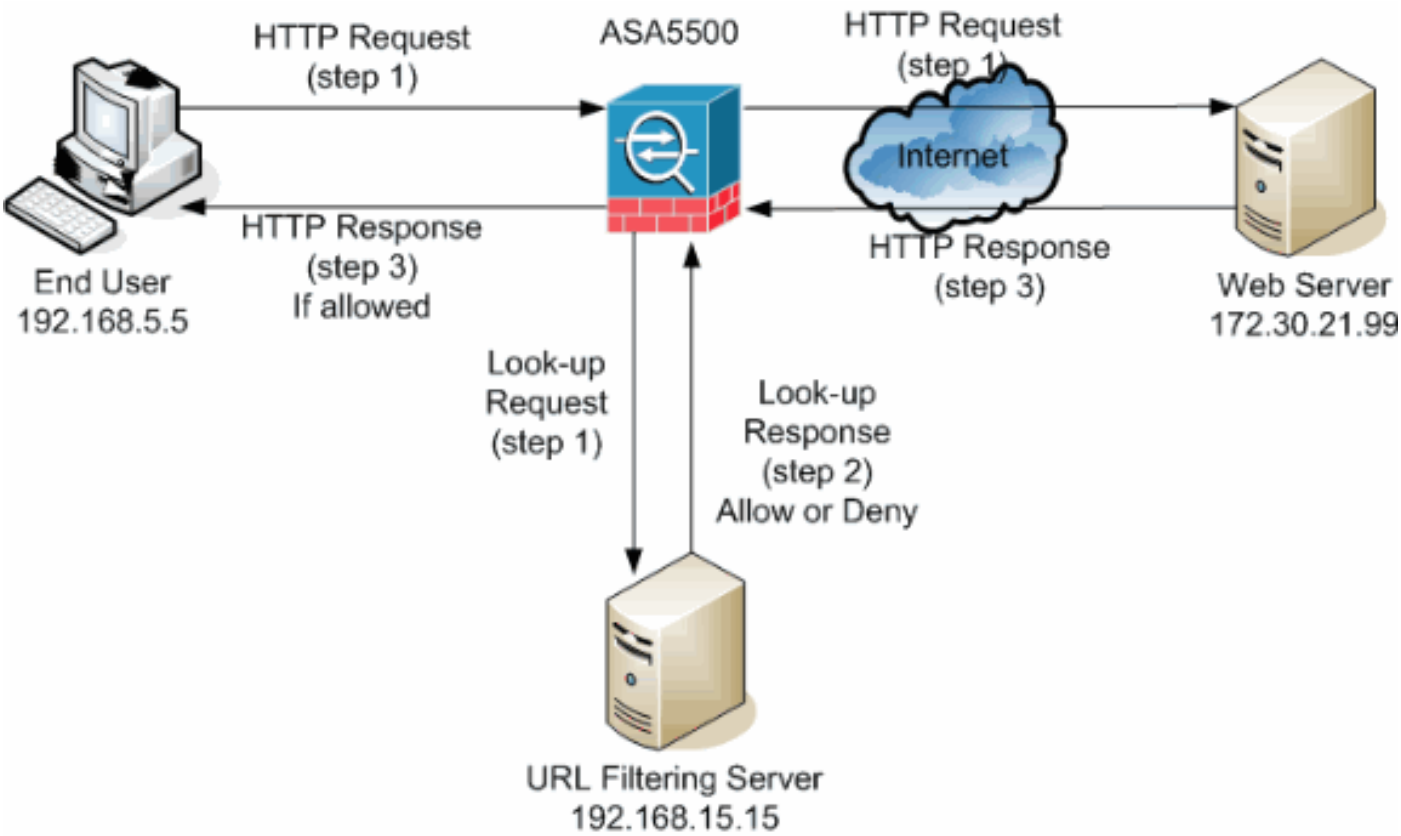
# Konfigurieren der ASA/PIX mit der CLI

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:




In diesem Beispiel befindet sich der URL-Filterserver in einem DMZ-Netzwerk. Endbenutzer im Netzwerk versuchen, über das Internet auf den Webserver außerhalb des Netzwerks zuzugreifen.

Diese Schritte werden bei der Benutzeranfrage für den Webserver ausgeführt:

1. Der Endbenutzer ruft eine Seite auf dem Webserver auf, und der Browser sendet eine HTTP-Anfrage.

2. Nachdem die Sicherheits-Appliance diese Anforderung erhält, leitet sie die Anforderung an den Webserver weiter und extrahiert gleichzeitig die URL und sendet eine Suchanfrage an den URL-Filterserver.
3. Nachdem der URL-Filterserver die Suchanfrage empfängt, überprüft er seine Datenbank, um festzustellen, ob die URL zugelassen oder verweigert werden soll. Sie gibt den Status "Zulassen" oder "Ablehnen" mit einer Nachfrageantwort auf die Cisco IOS® Firewall zurück.
4. Die Sicherheits-Appliance erhält diese Nachschlageantwort und führt eine der folgenden Funktionen aus:Wenn die Nachschlageantwort die URL zulässt, sendet sie die HTTP-Antwort an den Endbenutzer.Wenn die Nachschlageantwort die URL verweigert, leitet der URL-Filterserver den Benutzer zu seinem eigenen internen Webserver um, der eine Meldung anzeigt, in der die Kategorie beschrieben wird, unter der die URL blockiert wird. Anschließend wird die Verbindung an beiden Enden zurückgesetzt.

## Identifizieren des Filterservers

Sie müssen die Adresse des Filterservers mit dem Befehl **url-server** identifizieren. Sie müssen die entsprechende Form dieses Befehls basierend auf dem verwendeten Filterservertyp verwenden.

**Hinweis:** Bei Softwareversion 7.x und höher können Sie bis zu vier Filterserver für jeden Kontext identifizieren. Die Sicherheits-Appliance verwendet die Server in der richtigen Reihenfolge, bis ein Server antwortet. Sie können in Ihrer Konfiguration nur einen Servertyp konfigurieren, entweder Websense oder N2H2.

### Websense

Websense ist eine Filtersoftware eines Drittanbieters, mit der HTTP-Anfragen anhand der folgenden Richtlinien gefiltert werden können:

- Zielhostname
- Ziel-IP-Adresse
- Schlüsselwörter
- Benutzername

Die Software unterhält eine URL-Datenbank mit mehr als 20 Millionen Websites, die in mehr als 60 Kategorien und Unterkategorien unterteilt sind.

- Softwareversion 6.2:

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

  Der **URL-Server-**Befehl gibt den Server an, auf dem die URL-Filteranwendung N2H2 oder Websense ausgeführt wird. Das Limit ist 16 URL-Server. Sie können jedoch jeweils nur eine Anwendung verwenden, entweder N2H2 oder Websense. Wenn Sie Ihre Konfiguration auf der PIX-Firewall ändern, wird außerdem die Konfiguration auf dem Anwendungsserver nicht aktualisiert. Dies muss auf der Grundlage der Anweisungen des jeweiligen Anbieters separat erfolgen.
- Softwareversion 7.x und höher:

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

```
version 1|4
[connections num_conns] ]
```

Ersetzen Sie `if_name` durch den Namen der Sicherheitsappliance-Schnittstelle, die mit dem Filterserver verbunden ist. Der Standardwert ist "inside". Ersetzen Sie `local_ip` durch die IP-Adresse des Filterservers. Tauschen Sie `Sekunden` durch die Anzahl der Sekunden aus, die die Sicherheits-Appliance weiterhin versuchen muss, eine Verbindung zum Filterserver herzustellen.

Verwenden Sie die `Protokolloption`, um anzugeben, ob TCP oder UDP verwendet werden soll. Mit einem Websense-Server können Sie auch die `Version` von TCP angeben, die Sie verwenden möchten. Die TCP-Version 1 ist der Standardwert. Mit TCP-Version 4 kann die PIX-Firewall authentifizierte Benutzernamen und URL-Protokollierungsinformationen an den Websense-Server senden, wenn die PIX-Firewall den Benutzer bereits authentifiziert hat.

Führen Sie zum Beispiel den folgenden Befehl aus, um einen Websense-Filterserver zu identifizieren:

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

## Secure Computing SmartFilter

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

- Softwareversionen 7.0 und 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]]
  ```

- Softwareversion 7.2 und höher:
  ```
  hostname(config)#url-server (if_name) vendor {secure-computing | n2h2} host
  ```

  Für den `Anbieter {Secure-Computing | n2h2}`, können Sie `sicheres Computing` als Anbieterzeichenfolge verwenden. `n2h2` ist jedoch für die Abwärtskompatibilität akzeptabel. Wenn die Konfigurationseinträge generiert werden, wird `sicheres Computing` als Anbieterzeichenfolge gespeichert.

Ersetzen Sie `if_name` durch den Namen der Sicherheitsappliance-Schnittstelle, die mit dem Filterserver verbunden ist. Der Standardwert ist "inside". Ersetzen Sie `local_ip` durch die IP-Adresse des Filterservers und `Port <number>` durch die gewünschte Portnummer.

**Hinweis:** Der Standardport, der vom Secure Computing SmartFilter-Server für die Kommunikation

mit der Sicherheits-Appliance über TCP oder UDP verwendet wird, ist Port 4005.

Tauschen Sie `Sekunden` durch die Anzahl der Sekunden aus, die die Sicherheits-Appliance weiterhin versuchen muss, eine Verbindung zum Filterserver herzustellen. Verwenden Sie die `Protokolloption`, um anzugeben, ob TCP oder UDP verwendet werden soll.

Die `Verbindungen <number>` sind die Anzahl der Versuche, eine Verbindung zwischen Host und Server herzustellen.

Führen Sie zum Beispiel den folgenden Befehl aus, um einen einzelnen N2H2-Filterserver zu identifizieren:

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

Wenn Sie Standardwerte verwenden möchten, geben Sie den folgenden Befehl aus:

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

## Konfigurieren der Filterrichtlinie

**Hinweis:** Sie müssen den URL-Filterserver identifizieren und aktivieren, bevor Sie die URL-Filterung aktivieren.

### URL-Filterung aktivieren

Wenn der Filterserver eine HTTP-Verbindungsanforderung genehmigt, kann die Sicherheits-Appliance die Antwort vom Webserver an den Client weiterleiten, von dem die Anforderung stammt. Wenn der Filterserver die Anforderung ablehnt, leitet die Sicherheits-Appliance den Benutzer auf eine Blockseite um, die anzeigt, dass der Zugriff verweigert wird.

Geben Sie den **URL-Filter-**Befehl ein, um die Richtlinie zu konfigurieren, die zum Filtern von URLs verwendet wird:

- PIX Version 6.2:

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

- Softwareversion 7.x und höher:

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

Ersetzen Sie `port` durch die Portnummer, auf der HTTP-Datenverkehr gefiltert werden soll, wenn ein anderer Port als der Standard-Port für HTTP (80) verwendet wird. Um einen Bereich von Portnummern zu identifizieren, geben Sie den Anfang und das Ende des Bereichs getrennt durch

einen Bindestrich ein.

Bei aktivierter Filterung stoppt die Sicherheits-Appliance ausgehenden HTTP-Datenverkehr, bis ein Filterserver die Verbindung zulässt. Wenn der primäre Filterserver nicht antwortet, leitet die Sicherheits-Appliance die Filteranforderung an den sekundären Filterserver weiter. Die `allow`-Option veranlasst die Sicherheits-Appliance, HTTP-Datenverkehr ohne Filterung weiterzuleiten, wenn der primäre Filterserver nicht verfügbar ist.

Geben Sie den Befehl **proxy-block ein**, um alle Anfragen an die Proxyserver zu verwerfen.

**Hinweis:** Der Rest der Parameter wird verwendet, um lange URLs abzuschneiden.

## Kürzung langer HTTP-URLs

Die `langurl-truncate`-Option veranlasst die Sicherheits-Appliance, nur den Hostnamen oder die IP-Adressteil der URL zur Bewertung an den Filterserver zu senden, wenn die URL länger als die maximal zulässige Länge ist.

Verwenden Sie die Option `longurl-deny`, um ausgehenden URL-Datenverkehr abzulehnen, wenn die URL den maximal zulässigen Wert überschreitet.

Verwenden Sie die Option `cgi-truncate`, um CGI-URLs so zu kürzen, dass sie nur den CGI-Skriptspeicherort und den Skriptnamen ohne Parameter enthalten.

Dies ist ein allgemeines Beispiel für die Filterkonfiguration:

```
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
```

## Datenverkehr von der Filterung ausschließen

Wenn Sie eine Ausnahme von der allgemeinen Filterrichtlinie machen möchten, geben Sie den folgenden Befehl aus:

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

Ersetzen Sie `local_ip` und `local_mask` durch die IP-Adresse und die Subnetzmaske eines Benutzers oder Subnetzwerks, die von Filterbeschränkungen ausgenommen werden sollen.

Ersetzen Sie `Foreign_ip` und `Foreign_mask` durch die IP-Adresse und die Subnetzmaske eines Servers oder Subnetzwerks, der bzw. das von Filterbeschränkungen ausgenommen werden soll.

Dieser Befehl veranlasst beispielsweise, dass alle HTTP-Anforderungen von den internen Hosts an 172.30.21.99 an den Filterserver weitergeleitet werden, mit Ausnahme der Anforderungen von Host 192.168.5.5:

Dies ist ein Konfigurationsbeispiel für eine Ausnahme:

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

## Erweiterte URL-Filterung

Dieser Abschnitt enthält Informationen zu erweiterten Filterparametern, darunter folgende Themen:

- Pufferung
- Zwischenspeicherung
- lange URL-Unterstützung

### Puffern der Webserver-Antworten

Wenn ein Benutzer eine Anforderung für die Verbindung mit einem Content-Server ausstellt, sendet die Sicherheits-Appliance die Anforderung gleichzeitig an den Content-Server und an den Filterserver. Wenn der Filterserver nicht vor dem Content-Server antwortet, wird die Serverantwort verworfen. Dies verzögert die Reaktion des Webservers aus Sicht des Web-Clients, da der Client die Anfrage erneut senden muss.

Wenn Sie den HTTP-Antwortpuffer aktivieren, werden Antworten von Webinhaltsservern gepuffert, und die Antworten werden an den Client weitergeleitet, der die Anforderung sendet, wenn der Filterserver die Verbindung zulässt. Dies verhindert Verzögerungen, die andernfalls auftreten können.

Gehen Sie wie folgt vor, um Antworten auf HTTP-Anforderungen zu puffern:

1. Führen Sie folgenden Befehl aus, um das Puffern von Antworten für HTTP-Anforderungen zu aktivieren, die eine Antwort vom Filterserver ausstehen:
   ```
   hostname(config)#url-block block block-buffer-limit
   ```

   Ersetzen Sie `die Blockpuffergrenze` durch die maximale Anzahl zu pufferender Blöcke.
2. Führen Sie folgenden Befehl aus, um den maximal verfügbaren Speicher für das Puffern ausstehender URLs zu konfigurieren und lange URLs mit Websense zu puffern:
   ```
   hostname(config)#url-block url-mempool memory-pool-size
   ```

   Ersetzen Sie die `Speicherpool-Größe` durch einen Wert zwischen 2 und 10.240 für eine maximale Speicherzuweisung von 2 KB bis 10 MB.

### Cache-Server-Adressen

Wenn ein Benutzer auf eine Site zugreift, kann der Filterserver der Sicherheits-Appliance erlauben, die Serveradresse für eine bestimmte Zeit zwischenzuspeichern, solange jeder an der Adresse gehostete Standort in einer Kategorie untergebracht ist, die jederzeit zulässig ist. Wenn der Benutzer dann erneut auf den Server zugreift oder ein anderer Benutzer auf den Server zugreift, muss die Sicherheits-Appliance den Filterserver nicht erneut konsultieren.

Geben Sie bei Bedarf den Befehl **url-cache ein**, um den Durchsatz zu verbessern:

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

Ersetzen Sie die `Größe` durch einen Wert für die Cache-Größe im Bereich von 1 bis 128 (KB).

Verwenden Sie das `dst`-Schlüsselwort, um Einträge auf der Grundlage der URL-Zieladresse zwischenzuspeichern. Wählen Sie diesen Modus aus, wenn alle Benutzer dieselbe URL-Filterungsrichtlinie auf dem Websense-Server verwenden.

Verwenden Sie das `src_dst`-Schlüsselwort, um Einträge sowohl anhand der Quelladresse, die die URL-Anforderung initiiert, als auch anhand der URL-Zieladresse zwischenzuleiten. Wählen Sie diesen Modus aus, wenn Benutzer nicht dieselbe URL-Filterungsrichtlinie auf dem Websense-Server verwenden.

### Filterung von langen URLs aktivieren

Standardmäßig betrachtet die Sicherheits-Appliance eine HTTP-URL als lange URL, wenn sie mehr als 1159 Zeichen beträgt. Mit dem folgenden Befehl können Sie die maximal zulässige Länge für eine einzelne URL erhöhen:

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

Ersetzen Sie die `Long-URL-Größe` durch die maximale Größe in KB für jede lange URL, die gepuffert werden soll.

Mit diesen Befehlen wird beispielsweise die Sicherheits-Appliance für erweiterte URL-Filterung konfiguriert:

```
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
```

## Konfiguration

Diese Konfiguration enthält die in diesem Dokument beschriebenen Befehle:

**ASA 8.0-Konfiguration**

```
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
```

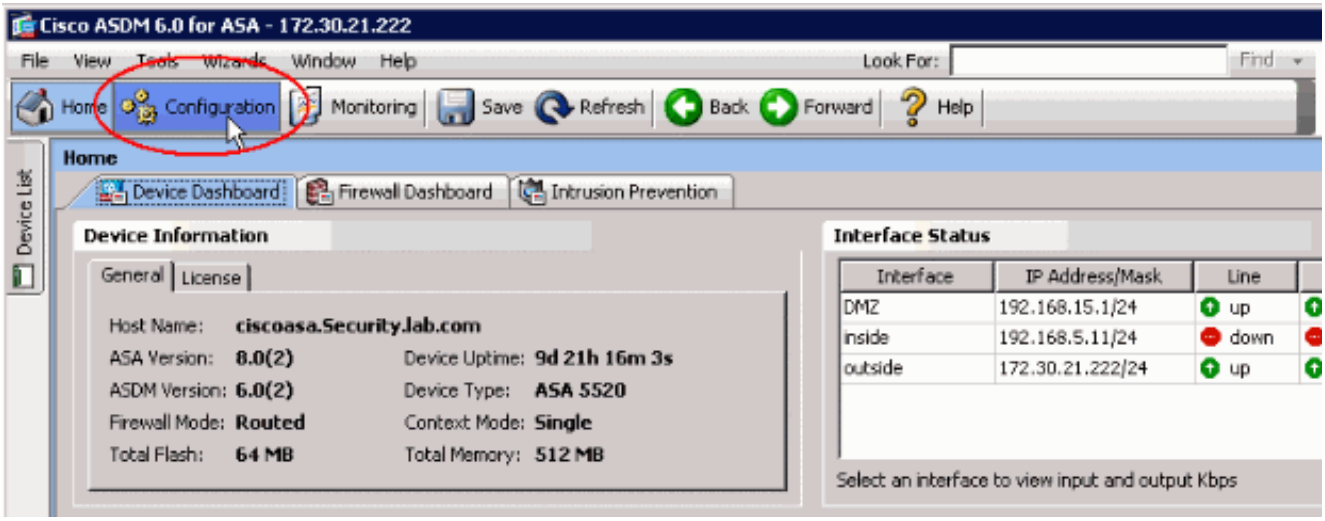
```
privilege 15
prompt hostname context
Cryptochecksum:db208a243faa71f9b3e92491a6ed2105
: end
```

# Konfigurieren von ASA/PIX mit ASDM

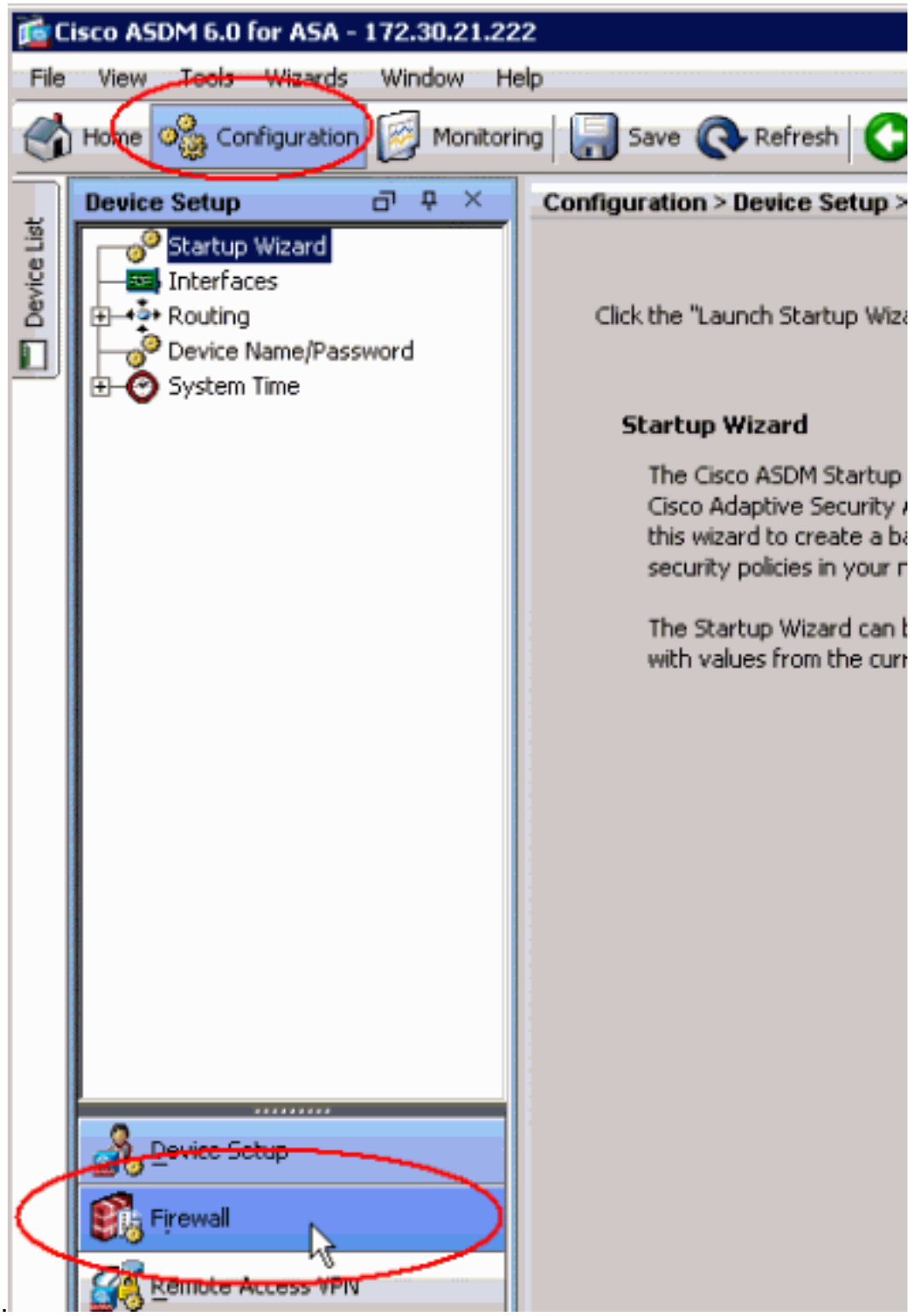
In diesem Abschnitt wird veranschaulicht, wie die URL-Filterung für die Sicherheits-Appliance mit dem Adaptive Security Device Manager (ASDM) konfiguriert wird.

Führen Sie nach dem Start von ASDM die folgenden Schritte aus:

1. Wählen Sie den Bereich **"Konfiguration"** aus.

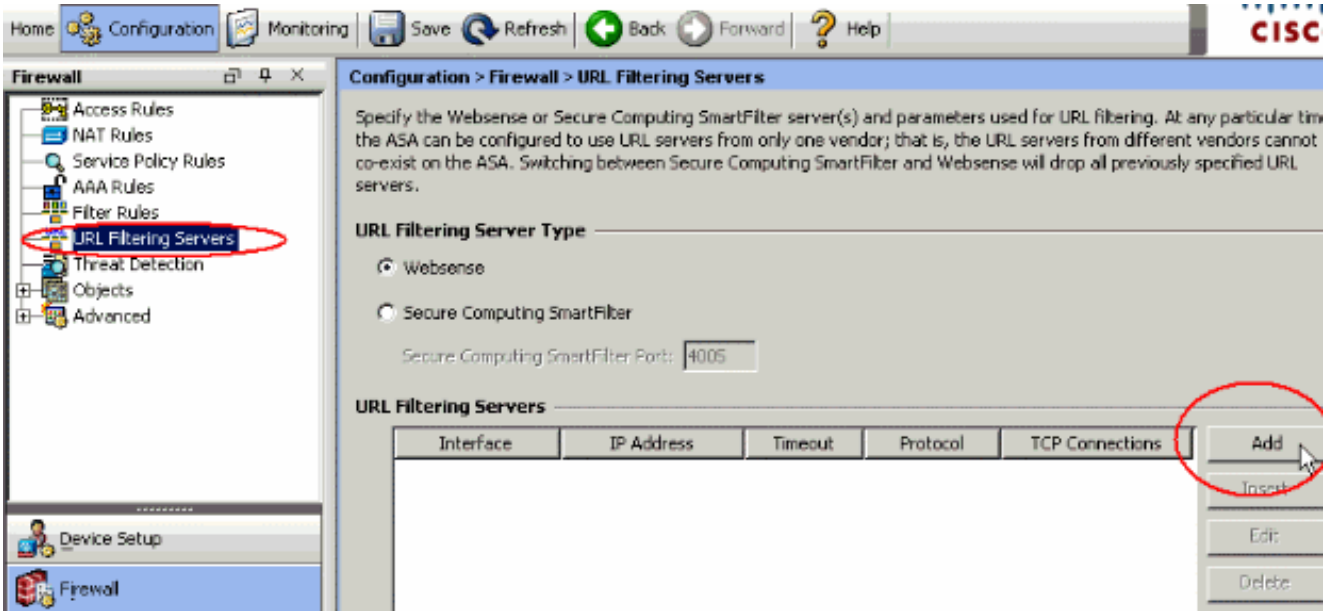



2. Klicken Sie in der Liste im **Konfigurationsbereich** auf

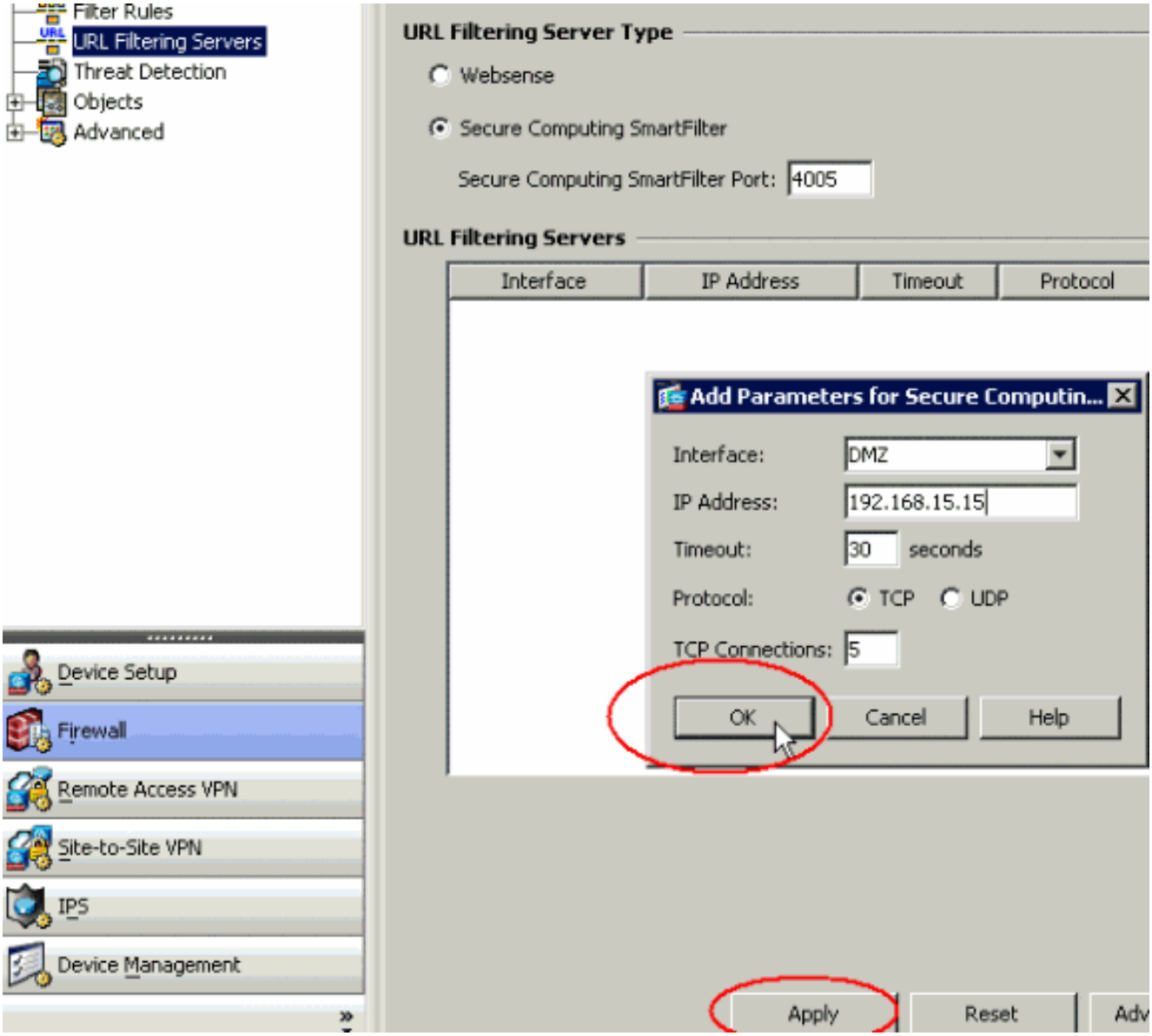



**Firewall**.

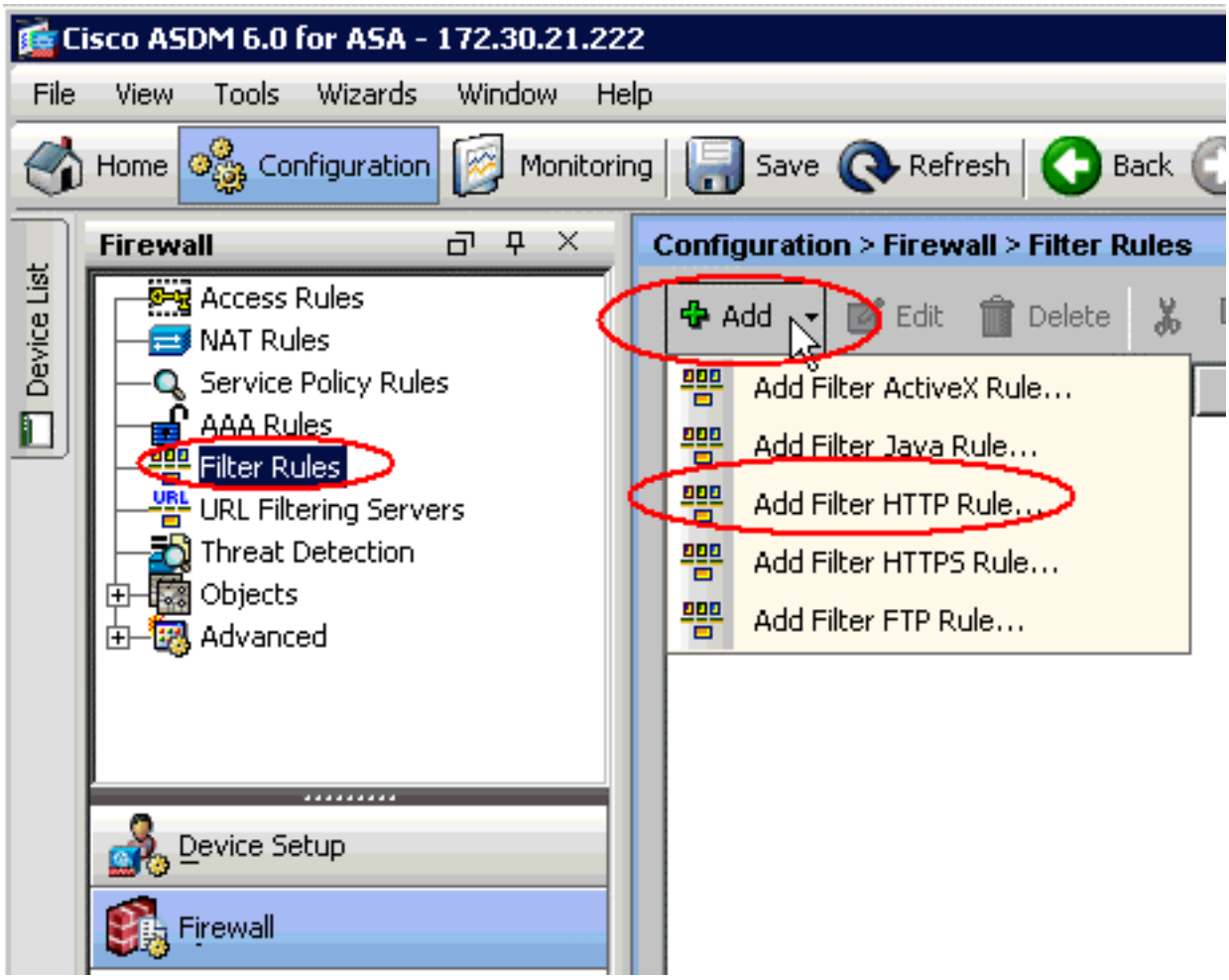
3. Wählen Sie aus der Dropdown-Liste **Firewall** die Option **URL-Filterungsserver aus**. Wählen Sie den URL-Filterserver-Typ aus, den Sie verwenden möchten, und klicken Sie auf **Hinzufügen**, um die Parameter zu konfigurieren.**Hinweis:** Sie müssen den Filterserver hinzufügen, bevor Sie Filterungsregeln für HTTP-, HTTPS- oder FTP-Filterung konfigurieren können.



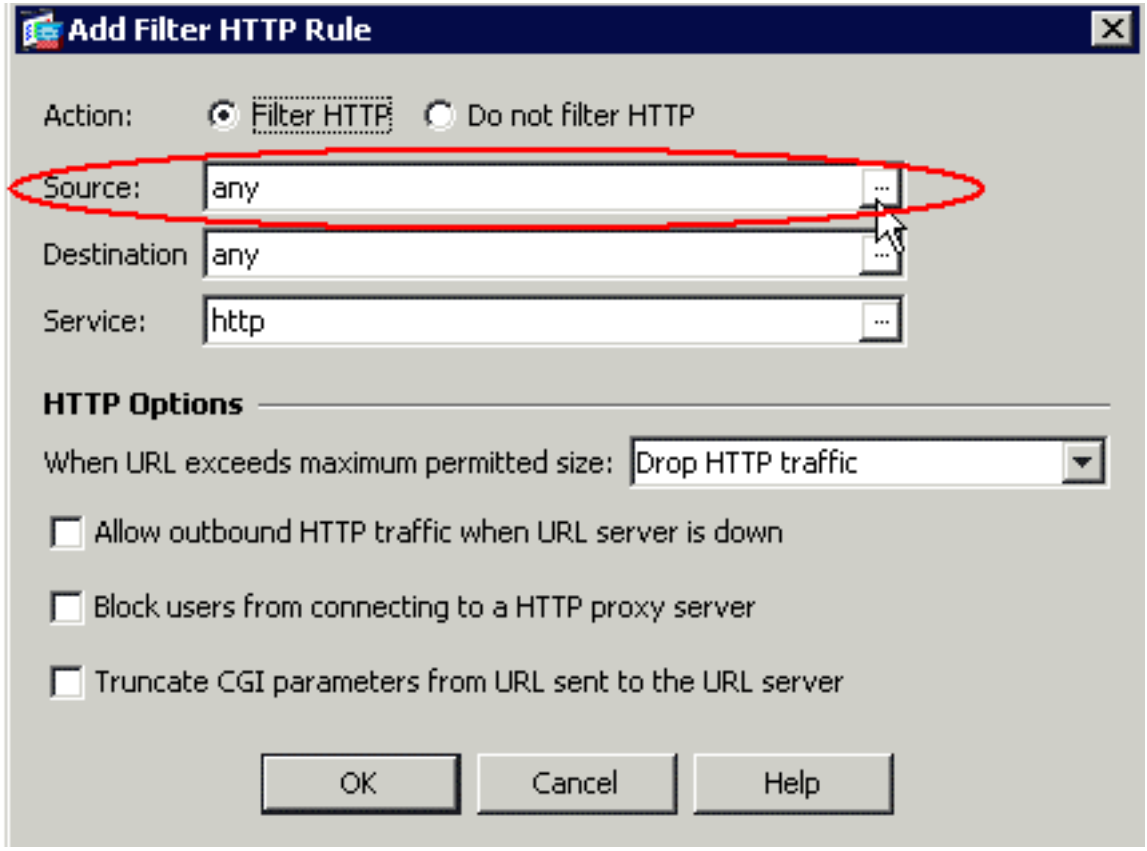

4. Wählen Sie die entsprechenden Parameter im Popup-Fenster aus:Interface (Schnittstelle): Zeigt die Schnittstelle an, die mit dem Filterserver verbunden ist.IP Address (IP-Adresse): Zeigt die IP-Adresse des Filterservers an.Timeout (Zeitüberschreitung): Zeigt die Anzahl der Sekunden an, nach denen die Anforderung an den Filterserver das Timeout überschreitet.Protocol (Protokoll): Zeigt das Protokoll an, das für die Kommunikation mit dem Filterserver verwendet wird. Die TCP-Version 1 ist der Standardwert. Mit TCP-Version 4 kann die PIX-Firewall authentifizierte Benutzernamen und URL-Protokollierungsinformationen an den Websense-Server senden, wenn die PIX-Firewall den Benutzer bereits authentifiziert hat.TCP Connections (TCP-Verbindungen): Zeigt die maximale Anzahl an TCP-Verbindungen an, die für die Kommunikation mit dem URL-Filterserver zulässig sindNachdem Sie die Parameter eingegeben haben, klicken Sie im Popup-Fenster auf **OK** und **Übernehmen** im Hauptfenster.




5. Wählen Sie aus der Dropdown-Liste **Firewall** die Option **Filterregeln** aus. Klicken Sie im Hauptfenster auf die Schaltfläche **Hinzufügen**, und wählen Sie den Regeltyp aus, den Sie hinzufügen möchten. In diesem Beispiel wird die **HTTP-Regel Filter hinzufügen** ausgewählt.

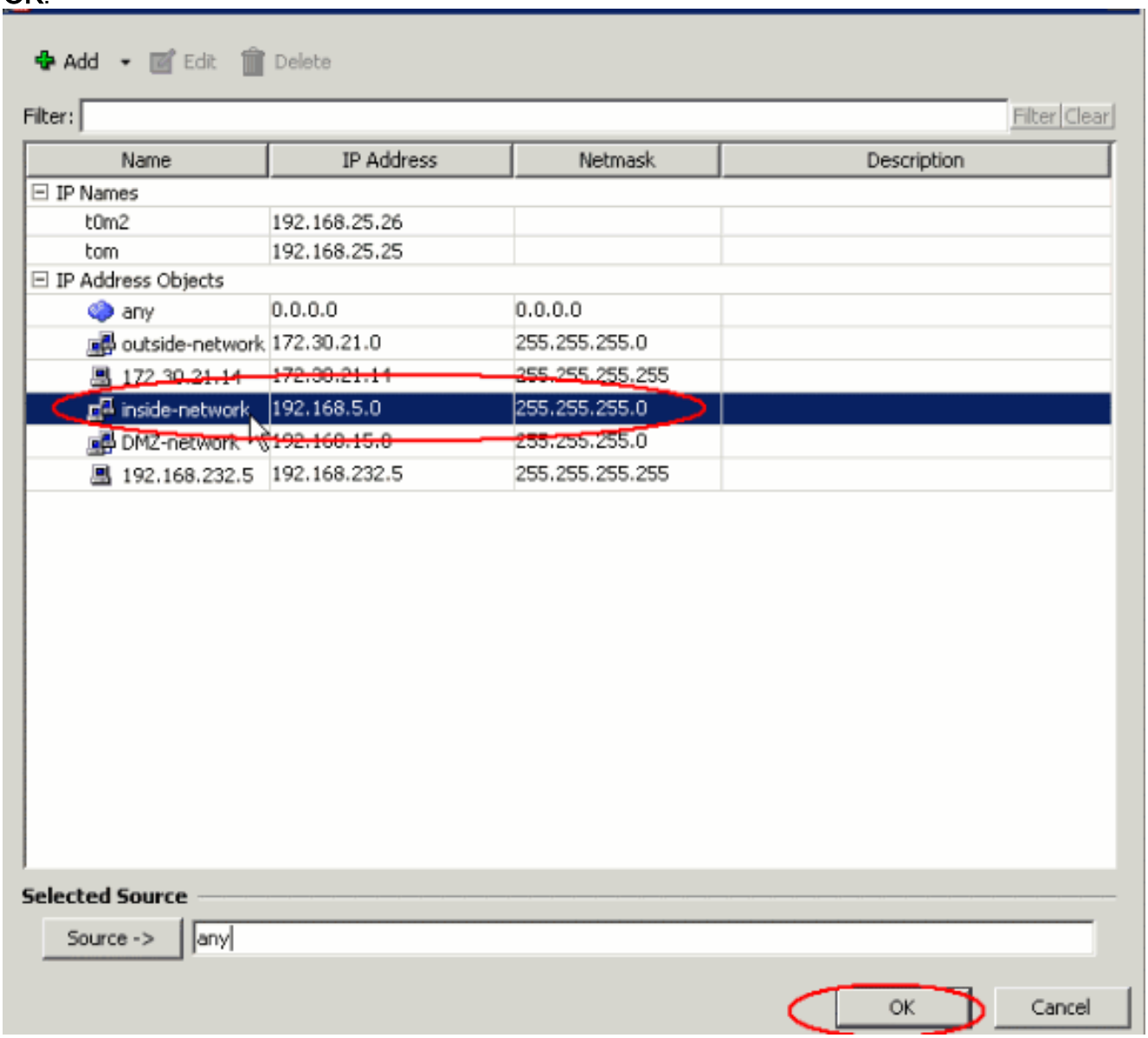



6. Sobald das Popup-Fenster angezeigt wird, können Sie auf die Schaltflächen für die Optionen **Quelle**, **Ziel** und **Service** klicken, um die entsprechenden Parameter auszuwählen.

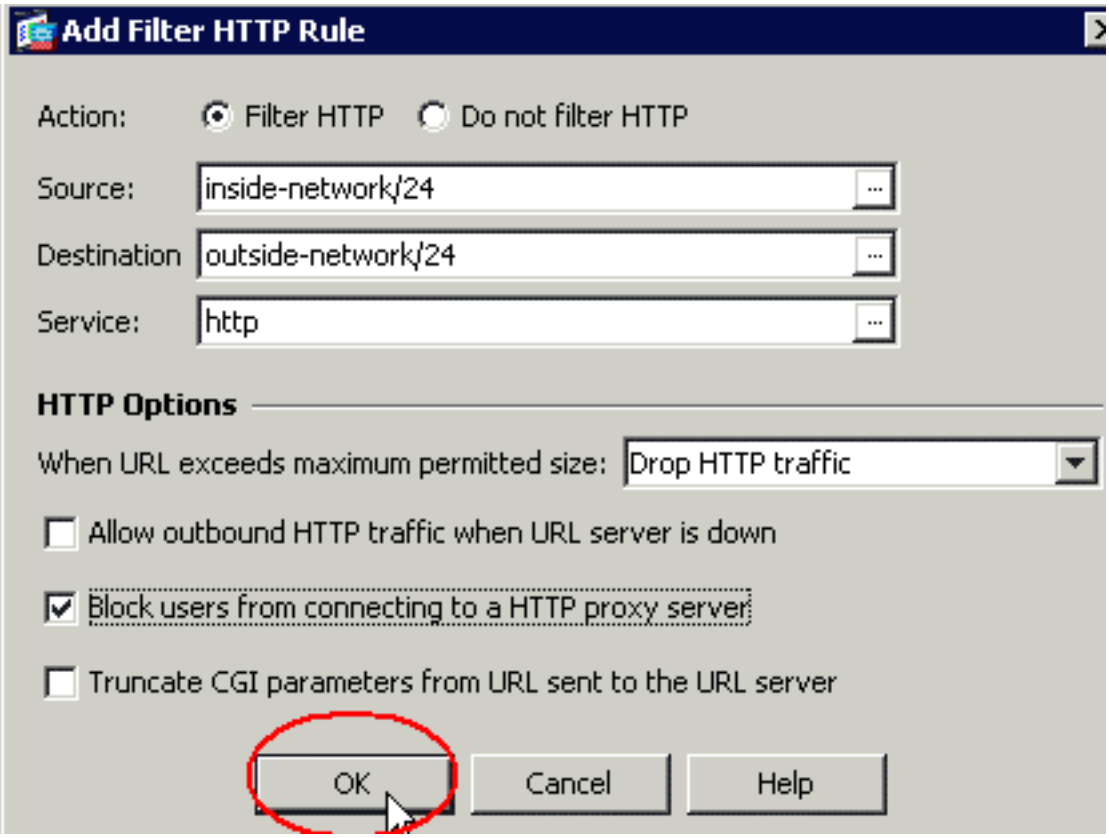



7. Es wird das Suchfenster für die Option **Quelle** angezeigt. Wählen Sie eine Option aus, und klicken Sie auf

OK.

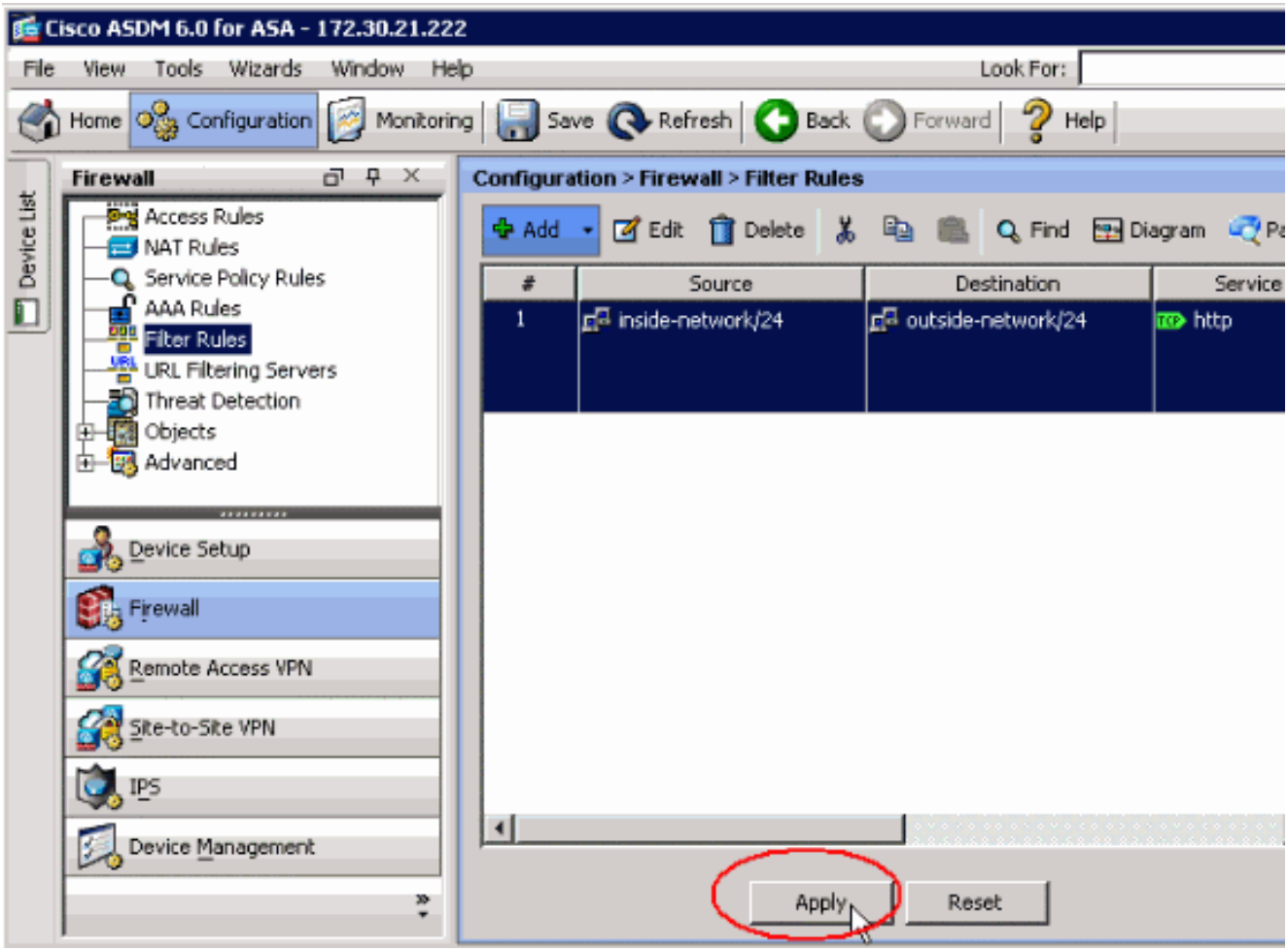



8. Wenn Sie die Auswahl für alle Parameter abgeschlossen haben, klicken Sie auf **OK**, um



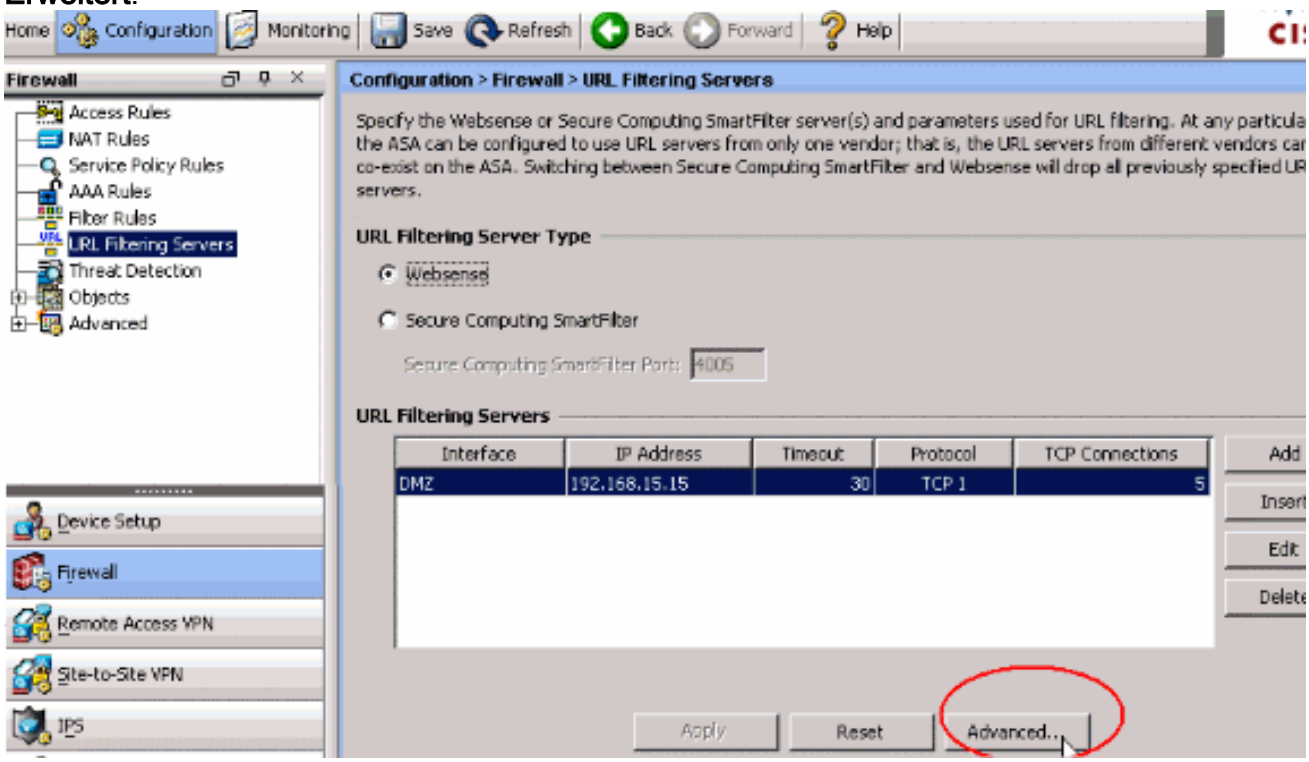

fortzufahren.

9. Wenn die entsprechenden Parameter konfiguriert sind, klicken Sie auf **Apply**, um die Änderungen einzusenden.

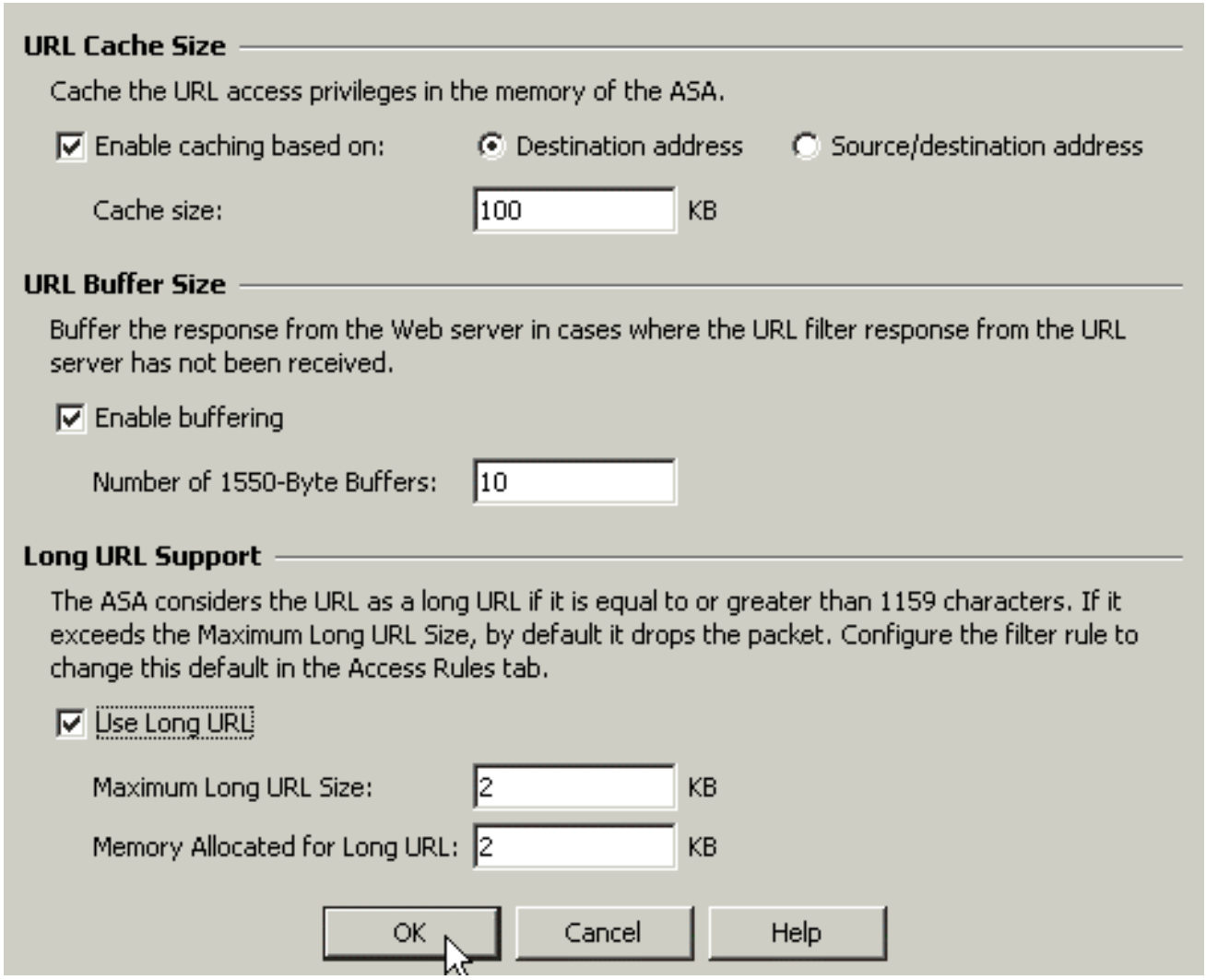



10. Für erweiterte URL-Filteroptionen wählen Sie **URL-Filterungsserver** erneut aus der **Firewall-**Dropdown-Liste aus, und klicken Sie im Hauptfenster auf die **Schaltfläche**

Erweitert.




11. Konfigurieren Sie die Parameter im Popup-Fenster, z. B. die Größe des URL-Cache, die Größe des URL-Puffers und die Long URL-Unterstützung. Klicken Sie im Popup-Fenster auf **OK**, und klicken Sie im Hauptfenster auf **Übernehmen**, um fortzufahren.



12. Stellen Sie abschließend sicher, dass Sie die vorgenommenen Änderungen speichern, bevor Sie die ASDM-Sitzung beenden.

# Überprüfen

Verwenden Sie die Befehle in diesem Abschnitt, um Informationen zur URL-Filterung anzuzeigen. Sie können diese Befehle verwenden, um Ihre Konfiguration zu überprüfen.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

- **show url-server**: Zeigt Informationen über den Filterserver anBeispiel:
  ```
  hostname#show url-server
  url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp
  connections 10
  ```

  Geben Sie in der Softwareversion 7.2 und höher die **show running-config url-server-**Form dieses Befehls an.
- **show url-server stats** - Zeigt Informationen und Statistiken über den Filterserver anGeben Sie für die Softwareversion 7.2 das **Statistikformular show running-config url-server** dieses Befehls ein.Geben Sie in der Softwareversion 8.0 und höher das **show url-server statistics-**Formular dieses Befehls aus.Beispiel:
  ```
  hostname#show url-server statistics

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

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

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

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

- **show url-block** - Zeigt die Konfiguration des URL-Block-Puffers anBeispiel:
```
hostname#show url-block
    url-block url-mempool 128
    url-block url-size 4
    url-block block 128
```

  Geben Sie in der Softwareversion 7.2 und höher die **show running-config url-block-**Form dieses Befehls an.
- **Statistik zu Url-Block-Blöcken anzeigen** - Zeigt die Statistiken zu URL-Blöcken anBeispiel:
```
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
```

  Geben Sie für die Softwareversion 7.2 das **Statistikformular** dieses Befehls **show running-config url-block ein**.
- **show url-cache stats** - Zeigt, wie der Cache verwendet wird.Beispiel:
```
hostname#show url-cache stats

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

  Geben Sie in Software Version 8.0 das **show url-cache statistics-**Formular dieses Befehls aus.
- **show perfmon** - Zeigt Leistungsstatistiken für die URL-Filterung zusammen mit anderen Leistungsstatistiken an. Die Filterstatistiken werden in den Zeilen URL-Zugriff und URL-Server-Anfragen angezeigt.Beispiel:
```
hostname#show perfmon

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

```
AAA Author              0/s             0/s
AAA Account             0/s             0/s
```

- **show filter** - Zeigt die Filterkonfiguration anBeispiel:
```
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
```

  Geben Sie in der Softwareversion 7.2 und höher die **Filterform show running-config** dieses Befehls ein.

# Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung bei Ihrer Konfiguration.

## Fehler: "%ASA-3-304009: Aus Pufferblöcken ausgeführt, die durch den Befehl url-block angegeben wurden."

Der URL-Cache der Firewall ist nicht mehr verfügbar. Der Server erhält Antworten, wenn die Firewall darauf wartet, vom URL-Server eine Bestätigung zu erhalten.

## Lösung

Das Problem betrifft im Wesentlichen eine Latenz zwischen der ASA und dem Websense-Server. Um dieses Problem zu beheben, versuchen Sie die folgenden Problemumgehungen.

- Versuchen Sie, das auf der ASA verwendete Protokoll in UDP zu ändern, um mit dem Websense zu kommunizieren.Es besteht ein Problem mit der Latenz zwischen dem Websense-Server und der Firewall, bei dem Antworten vom Websense-Server eine lange Zeit benötigen, um zur Firewall zurückzukehren. Dies führt dazu, dass sich der URL-Puffer füllt, während er auf eine Antwort wartet.Sie können UDP anstelle von TCP für die Kommunikation zwischen dem Websense-Server und der Firewall verwenden. Dies liegt daran, dass die ASA bei Verwendung von TCP für die URL-Filterung für jede neue URL-Anfrage eine TCP-Verbindung mit dem Websense-Server herstellen muss. Da UDP ein verbindungsloses Protokoll ist, ist die ASA nicht gezwungen, die Verbindung herzustellen, um die Antwort des Servers zu empfangen. Dies sollte die Leistung des Servers verbessern.
```
ASA(config)#url-server (inside) vendor websense host  X.X.X.X timeout 30
protocol UDP version 4 connections 5
```
- Stellen Sie sicher, dass Sie den Url-Block auf den höchstmöglichen Wert (128) erhöhen. Dies kann mit dem Befehl **show url-block** überprüft werden.Wenn 128 angezeigt wird, berücksichtigen Sie die CSCta27415 (nur registrierte **Kunden)-**Erweiterung von Cisco Bug ID.

# Zugehörige Informationen

- Produkt-Support für Cisco Adaptive Security Appliances der Serie ASA 5500
- Produkt-Support für Cisco PIX Security Appliances der Serie 500
- Cisco Adaptive Security Device Manager - Produktsupport
- PIX/ASA: Herstellen und Beheben von Verbindungen über die Cisco Security Appliance

- Fehlerbehebung bei Verbindungen über PIX und ASA
- Technischer Support und Dokumentation - Cisco Systems