PIX/ASA URL過濾配置示例

目錄

簡介

本文檔介紹如何在安全裝置上配置URL過濾。

過濾流量具有以下優點：

- 它有助於降低安全風險並防止不當使用。
- 它可以更好地控制通過安全裝置的流量。

注意：由於URL過濾是CPU密集型的，因此使用外部過濾伺服器可確保其他流量的吞吐量不會受到影響。但是，根據網路速度和URL過濾伺服器的容量，使用外部過濾伺服器過濾流量時，初始連線所需的時間可能會明顯較慢。

注意：不支援從較低安全級別到較高安全級別的過濾。URL過濾僅適用於傳出流量，例如，源自高安全介面且目的地為低安全介面上伺服器的流量。

必要條件

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX 500系列安全裝置（版本6.2及更高版本）
- ASA 5500系列安全裝置（版本7.x及更高版本）
- 調適型安全裝置管理員(ASDM)6.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

您可以過濾來自更安全網路的連線請求，將其傳送到安全性較低的網路。雖然可以使用訪問控制清單(ACL)來阻止對特定內容伺服器的出站訪問，但由於Internet的規模和動態性質，很難通過這種方式管理使用情況。您可以使用運行以下網際網路過濾產品之一的獨立伺服器來簡化配置並提高安全裝置的效能：

- Websense Enterprise — 過濾HTTP、HTTPS和FTP。PIX防火牆版本5.3及更高版本支援此功能。
- Secure Computing SmartFilter（以前稱為N2H2） — 過濾HTTP、HTTPS、FTP和長URL過濾。PIX防火牆版本6.2及更高版本支援此功能。

與使用訪問控制清單相比，這減少了管理任務並提高了過濾效率。此外，由於URL過濾是在單獨的平台上處理的，因此PIX防火牆的效能受到的影響要小得多。但是，當過濾伺服器與安全裝置處於遠端狀態時，使用者可能會注意到訪問網站或FTP伺服器的時間更長。

PIX防火牆使用URL過濾伺服器上定義的策略檢查出站URL請求。PIX防火牆根據過濾伺服器的響應允許或拒絕連線。

當啟用過濾並通過安全裝置定向內容請求時，該請求將同時傳送到內容伺服器和過濾伺服器。如果過濾伺服器允許連線，安全裝置會將來自內容伺服器的響應轉發到發出請求的客戶端。如果過濾伺服器拒絕連線，安全裝置將丟棄響應並傳送指示連線不成功的消息或返回代碼。

如果在安全裝置上啟用使用者身份驗證，則安全裝置還會將使用者名稱傳送到過濾伺服器。過濾伺服器可以使用使用者特定的過濾設定，或者提供有關使用情況的增強報告。

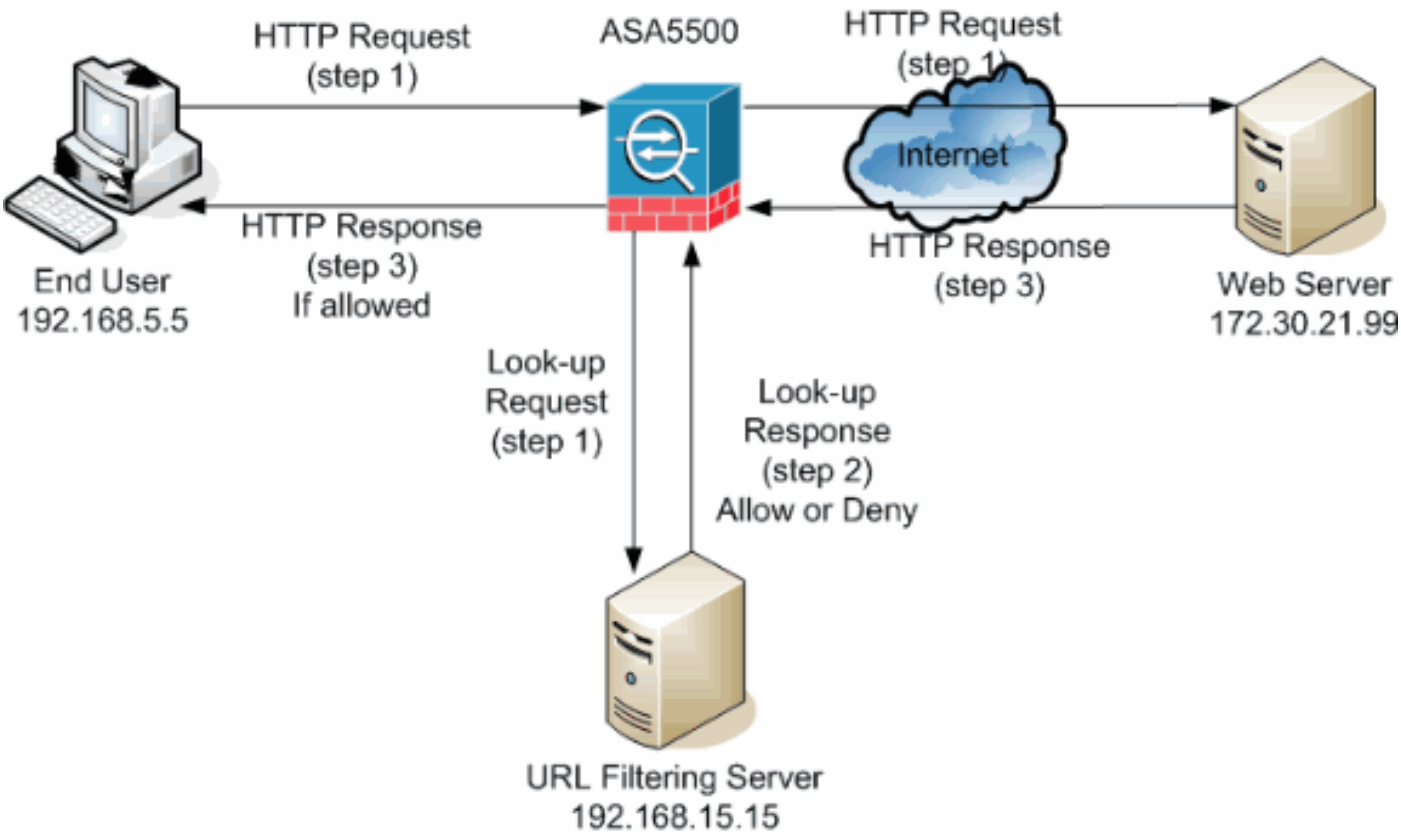
使用CLI配置ASA/PIX

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



在此範例中，URL過濾伺服器位於DMZ網路中。位於網路內部的終端使用者嘗試通過Internet訪問位於網路外部的Web伺服器。

在使用者請求Web伺服器期間完成以下步驟：

1. 終端使用者瀏覽到Web伺服器上的頁面，然後瀏覽器傳送HTTP請求。
2. 安全裝置收到此請求後，會將該請求轉發到Web伺服器，同時提取URL並向URL過濾伺服器傳送查詢請求。
3. URL過濾伺服器收到查詢請求後，會檢查其資料庫，以確定是允許還是拒絕URL。它會返回permit或deny狀態，並向Cisco IOS®防火牆作出查詢響應。
4. 安全裝置收到此查詢響應並執行下列功能之一：如果查詢響應允許URL，則會將HTTP響應傳送給終端使用者。如果查詢響應拒絕URL，則URL過濾伺服器會將使用者重定向到其自己的內部Web伺服器，該伺服器將顯示一條消息，說明阻止URL的類別。此後，在兩端重置連線。

確定過濾伺服器

您需要使用**url-server**命令識別過濾伺服器的地址。您必須根據所使用的過濾伺服器型別使用此命令的相應形式。

註：對於軟體版本7.x及更高版本，您最多可以為每個環境確定四個過濾伺服器。安全裝置按順序使用伺服器，直到伺服器作出響應。在配置中只能配置單一型別的伺服器，即Websense或N2H2。

Websense

Websense是一個第三方過濾軟體，可以根據以下策略過濾HTTP請求：

- 目標主機名
- 目的IP地址

- 關鍵字
- 使用者名稱

該軟體維護著一個包含2000多萬個站點的URL資料庫，這些站點被劃分為60多個類別和子類別。

- 軟體版本6.2:

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

url-server命令指定運行N2H2或Websense URL過濾應用程式的伺服器。限製為16個URL伺服器。但是，一次只能使用一個應用程式，可以是N2H2或Websense。此外，如果您更改PIX防火牆上的配置，它不會更新應用伺服器上的配置。此操作必須根據各個供應商的說明單獨完成。

- 軟體版本7.x及更高版本：

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

用連線到過濾伺服器的安全裝置介面名稱替換if_name。預設值為inside。用過濾伺服器的IP地址替換local_ip。將seconds替換為安全裝置必須繼續嘗試連線到過濾伺服器的秒數。

使用protocol選項指定您要使用TCP還是UDP。使用Websense伺服器，您還可以指定要使用的TCP。TCP第1版是預設值。如果PIX防火牆已經對使用者進行了身份驗證，TCP版本4允許PIX防火牆向Websense伺服器傳送經過身份驗證的使用者名稱和URL日誌記錄資訊。

例如，若要識別單個Websense過濾伺服器，請發出以下命令：

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

安全計算SmartFilter

- PIX版本6.2:

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

- 軟體版本7.0和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]]
```

- 軟體版本7.2及更高版本：

```
hostname(config)#url-server (if_name) vendor {secure-computing | n2h2} host
```

對於供{secure-computing | n2h2},您可以將安全供應商字串。但是，n2h2受向後相容性。當生成配置條目時，將儲存為供應商字串。

用連線到過濾伺服器的安全裝置介面名稱替換if_name。預設值為inside。將local_ip替換為過濾伺服器的IP地址，將port <number>替換為所需的埠號。

注意：安全計算SmartFilter伺服器用於通過TCP或UDP與安全裝置通訊的預設埠是埠4005。

將seconds替換為安全裝置必須繼續嘗試連線到過濾伺服器的秒數。使用protocol選項指定您要使用TCP還是UDP。

connections <number>是嘗試在主機和伺服器之間建立連線的次數。

例如，要標識單個N2H2過濾伺服器，請發出以下命令：

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

或者，如果要使用預設值，請發出以下命令：

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

配置過濾策略

注意：在啟用URL過濾之前，必須標識並啟用URL過濾伺服器。

啟用URL篩選

當過濾伺服器批准HTTP連線請求時，安全裝置允許來自Web伺服器的回復到達發起該請求的客戶端。如果過濾伺服器拒絕該請求，安全裝置會將使用者重定向到指示訪問被拒絕的阻止頁面。

發出**filter url**命令，以設定用於篩選URL的策略：

- PIX版本6.2:

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

- 軟體版本7.x及更高版本：

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

如果使用與HTTP(80)的預設埠不同的埠，則將port替換為要過濾HTTP流量的埠號。要標識埠號範圍，請輸入以連字元分隔的範圍的開始和結束。

啟用過濾後，安全裝置會停止出站HTTP流量，直到過濾伺服器允許連線。如果主過濾伺服器沒有響應，安全裝置會將過濾請求定向到輔助過濾伺服器。allow選項會導致安全裝置在主過濾伺服器不可用時轉發HTTP流量而不進行過濾。

發出**proxy-block**命令，以刪除對代理伺服器的所有請求。

註：其餘引數用於截斷長URL。

截斷長HTTP URL

longurl-truncate選項會導致安全裝置在URL長於允許的最大長度時，僅將URL的主機名或IP地址部分傳送給過濾伺服器，以便進行評估。

使用longurl-deny選項，在URL超過允許的最大值時拒絕出站URL流量。

使用cgi-truncate選項可截斷CGI URL，使其僅包含CGI指令碼位置和指令碼名稱，而不包含任何引數。

以下是一般過濾器組態範例：

```
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
```

免除流量過濾

如果要對常規過濾策略設定例外，請發出以下命令：

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

使用要免除過濾限制的使用者或子網的IP地址和子網掩碼替換local_ip和local_mask。

使用要免除過濾限制的伺服器或子網的IP地址和子網掩碼替換foreign_ip和foreign_mask。

例如，此命令會導致從內部主機發往172.30.21.99的所有HTTP請求被轉發到過濾伺服器，來自主機192.168.5.5的請求除外：

以下是例外情況的組態範例：

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

進階URL篩選

本節提供有關高級過濾引數的資訊，包括以下主題：

- 緩衝
- 快取
- 長URL支援

緩衝Web伺服器響應

當使用者發出連線到內容伺服器的請求時，安全裝置會同時將該請求傳送到內容伺服器和過濾伺服器。如果過濾伺服器在內容伺服器之前沒有響應，則伺服器響應將被丟棄。這會從Web客戶端的角度延遲Web伺服器響應，因為客戶端必須重新發出請求。

如果啟用HTTP響應緩衝區，來自Web內容伺服器的響應將被緩衝，並且如果過濾伺服器允許連線，響應將被轉發到發出請求的客戶端。這可以防止否則可能發生的延遲。

為了緩衝對HTTP請求的響應，請完成以下步驟：

1. 要對等待來自過濾伺服器的響應的HTTP請求啟用緩衝功能，請發出以下命令：
   ```
   hostname(config)#url-block block block-buffer-limit
   ```
   將`block-buffer-limit`替換為要緩衝的最大塊數。
2. 若要設定可用的最大記憶體來緩衝待定URL，以及使用Websense緩衝長URL，請發出以下命令：
   ```
   hostname(config)#url-block url-mempool memory-pool-size
   ```
   將`memory-pool-size`替換為2到10240之間的值，以使最大記憶體分配為2 KB到10 MB。

快取伺服器地址

在使用者訪問站點後，只要該地址上託管的每個站點都屬於在所有時間都允許的類別，過濾伺服器就可以允許安全裝置快取伺服器地址一定時間。然後，當使用者再次訪問伺服器，或者如果其他使用者訪問伺服器，安全裝置就不需要再次查詢過濾伺服器。

如果需要提高吞吐量，請發出**url-cache**命令：

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

將`size`替換為1到128(KB)範圍內的快取大小值。

使用`dst`關鍵字可根據URL目標地址快取條目。如果所有使用者在Websense伺服器上共用相同的URL過濾策略，則選擇此模式。

使用`src_dst`關鍵字可根據起始URL請求的源地址和URL目標地址快取條目。如果使用者在Websense伺服器上沒有共用同一URL過濾策略，請選擇此模式。

啟用長URL過濾

預設情況下，如果HTTP URL超過1159個字元，安全裝置會將其視為長URL。您可以使用以下命令增加單個URL允許的最大長度：

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

將`long-url-size`替換為要緩衝的每個長URL的最大大小(KB)。

例如，以下命令配置安全裝置以進行高級URL過濾：

```
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
```

組態

此組態包括本檔案所述的命令：

ASA 8.0配置

```
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
```

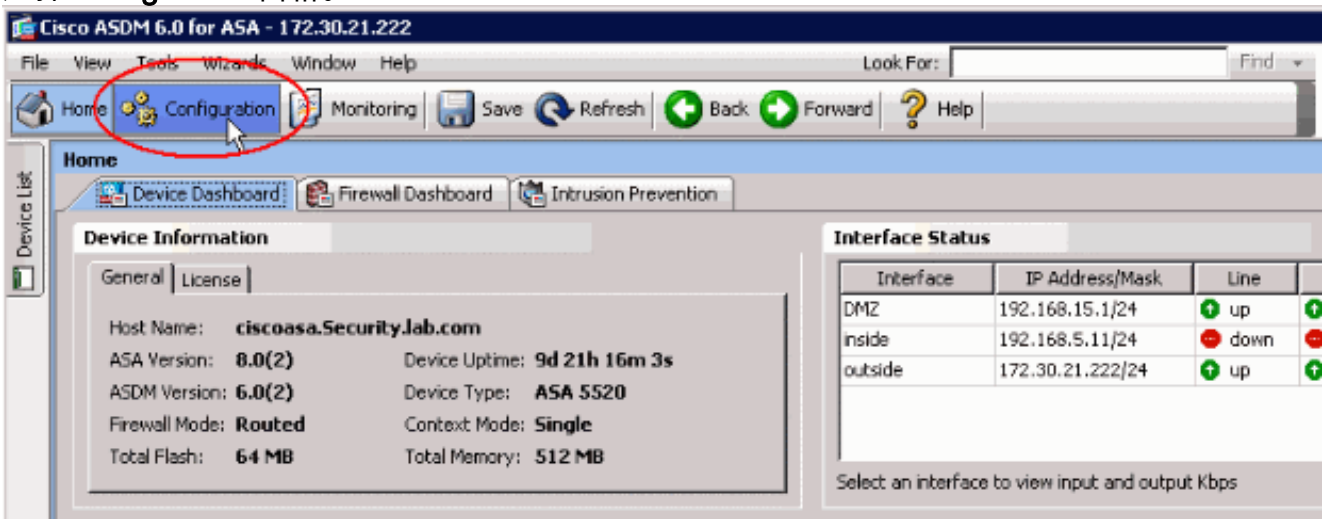
```
dhcpd address 192.168.5.12-192.168.5.20 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect 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
```

使用ASDM配置ASA/PIX

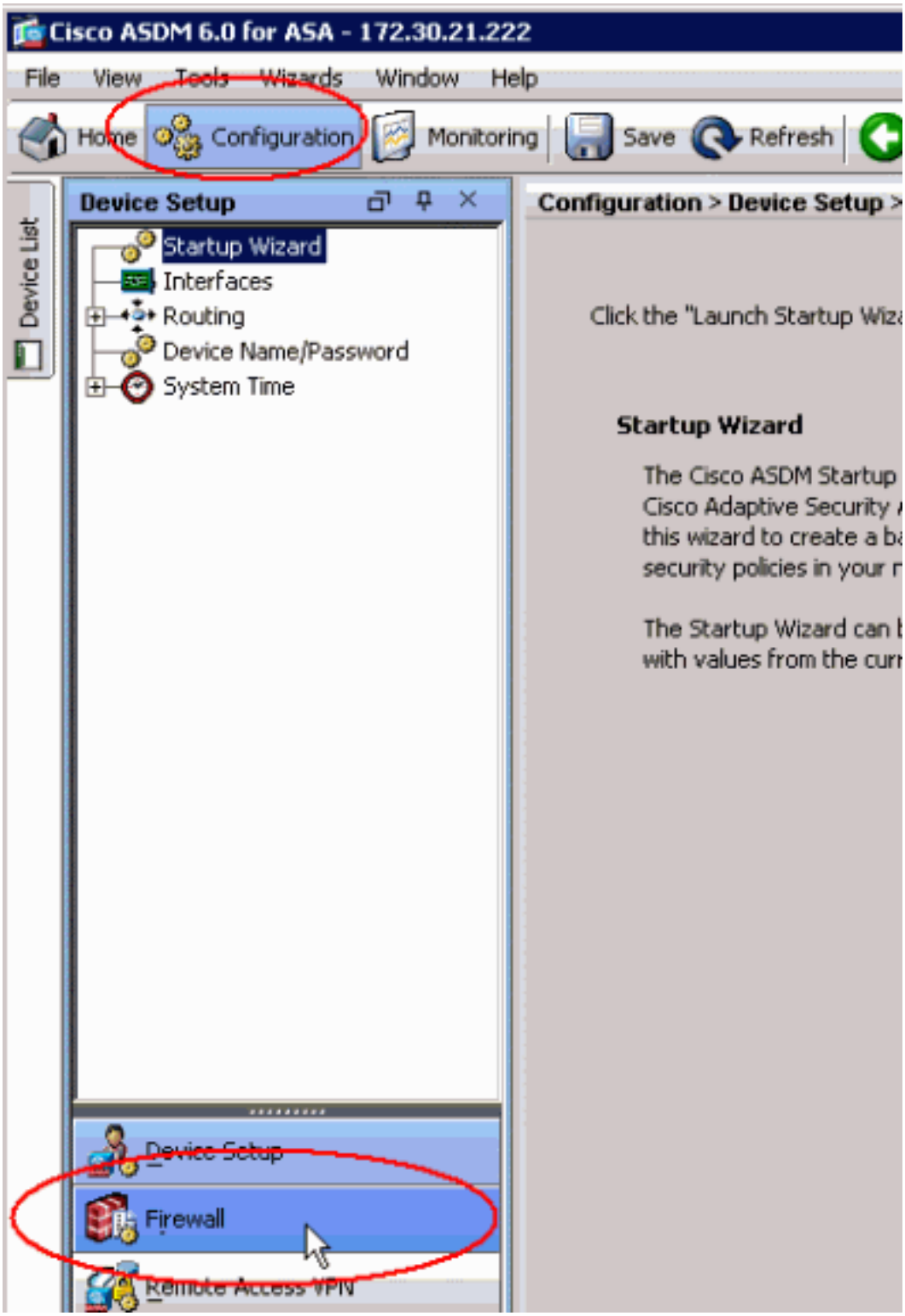
本節演示如何使用自適應安全裝置管理器(ASDM)為安全裝置配置URL過濾。

啟動ASDM後，請完成以下步驟：

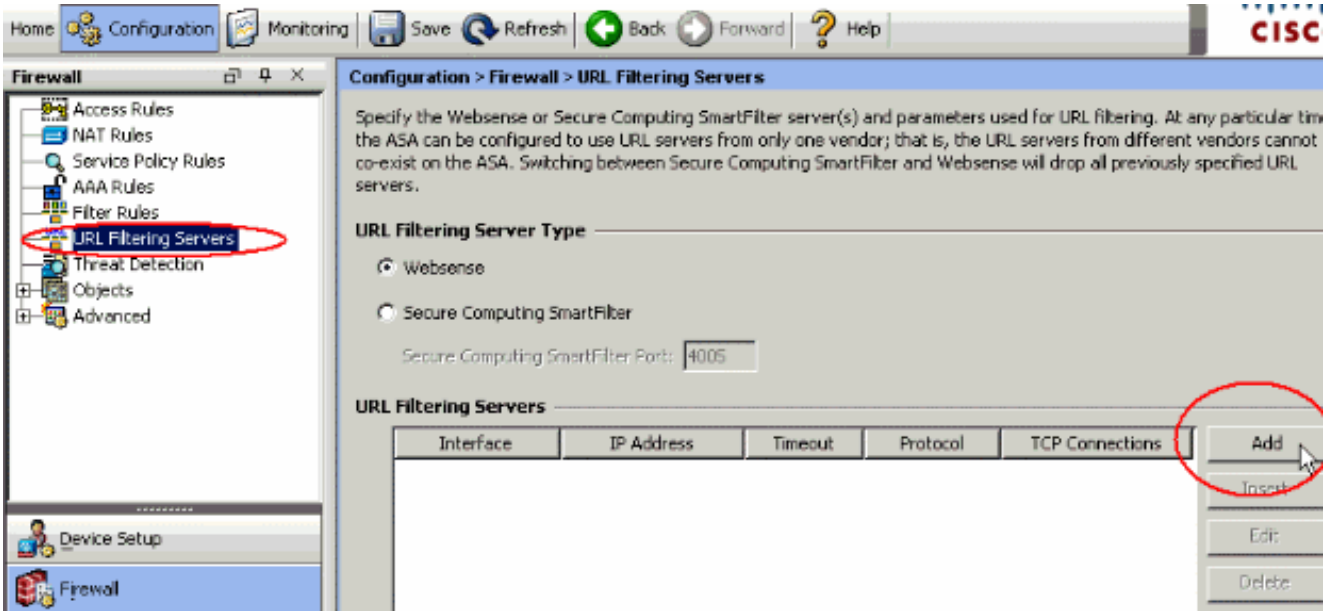
1. 選擇**Configuration**窗格。



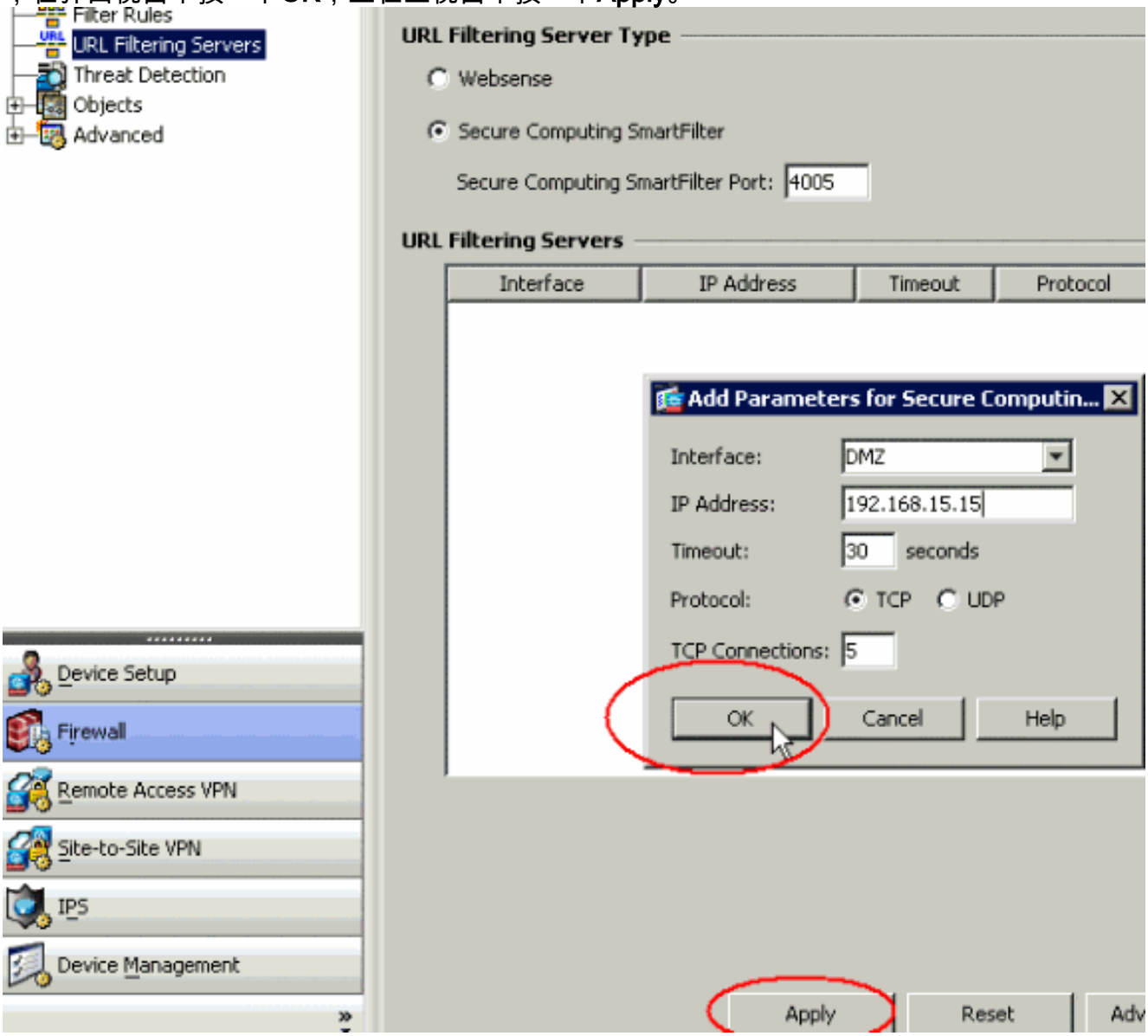
2. 在**Configuration**窗格中顯示的清單中按一下**Firewall**。



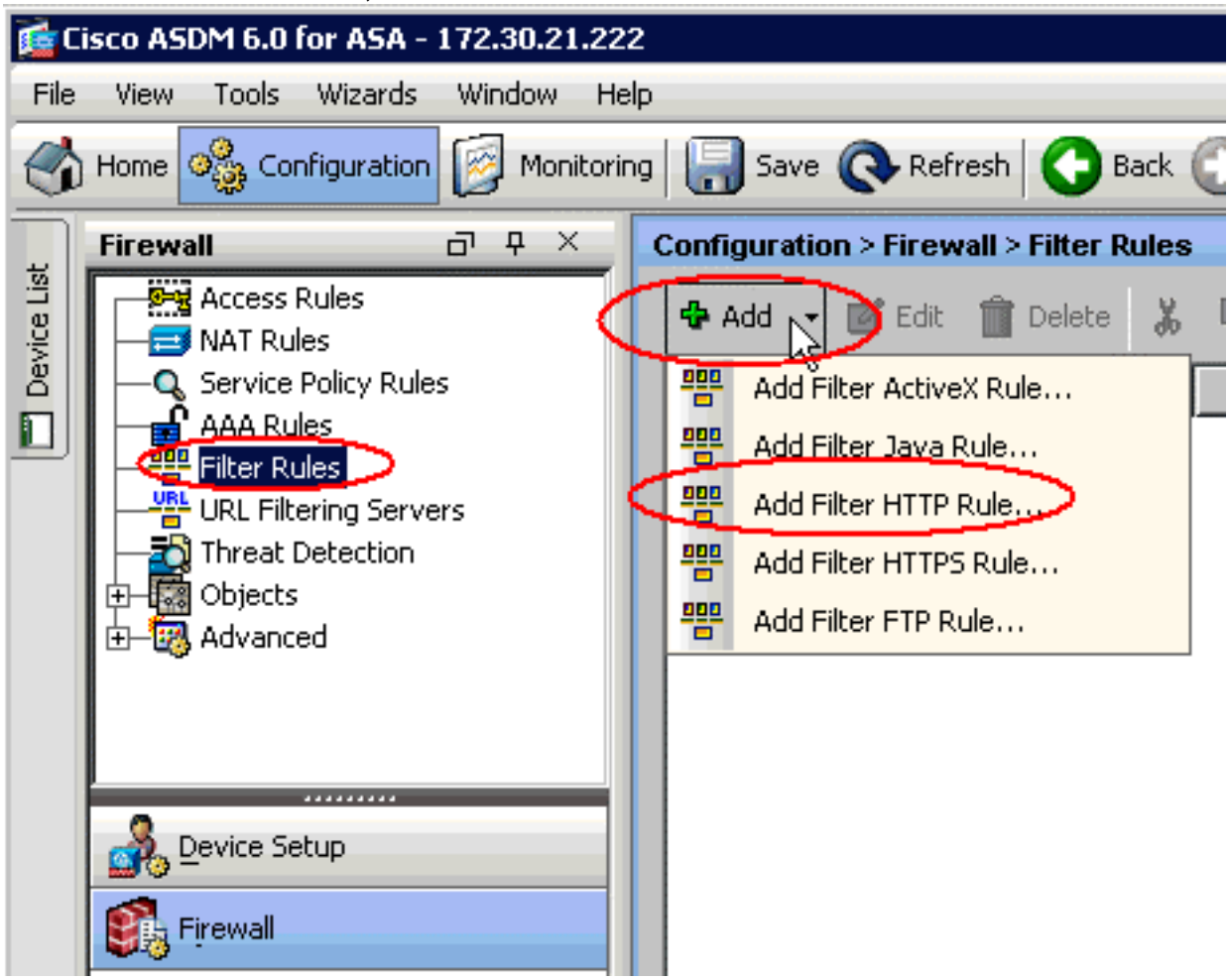
3. 在「**Firewall**」下拉選單中，選擇「**URL Filtering Servers**」。選擇要使用的URL過濾伺服器型別，然後按一下**Add**以配置其引數。**注意**：必須先新增過濾伺服器，然後才能為HTTP、HTTPS或FTP過濾規則配置過濾。



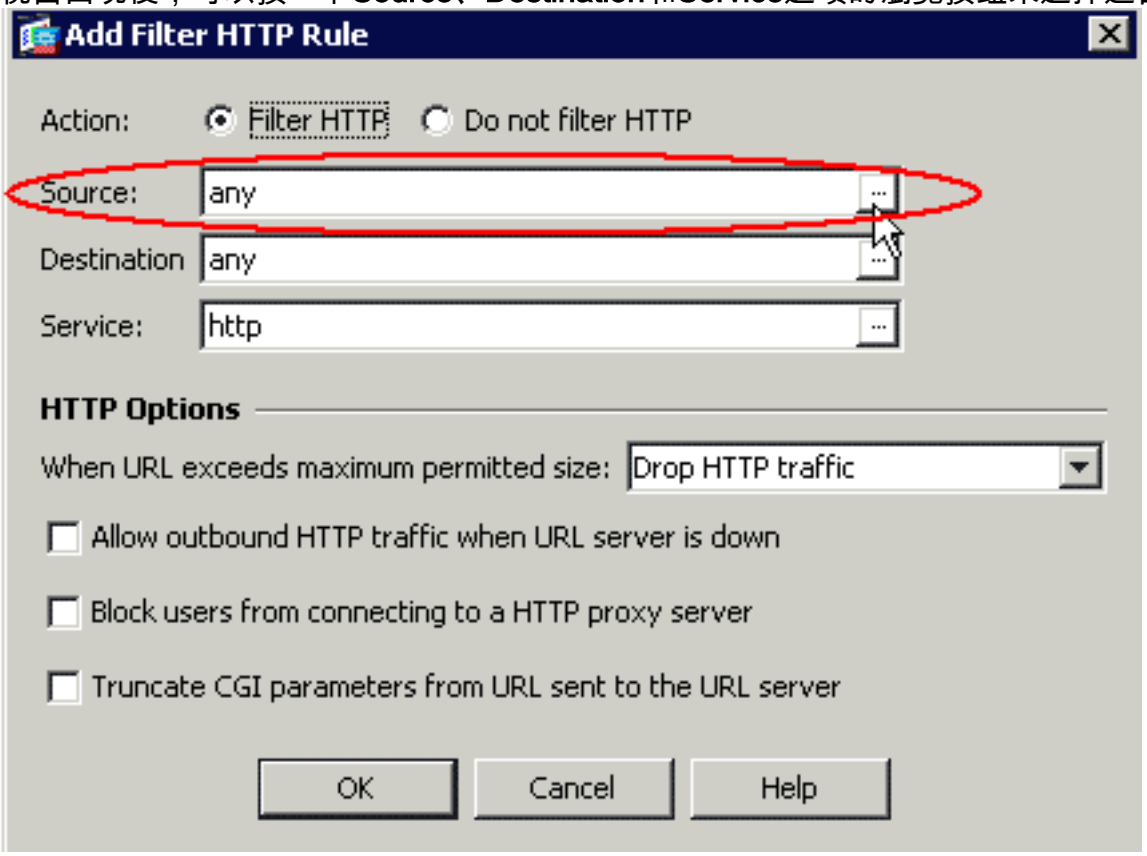
4. 在彈出視窗中選擇相應的引數：Interface — 顯示連線到過濾伺服器的介面IP Address — 顯示過濾伺服器的IP地址Timeout — 顯示向過濾伺服器的請求超時之前的秒數Protocol — 顯示用於與過濾伺服器通訊的協定。TCP第1版是預設值。如果PIX防火牆已經對使用者進行了身份驗證，TCP版本4允許PIX防火牆向Websense伺服器傳送經過身份驗證的使用者名稱和URL日誌記錄資訊TCP Connections — 顯示允許與URL過濾伺服器通訊的最大TCP連線數輸入引數後，在彈出視窗中按一下**OK**，並在主視窗中按一下**Apply**。



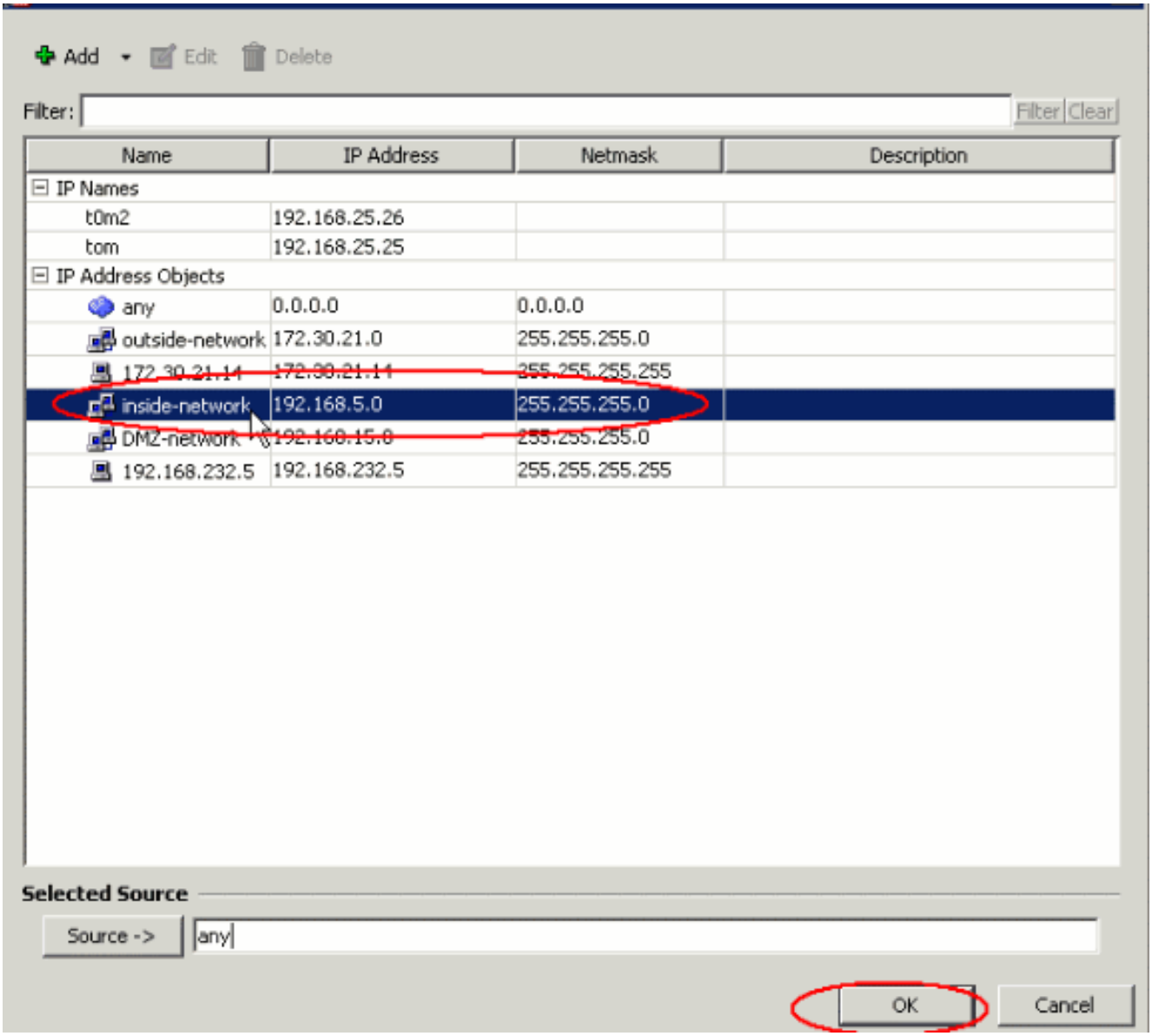
5. 在「Firewall」下拉式清單中選擇「Filter Rules」。按一下主視窗中的Add按鈕，選擇要新增的規則型別。在本示例中，選擇了Add Filter HTTP Rule。



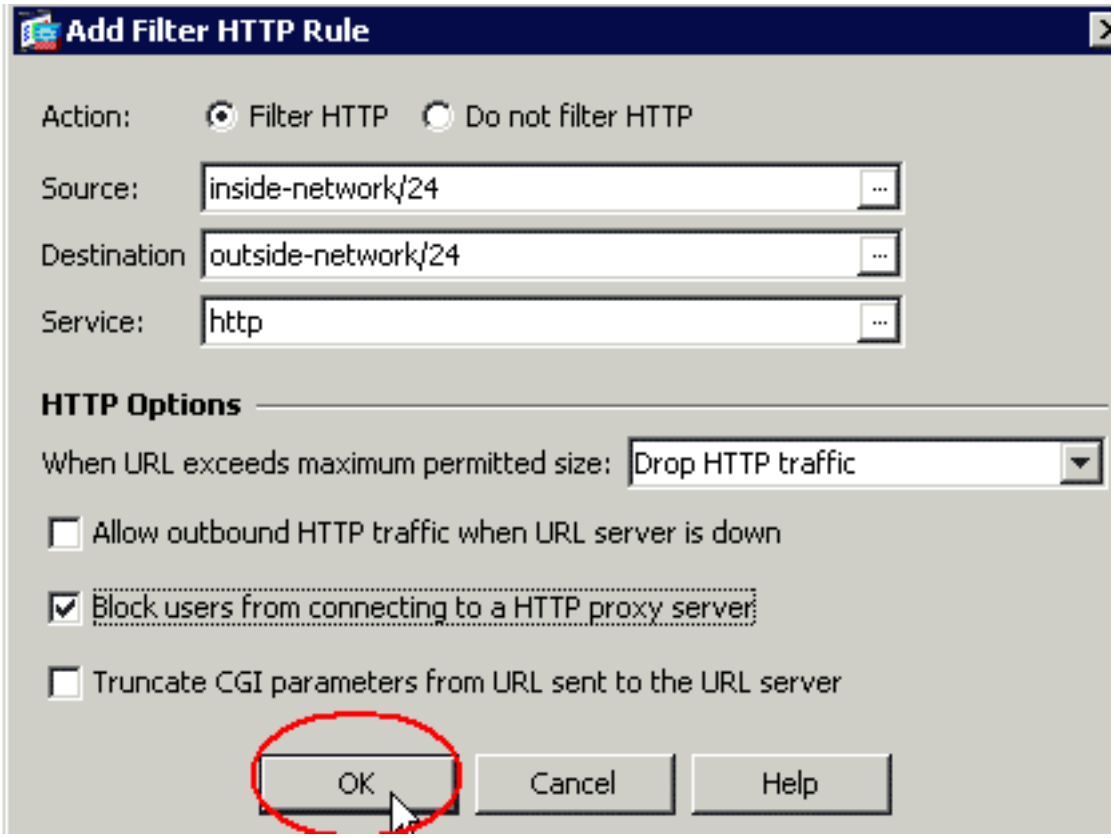
6. 彈出視窗出現後，可以按一下Source、Destination和Service選項的瀏覽按鈕來選擇適當的引數。



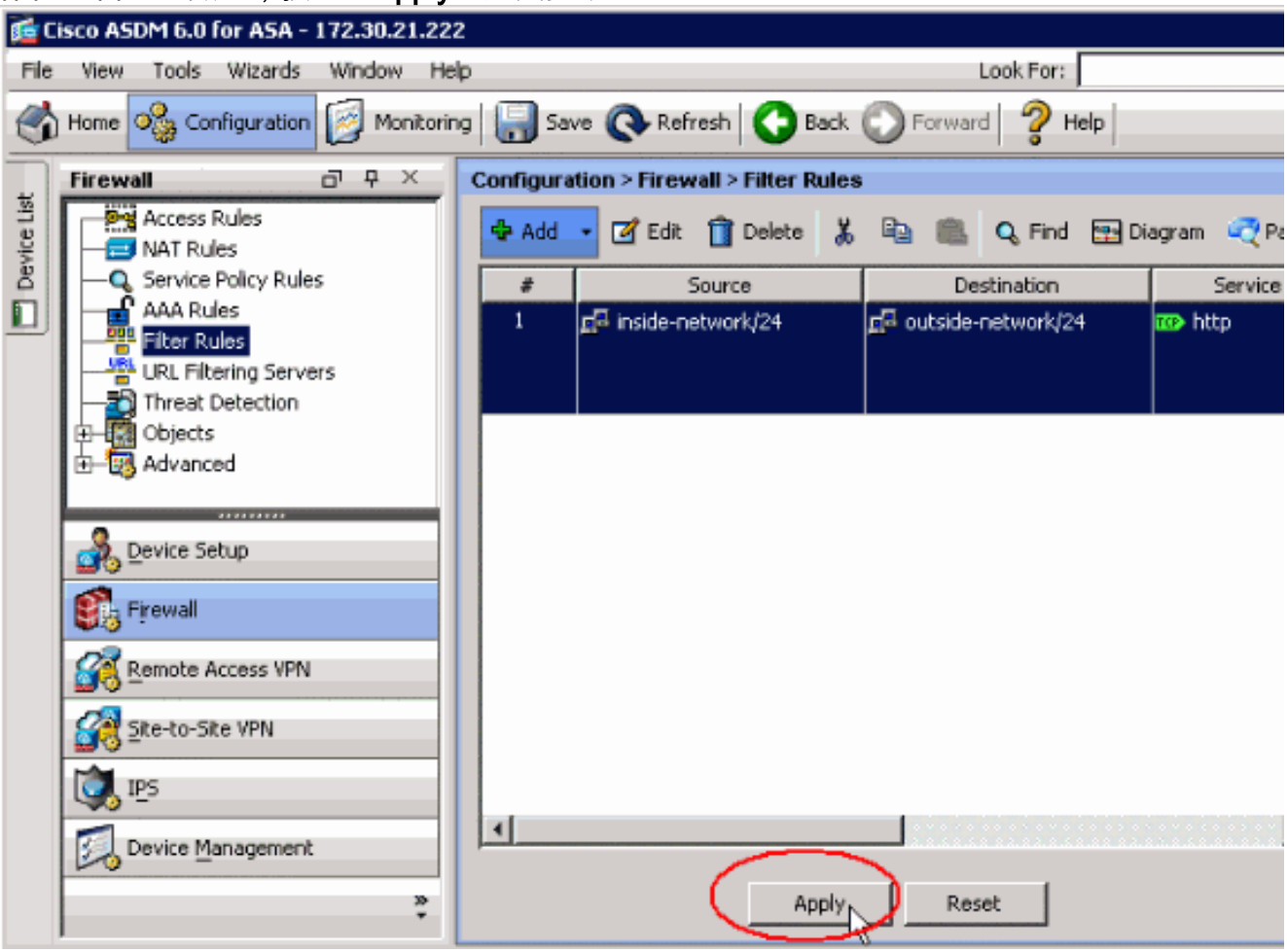
7. 這顯示了Source選項的瀏覽視窗。進行選擇，然後按一下OK。



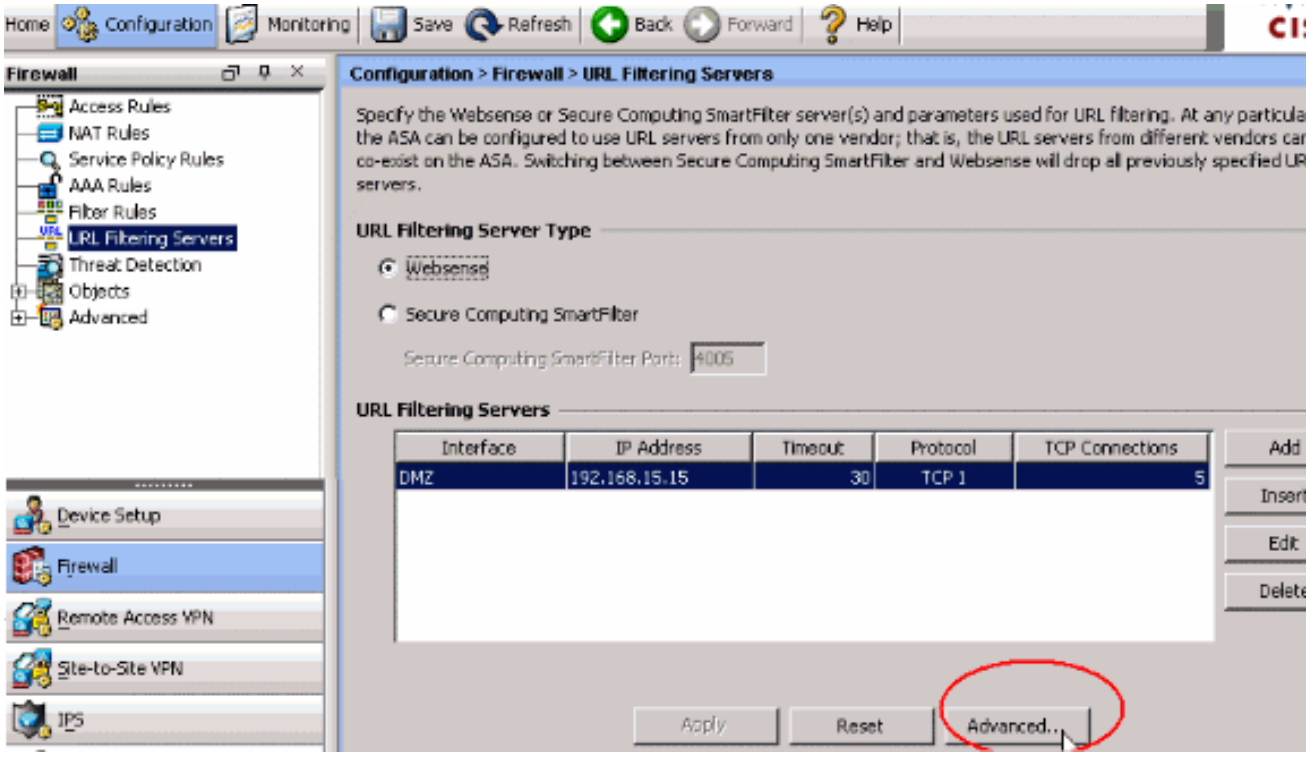
8. 完成所有引數的選擇後，按一下**OK**繼續。



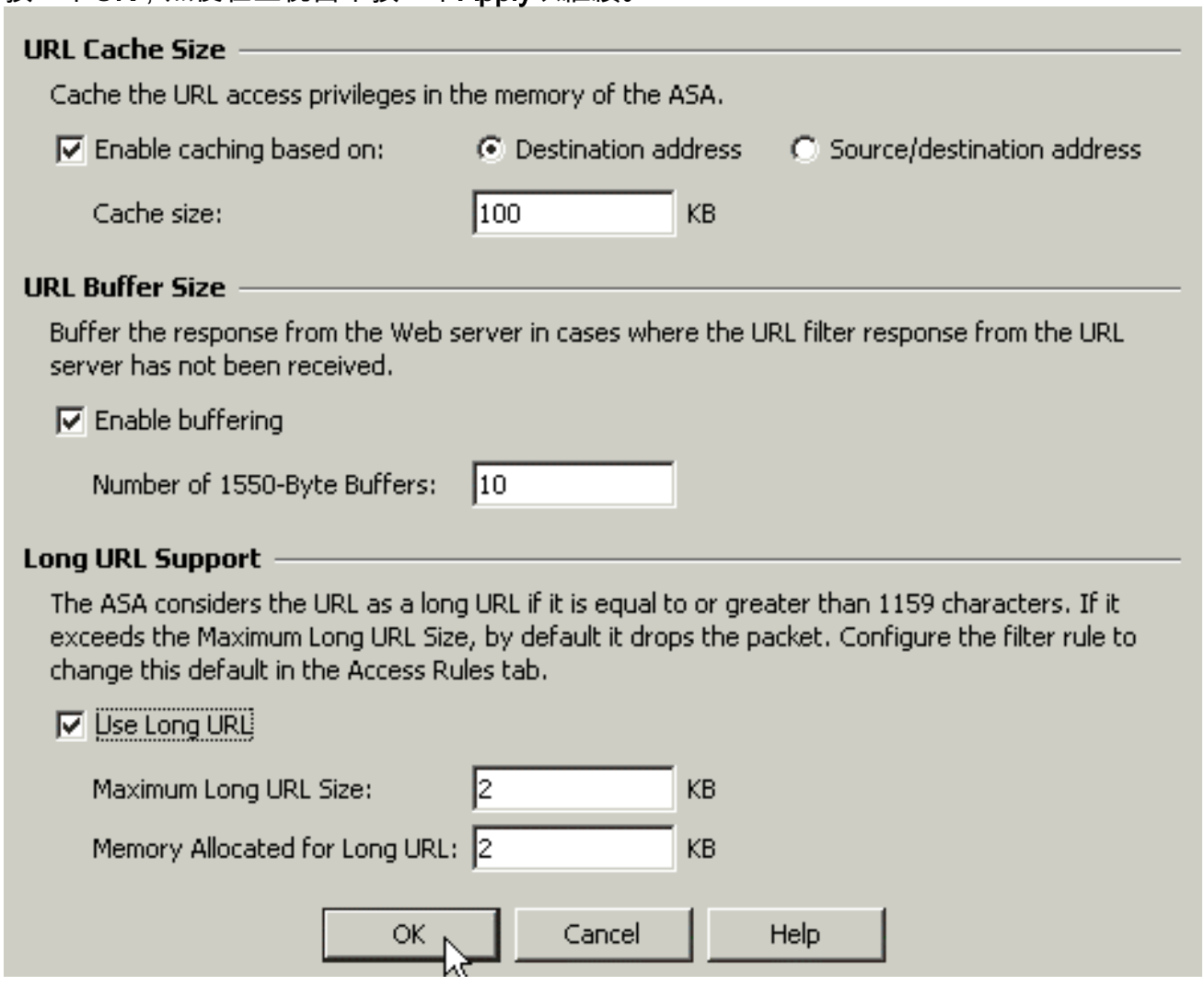
9. 配置適當的引數後，按一下**Apply**以提交更改。



10. 對於高級URL過濾選項，請再次從**Firewall**下拉選單中選擇**URL Filtering Servers**，然後按一下主視窗中的**Advanced**按鈕。



11. 在彈出視窗中配置引數，例如URL快取大小、URL緩衝區大小和長URL支援。在彈出視窗中按一下**OK**，然後在主視窗中按一下**Apply**以繼續。



12. 最後，確保在終止ASDM會話之前儲存所做的更改。

驗證

使用本節中的命令可檢視URL過濾資訊。您可以使用以下命令驗證設定。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**指令輸出的分析。

- **show url-server** — 顯示有關過濾伺服器的資訊例如：

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

在軟體版本7.2和更新版本中，發出此命令的**show running-config url-server**形式。

- **show url-server stats** — 顯示有關過濾伺服器的資訊和統計資訊對於軟體版本7.2，請發出此命令的**show running-config url-server statistics**形式。在軟體版本8.0及更高版本中，發出此命令的**show url-server statistics**形式。例如：

```
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** — 顯示URL塊緩衝區的配置例如：

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

```
    url-block block 128
```

在軟體版本7.2和更新版本中，發出此命令的**show running-config url-block**形式。

- **show url-block block statistics** — 顯示URL塊統計資訊例如：

```
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
```

對於軟體版本7.2，請發出此命令的**show running-config url-block block statistics**形式。

- **show url-cache stats** — 顯示如何使用快取例如：

```
hostname#show url-cache stats

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

在軟體版本8.0中，發出此命令的**show url-cache statistics**形式。

- **show perfmon** — 顯示URL過濾效能統計資訊以及其他效能統計資訊。過濾統計資訊顯示在「URL訪問」和「URL伺服器請求」行中。例如：

```
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** — 顯示過濾配置例如：

```
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
```

在軟體版本7.2和更新版本中，發出此命令的**show running-config filter**形式。

疑難排解

本節提供有關如何對配置進行故障排除的資訊。

錯誤：%ASA-3-304009:URL-block命令"指定的緩衝區塊已用盡

當防火牆等待從URL伺服器獲取確認時，用於儲存伺服器答覆的URL快取將用盡。

解決方案

此問題基本上與ASA和Websense伺服器之間的延遲有關。若要解決此問題，請嘗試以下解決方法。

- 嘗試將ASA上使用的協定更改為UDP，以便與Websense通訊。Websense伺服器和防火牆之間存在延遲問題，來自Websense伺服器的回覆需要很長時間才能返回到防火牆，因此這會導致URL緩衝區在等待響應時過滿。Websense伺服器和防火牆之間的通訊可以使用UDP而不是TCP。這是因為當您將TCP用於URL過濾時，對於每個新URL請求，ASA需要與Websense伺服器建立TCP連線。由於UDP是無連線協定，因此ASA不會被迫建立連線以接收伺服器的響應。這應會提高伺服器的效能。
  ```
  ASA(config)#url-server (inside) vendor websense host  X.X.X.X timeout 30
  protocol UDP version 4 connections 5
  ```
- 確保將url-block塊增大到可能的最大值，即128。可以使用**show url-block**命令檢查此值。如果顯示128，請考慮Cisco錯誤ID CSCta27415(僅限註冊客戶)增強功能。

相關資訊

- Cisco ASA 5500系列自適應安全裝置產品支援
- Cisco PIX 500系列安全裝置產品支援
- Cisco Adaptive Security Device Manager產品支援
- PIX/ASA:通過思科安全裝置建立連線並排除連線故障
- 排除通過PIX和ASA的連線故障
- 技術支援與文件 - Cisco Systems