PIX/ASA URL过滤配置示例

目录

简介

本文档将介绍如何在安全设备上配置 URL 过滤。

对流量进行过滤有以下优点：

- 有助于降低安全风险，防止滥用网络资源。
- 可以提高对安全设备流量的控制能力。

注意： 由于 URL 过滤比较占用 CPU，因此使用外部过滤服务器可确保其他数据流的吞吐量不受影响。但是，根据您的网络速度和 URL 过滤服务器的容量，使用外部过滤服务器过滤流量时，初始连接所需的时间可能会明显加长。

注意： 不支持从较低安全级别到较高安全级别的过滤。URL 过滤只适用于出站流量，例如，来自安全级别较高的接口，发往服务器上安全级别较低的接口的流量。

先决条件

使用的组件

本文档中的信息基于以下软件和硬件版本：

- PIX 500 系列安全设备（安装了软件版本 6.2 或更高版本）
- ASA 5500 系列安全设备（安装了软件版本 7.x 或更高版本）
- 自适应安全设备管理器 (ASDM) 6.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

您可以过滤从较高安全级别网络发往较低安全级别网络的连接请求。尽管您可以使用访问控制列表 (ACL) 来防止针对特定内容服务器的出站访问，但由于 Internet 的规模和动态特性，很难管理这种使用方式。您可以通过在单独的服务器上运行以下任意 Internet 过滤产品，来简化配置并改善安全设备的性能：

- Websense Enterprise — 能够过滤 HTTP、HTTPS 和 FTP。PIX 防火墙 5.3 及更高版本支持该产品。
- Secure Computing SmartFilter（以前称为 N2H2）— 能够过滤 HTTP、HTTPS、FTP 以及长 URL 过滤。PIX 防火墙 6.2 及更高版本支持该产品。

与使用访问控制列表相比，这会减少管理任务并改善过滤效果。此外，由于 URL 过滤是在单独的平台上进行的，对 PIX 防火墙性能的影响会大大减少。但是，如果过滤服务器与安全设备距离较远，用户可能会注意到，访问网站或 FTP 服务器的速度会降低。

PIX 防火墙使用 URL 过滤服务器上定义的策略来检查出站 URL 请求。PIX 防火墙会根据过滤服务器的响应来允许或拒绝连接。

如果启用了过滤功能，并且针对内容的请求通过安全设备进行定向，该请求将被同时发送到内容服务器和过滤服务器。如果过滤服务器允许连接，安全设备会将内容服务器的响应转发到发出请求的客户端。如果过滤服务器拒绝连接，安全设备将丢弃响应，并发送一条消息或返回代码，表明连接不成功。

如果安全设备上启用了用户认证，安全设备还会将用户名发送给过滤服务器。过滤服务器可以使用针对特定用户的过滤设置或提供增强的使用情况报告。

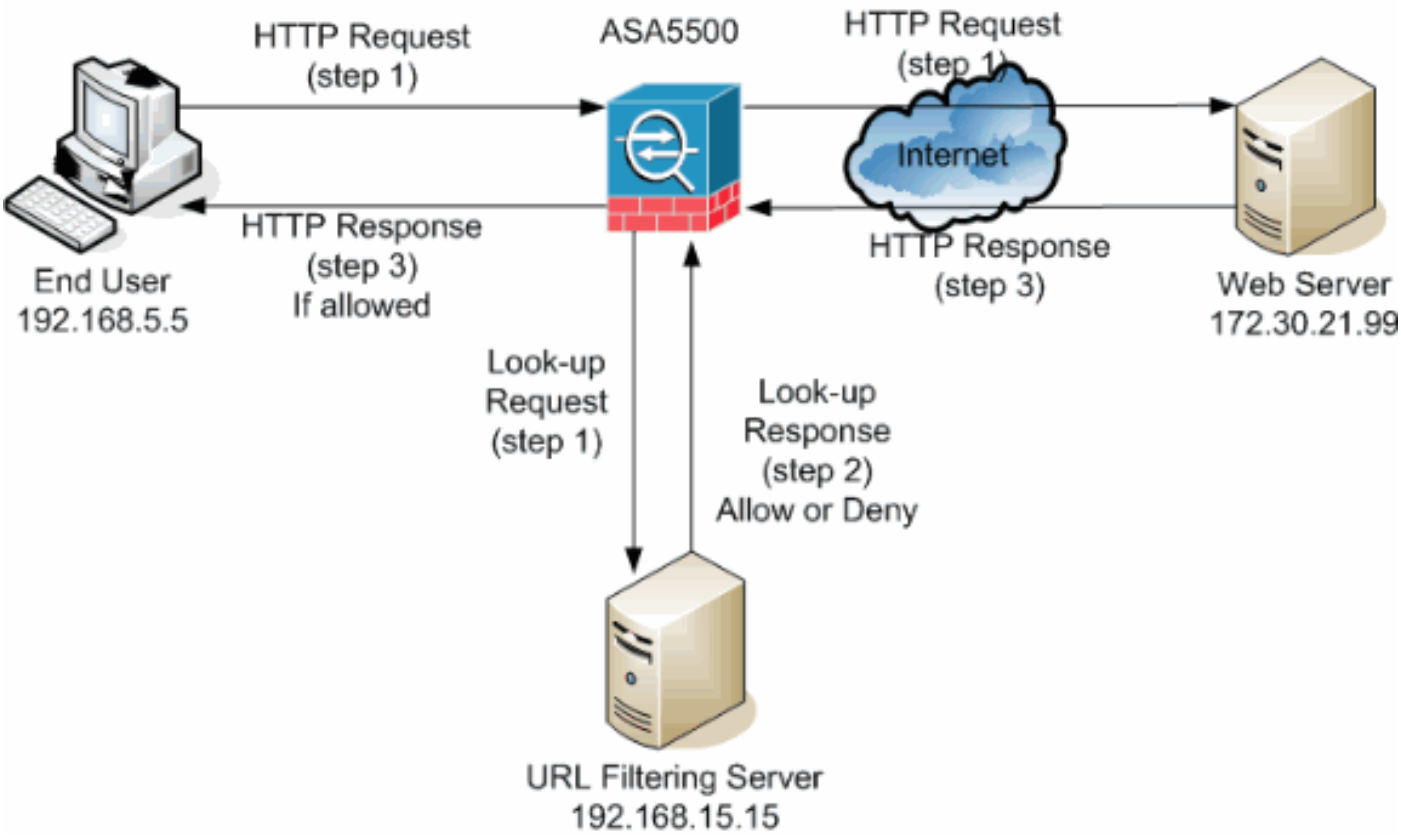
使用 CLI 配置 ASA/PIX

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



在本示例中，URL 过滤服务器位于 DMZ 网络中。网络内部的最终用户尝试通过 Internet 访问网络外部的 Web 服务器。

在用户请求访问 Web 服务器时，会完成以下步骤：

1. 最终用户浏览到 Web 服务器上的某个页面，然后浏览器发送 HTTP 请求。
2. 安全设备收到此请求后，会将请求转发给 Web 服务器，同时提取 URL 并向 URL 过滤服务器发送查找请求。
3. URL 过滤服务器收到查找请求后，检查其数据库以确定是允许还是拒绝该 URL。URL 过滤服务器对 Cisco IOS® 防火墙做出查找响应，同时返回允许或拒绝状态。
4. 安全设备收到此查找响应后，执行以下某项功能：如果查找响应允许该 URL，则向最终用户发送 HTTP 响应。如果查找响应拒绝该 URL，则 URL 过滤服务器将用户重定向到自己的内部 Web 服务器，此服务器将显示一条消息，说明该 URL 的阻止类别。然后，两端的连接都将重置。

标识过滤服务器

您需要使用 **url-server** 命令来识别过滤服务器的地址。必须根据所使用的过滤服务器的类型以适当的形式使用此命令。

注意： 对于软件版本 7.x 及更高版本，您最多可以为每个上下文识别四个过滤服务器。安全设备将依次使用这些服务器，直到某个服务器做出响应。在您的配置中，您只能采用一种服务器类型，即 Websense 或 N2H2。

Websense

Websense 是一种可根据以下策略过滤 HTTP 请求的第三方过滤软件：

- 目标主机名
- 目的 IP 地址
- 关键字
- 用户名

此软件维护有一个 URL 数据库，该数据库拥有超过 2 千万个站点，并将这些站点归入 60 多种类别和子类别。

- 软件版本 6.2：
  `url-server [(if_name)] vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP} version]` **url-server** 命令可指定运行 N2H2 或 Websense URL 过滤应用程序的服务器。上限为 16 个 URL 服务器。但是，您每次只能使用一个应用程序：N2H2 或 Websense。此外，如果您更改 PIX 防火墙上的配置，应用程序服务器上的配置并不会更新。必须根据相应供应商的指示，分别完成更改配置操作。
- 软件版本 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] ]`

用连接到过滤服务器的安全设备接口的名称替换 if_name。默认名称是 inside。用过滤服务器的 IP 地址替换 local_ip。用安全设备必须持续尝试连接过滤服务器的秒数替换 seconds。

使用 protocol 选项指定要使用 TCP 还是 UDP。对于 Websense 服务器，您还可以指定要使用的 TCP 的 version。默认值为 TCP 版本 1。如果 PIX 防火墙已对用户进行了认证，TCP 版本 4 还允许 PIX 防火墙将已认证的用户名和 URL 日志记录信息发送给 Websense 服务器。

例如，要识别单个 Websense 过滤服务器，请发出以下命令：

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

Secure Computing SmartFilter

- PIX 版本 6.2：`pix(config)#`**`url-server [(if_name)] vendor n2h2 host local_ip[:port number] [timeout <seconds>] [protocol TCP | UDP]`**
- 软件版本 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]]`**
- 软件版本 7.2 及更高版本：`hostname(config)#`**`url-server (if_name) vendor {secure-computing | n2h2} host <local_ip> [port <number>] [timeout <seconds>] [protocol {TCP [connections <number>]} | UDP]`** 对于 vendor {secure-computing|n2h2}，您可以使用 secure-computing 作为供应商字符串。但是，如果想具备向后兼容性，则可以使用 n2h2。生成配置条目时，secure-computing 被保存为供应商字符串。

用连接到过滤服务器的安全设备接口的名称替换 if_name。默认名称是 inside。用过滤服务器的 IP 地址替换 local_ip，用所需的端口号替换 port <number>。

注意： Secure Computing SmartFilter 服务器用来与使用 TCP 或 UDP 的安全设备通信的默认端口为端口 4005。

用安全设备必须持续尝试连接过滤服务器的秒数替换 seconds。使用 protocol 选项指定要使用 TCP 还是 UDP。

connections <number> 是在主机和服务器之间尝试建立连接的次数。

例如，要识别单个 N2H2 过滤服务器，请发出以下命令：

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

或者，如果要使用默认值，请发出以下命令：

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

配置过滤策略

注意： 启用 URL 过滤之前，必须标识并启用 URL 过滤服务器。

启用 URL 过滤

如果过滤服务器批准 HTTP 连接请求，安全设备会允许 Web 服务器的回复到达发出请求的客户端。如果过滤服务器拒绝请求，安全设备会将用户重定向到一个阻止页面，表明访问被拒绝。

发出 **filter url** 命令，以配置用来过滤 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]
- 软件版本 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]

如果要使用 HTTP (80) 默认端口以外的其他端口，请使用用来过滤 HTTP 流量的端口号替换 port。要识别端口号范围，请输入该范围的开始和结束端口号，以连字符分隔。

如果启用了过滤功能，安全设备会阻止出站的 HTTP 流量，直到过滤服务器允许连接。如果主过滤服务器不响应，安全设备会将过滤请求转到辅助过滤服务器。如果使用 allow 选项，则在主过滤服务器不可用时，安全设备会转发 HTTP 流量，而不进行过滤。

发出 **proxy-block** 命令，以将所有请求转给代理服务器。

注意： 剩余参数则用于截断长 URL。

截断较长的 HTTP URL

如果使用 longurl-truncate 选项，则当 URL 的长度超过允许的最大长度时，安全设备只将 URL 的主机名或 IP 地址部分发送给过滤服务器进行评估。

使用 longurl-deny 选项可以在 URL 的长度超过最大长度限制时拒绝出站的 URL 流量。

使用 cgi-truncate 选项可以截断 CGI URL，使其只包含 CGI 脚本位置和脚本名称，而不包含任何参数。

下面是一个常规的过滤配置示例：

```
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
```

使流量免于过滤

如果要在常规过滤策略中添加例外，请发出以下命令：

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

用您想从过滤限制中排除的用户或子网的 IP 地址和子网掩码替换 local_ip 和 local_mask。

用您想从过滤限制中排除的服务器或子网的 IP 地址和子网掩码替换 foreign_ip 和 foreign_mask。

例如，以下命令将把所有内部主机对 172.30.21.99 的 HTTP 请求转发到过滤服务器，除了来自主机 192.168.5.5 的请求：

以下是一个例外配置示例：

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

高级 URL 过滤

本部分提供有关高级过滤参数的信息，其中包括以下主题：

- 缓冲
- 缓存
- 长 URL 支持

对 Web 服务器响应进行缓冲

当用户发出连接内容服务器的请求时，安全设备会同时把请求发送给内容服务器和过滤服务器。如果过滤服务器未在内容服务器之前做出响应，服务器响应会被丢弃。从 Web 客户端的角度来说，Web 服务器的响应会被延迟，因为客户端必须重新发出请求。

如果您启用了 HTTP 响应缓冲，来自 Web 内容服务器的响应将被缓冲，如果过滤服务器允许连接，这些响应会被转发给发出请求的客户端。这可以防止出现延迟。

要缓冲针对 HTTP 请求的响应，请完成以下步骤：

1. 对于正在等待过滤服务器响应的 HTTP 请求，要想为其启用响应缓冲，请发出以下命令：`hostname(config)#url-block block block-buffer-limit` 用要缓冲的块的最大数量替换 block-buffer-limit。
2. 要配置可用的最大内存量，以便用来缓冲等待的 URL 以及使用 Websense 缓冲长 URL，请发出以下命令：`hostname(config)#url-block url-mempool memory-pool-size` 用 2 到 10240 之间的值替换 memory-pool-size，表示 2 KB 到 10 MB 之间的最大内存分配。

缓存服务器地址

用户访问某个站点后，过滤服务器可以允许安全设备将服务器地址缓存一段时间，只要该地址处的每个站点都属于始终被允许的类别。然后，当用户再次访问该服务器，或者当其他用户访问该服务器时，安全设备就不必再次咨询过滤服务器。

如果要提高吞吐率，请发出 **url-cache** 命令：

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

用 1 到 128 (KB) 之间的缓存大小值替换 size。

使用 dst 关键字可以根据 URL 目标地址缓存条目。如果所有用户在 Websense 服务器上使用的 URL 过滤策略都相同，请选择此模式。

使用 src_dst 关键字可以根据发出 URL 请求的源地址和 URL 目标地址来缓存条目。如果用户在 Websense 服务器上使用的 URL 过滤策略不同，请选择此模式。

启用长 URL 过滤

默认情况下，如果 HTTP URL 的长度超过 1159 个字符，安全设备就会将该 URL 视为长 URL。您可以使用以下命令增大单个 URL 所允许的最大长度：

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

用每个要缓冲的长 URL 的最大大小（以 KB 为单位）替换 long-url-size。

例如，以下命令用于为安全设备配置高级 URL 过滤功能：

```
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
```

配置

此配置包含本文档中介绍的命令：

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
```

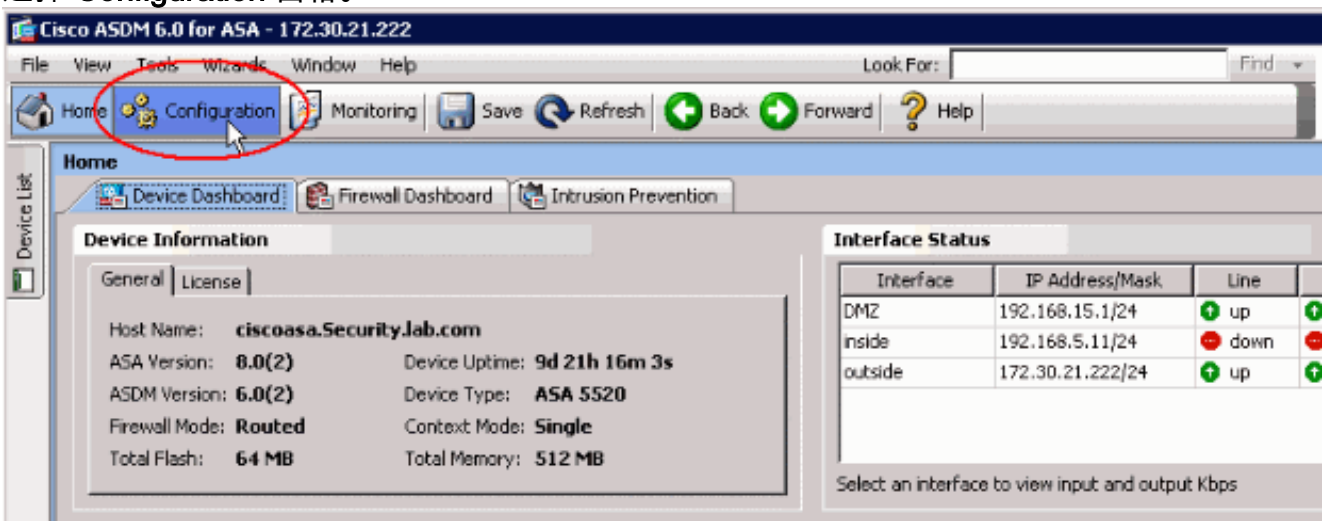
```
255.255.255.255 172.30.21.99 255.255.255.255 filter url
http 192.168.5.0 255.255.255.0 172.30.21.99
255.255.255.255 allow proxy-block longurl-truncate cgi-
truncate http server enable http 172.30.0.0 255.255.0.0
outside no snmp-server location no snmp-server contact
telnet 0.0.0.0 0.0.0.0 inside 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

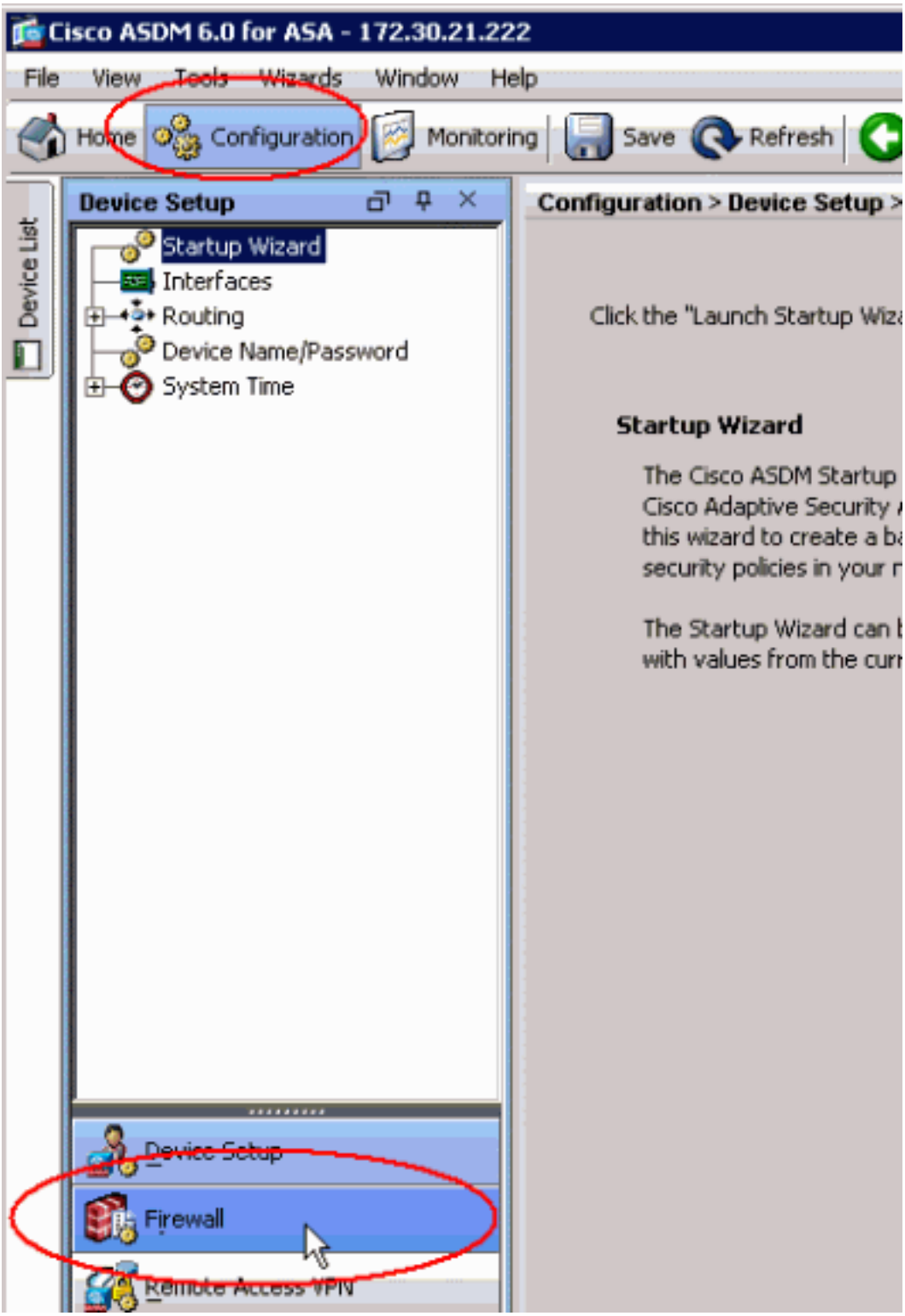
本部分介绍如何使用 Adaptive Security Device Manager (ASDM) 为安全设备配置 URL 过滤功能：

启动 ASDM 之后，完成以下步骤：

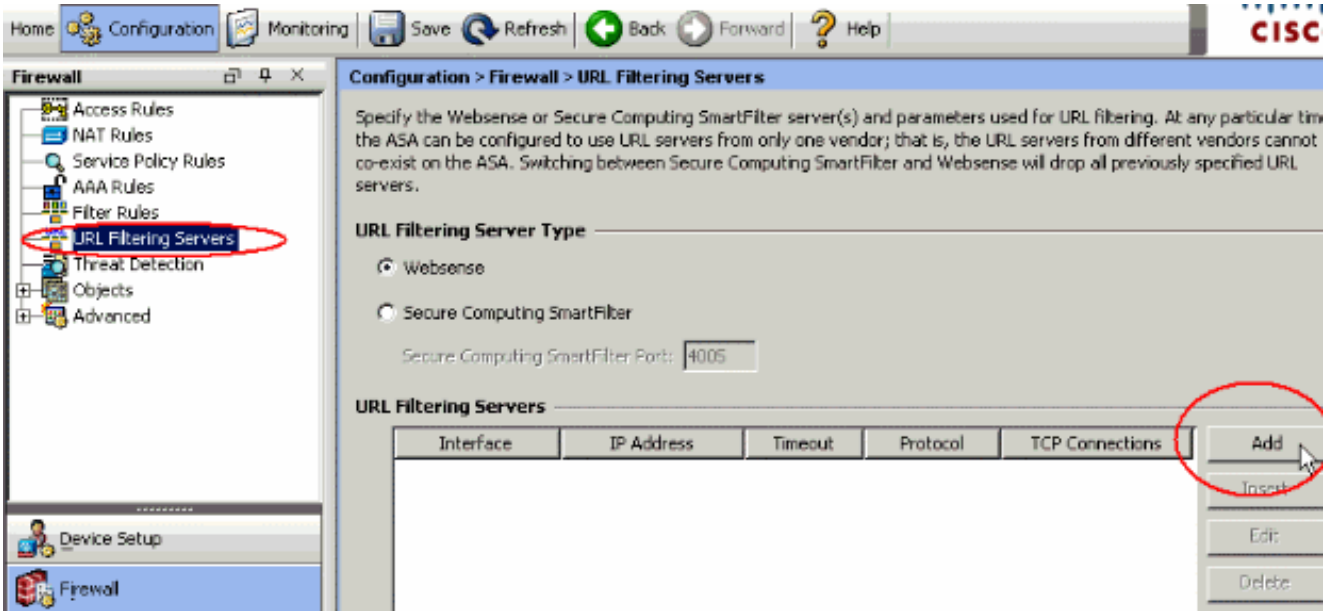
1. 选择 **Configuration** 窗格。



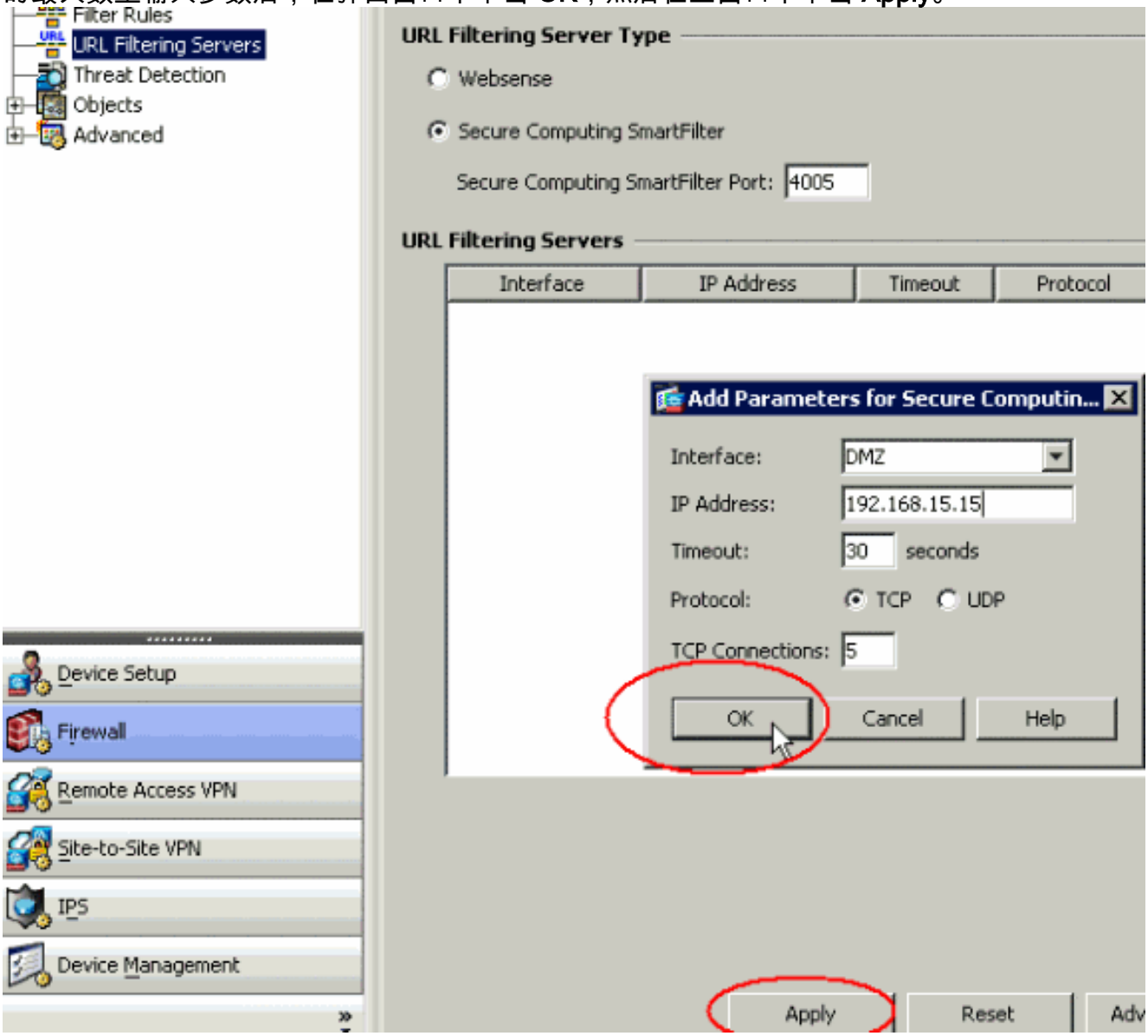
2. 在 **Configuration** 窗格所显示的列表中，单击 **Firewall**。



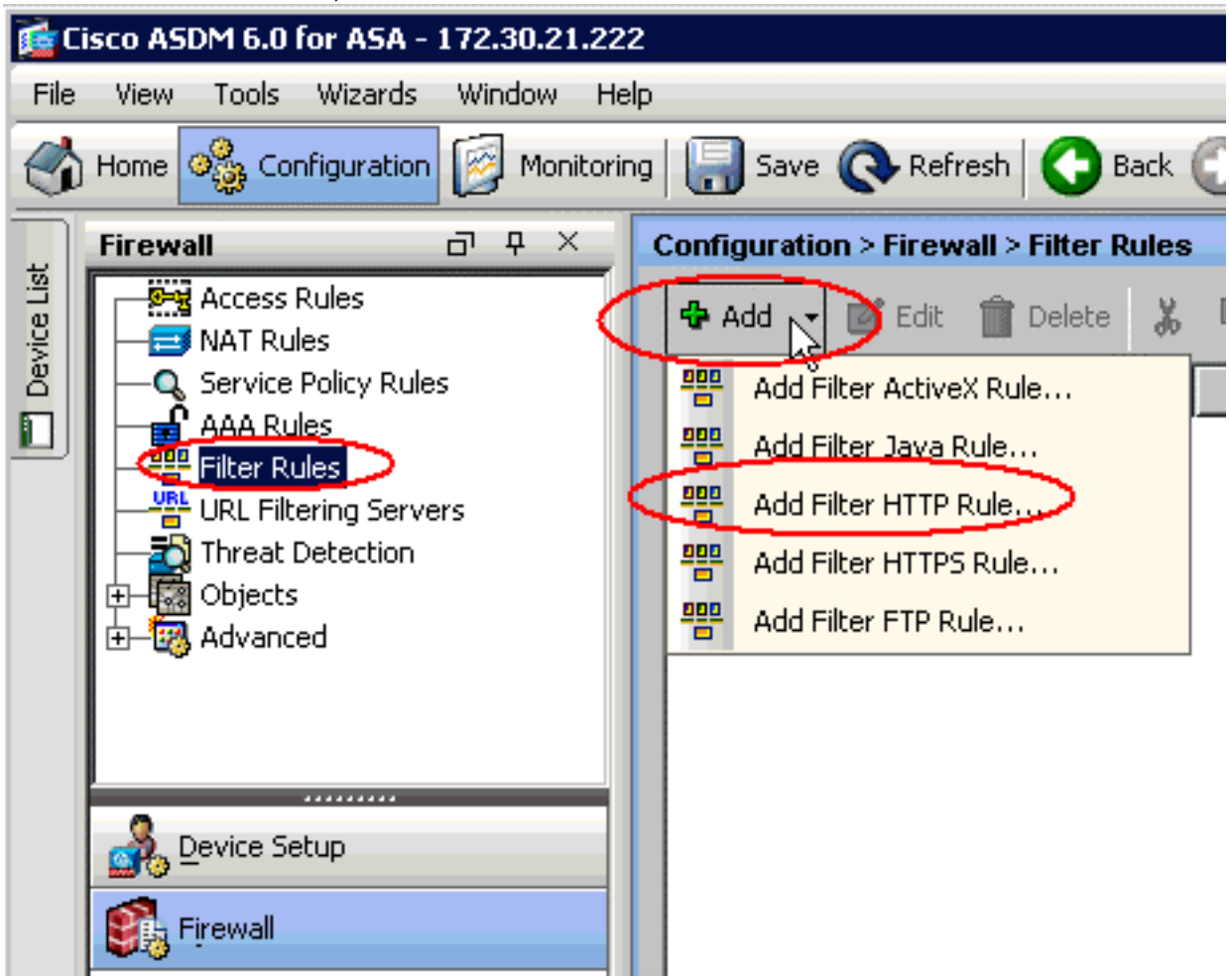
3. 从 **Firewall** 下拉列表中，选择 **URL Filtering Servers**。选择您要使用的 URL 过滤服务器类型，然后单击 **Add** 配置其参数。**注意：** 您必须先添加过滤服务器，然后才能为 HTTP、HTTPS 或 FTP 过滤规则配置过滤。



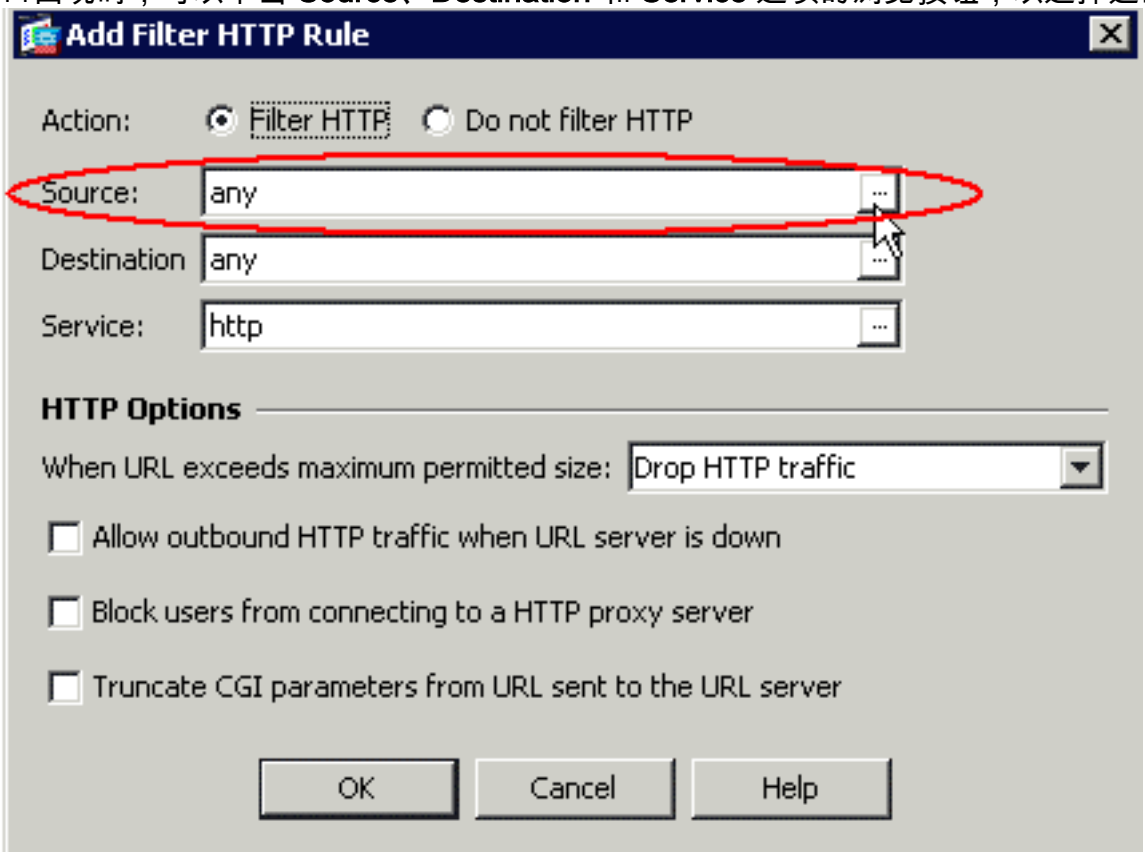
4. 在弹出窗口中选择适当的参数：Interface — 显示连接到过滤服务器的接口IP Address — 显示过滤服务器的 IP 地址Timeout — 显示一定的秒数，超过该时间后对过滤服务器的请求就会超时Protocol — 显示用来与过滤服务器通信的协议。默认值为 TCP 版本 1。如果 PIX 防火墙已对用户进行了认证，TCP 版本 4 还允许 PIX 防火墙将已认证的用户名和 URL 日志记录信息发送给 Websense 服务器。TCP Connections — 显示允许与 URL 过滤服务器通信的 TCP 连接的最大数量输入参数后，在弹出窗口中单击 **OK**，然后在主窗口中单击 **Apply**。



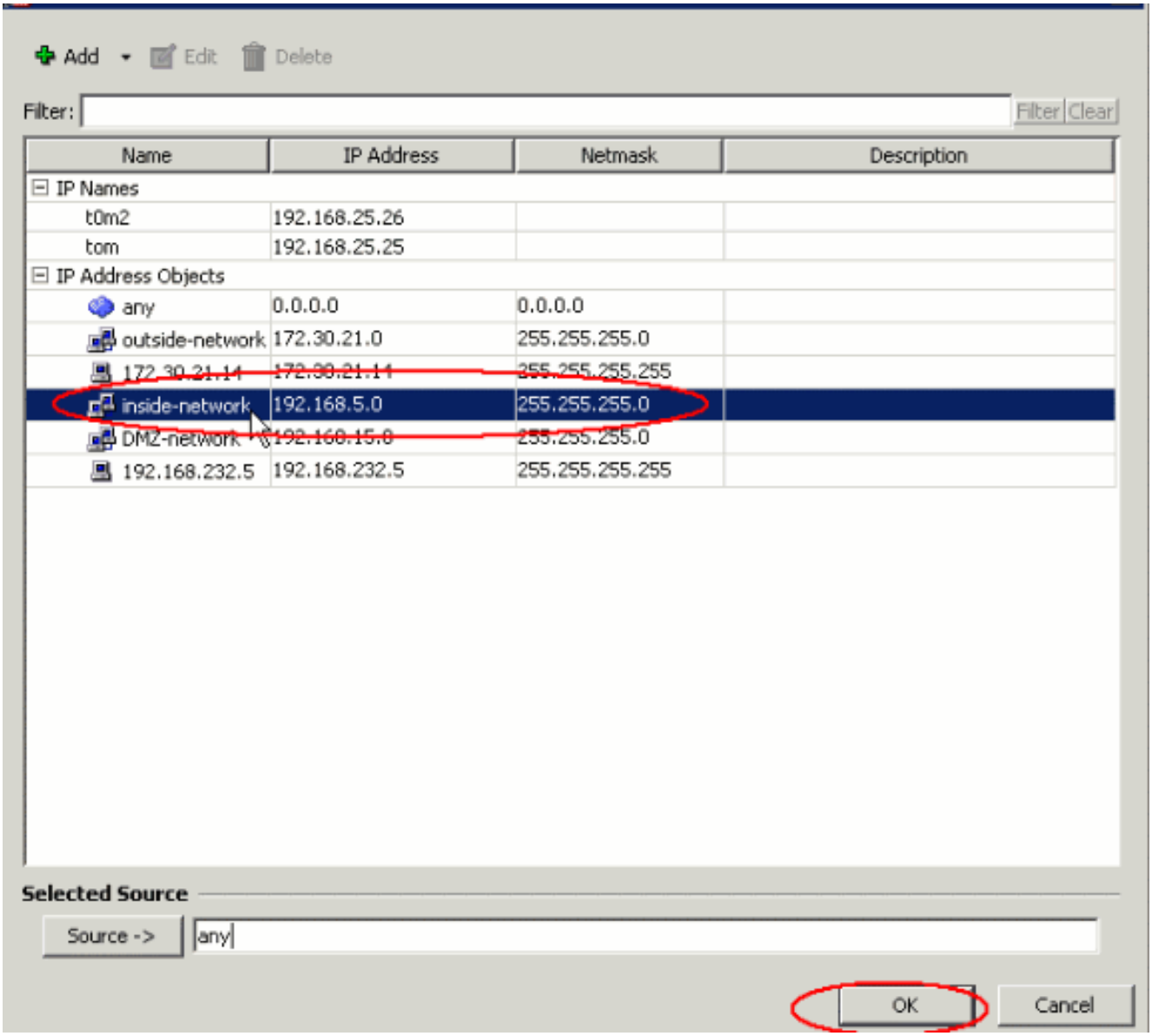
5. 从 **Firewall** 下拉列表中，选择 **Filter Rules**。在主窗口中单击 **Add** 按钮，然后选择您要添加的规则类型。在本示例中，选择 **Add Filter HTTP Rule**。



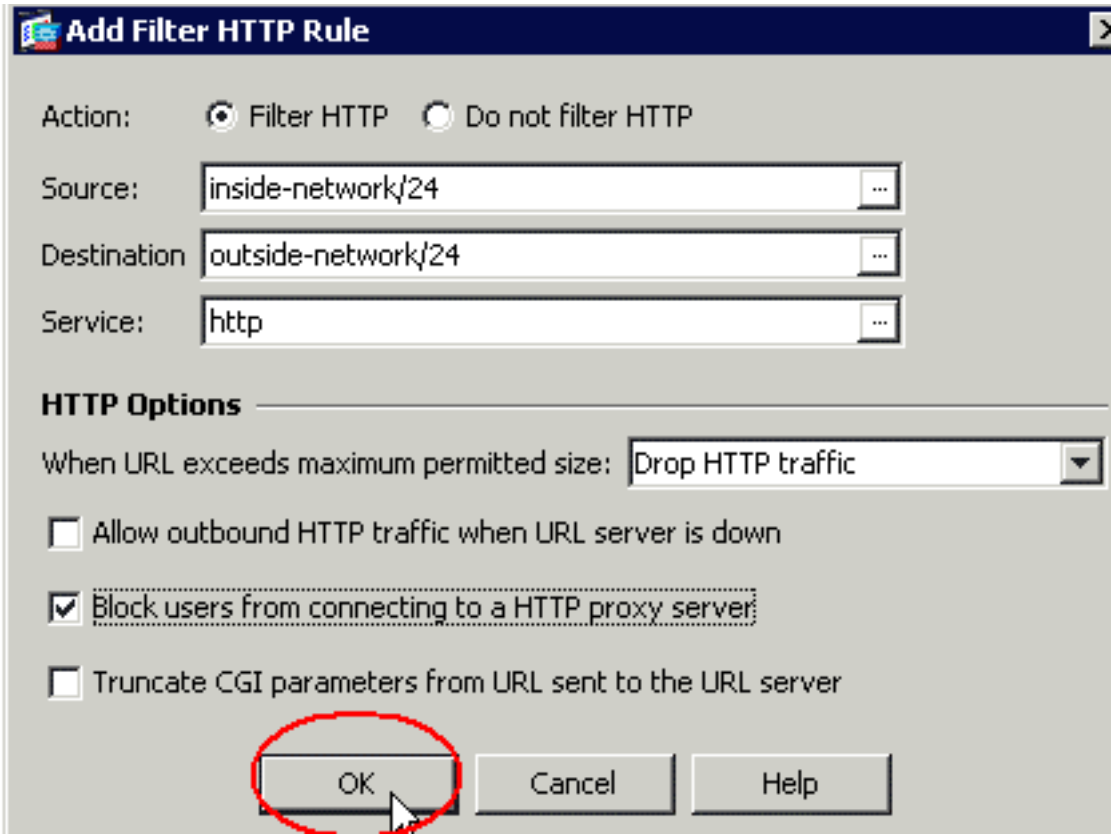
6. 当弹出窗口出现时，可以单击 **Source**、**Destination** 和 **Service** 选项的浏览按钮，以选择适当的参数。



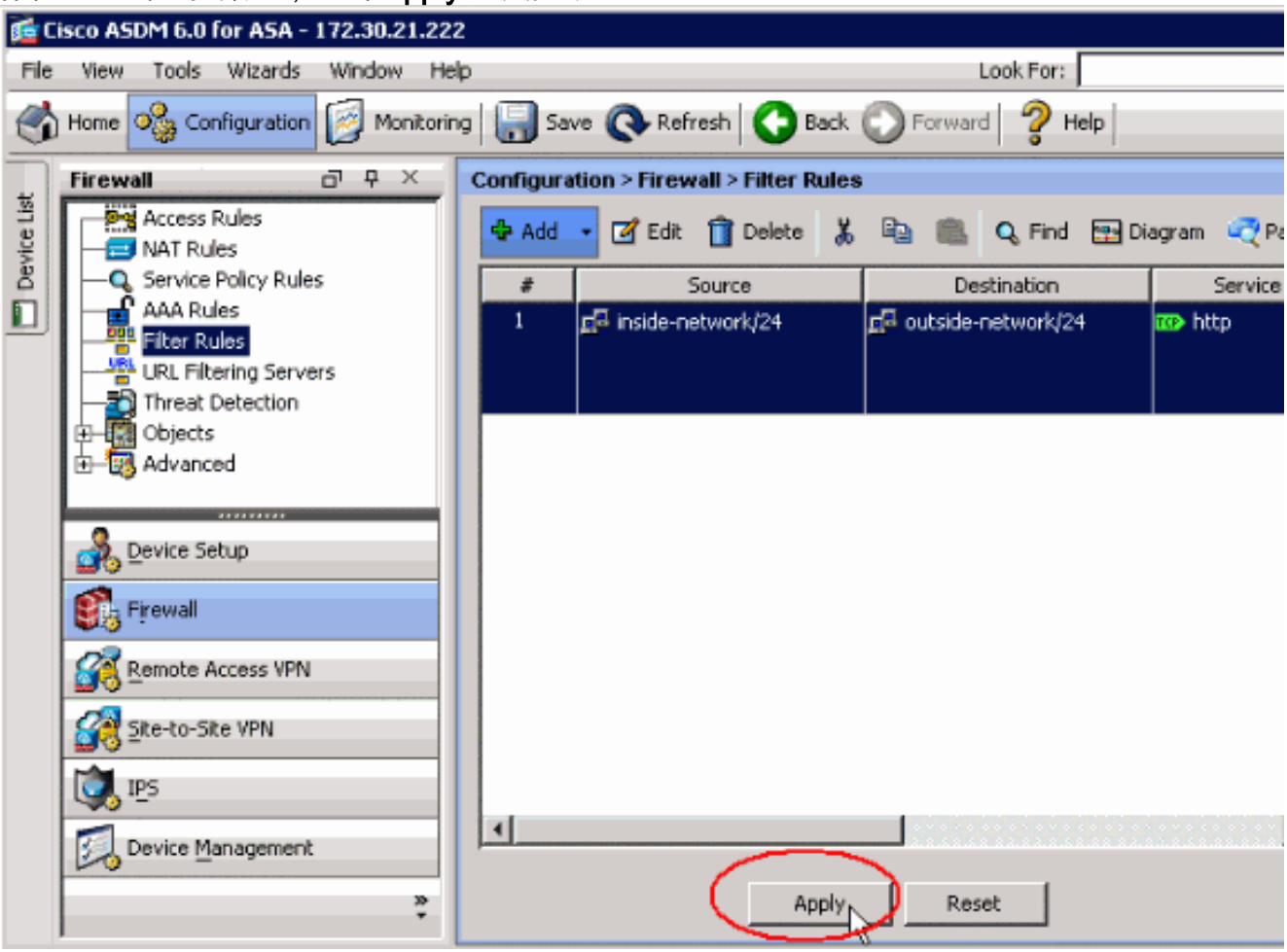
7. 以下是 **Source** 选项的浏览窗口。进行选择，然后单击 **OK**。



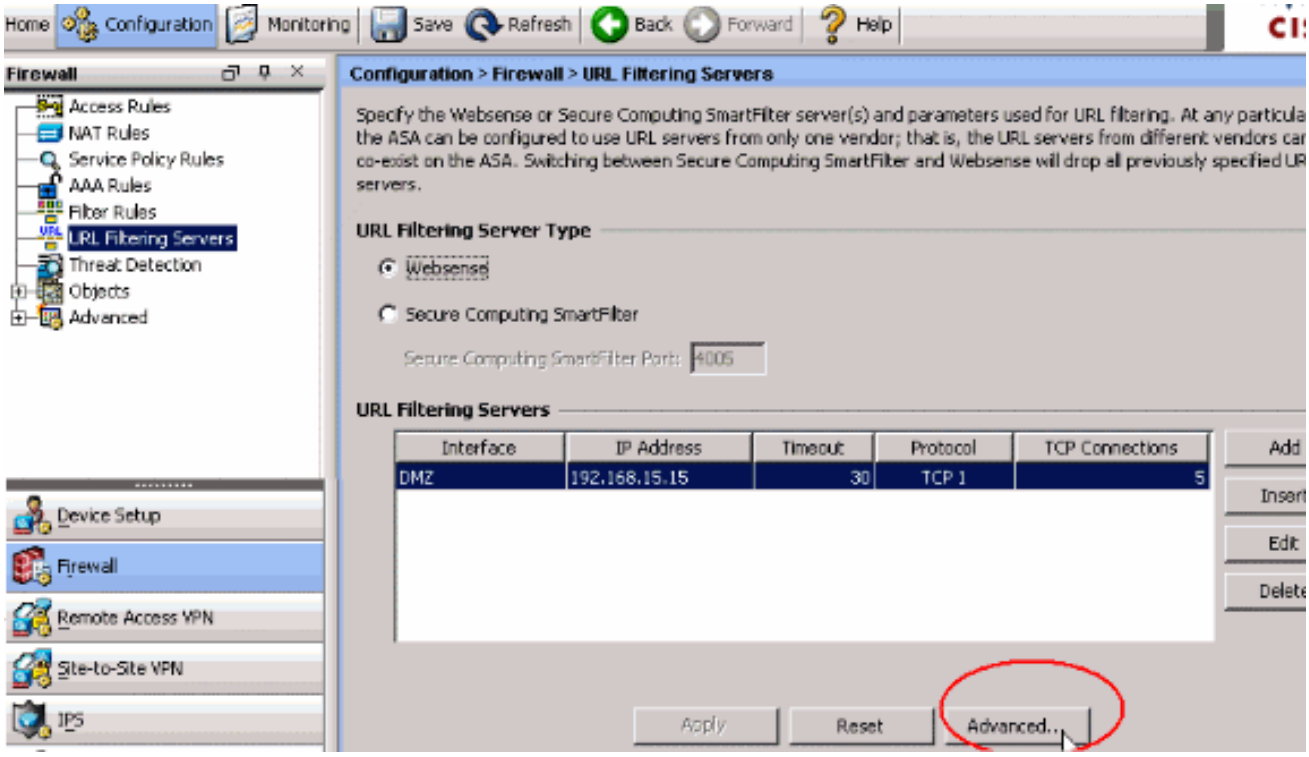
8. 完成所有参数的选择后，单击 OK 继续。



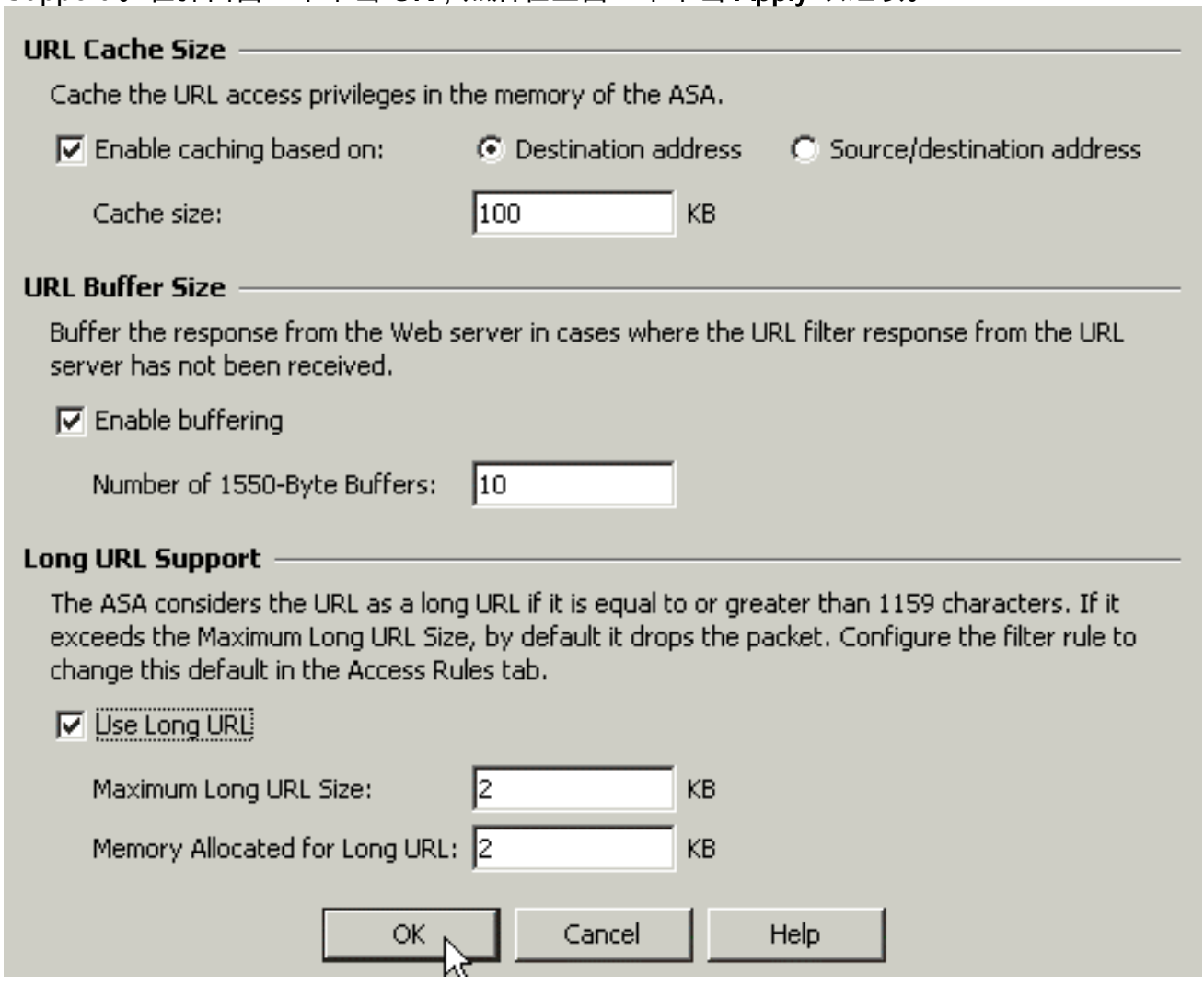
9. 配置完适当的参数后，单击 **Apply** 提交更改。



10. 对于高级 URL 过滤选项，从 **Firewall** 下拉列表中再次选择 **URL Filtering Servers**，然后单击主窗口中的 **Advanced** 按钮。



11. 在弹出窗口中配置各个参数，例如“URL Cache Size”、“URL Buffer Size”和“Long URL Support”。在弹出窗口中单击 **OK**，然后在主窗口中单击 **Apply** 以继续。



12. 最后，在终止 ASDM 会话前，确保您保存了所有更改。

验证

使用本部分中的命令查看 URL 过滤信息。可使用这些命令验证您的配置。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show url-server** — 显示有关过滤服务器的信息例如：`hostname#show url-server url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp connections 10` 在软件版本 7.2 及更高版本中，此命令的形式为 **show running-config url-server**。
- **show url-server stats** — 显示有关过滤服务器的信息和统计信息对于软件版本 7.2，此命令的形式为 **show running-config url-server statistics**。在软件版本 8.0 及更高版本中，此命令的形式为 **show url-server statistics**。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** — 显示 URL 块缓冲的配置例如：`hostname#show url-block url-block url-mempool 128 url-block url-size 4 url-block block 128` 在软件版本 7.2 及更高版本中，此命令的形式为 **show running-config url-block**。
- **show url-block block statistics** — 显示 URL 块统计信息例如：`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` 对于软件版本 7.2，此命令的形式为 **show running-config url-block block statistics**。
- **show url-cache stats** — 显示如何使用缓存例如：`hostname#show url-cache stats URL Filter Cache Stats ---------------------- Size : 128KB Entries : 1724 In Use : 456 Lookups : 45 Hits : 8` 在软件版本 8.0 中，此命令的形式为 **show url-cache statistics**。
- **show perfmon** — 显示 URL 过滤性能统计信息，以及其他性能统计信息。过滤统计信息显示在 URL Access 行和 URL Server Req 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** — 显示过滤配置例如：`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` 在软件版本 7.2 及更高版本中，此命令的形式为 **show running-config filter**。

故障排除

本部分提供有关如何对配置进行故障排除的信息。

Error:"%ASA-3-304009 ：Ran out of buffer blocks specified by url-block command"

防火墙用完了 URL 缓存，这些缓存用于在防火墙等待从 URL 服务器获得确认时保存服务器回复。

解决方案

这个问题主要是与 ASA 及 Websense 服务器之间的延迟有关。要解决此问题，请尝试以下解决方法。

- 设法将 ASA 上使用的协议改为 UDP，以便与 Websense 进行通信。在 Websense 服务器和防火墙之间存在延迟问题，因此 Websense 服务器的回复需要很长时间才能返回防火墙，从而导致 URL 缓冲区在等待响应时被填满。您可以使用 UDP 而不是 TCP 在 Websense 服务器和防火墙之间进行通信。这是因为，当您使用 TCP 进行 URL 过滤时，对于每个新的 URL 请求，ASA 都需要与 Websense 服务器建立一个 TCP 连接。由于 UDP 是一种无连接协议，所以 ASA 无需建立连接以接收服务器的响应。这应当会提高服务器的性能。`ASA(config)#` **`url-server (inside) vendor websense host X.X.X.X timeout 30`** `protocol UDP version 4 connections 5`
- 请确保将 url-block 块尽可能提高到最大值，即 128。可以通过 **show url-block** 命令进行查看这个值。如果已经是 128，请参考 Cisco bug ID CSCta27415 (仅限注册用户) 中提供的增强功能。

相关信息

- Cisco ASA 5500 系列自适应安全设备产品支持
- Cisco PIX 500 系列安全设备产品支持
- Cisco 自适应安全设备管理器产品支持
- PIX/ASA：通过Cisco安全设备的连通性建立和故障排除
- 排除通过 PIX 和 ASA 的连接故障
- 技术支持和文档 - Cisco Systems