Пример конфигурации фильтрации URL-адреса PIX/ASA

Содержание

Введение

В данном документе описана конфигурация фильтрации URL-адреса на устройстве обеспечения безопасности.

Фильтрация трафика имеет следующие преимущества:

- Помогает сократить угрозы безопасности и предотвратить несанкционированное использование.
- Обеспечивает лучший контроль трафика, проходящего через устройство защиты.

Примечание: Так как фильтрация URL-адресов способствует большей загрузке ЦП, использование внешнего сервера фильтрации гарантирует, что пропускная способность другого трафика не будет затронута. Однако основываясь на скорости передачи данных в сети и возможности сервера фильтрации URL-адреса, период времени, необходимый для первоначального подключения заметно увеличится, если трафик проходит фильтрацию с помощью внешнего сервера фильтрации.

Примечание: Фильтрация внедрения от низкого уровня безопасности до выше не поддерживается. Фильтрация URL-адресов только работает для исходящего трафика, например, трафик, который происходит на интерфейсе высокого уровня безопасности,

предназначенном для сервера на низком безопасном интерфейсе.

Предварительные условия

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Устройство защиты PIX серии 500 с версией 6.2 и более поздние
- Устройство защиты ASA серии 5500 с версией 7.x и более поздние
- Менеджер устройств адаптивной защиты (ASDM) версии 6.0

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Можно фильтровать запросы на соединение, которые исходят от более безопасной сети к менее безопасной. Хотя можно использовать списки управления доступом (ACL), чтобы предотвратить исходящий доступ к указанным серверам содержимого, таким образом трудно управлять использованием из-за размера и динамической сути Интернета. Можно упростить конфигурацию и улучшить производительность устройств защиты с помощью использования отдельного сервера, который работает с одним из продуктов фильтрации Интернета:

- Websense Enterprise: фильтры HTTP, HTTPS и FTP. Поддерживается с помощью межсетевого экрана PIX версии 5.3 и более поздние.
- Secure Computing SmartFilter, ранее известен как N2H2: фильтры HTTP, HTTPS, FTP и долгая фильтрация URL-адреса. Поддерживается с помощью межсетевого экрана PIX версии 6.2 и более поздние.

По сравнению со списками управления доступом, уменьшается административная задача и улучшается эффективность фильтрации. Так как фильтрация URL-адреса обрабатывается на отдельной платформе, производительность межсетевого экрана PIX меньше подвергается влиянию. Однако пользователи отмечают, что доступ к веб-сайтам или серверам FTP занимает более продолжительный период времени, если сервер фильтрации удален от устройства защиты.

Межсетевой экран PIX проверяет внешние запросы URL-адреса с помощью политики, определенной на сервере фильтрации URL-адреса. Межсетевой экран разрешает или отклоняет соединение, основываясь на ответе сервера фильтрации.

Если фильтрация включена, а запрос для содержимого направлен на устройство защиты,

данный запрос отправляется одновременно на сервер содержимого и сервер фильтрации. Если фильтрация сервера позволяет соединение, устройство защиты отправляет ответ с сервера содержимого к клиенту, который создал запрос. Если сервер фильтрации отклоняет содержимое, устройство защиты отбрасывает ответ и отправляет сообщение или возвращает код, который означает, что данное соединение не удалось выполнить.

Если на устройстве защиты включена аутентификация пользователя, устройство защиты также отправляет имя пользователя на сервер фильтрации. Сервер фильтрации может использовать параметры фильтрации для отдельных пользователей или предоставить расширенные отчеты в отношении использования.

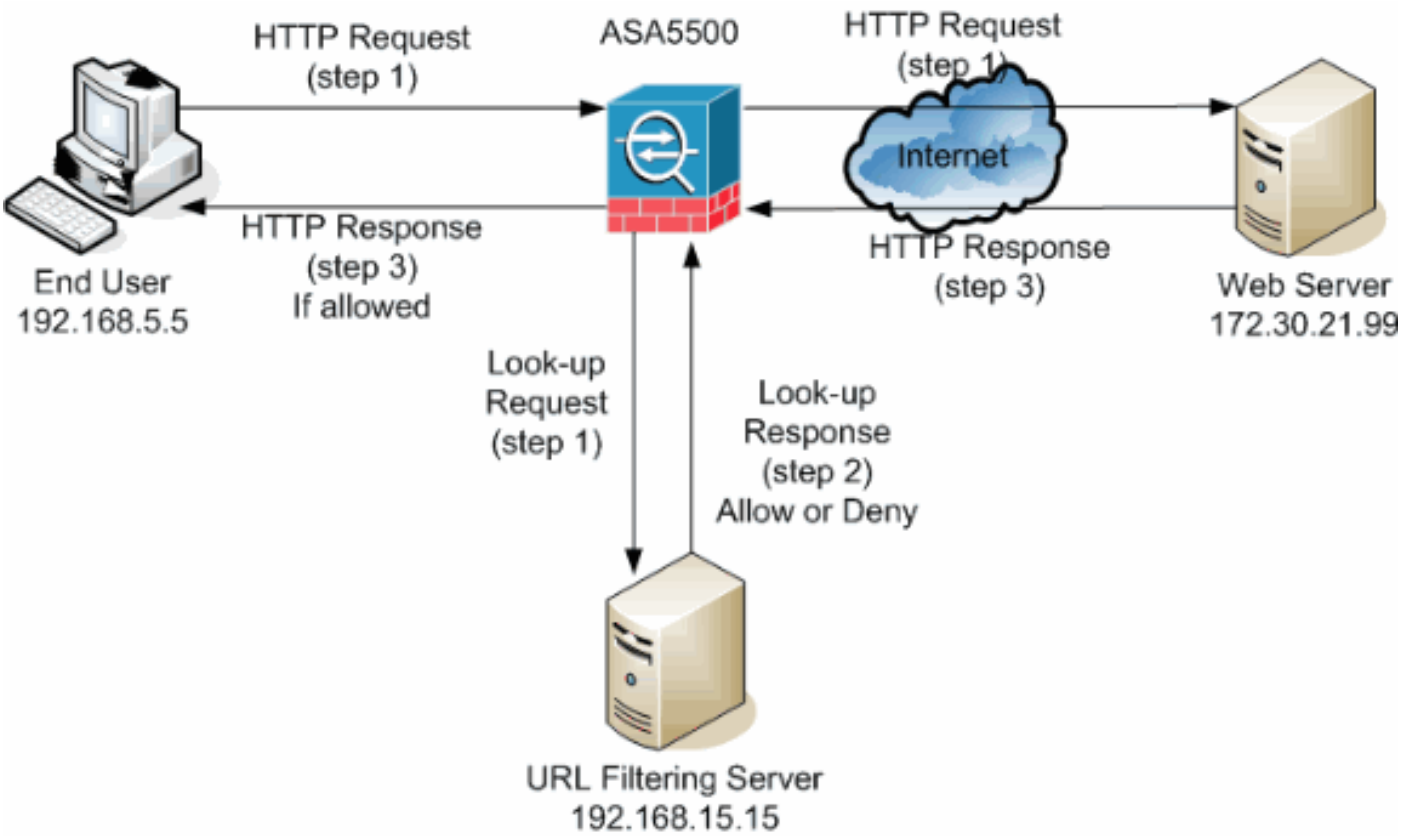
Конфигурация ASA/PIX с помощью CLI

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



В данном примере сервер фильтрации URL-адреса находится в сети DMZ. Конечные пользователи, которые находятся внутри сети, пытаются получить доступ к веб-серверу, находящемуся вне сети через Интернет.

Во время запроса пользователя для веб-сервера выполняются следующие действия:

1. Конечный пользователь просматривает страницы на веб-сервере, и браузер

отправляет HTTP-запрос.
2. Как только устройство защиты получает данный запрос, оно перенаправляет его на веб-сервер и сразу извлекает URL-адрес, а потом отправляет запрос о поиске на сервер фильтрации URL-адреса.
3. После того как сервер фильтрации URL-адресов получает данный запрос о поиске, он проверяет базу данных этого запроса, чтобы определить разрешить или запретить URL-адрес. Затем он возвращает состояние разрешить или отклонить вместе с ответом о поиске на межсетевой экран Cisco IOS®.
4. Устройство защиты получает данный ответ и выполняет одно из следующих действий:Если ответ о поиске разрешает URL-адрес, устройство обеспечения безопасности HTTP отправляет ответ конечному пользователю.Если ответ о поиске запретит URL-адрес, сервер фильтрации URL-адресов перенаправит пользователя на свой веб-сервер, который отображает сообщение о категории, где заблокирован URL-адрес. После этого соединение происходит на двух концах.

Определение сервера фильтрации

С помощью команды url-server необходимо определить адрес сервера фильтрации. Необходимо определить соответствующую форму данной команды, основываясь на типе сервера фильтрации, который вы используете.

Примечание: Для ПО версии 7.x и более поздних можно определить до четырех серверов фильтрации для каждого контекста. Устройство защиты использует серверы после того, как они отправят ответ. В вашей конфигурации настроить можно только один тип сервера: Websense или N2H2.

Websense

Websense — это ПО фильтрации сторонних производителей, которое может фильтровать HTTP-запросы на основе следующих политик:

- имя хоста места назначения
- iP-адрес ПОЛУЧАТЕЛЯ
- ключевые слова
- username

В ПО содержится база данных URL-адресов более чем 20 миллионов сайтов, объединенных в более 60 категорий и подкатегорий.

- ПО версии 6.2:
  `url-server [(if_name)] vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP} version]` **С помощью команды url-server можно указывать сервер, который использует приложение фильтрации URL-адресов N2H2 или Websense.** Максимальное количество – 16 серверов URL-адресов. Однако использовать можно только по одному приложению: N2H2 или Websense. Кроме того, если изменить конфигурацию на межсетевом экране PIX, он не обновит данную конфигурацию на сервере приложения. Это необходимо сделать отдельно, основываясь на инструкциях индивидуального поставщика.
- ПО версии 7.x и более поздние:
  `pix(config)# url-server (if_name) host local_ip [timeout seconds] [protocol TCP | UDP version 1|4 [connections num_conns] ]`

if_name , . По умолчанию имя находится внутри. local_ip IP- . seconds , .

protocol, , : TCP UDP. Websense TCP version. TCP версии 1 используется по умолчанию. TCP версии 4 позволяет межсетевому экрану PIX отправлять сведения об аутентифицированных именах пользователей и регистрации URL-адресов на сервер Websense, если межсетевой экран PIX уже выполнил аутентификацию пользователя.

Например, чтобы определить один сервер фильтрации Websense, выполните следующую команду:

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

Secure Computing SmartFilter

- PIX версии 6.2:`pix(config)#url-server [(if_name)] vendor n2h2 host local_ip[:port number] [timeout <seconds>] [protocol TCP | UDP]`
- ПО версий 7.0 и 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]]`
- ПО версии 7.2 и более поздние:`hostname(config)#url-server (if_name) vendor {secure-computing | n2h2} host <local_ip> [port <number>] [timeout <seconds>] [protocol {TCP [connections <number>]} | UDP]` vendor {secure-computing | n2h2} secure-computing . n2h2 . , secure-computing .

if_name , . По умолчанию имя находится внутри. local_ip IP- port <number> .

Примечание: По умолчанию порт, который используется сервером Secure Computing SmartFilter для связи и устройством защиты с помощью TCP или UDP, – это порт 4005.

seconds , . protocol, , : TCP UDP.

Connections <number> – , .

Например, чтобы определить один сервер фильтрации N2H2, выполните следующую команду:

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

Или если необходимо использовать значения по умолчанию, выполните следующую команду:

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

Конфигурация политики фильтрации

Примечание: Необходимо определить и активировать сервер фильтрации URL-адресов до включения фильтрации URL-адресов.

Включение фильтрации URL-адресов

Если сервер фильтрации одобряет запрос HTTP-соединение, устройство защиты отправляет ответ с веб-сервера к клиенту, который создал запрос. Если сервер фильтрации запрещает запрос, устройство защиты отправляет пользователя на страницу блокировки, которая означает запрет доступа.

Выполните команду filter url, чтобы настроить политику, которая используется для фильтрации URL адресов:

- PIX версии 6.2:
  filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]
- ПО версии 7.x и более поздние:
  filter url [http | port[-port] local_ip local_mask foreign_ip foreign_mask] [allow] [proxy-block] [longurl-truncate | longurl-deny] [cgi-truncate]

port , HTTP-, HTTP (80) . Чтобы определить диапазон номеров портов, введите начальный и конечный диапазон через дефис.

С помощью активированной фильтрации устройство защиты останавливает внешний HTTP-трафик, пока сервер фильтрации не разрешит соединение. Если первичный сервер фильтрации не отвечает, устройство защиты запрашивает вторичный сервер фильтрации.
allow HTTP- , .

Выполните команду proxy-block, чтобы перебросить все запросы на прокси-сервер.

Примечание: Остальная часть параметров используется, чтобы сокращать длинные URL-адреса.

Сокращение длинных URL-адресов HTTP

longurl-truncate IP- URL- , URL- .

longurl-deny, URL-, URL- .

cgi-truncate URL- CGI, CGI .

Ниже приведен основной пример конфигурации фильтров:

```
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
```

Освобождение трафика для фильтрации

Если необходимо сделать исключение для основной политики фильтрации, выполните следующую команду:

filter url except local_ip local_mask foreign_ip foreign_mask]
local_ip local_mask IP- , .

foreign_ip foreign_mask IP- , .

Например, с помощью следующей команды все HTTP-запросы для 172.30.21.99 из внутренних хостов направляются на сервер фильтрации кроме запросов из хоста 192.168.5.5:

Пример конфигурации данного исключения выглядит следующим образом:

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

Дополнительная фильтрация URL-адресов

В данном разделе содержатся сведения о следующих параметрах дополнительной фильтрации:

- буферизация
- кэширование
- поддержка длинных URL-адресов

Буферизация ответов веб-сервера

Если пользователь выполняет запрос для подключения к серверу содержимого, устройство защиты отправляет запрос на сервер содержимого и на сервер фильтрации одновременно. Если сервер фильтрации не отвечает раньше сервера содержимого, ответ сервера отбрасывается. Это задерживает ответ сервера с точки зрения веб-клиента, так как клиенту необходимо выполнить запрос повторно.

Если отключить буфер HTTP-ответов, ответы с веб-сервера содержимого буферизируются. Ответы перенаправляются клиенту, который выполняет запрос, если сервер фильтрации разрешает соединение. Это предотвратит задержку, которая произойдет в противном случае.

Чтобы буферизировать ответы на HTTP-запросы, выполните Staff:

1. Чтобы активировать буферизацию ответов на HTTP-запросы, которые обрабатывают ответ с сервера фильтрации, выполните следующую команду:`hostname(config)#` **`url-block block block-buffer-limit`** `block-buffer-limit .`
2. Чтобы настроить максимальный объем памяти, доступный для буферизации незавершенных и длинных URL-адресов с помощью Websense, выполните следующую команду:`hostname(config)#` **`url-block url-mempool memory-pool-size`** `memory-pool-size 2 10240 2 10 .`

Кэширование адресов сервера

Как только пользователь получит доступ к сайту, сервер фильтрации может позволить устройству защиты кэшировать адрес сервера на определенный период времени, пока для всех посещаемых сайтов не будет разрешен доступ в любое время. Тогда если пользователь снова получить доступ к серверу, или это сделает другой пользователь, устройство защиты не будет обращаться за справкой к серверу фильтрации снова.

Выполните команду url-cache, если необходимо улучшить пропускную способность:

```
hostname(config)#url-cache dst | src_dst size
 size        1  128 ().
```

`dst, , URL.` Выберите данный режим, если все пользователи используют одну политику фильтрации URL-адресов на сервере Websense.

`src_dst, , , URL-, URL-.` Выберите данный режим, если все пользователи не используют одну политику фильтрации URL-адресов на сервере Websense.

Включение фильтрации длинных URL-адресов

По умолчанию устройство защиты рассматривает URL-адрес HTTP как длинный URL-адрес, если он длиннее 1159 символов. С помощью следующей команды можно увеличить максимальную длину одного URL-адреса:

```
hostname(config)#url-block url-size long-url-size
 long-url-size        URL-,    .
```

Например, с помощью следующих команд можно настроить устройство защиты для дополнительной фильтрации URL-адресов:

```
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
```

!--- конфигурацию

В конфигурацию включены команды, описанные в данном документе:

ASA 8. 0 конфигураций

```
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
```

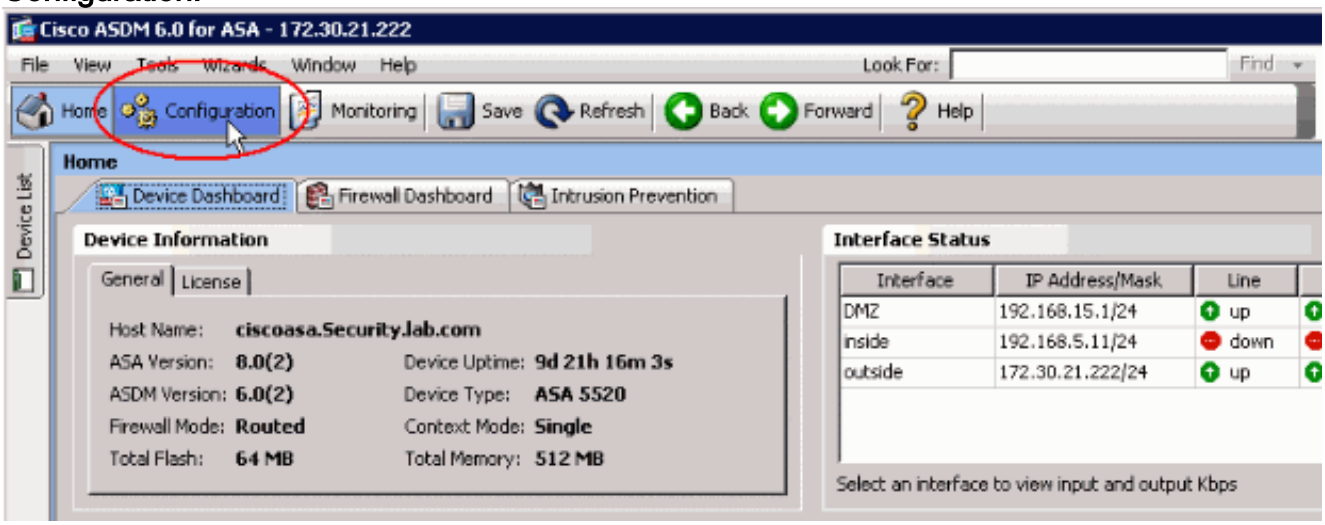
```
http 192.168.5.0 255.255.255.0 172.30.21.99
255.255.255.255 allow proxy-block longurl-truncate cgi-
truncate http server enable http 172.30.0.0 255.255.0.0
outside no snmp-server location no snmp-server contact
telnet 0.0.0.0 0.0.0.0 inside telnet timeout 5 ssh
0.0.0.0 0.0.0.0 inside ssh timeout 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
```

Конфигурация ASA/PIX с помощью ASDM

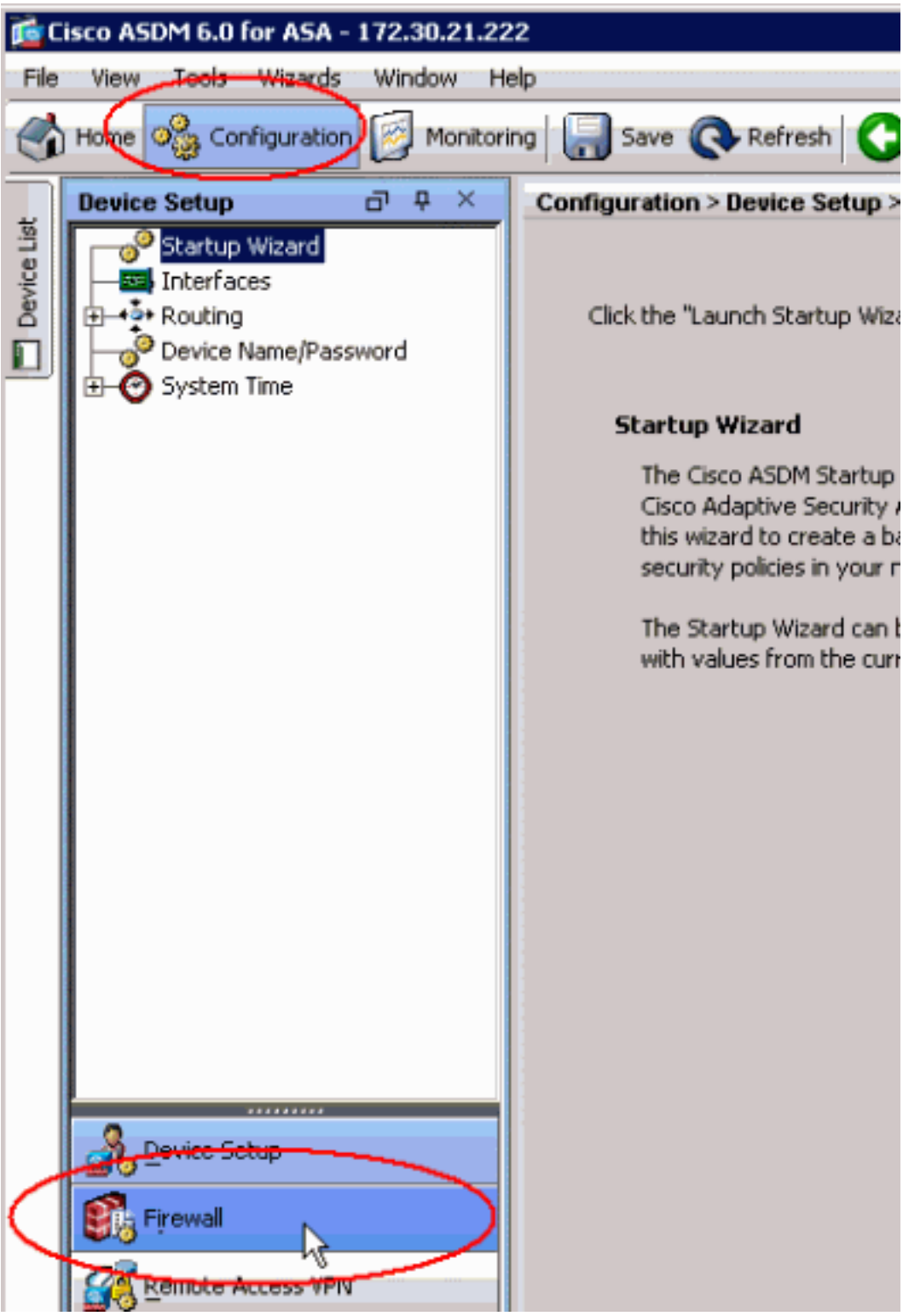
В данном разделе описана конфигурация фильтрации URL-адресов для устройства защиты с помощью менеджера устройств адаптивной защитны (ASDM).

После загрузки ASDM выполните следующие действия:

1. **Выберите панель Configuration.**

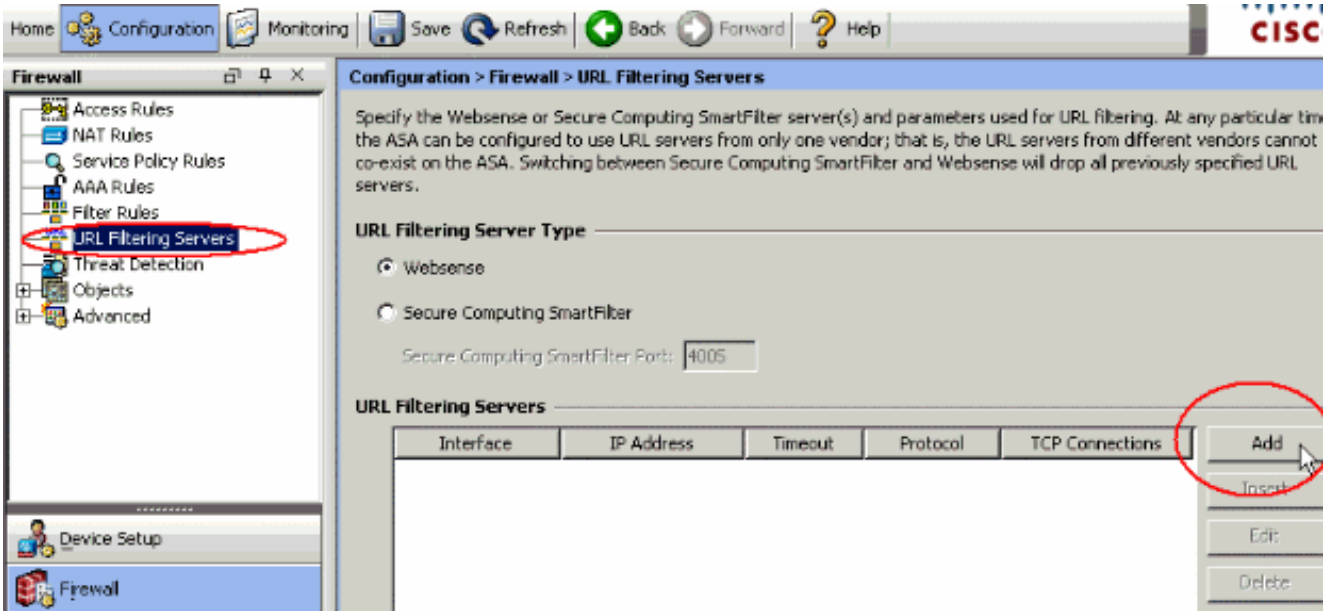


2. **Выберите Firewall в списке на панели**

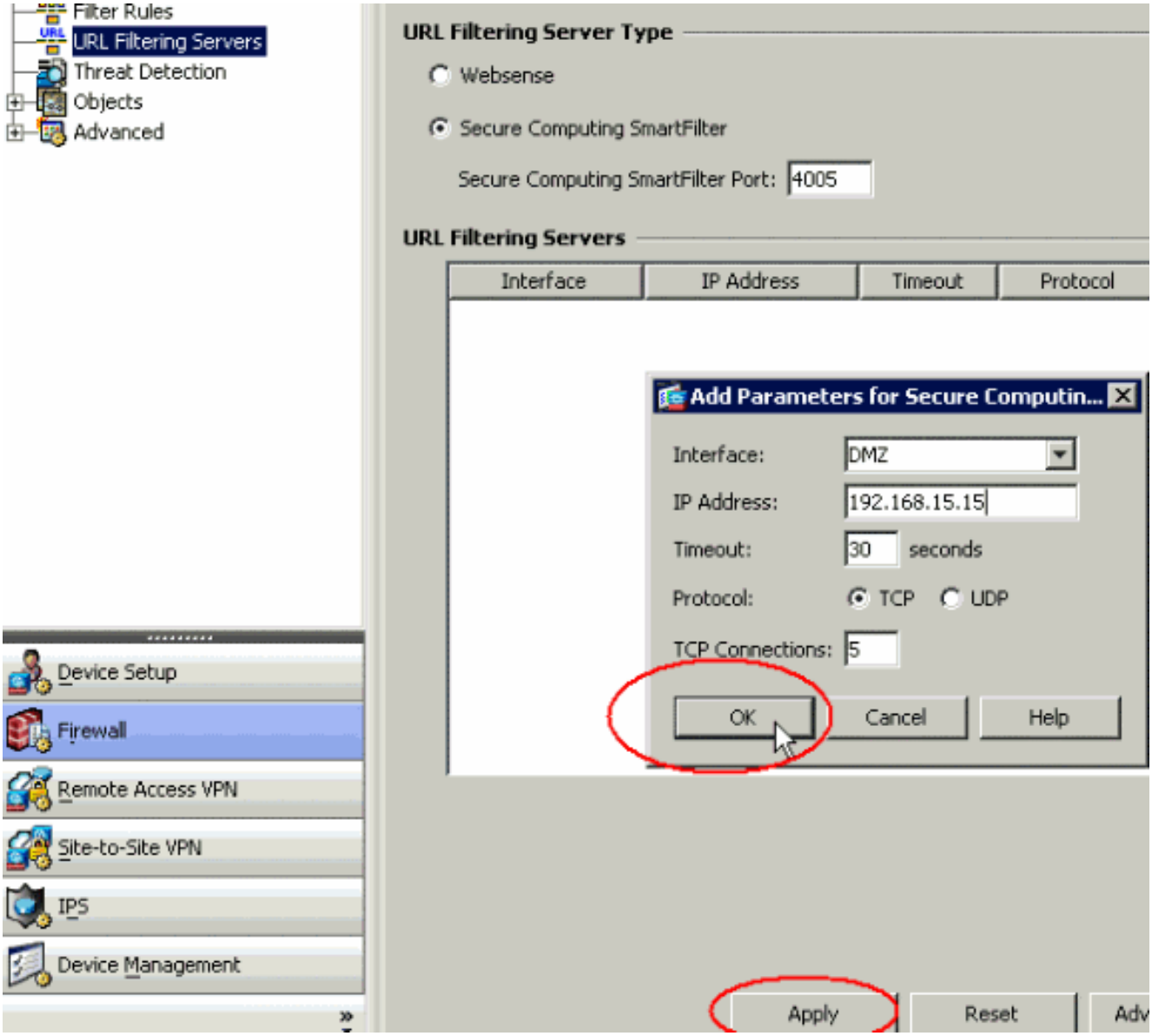


Configuration.

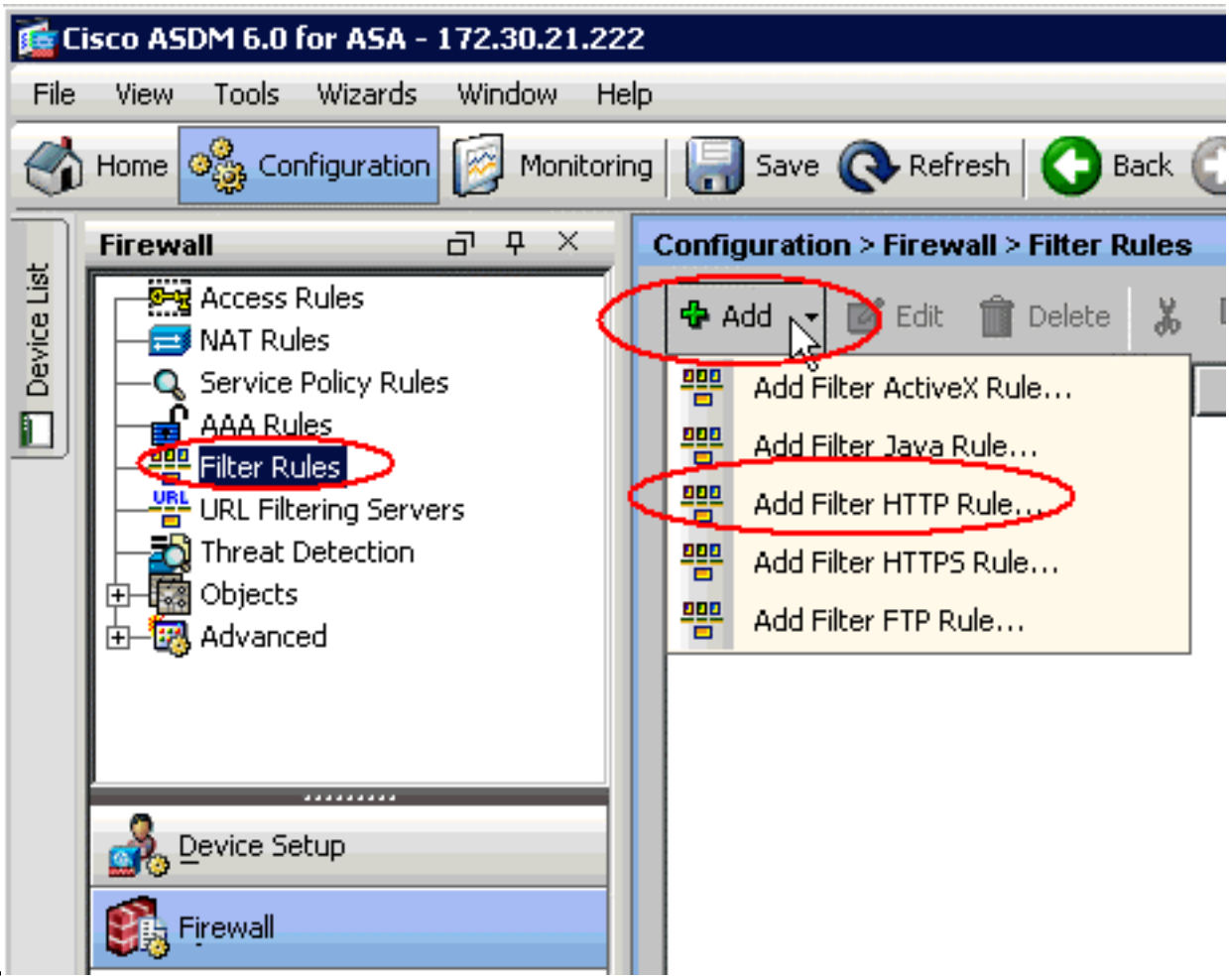
3. **В раскрывающемся списке Firewall выберите URL Filtering Servers. Выберите необходимый тип сервера фильтрации URL-адресов и нажмите Add, чтобы настроить его параметры.Примечание:** Необходимо выбрать сервер фильтрации до настройки фильтрации для HTTP, HTTPS или правил фильтрации
FTP.



4. Во всплывающем окне выберите соответствующие параметры:Интерфейс. Отображает интерфейс, подключенный к серверу фильтрацииIP-адрес. Отображает IP-адрес сервера фильтрацииВремя ожидания. Отображает количество секунд, по истечении которых запрос превысит время ожидания для сервера фильтрацииПротокол. Отображает протокол для связи с сервером фильтрации. TCP версии 1 используется по умолчанию. TCP версии 4 позволяет межсетевому экрану PIX отправлять сведения об аутентифицированных именах пользователей и регистрации URL-адресов на сервер Websense, если межсетевой экран PIX уже выполнил аутентификацию пользователяСоединение TCP. Отображает максимальное количество соединений TCP, разрешенных для связи с сервером фильтрации URL-адресов**После ввода параметров в всплывающем окне нажмите OK и в главном окне Apply.**

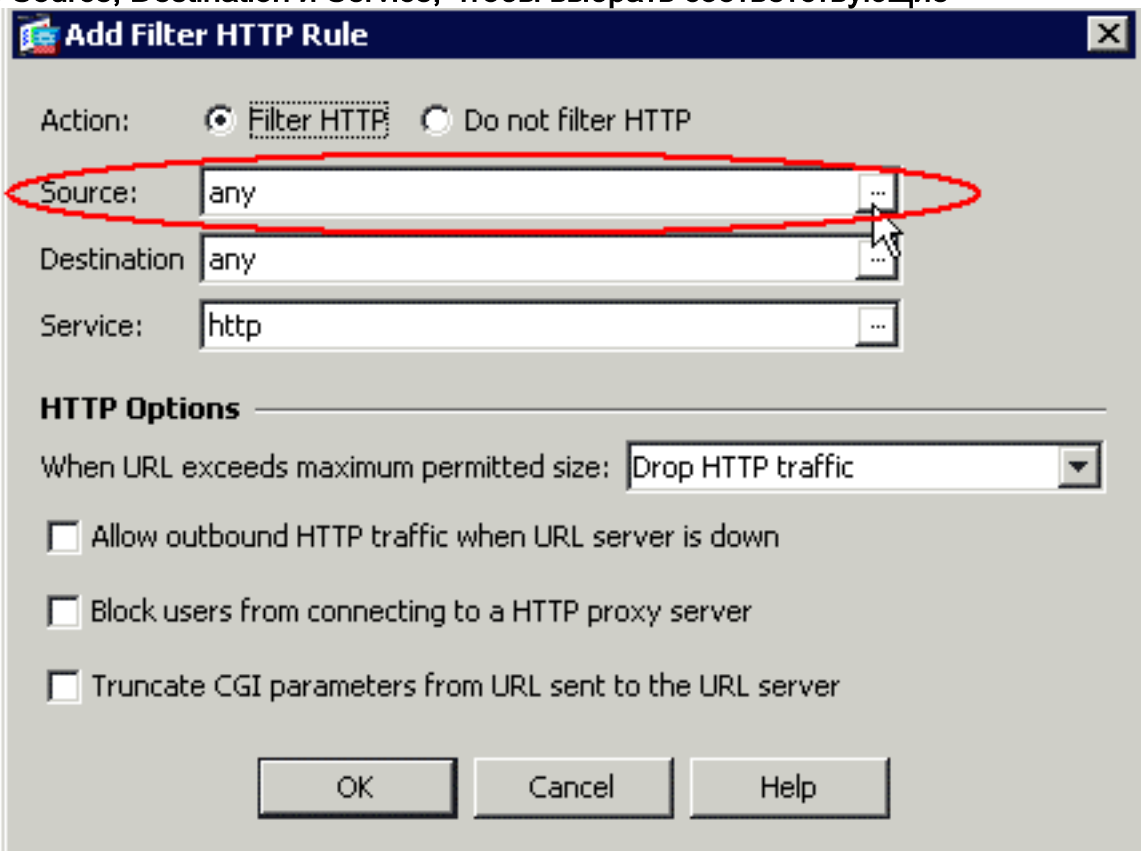


5. В раскрывающемся списке Firewall выберите Filter Rules. В главном окне нажмите кнопку Add и выберите необходимый тип правила. В следующем примере выбран тип Add Filter HTTP

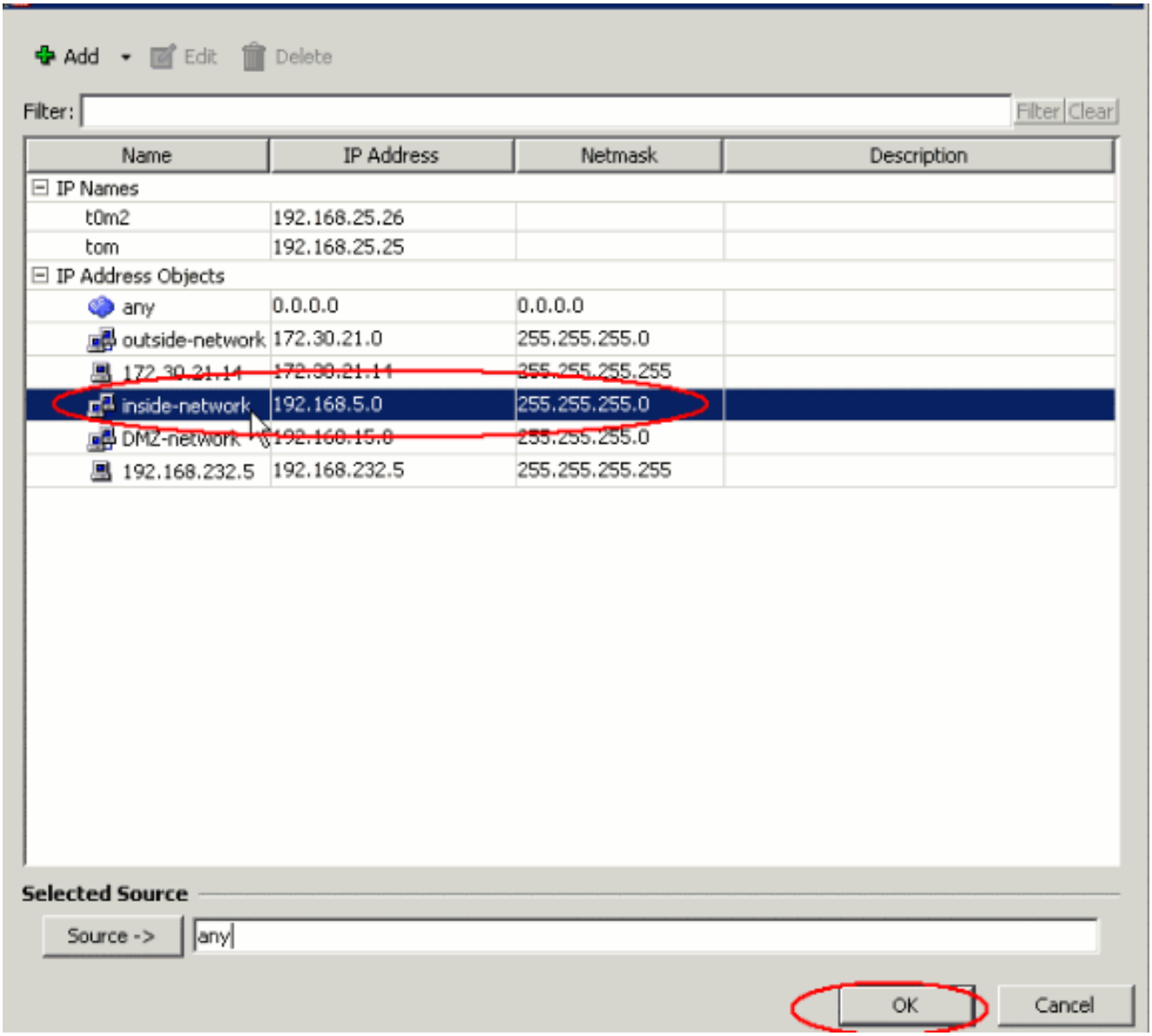


Rule.

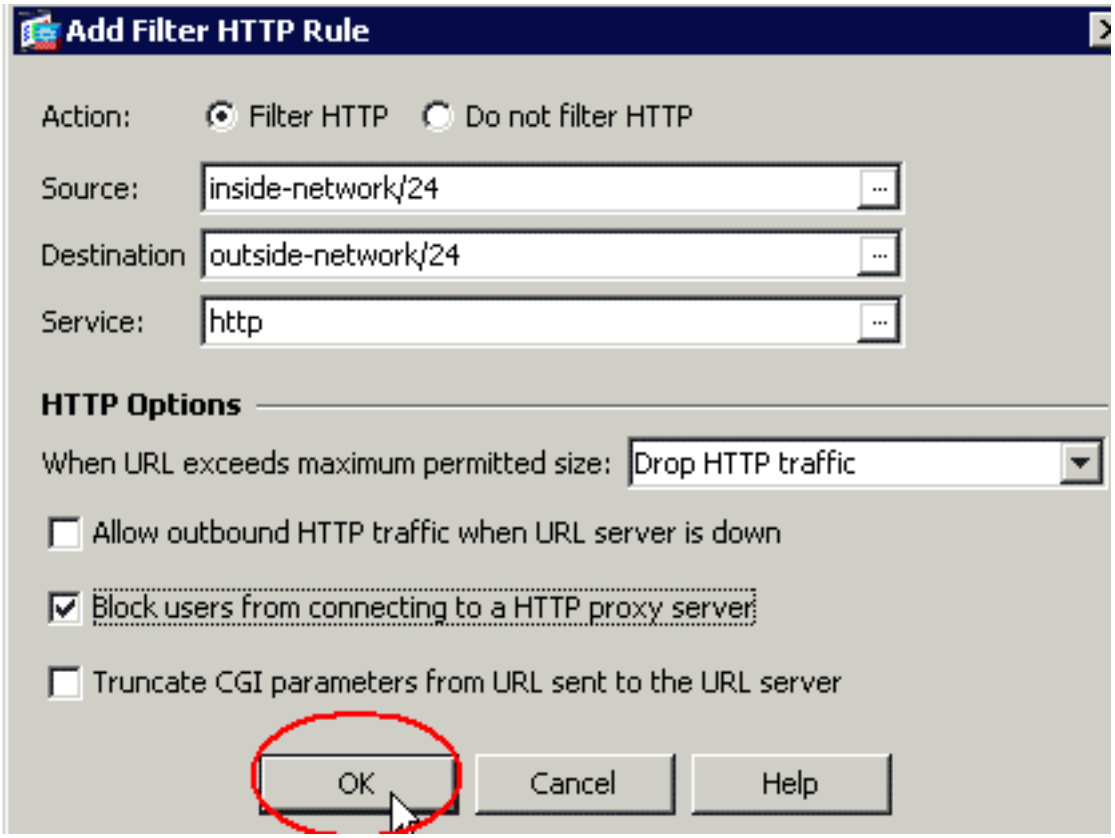
6. Откроется всплывающее окно. Здесь можно нажать кнопки обзора для отображения параметров Source, Destination и Service, чтобы выбрать соответствующие параметры.



7. Ниже отображено окно обзора параметра Source. Сделайте выбор и нажмите OK.

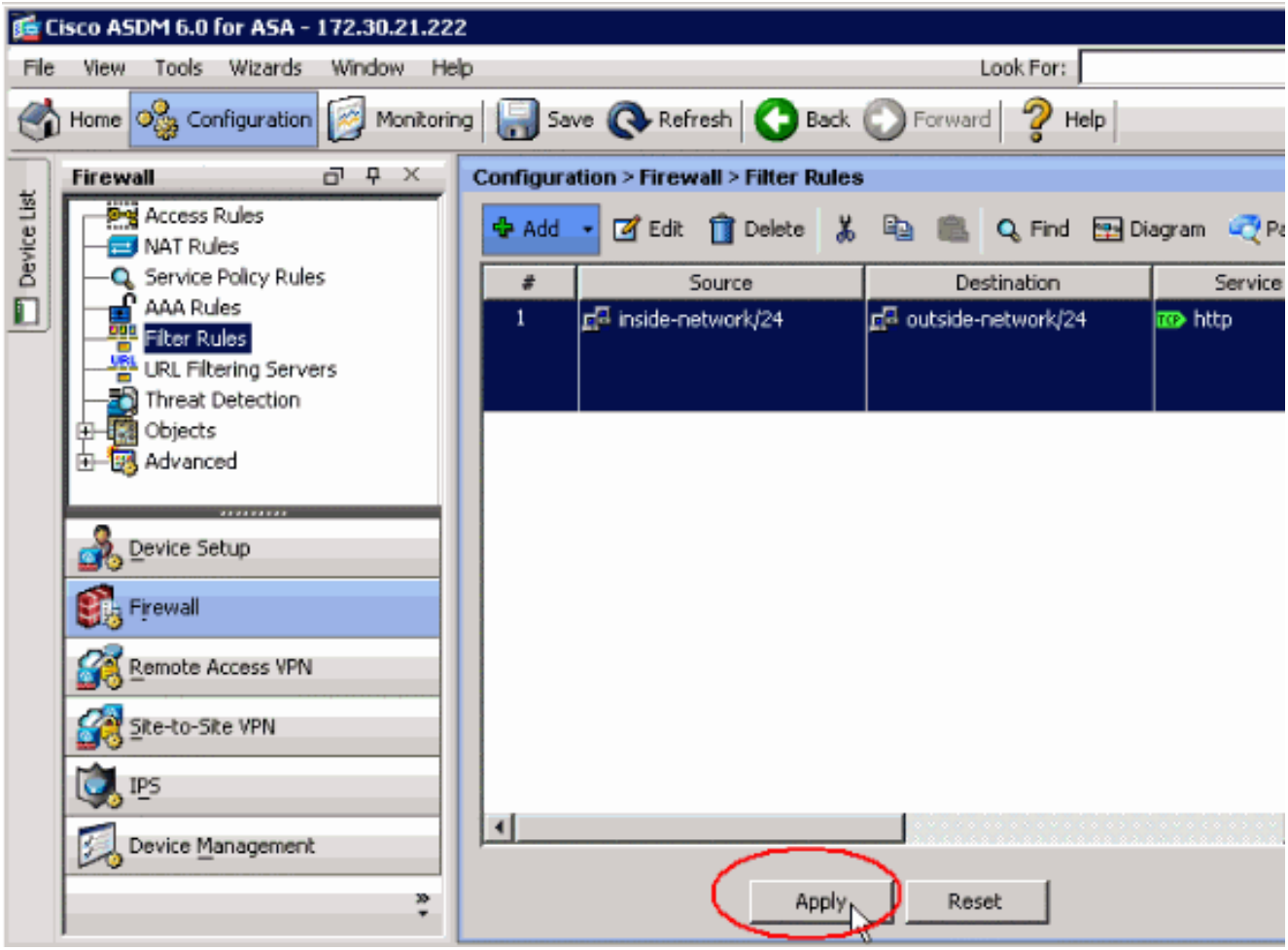


8. Завершив выбор всех параметров, нажмите OK, чтобы



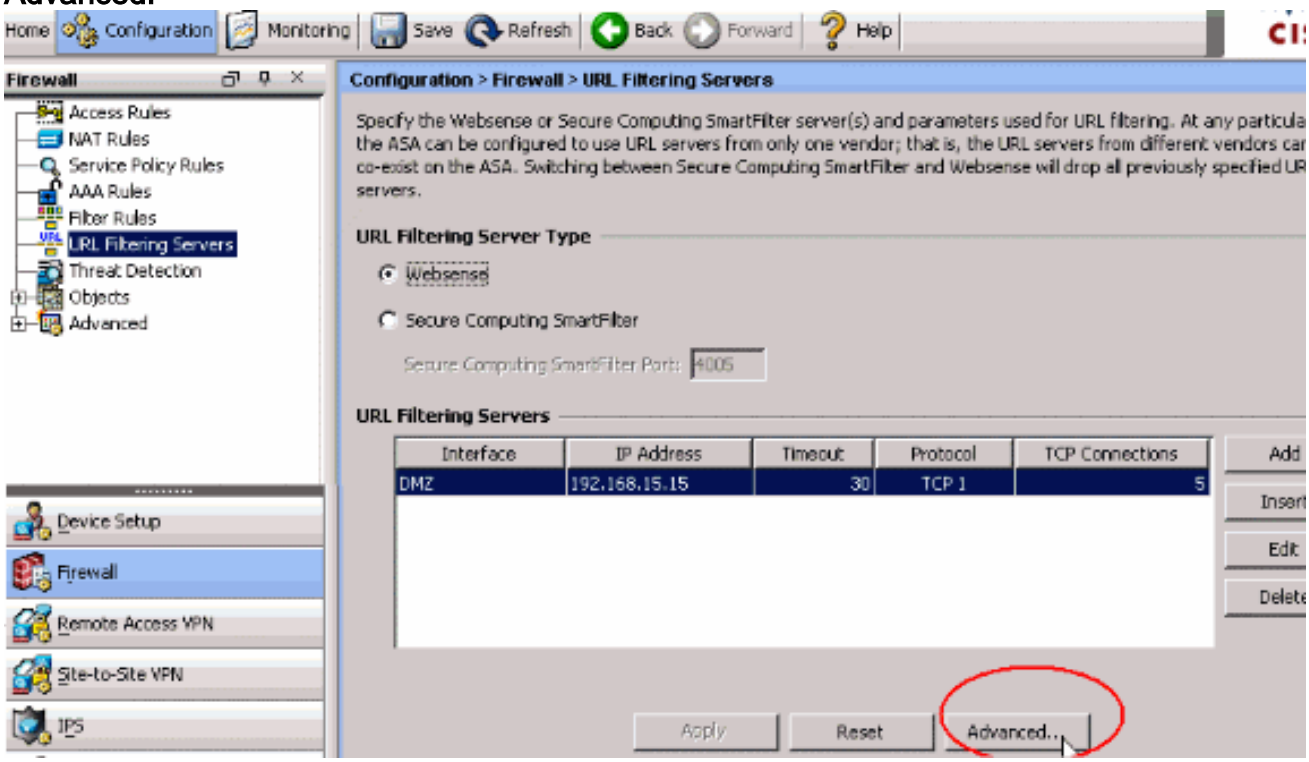
продолжить.

9. Настроив соответствующие параметры, нажмите Apply, чтобы подтвердить изменения.

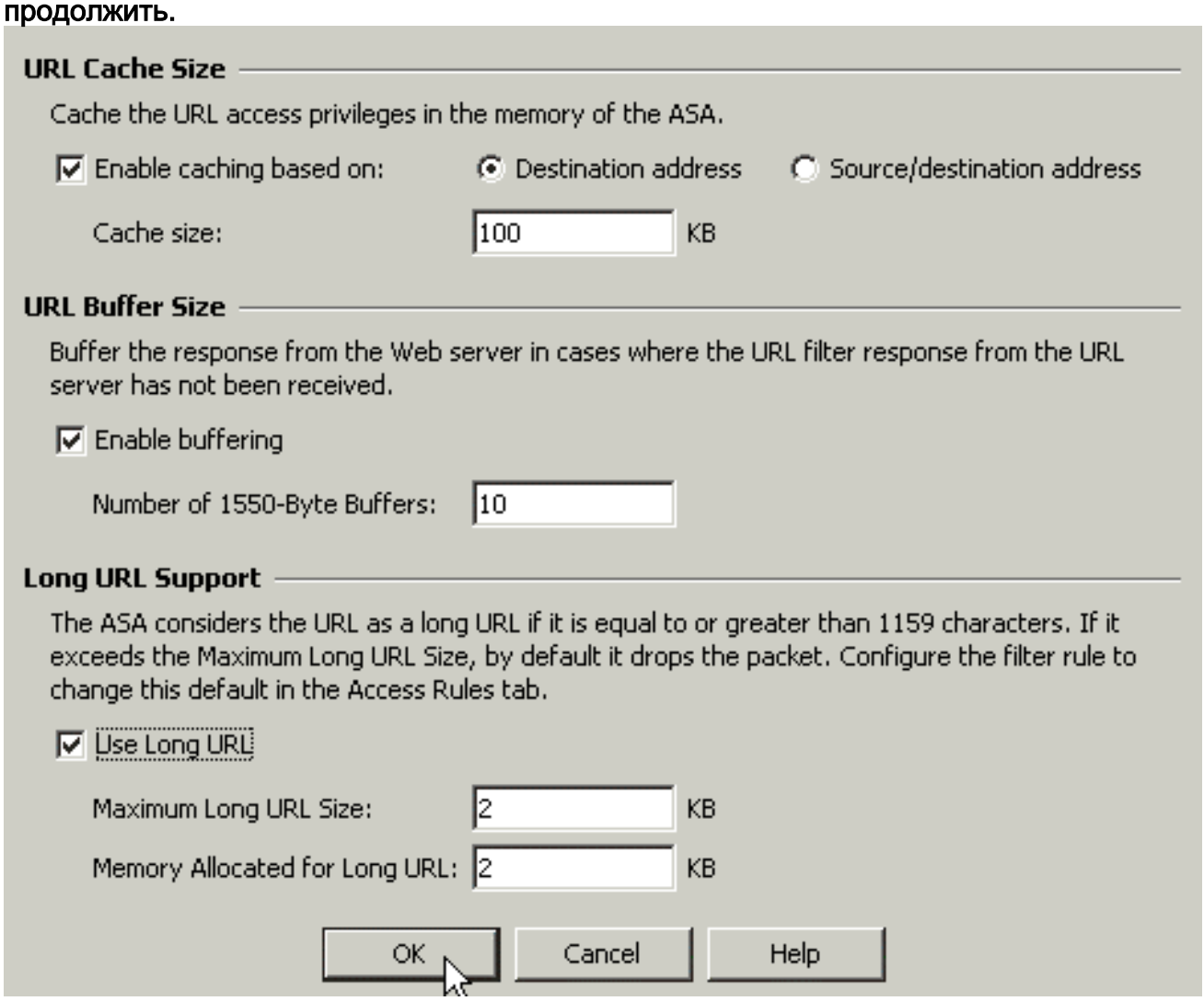


10. Для выбора дополнительных параметров фильтрации URL-адресов снова выберите URL Filtering Servers в раскрывающемся списке Firewall и в главном окне нажмите кнопку

Advanced.



11. Во всплывающем окне настройте параметры, например размер кэша URL-адреса, размер буфера URL-адреса и поддержка длинного URL-адреса. **Во всплывающем окне нажмите OK и в главном окне Apply, чтобы продолжить.**



12. Наконец, убедитесь, что все выполненные изменения сохранены до окончания сеанса ASDM.

Проверка

Используйте команды, приведенные в данном разделе, чтобы просматривать сведения о фильтрации URL-адресов. Чтобы проверить конфигурацию, можно использовать следующие команды.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Используйте OIT для просмотра анализа выходных данных команды show.**

- **show url-server – отображает сведения о сервере фильтрации**Пример:`hostname#show url-server url-server (DMZ) vendor n2h2 host 192.168.15.15 port 4444 timeout 45 protocol tcp connections 10` **В ПО версии 7.2 и более поздних выполните форму show running-config url-server данной команды.**
- **show url-server stats – отображает сведения и статистику сервера фильтрации**В ПО версии 7.2 выполните форму show running-config url-server statistics данной команды.В ПО версии 8.0 и более поздних выполните форму show url-server statistics данной команды.Пример:`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 – отображает конфигурацию буфера блоков URL-адресов**Пример:`hostname#show url-block url-block url-mempool 128 url-block url-size 4 url-block block 128` **ПО версии 7.2 и более поздних выполните форму show running-config url-block данной команды.**
- **show url-block block statistics – отображает статистику блоков URL-адресов**Пример:`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` **В ПО версии 7.2 и более поздних выполните форму show running-config url-block block statistics данной команды.**
- **show url-cache stats – отображает использование кэша**Пример:`hostname#show url-cache stats URL Filter Cache Stats ---------- Size : 128KB Entries : 1724 In Use : 456 Lookups : 45 Hits : 8` **В ПО версии 8.0 и более поздних выполните форму show url-cache statistics данной команды.**
- **show perfmon – отображает статистику производительности фильтрации URL-адресов вместе с другими статистиками производительности.** Статистика фильтрации отображена в строках доступа URL-адресов и запросе сервера URL-адресов.Пример:`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 – отображает конфигурацию фильтрации**Пример:`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` **В ПО версии 7.2 и более поздних выполните форму show running-config filter данной команды.**

Устранение неполадок

Этот раздел предоставляет сведения о том, как устранить неполадки вашей конфигурации.

Ошибка: "%ASA-3-304009: Исчерпал буферные блоки, заданные блокировкой команды URL"

Межсетевой экран исчерпывает кэш URL, который предназначается для удержания ответов сервера, когда межсетевой экран ждет для получения подтверждения от сервера URL.

Решение

Проблема в основном отнесена к задержке между ASA и Сервером Websense. Чтобы решить, что эта проблема пробует эти обходные пути.

- Попытайтесь изменить протокол, который используется на ASA к UDP для передачи с Websense.Существует проблема с задержкой между Сервером Websense и межсетевым экраном, в котором ответы от Сервера Websense занимают много времени для возврата к межсетевому экрану, таким образом это заставляет буфер URL заполняться, в то время как это ждет ответа.Можно использовать UDP вместо TCP для связи между Сервером Websense и Межсетевым экраном. Это вызвано тем, что при использовании TCP для фильтрации URL-адресов, для каждого нового URL-запроса, ASA должен установить TCP - подключение с Сервером Websense. Так как UDP является протоколом без установления соединения, ASA не вынужден установить соединение для получения ответа сервера. Это должно улучшить производительность сервера.`ASA(config)#`**`url-server (inside) vendor websense host X.X.X.X timeout 30`** `protocol UDP version 4 connections 5`
- Удостоверьтесь, что увеличили блочный URL блок до самого высокого возможного значения, который равняется 128. Это может быть проверено с **командой show url-block**.Если это показывает 128, возьмите идентификатор ошибки Cisco CSCta27415 (только зарегистрированные клиенты) усовершенствование в рассмотрение.

Дополнительные сведения

- Поддержка устройств адаптивной безопасности Cisco ASA серии 5500
- Поддержка продуктов устройств защиты Cisco PIX серии 500
- Поддержка продуктов Cisco Adaptive Security Device Manager
- PIX/ASA: Установка и устранение неполадок подключения через устройство защиты Cisco
- Устранение неполадок в подключениях через PIX и ASA
- Cisco Systems – техническая поддержка и документация