SDM: фильтрация URL-адресов на примере конфигурации маршрутизатора Cisco IOS

Содержание

Введение
Предварительные условия
Ограничения для фильтрации URL-адресов Websense межсетевого экрана
Используемые компоненты
Условные обозначения
Общие сведения
Настройте маршрутизатор с CLI
Схема сети
Определение сервера фильтрации
Конфигурация политики фильтрации
Конфигурация для маршрутизатора, которая выполняет версию Cisco IOS 12.4
Настройте маршрутизатор с SDM
Настройка маршрутизатора с помощью SDM
Проверка
Устранение неполадок
Сообщения об ошибках
Дополнительные сведения

Введение

Этот документ иллюстрирует настройку фильтрации URL-адресов на маршрутизаторе Cisco IOS. Возможность фильтрации URL-адресов повышает контролируемость трафика, проходящего через маршрутизатор Cisco IOS. Фильтрация URL-адресов поддерживается в версиях Cisco IOS в версии 12.2 (11) YU и позже.

Примечание: Так как фильтрация URL-адресов способствует большей загрузке ЦП, использование внешнего сервера фильтрации гарантирует, что пропускная способность другого трафика не будет затронута. Когда трафик фильтруется с внешней фильтрацией серверных, на основе скорости вашей сети и емкости вашего сервера фильтрации URL-адресов, время, требуемое для первоначального подключения, может быть заметно медленнее.

Предварительные условия

Ограничения для фильтрации URL-адресов Websense межсетевого экрана

Требование Сервера Websense: для активации этой опции у вас должен быть по крайней

мере один Сервер Websense; но предпочтены два или больше Сервера Websense. Несмотря на то, что нет никакого предела количеству Серверов Websense, которые вы можете иметь, и можно настроить столько серверов, сколько вы желаете, только один сервер может быть активным в любое заданное время — основной сервер. Запросы наведения справки URL передаются только основному серверу.

Ограничение Поддержки Фильтрации URL-адресов: Это поддержки характеристик только одна активная схема фильтрации URL-адресов за один раз. (Перед включением фильтрации URL-адресов Websense необходимо всегда гарантировать, что нет другой настроенной схемы фильтрации URL-адресов, такой как N2H2.)

Ограничение имени пользователя: Эта функция не передает имя пользователя и информацию о группе к Серверу Websense, но Сервер Websense может работать для основанной на пользователе политики, потому что это имеет другой механизм, чтобы позволить имени пользователя соответствовать IP-адресу.

Используемые компоненты

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

- Маршрутизатор Cisco 2801 с Выпуском 12.4 (15) T программного обеспечения Cisco IOS
- Диспетчер устройств защиты CISCO SDM версии 2.5

Примечание: См. Базовую настройку маршрутизатора с помощью SDM, чтобы позволить маршрутизатору быть настроенным SDM.

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

Функция Фильтрации URL-адресов Websense Межсетевого экрана позволяет вашему межсетевому экрану Cisco IOS (также известный как Cisco Secure Integrated Software [CSIS]) взаимодействовать с программным обеспечением фильтрации URL-адресов Websense. Это позволяет вам предотвращать пользовательский доступ к указанным веб-сайтам на основе некоторой политики. Межсетевой экран Cisco IOS работает с Сервером Websense, чтобы знать, может ли определенный URL быть позволен или запрещен (заблокированный).

Настройте маршрутизатор с CLI

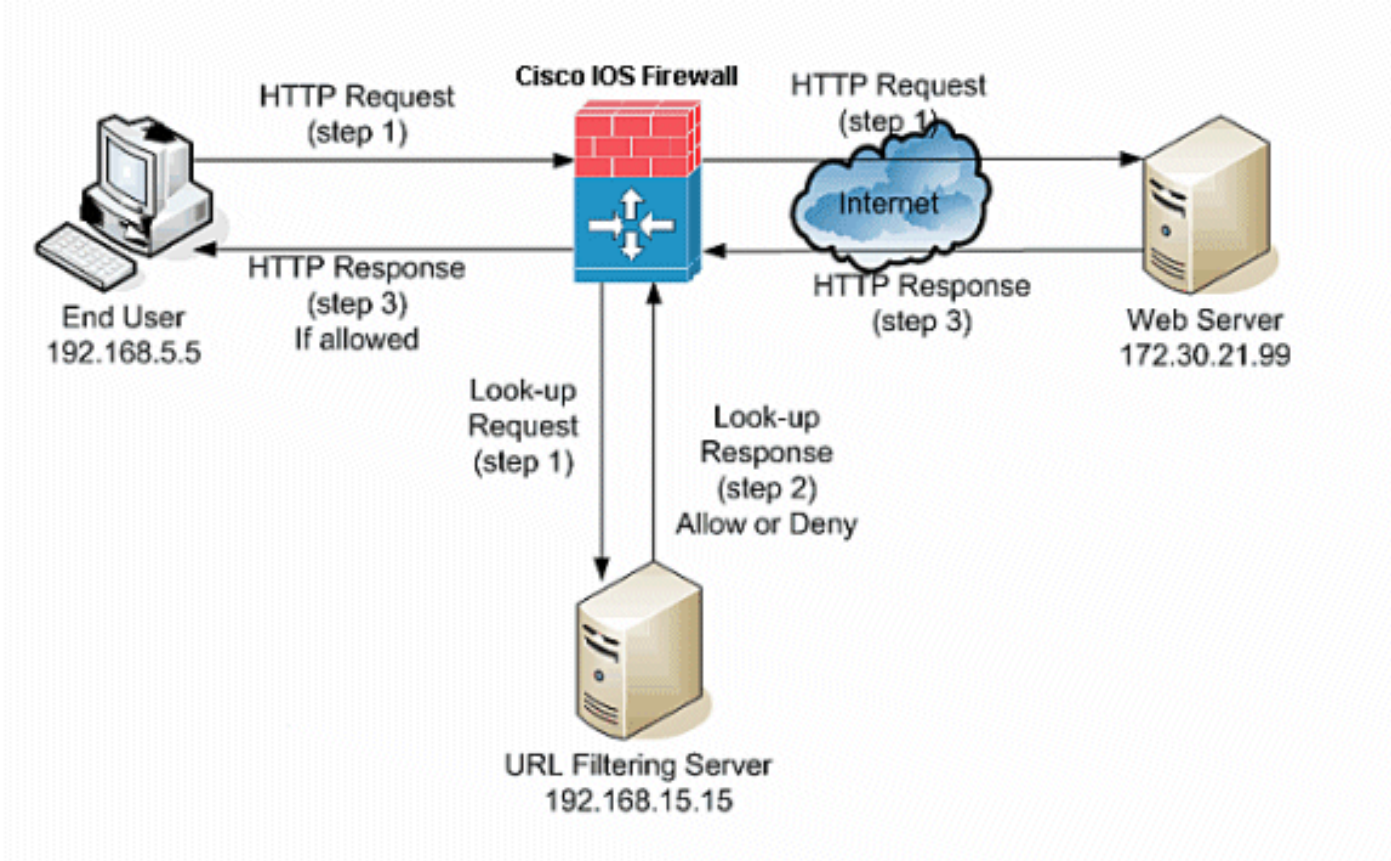
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

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-адресов расположен во внутренней сети. Конечные пользователи, которые находятся внутри сети, пытаются получить доступ к веб-серверу, находящемуся вне сети через Интернет.

Эти шаги выполнены в запросе пользователя для Web-сервера:

1. Конечный пользователь просматривает страницы на веб-сервере, и браузер отправляет HTTP-запрос.
2. После того, как межсетевой экран Cisco IOS получает этот запрос, он пересылает запрос на Web-сервер. Это одновременно извлекает URL и передает запрос наведения справки к серверу фильтрации URL-адресов.
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. Межсетевой экран Cisco IOS® получает этот ответ поиска и выполняет одну из этих функций: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

Необходимо определить адрес фильтрации серверных с **командой ip urlfilter server vendor**. Необходимо определить соответствующую форму данной команды, основываясь на типе сервера фильтрации, который вы используете.

Примечание: 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.

Команда ip urlfilter server vendor определяет сервер, который выполняет N2H2 или приложение фильтрации URL-адресов Websense. Для настройки сервера поставщика для фильтрации URL-адресов используйте **команду ip urlfilter server vendor** в режиме глобальной конфигурации. Для удаления сервера из конфигурации используйте эту команду с параметром no. Это - синтаксис **команды ip urlfilter server vendor**:

```
hostname(config)# ip urlfilter server vendor {websense | n2h2} ip-address [port port-number]
[timeout seconds] [retransmit number] [outside] [vrf vrf-name]
```

Замените `ip-address` IP-адресом сервера Websense. Замените `seconds` кол-вом секунд, которое Межсетевой экран IOS должен продолжить пытаться подключить с фильтрацией серверных.

Например, для настройки одиночной фильтрации серверных Websense для фильтрации URL-адресов, выполните эту команду:

```
hostname(config)#
   ip urlfilter server vendor websense 192.168.15.15
```

Конфигурация политики фильтрации

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

Сокращение длинных URL-адресов HTTP

Чтобы позволить фильтру URL усекать длинные URL к серверу, используйте IP urlfilter усеченная команда в режиме глобальной конфигурации. Для отключения опции усечения используйте эту команду с параметром no. Эта команда поддерживается в версии Cisco IOS 12.4 (6) T и позже.

`ip urlfilter truncate {script-parameters | hostname}` является синтаксисом этой команды.

параметры сценария: Только URL до опций сценария передается. Например, если всем URL является `http://www.cisco.com/dev/xxx.cgi?when=now`, только URL через `http://www.cisco.com/dev/xxx.cgi` передается (если максимальная поддерживаемая длина URL не превышена).

Host name: Только имя хоста передается. Например, если весь URL является `http://www. cisco . com/dev/xxx.cgi? when=now`, только `http://www. cisco . com` передается.

Если параметры сценария и ключевые слова имени хоста оба настроены, ключевое слово параметров сценария имеет приоритет по ключевому слову имени хоста. Если оба ключевых слова настроены, и URL параметров сценария усеченный, и максимальная поддерживаемая длина URL превышена, URL усеченный до имени хоста.

Примечание: Если параметры сценария обоих ключевых слов и имя хоста настроены, они должны быть на отдельных линиях как показано ниже. Они не могут быть объединены в одной линии.

Примечание: `IP urlfilter`

Примечание: `IP urlfilter`

Конфигурация для маршрутизатора, которая выполняет версию Cisco IOS 12.4

В конфигурацию включены команды, описанные в данном документе:

Конфигурация для маршрутизатора, которая выполняет версию Cisco IOS 12.4

```
R3#show running-config : Saved version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec service password-encryption ! hostname R3
! ! !--- username cisco123 privilege 15 password 7
104D000A061843595F ! aaa session-id common ip subnet-
zero ! ! ip cef ! ! ip ips sdf location
flash://128MB.sdf ip ips notify SDEE ip ips po max-
events 100 !--- use the ip inspect name command in
global configuration mode to define a set of inspection
rules. This Turns on HTTP inspection. The urlfilter
keyword associates URL filtering with HTTP inspection.
ip inspect name test http urlfilter !--- use the ip
urlfilter allow-mode command in global configuration
mode to turn on the default mode (allow mode) of the
filtering algorithm. ip urlfilter allow-mode on !--- use
the ip urlfilter exclusive-domain command in global
configuration mode to add or remove a domain name to or
from the exclusive domain list so that the firewall does
not have to send lookup requests to the vendor server.
Here we have configured the IOS firewall to permit the
URL www.cisco.com without sending any lookup requests to
the vendor server. ip urlfilter exclusive-domain permit
www.cisco.com !--- use the ip urlfilter audit-trail
command in global configuration mode to log messages
into the syslog server or router. ip urlfilter audit-
trail !--- use the ip urlfilter urlf-server-log command
in global configuration mode to enable the logging of
system messages on the URL filtering server. ip
urlfilter urlf-server-log !--- use the ip urlfilter
server vendor command in global configuration mode to
```

```
configure a vendor server for URL filtering. Here we
have configured a websense server for URL filtering ip
urlfilter server vendor websense 192.168.15.15 no ftp-
server write-enable ! ! !--- Below is the basic
interface configuration on the router interface
FastEthernet0 ip address 192.168.5.10 255.255.255.0 ip
virtual-reassembly !--- use the ip inspect command in
interface configuration mode to apply a set of
inspection rules to an interface. Here the inspection
name TEST is applied to the interface FastEthernet0. ip
inspect test in duplex auto speed auto ! interface
FastEthernet1 ip address 192.168.15.1 255.255.255.0 ip
virtual-reassembly duplex auto speed auto ! interface
FastEthernet2 ip address 10.77.241.109 255.255.255.192
ip virtual-reassembly duplex auto speed auto ! interface
FastEthernet2 no ip address ! interface Vlan1 ip address
10.77.241.111 255.255.255.192 ip virtual-reassembly ! ip
classless ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65 ! ! !---
Configure the below commands to enable SDM access to the
cisco routers ip http server ip http authentication
local no ip http secure-server ! ! line con 0 line aux 0
line vty 0 4 privilege level 15 transport input telnet
ssh ! end
```

Настройте маршрутизатор с SDM

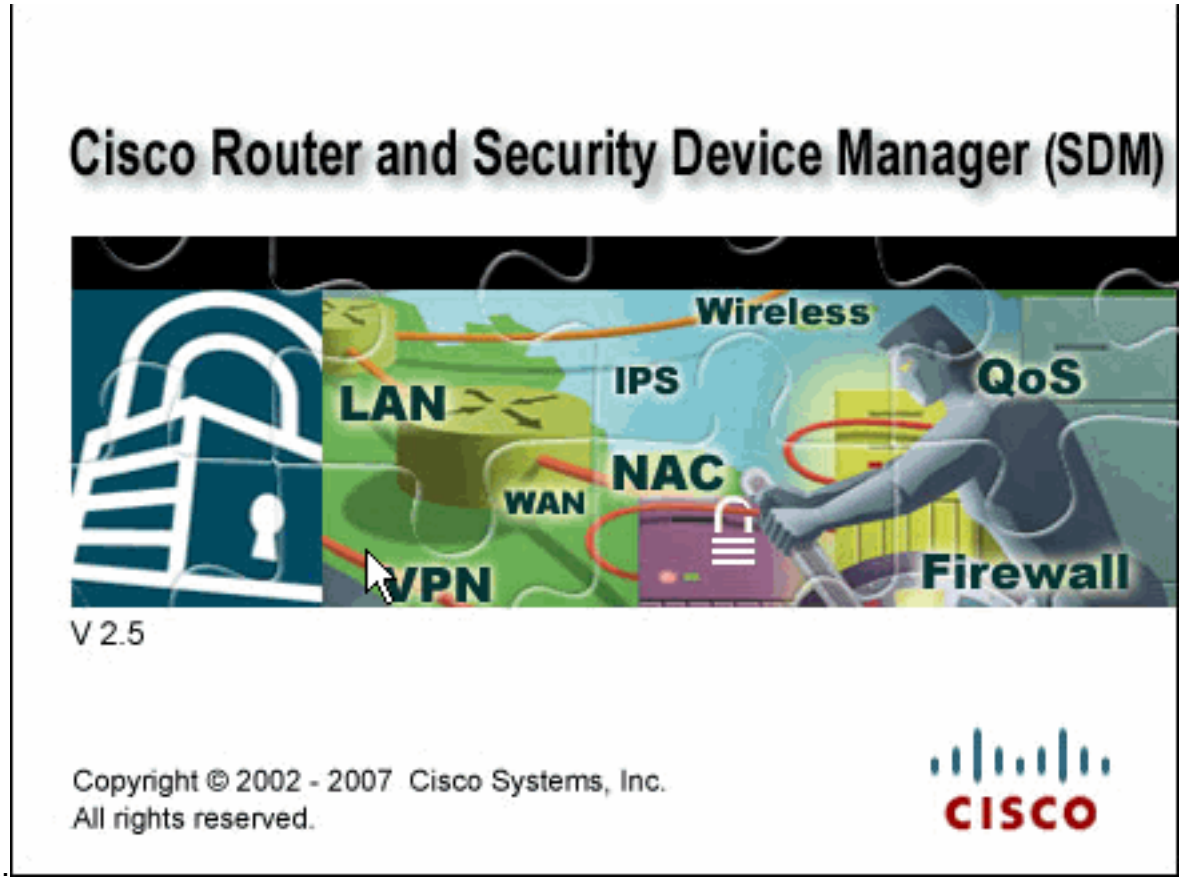
Настройка маршрутизатора с помощью SDM

Выполните эти шаги для настройки фильтрации URL-адресов на маршрутизаторе Cisco IOS:

Примечание: Для настройки Фильтрации URL-адресов с SDM используйте **команду ip inspect name** в режиме глобальной конфигурации для определения ряда инспекционных правил. Это включает Проверку HTTP. Ключевое слово urlfilter привязывает фильтрацию URL-адресов к Проверке HTTP. Затем инспекционное настроенное название может быть сопоставлено с интерфейсом, на котором фильтрация должна быть сделана, например:

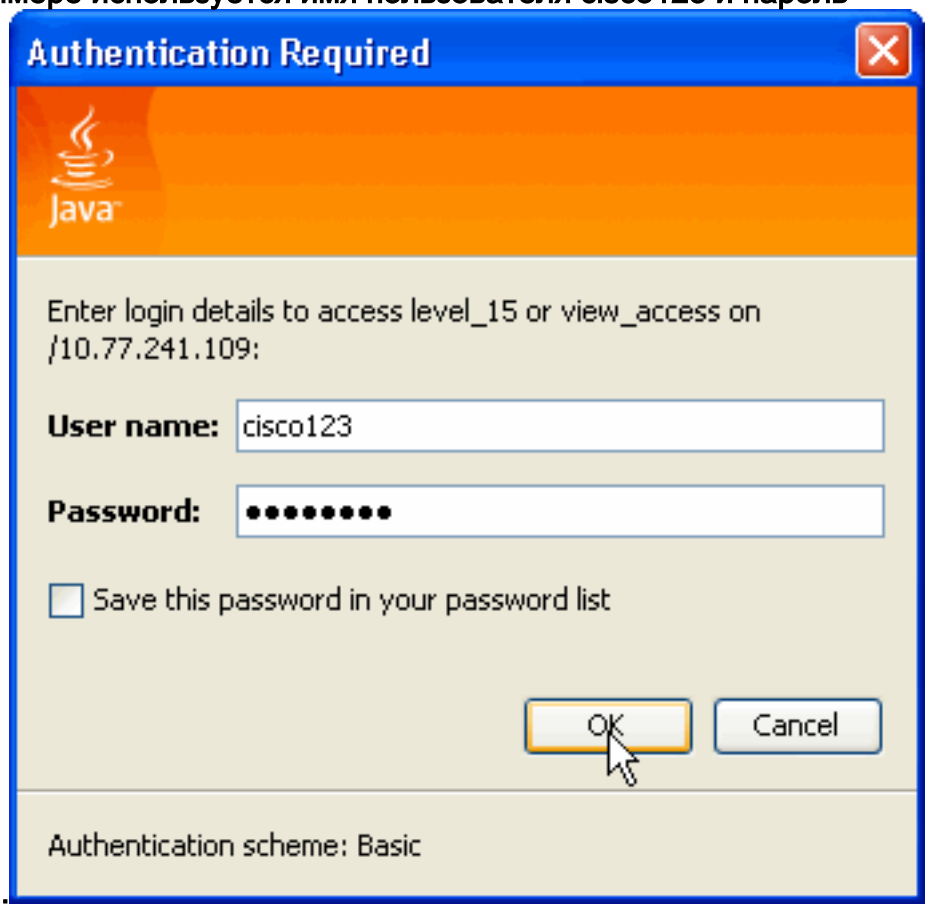
```
hostname(config)#ip inspect
   name test http urlfilter
```

1. **Откройте браузер и введите адрес https://<IP_адрес интерфейса_маршрутизатора,_который_необходимо_настроить_для_доступа_SDM>, чтобы подключиться к SDM на маршрутизаторе.**Удостоверьтесь, что авторизовали любые предупреждения, которые ваш браузер дает вам отнесенный подлинности сертификата SSL. По умолчанию имя пользователя и пароль являются пустыми.Маршрутизатор отобразит следующее окно для загрузки приложения SDM. В данном примере используется приложение, загруженное на локальный компьютер, а не приложение



Java.

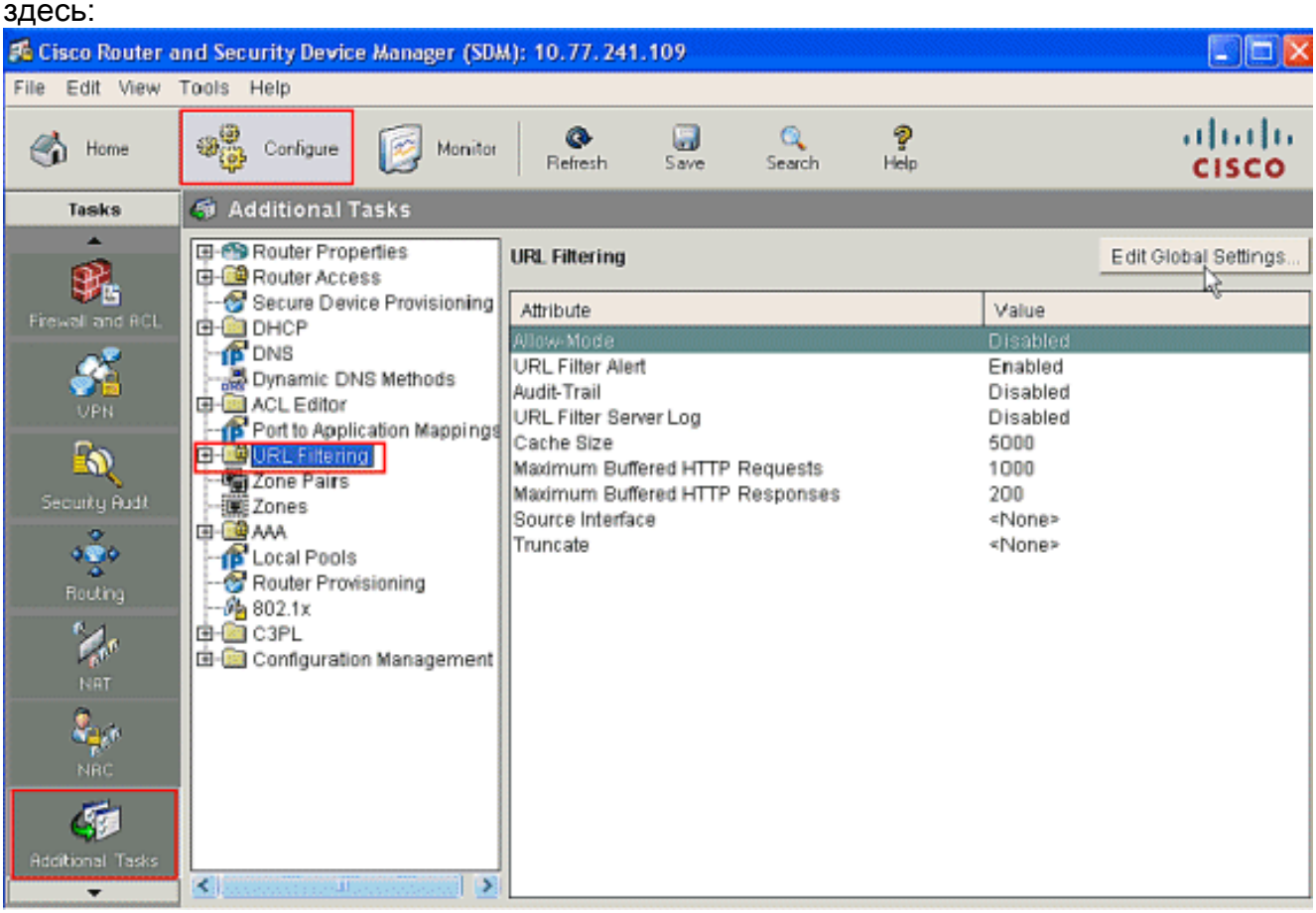
2. Начнется загрузка SDM. После загрузки SDM Launcher выполните все шаги, сопровождаемые соответствующими подсказками, необходимые для установки приложения и запуска Cisco SDM Launcher.
3. **Введите имя пользователя и пароль (если вы их ранее указали) и нажмите кнопку OK.В этом примере используется имя пользователя cisco123 и пароль**



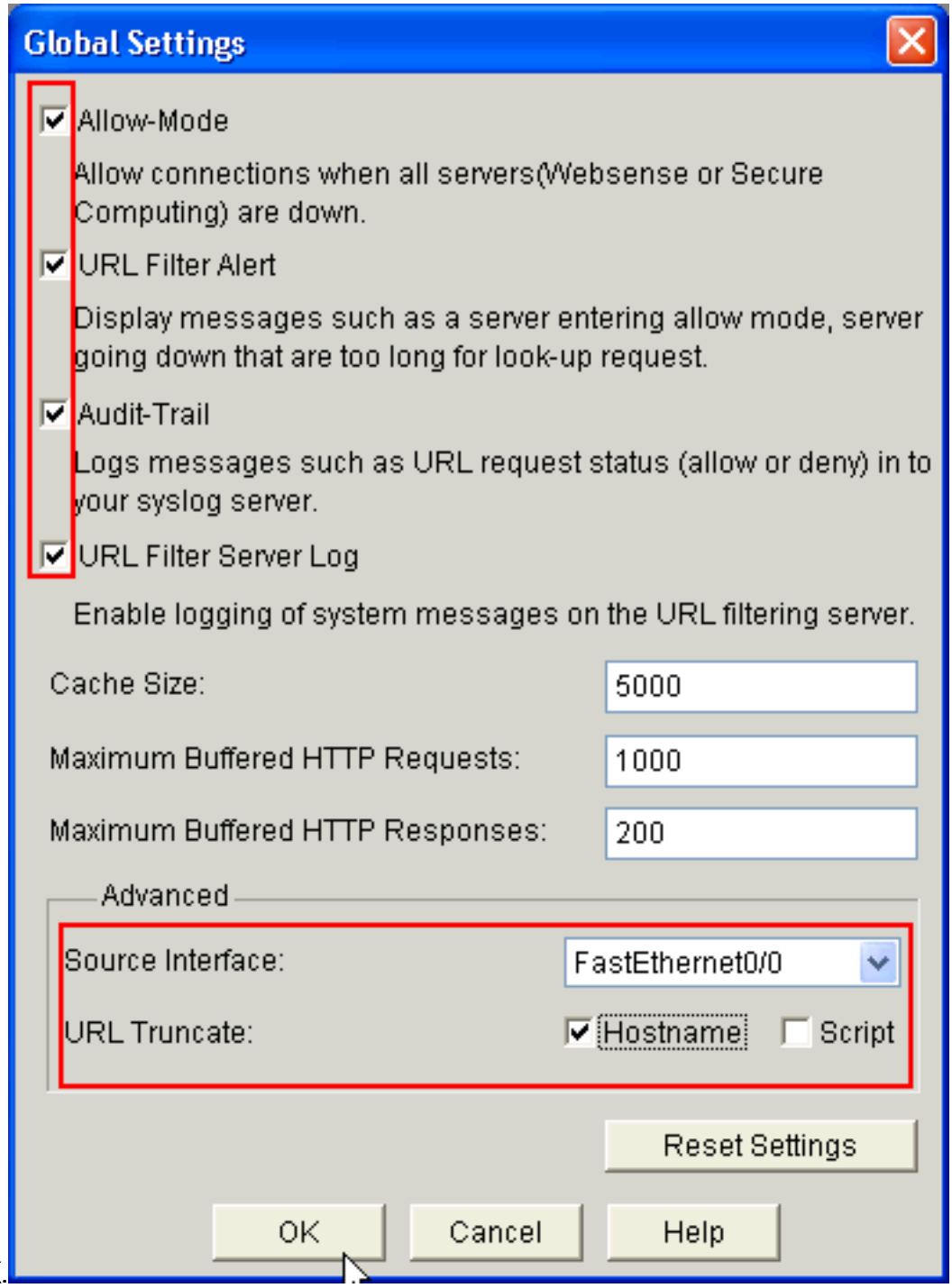
cisco123.

4. Выберите **Configuration-> Additional Tasks** и нажмите **URL Filtering** на домашней

странице SDM. Затем нажмите **Edit Global Settings**, как показано здесь:

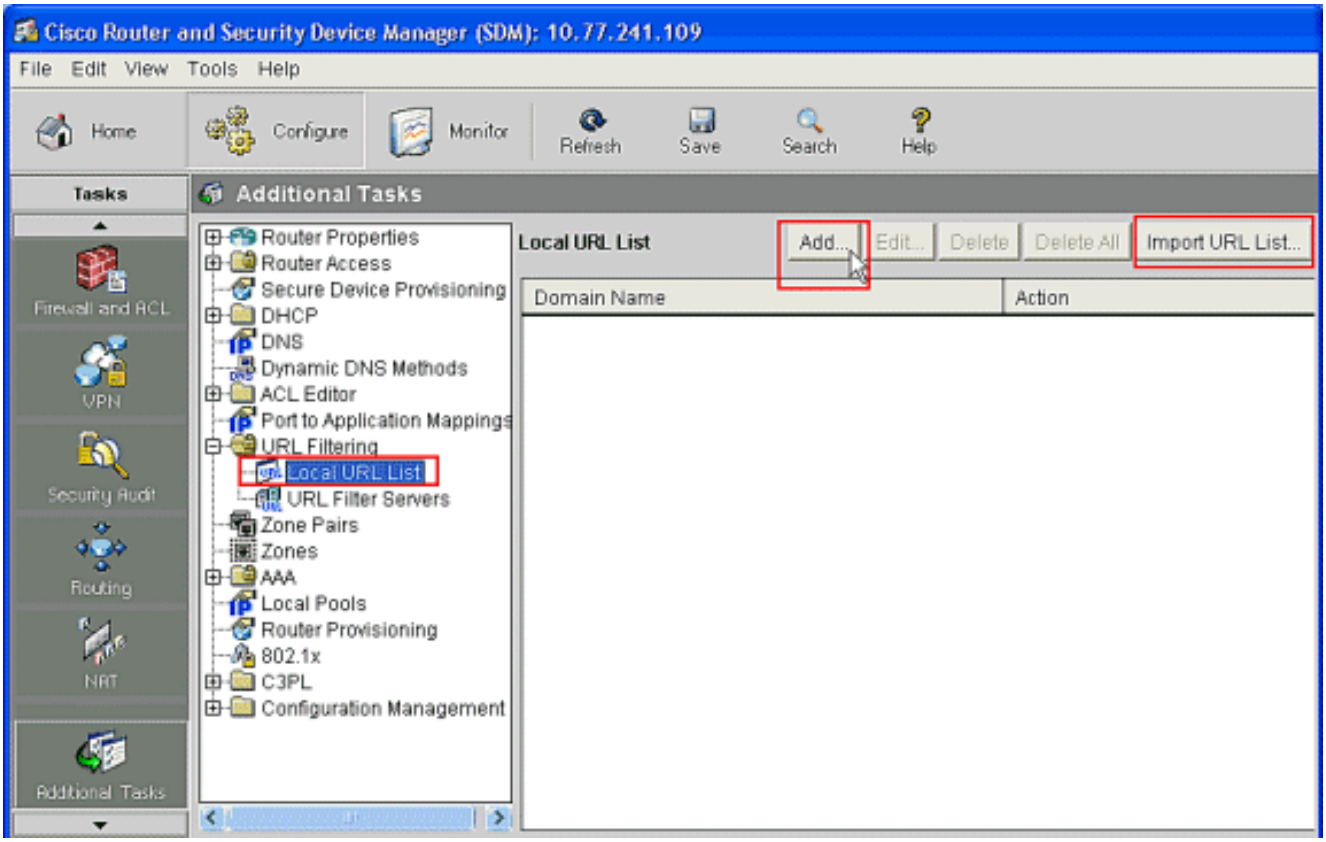


5. В новом окне, которое появляется, включите параметры, требуемые для фильтрации URL-адресов, такие как **Allow-Mode, Предупреждение Фильтра URL, Контрольное Испытание** и **Журнал сервера Фильтрации URL-адресов**. Проверьте флажки рядом с каждым параметры как показано. Теперь предоставьте **Размер кэша** и информацию **о Буфере HTTP**. Также предоставьте **Исходный интерфейс** и URL Усеченный метод под **Усовершенствованным** разделом как показано, чтобы позволить фильтру URL усекать длинные URL к серверу. (Здесь параметр Усечения выбран в качестве **Имени хоста**.) Теперь нажимают

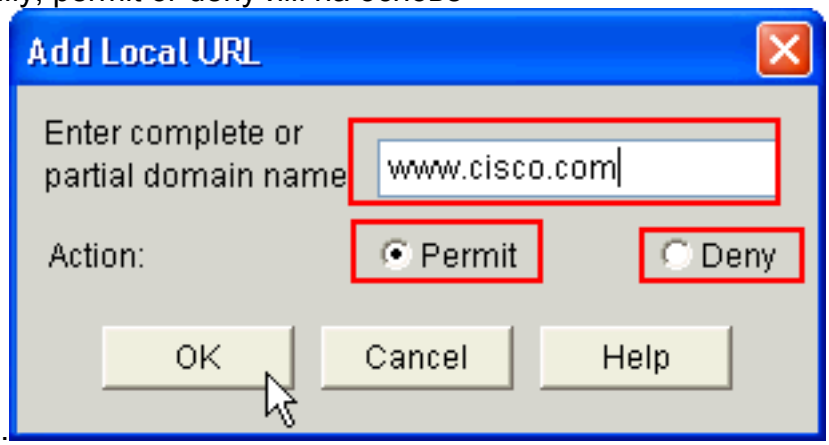


OK.

6. Теперь выберите опцию **Local URL List**, расположенную под вкладкой **URL Filtering**. **Нажмите Add**, чтобы добавить доменное имя и настроить межсетевой экран для permit or deny добавленного доменного имени. Если список необходимых URL присутствует как файл, можно также выбрать **опцию Import URL List**. Выбор является вашим для выбора **Add URL** или опций **Import URL List** на основе требования и доступности Списка URL -
адресов.

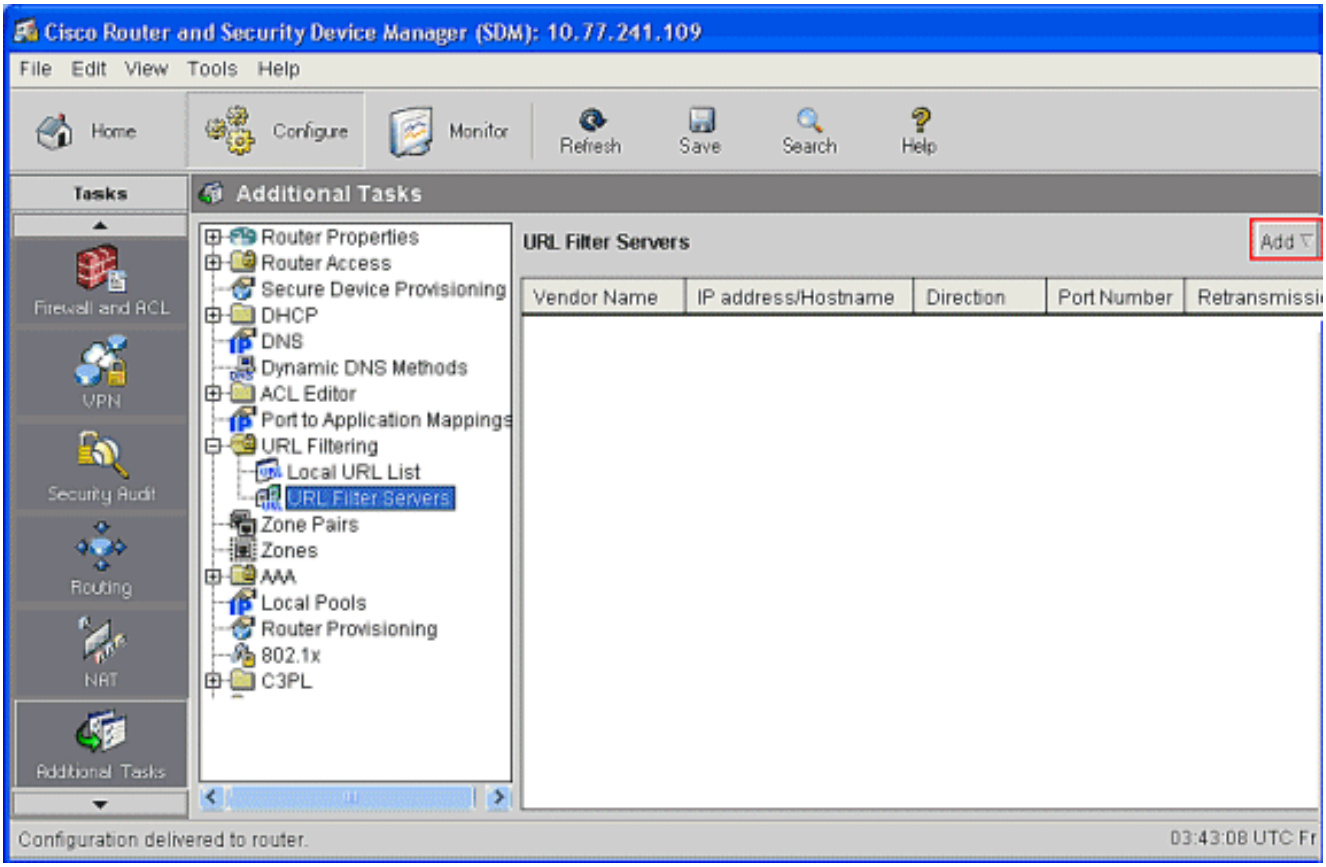


7. В данном примере **нажмите Add**, чтобы добавить URL и настроить Межсетевой экран IOS для permit or deny URL как требуется. Теперь новое окно назвало **ADD**, который открывает **Локальный URL**, в котором пользователь должен предоставить доменное имя и решить, permit ли or deny URL. Нажмите кнопку с зависимой фиксацией рядом с Разрешением или опцией Deny как показано. Здесь доменным именем является **www. cisco . com** и пользователь **разрешают URL www. cisco . com**. Таким же образом можно **нажмите Add**, добавить как много URL по мере необходимости и настроить межсетевой экран любому, permit or deny им на основе

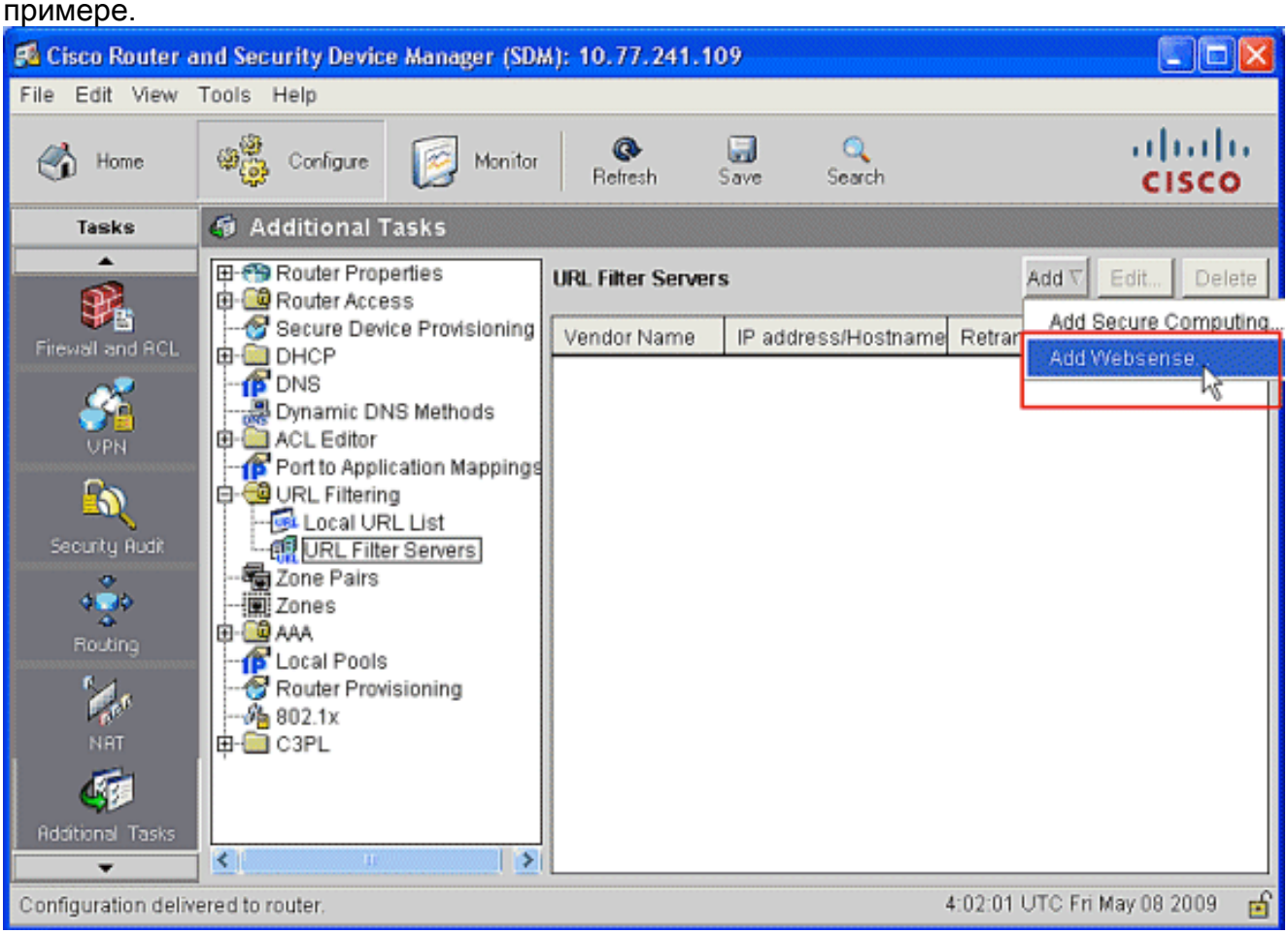


требования.

8. Выберите **URL Filter Servers option**, расположенный под вкладкой **URL Filtering**, как показано. **Нажмите Add** для добавления Имени сервера Фильтрации URL-адресов, которое выполняет функцию URL
Filtering.

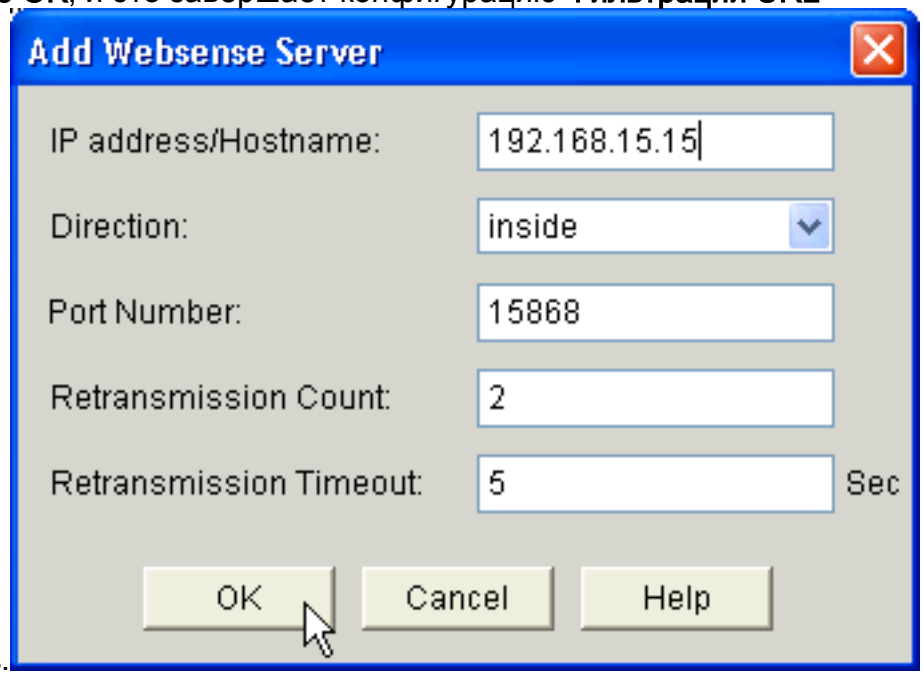


9. После того, как вы **нажмите Add**, выберете фильтрацию серверных в качестве **Websense** как показано ниже, так как Фильтрация серверных Websense используется в данном
примере.



10. В этом окне **Add Websense Server** предоставьте **IP-адрес** Сервера Websense наряду с **Направлением**, в котором фильтр работает и **Номер порта,** (Номер порта по

умолчанию для Сервера Websense **15868**). Также предоставьте **количество Повторной передачи** и значения **Тайм-аута повторной передачи**, как показано. **Нажмите OK**, и это завершает конфигурацию **Фильтрации URL-адресов**.



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 ip urlfilter statistics — Показывает информацию и статистику о фильтрации серверныхПример:`Router# show ip urlfilter statistics URL filtering statistics ================ Current requests count:25 Current packet buffer count(in use):40 Current cache entry count:3100 Maxever request count:526 Maxever packet buffer count:120 Maxever cache entry count:5000 Total requests sent to URL Filter Server: 44765 Total responses received from URL Filter Server: 44550 Total requests allowed: 44320 Total requests blocked: 224`
- show ip urlfilter cache — Отображает максимальное число записей, которые могут кэшироваться в таблицу кэш-памяти, количество записей и IP - адреса назначения, которые кэшируются в таблицу кэш-памяти, когда вы используете команду show ip urlfilter cache в привилегированном режиме EXEC
- config фильтра urlfilter show ip — Показывает конфигурацию фильтрацииПример:`hostname#show ip urlfilter config URL filter is ENABLED Primary Websense server configurations ======================================= Websense server IP address Or Host Name: 192.168.15.15 Websense server port: 15868 Websense retransmission time out: 6 (in seconds) Websense number of retransmission: 2 Secondary Websense servers configurations === None Other configurations ==================== Allow Mode: ON System Alert: ENABLED Audit Trail: ENABLED Log message on Websense server: ENABLED Maximum number of cache entries: 5000 Maximum number of packet buffers: 200 Maximum outstanding requests: 1000`

Устранение неполадок

Сообщения об ошибках

`%URLF-3-SERVER_DOWN: Connection to the URL filter server 10.92.0.9 is down` — Этот уровень три индикатора сообщения LOG_ERR-типа, когда выключается настроенный UFS. Когда это произойдет, межсетевой экран отметит настроенный сервер как вторичный и попытается перевести один в рабочее состояние из других дополнительных серверов и отметить тот сервер как основной сервер. Если не будет никакого другого настроенного сервера, то межсетевой экран войдет, позволяют режим и отображают сообщение `URLF-3-ALLOW_MODE`.

`%URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE is OFF` — Этот LOG_ERR вводит индикаторы сообщения, когда все UFSs не работают, и система входит, позволяют режим.

Примечание: Каждый раз, когда система входит, позволяют режим (все серверы фильтра не работают), периодический таймер поддержки активности инициирован что попытки открыть TCP - подключение и перевести сервер в рабочее состояние.

`%URLF-5-SERVER_UP: Connection to an URL filter server 10.92.0.9 is made; the system is returning from ALLOW MODE` — Этот LOG_NOTICE-тип индикаторы сообщения, когда UFSs обнаружены как и система, возвращается из позволять режима.

`%URLF-4-URL_TOO_LONG:URL too long (more than 3072 bytes), possibly a fake packet?` — Эти индикаторы сообщения LOG_WARNING-типа, когда URL в запросе наведения справки является слишком длинным; любой URL дольше, чем 3K отброшен.

`%URLF-4-MAX_REQ: The number of pending request exceeds the maximum limit <1000>` — Этот LOG_WARNING-тип индикаторы сообщения, когда количество запросов в состоянии ожидания в системе превышает ограничение максимального значения и все дальнейшие запросы, отброшен.

Дополнительные сведения

- (межсетевой экран Cisco IOS)
- Фильтрация URL-адресов Websense межсетевого экрана
- Руководство по конфигурации безопасности Cisco IOS, выпуск, с 12.4 поддержкой
- Cisco Systems – техническая поддержка и документация