ASA 8. X и позже: Добавьте или Модифицируйте Список доступа через Пример Конфигурации GUI ASDM

Содержание

Введение

Этот документ объясняет, как использовать Cisco Adaptive Security Device Manager (ASDM) для работы со списками контроля доступа. Это включает создание нового списка доступа, как отредактировать существующий список доступа и другую функциональность со списками доступа.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Устройство адаптивной защиты Cisco (ASA) с версией 8.2. X
- Cisco Adaptive Security Device Manager (ASDM) с версией 6.3. X

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

Списки доступа прежде всего используются для управления трафиком через межсетевой экран. Можно позволить или запретить определенные типы трафика со списками доступа. Каждый список доступа содержит много записей списка доступа (ACE), которые управляют трафиком от определенного источника до определенного назначения. Обычно, этот список доступа связан с интерфейсом уведомить направление потока, в который это должно посмотреть. Списки доступа в основном категоризированы в два широких типа.

1. Списки доступа на вход
2. Списки исходящего доступа

Списки доступа на вход применяются к трафику, который вводит тот интерфейс, и списки исходящего доступа применяются к трафику, который выходит из интерфейса. Входящая/исходящая нотация относится к направлению трафика с точки зрения того интерфейса, но не к перемещению трафика между выше и интерфейсы с более низким уровнем безопасности.

Для TCP и UDP - подключений, вам не нужен список доступа, чтобы позволить возвращать трафик, потому что устройство безопасности позволяет весь трафик возврата для установленных двунаправленных подключений. Для протоколов без установления соединения, таких как ICMP, устройство безопасности устанавливает однонаправленные сеансы, таким образом, вам или нужны списки доступа для применения списков доступа к источнику и интерфейсам назначения для разрешения ICMP в обоих направлениях, или необходимо включить механизм Инспектирования icmp. Механизм Инспектирования icmp рассматривает сеансы ICMP как двунаправленные подключения.

От версии 6.3. X ASDM существует два типа списков доступа, которые можно настроить.

1. Интерфейсные правила доступа
2. Правила глобального доступа

Примечание: Правило доступа относится к записи списка индивидуального адреса (ACE).

Интерфейсные правила доступа связаны с любым интерфейсом во время их создания. Не связывая их с интерфейсом, вы не можете создать их. Это отличается от примера Командной строки. С CLI вы сначала создаете список доступа с **командой списка доступа**, и

затем связываете этот список доступа с интерфейсом с **командой access-group**. ASDM 6.3 и позже, список доступа создан и связан с интерфейсом как одиночная задача. Это применяется к потоку трафика через тот определенный интерфейс только.

Правила глобального доступа не связаны ни с каким интерфейсом. Они могут быть настроены через Вкладку Диспетчер ACL в ASDM и применены к глобальному входному трафику. Когда существует соответствие на основе источника, назначения и типа протокола, они внедрены. Эти правила не реплицированы в каждый интерфейс, таким образом, они сохраняют область памяти.

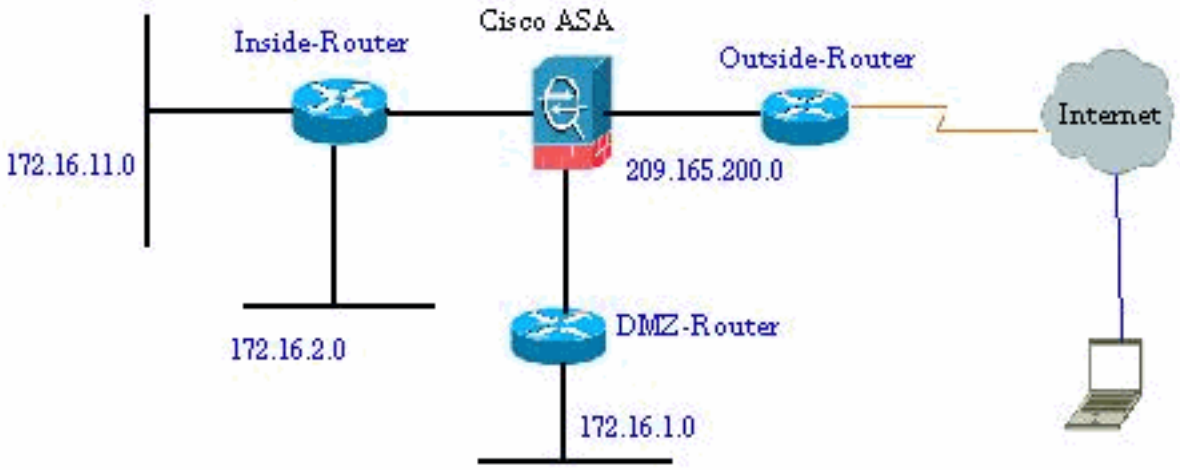
Когда оба этих правила состоят в том, чтобы быть внедрены, интерфейсные правила доступа обычно берет приоритеты по правилам глобального доступа.

Настройка

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

Схема сети

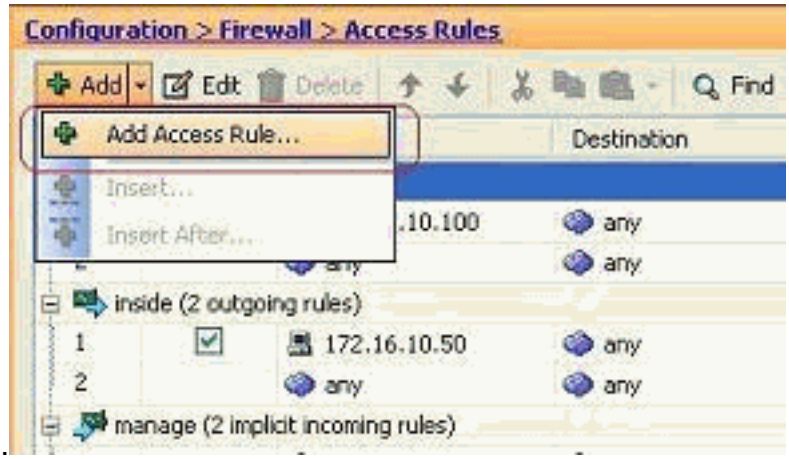
В настоящем документе используется следующая схема сети:



Добавьте новый список доступа

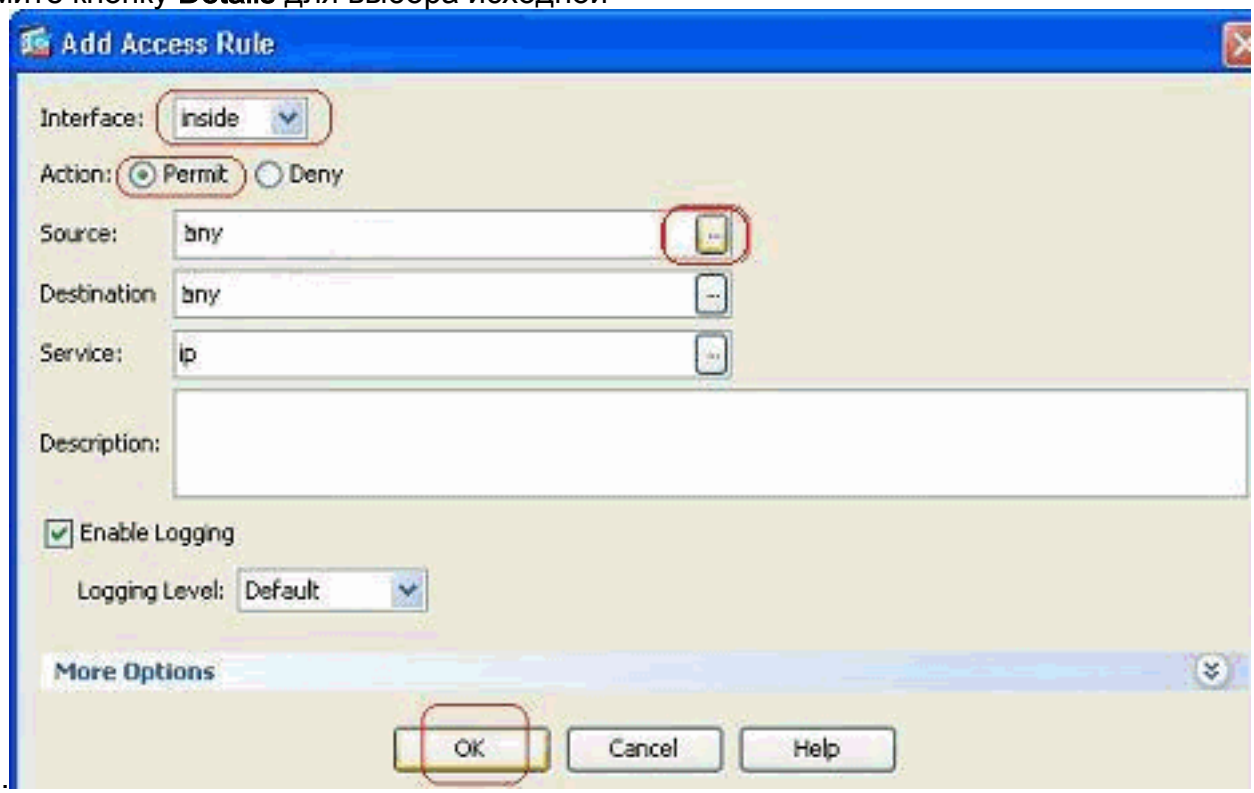
Выполните эти шаги для создания нового списка доступа с ASDM:

1. Выберите **Configuration> Firewall> Access Rules** и нажмите кнопку **Add Access**



Rule.

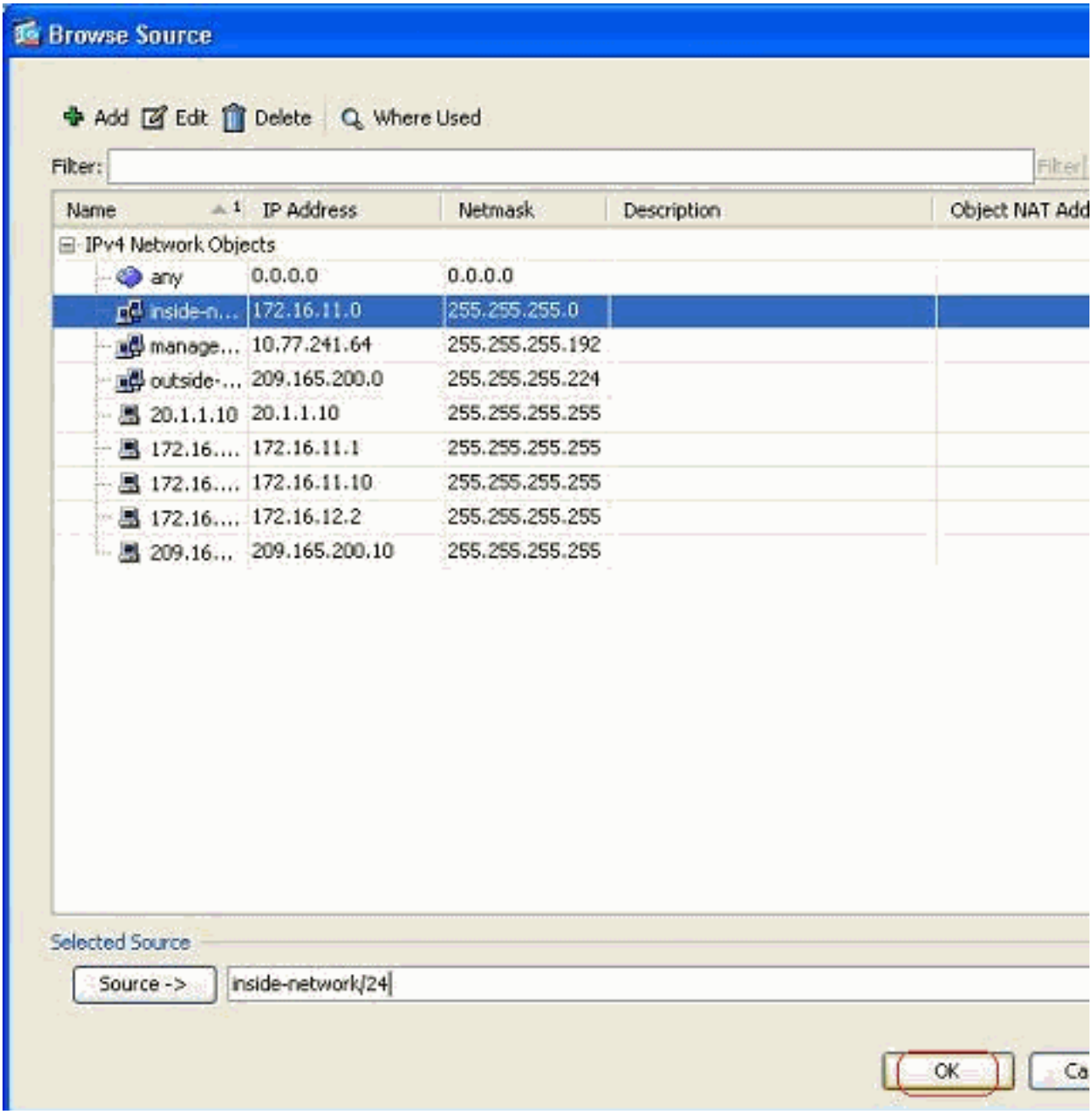
2. Выберите интерфейс, к которому этот список доступа имеет к связанному, наряду с действием, которое будет выполнено на трафике, т.е. разрешить/запретить. Затем нажмите кнопку **Details** для выбора исходной



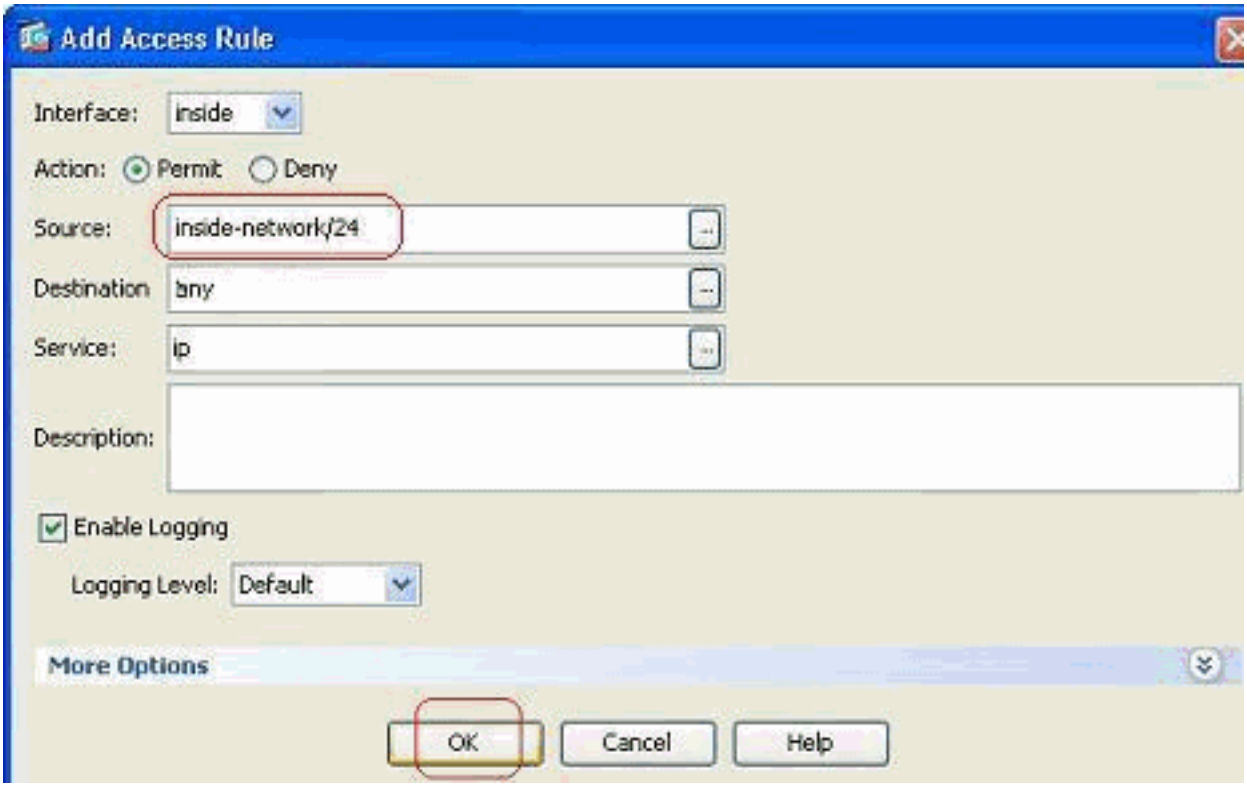
сети.

Примечание: Вот краткое объяснение других полей, которые показывают в этом окне:**Интерфейс** — Определяет интерфейс, с которым связан этот список доступа.**Действие** — Определяет тип действия нового правила. Две опции доступны. **Разрешение** позволяет весь аналогичный трафик, и **Запретите**, блокирует весь аналогичный трафик.**Источник** — Это поле задает источник трафика. Это может быть чем-либо среди Одного IP-адреса, сети, IP-адреса интерфейса межсетевого экрана или группы сетевых объектов. Они могут быть выбраны кнопкой **Details**.**Destination** поле задает источник трафика. Это может быть чем-либо среди Одного IP-адреса, сети, IP-адреса интерфейса межсетевого экрана или группы сетевых объектов. Они могут быть выбраны кнопкой **Details**.**Сервис** — Это поле определяет протокол или сервис трафика, к которому применен этот список доступа. Можно также определить группу сервисов, которая содержит ряд других протоколов.

3. После нажатия кнопки **Details** новое окно, которое содержит Объекты существующей сети, отображено. Выберите **внутреннюю сеть** и нажмите **OK**.

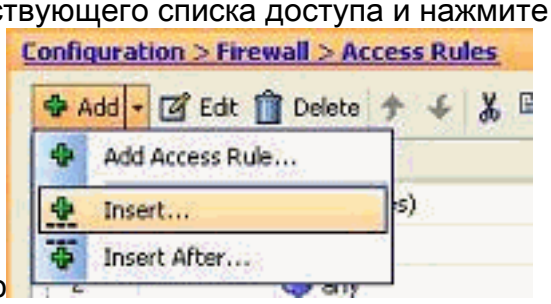


4. Вы возвращены к окну **Add Access Rule**. Введите **любого** в Поле Назначение. и нажмите **OK** для завершения конфигурации правила доступа.

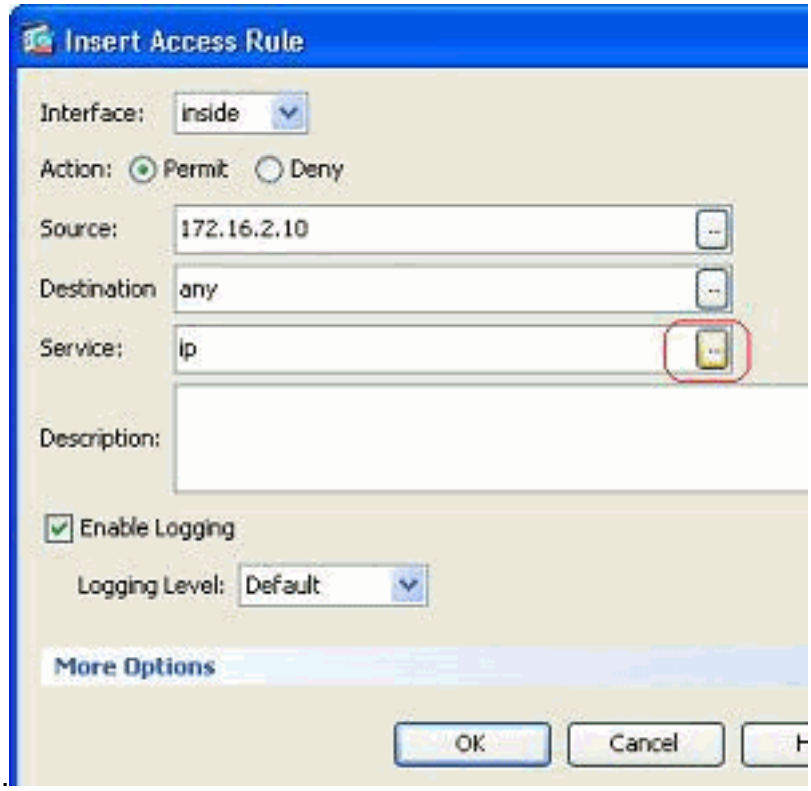


Добавьте правило доступа перед существующим:

Выполните эти шаги для добавления правила доступа незадолго до уже существующего правила доступа:

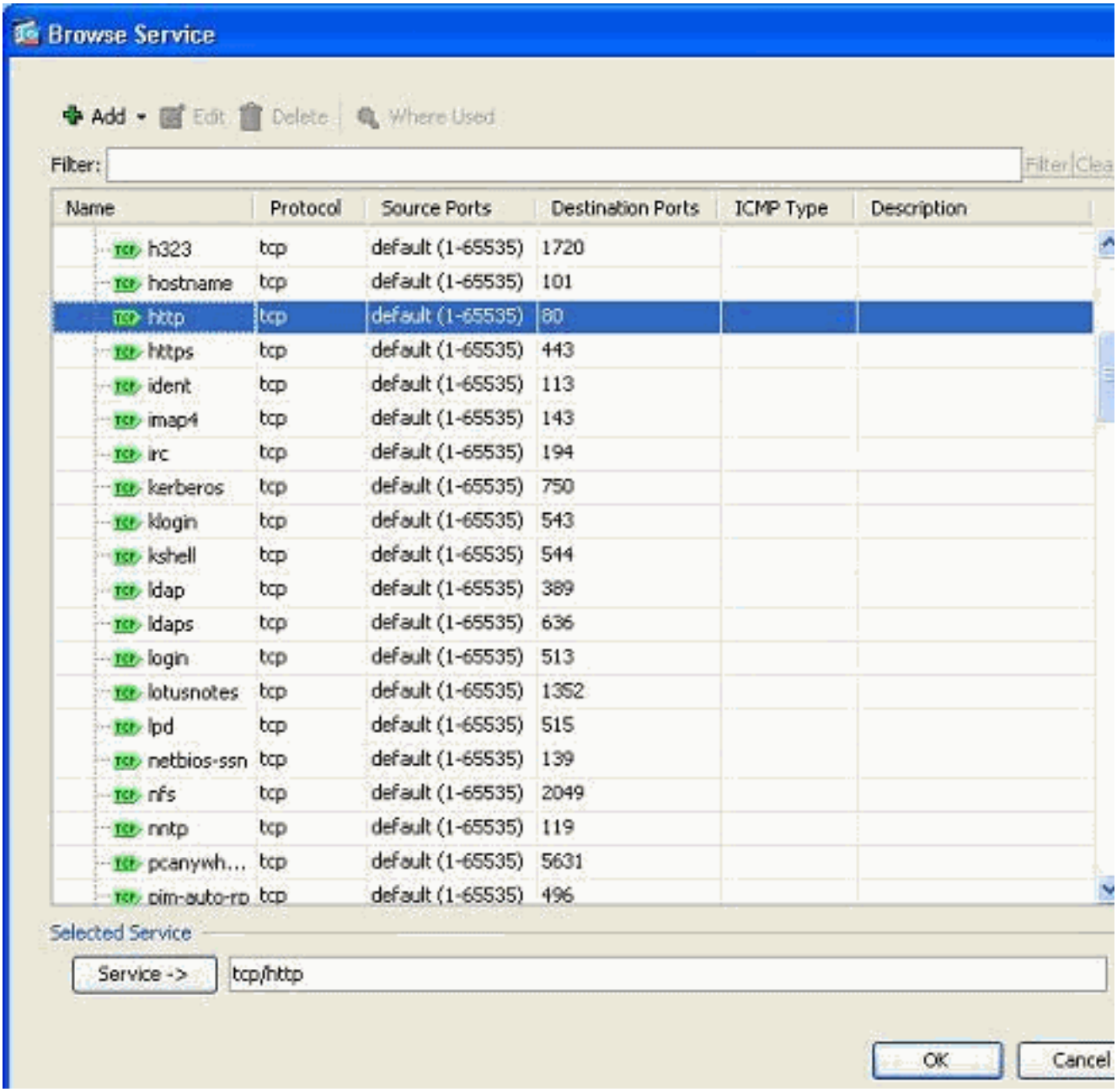
1. Выберите запись существующего списка доступа и нажмите **Insert** от **Добавить** раскрывающегося меню 

2. Выберите Source и Destination, и нажмите кнопку **Details** поля Service для выбора



Protocol.

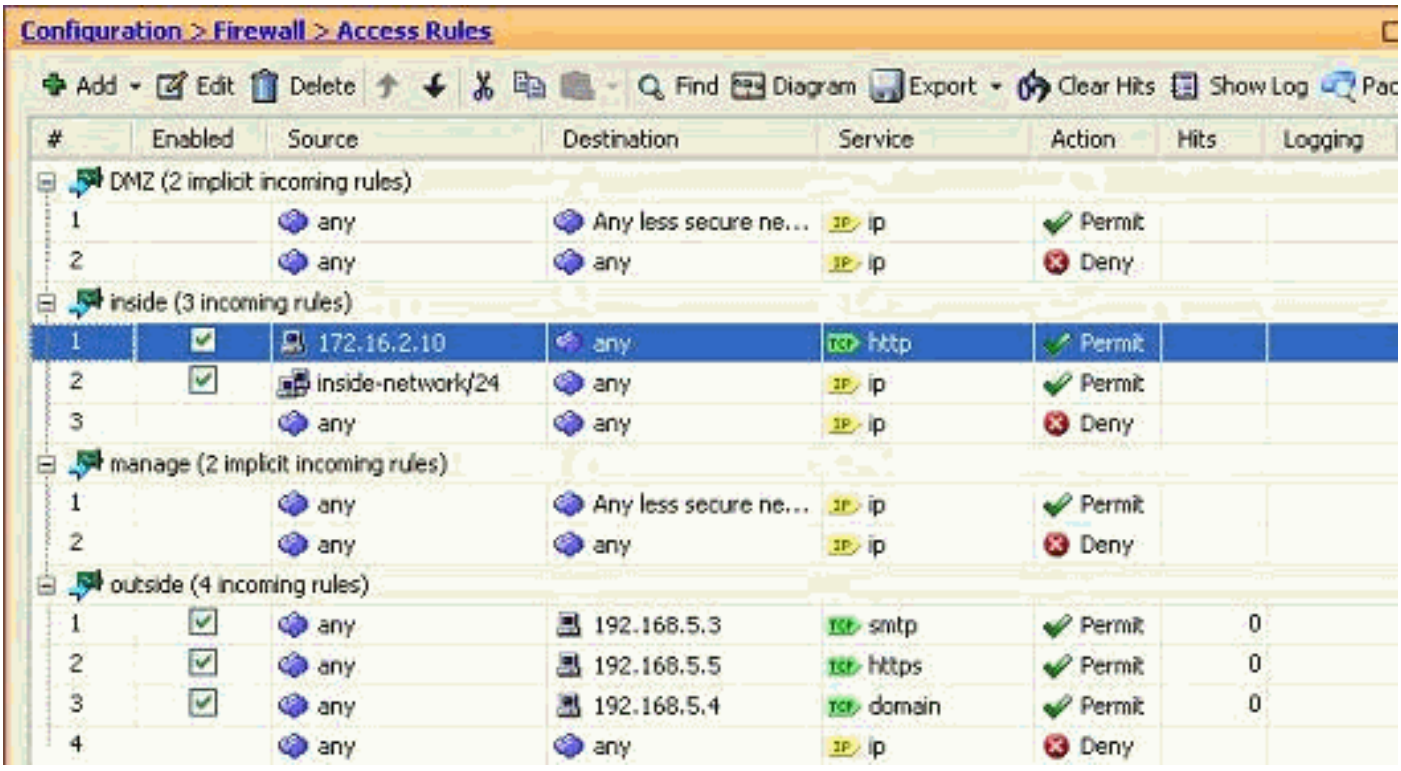
3. Выберите HTTP протокол и нажмите **OK**.



4. Вы возвращены к окну Insert Access Rule. Поле Service заполнено **tcp/http** как выбранный протокол. Нажмите **OK** для завершения конфигурации записи нового

списка доступа.

Уже можно теперь наблюдать новое правило доступа, показанное незадолго до существующая запись для Внутренней сети.

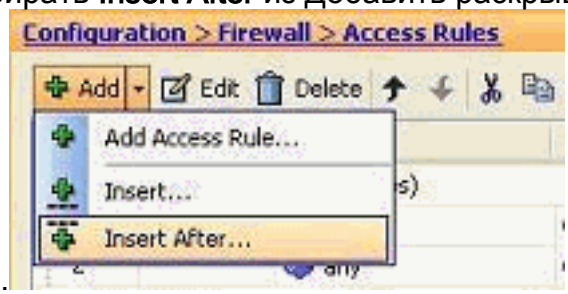


Примечание: Заказ правил доступа очень важен. При обработке каждого пакета для фильтрации ASA исследует, если пакет совпадает с каким-либо критерием правила доступа в последовательном порядке и если соответствие происходит, это внедряет действие того правила доступа. Когда с правилом доступа совпадают, оно не продолжает далее обращаться к правилам и проверять их снова.

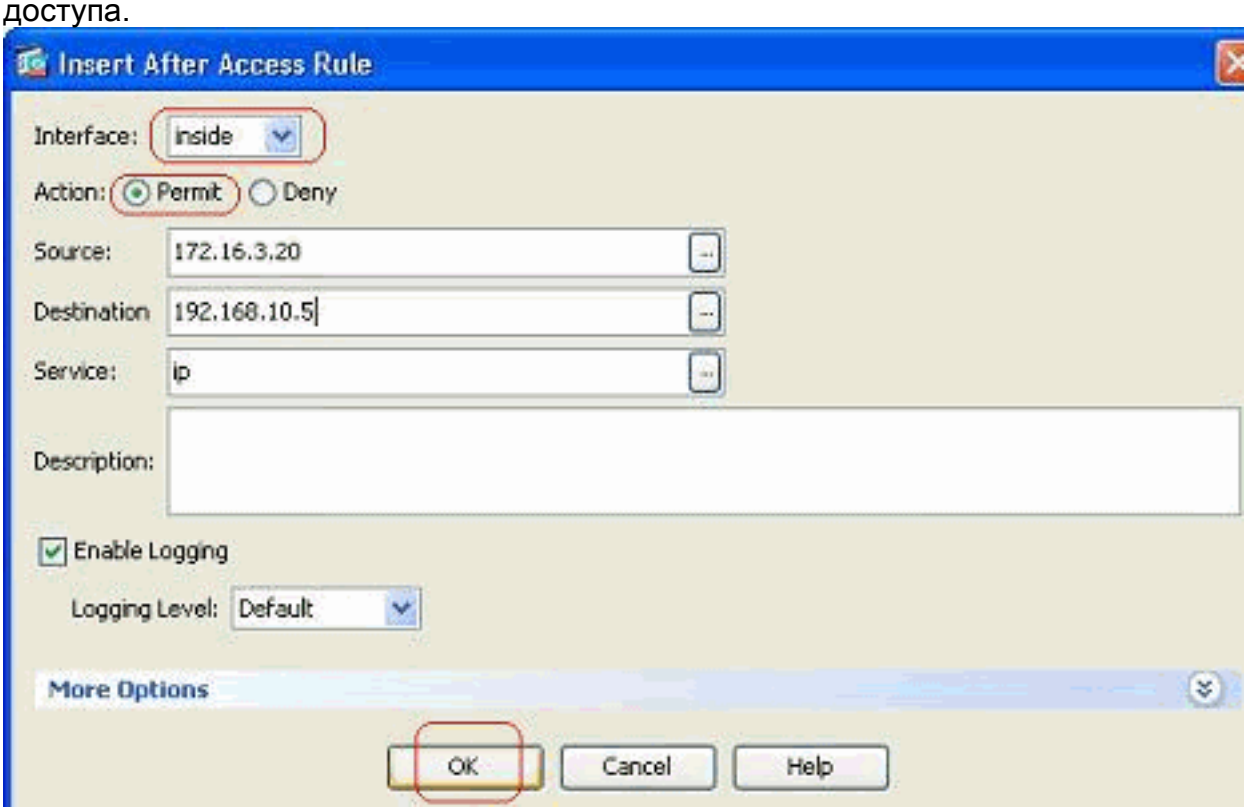
Добавьте Правило Доступа после существующего:

Выполните эти шаги для создания правила доступа сразу после уже существующего правила доступа.

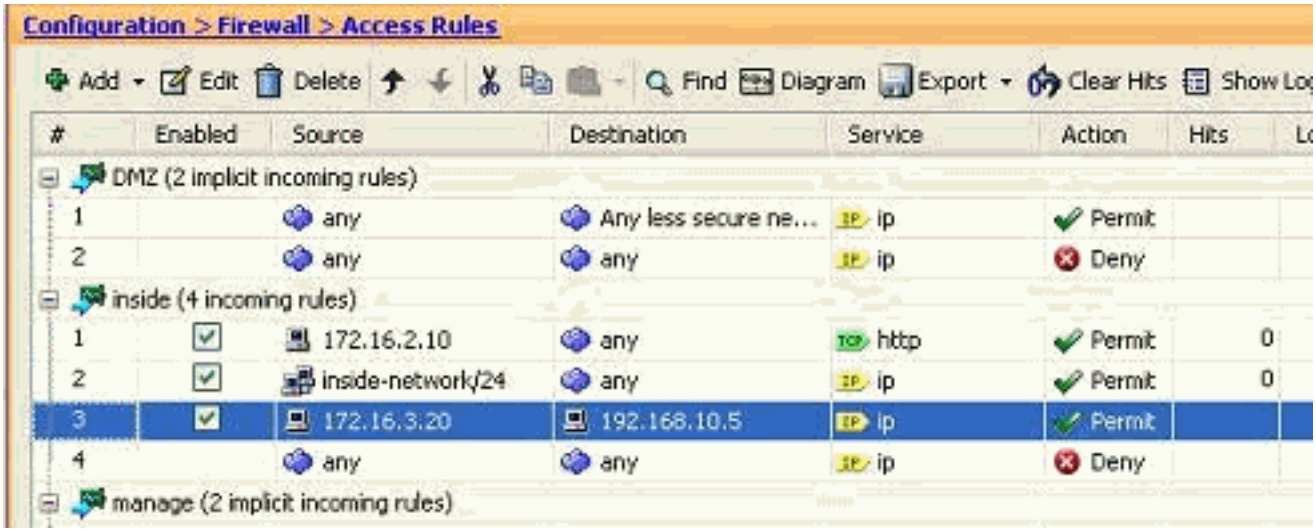
1. Выберите правило доступа, после которого у вас должно быть новое правило доступа, и выбирать **Insert After** из Добавить раскрывающегося меню.



2. Задайте Интерфейс, Действие, Источник, поля Destination и Service, и нажмите **OK** для завершения конфигурации это правило доступа.

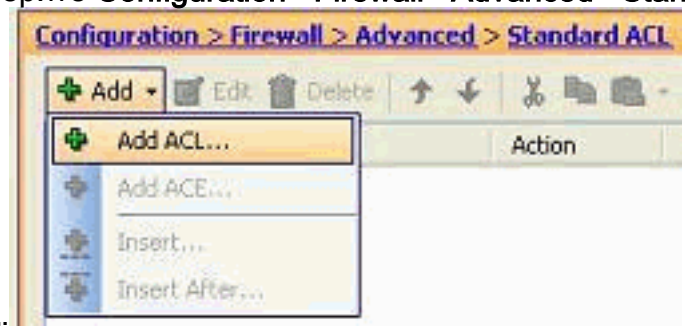


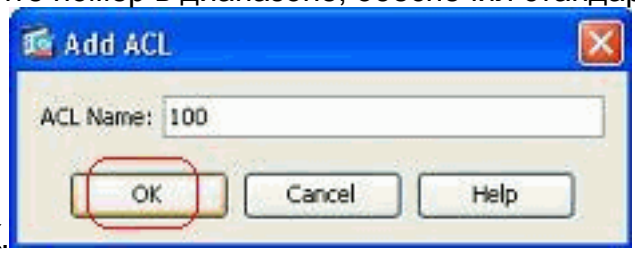
Можно просмотреть это недавно, правило настроенного адреса находится сразу после уже настроенного.

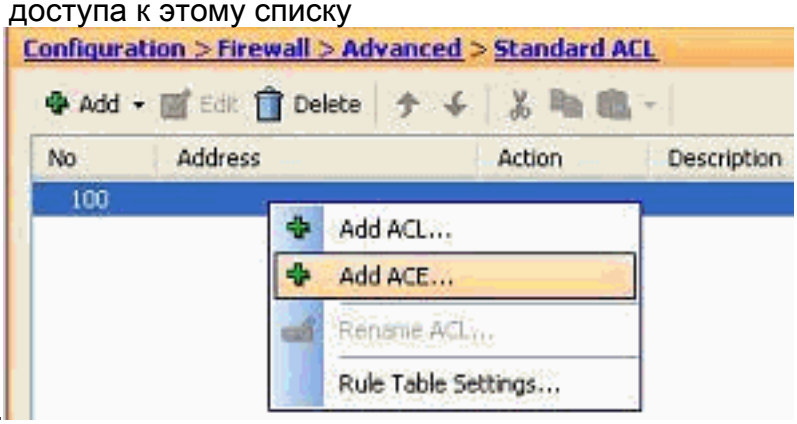


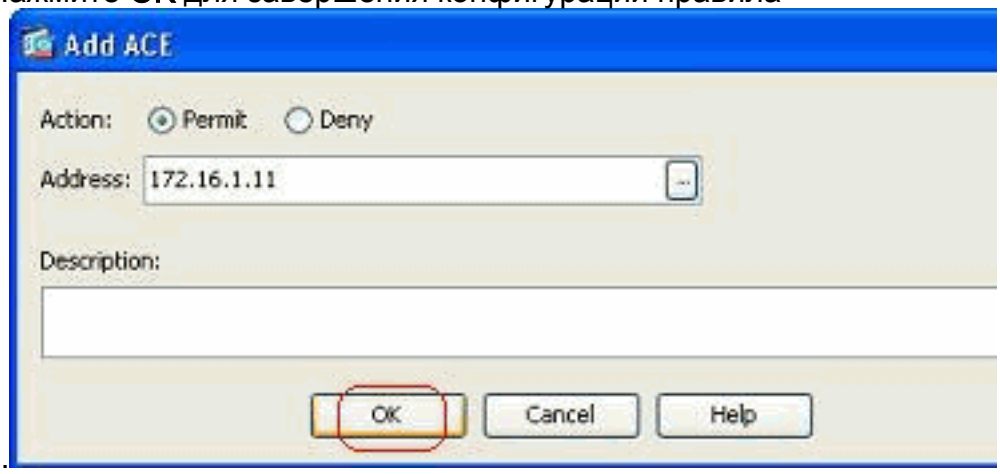
Создайте стандартный список доступа

Выполните эти шаги для создания стандартного списка доступа с GUI ASDM.

1. Выберите **Configuration> Firewall> Advanced> Standard ACL> Add** и **нажмите Add ACL**.


2. Дайте номер в диапазоне, обеспечил стандартный список доступа, и нажмите **OK**.


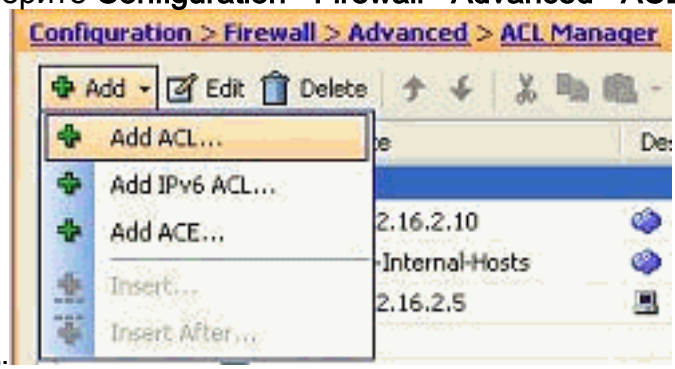
3. Щелкните правой кнопкой мыши список доступа и выберите **Add ACE** для добавления правила доступа к этому списку доступа.


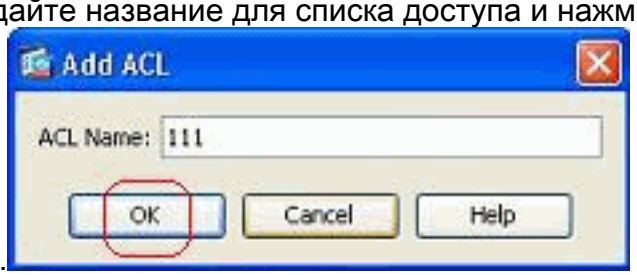
4. Выберите **Action** и задайте **Адрес источника**. При необходимости задайте **Описание** также. Нажмите **OK** для завершения конфигурации правила доступа.


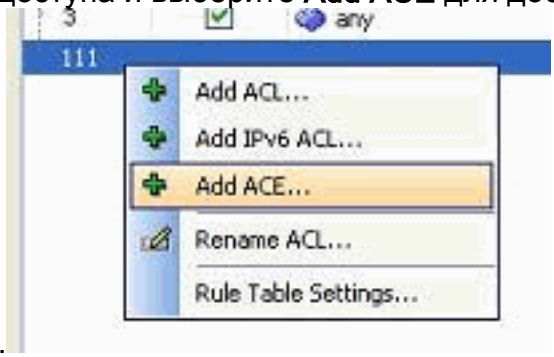
Создайте правило глобального доступа

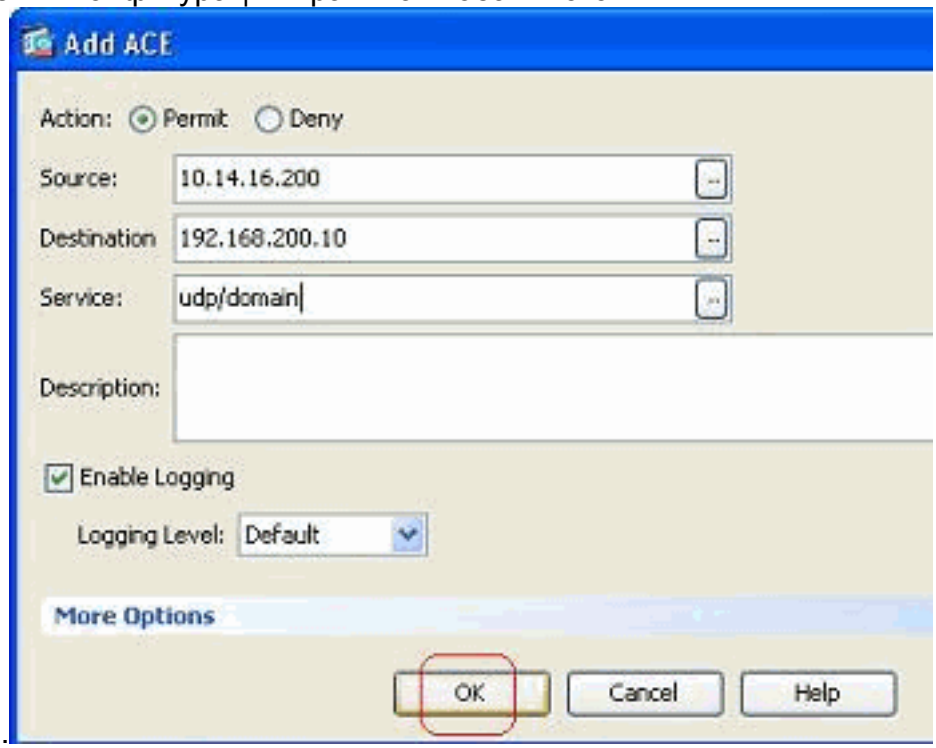
Выполните эти шаги для создания расширенного списка доступа, который содержит

правила глобального доступа.

1. Выберите **Configuration> Firewall> Advanced> ACL Manager> Add** и **нажмите Add** кнопку **ACL**.


2. Задайте название для списка доступа и нажмите **OK**.


3. Щелкните правой кнопкой мыши список доступа и выберите **Add ACE** для добавления правила доступа к этому списку доступа.


4. Завершите Действие, Источник, Назначение и поля Service, и нажмите **OK** для завершения конфигурации правила глобального доступа.


Можно теперь просмотреть правило глобального доступа, как показано.

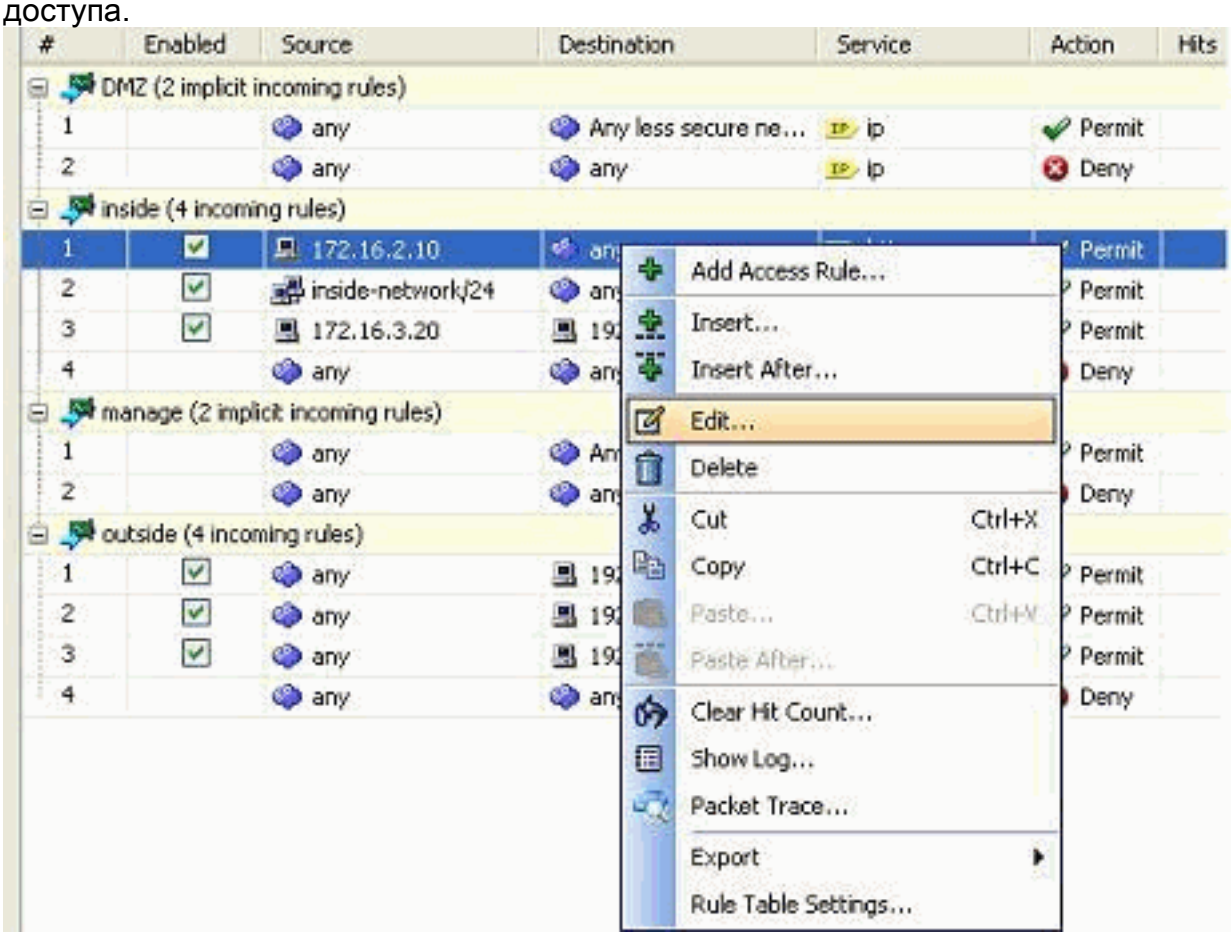
Отредактируйте существующий список доступа

В этом разделе рассматриваются, как отредактировать существующий доступ.

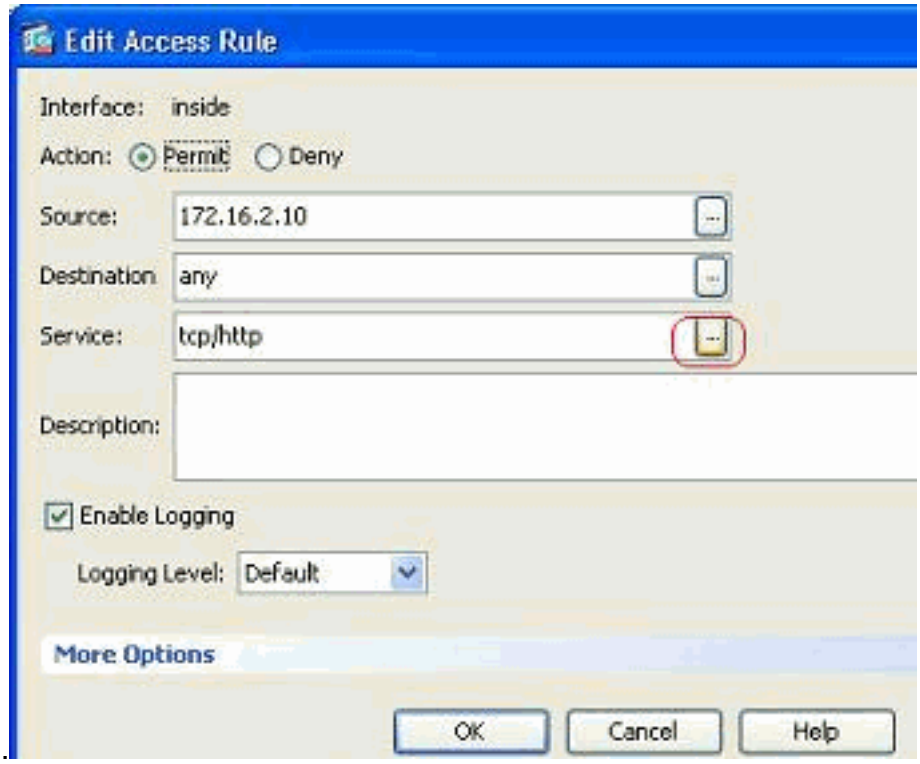
Отредактируйте Поле протокола для создания группы сервисов:

Выполните эти шаги для создания новой группы сервисов.

1. Щелкните правой кнопкой мыши доступ постановляют, что потребности, которые будут модифицироваться, и выбирают **Edit** для изменения того определенного правила доступа.

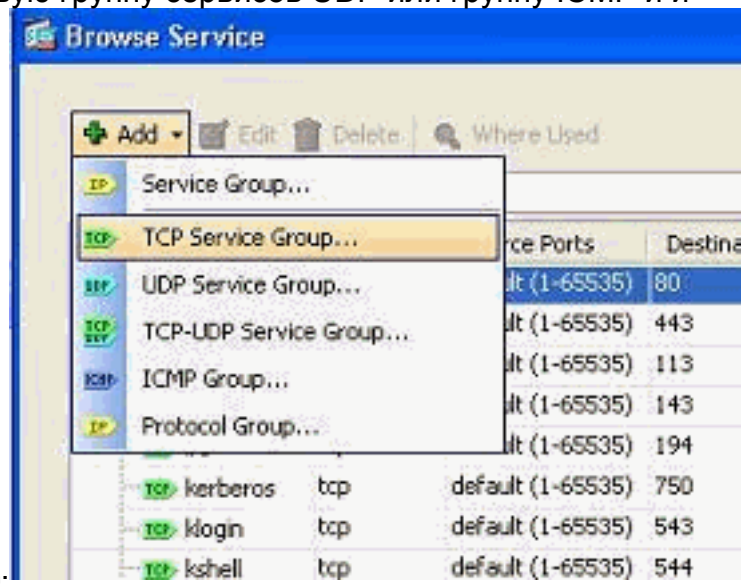


2. Нажмите кнопку **Details** для изменения протокола, привязанного к этому правилу



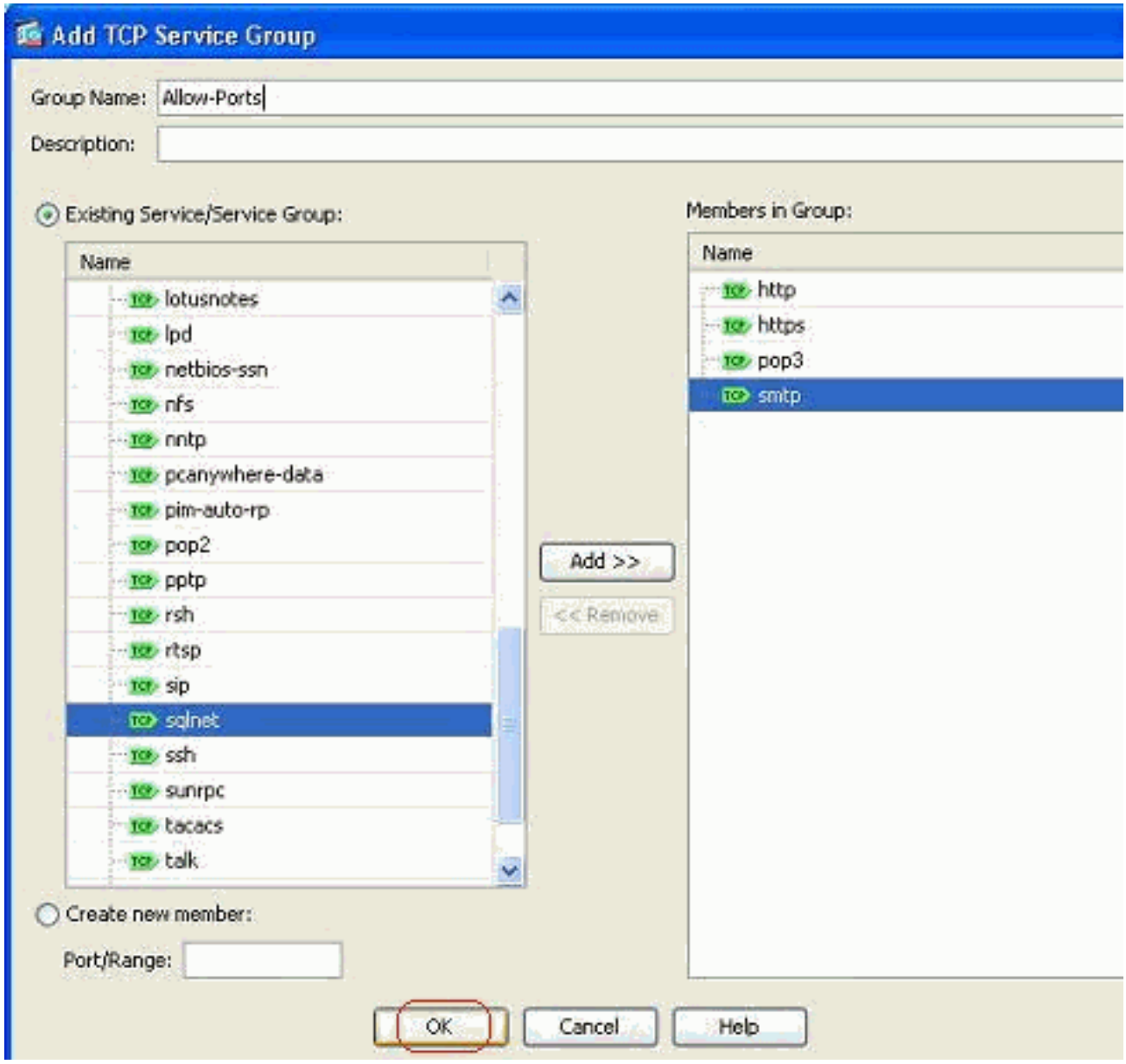
доступа.

3. Можно выбрать любой протокол кроме HTTP при необходимости. Если существует только отдельный протокол, который будет выбран, то нет никакой потребности создать группу сервисов. Полезно создать группу сервисов, когда существует требование для определения многочисленных несмежных протоколов, с которыми совпадет это правило доступа.Выберите **Add> группа сервисов TCP** для создания новой группы сервисов TCP.**Примечание:** Таким же образом можно также создать новую группу сервисов UDP или группу ICMP и и

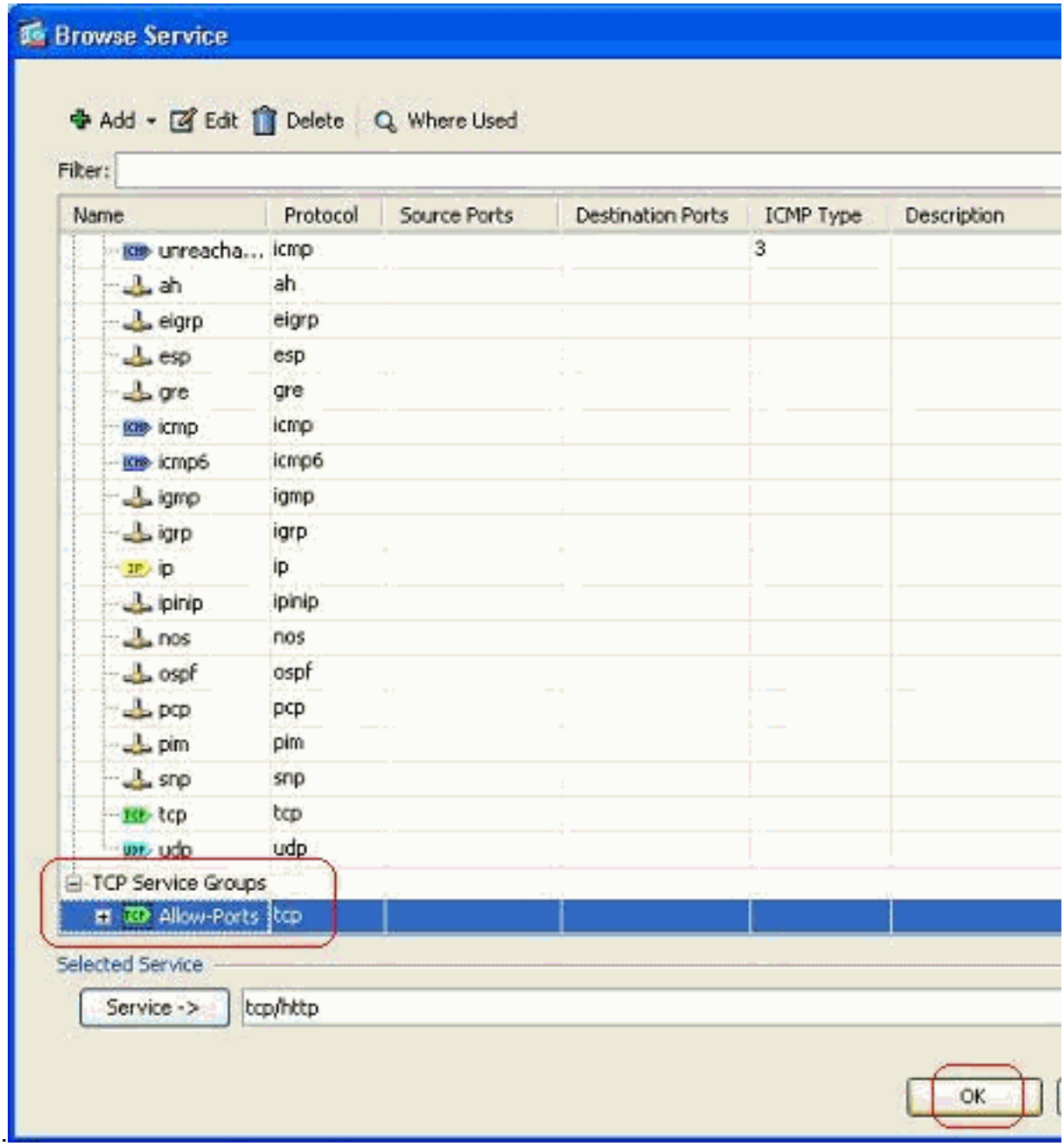


т.д.

4. Задайте название для этой группы сервисов, выберите протокол в левом боковом меню и **нажмите Add** для перемещения их в меню Members in Group на правой части. Многочисленные протоколы могут быть добавлены в качестве участников группы сервисов на основе требования. Протоколы добавлены один за другим. После того, как все участники добавлены, нажимают
OK.

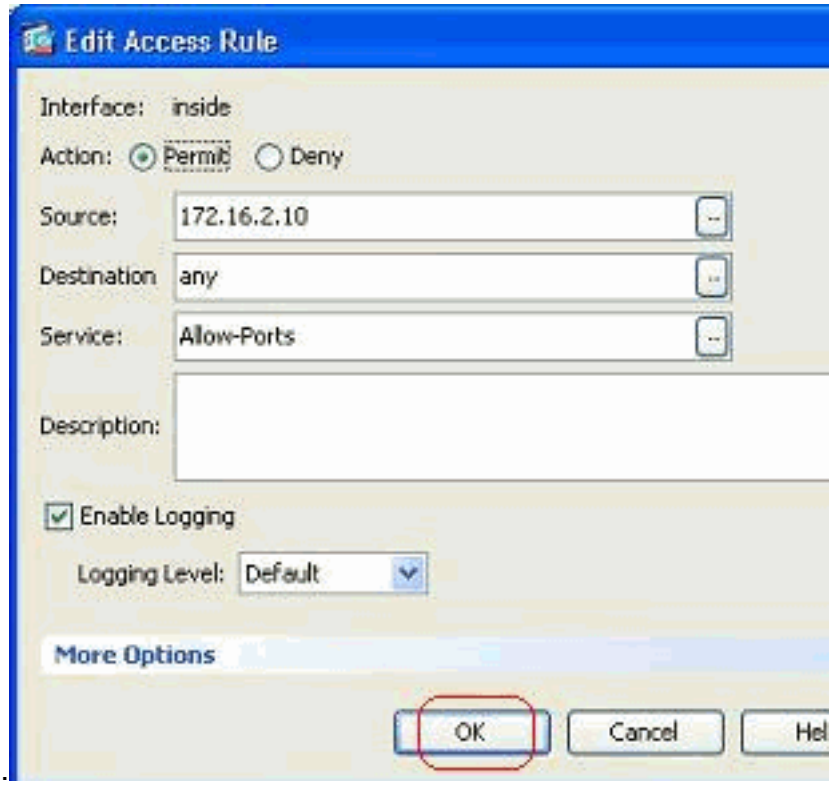


5. Недавно созданная группа сервисов может быть просмотрена под **группами сервисов вкладки TCP**. Нажмите **кнопку OK** для возврата к окну Edit Access



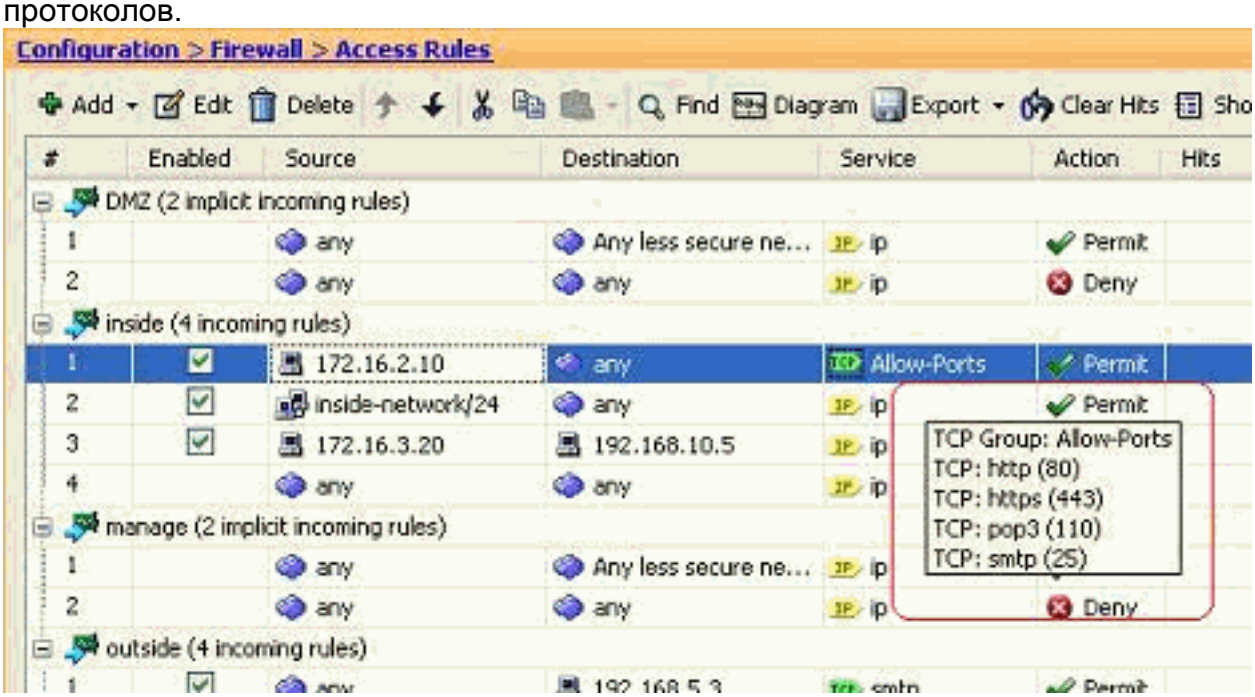
Rule.

6. Вы видите, что поле Service заполнено с недавно созданной группой сервисов. Нажмите **OK** для завершения



редактирования.

7. Нависают ваша мышь над той определенной группой сервисов для просмотра всех связанных
протоколов.



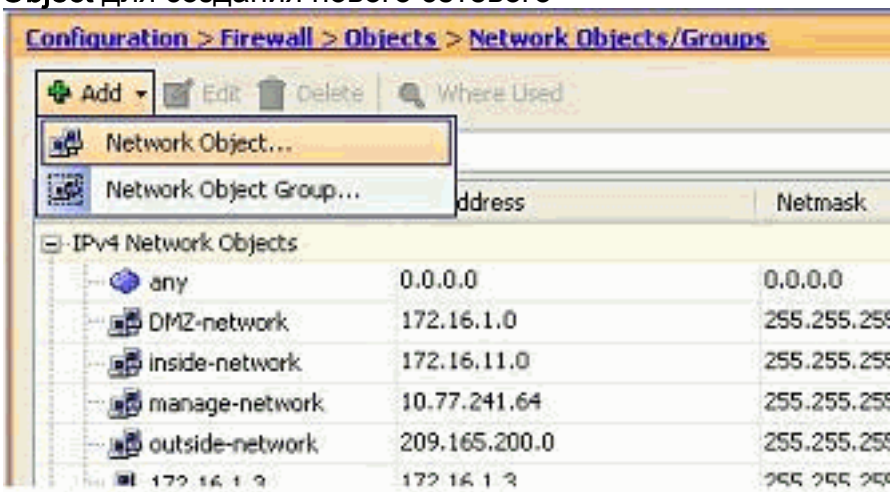
Отредактируйте Источник/Поля Назначение для создания Группы сетевых объектов:

Групповые объекты используются для упрощения создания и обслуживания списков доступа. Когда вы группируетесь как объекты вместе, можно использовать групповой объект в одиночном ACE вместо того, чтобы иметь необходимость ввести ACE для каждого объекта отдельно. Перед созданием группового объекта необходимо создать объекты. В терминологии ASDM объект называют сетевым объектом, и групповой объект называют группой сетевых объектов.

Выполните следующие действия:

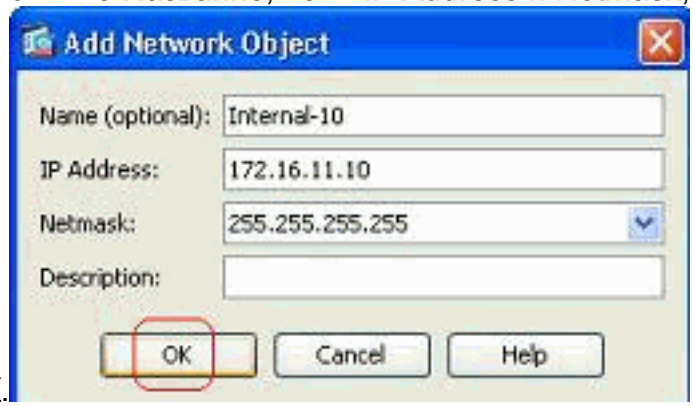
1. Выберите **Configuration> Firewall> Objects> Network Objects/Groups> Add** и нажмите

Network Object для создания нового сетевого



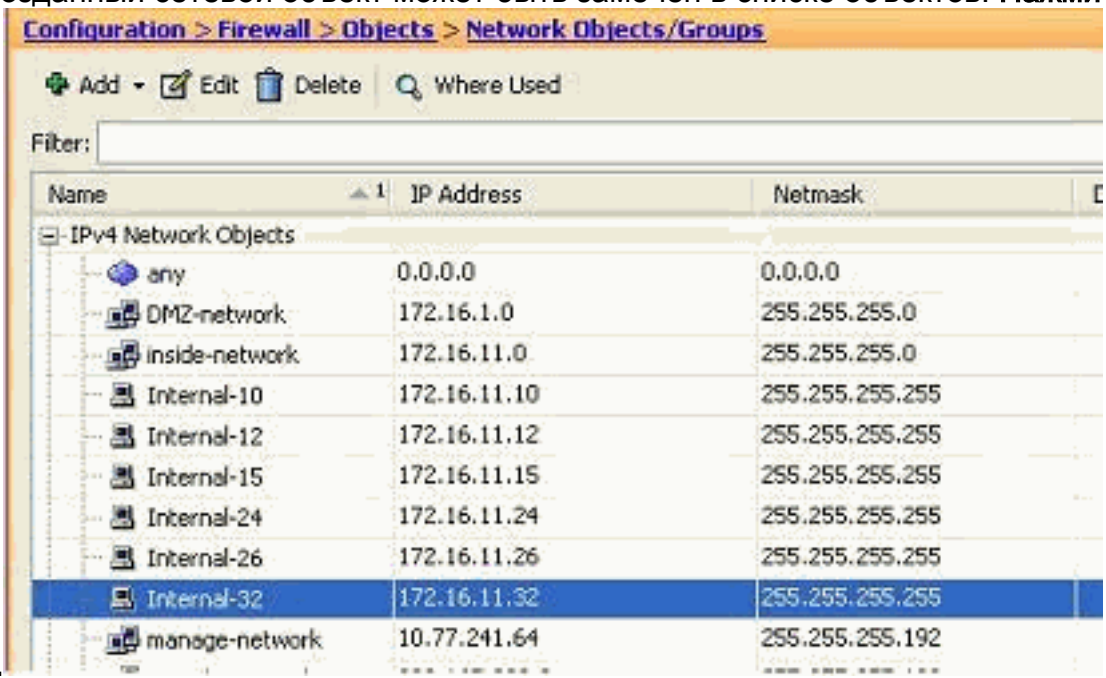
объекта.

2. Заполните **Название**, поля **IP Address и Netmask**, и нажмите



OK.

3. Недавно созданный сетевой объект может быть замечен в списке объектов. **Нажмите**

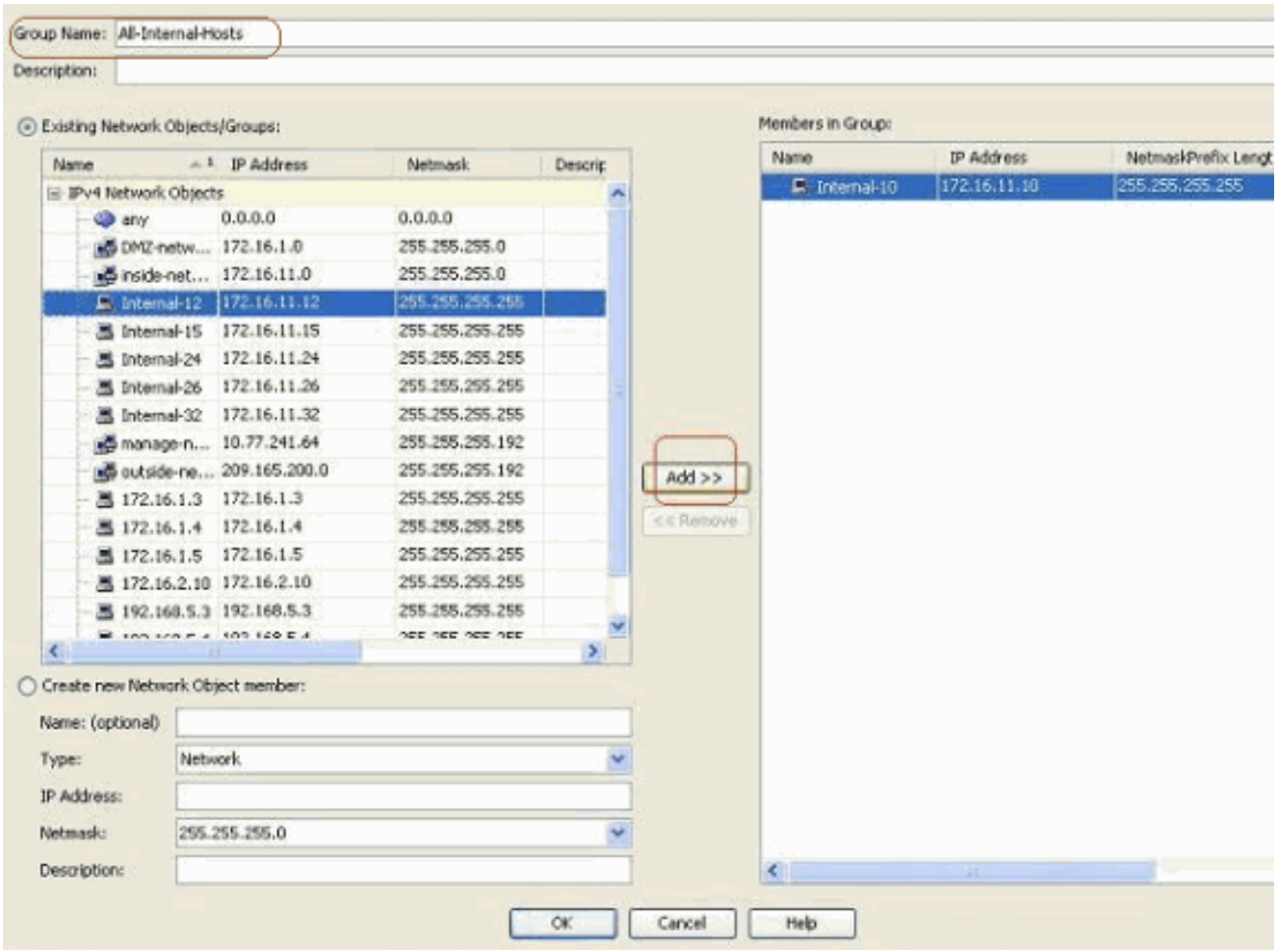


кнопку OK.

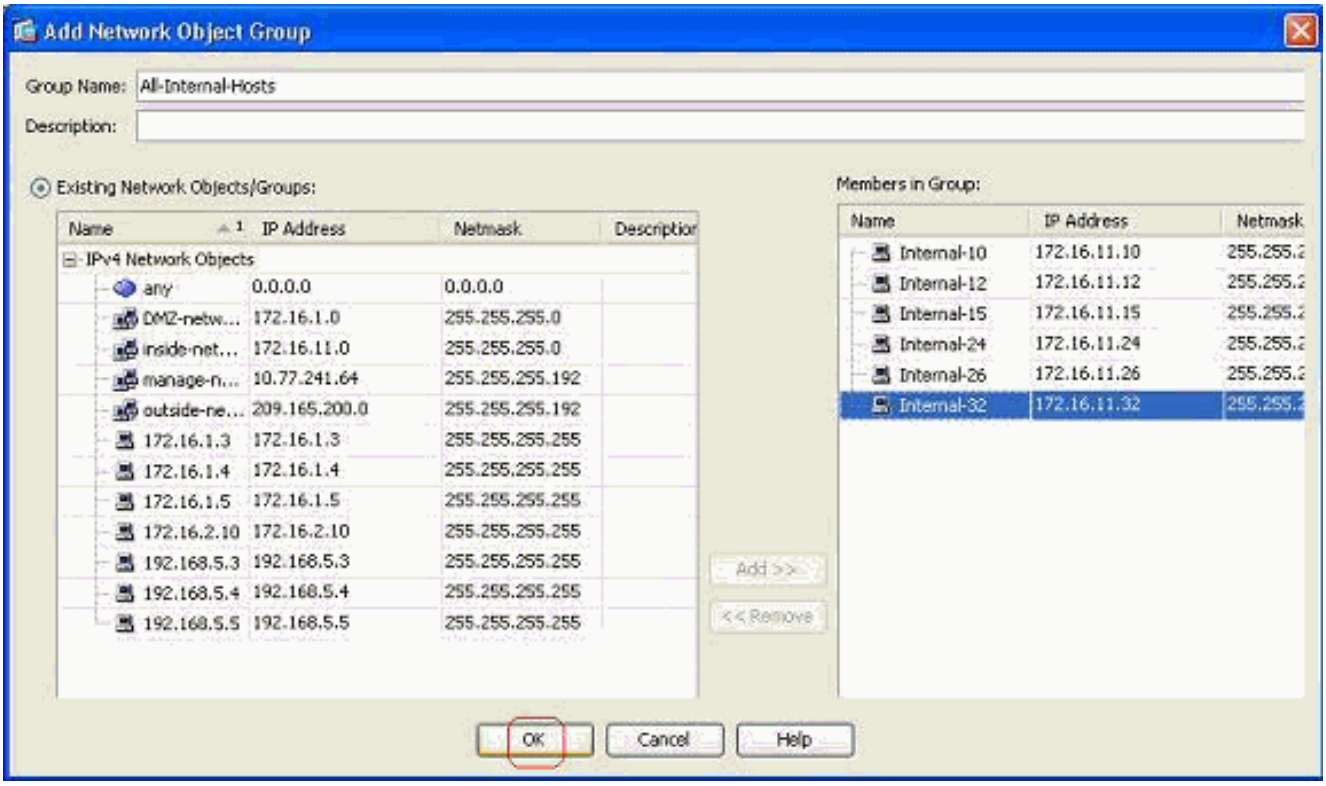
4. Выберите **Configuration> Firewall> Objects> Network Objects/Groups> Add** и нажмите **Network Object Group** для создания новой группы сетевых

объектов.

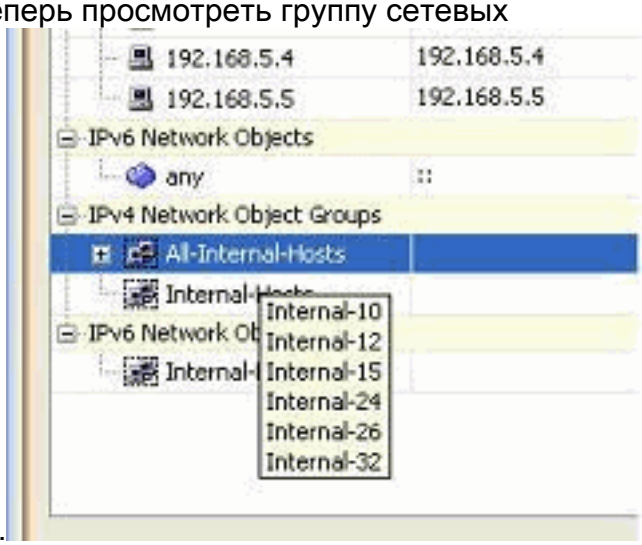
5. Список готовности всех сетевых объектов может быть найден на левой панели окна. Выберите объекты отдельной сети и нажмите **кнопку Add** для создания их участниками недавно созданной группы сетевых объектов. Имя группы должно быть задано в поле, выделенном для
него.



6. Нажмите **OK** после того, как вы включите всех участников для группировки.

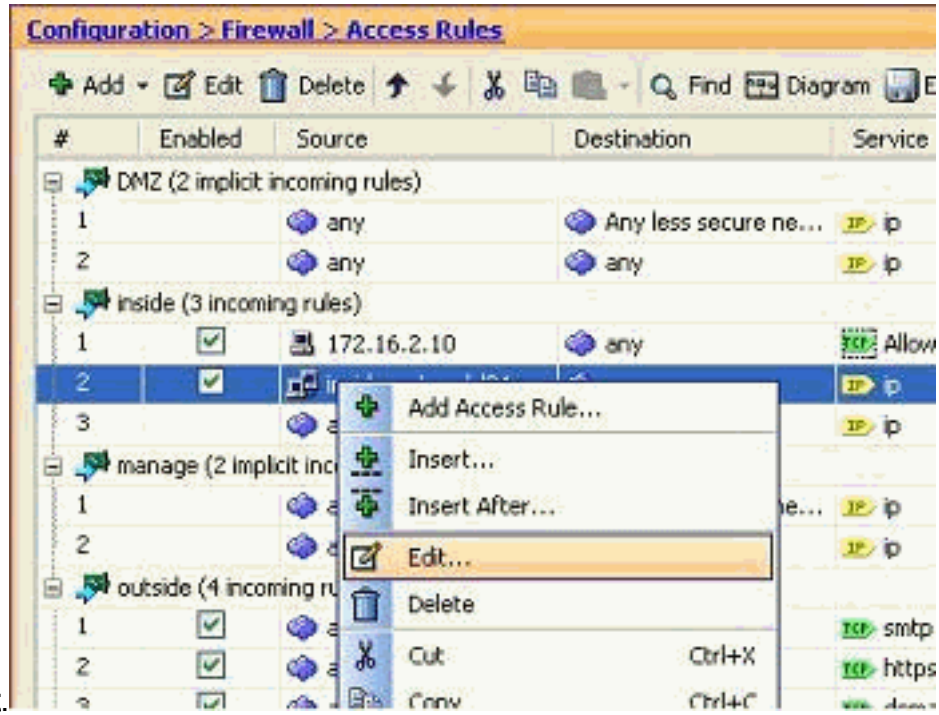


Можно теперь просмотреть группу сетевых



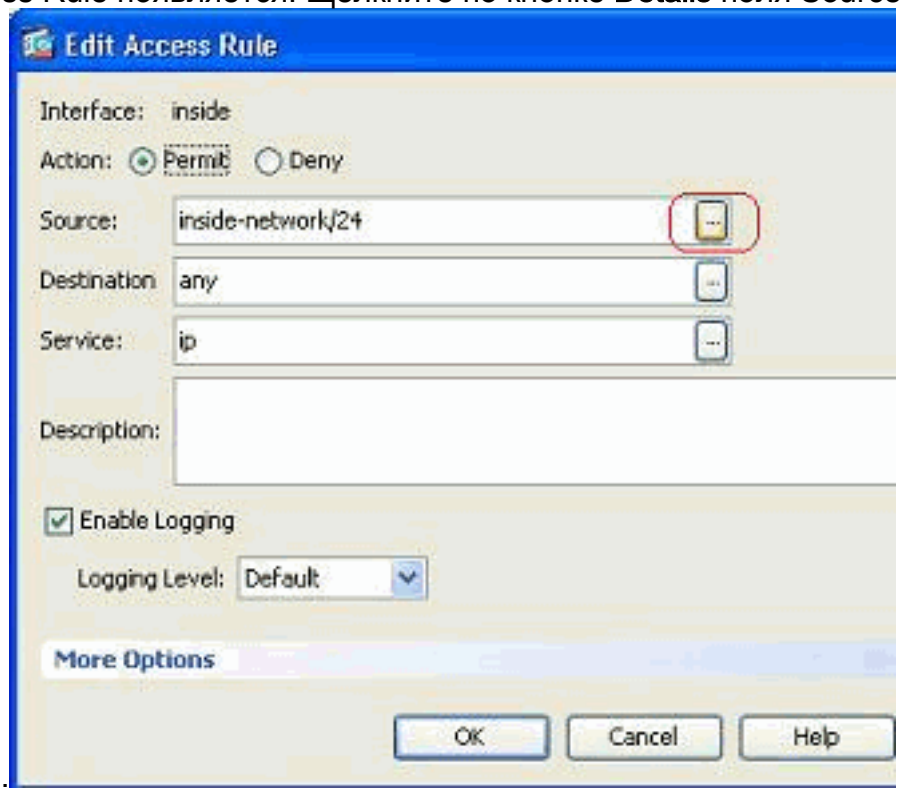
объектов.

7. Для изменения любого источника/поля Назначение существующего списка доступа с объектом группы организации сети щелкните правой кнопкой мыши определенное правило доступа и выберите



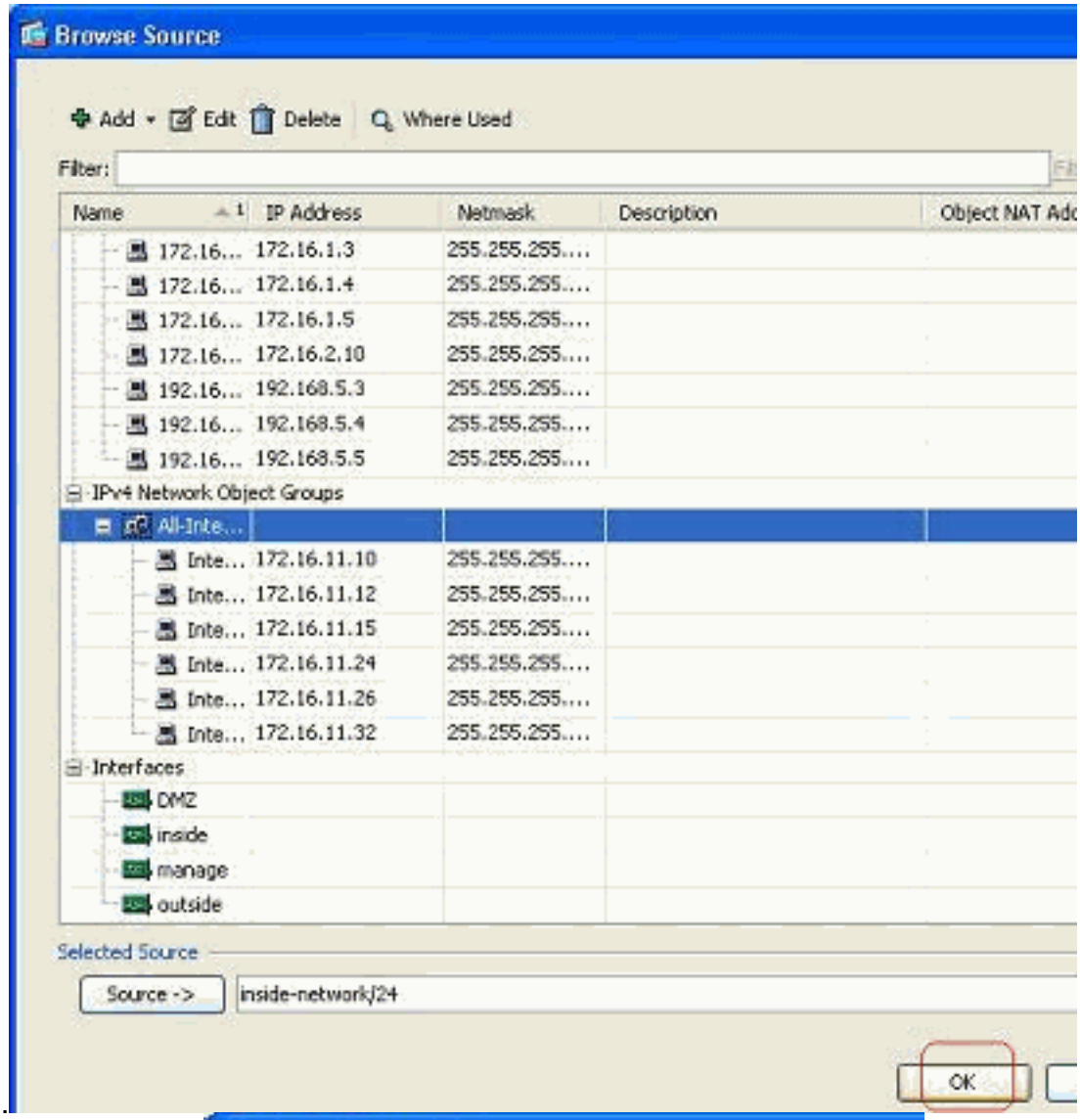
Edit.

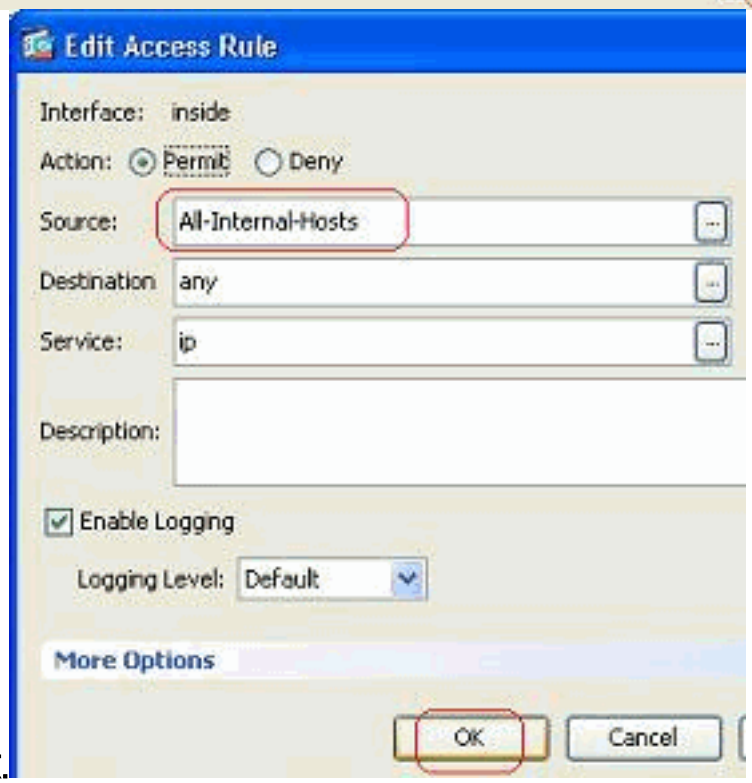
8. Окно Edit Access Rule появляется. Щелкните по кнопке **Details** поля Source для изменения его.



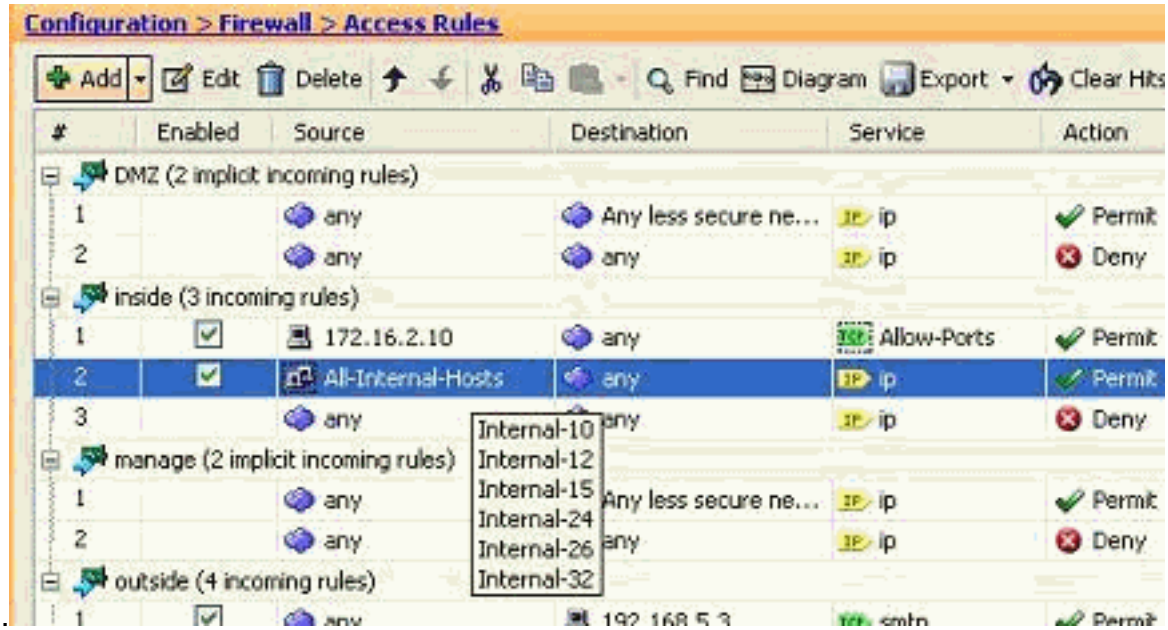
9. Выберите группу сетевых объектов **Все-внутренних хостов** и **кнопку OK**

щелчка.





10. **Нажмите кнопку OK.**
11. Парение, которым ваша мышь по полю Source доступа управляет для просмотра участников

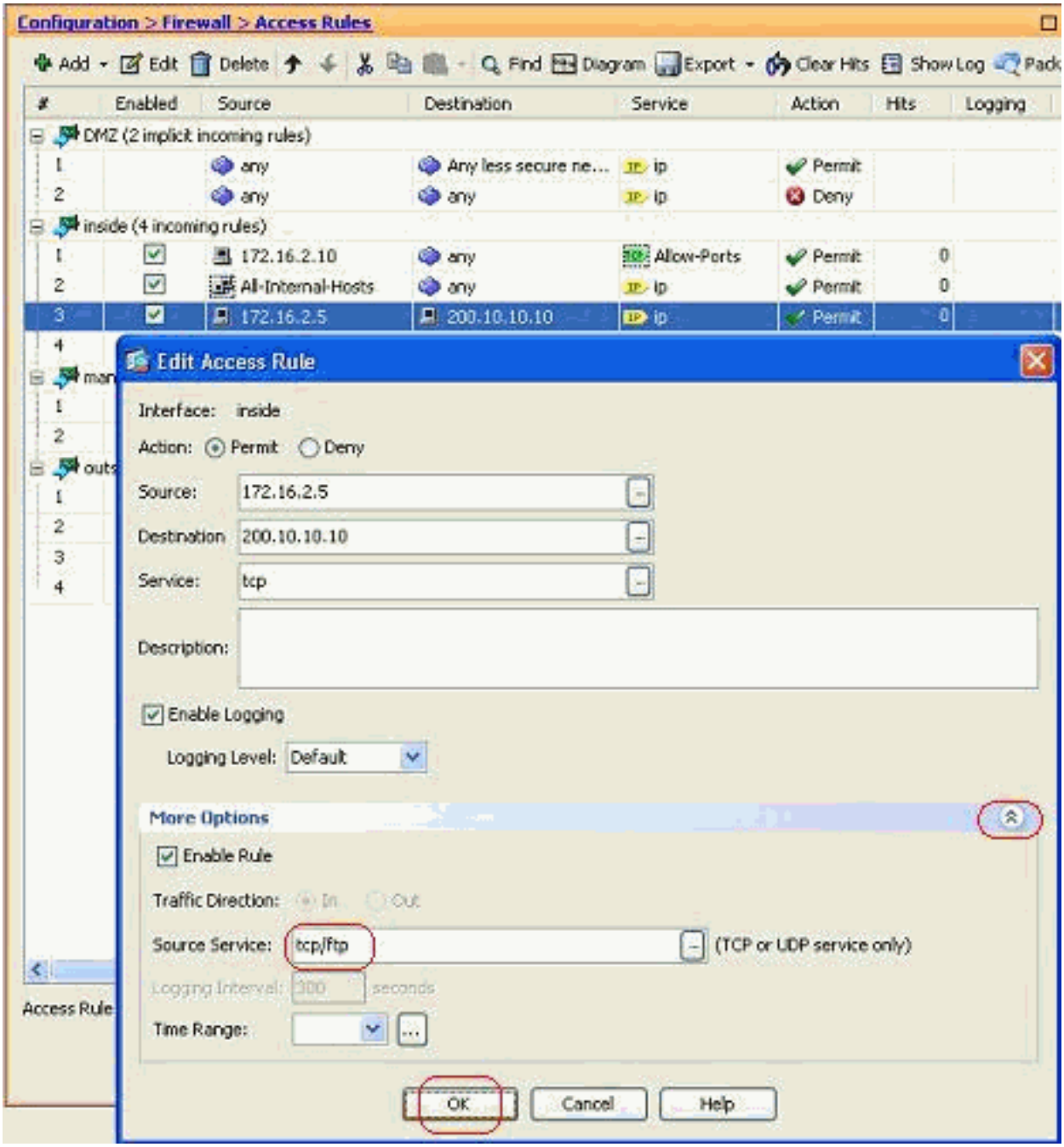


группы.

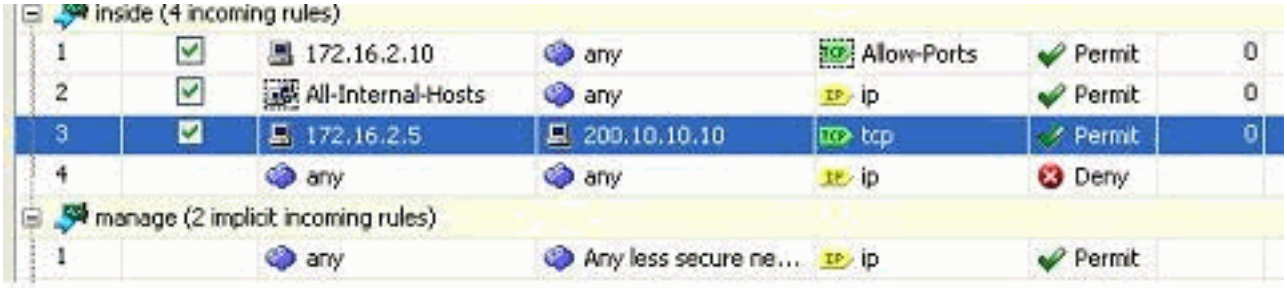
Отредактируйте исходный порт:

Выполните эти шаги для изменения исходного порта правила доступа.

1. Для изменения исходного порта существующего правила доступа щелкните правой кнопкой мыши его и выберите **Edit**.Окно Edit Access Rule появляется.



2. Нажмите **Больше** кнопки раскрытия списка **Опций**, чтобы модифицировать поле Source Service и нажать **OK**.Можно просмотреть модифицированное правило доступа, как показано.

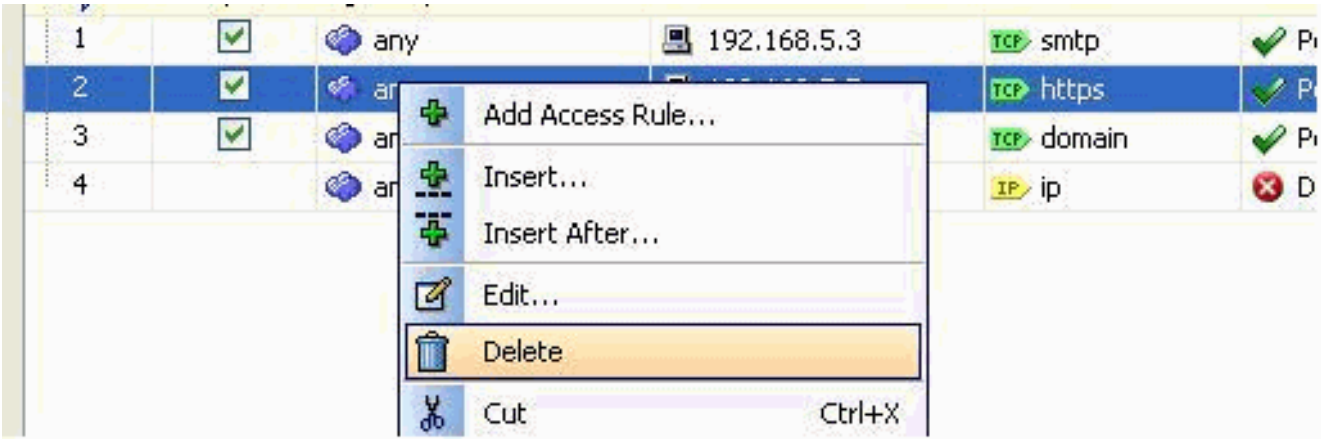


Удалите список доступа

Выполните эти шаги для удаления списка доступа:

1. Перед удалением существующего списка доступа необходимо удалить записи списка доступа (правила доступа). Не возможно удалить список доступа, пока вы сначала не

удаляете все правила доступа.Щелкните правой кнопкой мыши правило доступа, которое будет удалено и выберет
Delete.



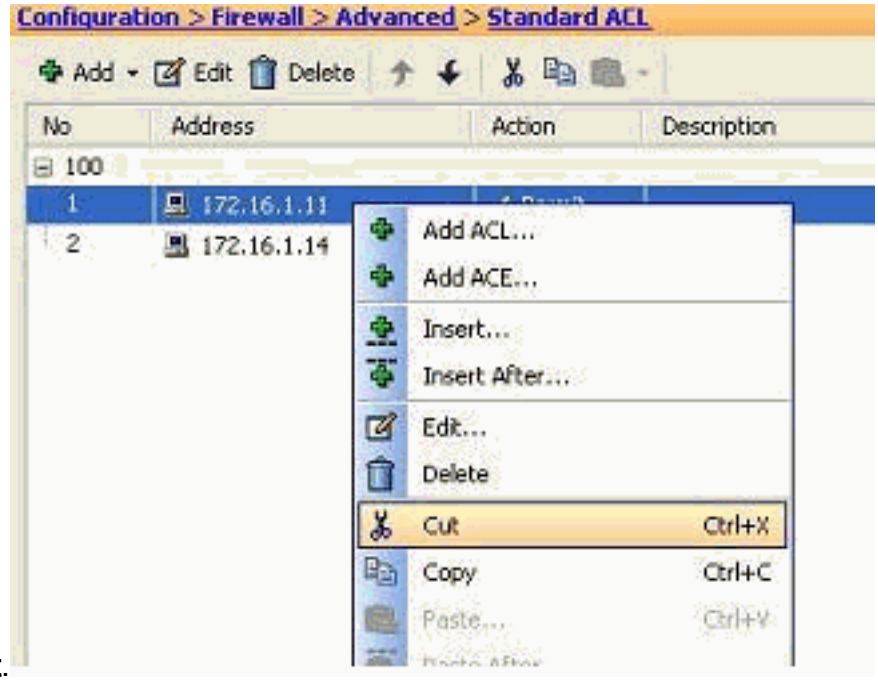
2. Завершите то же, Удаляют операцию на всех существующих правилах доступа, и затем выбирают список доступа и выбирают **Delete** для удаления его.

Экспортируйте правило доступа

В то время как Менеджер ACL отслеживает все расширенные списки доступа, правила доступа ASDM связывают список доступа с соответствующим интерфейсом. Правила доступа, которые созданы с Менеджером ACL, не связывают ни с каким интерфейсом. Эти списки доступа обычно используются в целях Освобожденного от NAT, VPN-Filter и подобных других функций, где нет никакой ассоциации с интерфейсом. Менеджер ACL содержит все записи, которые вы имеете в **Конфигурации> Межсетевой экран>** раздел **Правил Доступа**. Кроме того, **Менеджер ACL** также содержит правила глобального доступа, которые не привязаны ни к какому интерфейсу. ASDM организован таким способом, которым можно экспортировать правило доступа от любого списка доступа до другого легко.

Например, если вам нужно правило доступа, которое уже является частью правила глобального доступа, которое будет привязано к интерфейсу, вы не должны настраивать это снова. Вместо этого можно выполнить **Вырезку и Операцию вставки** для достижения этого.

1. Щелкните правой кнопкой мыши указанное правило доступа и выберите



Cut.

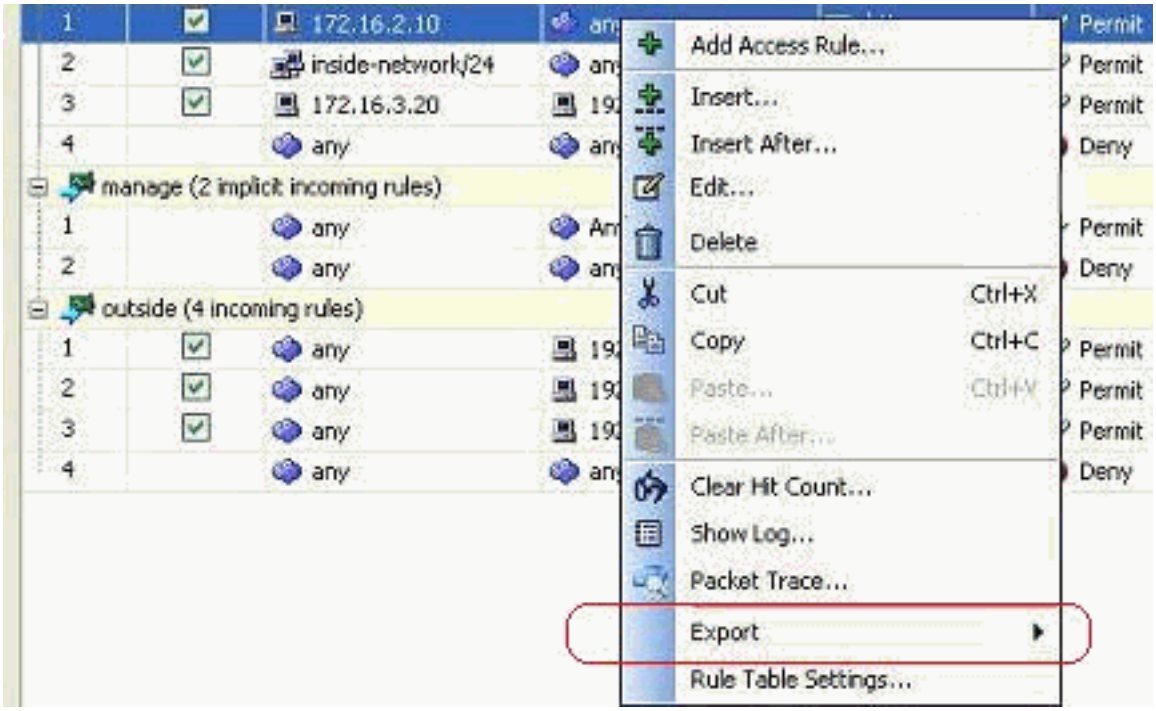
2. Выберите требуемый список доступа, в который необходимо вставить это правило доступа. Можно использовать **Вставку** в строке инструментов для вставки правила доступа.

Экспортируйте информацию о списке доступа

Можно экспортировать информацию о списке доступа в другой файл. Два формата поддерживаются для экспортирования этой информации.

1. Формат Отделенного запятой значения (CSV)
2. Формат HTML

Щелкните правой кнопкой по любому из правил доступа и выберите **Export** для передачи информации о списке доступа к файлу.



Вот информация о списке доступа, показанная в формате HTML.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Примеры конфигурации ASDM и технические примечания
- Примеры конфигурации ASA и технические примечания
- Cisco Systems – техническая поддержка и документация