Пример конфигурации ACL на контроллере беспроводных LAN

Содержание

Введение

Этот документ объясняет, как настроить списки контроля доступа (ACL) на Контроллерах беспроводной локальной сети (WLC), чтобы к трафику фильтрации, который вводит и оставляет WLAN.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Знание того, как настроить WLC и Облегченную точку доступа (LAP) для главной операции
- Базовые знания о Протоколе LWAPP и методах безопасности беспроводной связи

Используемые компоненты

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

- Cisco WLC серии 2000, который выполняет микропрограммное обеспечение 4.0

- LAP серии 1000 Cisco
- Беспроводной клиентский адаптер Cisco 802.11a/b/g, который выполняет микропрограммное обеспечение 2.6
- Версия 2.6 Утилиты Cisco Aironet Desktop Utility (ADU)

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

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

ACL на WLC

ACL на WLC предназначаются, чтобы ограничить или разрешить беспроводным клиентам к сервисам на его WLAN.

Перед версией микропрограммы 4.0 WLC ACL обойдены на Интерфейсе управления, таким образом, вы не можете влиять на трафик, предназначенный к WLC кроме препятствования тому, чтобы беспроводные клиенты управляли контроллером с **менеджментом Через опцию Wireless**. Поэтому ACL могут только быть применены к динамическим интерфейсам. В версии микропрограммы 4.0 WLC существуют ACL ЦП, которые могут трафик фильтрации, предназначенный для Интерфейса управления. Пример того, как настроить ACL ЦП, предоставлен позже в этом документе.

Можно определить до 64 ACL, каждого максимум с 64 правилами (или фильтры). Каждое правило имеет параметры, которые влияют на его действие. Когда пакет совпадает со всеми параметрами для правила, набор действия для того правила применен к пакету. Можно настроить ACL или через GUI или через CLI.

Это некоторые правила, которые необходимо понять перед настройкой ACL на WLC:

- Если источник *и* назначение - **кто-либо**, направление, в котором применен этот ACL, может быть **любым**.
- Если или источник *или* назначение не **никто**, то направление фильтра должно быть задано, и должен быть создан обратный оператор в противоположном направлении.
- Понятие WLC входящих по сравнению с исходящим неинтуитивно. Это с точки зрения направления WLC к беспроводному клиенту, а не с точки зрения клиента. Так, входящее направление означает пакет, который входит в WLC от беспроводного клиента, и исходящее направление означает пакет, который выходит от WLC к беспроводному клиенту.
- Существует неявное, запрещают в конце ACL.

Факторы, когда ACL Настройки в WLC

ALC в WLC работают по-другому, чем в маршрутизаторах. Это несколько вещей помнить при настройке ACL в WLC:

- Когда вы намереваетесь запретить или позволить пакеты IP, наиболее распространенная ошибка состоит в том, чтобы выбрать IP. Поскольку вы выбираете то, что в пакете IP, вы заканчиваете тем, что запретили или позволили пакеты IPINIP.
- ACL контроллера не могут заблокироваться 1.1.1.1 (виртуальный IP - адрес), и следовательно пакеты DHCP для беспроводных клиентов.
- ACL контроллера не могут заблокировать многоадресный трафик, полученный от проводных сетей, который предназначен беспроводным клиентам. ACL контроллера обработаны для многоадресного трафика, инициируемого от беспроводных клиентов, предназначенных к проводным сетям или другим беспроводным клиентам на том же контроллере.
- В отличие от маршрутизатора, ACL управляет трафиком в обоих направлениях, когда применено к интерфейс, но это не выполняет использование систем защиты сетей с отслеживанием состояния. Если вы забываете открывать дыру в ACL для возврата трафика, это вызывает проблему.
- ACL контроллера только блокируют пакеты IP. Вы не можете заблокировать ACL Уровня 2 или пакеты Уровня 3, которые не являются IP.
- ACL контроллера не используют обратные маски как маршрутизаторы. Здесь, 255 соответствий средств, что октет IP-адреса точно.
- ACL на контроллере сделаны в программном обеспечении и влияют на скорость переадресации.

Примечание: При применении ACL к интерфейсу или WLAN беспроводная пропускная способность ухудшена и может привести к потенциальным потерям пакетов. Для улучшения пропускной способности удалите ACL из интерфейса или WLAN и переместите ACL в соседнее подключенное устройство.

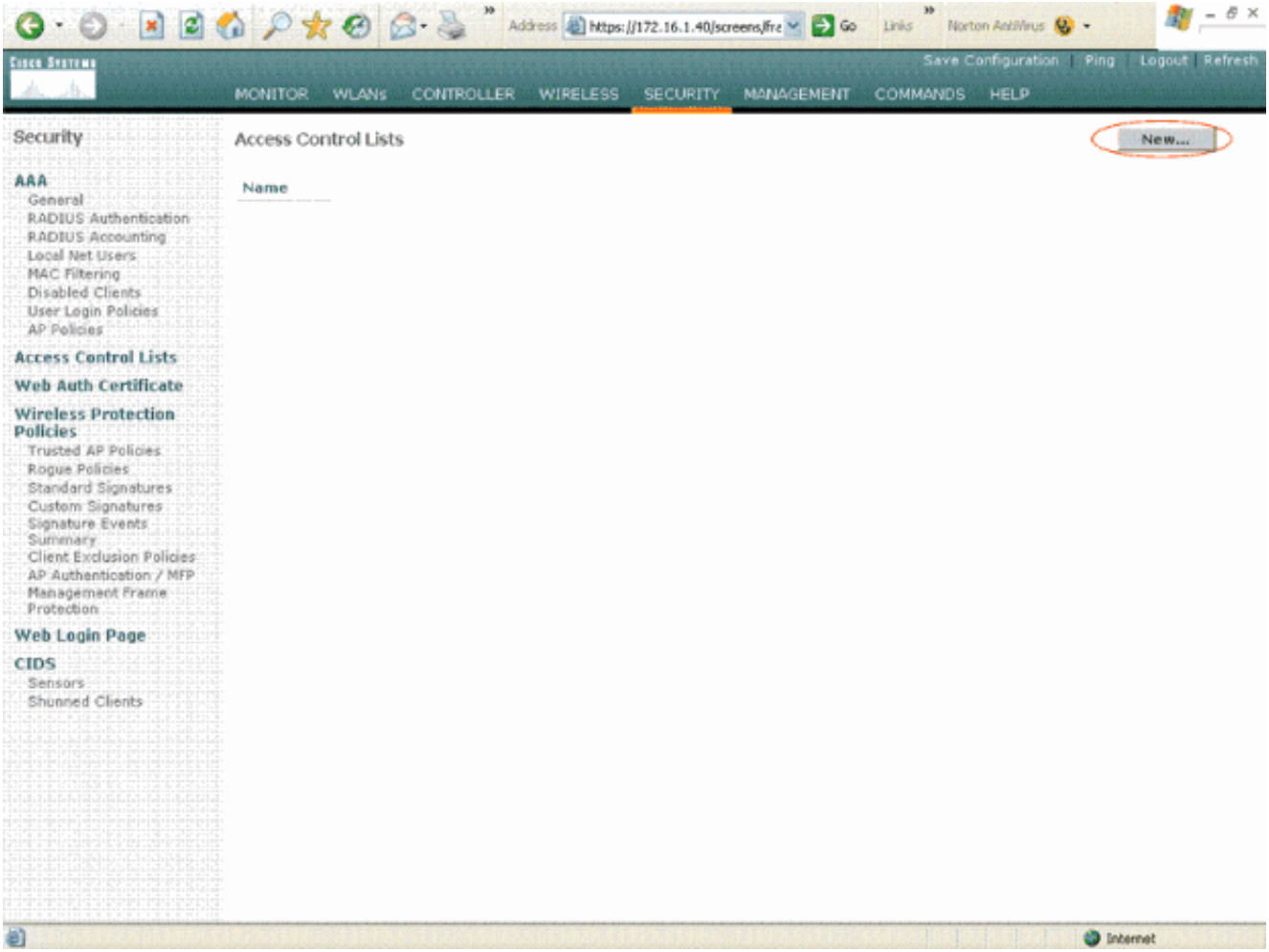
Настройте ACL на WLC

В этом разделе описывается настроить ACL на WLC. Цель состоит в том, чтобы настроить ACL, который позволяет гостевым клиентам обращаться к этим сервисам:

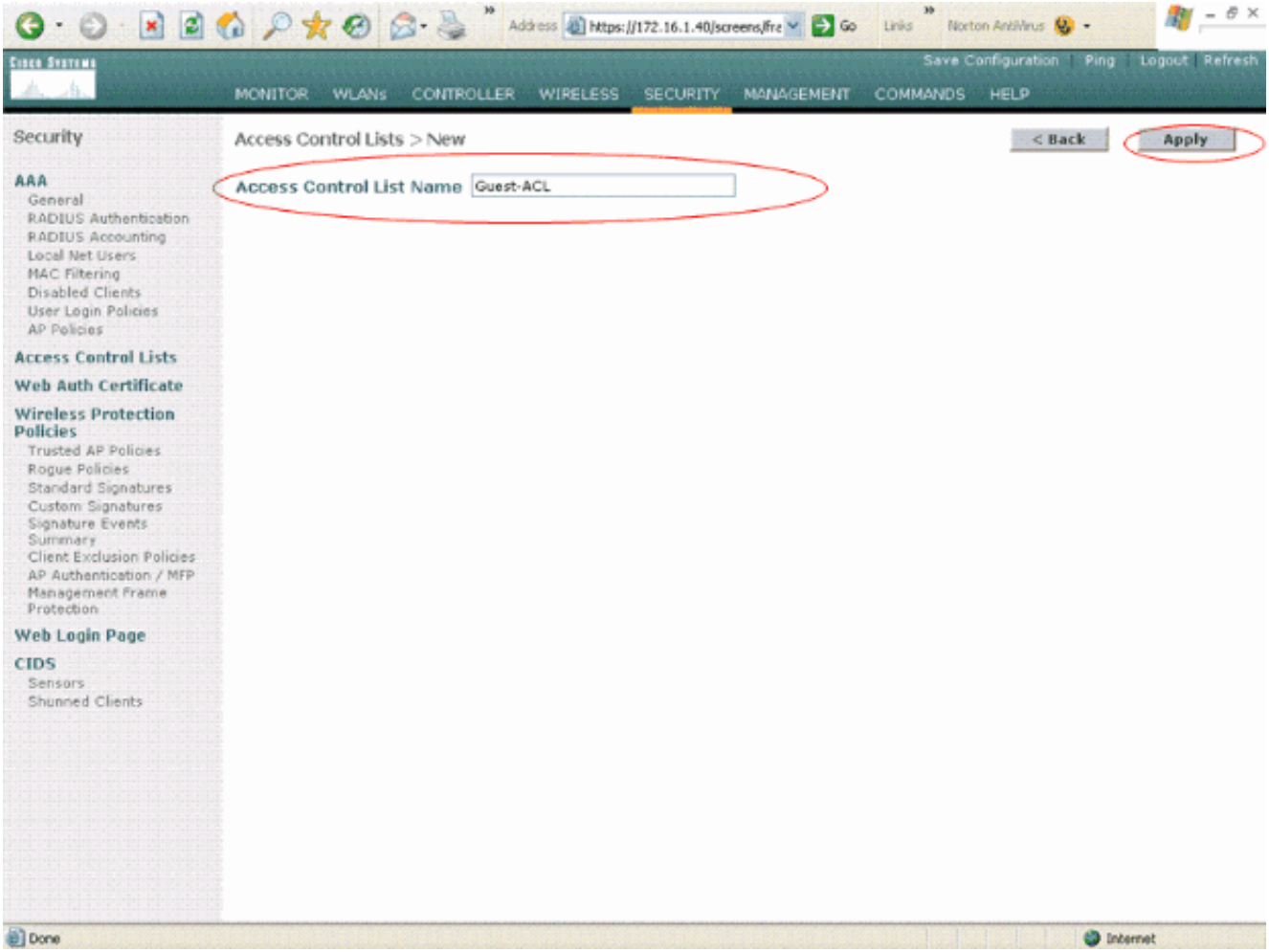
- Протокол DHCP (динамического конфигурирования узла) между беспроводными клиентами и сервером DHCP
- Протокол ICMP между всеми устройствами в сети
- Система доменных имен (DNS) между беспроводными клиентами и сервером DNS
- Telnet к определенной подсети

Все другие сервисы должны быть заблокированы для беспроводных клиентов. Выполните эти шаги для создания ACL с помощью GUI WLC:

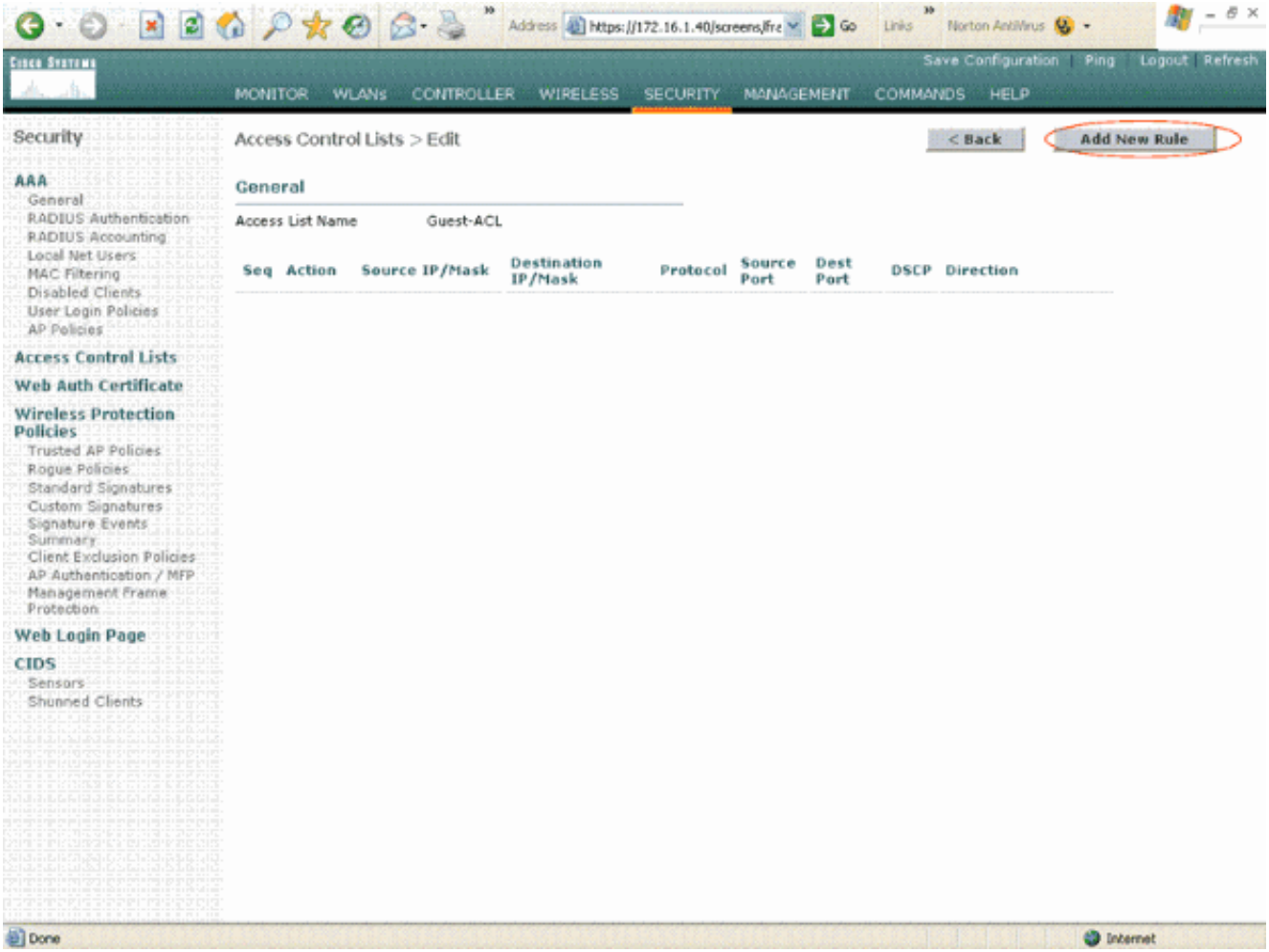
1. Перейдите к GUI WLC и выберите **Security> Access Control Lists**.Страница Access Control Lists появляется. Эта страница перечисляет ACL, которые настроены на WLC. Это также позволяет вам отредактировать или удалить любой из ACL. Для создания нового ACL нажмите
   New.



2. Введите имя ACL и нажмите **Apply**.Можно ввести до 32 алфавитно-цифровых знаков. В данном примере названием ACL является **Гостевой ACL**. Как только ACL создан, нажмите **Edit** для создания правил для ACL.



3. Когда Списки контроля доступа> страница Edit появится, **нажать add new rule**.Страница Access Control Lists> Rules> New
появляется.



4. Настройте правила, которые позволяют гостю эти сервисы:DHCP между беспроводными клиентами и сервером DHCPICMP между всеми устройствами в сетиDNS между беспроводными клиентами и сервером DNSTelnet к определенной подсети

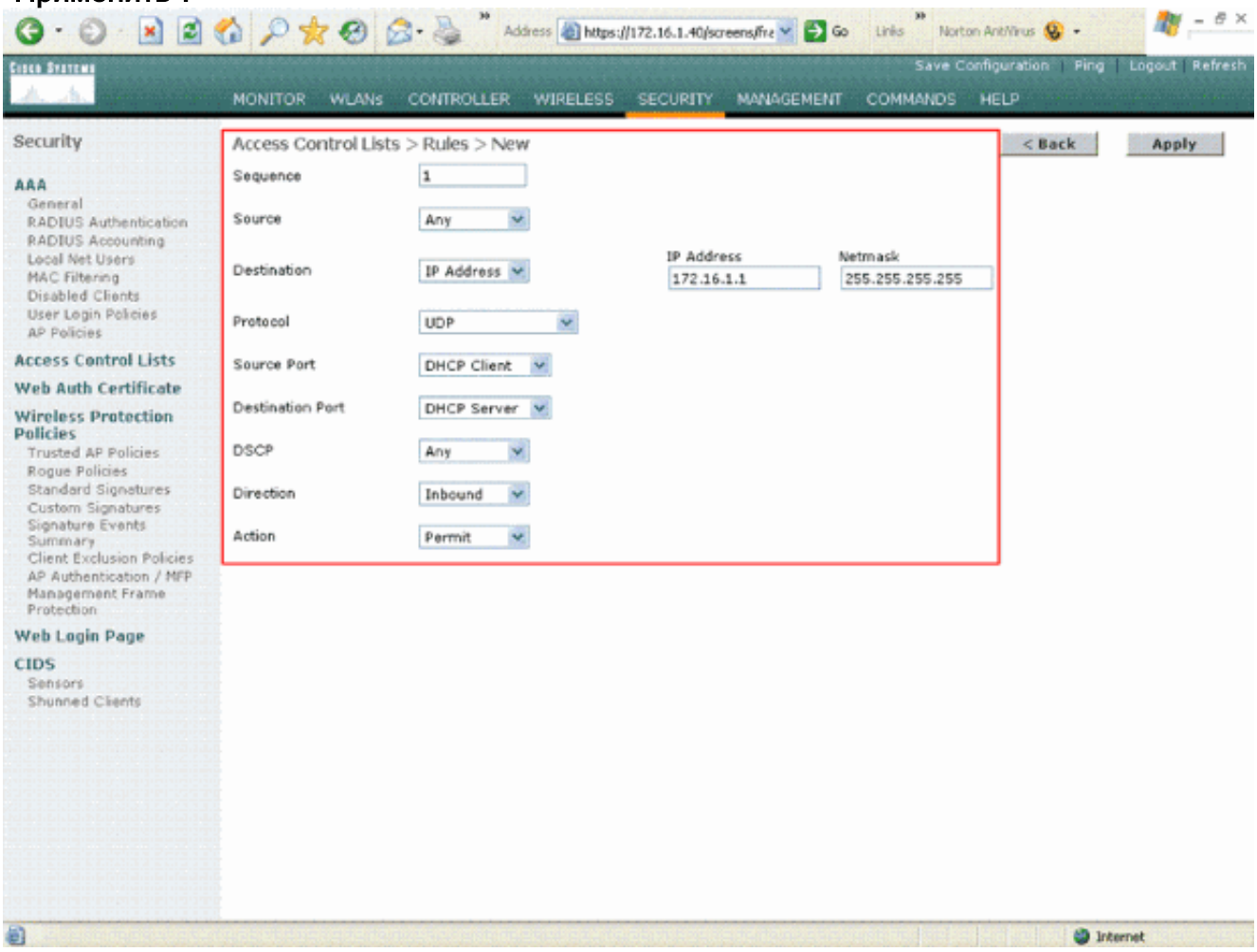
Настройте Правила что Allow Guest User Services

Этот раздел показывает пример для того, как настроить правила для этих сервисов:

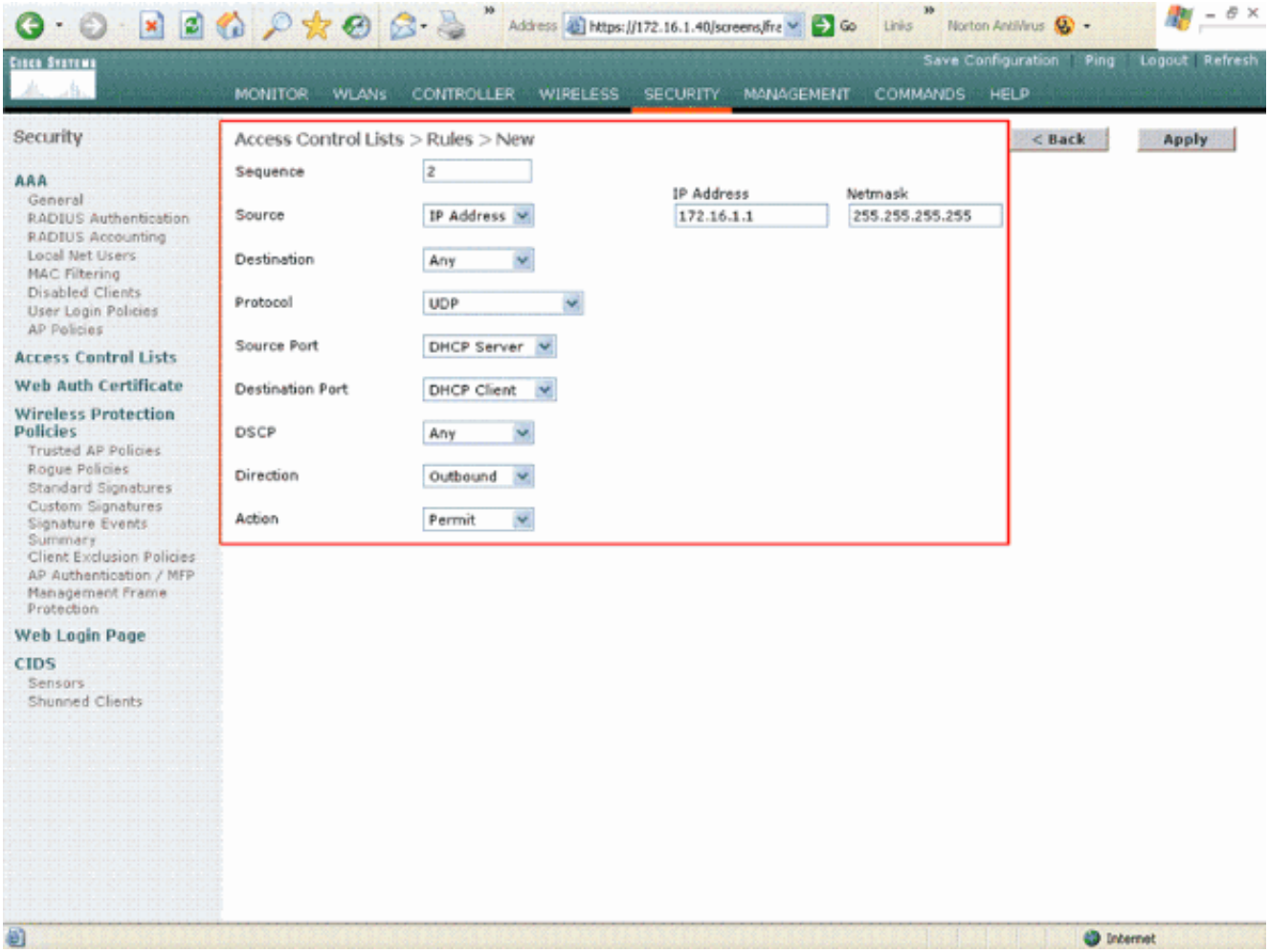
- DHCP между беспроводными клиентами и сервером DHCP
- ICMP между всеми устройствами в сети
- DNS между беспроводными клиентами и сервером DNS
- Telnet к определенной подсети

1. Для определения правила для сервиса DHCP выберите диапазоны IP - адреса назначения и источник.Данный пример использует **любого** для источника, что означает, что любой беспроводной клиент является предоставленным доступом к серверу DHCP. В данном примере, сервер 172.16.1.1 действия как DHCP и сервер DNS. Так, IP - адрес назначения является 172.16.1.1/255.255.255.255 (с маской хоста).Поскольку DHCP является протоколом на основе UDP, выберите **UDP** из Протокола выпадающее поле. При выборе TCP или UDP в предыдущем шаге два дополнительных параметра появляются: Исходный порт и Порт назначения. Задайте подробные данные Порта источника и порт назначения. Для этого правила Исходный порт является **Клиентом DHCP**, и Портом назначения является **Сервер DHCP**.Выберите Direction, в котором должен быть применен ACL. Поскольку это

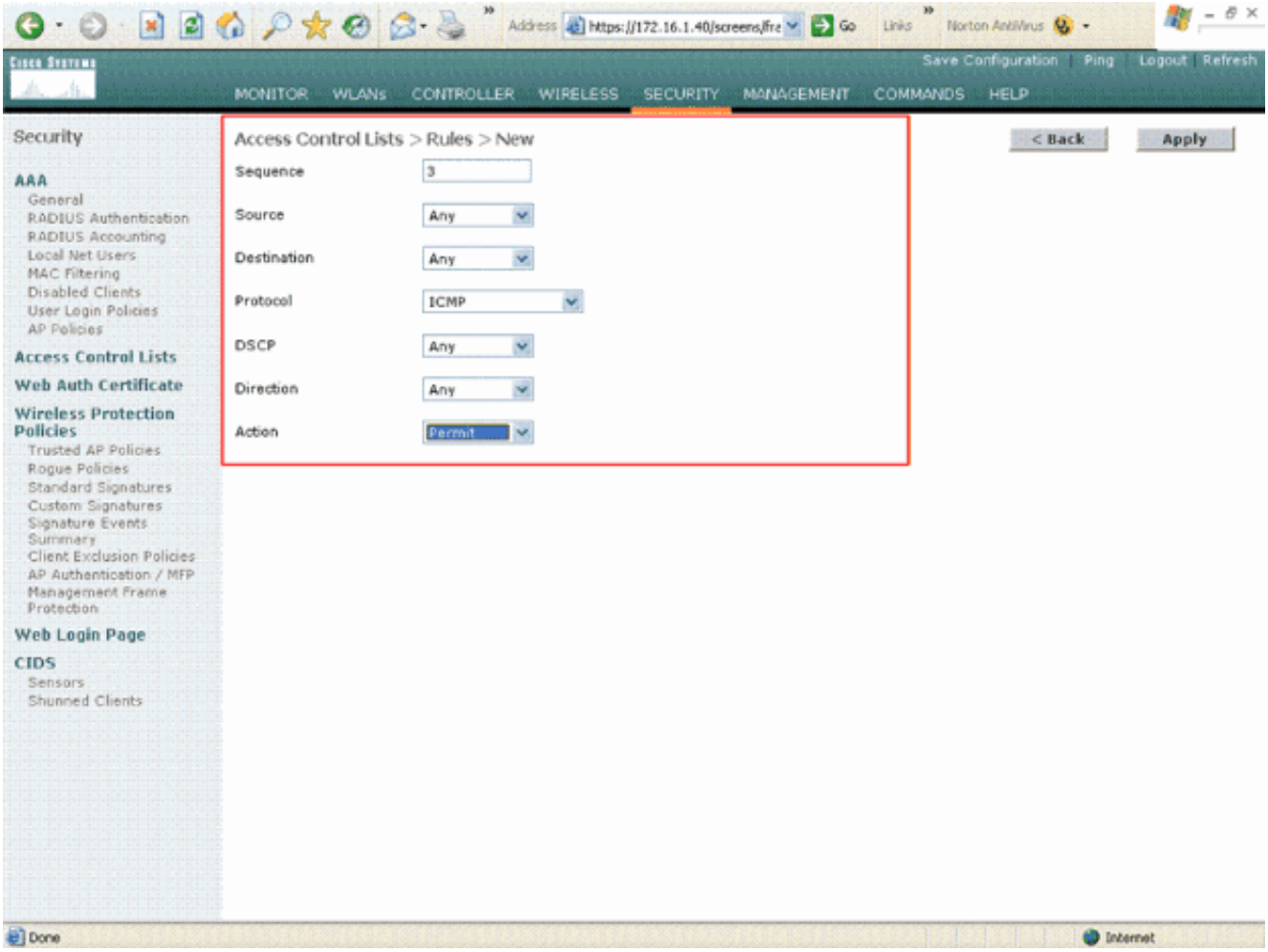
правило от клиента к серверу, **Входящее** использование данного примера. От раскрывающегося окна Действия выберите **Permit**, чтобы заставить этот ACL позволять пакеты DHCP от беспроводного клиента к серверу DHCP. Значение по умолчанию, Запрещают. **Щелкните**
"Применить".



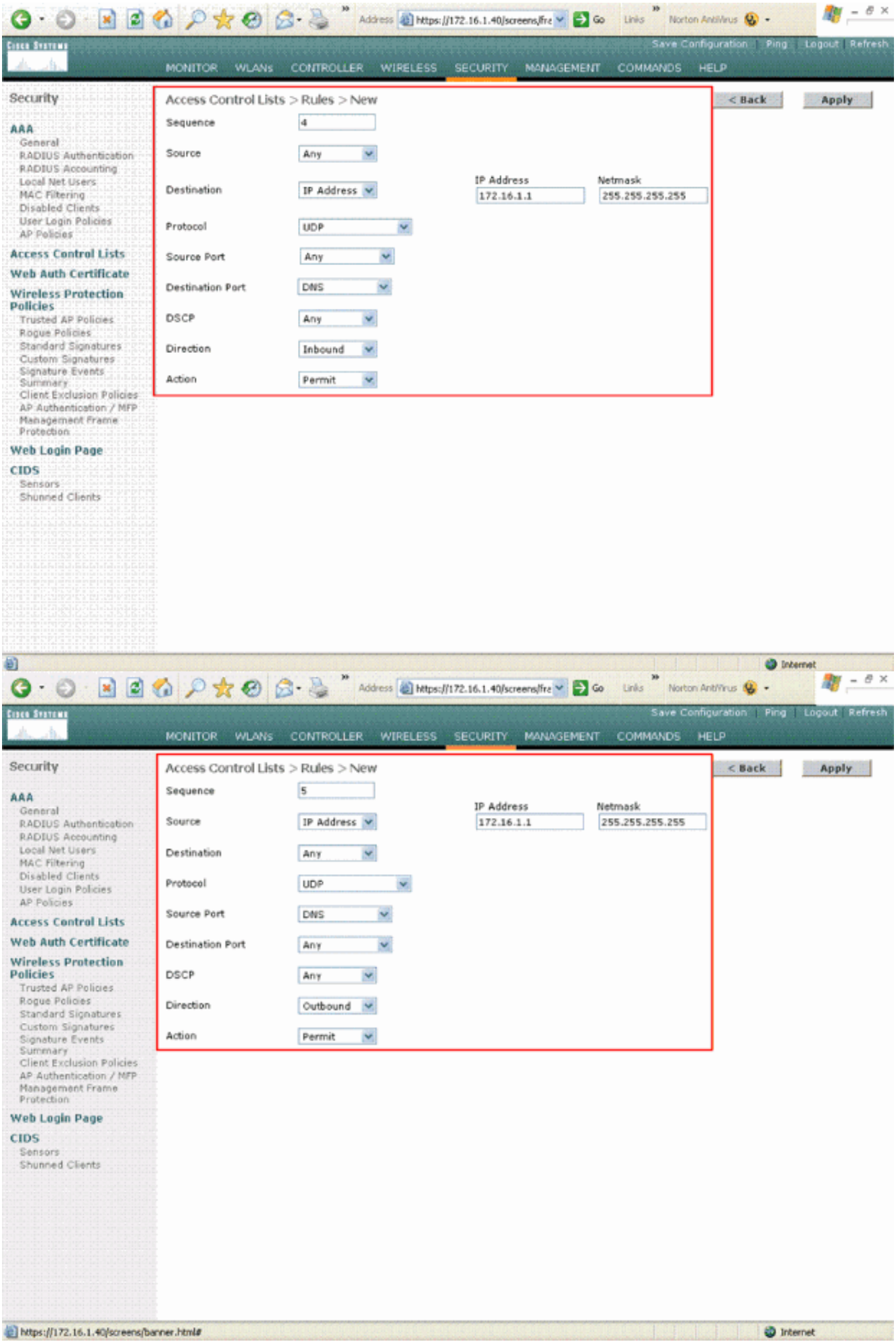
Если или источник или назначение не **никто**, то обратный оператор в противоположном направлении должен быть создан.
Например.



2. Для определения правила, которое позволяет пакеты ICMP между всеми устройствами, выберите **любого** для Источника и Полей Назначение. Это значение используется по умолчанию.Выберите **ICMP** из Протокола выпадающее поле. Поскольку данный пример использует **любого** для Источника и Полей Назначение, вы не должны задавать направление. Это можно оставить в его значении по умолчанию **любого**. Кроме того, обратный оператор в противоположном направлении не требуется.От раскрывающегося меню Действия выберите **Permit**, чтобы заставить этот ACL позволять пакеты DHCP от сервера DHCP до беспроводного клиента. **Щелкните "Применить".**

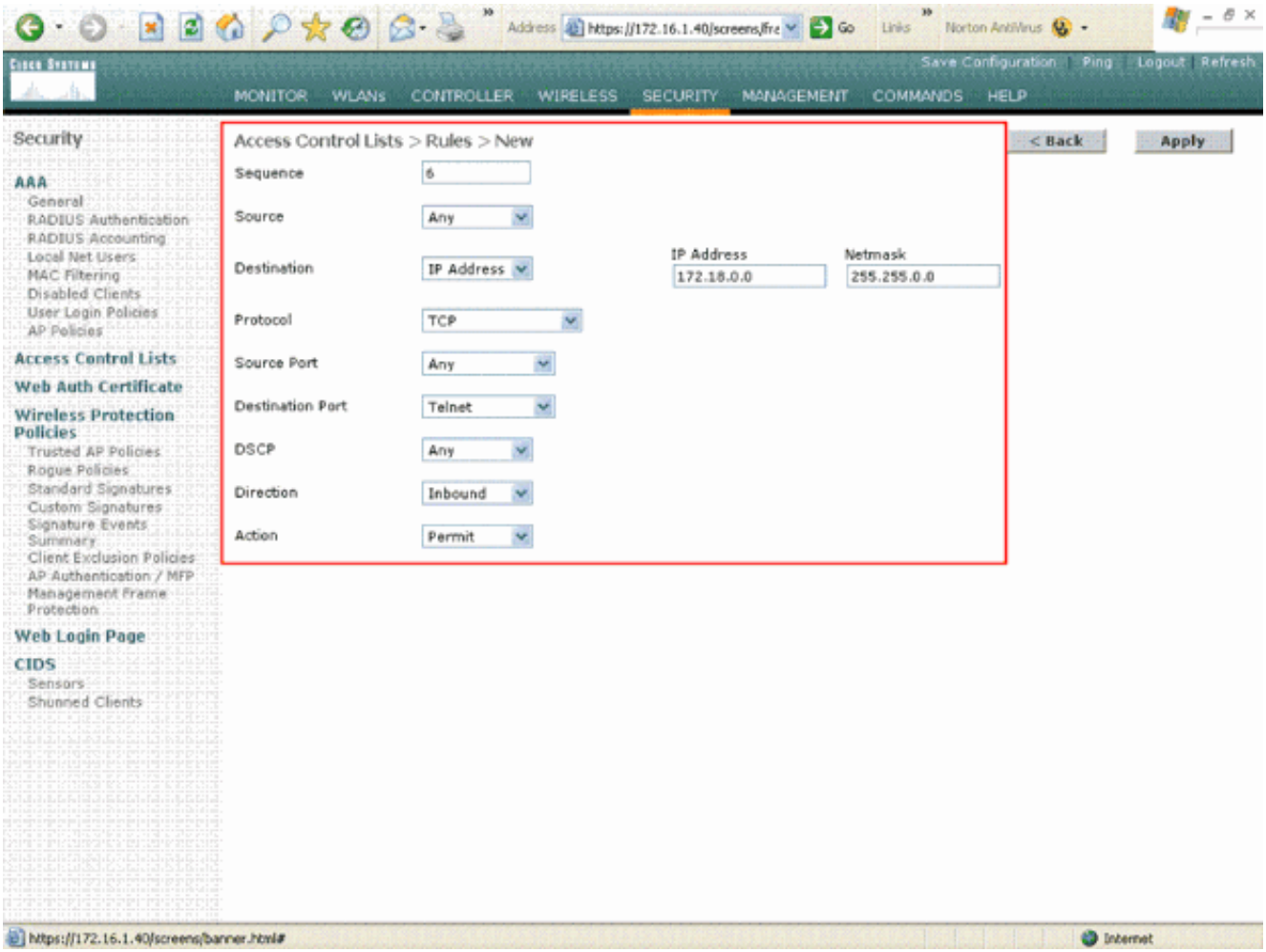


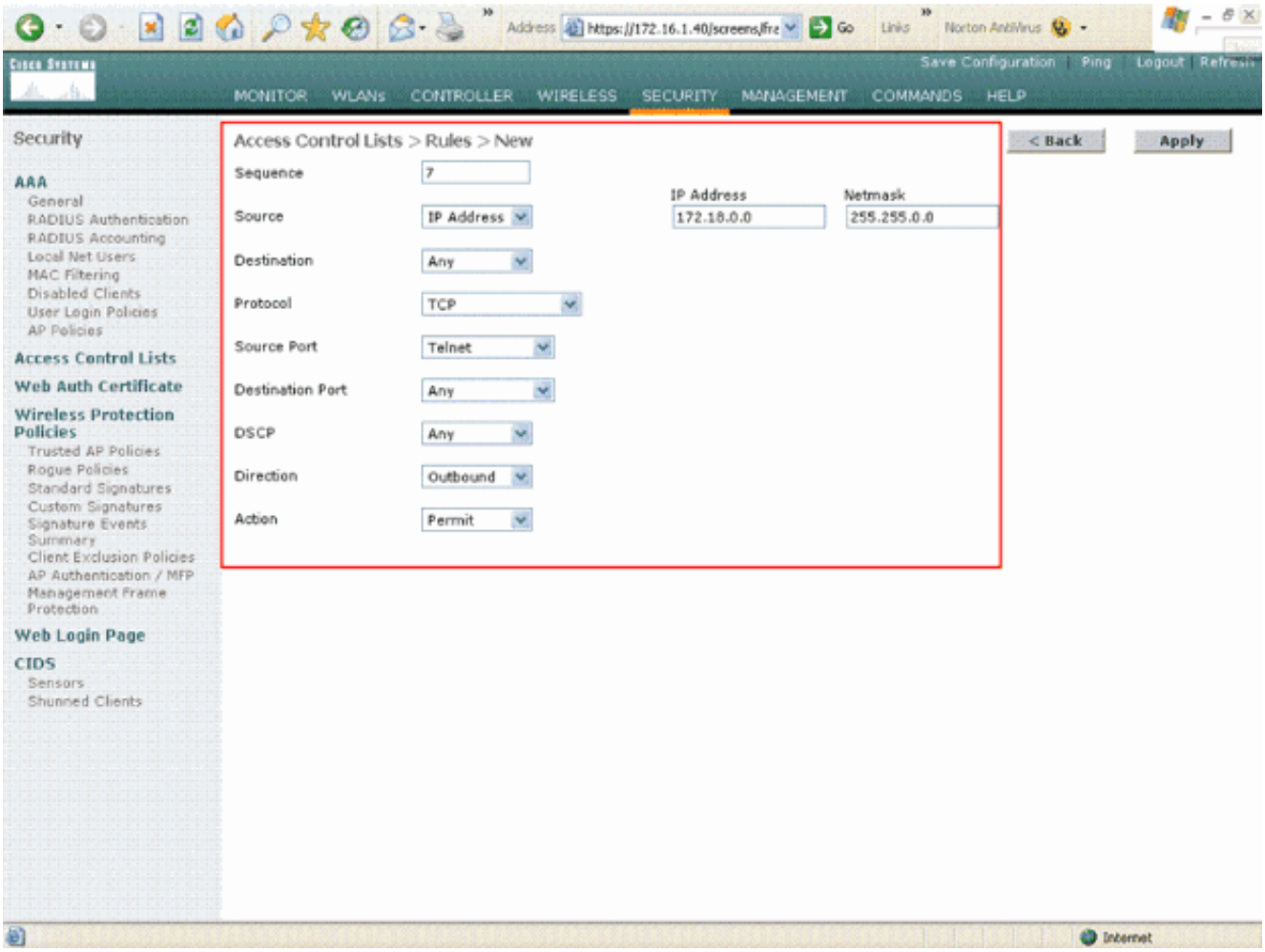
3. Точно так же создайте правила, которые предоставляют доступ сервера DNS всем беспроводным клиентам и доступ сервера Telnet для беспроводного клиента к определенной подсети. Вот
примеры.



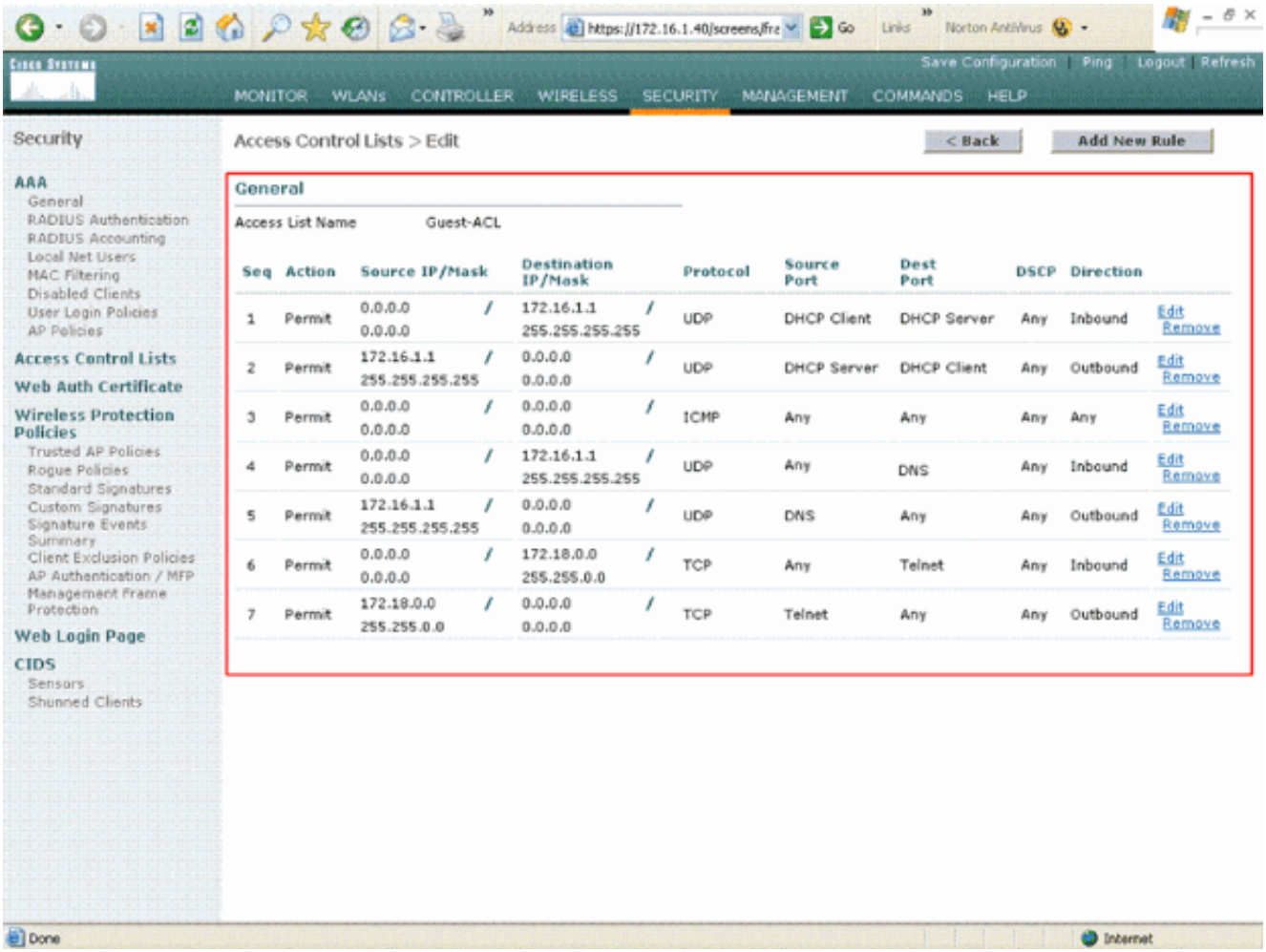
Определите это правило для предоставления доступа для беспроводного клиента к

Сервису
Telnet.

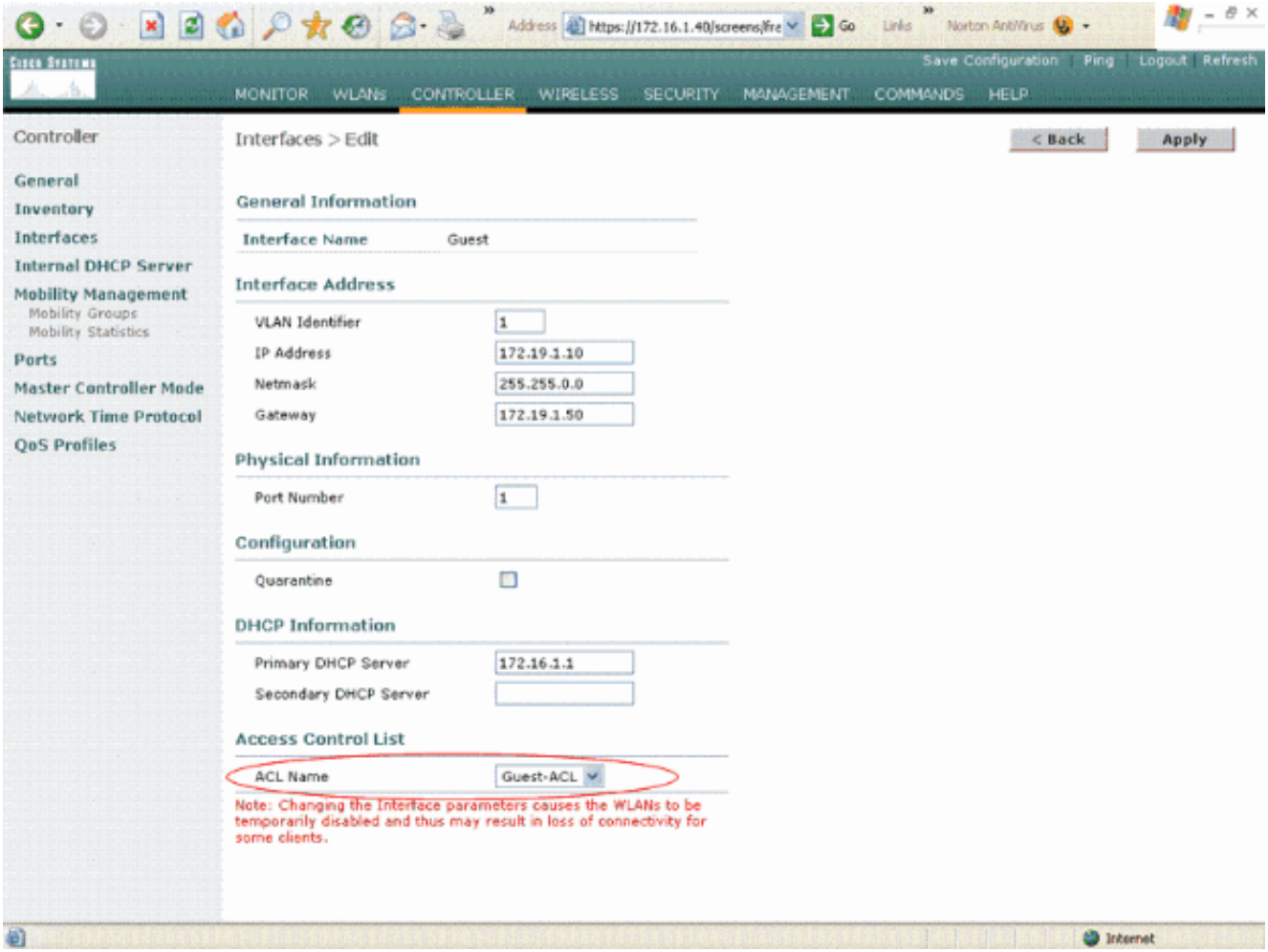




ACL> страница Edit перечисляет все правила, которые определены для ACL.



4. Как только ACL создан, он должен быть применен к динамическому интерфейсу. Для применения ACL выберите **Controller> Interfaces** и отредактируйте интерфейс, к которому вы хотите применить ACL.
5. В **Интерфейсах> страница Edit** для динамического интерфейса, выберите соответствующий ACL из раскрывающегося меню Списков контроля доступа. Например.



Как только это сделано, ACL разрешает и запрещает трафик (на основе настроенных правил) на WLAN, который использует этот динамический интерфейс. Интерфейсному ACL можно только примениться к AP H-Reap в Связанном режиме, но не в Автономном режиме.

Примечание: См. Использование CLI для Настройки Списков контроля доступа для получения информации о том, как создать ACL с CLI на WLC.

Примечание: Этот документ предполагает, что настроены WLAN и динамические интерфейсы. См. VLAN на Примере конфигурации Контроллеров беспроводной локальной сети для получения информации о том, как создать динамические интерфейсы на WLC.

Настройте ACL ЦП

Ранее, ACL на WLC не имели опции для фильтрации трафика данных LWAPP/CAPWAP, контрольного трафика LWAPP/CAPWAP и трафика мобильности, предназначенного к менеджменту и интерфейсам диспетчера точки доступа. Для решения этой проблемы и LWAPP фильтра и трафика мобильности, ACL ЦП были начаты с микропрограммы версии 4.0 WLC.

Конфигурация ACL ЦП включает два шага:

1. Настройте правила для ACL ЦП.
2. Примените ACL ЦП на WLC.

Правила для ACL ЦП должны быть настроены похожим способом к другим ACL. См. раздел ACL ЦП Обеспечения Контроллеров беспроводной локальной сети (WLC) для получения дополнительной информации о ACL ЦП.

Проверка

Cisco рекомендует протестировать конфигурации списков управления доступом (ACL) с беспроводным клиентом, чтобы гарантировать настройку их правильно. Если они не в состоянии работать правильно, проверять ACL на веб-странице ACL и проверять, что ваши изменения ACL были применены к интерфейсу контроллера.

Можно также использовать эти **команды показа** для проверки конфигурации:

- **show acl summary** — Для отображения ACL, которые настроены на контроллере, используют **команду show acl summary**.Например:`(Cisco Controller) >show acl summary`

```
ACL Name                         Applied
-------------------------------- -------
Guest-ACL                        Yes
```

- **show acl детализировал** *ACL_Name* — Отображает подробные сведения на настроенных ACL.Например:`(Cisco Controller) >show acl detailed` **`Guest-ACL`** `Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action -- --- ------------------------------ ------------------------------ --- - ---------- ---------- ---- ------ 1 In 0.0.0.0/0.0.0.0 172.16.1.1/255.255.255.255 17 68-68 67-67 Any Permit 2 Out 172.16.1.1/255.255.255.255 0.0.0.0/0.0.0.0 17 67-67 68-68 Any Permit 3 Any 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 1 0-65535 0-65535 Any Permit 4 In 0.0.0.0/0.0.0.0 172.16.1.1/255.255.255.255 17 0-65535 53-53 Any Permit 5 Out 172.16.1.1/255.255.255.255 0.0.0.0/0.0.0.0 17 53-53 0-65535 Any Permit 6 In 0.0.0.0/0.0.0.0 172.18.0.0/255.255.0.0 60-65535 23-23 Any Permit 7 Out 172.18.0.0/255.255.0.0 0.0.0.0/0.0.0.0 6 23-23 0-65535 Any Permit`
- **show acl cpu** — Для отображения ACL, настроенных на ЦП, используйте **команду show acl cpu**.Например:`(Cisco Controller) >show acl cpu`

```
CPU Acl Name.............................. CPU-ACL
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

Устранение неполадок

Выпуск ПО контроллера 4.2.61.0 или позже позволяет вам настроить счетчики ACL. Счетчики ACL могут помочь в определении, какие ACL были применены к пакетам, переданным через контроллер. Эта функция полезна при устранении проблем системы.

Счетчики ACL доступны на этих контроллерах:

- Серии 4400
- Cisco WiSM
- Catalyst 3750G интегрированный коммутатор контроллера беспроводной локальной сети

Для активации этой опции выполните эти шаги:

1. Выберите **Security> Access Control Lists> Access Control Lists** для открытия страницы Access Control Lists.Эта страница перечисляет все ACL, которые были настроены для этого контроллера.
2. Чтобы видеть, поражают ли пакеты какой-либо из ACL, настроенных на вашем контроллере, проверьте флажок **Enable Counters** и нажмите **Apply**. В противном случае оставьте флажок неконтролируемым. Это значение используется по умолчанию.

3. Если вы хотите очистить счетчики для ACL, нависнуть ваш курсор над синей стрелкой выпадающего списка для того ACL и выбрать **Clear Counters**.

Дополнительные сведения

- Настройка и применение списков контроля доступа
- Пример конфигурации сетей VLAN на контроллерах беспроводной LAN
- Регистрация облегченных точек доступа у контроллеру беспроводных LAN (WLC)
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Поддержка технологии беспроводных сетей/Мобильности
- Cisco Systems – техническая поддержка и документация