Управляйте базирующейся посторонней классификацией в контроллерах беспроводной локальной сети (WLC) и Wireless Control System (WCS)

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Управляйте базирующейся посторонней классификацией
Управляйте базирующейся посторонней терминологией классификации
Посторонние правила классификации
Посторонняя классификация и страны-изгои
Объясненные страны-изгои
Как настроить посторонние правила в WLC
Как настроить посторонние правила в WCS
Дополнительные сведения

Введение

В Wireless Control System (WCS) 5.0 выпусков WCS улучшил Посторонние Функциональные возможности управления для других посторонних типов AP и предоставил определяемые пользователем правила автоматически классифицировать посторонние AP. WCS применил посторонние правила классификации AP к контроллерам. Этот документ объясняет расширенные Посторонние Функциональные возможности управления и шаги, необходимые для настройки этой функциональности на Контроллере беспроводной локальной сети (WLC) и WCS.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание протокола LWAPP
- Знание решений по обеспечению безопасности контроллера беспроводной локальной сети

Используемые компоненты

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

- Cisco WLC серии 4400, который выполняет микропрограммное обеспечение 5.2
- Облегченные точки доступа Cisco Aironet серии 1130 AG (LAP)
- Версия 5.2 Cisco Wireless Control System

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.

Управляйте базирующейся посторонней классификацией

В версиях WCS до выпуска 5.0 WCS отобразил слишком много неавторизованных точек доступа (AP) в **Сводной странице Безопасности**. Даже при том, что страны-изгои отличаются, они все появляются на одной странице, сортированной адресом BSSID/MAC жулика.

В выпуске WCS 5.0 WCS улучшил Посторонние Функциональные возможности управления и представил новую терминологию (Несекретный, Злонамеренный, и Дружественный) для других посторонних типов AP и предоставил определяемые пользователем правила автоматически классифицировать посторонние AP. WCS применил посторонние правила классификации AP к контроллерам.

WCS улучшил функцию управления страны-изгоя для хранения страны-изгоя как *Внешней*, как только состояние жулика было вручную изменено на *Внешний*. Когда получения по запросу WCS или обрабатывают сообщение прерывания от других контроллеров, WCS также обновляет *Внешнее* состояние для других контроллеров.

Чтобы поддерживать эту функцию, и WLC и WCS должны выполнять 5.0 выпусков.

Управляйте базирующейся посторонней терминологией классификации

С этой новой функциональностью представлены эти новые посторонние типы AP:

- **Злонамеренный AP:** обнаруженный AP, который совпадает с определяемыми пользователем Злонамеренными правилами или был вручную перемещен от Дружественных AP.
- **Дружественный AP:** Существующий известный, Подтвердите, и Трастовые Недостающие страны-изгои классифицированы как Дружественные. Кроме того,

обнаруженные AP, которые совпадают с определяемыми пользователем Дружественными правилами, классифицированы как Дружественные. Дружественные AP не могут содержаться.

- **Несекретный AP:** обнаруженный AP, который не совпадал со Злонамеренными или Дружественными правилами. Может содержаться Несекретный AP. Несекретный AP может быть вручную перемещен в Дружественный пользователем. Определяемые пользователем правила автоматически переместить Несекретный AP в Дружественный или Злонамеренное, например, на обнаружении, SSID пуст. На следующем постороннем отчёте найден SSID, и это, оказывается, настраиваемый SSID.

Посторонние правила классификации

Это правила классификации, применимые к каждому из посторонних типов AP:

- Злонамеренные правилаСоответствия управляли SSIDСовпадает с SSID настройки пользователяНикакое шифрование на SSIDМинимальный RSSIПродолжительность времениКоличество клиентов связалось
- Дружественные правилаУправляемый SSIDНастраиваемый SSID
- Несекретные правилаНе совпадает со Злонамеренными или Дружественными правилами

Parameter	Description
Time Duration (0 to 3600)	Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration field. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
Minimum RSSI (-95 to -50)	Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI field. The valid range is -95 to -50 dBm (inclusive), and the default value is 0 dBm.
Minimum number of Rogue client (1-10)	Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients field. The valid range is 1 to 10 (inclusive), and the default value is 0.
No Encryption	Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option. **Note** WCS refers to this option as "Open Authentication."
Managed SSID[1]	Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.
User configured SSID[1]	Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User Configured SSID field, and click **Add SSID**. You can add multiple SSIDs. To remove an SSID, select the SSID and click **Remove**.

[1]The SSID and Managed SSID conditions cannot be used with the Match All operation as these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

Пользователь может принять решение совпасть **со всеми, любым** или **некоторыми** условиями правила по каждому правилу:

- **Все** средства совпадают со всеми настроенными условиями для правила.

- **Любые** средства совпадают с любым из настроенных условий для правила.
- **Некоторые** средства совпадают с немногими настроенными условиями для правила

Например, по *Злонамеренным Правилам*, пользователь настраивает *Управляемый SSID* и *Минимальный RSSI*. Затем у пользователя есть выбор, чтобы совпасть **со всеми** или **любым** из этих двух условий, или совпасть просто *с Минимальным* условием *RSSI*.

Когда контроллер получает посторонний отчёт, он делает это:

- Проверки, если обнаруженный AP находится в настраиваемом списке MAC. Если так, классифицируйте AP как Дружественный тип.
- Если обнаруженный AP не находится в списке, он начинает применять правила.
- Во-первых, это применяет *Злонамеренные Правила*. Если *Злонамеренные Правила* совпадают, это классифицировано как Злонамеренный тип. Если детектор RLDP/rogue решает, что этот жулик находится в сети, он отмечает страну-изгой как **Угрозу**. Пользователь может вручную содержать AP, который изменяет страну-изгой на **Содержавший**. Если AP не находится в сети, он отмечает страну-изгой как **Предупреждение**, и пользователь может содержать его вручную.
- Если *Злонамеренные Правила* не совпадают, применяют *Дружественные Правила*. Если *Дружественные Правила* совпадают, то классифицируют его как Дружественный тип.
- Если *Дружественные Правила* не совпадают, классифицируйте этот AP как Несекретный. Если детектор RLDP/rogue решает, что этот жулик находится в сети, отметьте страну-изгой как **Угрозу** и классифицируйте ее как Злонамеренный тип. Пользователь может вручную содержать AP, который изменяет страну-изгой на **Содержавший**. Если AP не находится в сети, отметьте страну-изгой как **Предупреждение**, и пользователь может содержать его вручную.
- Пользователь может вручную переместить AP в другой тип классификации.

Посторонняя классификация и страны-изгои

Эта таблица показывает другие классификации жуликов и стран-изгоев для каждой классификации.

Основанный на правилах тип классификации	**Страны-изгои**
Злонамеренный AP	Аварийная угроза содержавшее содержавшее удаленное ожидание
Несекретный AP	Аварийное содержавшее содержавшее удаленное ожидание
Дружественный AP	Внутренний (Известный в настоящее время) Внешний (В настоящее время подтверждают), Внутренние Пропавшие без вести (Пропавшие без вести Доверия) Предупреждение

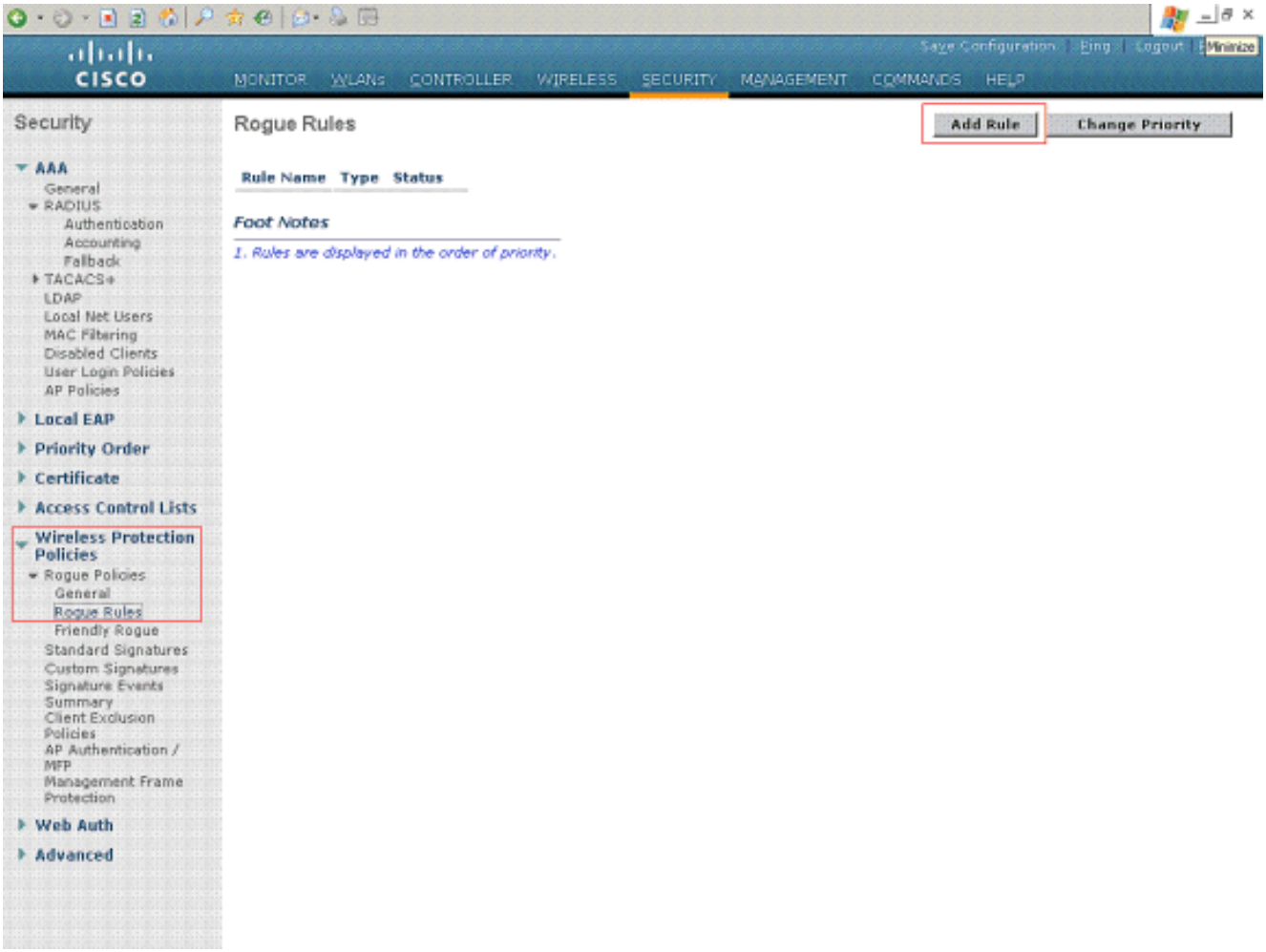
Объясненные страны-изгои

- **Ожидая —** На первом обнаружении, обнаруженный AP помещен в состояние в состоянии ожидания в течение 3 минут. На этот раз достаточно для управляемых AP, чтобы определить, является ли обнаруженный AP соседним AP.
- **Предупреждение —** После 3-минутного таймаута, обнаруженный AP перемещен в **Предупреждение**, если это не находится в соседнем списке или настраиваемом Дружественном списке MAC.
- **Угроза —** обнаруженный AP найден в сети.
- **Содержавший —** обнаруженный AP содержится.
- **Содержавшее Ожидание —** обнаруженный AP отмечен содержавший, но действие включения задержано из-за ней имеющихся в наличии ресурс.
- **Внутренний —** обнаруженный AP в сети, и пользователь вручную настраивает его как **Дружественный, Внутренний**, например, AP в лабораторной сети.
- **Внешний —** обнаруженный AP вне сети, и пользователь вручную настраивает его как **Дружественный, Внешний**, например, AP, которые принадлежат соседней сети.
- **Доверяемое Отсутствие —** Если настраиваемый Дружественный MAC обнаружили и не слышат на время трастового таймаута, страну-изгой Дружественного AP, отмечено как Доверяемые Пропавшие без вести.
- **Удаленный —** Если Злонамеренный или Несекретный AP не слышат от всех контроллеров на время постороннего таймаута, страна-изгой AP отмечена как **Удаленная**.

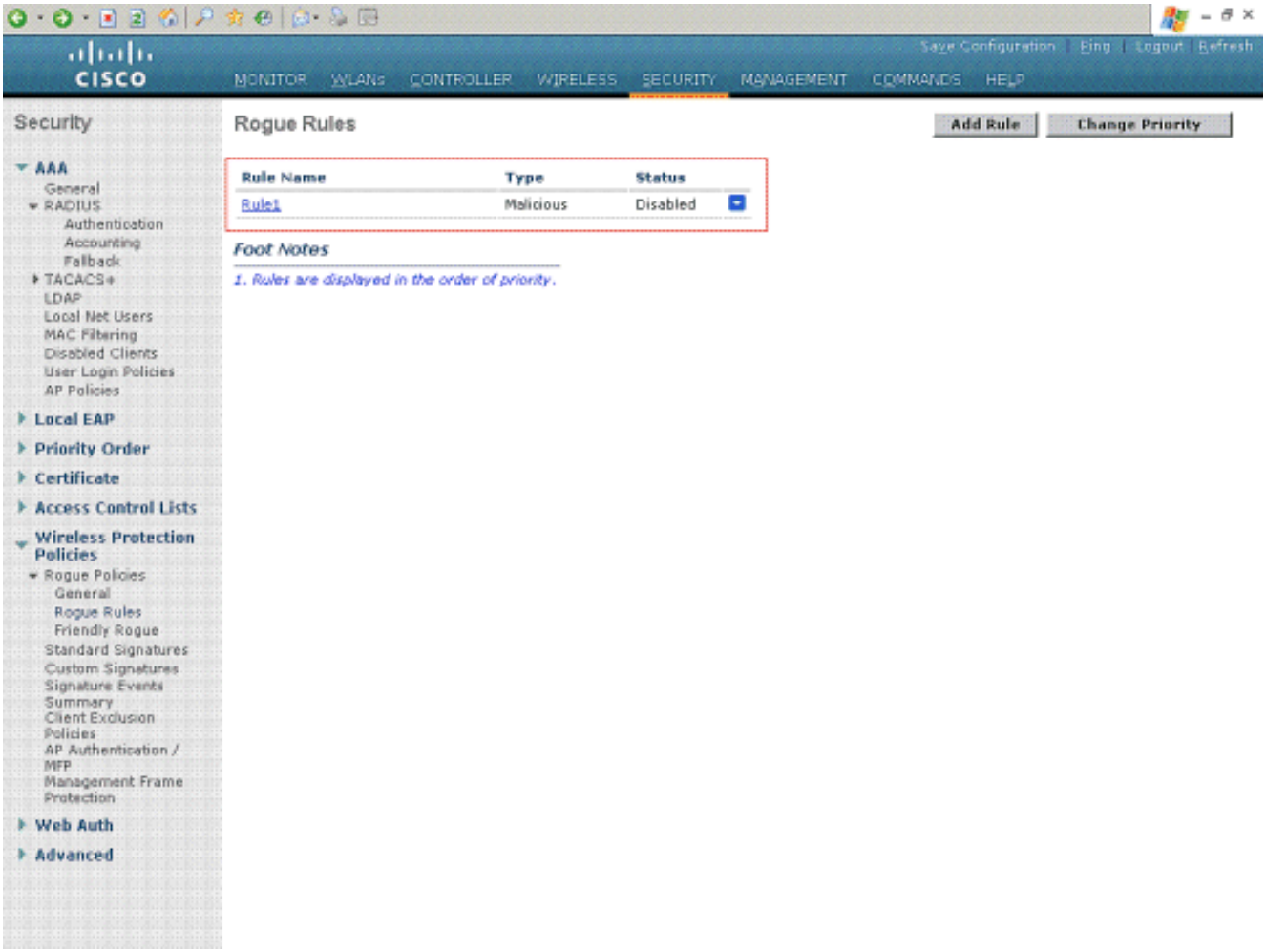
Как настроить посторонние правила в WLC

Для настройки посторонних правил о Контроллере беспроводной локальной сети выполните эти шаги.

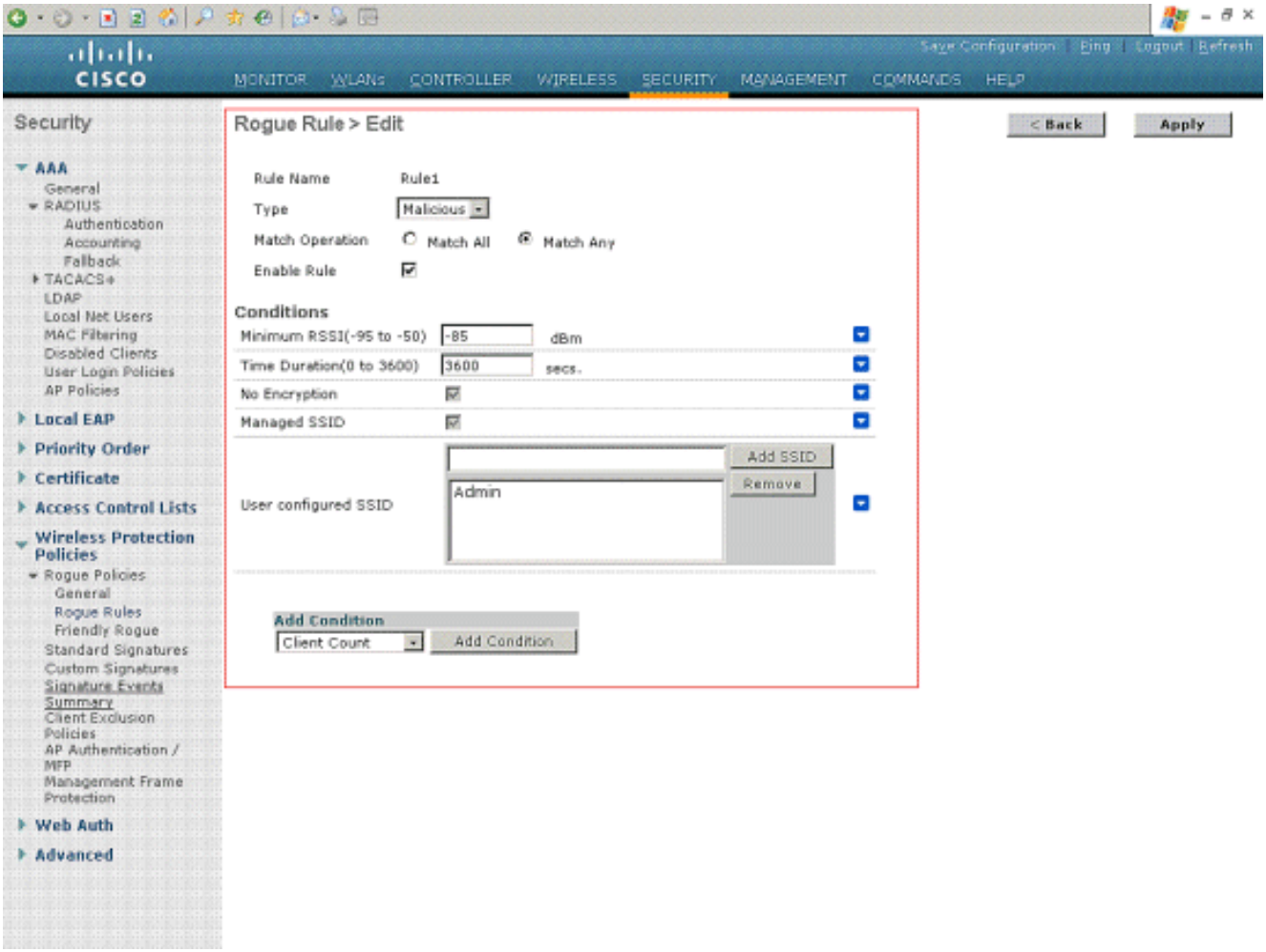
1. Посторонние правила могут быть созданы от WLC от страницы **Security> Wireless Protection Policies> Rogue Policies> Rogue Rules**.



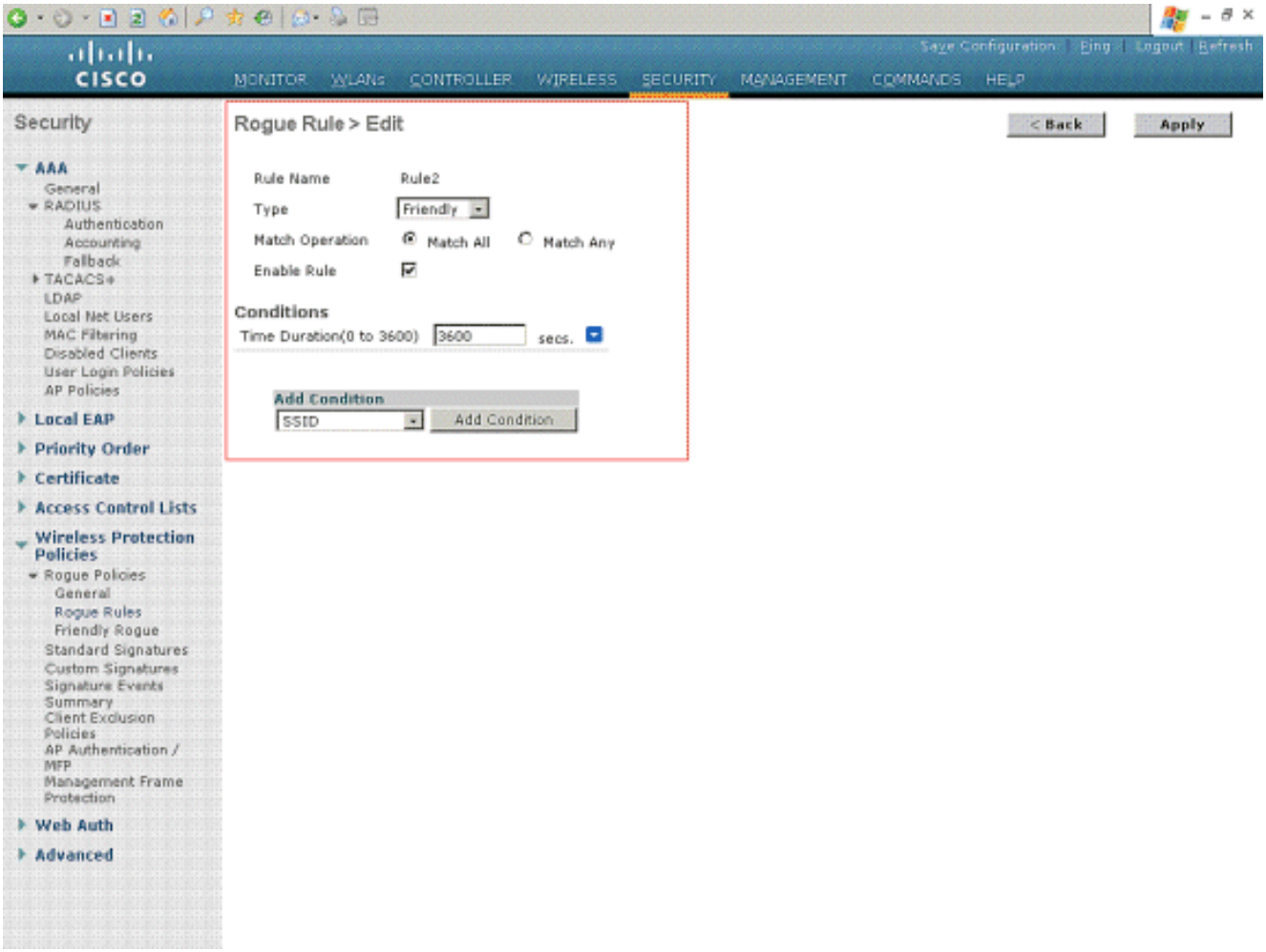
2. Для создания новой посторонней политики нажмите кнопку **Add Rule**. Окно **Rogue Rules** появляется. Введите имя для правила. Данный пример использует Rule1. Выберите тип правила. Это - пример Злонамеренного правила. **Нажмите Add**. Rule1 создан.



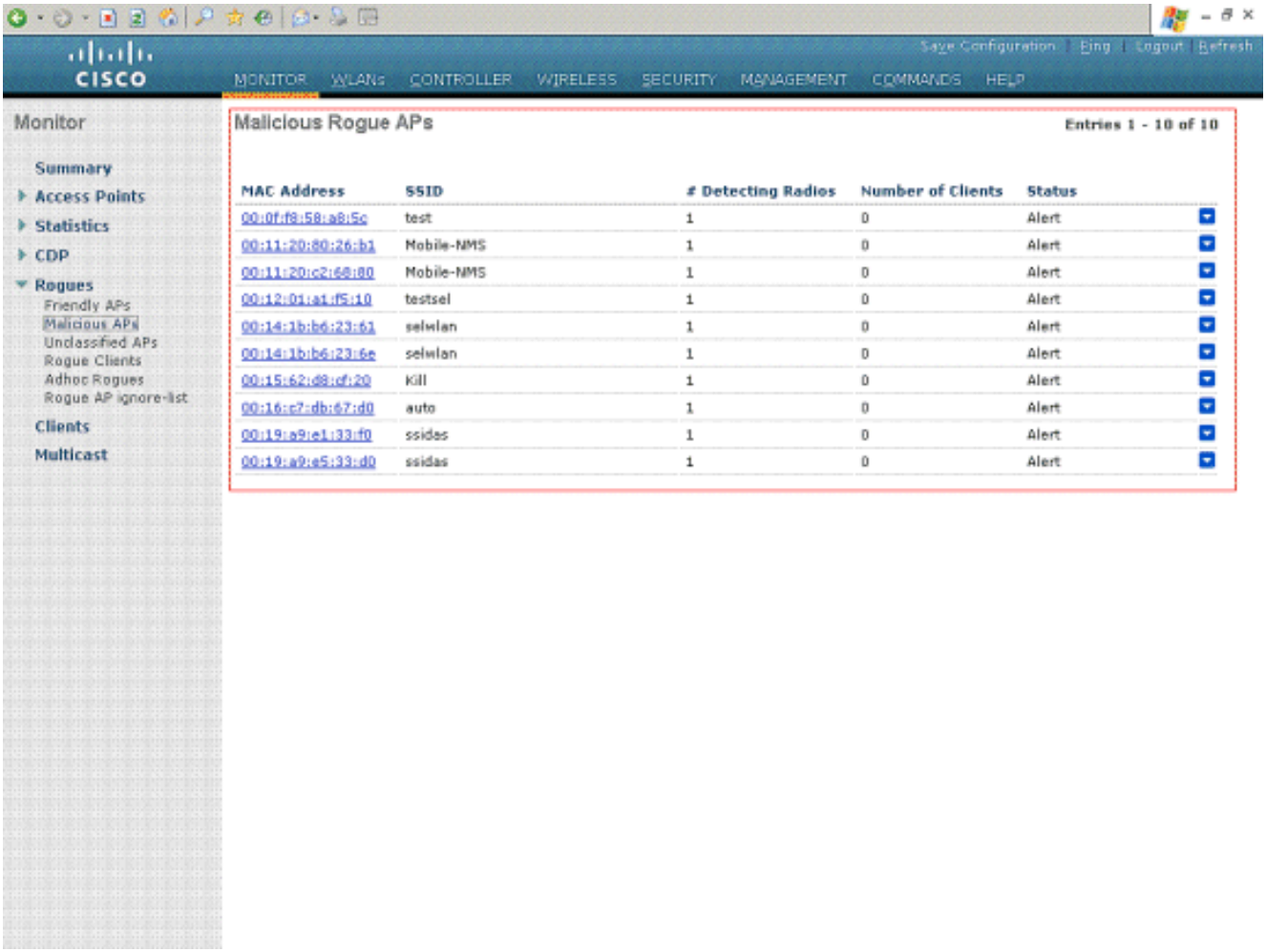
3. Для редактирования этого правила нажмите правило, которое было создано. **Постороннее Правило> страница Edit** появляется. На этой странице проверьте флажок **Enable Rule** для активации правила. Выберите Match Operation type и другие условия на основе требования как в данном
примере.



4. Это - пример Дружественной посторонней политики правила.



5. Выходные данные посторонних правил могут быть замечены в **Мониторе> Жулики> Злонамеренный AP**.

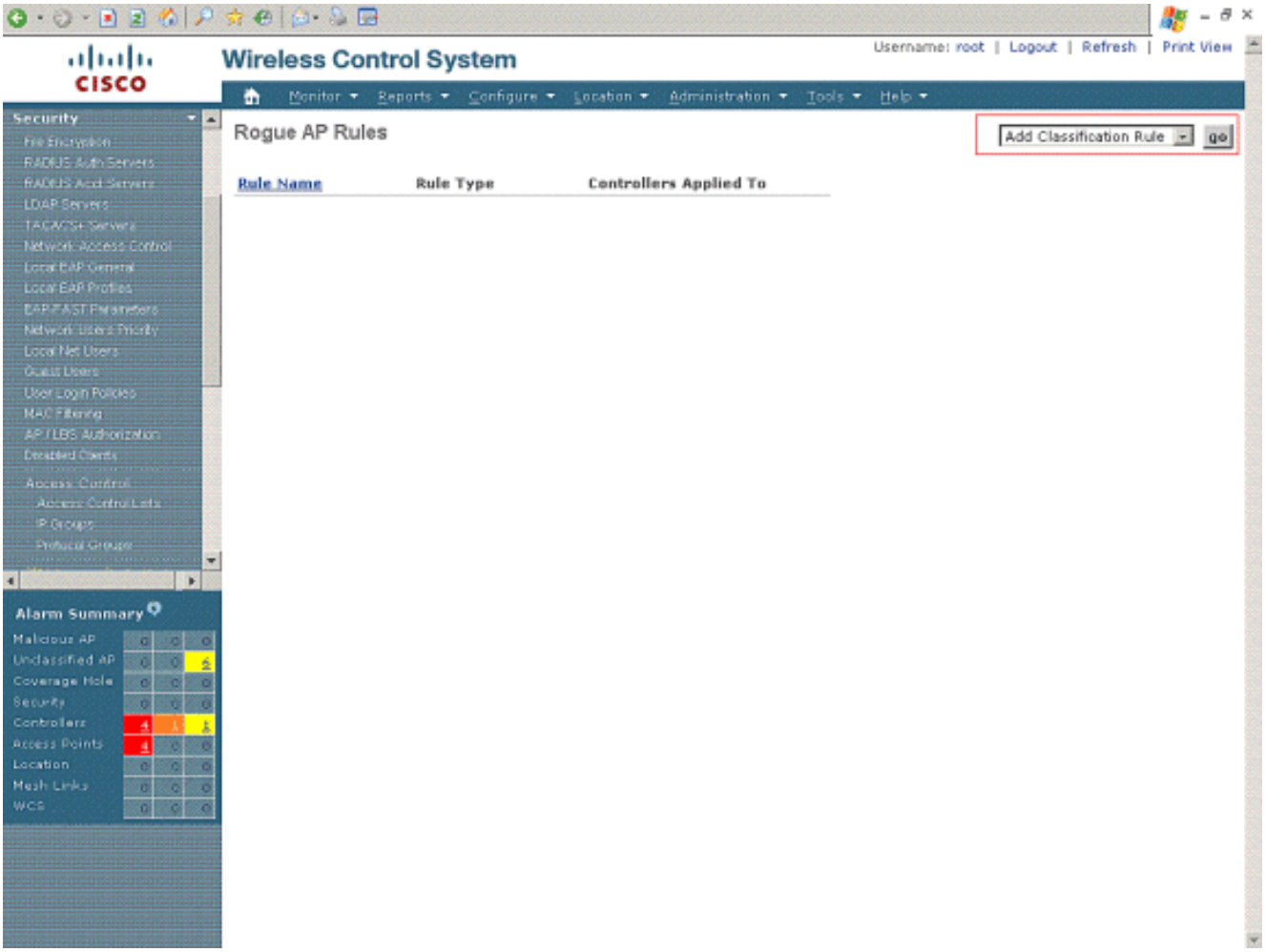


6. Точно так же выходные данные *Дружественных Правил* и *Несекретных Правил* могут быть просмотрены в страницах **Monitor> Rogues> Unclassified AP и Monitor> Rogues> Friendly AP**, соответственно.

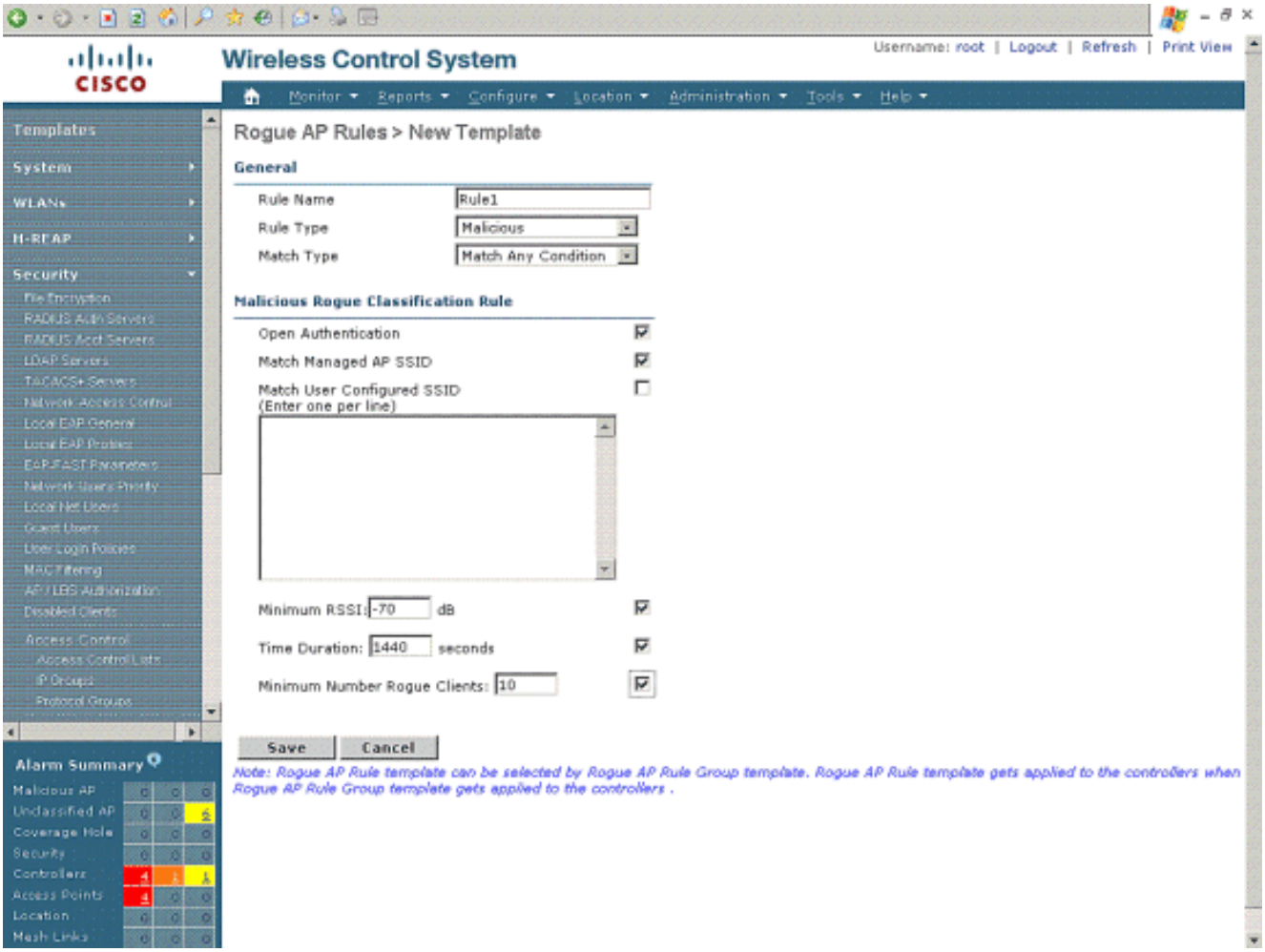
Как настроить посторонние правила в WCS

Постороннее Правило List:WCS предоставляет значение правила жулика уровня системы. Для настройки посторонних правил о WCS выполните эти шаги.

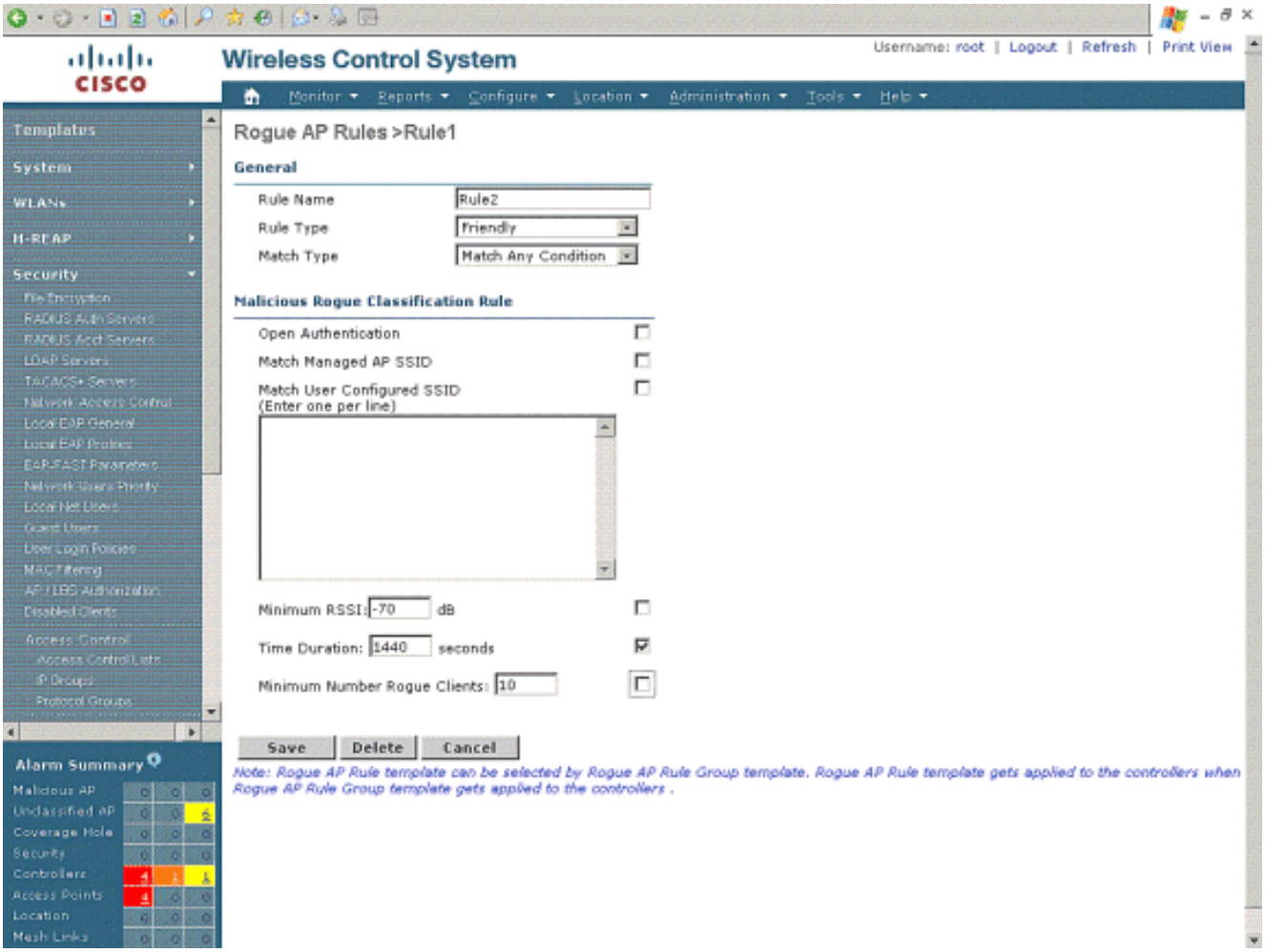
1. Выберите **Configure> Controller Template**, и затем нажмите **Security> Rogue AP Rules** для доступа к Посторонней странице списка Правил AP.
2. **Нажмите Add Правило Классификации** о правильном главном раскрывающемся меню для добавления нового правила
   классификации.



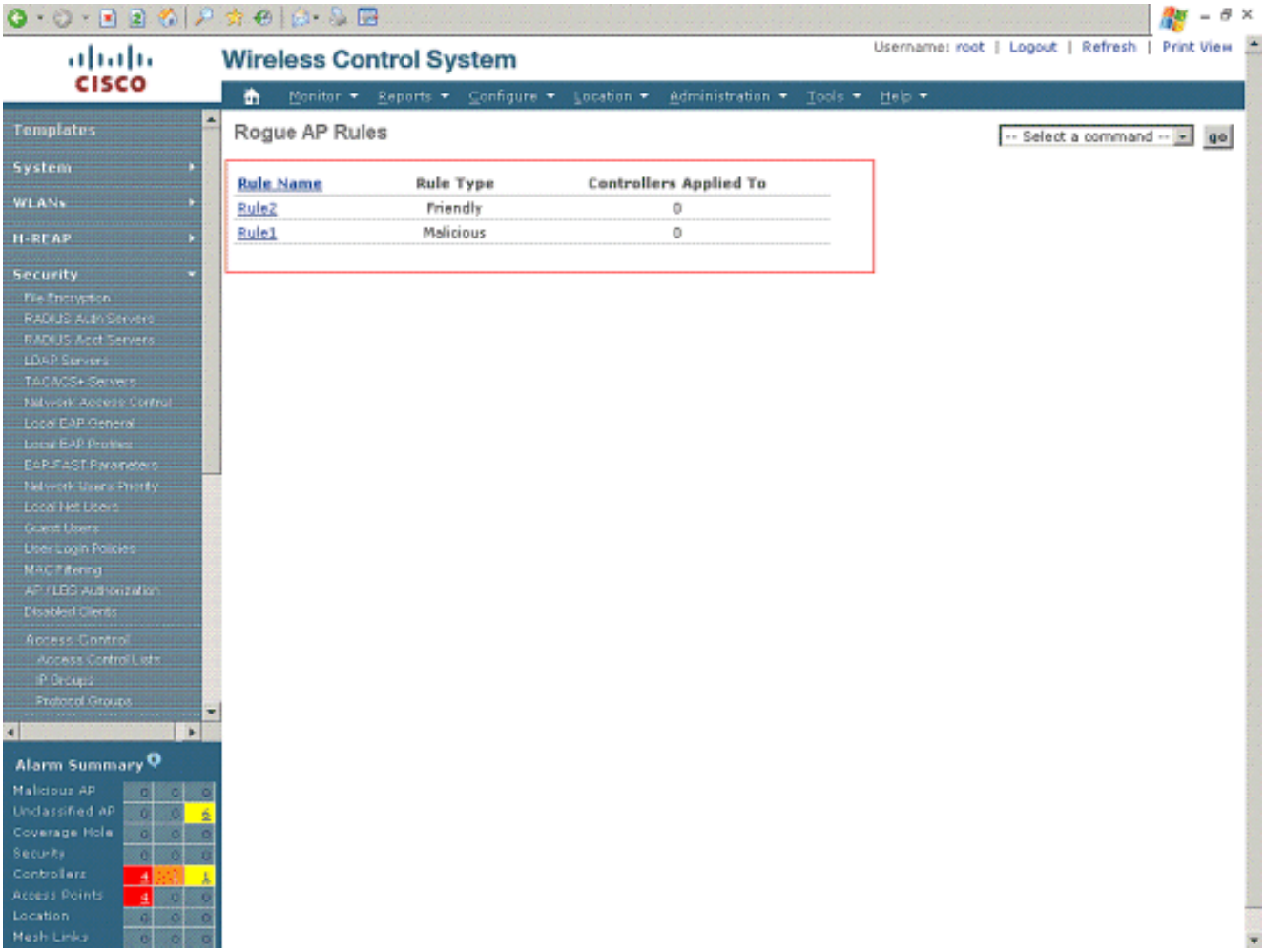
3. Нажмите имя шаблона для редактирования постороннего правила. Эта подробная страница правила позволяет вам отредактировать, обновить постороннее правило AP или удалить правило.**Посторонний AP Управляет Устанавливающий Parameters:On** эта страница, пользователи могут включить любое условие, когда они проверяют флажок для конкатенации любых из этих условий:Никакое шифрованиеСовпадите с управляемым APСовпадите с SSID настройки пользователяМинимальный RSSIПродолжительностьКлиент жулика минимального количестваЭто - пример Злонамеренного
правила:



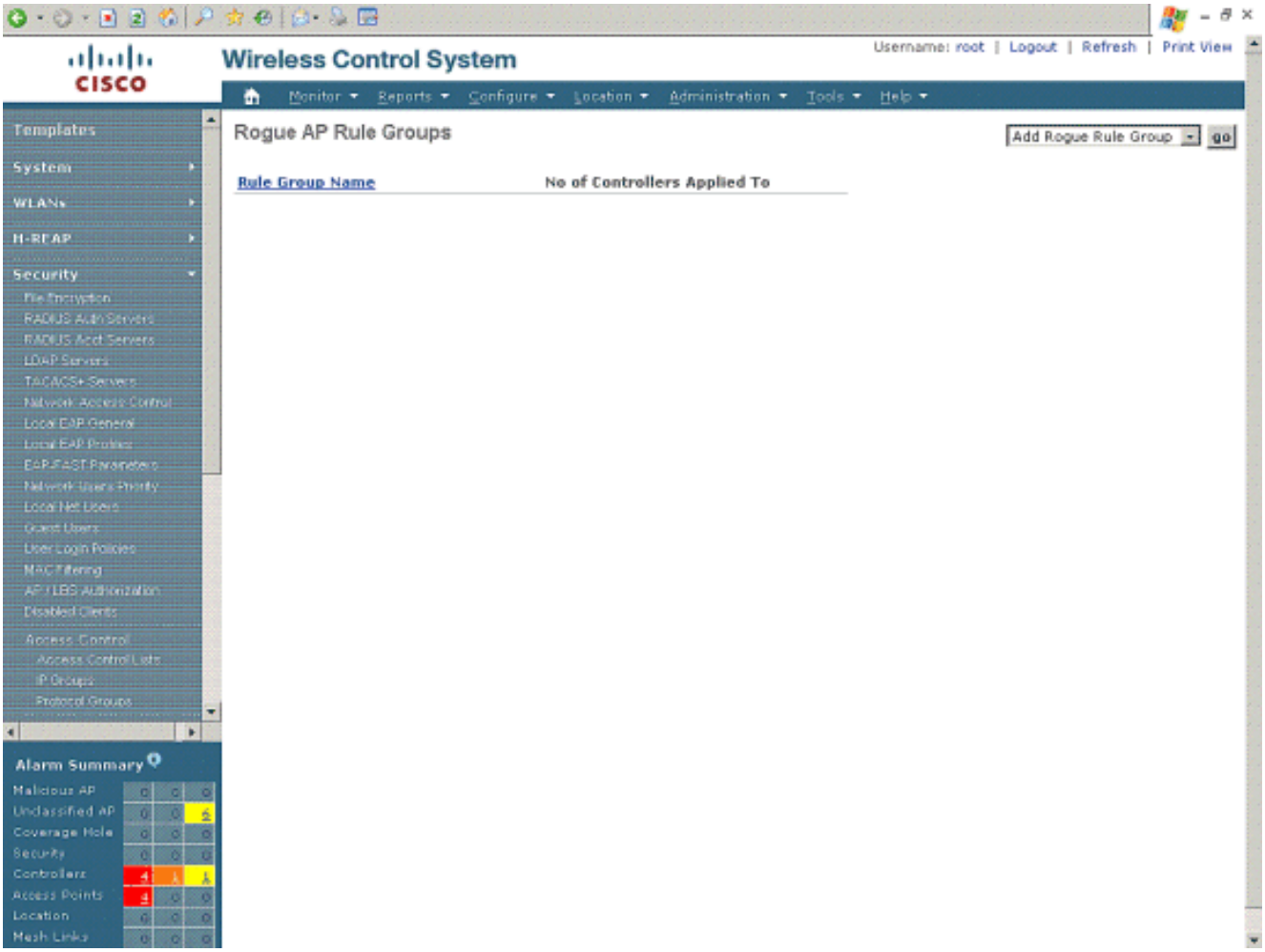
Это - пример Дружественного правила:



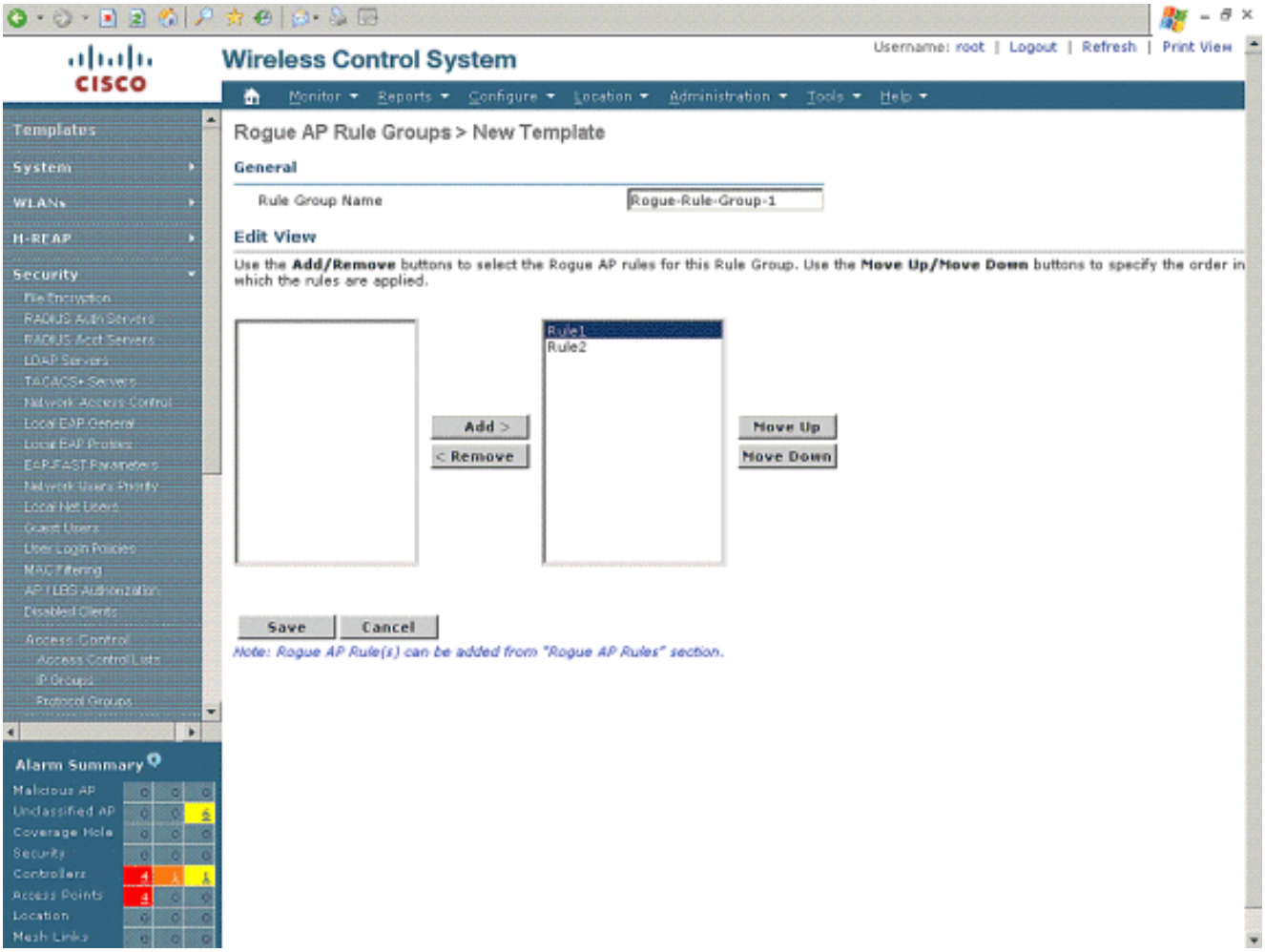
4. Страница Rogue AP Rules перечисляет все созданные правила.



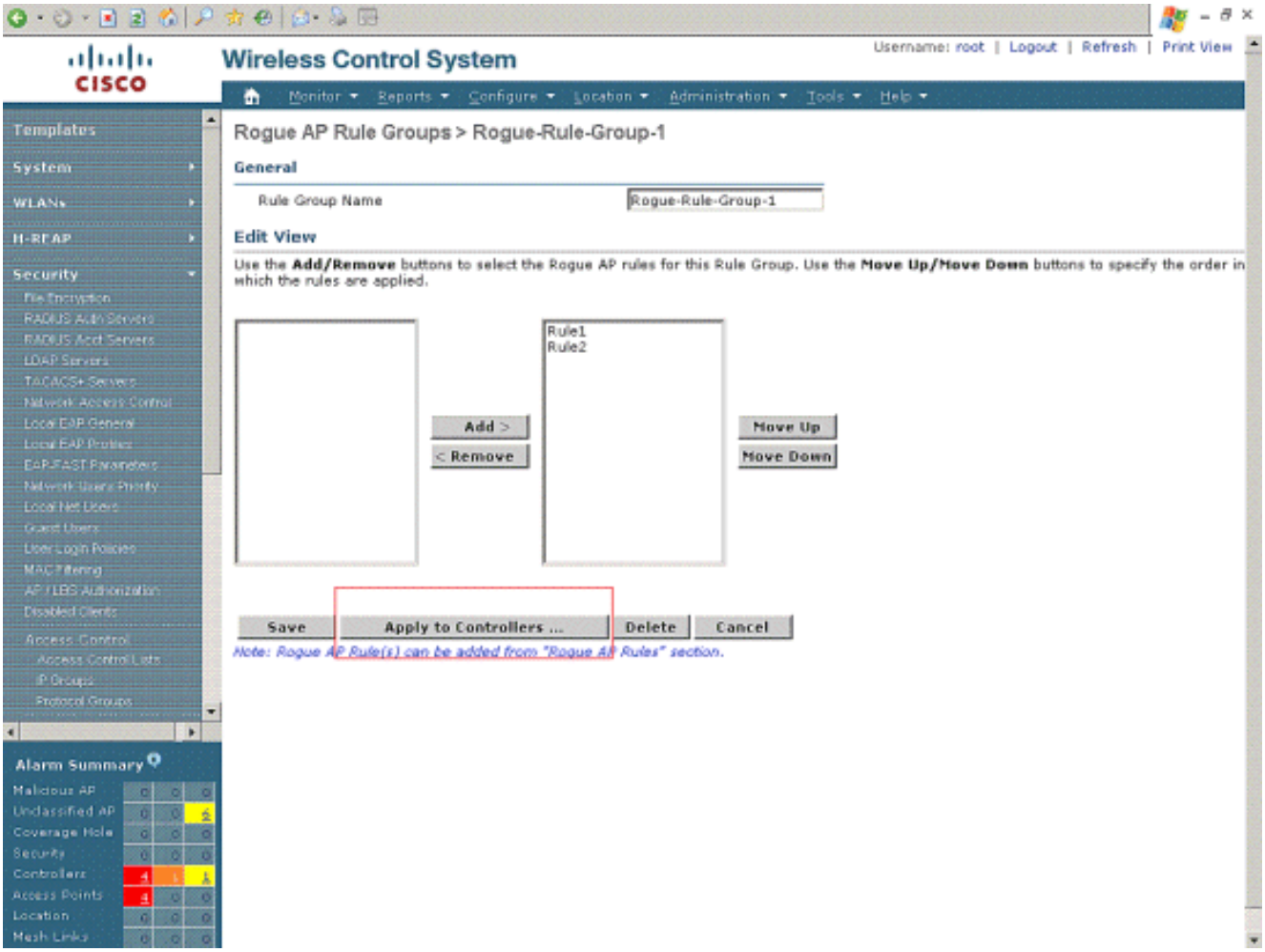
5. Следующий шаг должен настроить группу правила и применить эти правила к контроллерам. Чтобы к этому, используйте значение **Rogue AP Rule Groups** на WCS.
6. Для создания новой группы правила выберите **Configure> Controller Template**, и затем нажмите **Security> Rogue AP Rule Groups** от GUI
WCS.



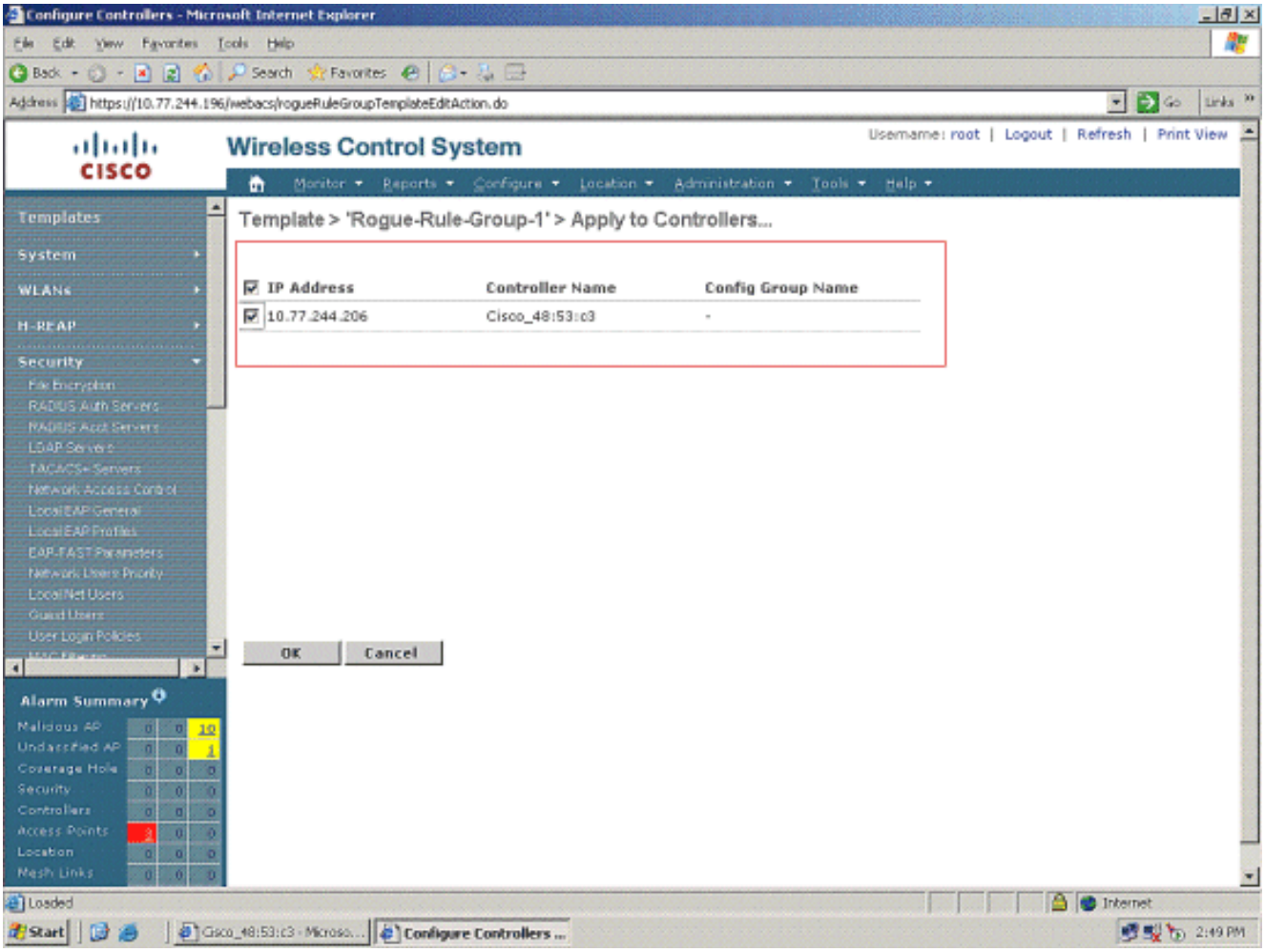
7. Страница Rogue AP Rule Groups> New Template позволяет вам добавить, обновить постороннюю группу правила AP, удалить правило и применить группу правила к контроллеру. Используйте кнопки Add/Remove для выбора посторонних правил AP для этой группы правила. Используйте кнопки Up/Down для определения заказа, в котором применены правила. Ниже представлен пример. Как только группа правил настроена, нажмите
Save.



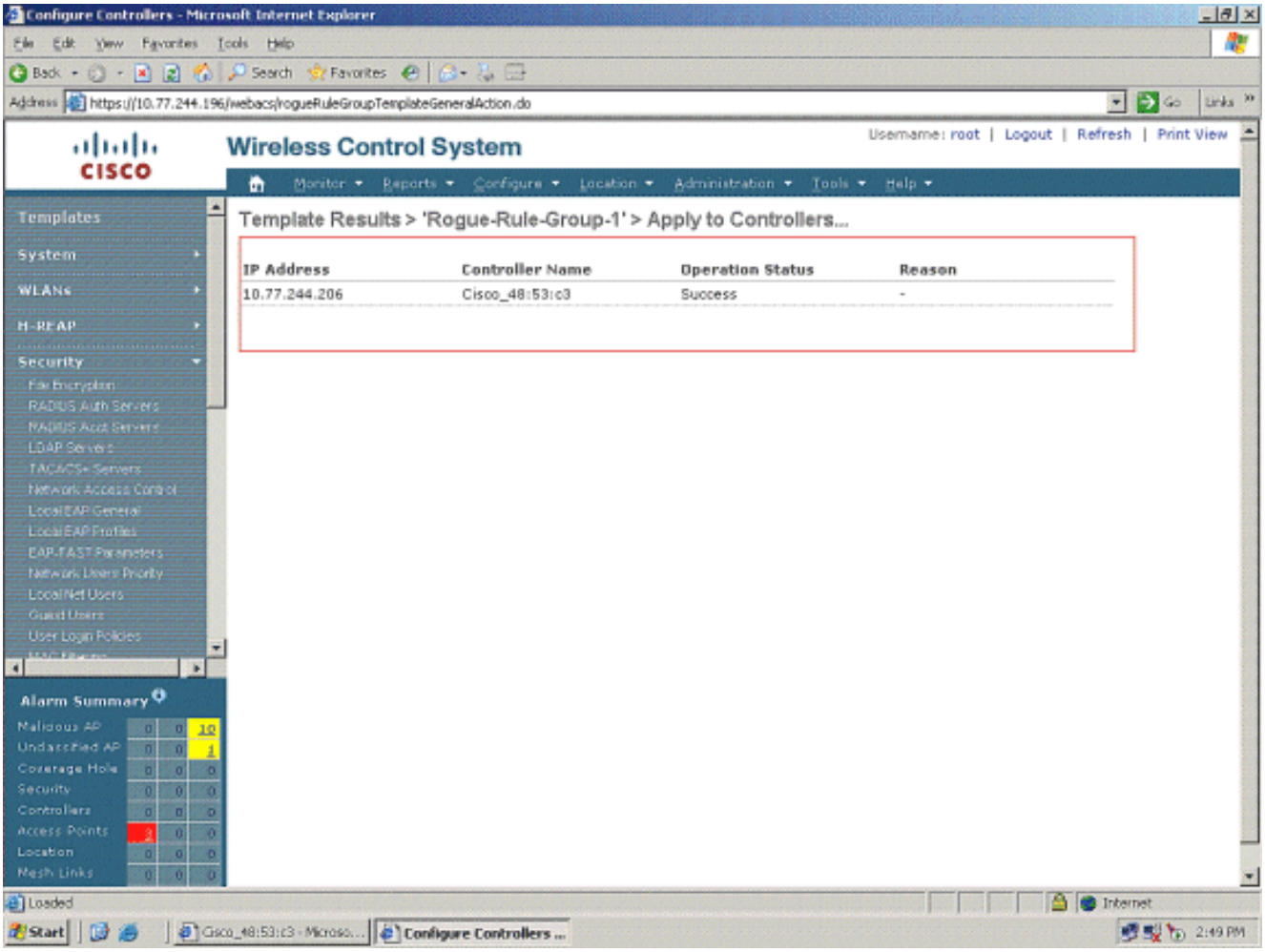
8. Как только вы сохраняете группу правила, она может быть применена к контроллерам. Для применения группы правила к контроллеру отредактируйте группу правила. Нажмите имя группы
правила.



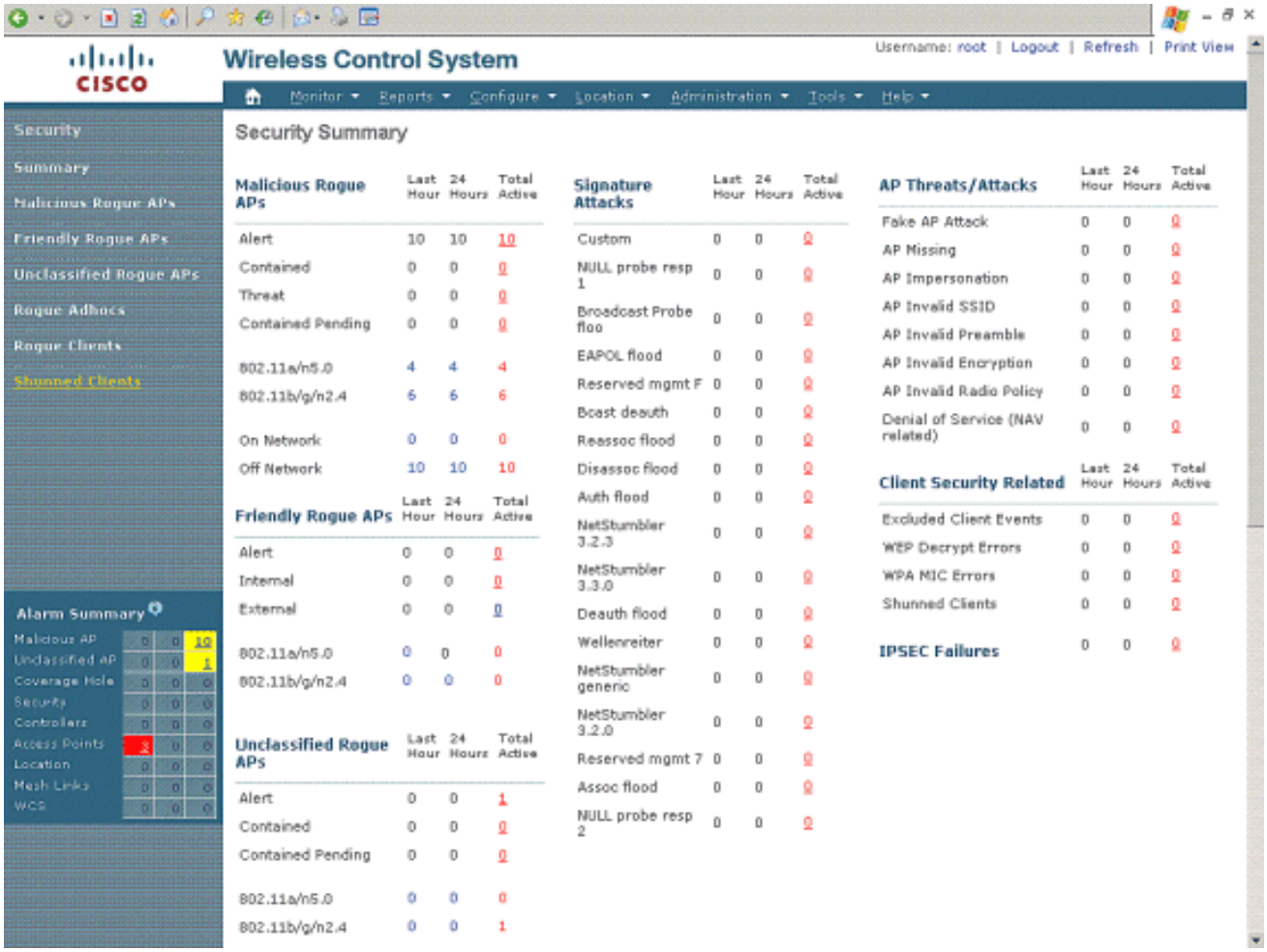
Нажмите **Apply to Controllers**. На следующей странице выберите контроллеры, к которым применено это правило. Ниже представлен пример.



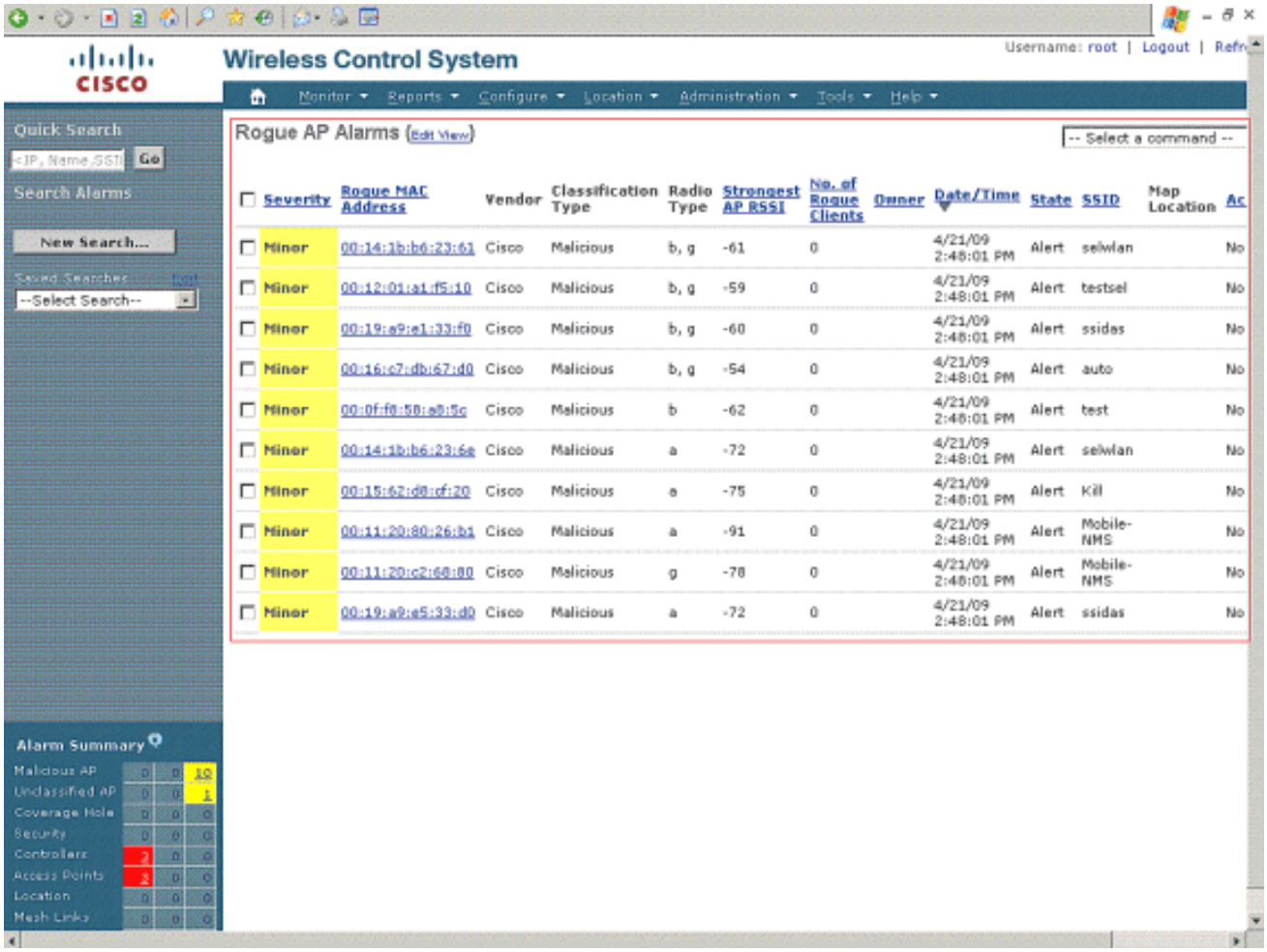
9. Как только правила применены к контроллерам, вы видите **Сообщение об успешном завершении** на
WCS.



10. Детали о классифицированных AP могут посмотреться на **Сводной странице Безопасности**. Ниже представлен пример.



11. Детали о классифицированных AP, в частности Злонамеренных, Дружественных, и Несекретных AP, могут посмотреться при нажатии соответствующей классификации от Сводной страницы Безопасности. Это - пример для Злонамеренных AP.



Дополнительные сведения

- Обнаружение несанкционированных точек доступа в Unified Wireless Networks
- Cisco Systems – техническая поддержка и документация