# Руководство по Cisco Security Agent 4.5

Перевод: Денис Батранков (декабрь 2004 года)

## *Введение в Cisco Security Agent*

Cisco Security Agent (далее CSA) это система предотвращения атак на уровне хоста. Эта технология ведет свою историю от систем **обнаружения** атак, которые лишь пассивно обнаруживали атаки и сигнализировали об этом. Основным недостатком этих систем было то, что они использовали сигнатуры атак, которые нужно было постоянно обновлять с появлением новых видов атак. То есть как только мы прекращали обновлять сигнатуры, то сразу обнаруживалось множество атак, которые эти системы не были способны обнаруживать.
Системы **предотвращения** атак работают совершенно по другому. Они активно отслеживают поведение приложений, код исполняемый на машине, локальные сетевые соединения на машине и выявляют аномалии в их работе, чтобы определить следуют ли разрешать эту активность. Очевидным преимуществом аномальных систем предотвращения атак является то, что им не требуются сигнатуры атак.

## *Возможности CSA*

После инсталляции на конечную систему CSA начинает следить за ресурсами системы и составлять таблицы с информацией обо всем том, что происходит в системе, с целью проследить за тем, чтобы заданные заранее правила поведения этой системы не нарушались. Агент следит за использованием и доступом к файлам и приложениям, сетевыми транзакциями, доступом к реестру, использованием ядра, доступом к COM объектам и другим компонентам системы, чтобы гарантировать четкую работу системы согласно заданным правилам.
Благодаря таким глубоким знаниям о всем том, что происходит в системе в реальном времени CSA может контролировать то, нужно ли разрешать затребованные действия или запрещать. Это происходит, когда некоторые действия производятся пользователем, либо злонамеренный код пытается выполниться сам. Когда CSA обнаруживает, что запрос не может быть разрешен в соответствии с локальной политикой безопасности, то агент блокирует это действие и посылает сообщение о неверном поведении системы.
Располагаясь глубоко в системе и непосредственно контролируя ее и любое ее поведение, агент выполняет множество ролей предотвращая как известные, так и неизвестные атаки, включая следующие функции:

- Глобальная автоматическая корреляция событий и реагирование.
- Распределенное управление экранированием хостов.
- Контроль приложений.
- Защита файлов и директорий.
- Контроль доступа к сети.
- Исследование распространения приложений и их поведения.

## *Структура CSA*

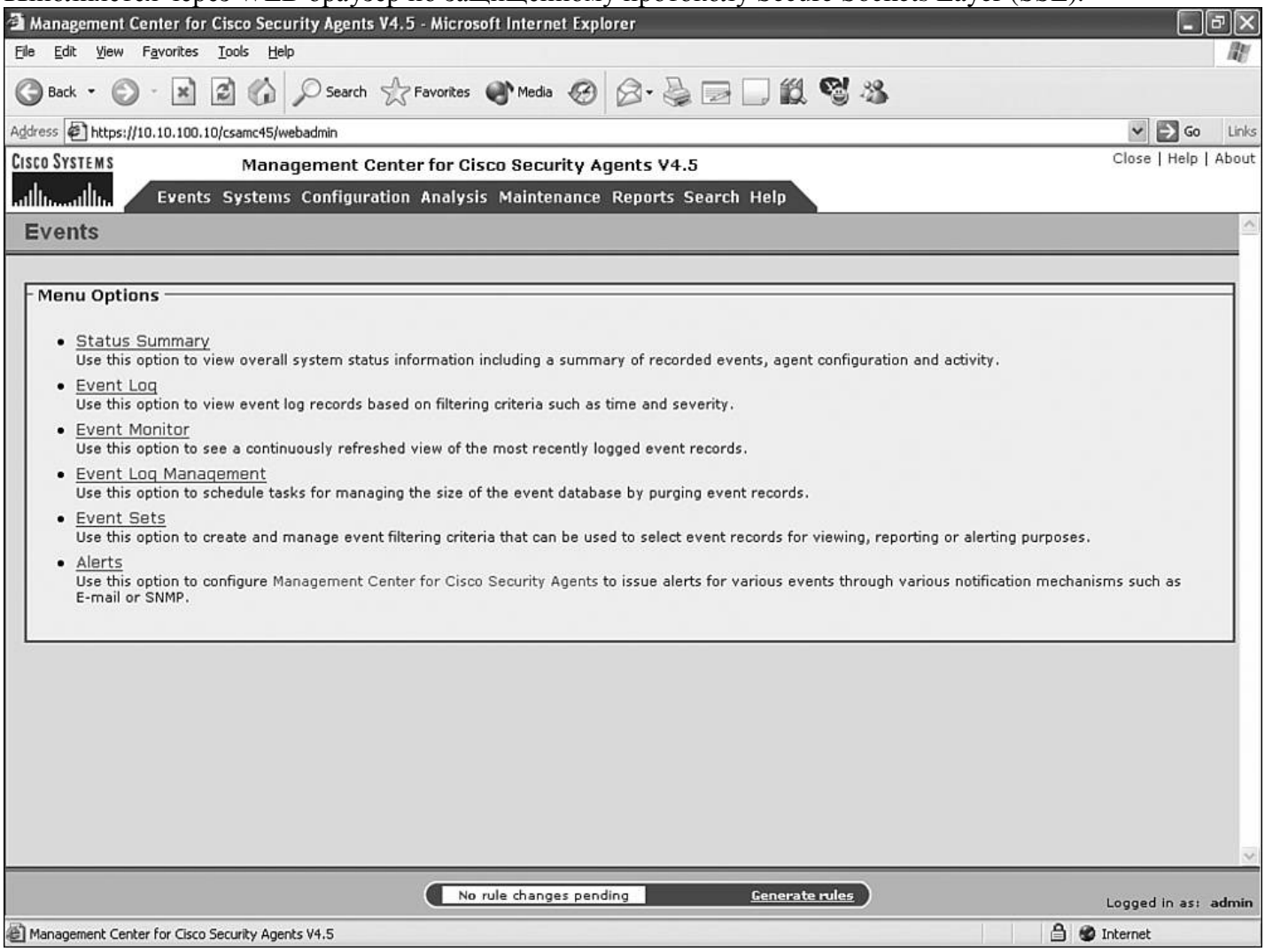
CSA состоит из двух основных частей

- Центр управления (Management Center)
- Агенты (Agents)

### Центр управления (Management Center)

Management Center (далее MC) выполняет такие важные задачи как настройка агентов, настройка политик и правил, централизованный сбор отчетов. Для ее работы требуется Windows 2000 Server. В качестве базы данных используется Microsoft Database Engine (MSDE) либо Microsoft SQL 2000 если планируется использовать более 500 агентов. Все функции по управлению агентами осуществляются через консоль управления. Консоль управления является частью Cisco Works VPN Management

Solution (VMS) и выглядит также как и другие утилиты управления от фирмы Cisco. Конфигурация выполняется через WEB браузер по защищенному протоколу Secure Sockets Layer (SSL).



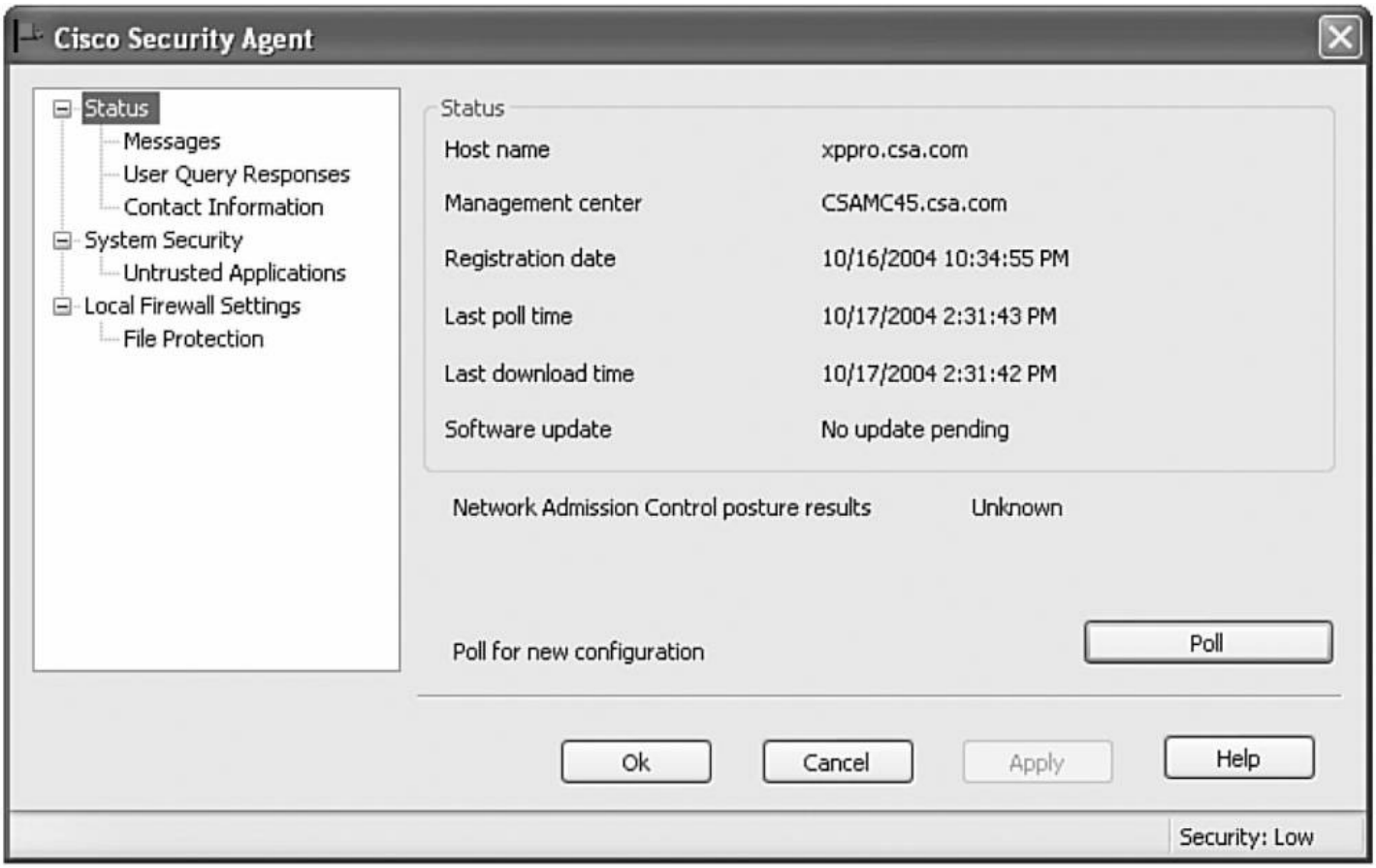

Также важными составными компонентами Management Center являются просмотр событий и создание отчетов.

## Агенты

Агент это программа, которая инсталлируется на конечную систему. Версия 4.5 поддерживает следующие операционные системы:

- Microsoft Windows NT
- Microsoft Windows 2000
- Microsoft Windows 2003
- Microsoft Windows XP
- Solaris 8
- Linux RedHat Enterprise v3.0

Агент контролирует локальную политику безопасности и защищает локальные ресурсы от компрометации. Как только агент обнаруживает нарушение, он сразу же посылает сообщение консоли управления для централизованного просмотра событий и создания отчетов. В определенные интервалы времени агент запрашивает центр управления об изменениях политики безопасности. Вот так выглядит интерфейс агента:




## *Взаимодействие компонентов CSA*

CSA устанавливается на рабочие станции и сервера непосредственно имеющиеся в сети, а MC устанавливается в защищенном сегменте сети из которого вы осуществляете управление сетью. Вы должны понимать, какие взаимодействия происходят между MC и агентами. Всего два информационных потока может быть связано с работой MC и агентов:

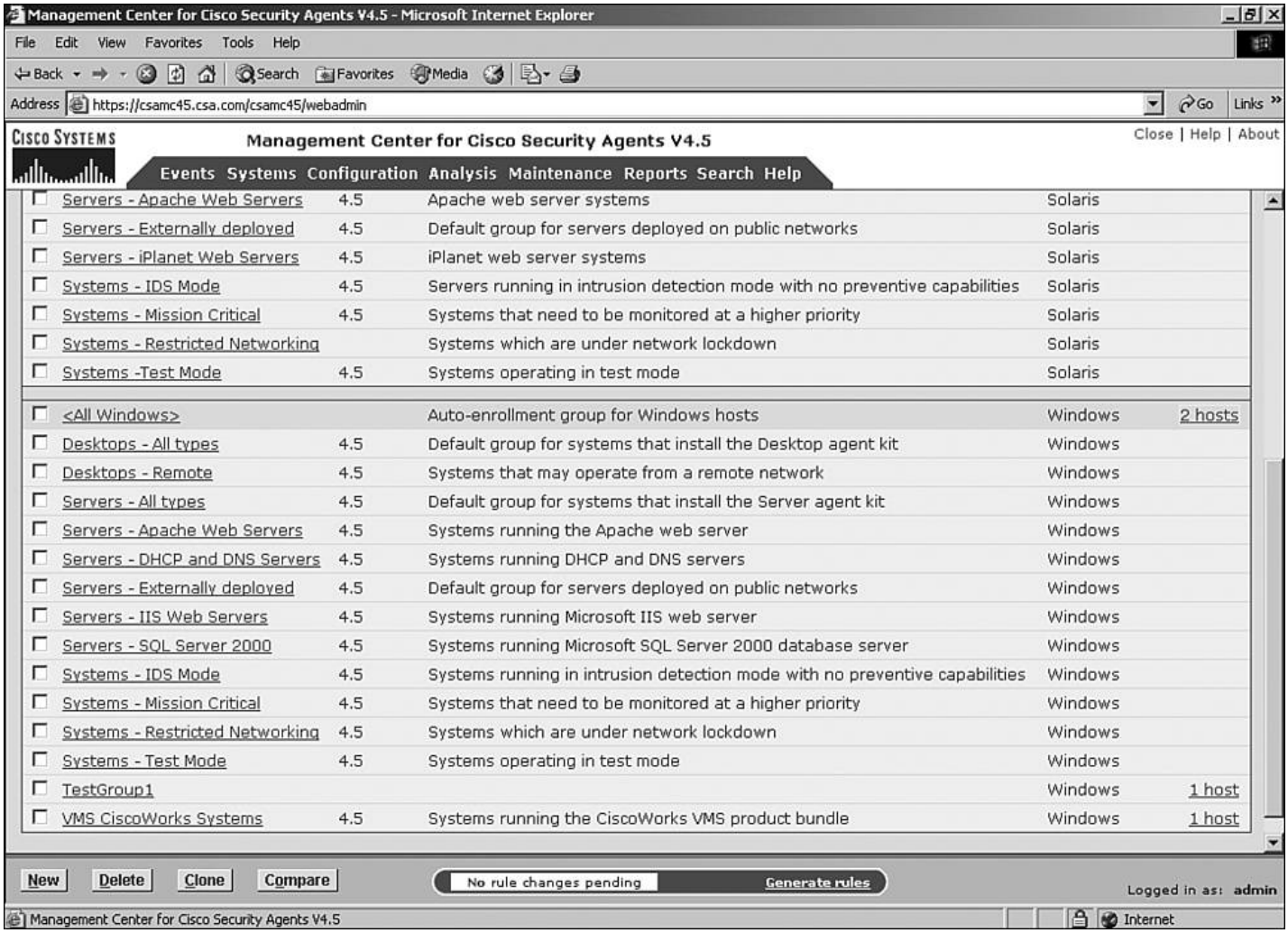
- Управляющее соединение от компьютера администратора до центра управления
- Информационное соединение между центром управления и агентами.

Управляющие соединение идет с компьютера администратора внутри защищенного туннеля SSL на TCP порты 1741 и 1742 центра управления. Обычно используется локально сгенерированный на CiscoWorks сертификат, но вы можете импортировать сертификат из имеющейся текущей Public Key Infrastructure (PKI).
Информационное соединение между MC и агентом происходит тоже по SSL на стандартный порт 443 либо TCP/5401. Большие транзакции осуществляются по протоколу HTTP (TCP/80). Эти большие объемы данных ни что иное, как инсталляционные модули агентов и обновления политик.

CSA содержит большое число компонент, которые вы должны знать, чтобы эффективно пользоваться продуктом.

## *Группы и хосты*

Хост – компьютер который вы защищаете устанавливая на него агента. Хост должен состоять как минимум в одной группе. Если хост принадлежит к нескольким группам, то вы должны понимать как вместе состыковываются правила из разных групп, учитывая их приоритет.
Группы – логическое объединение хостов базирующееся на их некоторых одинаковых свойствах. Есть обязательные группы: Windows, Solaris, Linux. Существуют некоторые предопределенные в CSA группы, например некоторые видны на скриншоте:

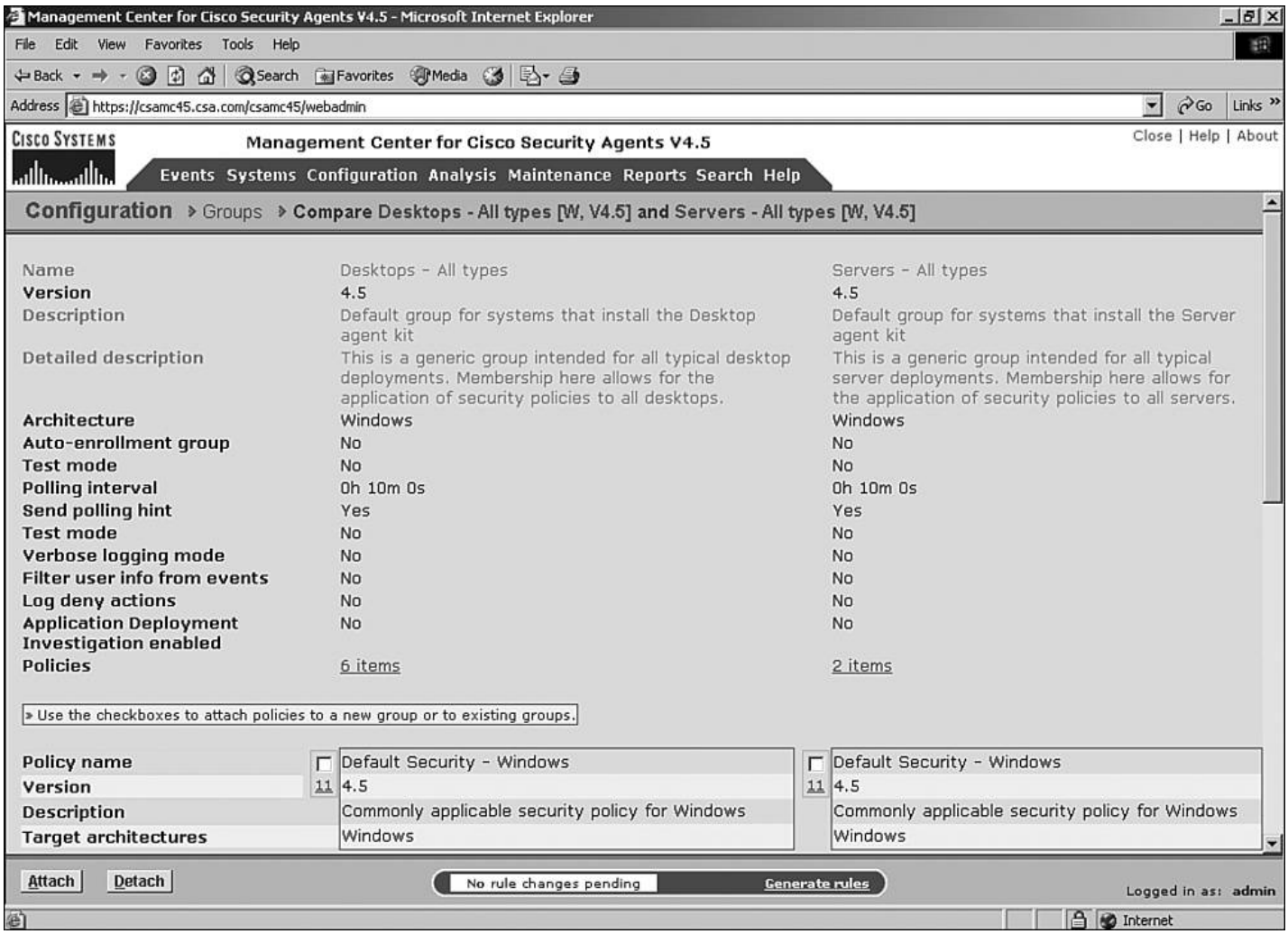



И наконец вы можете создавать свои собственные группы. Типичными примерами группировки хостов являются: наличие одинаковых функций или приложений, отношение к одному отделу организации, физическое или географическое расположение, критичность ресурса для бизнеса.

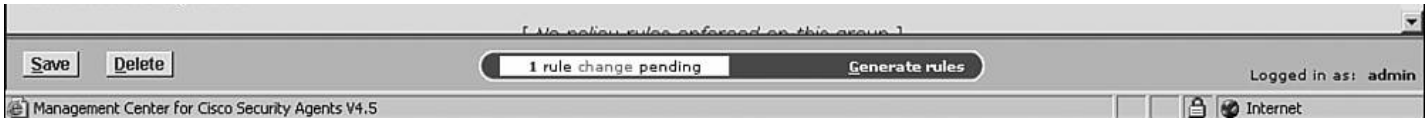
Группами удобно пользоваться для составления отчетов, выделяя хосты из общей массы по какому-либо критерию.

## Просмотр групп

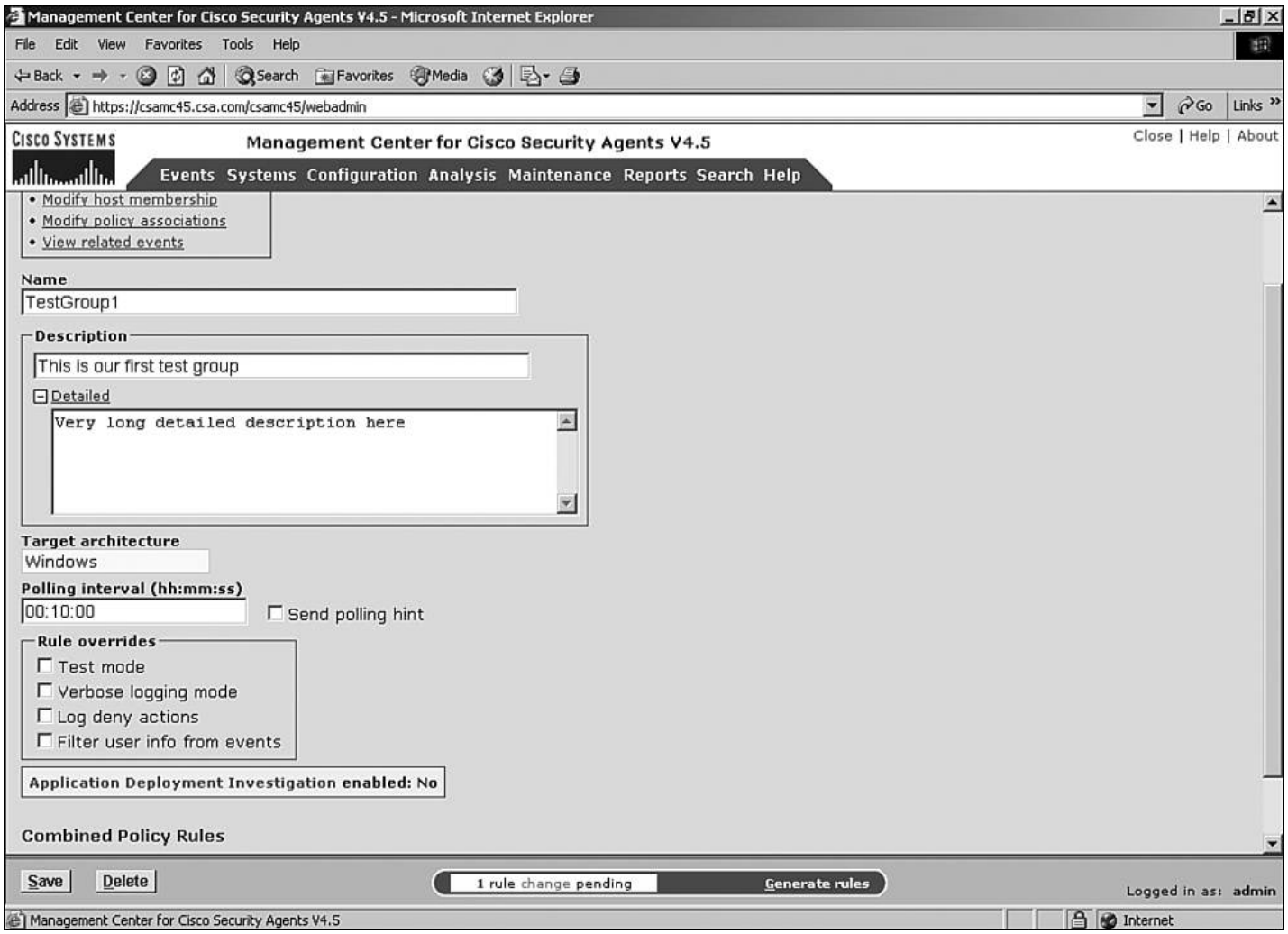
В меню **Systems > Group** вы увидите уже имеющиеся группы. Вы можете удалять и создавать группы. Создание осуществляется кнопками **New** и **Clone**. Новая группа создаваемая через **Clone** будет наследовать все настройки конфигурации от которой она клонирована, что удобно для создания и тестирования групп, которые лишь слегка отличаются от базовых. Полезная функция сравнения групп выполняется кнопкой **Compare**. Вы можете сравнить две группы по используемым политикам, интервалам опросов, архитектурам и описаниям и др.




Нужно помнить, что после того как вы закончили изменять конфигурации в MC, то для того чтобы изменения дошли до агентов на конечных хостах нужно нажать ссылку **Generate Rules** внизу страницы:




Когда вы создаете новую группу, то у вас есть целый набор опций:




По умолчанию интервал опроса центра управления агентом стоит 10 минут. Каждые 10 минут агент соединяется с MC чтобы узнать были ли изменения конфигурации. Вы можете поставить галочку **Send Polling Hint**, чтобы заставить MC посылать подписанные UDP пакеты на последний известный адрес агента, содержащий информацию о том, что конфигурация изменилась. Эту опцию есть смысл использовать если вы выбираете достаточно большой интервал опроса, но хотите ускорить обновление конфигураций.

Рассмотрим остальные опции:

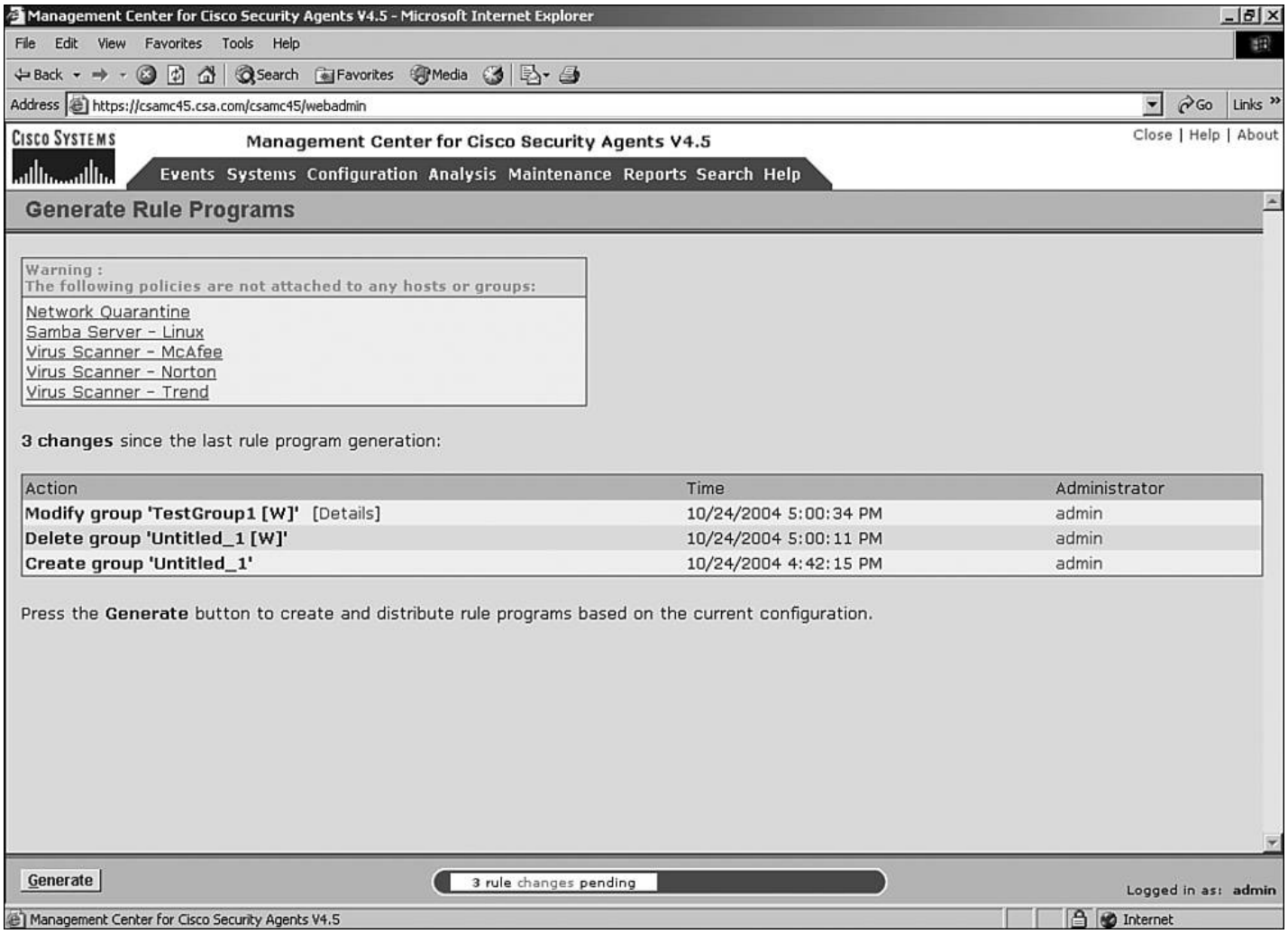
- **Test Mode** – означает что агенты внутри этой группы только сообщают MC о том какие бы действия они предприняли согласно текущей политике безопасности, но сами действия в тестовом режиме не выполняются. Эта опция полезна на реально работающих системах при начальной инсталляции агента. Администратор имеет возможность отследить конфликты которые могу возникнуть после применения политики и подправить конфигурацию.
- **Verbose Logging Mode** – заставляет агента сообщать о каждом событии, тогда как без этой опции одинаковые события будут группироваться и посылаться только одно сообщение.
- **Log Deny Actions** – заставляет логировать все запрещающие события, несмотря на то что в самом правиле может не стоять опция логирования этого события.
- **Filter User Info from Events** – предотвращает показ личных данных в логах CSA. Эта опция полезна когда у вас в политике заложены ограничения на сбор личной информации.

В дополнение к параметрам группы вы имеете возможность перейти по ссылкам для просмотра различной информации:

- **Modify Host Membership** — Ссылаются на страницу которая показывает какие хосты входят в эту группу и позволяет вам добавлять новые хосты.

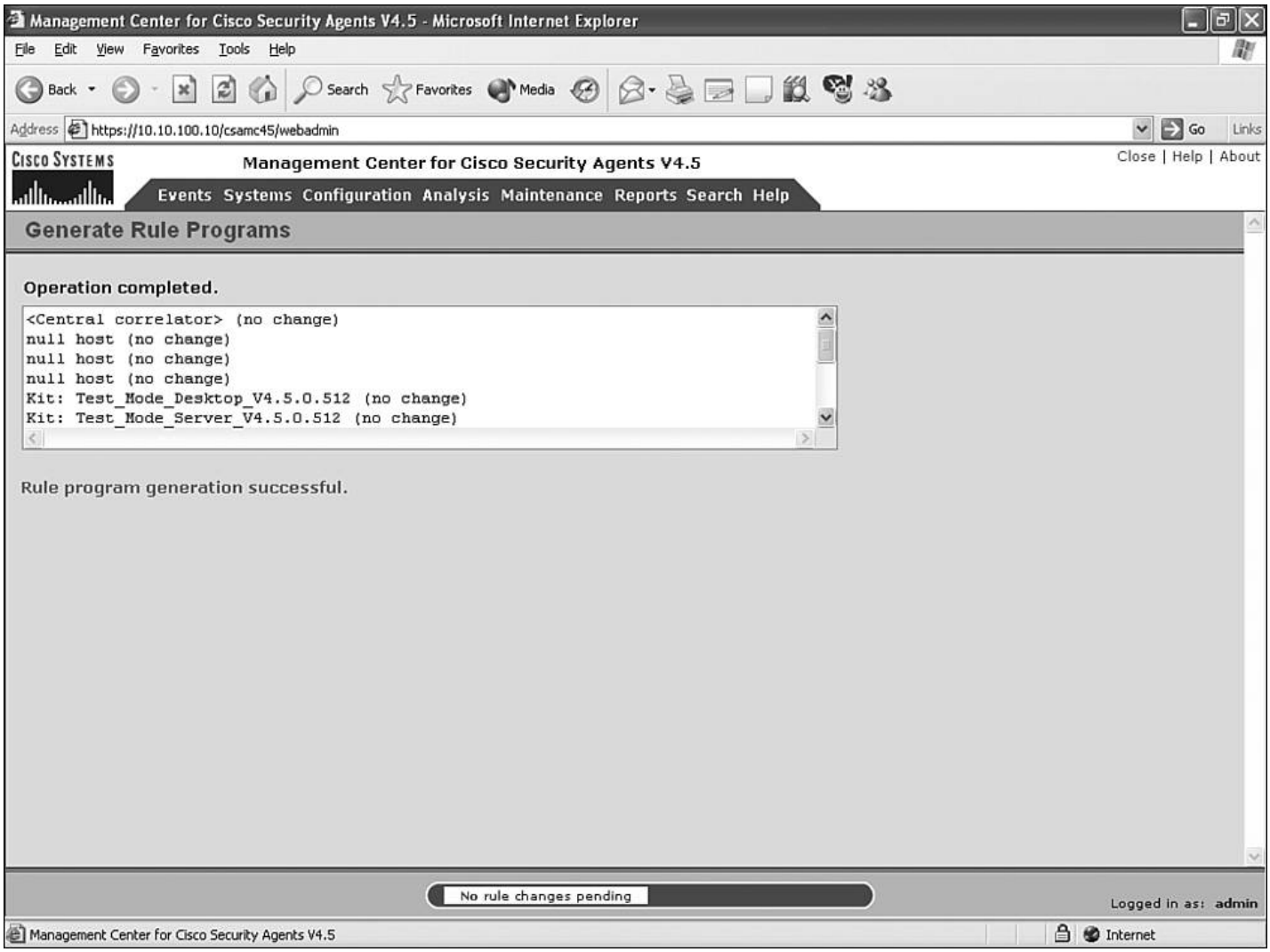
- **Modify Policy Associations** — приводит вас на страницу где вы можете выбрать политику связанную с этой группой и таким образом распределяемую по всем хостам группы.
- **View Related Events** — ссылается на страницу где показаны отфильтрованные события связанные только с хостами из этой группы.

Окончательным шагом создания или модификации группы является нажатие на **Generate Rules** внизу страницы. После нажатия на эту ссылку вы увидите список изменений который нужно сделать и кнопку **Generate** как видно на скриншоте:



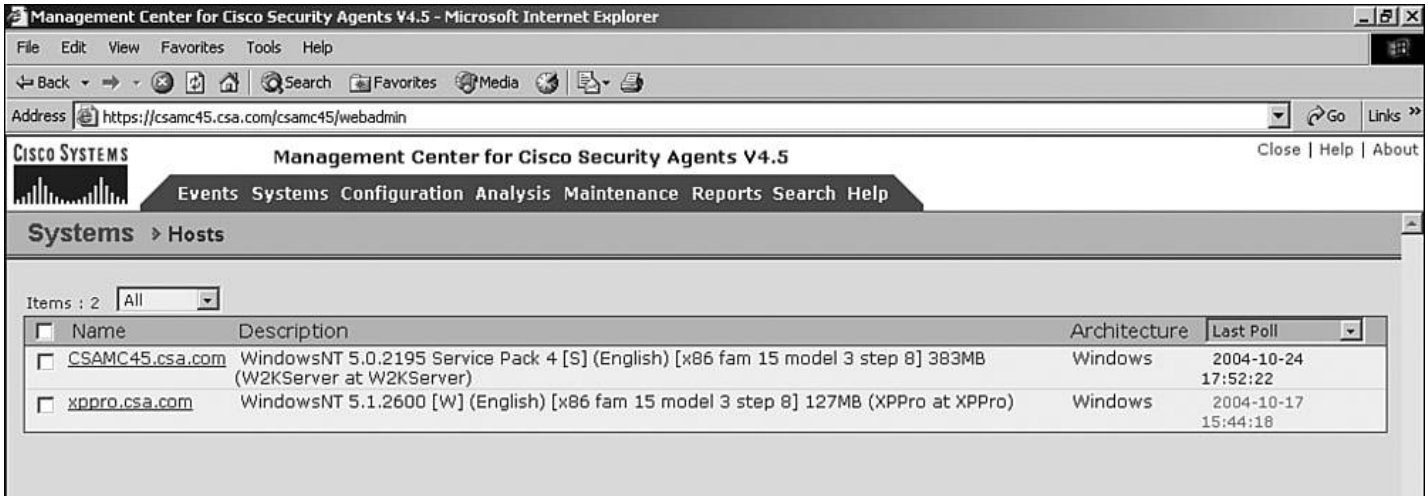

Также вы видите что некоторые опции имеют ссылки Details, на которые вы можете нажать чтобы посмотреть какие конкретные изменения будут сделаны.

После нажатия кнопки Generate все изменения будут применены и результат появится на экране:




## Просмотр хостов

Просмотр всех зарегистрированных в хостов осуществляется в меню **Systems > Hosts**.




Вы можете фильтровать выводимый список хостов по следующим критериям:

- **Active** – хосты которые были активны во время последнего опроса.
- **Protected** – хосты которые имеют политики связанные с группами в которых хосты находятся.
- **Latest Software** – хосты которые не нуждаются в обновлениях агента.
- **Test Mode** – хосты работающие в тестовом режиме.

- **Last Poll** – сортировать хосты по времени последнего опроса.

Информация о хосте содержит основные параметры хоста: имя, описание, операционная система, сервис пак, процессор, память.

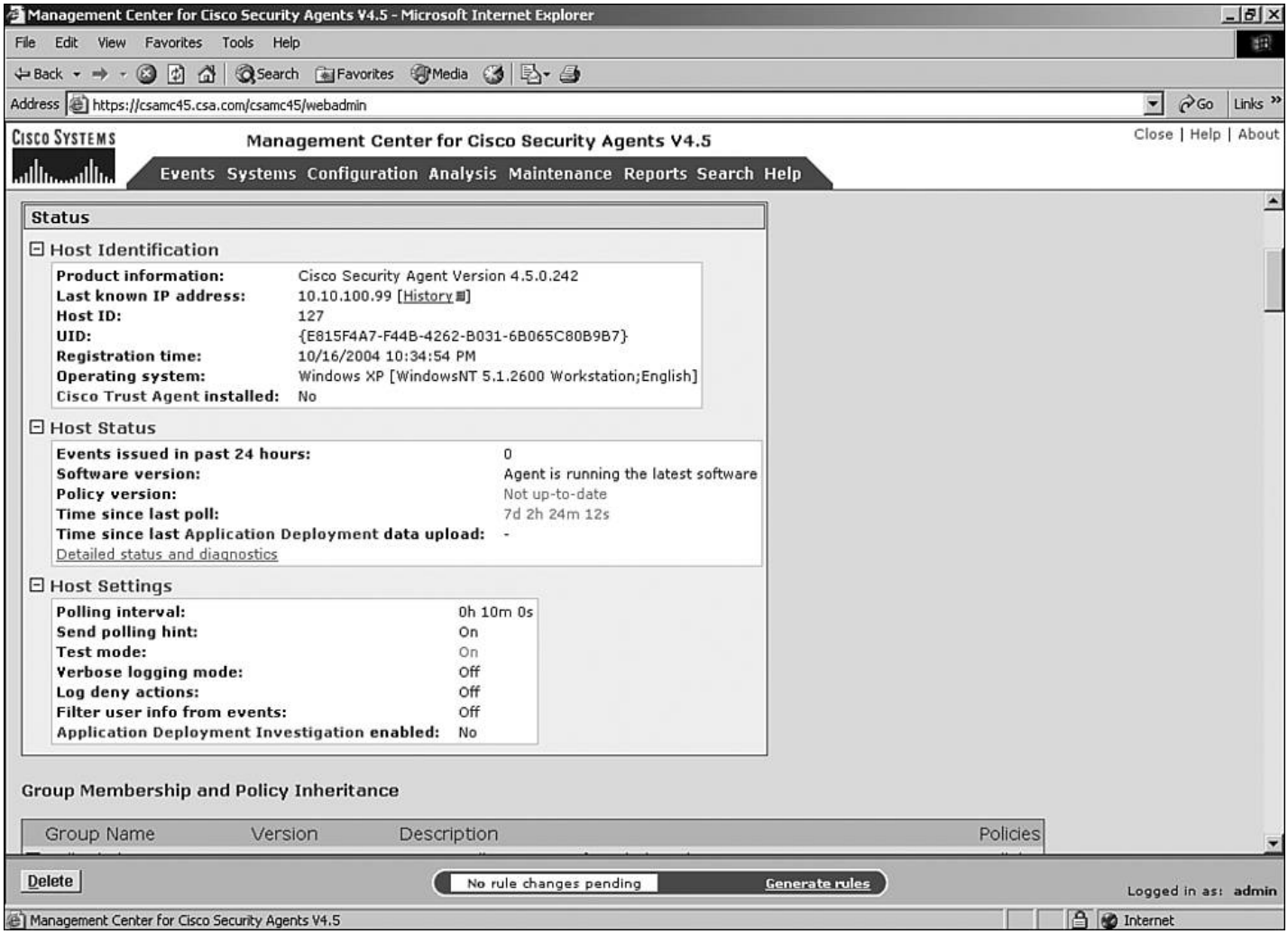
Вы можете удалить хост из списка. Таким образом вы освобождаете одну лицензию.

## Тестовый режим

Тестовый режим работы агента на хосте необходим в случае начальной инсталляции агента, при настройке политики или для разрешения возникших конфликтов и проблем на хосте. Работая в этом режиме агент перестает вмешиваться в работу системы а лишь отслеживает ее состояние и логирует те действия, которые бы он делал, если бы работал в режиме защиты хоста.

## Работа с хостами

Нажимая мышкой на хост, вы переходите на страницу которая дает подробную информацию о хосте:




- **Host Identification**— Здесь вы видите подробные сведения:
  - **Product Information**— версия CSA.
  - **Last Known IP Address (and History)** — последний IP адрес с которого агент запрашивал информацию. Все изменения IP адресов, включая время начала и окончания использования IP возможно просмотреть кликнув на ссылку **History**.
  - **Host ID**— идентификатор ассоциированный с хостом во время регистрации, необходимый для идентификации хоста внутри базы данных CSA MC.

    - **UID**— идентификатор связанный с используемым агентом во время инсталляции.
    - **Registration Time**— Начальная дата регистрации.
    - **Operating System**— Заявленная версия операционной системы.
    - **Cisco Trust Agent Installed**— информация о том инсталлирован ли Cisco Trust и если инсталлирован, то его состояние. Эта опция часть Cisco Self-Defending Network Initiative или более точно Network Admission Control (NAC).
- **Host Status**— From here, you obtain information regarding the current operational status of the agent, such as the following:
    - **Events Issued in the Past 24 Hours**— ссылка ведущая на страницу где показаны все события связанные с этим хостом за последние сутки.
    - **Software Version**— текущая версия агента.
    - **Policy Version**— текущая версия политики.
    - **Time Since Last Poll** — время прошедшее с момента последнего запроса от агента.
    - **Time Since Last Application Deployment Data Upload**— если задача по развертыванию приложений была запущена для этого агента, то информация с момента последней загрузки будет выведена.
    - **Detailed Status and Diagnostics Link**— эта опция позволяет вам получить текущую информацию о конечной системе, включая IP адрес, текущую или старую политику, запросив агента немедленно предоставить эту информацию. Вы также можете очистить кэш на удаленном хосте прямо с этого экрана и сбросить агента назад на настройки по умолчанию без физического доступа к устройству.
- **Host Settings**— дает возможность посмотреть на некоторые параметры конфигурации агента. Большинство опций настраиваются в группах членами которых является этот хост, но здесь вы может хорошо увидеть как хост справляется с конфликтом политик которые содержатся в разных группах. Вот что выводится в этой ветке:
    - **Polling Interval**— Интервал опроса центра управления агентом.
    - **Send Poll Hint**— включены ли UDP сообщения для этого хоста.
    - **Test Mode**— показывает находится ли агент в тестовом режиме.
    - **Verbose Logging Mode**— уменьшает ли хост количество одинаковых сообщений.
    - **Log Deny Actions**— посылает ли хост информацию о всех блокирующих операциях или только о тех что явно заданы в правилах на логирование.
    - **Filter User Info from Events**— фильтрует ли хост личную информацию в логах.
    - **Application Deployment Investigation Enabled**— показывает запущен ли процесс исследования действий программ.

## *Политики, модули и правила CSA*

Политики, модули и правила это механизмы которые служат для выполнения политики безопасности записанной на бумаге. На самом нижнем уровне этих трех компонентов лежат правила. Одно правило – это компонент который отвечает за конкретное действие в системе. После того как создано несколько таких правил их комбинируют в модули. Модули правил – набор правил, собранных вместе, чтобы служить специальной цели. Эти модули правил затем группируются в политику.

Например вы можете построить политику которая будет защищать директорию и файлы в ней от изменения и уничтожения. Эта политика возможно будет включать три модуля выполняющих эту функцию но специфических для трех разных операционных систем. То есть вы в частности будете иметь набор правил защищающих файловую систему Solaris сгруппированный в модуль защиты файловой системы Solaris.

## *Множества состояний*

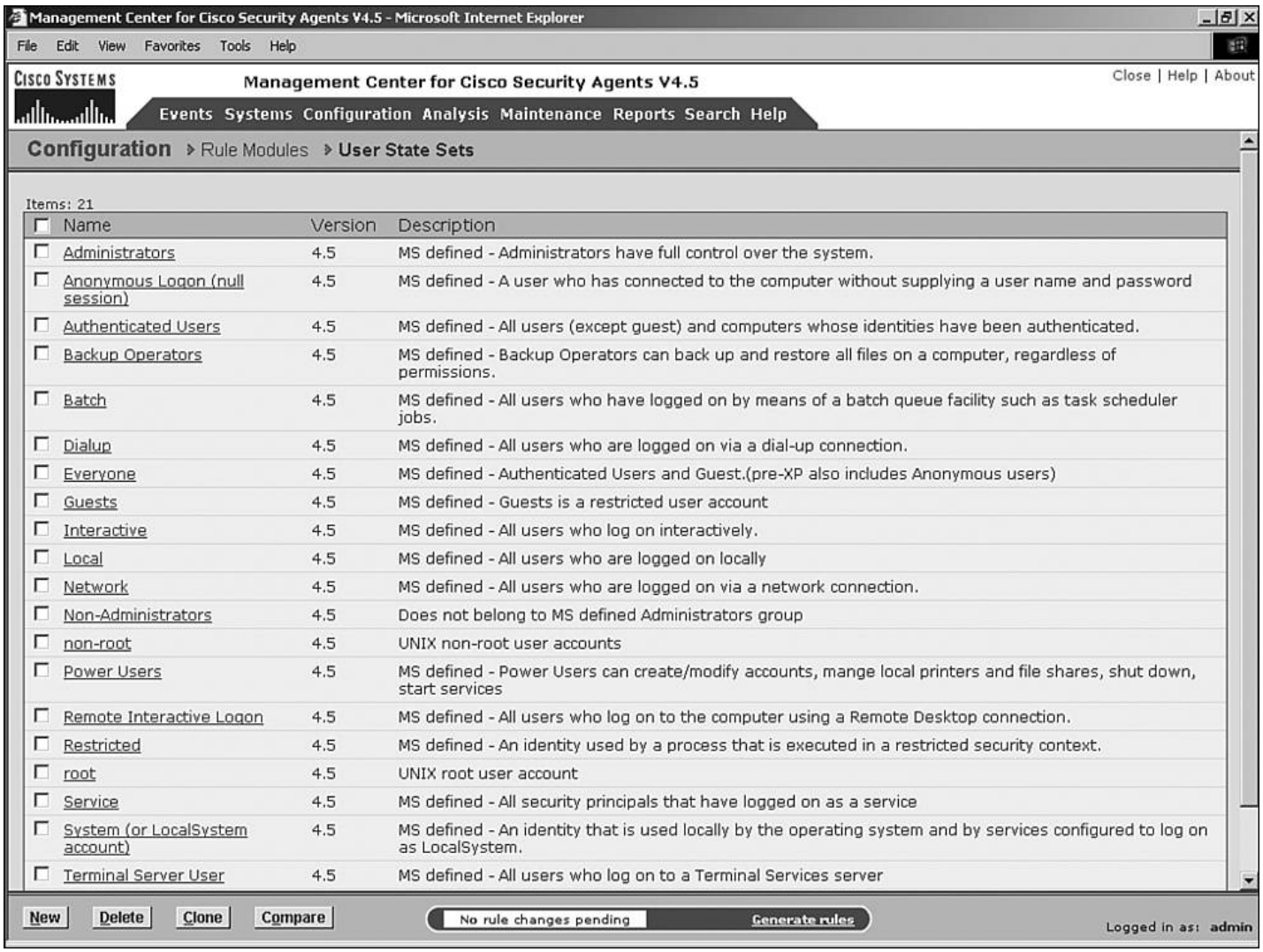
Множества состояний (State Sets) это новая концепция появившаяся в версии 4.5. Эта новая возможность позволяет вам задать правила которые могу быть установлены на агентах во время нормального процесса обновления на них конфигурации. Эти правила остаются неактивными до тех

пор пока не выполнится заложенный в них критерий срабатывания. Есть два типа таких множеств: состояние пользователя и состояние системы. Каждый тип состояний позволяет вам задать политики, которые начинают работать, как только пользователь вошел в локальную систему или в зависимости от расположения компьютера в данный момент времени.

## Пользовательские множества состояний

Пользовательские множества состояний обеспечивают механизм наложения политик, зависящий от того, какой пользователь вошел в систему. Это замечательный способ обеспечить обычным пользователям ограниченный набор средств управления системой и сетевой доступ и позволить администраторам использовать все средства управления и сетевого доступа. Например, если вы можете настроить политику, которая бы запрещала пользователям останавливать агента на локальной машине, но разрешала это делать пользователям, входящим в группу администраторов. Однако, несмотря на то что этот метод видится как очень полезный, нужно использовать его только по необходимости, поскольку он увеличивает размер политики передаваемой к и от защищаемой системе и увеличивает время необходимое для проверки условий.

Конфигурация пользовательских множеств состояний производится в меню Configuration > User State Sets




Если вы определяете новые множества состояний, то вы можете использовать для Windows идентификаторы пользователей SID, чтобы не зависеть от того как имя пользователя пишется в зависимости от используемого в системе языка.

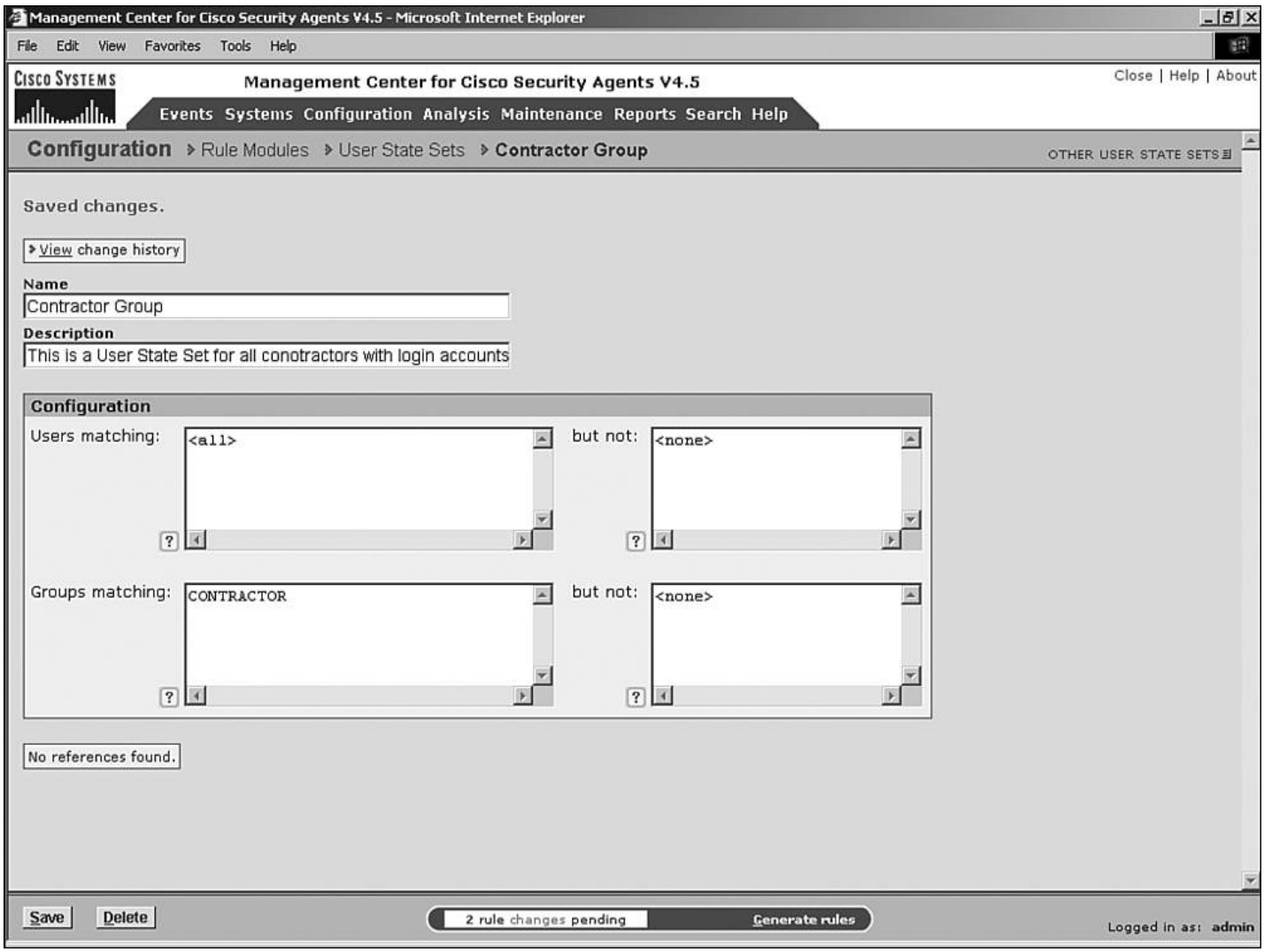
Рассмотрим несколько предопределенных множеств состояний:

- **Administrators**— Это множество показывает пользователей в группе администраторов заданной SID S-1-5-32-544 а не именем группы (что будет верно вне зависимости от языка в системе).
- **Anonymous Login (Null Session)** — Содержит нулевые сессии используя соответствующий SID.
- **Dialup**— содержит всех пользователей получивших доступ в систему по Dialup
- **Root**— Содержит список пользователей root из UNIX.
- **Service** — Содержит компоненты которые зарегистрировались в системе как сервис по SID.

Чтобы задать новое множество нажмите New. Откроется окно конфигурации, в котором нужно проделать несколько простых шагов.

- **Name and Description** — Имя и описание по желанию.
- **Configuration**— несколько параметров чтобы это множество отличалось от других:
  - **Users Matching**— введите имя пользователя, по умолчанию введены все пользователи. Вы можете использовать поле **but not**, чтобы исключить некоторых пользователей из множества по имени.
  - **Groups Matching** — введите имя или несколько имен групп соответствующих этому множеству. Вы можете использовать поле **but not**, чтобы исключить некоторые группы.
- **References Link** — Если какие-то правила используют это множество, то вы можете сразу перейти к ним нажав на эту ссылку.
- **Save and Delete** — запишите или удалите изменения.

Как пример посмотрите на рисунок:



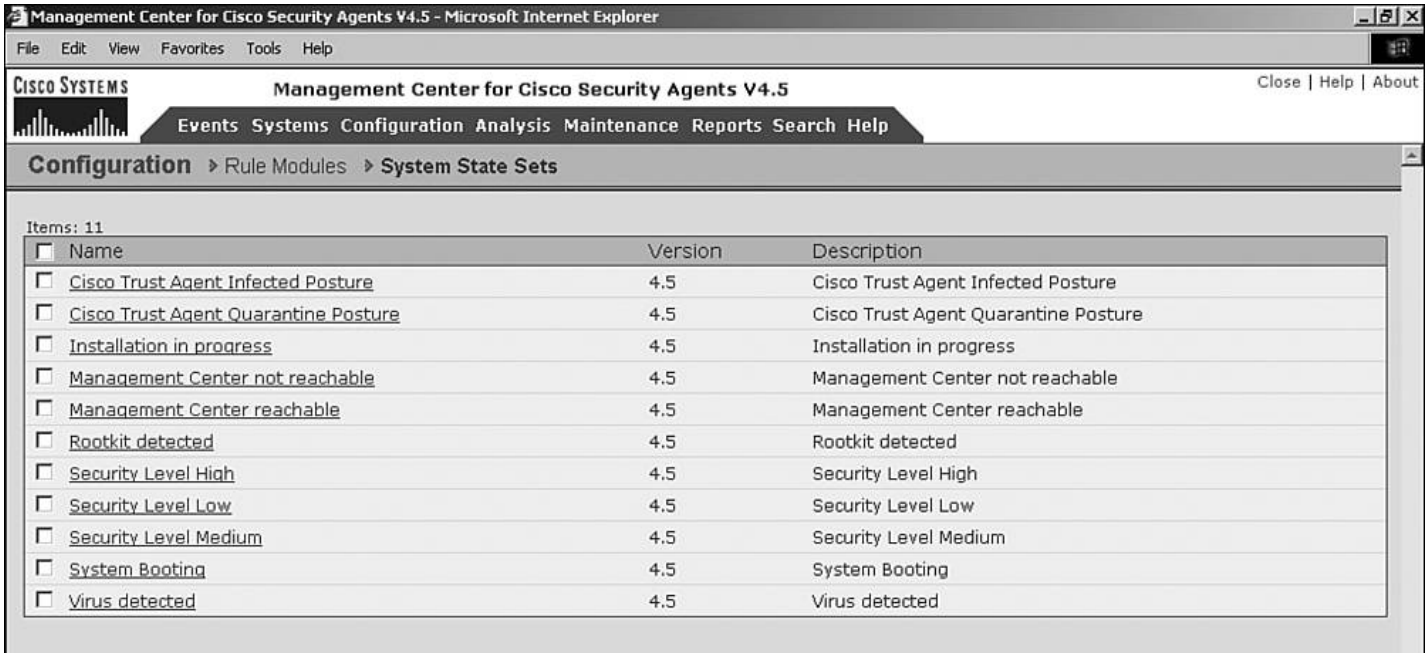
Заметьте что звездочка (*) разрешена в поле User, но не в поле Group

## Множества состояний системы

Множества состояний системы – это механизм, накладывающий различные уровни политики в модуле правил в соответствии с текущим состоянием системы. Параметрами состояния являются:

- Состояние Network Admission Control (NAC)
- Уровень безопасности системы
- IP адрес или подсеть
- DNS суффикс
- Загружается ли в настоящий момент система
- Идет ли инсталляция софта
- Доступен ли CSA MC сервер
- Найден ли руткит в системе
- Найден ли вирус в системе

Вы может установить эти преопределенные факторы по одному или несколько сразу. Обычно ставят как минимум 2 параметра, чтобы ограничить возможность конечной системы исказить этот один параметр, например, такой как IP адрес и попытаться начать обходить настройки локальной базы правил. Некоторые правила уже предопределены и могут быть просмотрены в меню **Configuration > Rule Modules > System State Sets**.




Наиболее полезными являются следующие состояния

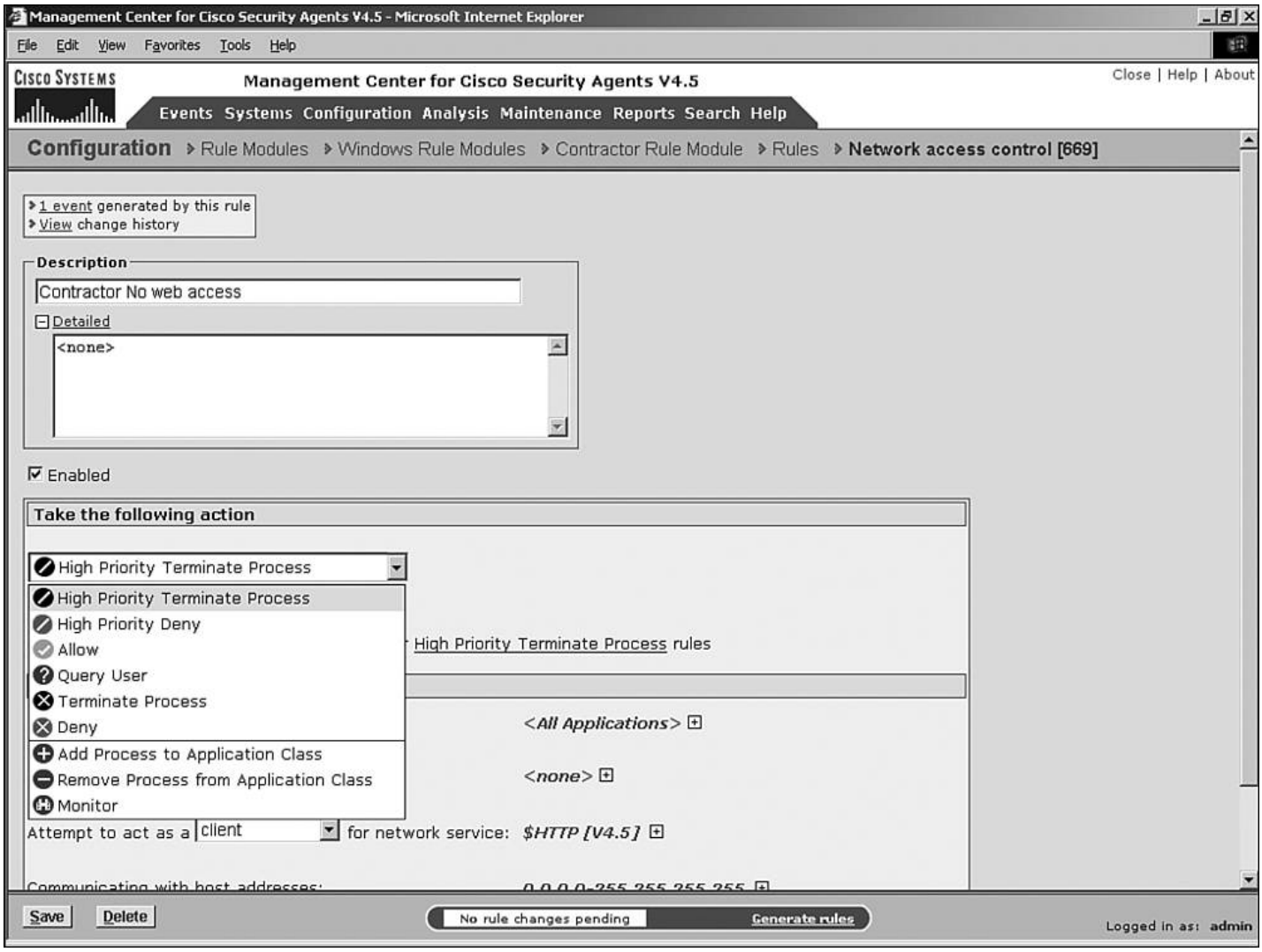
- **Cisco Trust Agent Infected Posture** — как критерий используется только Cisco Trust Agent Posture параметр. Если NAC posture, переданное CTA инфицировано, то вы можете применить правило к агенту.
- **Management Center Reachable** — критерием является доступность CSA MC сервера.
- **Security Level Low** — это случается когда выставлен уровень безопасности Low на агенте.
- **System Booting** — когда система загружается вы можете указать какие операции разрешены а какие нет.
- **Virus Detected** — если обнаружен вирус локальным антивирусом который поддерживает агент, то вы можете ужесточить политику на локальном хосте.

Они очень простые, но очень полезные. Чтобы создать собственное множество состояний нажмите кнопку **New** и установите параметры.

- **Name and Description**— Имя и описание нужные администраторам.
- **Network Admission Control**— Используйте опцию Cisco Trust Agent Posture внутри этого параметра. Варианты опций здесь **Don't Care**, **Healthy**, **Checkup**, **Quarantine**, **Infected**, **Unknown** или **Other**. **Don't Care** соответствует всем токенам. Чтобы выбрать несколько состояний, используйте кнопку Ctrl, нажимая левую кнопку мыши.
- **System Security**— используйте, чтобы выбрать какому положению движка безопасности в агенте соответствует данное множество. Значением по-умолчанию является Medium.
- **System Location**— варианты настройки здесь относятся к расположению, базирующемуся на знании IP адреса локального компьютера.
    - **Network Address Range**— Ввести значения соответствующие текущему адресу системы.
    - **DNS Suffix Matching**— Ввести DNS суффиксы которые система может использовать. Используйте поле **but not** чтобы ввести DNS суффиксы, которые надо исключить из этого множества.
- **Additional State Conditions** — Все следующие опции имеют варианты **Don t Care**, **Yes** и **No**:
    - **System Booting** — критерий того что система загружается.
    - **Installation Process Detected** — критерий того что инсталлируется программное обеспечение. Используется чтобы увеличить или уменьшить настройки безопасности в этот момент.
    - **Management Center Reachable** — как только сервер становится недоступен вы можете включить другие настройки безопасности.
    - **Rootkit Detected** — можно включить другие настройки если обнаружен руткит .
    - **Virus Detected** — если локальный антивирус сообщил о найденном вирусе вы можете ужесточить защиту компьютера.
- **References**— если состояния были использованы, то можно посмотреть где.
- **Save and Delete**— записать изменения или удалить.

## Какие действия выполняют правила

В случае наступления заданных условий, правила выполняют различные действия.




- **High Priority Terminate Process** — Отвергает действие или доступ к ресурсу и пытается завершить процесс делающий запрос. Завершение определенных системных процессов может сделать систему нестабильной, чтобы предотвратить это CSA пытается завершить в таких процессах только вызвавшую событие нитку.
- **Terminate Process** — Делает то же что и действие выше, но с меньшим приоритетом. Смотрите раздел о приоритетах.
- **High Priority Deny** — Отвергает доступ к ресурсу и не завершает процесс.
- **Deny** — То же что и high priority deny, но с меньшим приоритетом.
- **Allow** — Разрешает доступ к ресурсу.
- **Default Action (Allow)** — CSA отличается от многих продуктов тем, что разрешает все взаимодействия в системе по умолчанию, запрещая только действия специально указанные. Выбирайте эту опцию если вам нужно разрешить действие которое может быть запрещено в конфликтной ситуации между разными правилами.
- **Query User Default Terminate** — Спрашивает пользователя о том что делать, и если пользователь не отвечает в течение 5 минут или просто не может ответить то выбирается действие – **Terminate**.
- **Query User Default Deny** — Спрашивает пользователя и по умолчанию выбирает операцию – **Deny**.
- **Query User Default Allow** — Спрашивает пользователя и по умолчанию выбирает **Allow**.
- **Monitor** — логирует событие без каких либо других действий.
- **Add or Remove to/from Application Class** — базируясь на запросах к ресурсам вы можете добавить процесс в динамический класс приложений или удалить из этого класса.

Заметьте, что запросы типа Query не доступны в Solaris, поскольку в этой ОС пользователь не может интерактивно общаться с агентом. Там действия по умолчанию выполняются сразу.

### Разрешение конфликтов правил

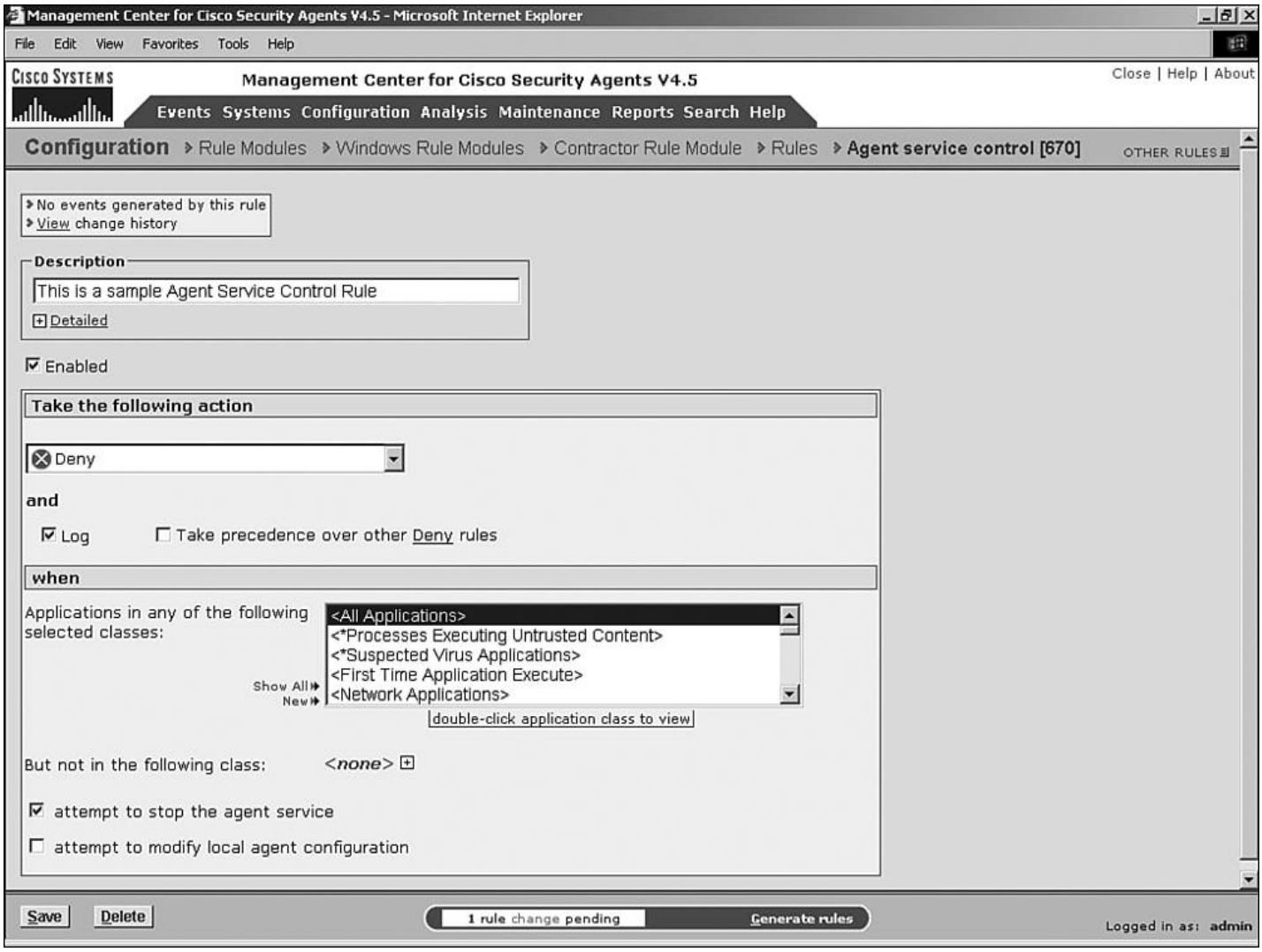
Когда правила конфликтуют, то существует приоритет выполнения правил. Верхнее приоритетней нижнего:

1. **High priority terminate process**
2. **High priority deny**
3. **Allow**
4. **Query user (terminate)**
5. **Query user (deny)**
6. **Query user (allow)**
7. **Terminate process**
8. **Deny**
9. **Default action allow**
10. **Add process to application class**
11. **Remove process from application class**
12. **Monitor**

## *Типы правил*

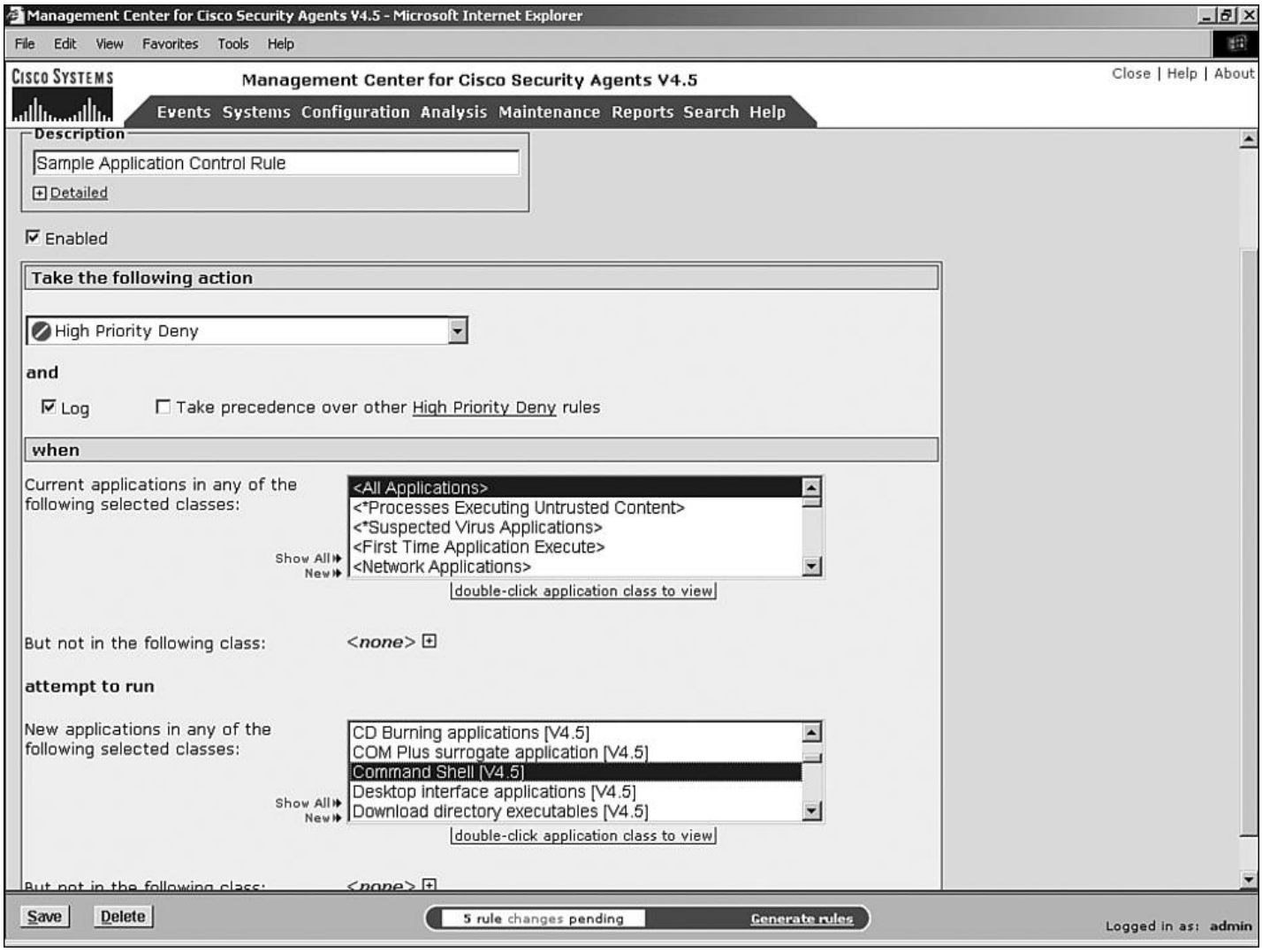
### Agent Service Control

Контролирует возможность остановить агента на локальной машине.



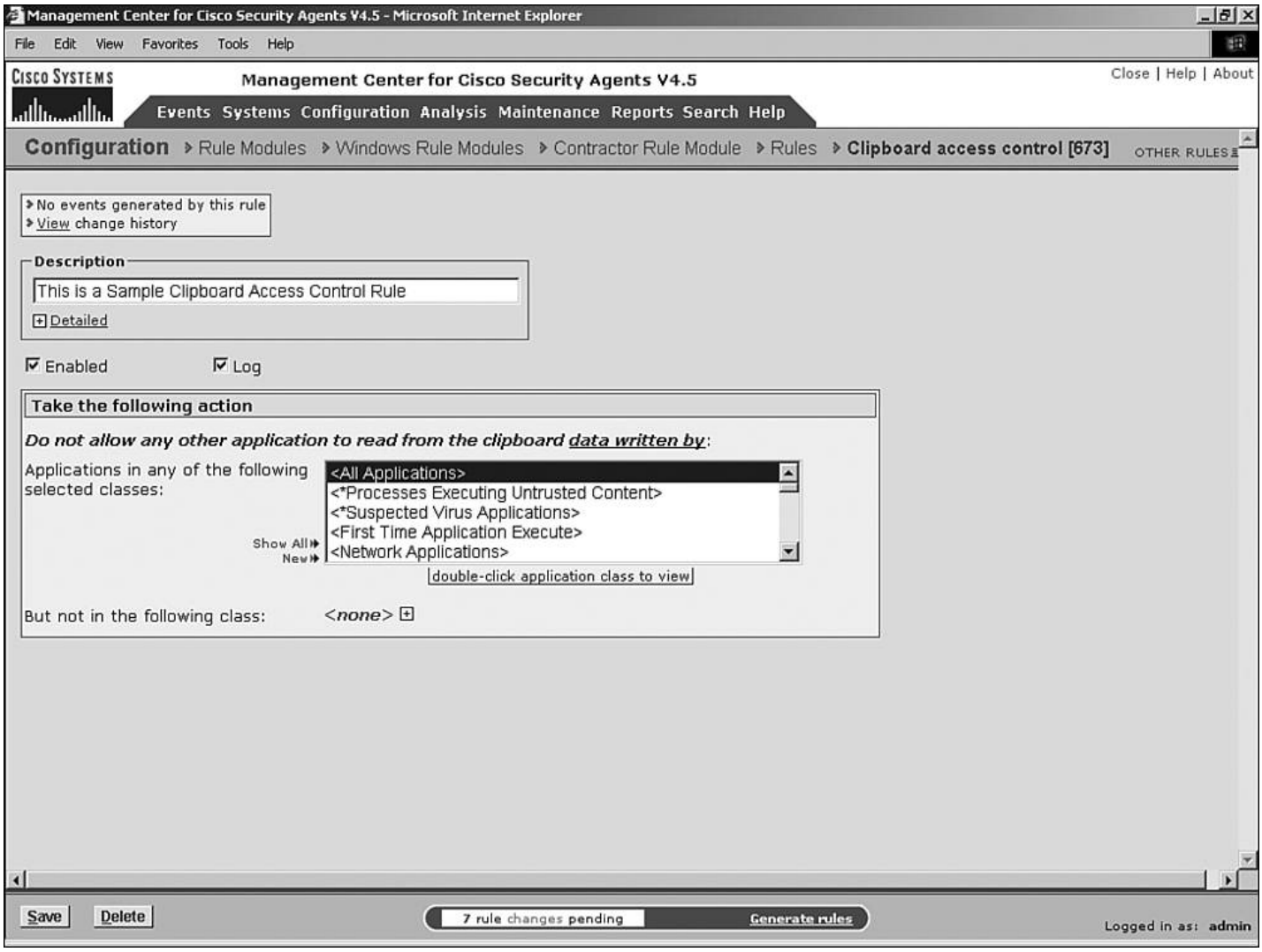

## Application Control

Контролирует каким приложениям нельзя или можно работать на локальной машине:



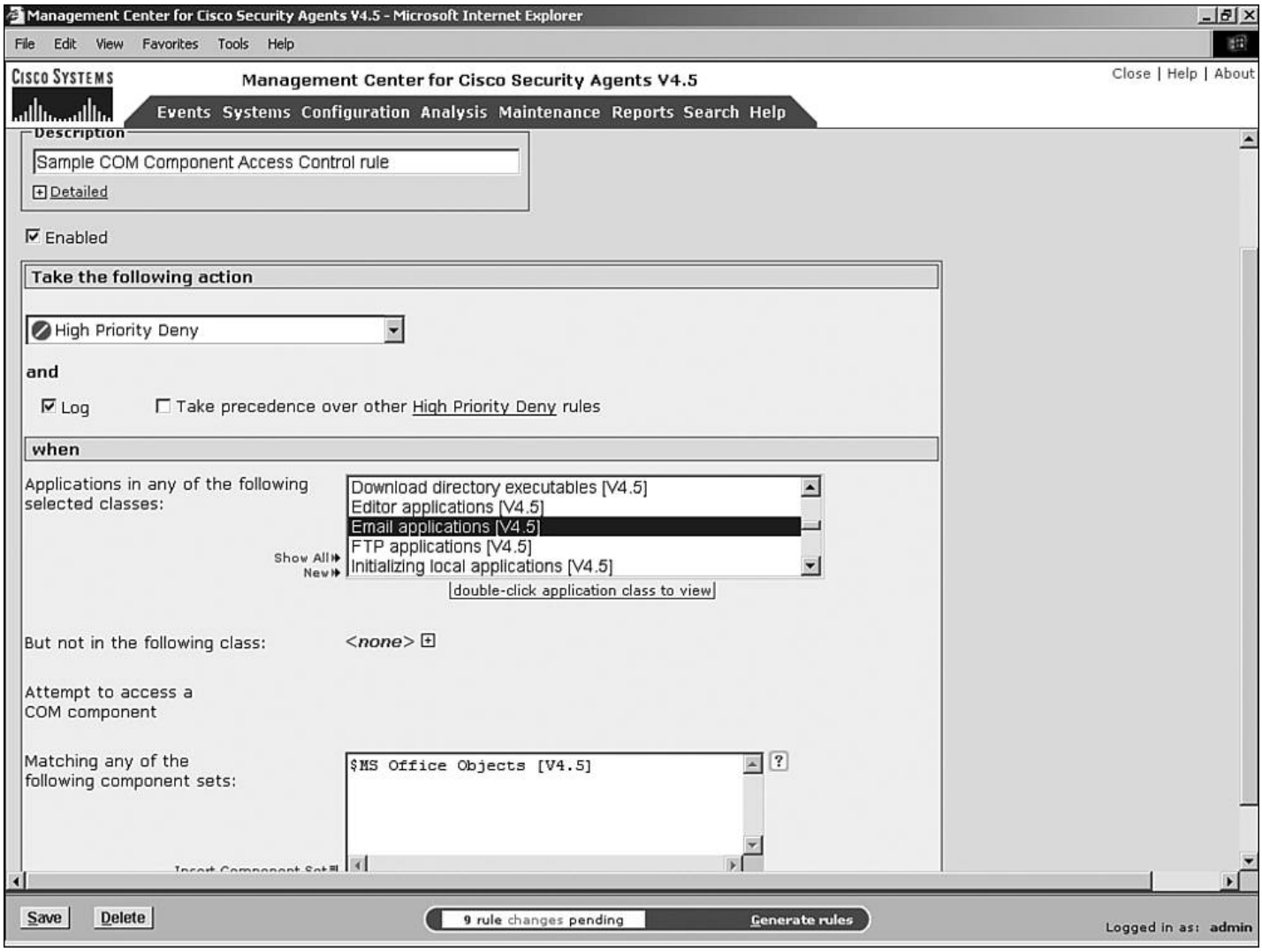

## Clipboard Access Control

Разрешает переносить данные через Clipboard только между заданными приложениями:



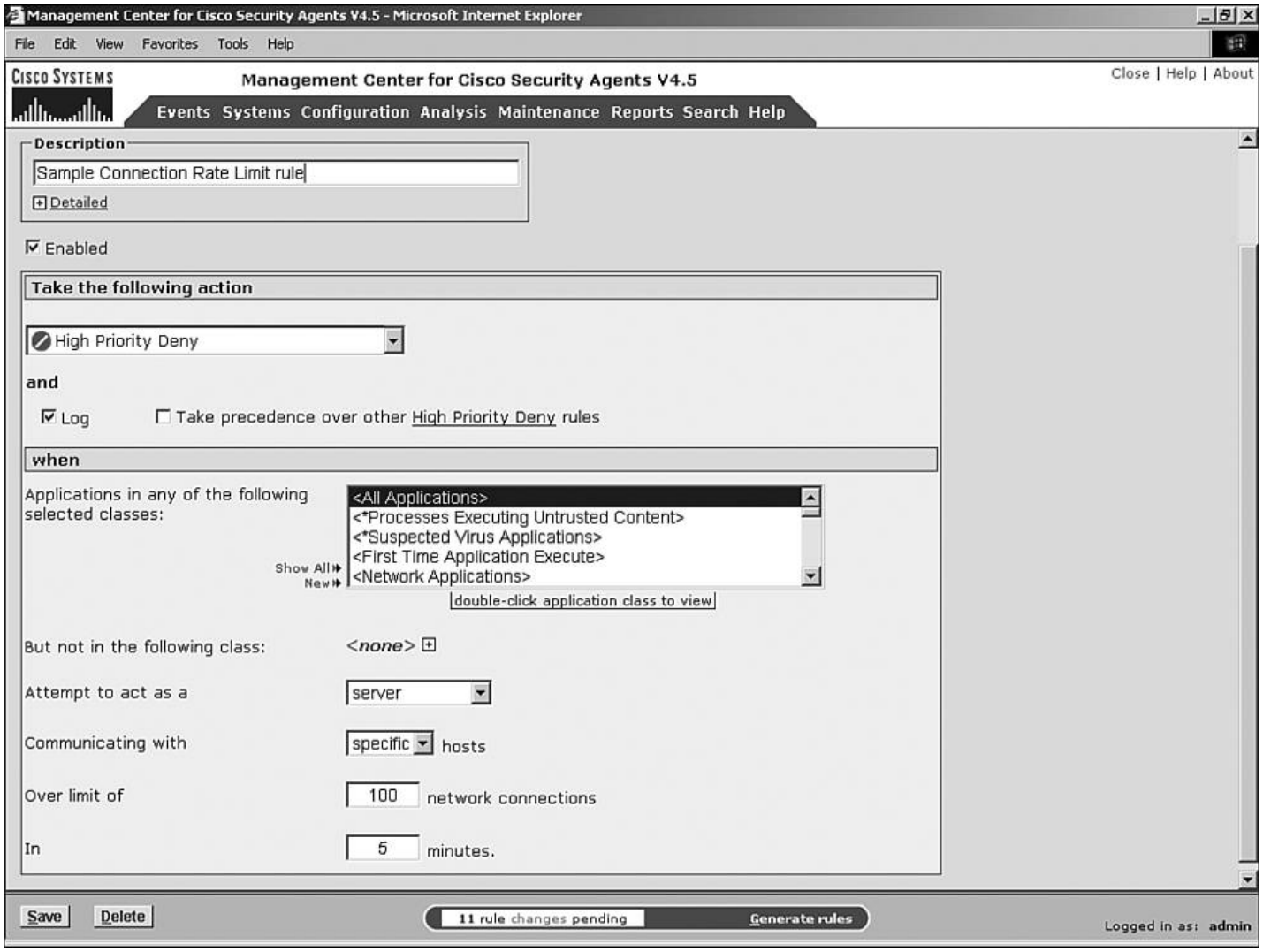

## COM Component Access Control

Указывает какие COM объекты могут быть доступны указанным приложениям:



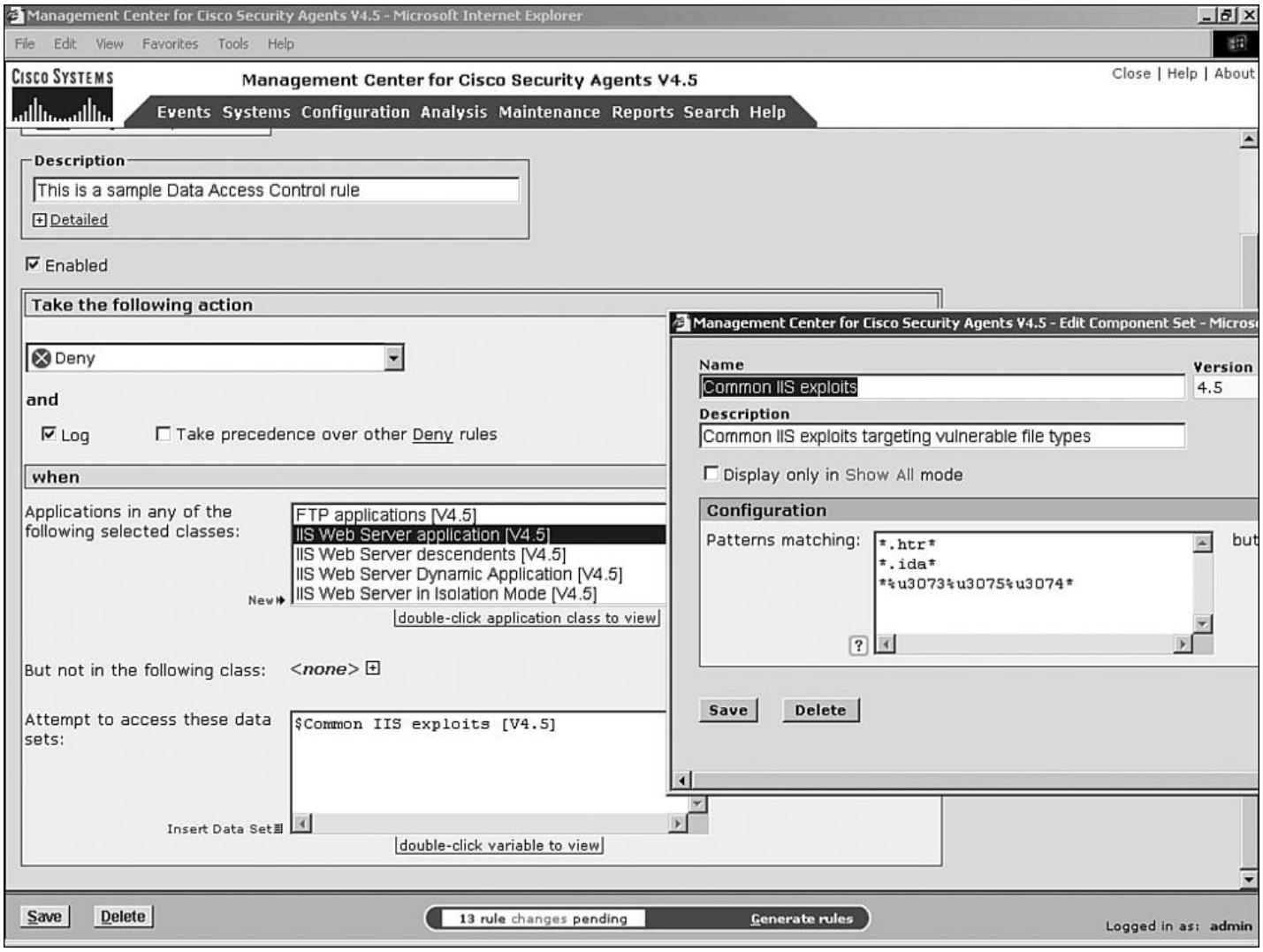

## Connection Rate Limit

Контролирует число входящих  и исходящих соединений локального компьютера. Таким образом, выполняется защита от DoS атак:



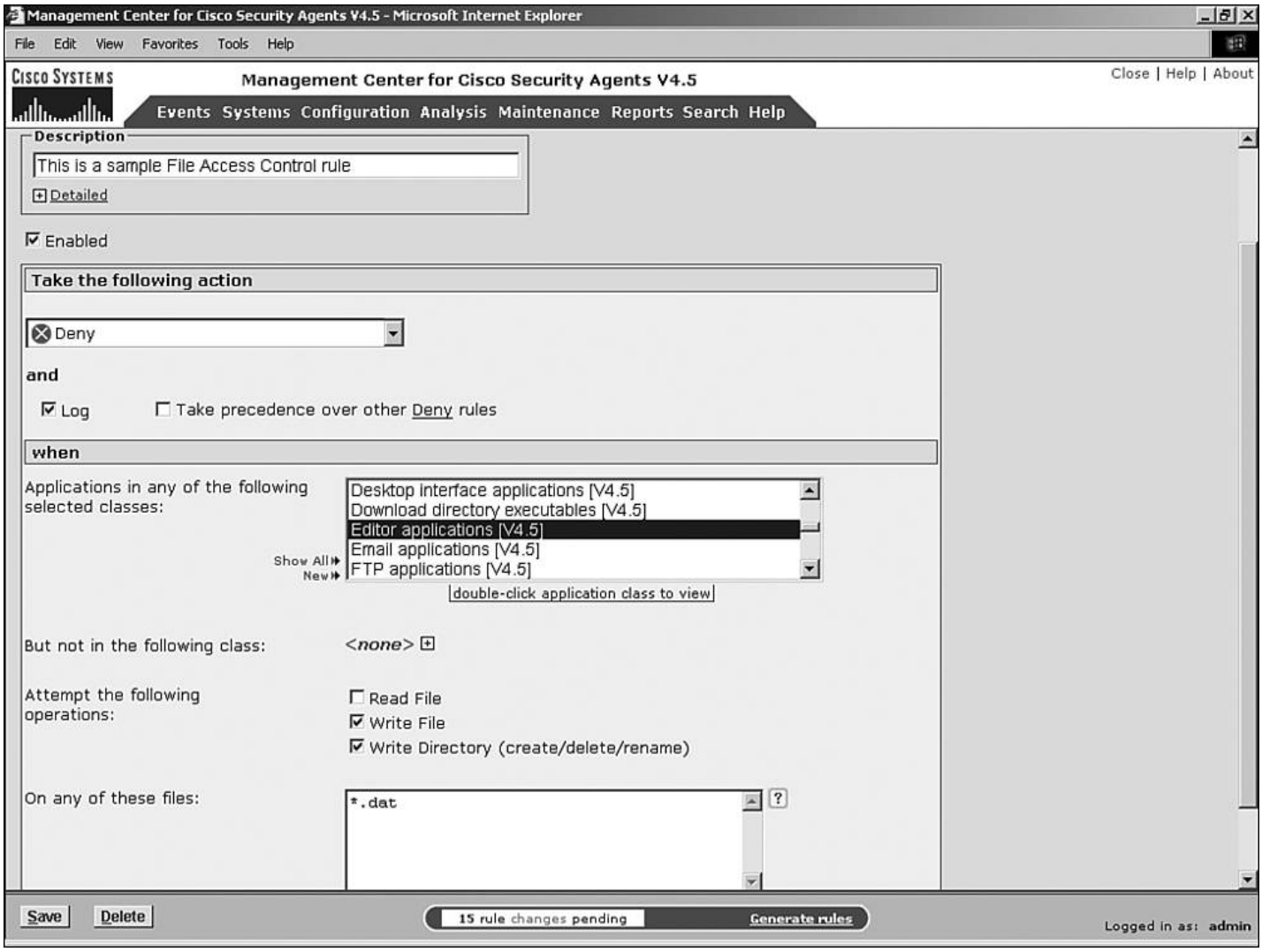

## Data Access Control

Используется для систем содержащих WEB сервер. Этот тип правил просматривает входящие запросы, а именно Uniform Resource Identifier (URI) порцию запроса. Он пытается найти неправильные запросы. Большинство неправильных запросов уже содержится при инсталляции MC, но вы можете добавить свои чтобы ловить новые или специальные виды атак. Для работы нужно чтобы в системе был инсталлирован CSA data filter. При инсталляции агента на Windows, если там стоит IIS или Apache то этот фильтр ставится сразу. На платформе UNIX фильтр всегда требует ручной инсталляции.



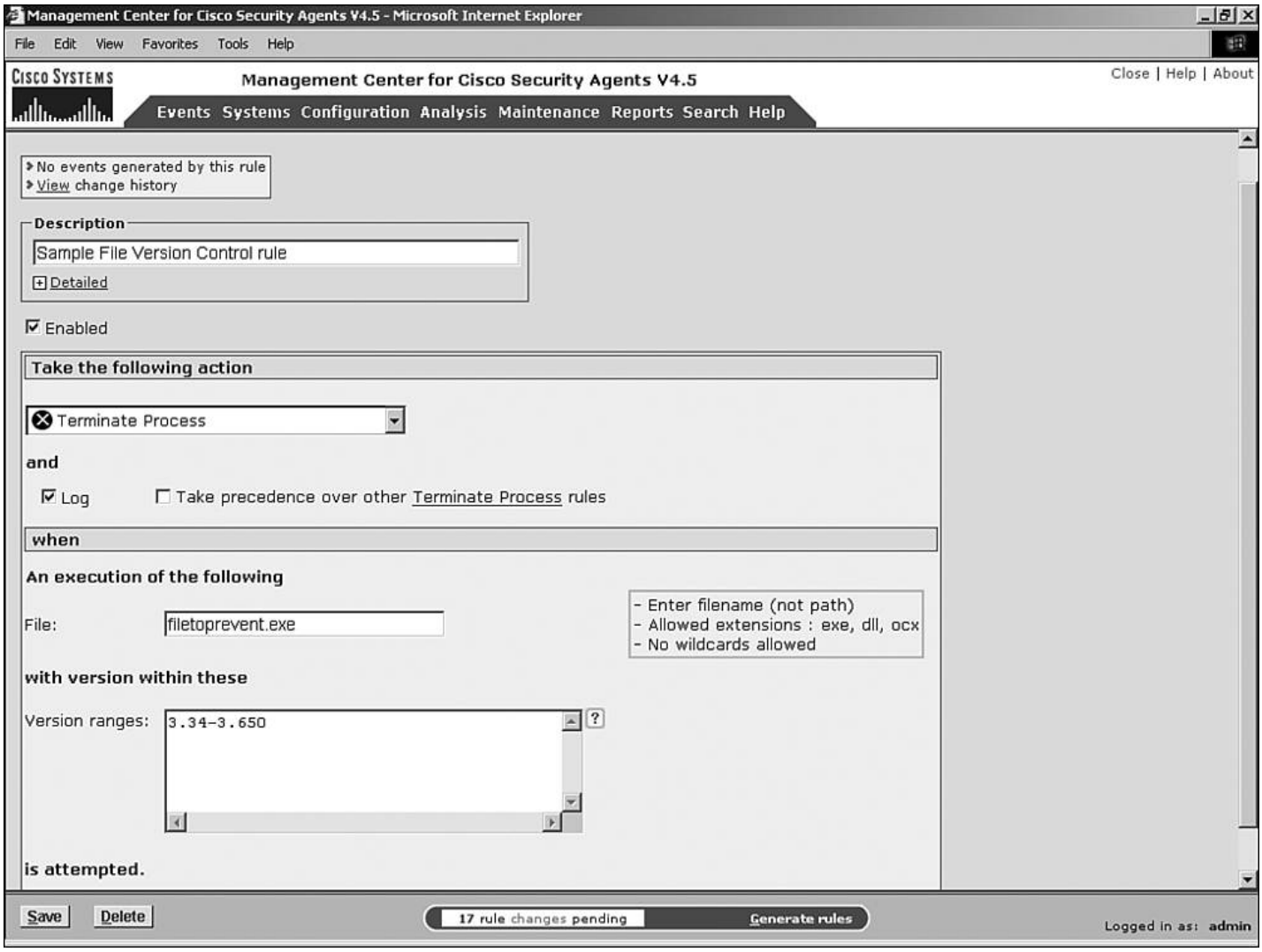

## File Access Control

Обеспечивает механизм проверки, какие процессы могу читать файлы и папки. Если в UNIX запрещен доступ к символьным ссылкам, то нужно понимать что это не означает автоматически запрещения доступа к самому файлу.



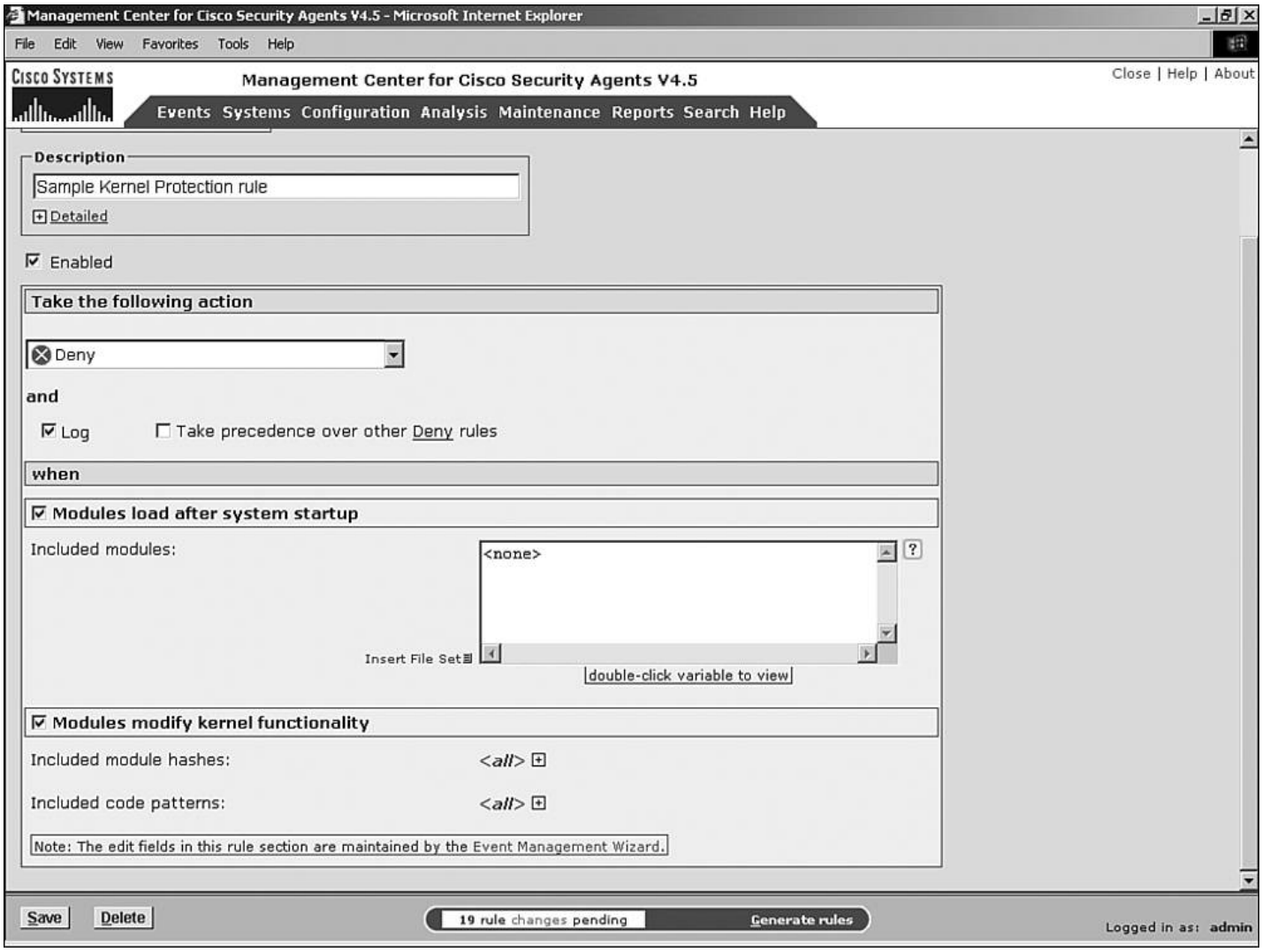

## File Version Control

Контролирует какие версии программ разрешены к исполнению.



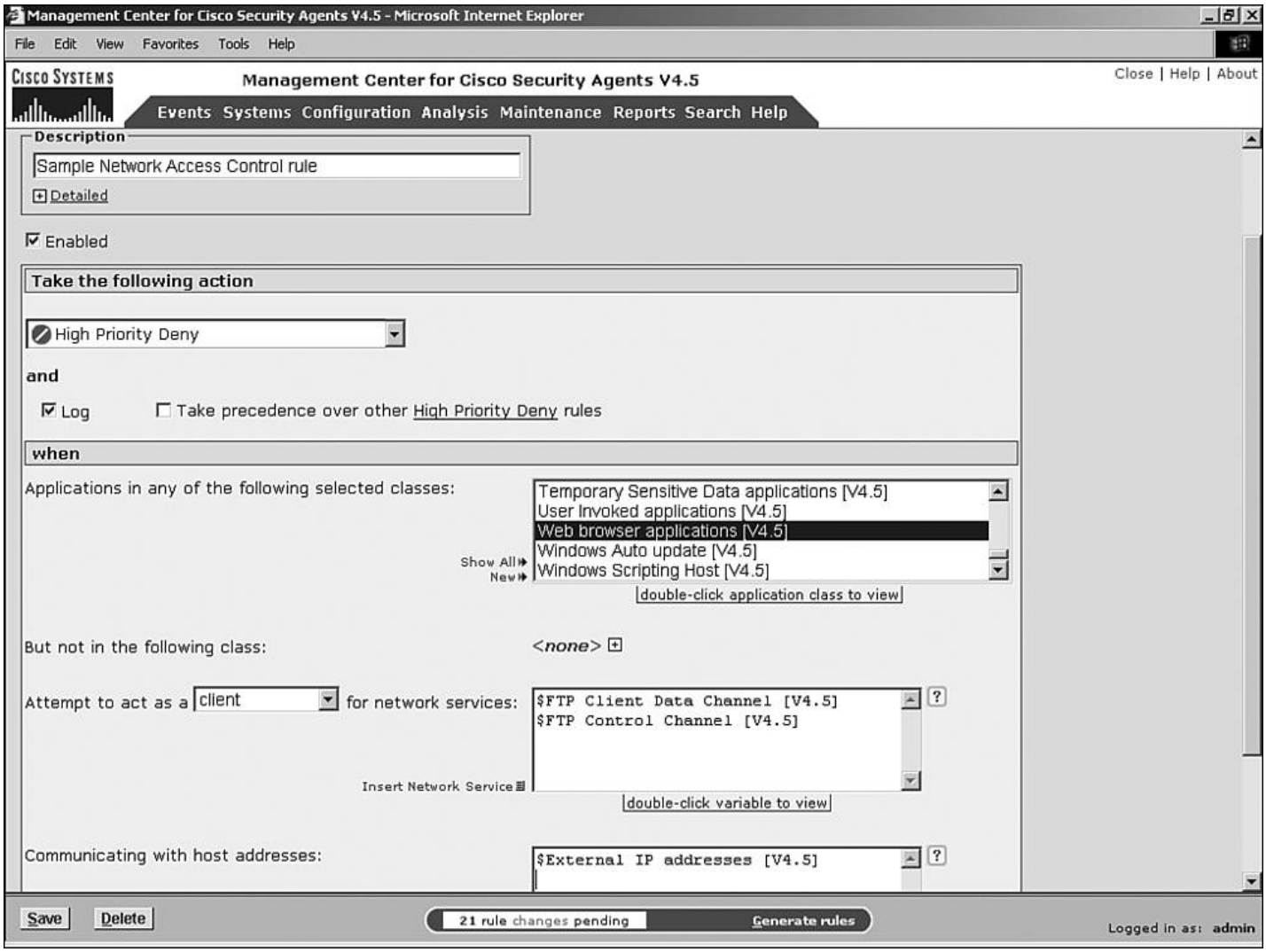

## Kernel Protection

Запрещает динамическую загрузку драйверов после загрузки системы:



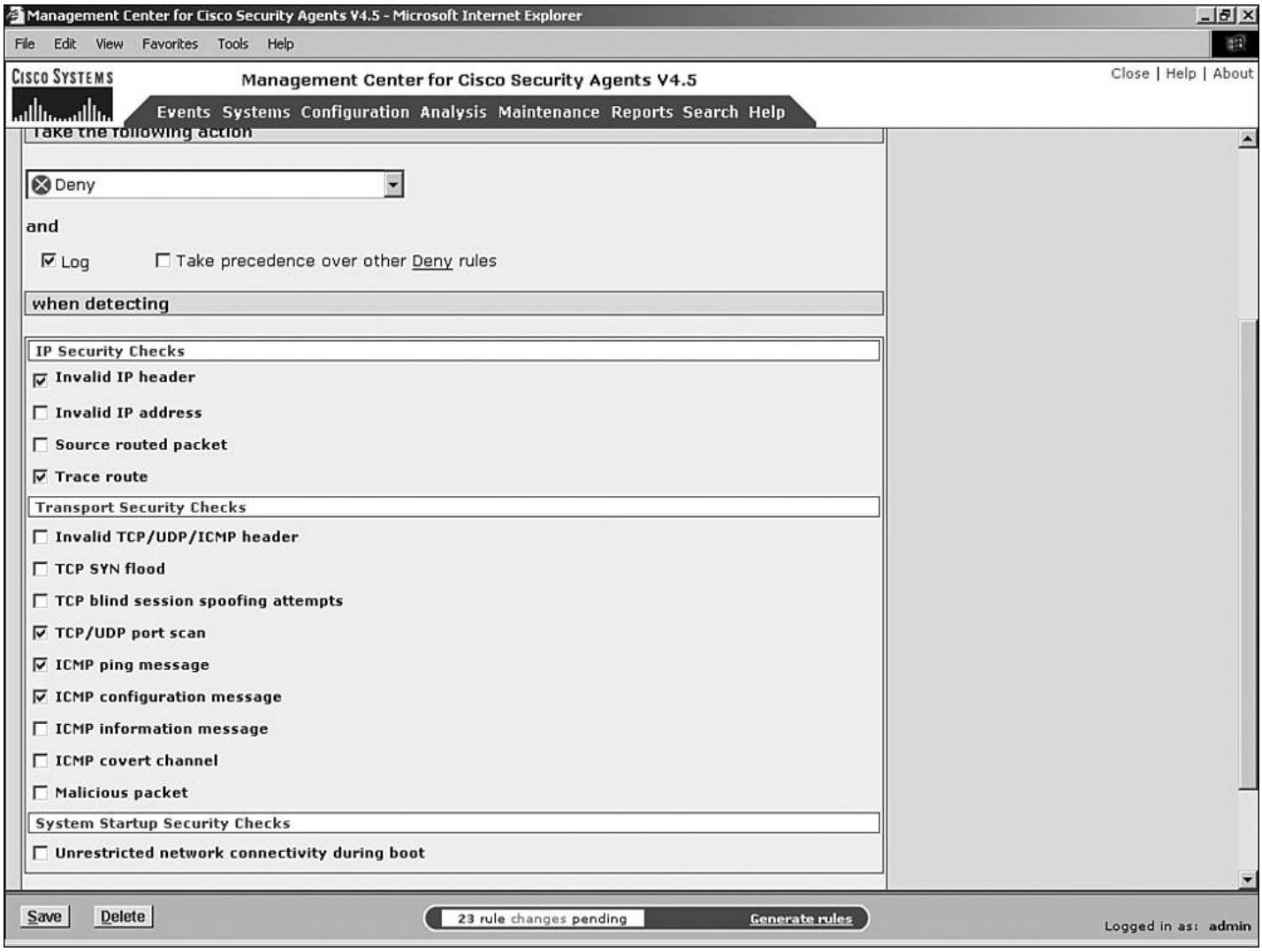

## Network Access Control

Позволяет контролировать доступ приложений в сеть и доступ к ним из сети.



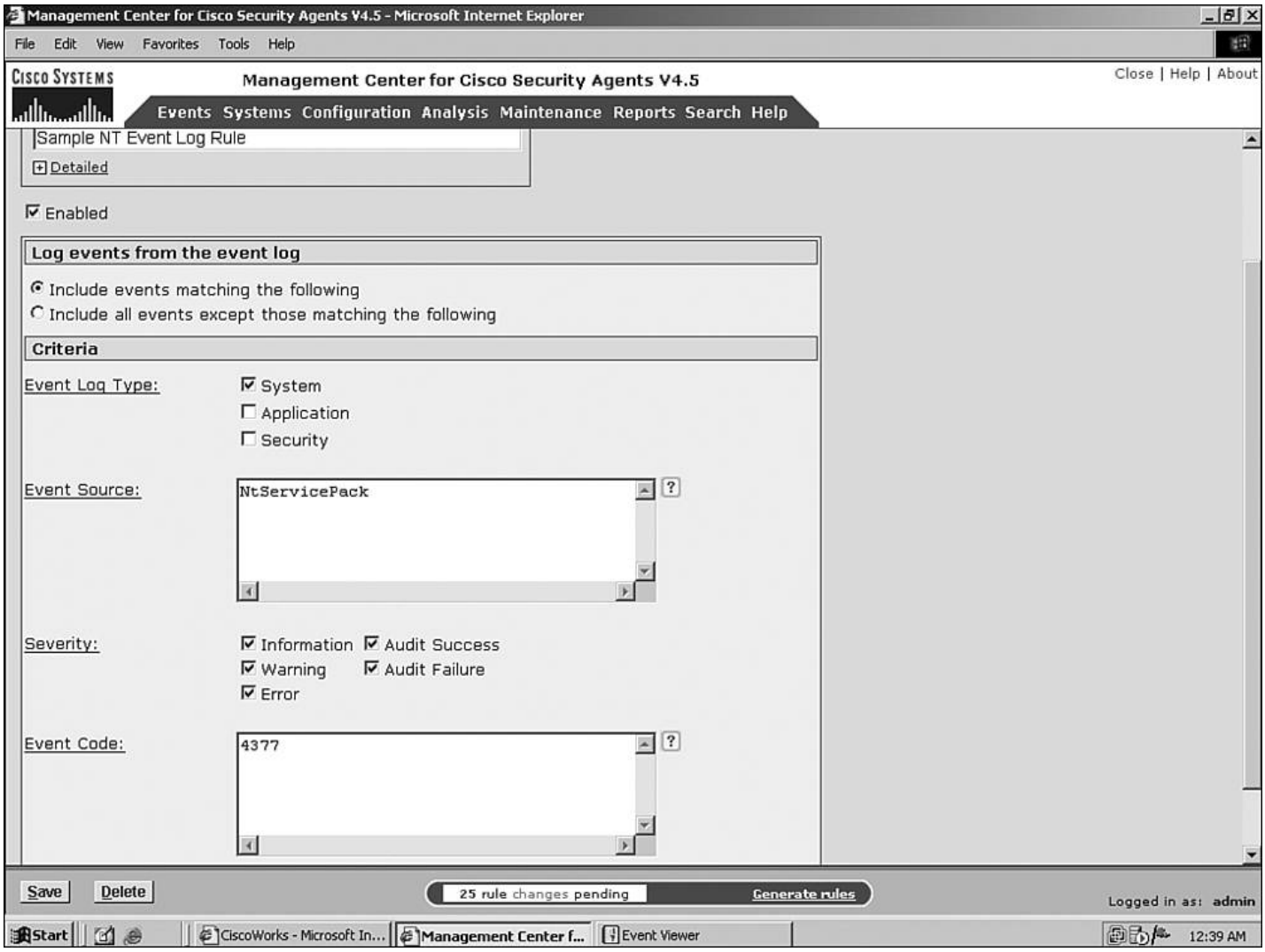

## Network Shield

Заставляет проверять сетевой трафик на правильность. Эта функция должна быть включена при инсталляции CSA. Называется Network Shim.



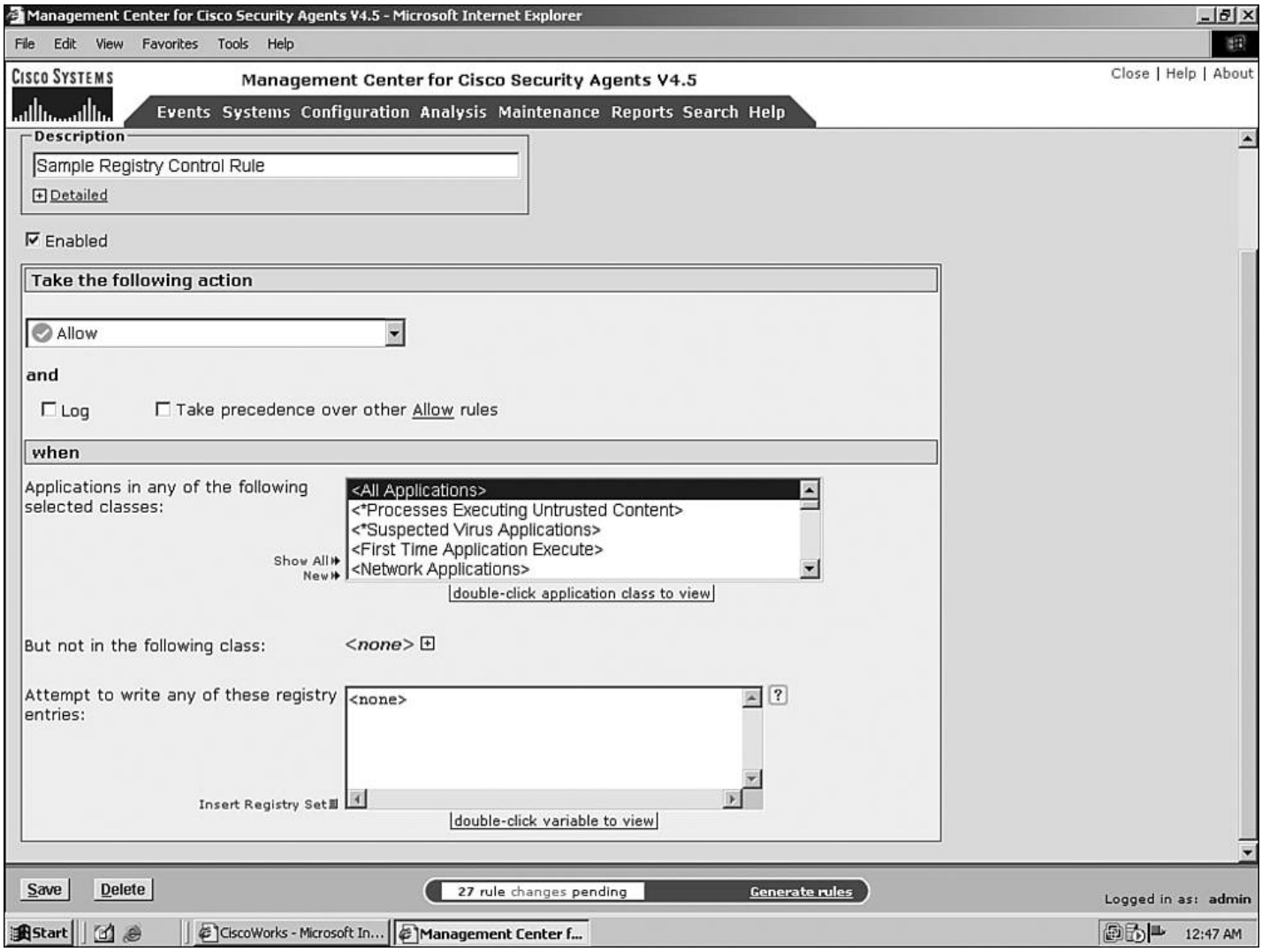

## NT Event Log

Позволяет собирать некоторые события из Event Log в журнале центра управления.



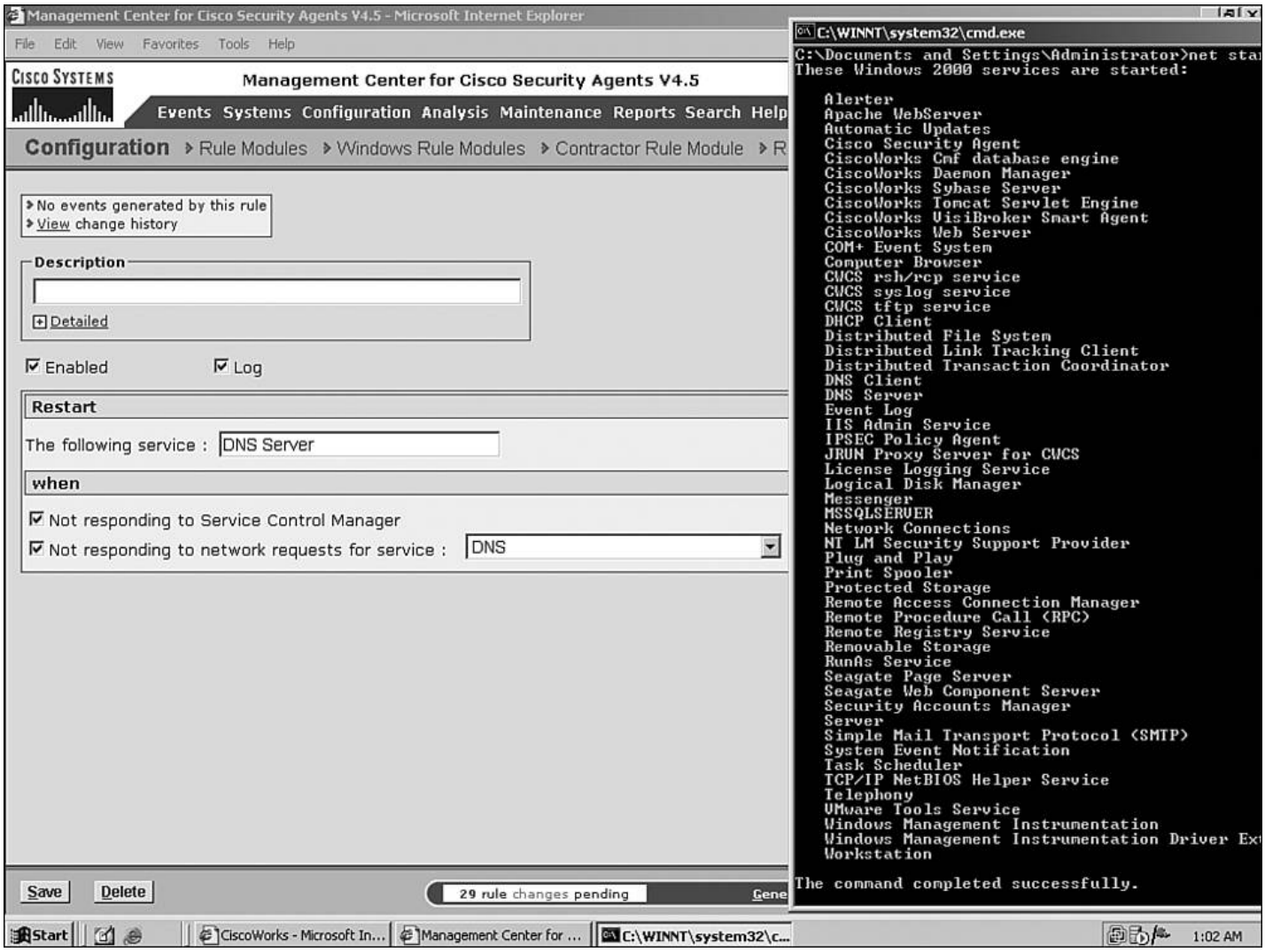

## Registry Access Control

Механизм контролирующий доступ приложений в ключи реестра, запрещает или разрешает запись и чтение из них.



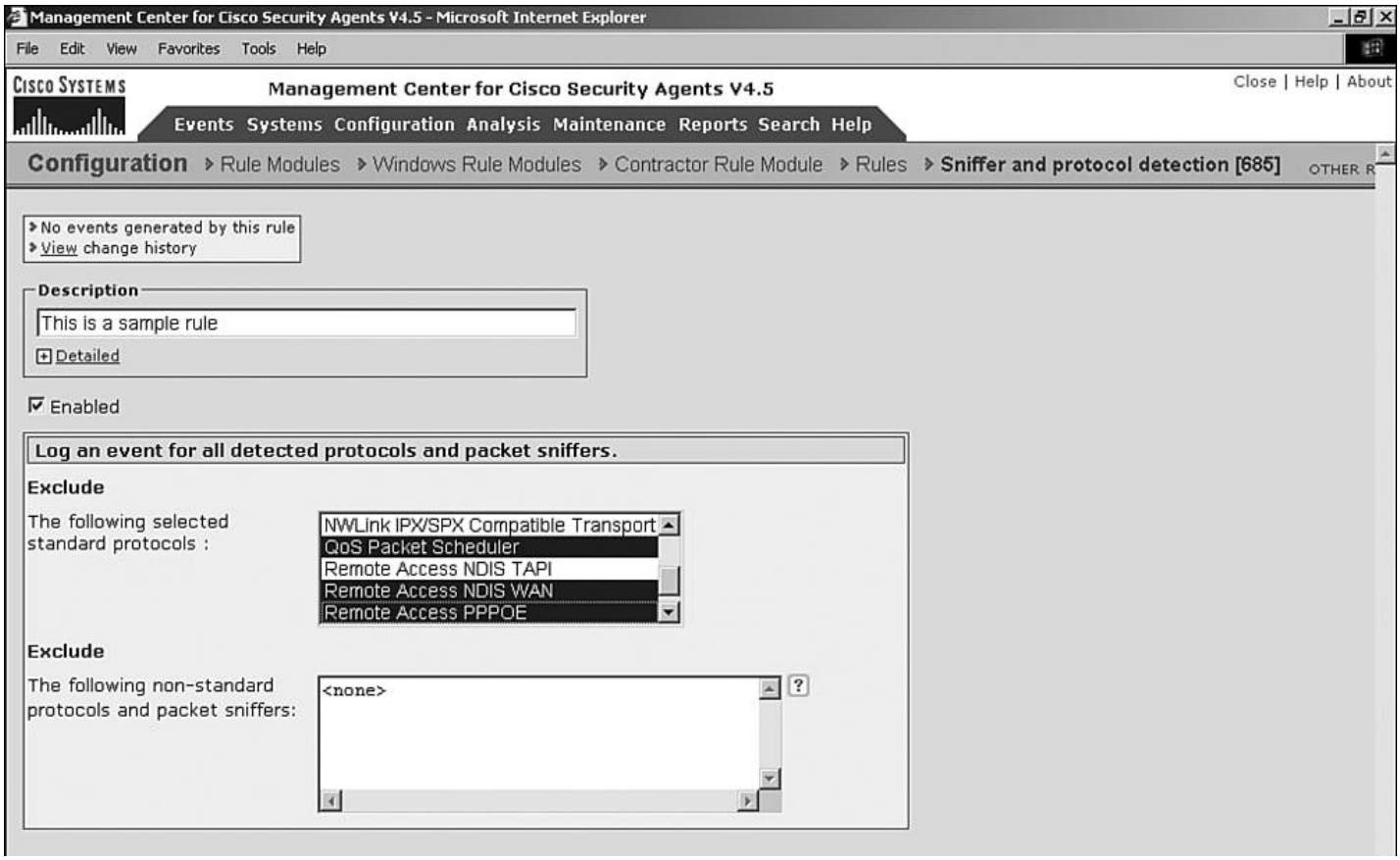

## Service Restart

Позволяет перезапускать сервисы, которые остановились или не отвечают на запросы.



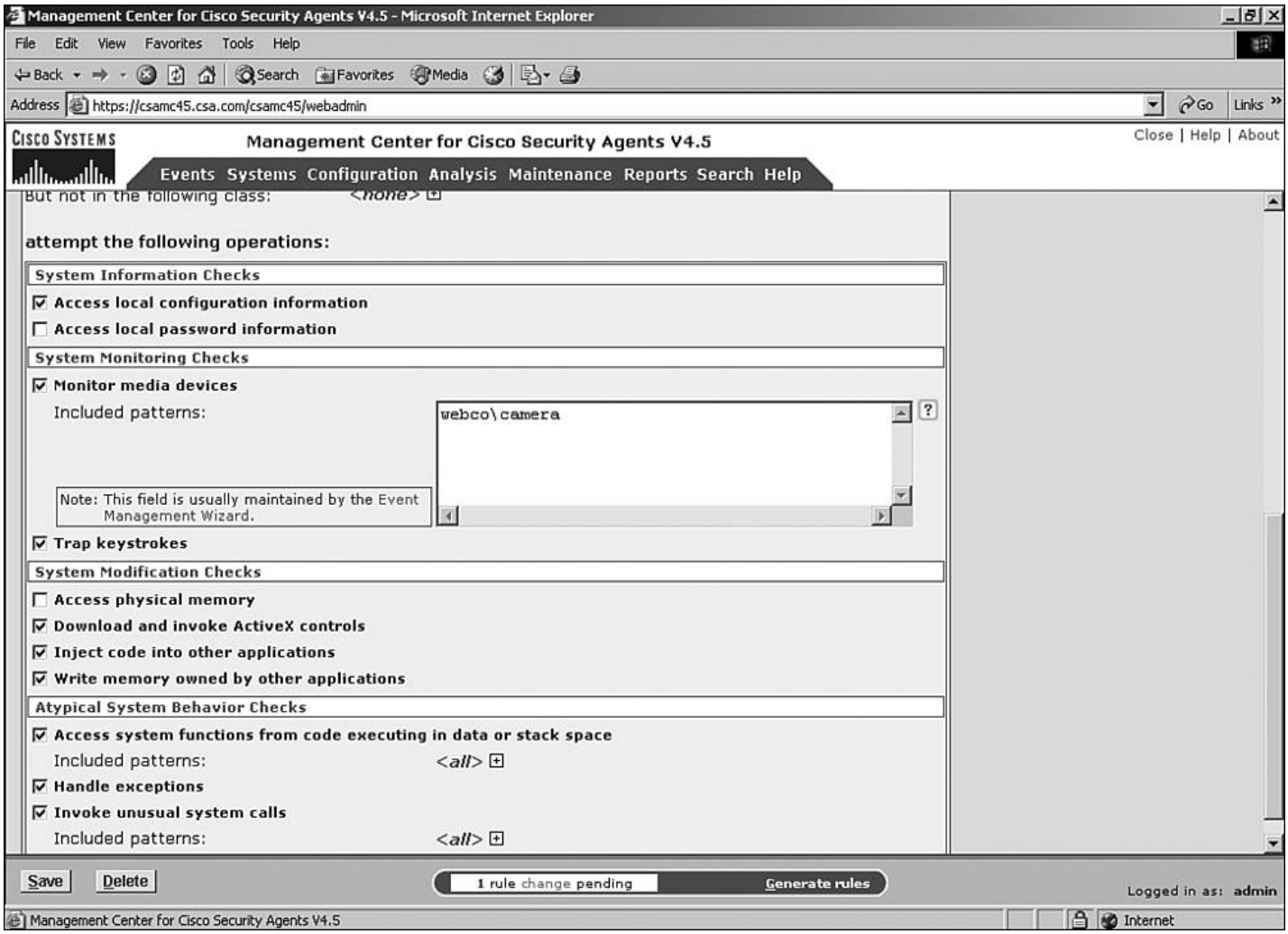

## Sniffer and Protocol Detection

Пишет сообщение о том, что был обнаружен не IP протокол и то что были обнаружены снифферы на машине защищенной агентом.



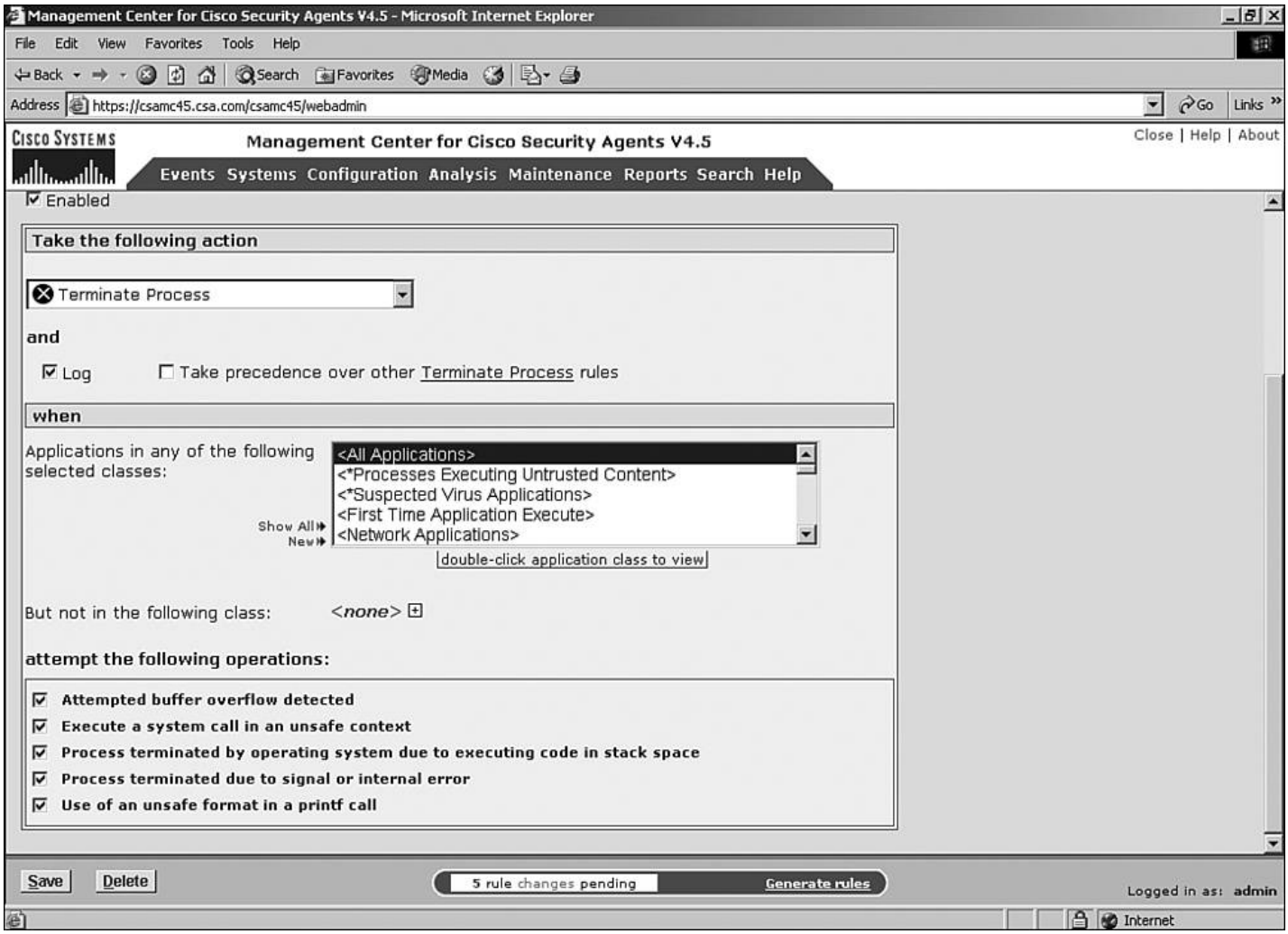

## System API

Предотвращает выполнение троянских программ и враждебного кода на машине с Windows.



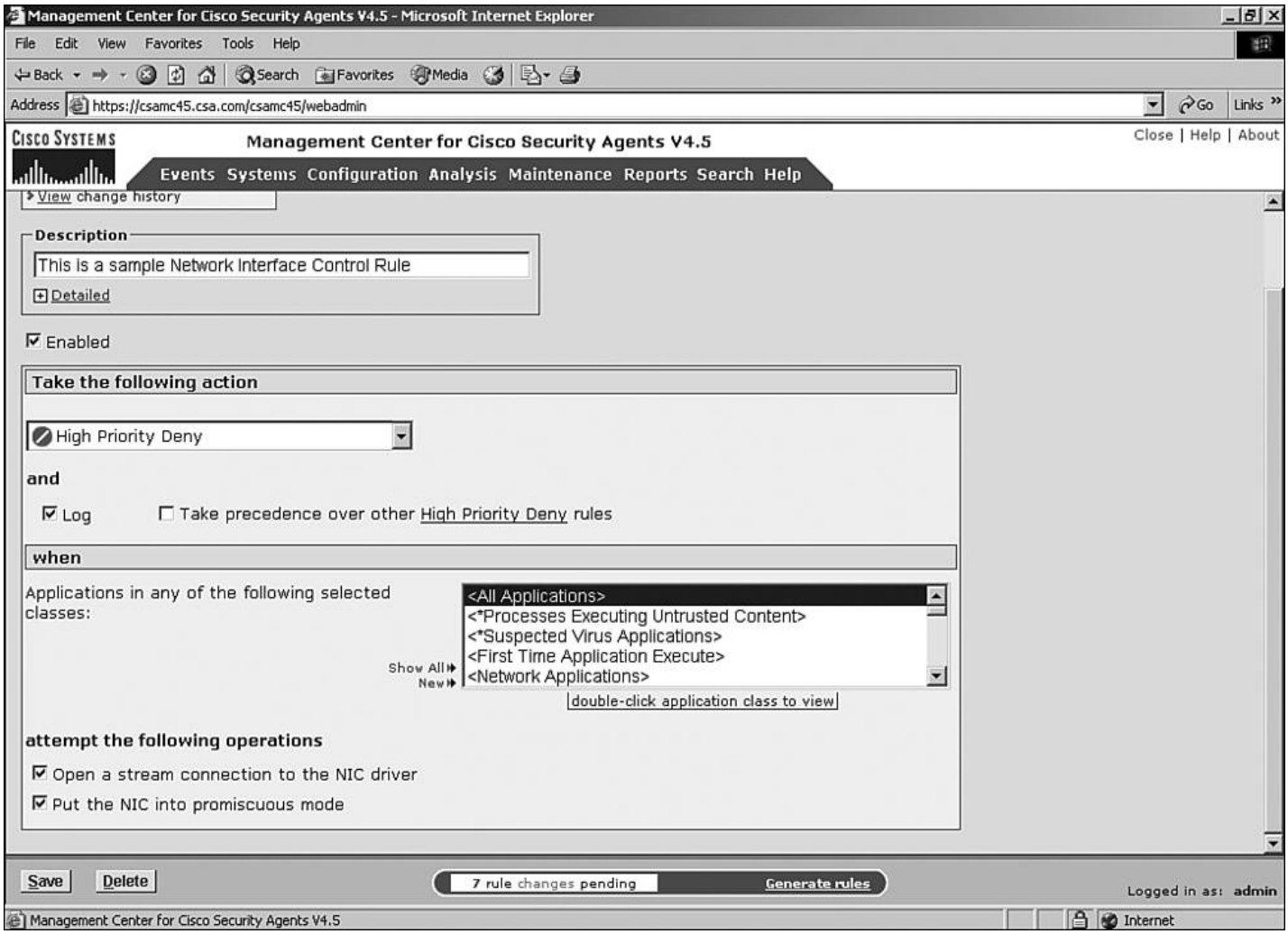

## Buffer Overflow

В UNIX делает то же самое что System API в Windows. Предотвращает использование переполенния буфера для повышения привилегий пользователей.




## Network Interface Control

В UNIX запрещает переводить интерфейс в Promiscuous mode.

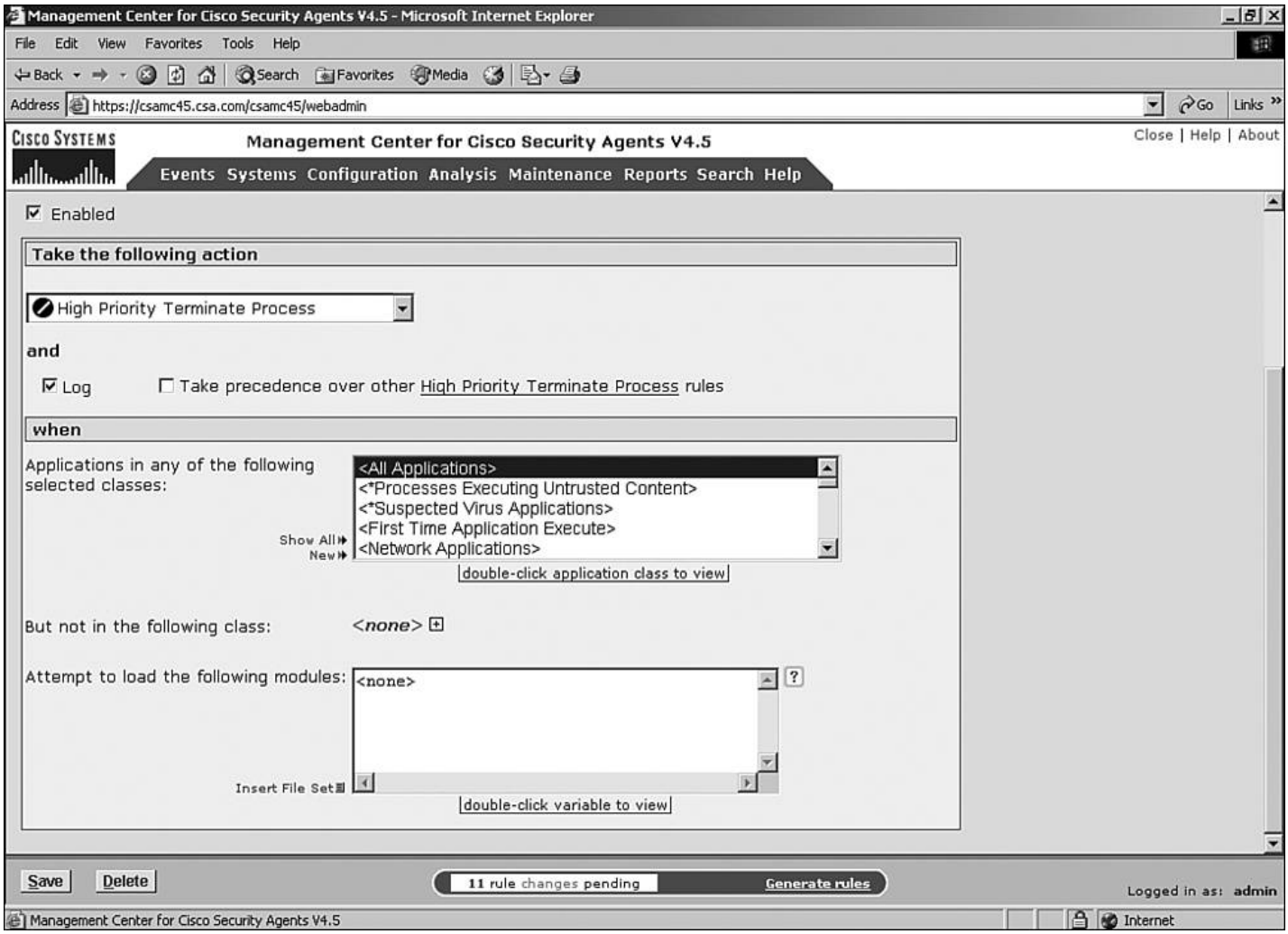



## Resource Access Control

Предотвращает атаки на используемые символические ссылки.

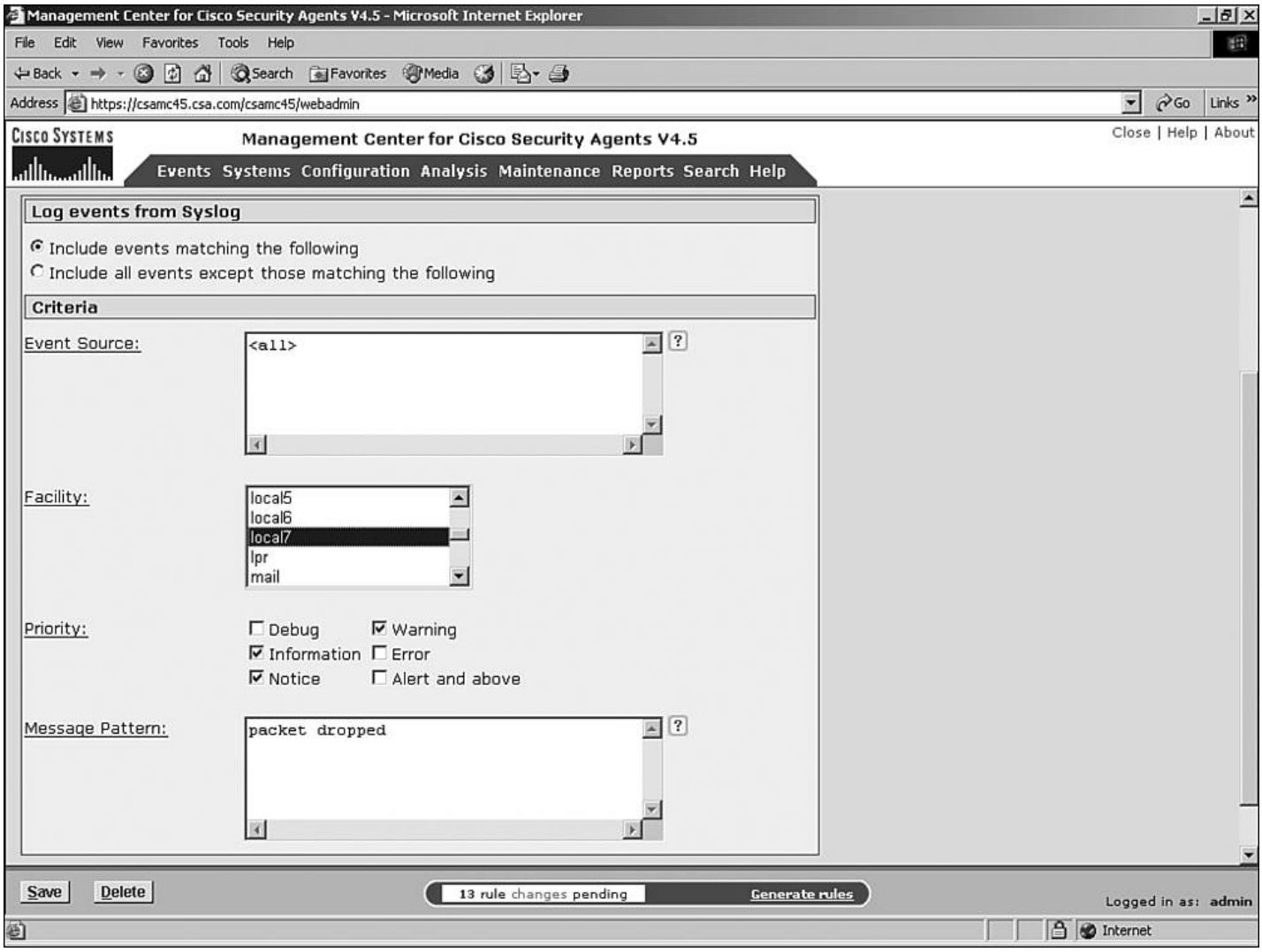

## Rootkit/Kernel Protection

Предотвращает загрузку драйверов после старта системы в UNIX.




## Syslog Control

Записывает некоторые сообщения Syslog в журнал цента управления CSA.



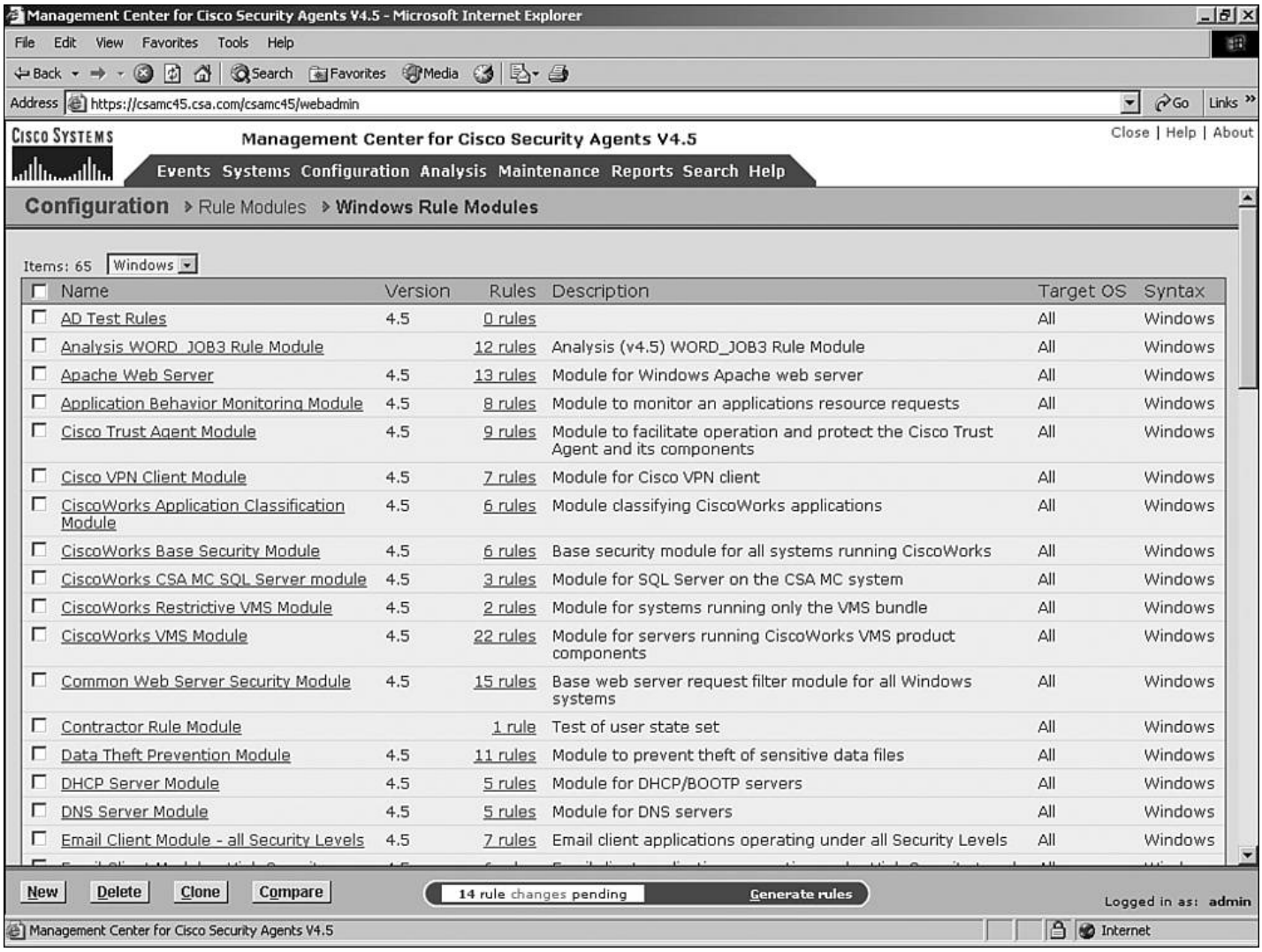

## *Модули правил*

Модули правил – это группа правил  служащих одной цели. В CSA есть два типа модулей: исполнители и детекторы. Исполнители заставляют агента разрешить или запретить какую-то операцию. А детекторы просто сообщают о наступлении события. С каждым правилом есть объяснение в понятной форме на английском языке о том, что этот модуль делает. Можно также проверить модуль на отсутствие конфликтов правил и создавать свои модули.

В CSA есть уже предопределенные модули, например

- **E-Mail Protection**
- **Apache Web Server**
- **Cisco VPN Client**
- **CiscoWorks Base Security**
- **CiscoWorks CSA MC SQL Server**
- **SendMail**
- **Samba**
- **Data Theft Prevention**
- **DHCP Server**
- **DNS Server**
- **Microsoft Office**

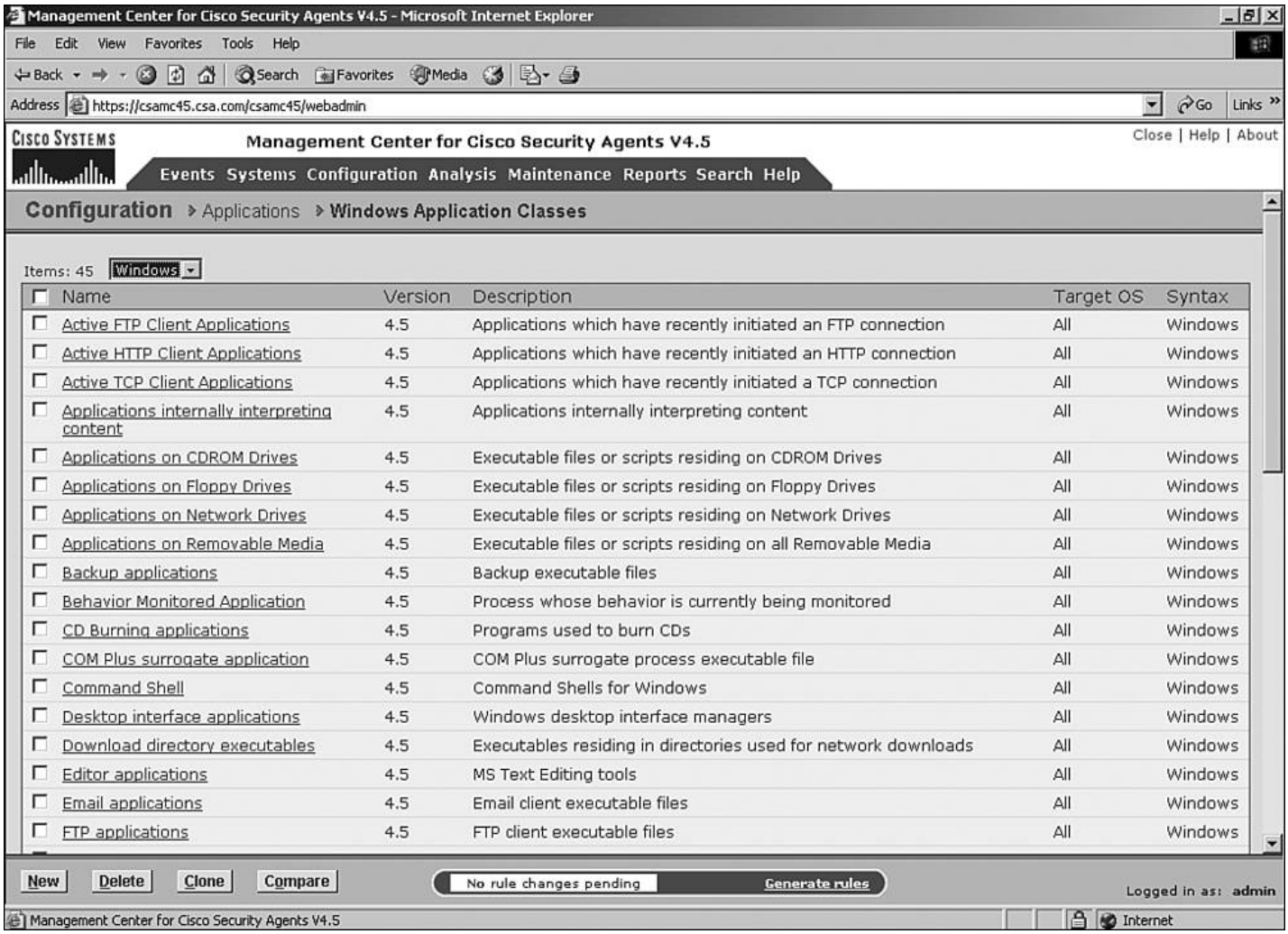
Чтобы получить к ним доступ войдите в меню **Configuration > Rule Modules [UNIX]** или **Rule Modules [Windows]**.




## *Классы приложений*

Классы приложений – это группа приложений одинаковых по функциям. Если вы хотите, чтобы какой то группе приложений, допустим, был разрешен доступ по telnet (TCP/23) а потом хотите контролировать какие приложения запустила эта группа программ, то вам нужно использовать какое-то выражение обозначающее эти приложения. Именно оно и будет классом приложений.

Чтобы лучше понять что это такое, посмотрите на уже предопределенные классы приложений через меню **Configuration > Applications > Application Classes [Windows].**




Если вы определяете процесс по имени, то такой класс является **статическим**, но вы можете определить и **динамический** класс, членство в котором для процесса появляется в результате какого-то его поведения. Таким образом, например, вы можете создать класс telnet клиентов, не зная реальных имен приложений.

## *Переменные*

Для упрощения конфигурации CSA использует переменные которые обычно называются множества или списки. Задав один раз вы можете использовать их в различных местах. Доступны следующие типы переменных:

- **Network address sets**
- **Network services sets**
- **Data sets**
- **File sets**
- **Dynamic file sets**
- **Query settings**
- **COM component sets**
- **Registry sets**

Чтобы сконфигурировать переменные заходите в меню **Configuration > Variables.**

## *Инсталляция агента*

Чтобы установить агента на машину не нужно обладать специальной подготовкой. Нужно лишь проверить системные требования. В версии 4.5 это должна быть операционная система Windows, Solaris или Linux.

| **Компонент** | **Требования к компоненту для агента под Windows** |
|---|---|
| Процессор | Intel Pentium 200 MHz or higher.<br><br>Note: Uni/dual/quad processors are all supported. |
| Операционная система | Windows 2003.<br><br>Windows XP (Professional English 128 bit) with Service Pack 0, 1, or 2.<br><br>Windows 2000 (Professional, Server, or Advanced Server) with Service Pack 0, 1, 2, or 3 or higher.<br><br>Windows NT (Workstation, Server, or Enterprise Server) with Service Pack 5 or higher.<br><br>Note: Citrix MetaFrame and Citrix XP are supported. Terminal Services are supported on XP and Windows 2000. Terminal Services is not supported on Windows NT. |
| Память | 128 MB minimum. |
| Место на жестком диске | 15 MB or higher. |
| Сеть | Ethernet or dialup.<br><br>Note: Maximum of 64 IP addresses supported on a single system. |

| **Компонент** | **Требования к компоненту для Solaris** |
|---|---|
| Процессор | UltraSPARC 400 MHz or higher.<br><br>Note: Uni/dual/quad processors are all supported. |
| Операционная система | Solaris 8, 64-bit 7/01 edition or higher.<br><br>Note: Solaris minimum core installation is not sufficient. You must also install the SUNWlibCx library. |
| Память | 256 MB minimum. |
| Место на жестком диске | 15 MB or higher. |
| Сеть | Ethernet.<br><br>Note: Maximum of 64 IP addresses supported on a single system. |

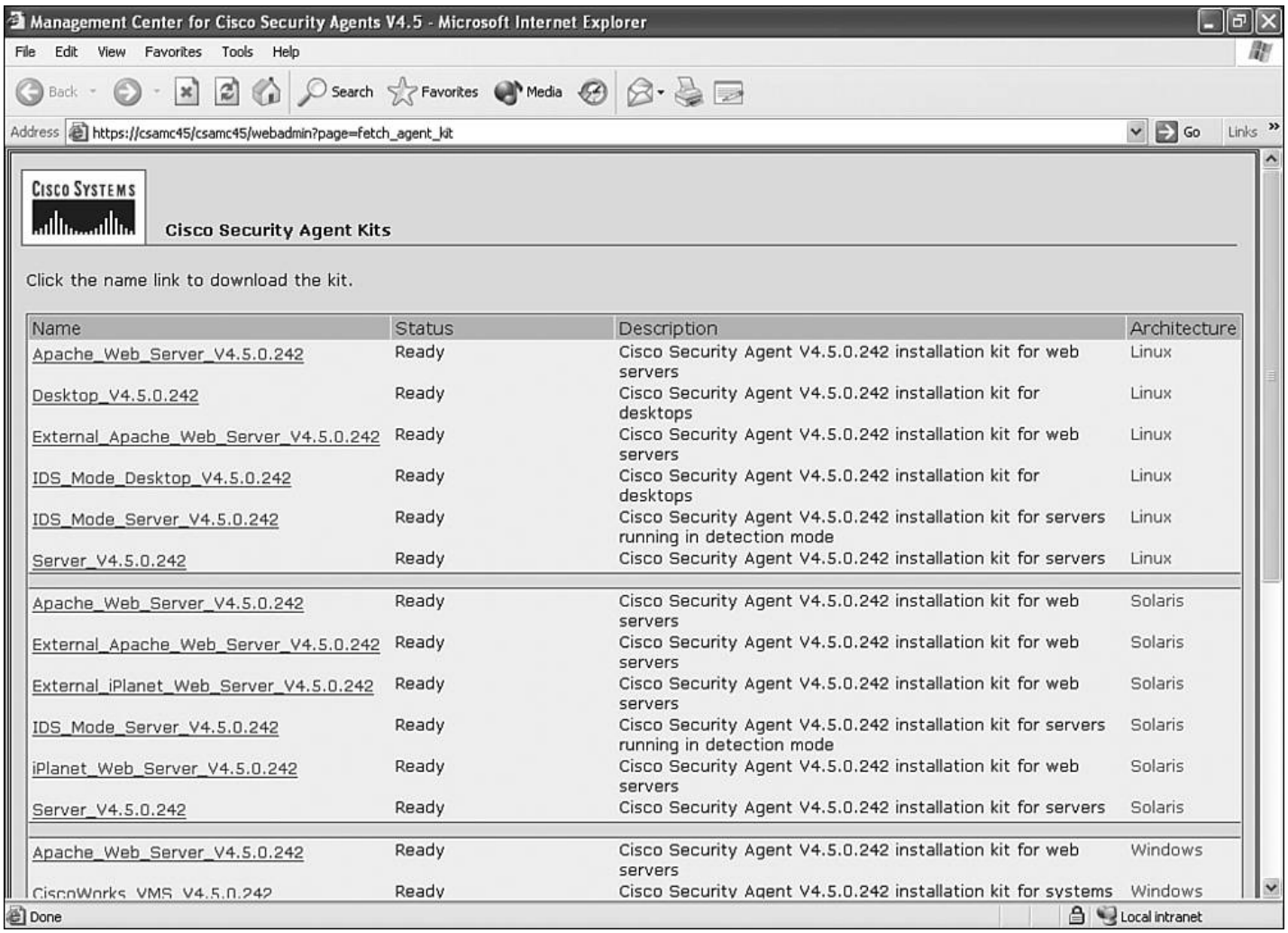
| **Компонент** | **Требования к компоненту для Linux** |
|---|---|
| Процессор | 500 MHz or higher x86 processor.<br><br>Note: Uni/dual/quad processors are all supported. |
| Операционная система | RedHat Enterprise Linux 3.0 ES, AS, or WS. |
| Память | 256 MB minimum. |
| Место на жестком диске | 15 MB or higher. |
| Сеть | Ethernet.<br><br>Note: Maximum of 64 IP addresses supported on a single system. |

Есть еще одно требование. Агент должен иметь возможность узнать IP адрес центра управления по его FQDN имени через DNS. Дело в том, что инсталляционный пакет содержит адрес центра управления в виде FQDN имени. Заполнение файла hosts может решить ту же задачу.

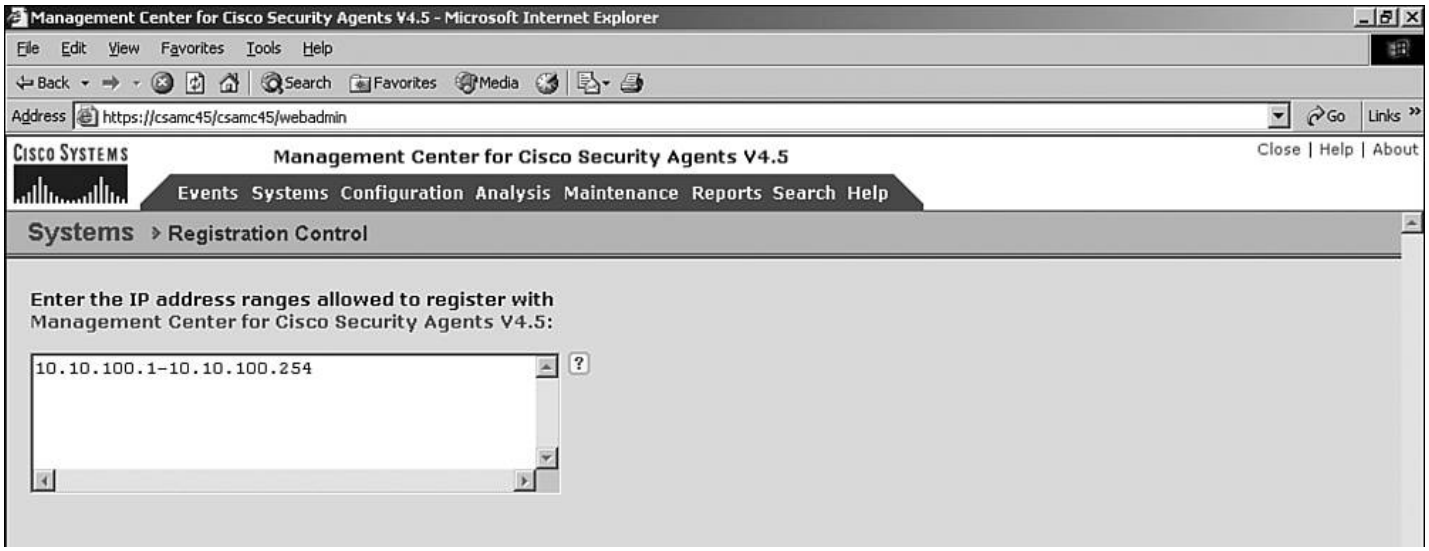
Если MC и агент находятся в разных сегментах сети, то нужно проверить что сетевые взаимодействия между ними не блокированных списками доступа или правилами межсетевых экранов. Взаимодействие между ними происходит по протоколу SSL по стандартному порту 443 протокола TCP.

Чтобы установить агента на машину вам нужно либо создать новой инсталляционный пакет в центре управления CSA через меню **System > Agent Kits** или воспользоваться уже готовыми пакетами.

Если вы создали пакет или он уже был сделан, то вы должны с машины на которой устанавливаете агента зайти по адресу https://ciscoworks_system_name/csamc45/kits и скачать нужный пакет.




Не забудьте посмотреть в меню **Systems > Registration Control** есть ли у вашего IP адреса доступ к этому URL.




После того как вы скачали пакет, вы запускаете его.

## Инсталляция в Windows

Пакет идет в виде exe файла в котором уже заложены все правила и адрес центра управления.

Нажимая кнопку Next вы проходите несколько окошек, соглашаясь с лицензией, выбирая путь для установки, выбираю опцию Network Shim или отключая ее и по окончании инсталляции перезагружаетесь. Опция Network Shim включает в себя следующие возможности

- **Port scan detection**
- **SYN flood protection**
- **Malformed packet protection**

Вы можете отказаться от инсталляции этого компонента, поскольку иногда он может конфликтовать с другими программами защиты на хосте, например с VPN клиентами или персональными межсетевыми экранами. Cisco VPN Client не конфликтует с этой опцией. Выключив эту опцию вы просто уменьшите число способов контроля за трафиком. Возможно что вам и не надо защищать вашу станцию от DoS атак. В любом случае решение принимает администратор о том включать или не включать.

### Инсталляция на Solaris

Тоже нужно скачать программу инсталляции и затем руками установить:

- tar xvf CSA-Server_4.5.0.15-setup.tar
- pkgadd -a CSCOcsa/reloc/cfg/admin –d
- shutdown -y i6 g0

### Инсталляция в Linux

- tar xvf CSAagent-4.5-51.i386.tar
- ./install_rpm.

## *Пользовательский интерфейс агента*

В Windows агент появляется в трее в виде красного флага. Если флажок движется то значит сработало какое-то правило и оно привлекает внимание пользователя. Другой способ привлечь внимание – всплывающие окна. Если вас отвлекают всплывающие окна то вы можете выключить их вписав в реестр

HKEY_CURRENT_USER\Software\Okena\Cisco Security Agent\

key="BalloonPopupsDisabled"=dword:00000001

Вообще настроек агента очень мало, поскольку все выполняется в центре управления CSA. Пользователь может установить уровень безопасности в Low, Medium, High, но это работает только такие уровни поддерживаются в политике. По умолчанию это все одно и то же. Можно вообще выключить защиту CSA.

В агенте есть поля для контактной информации – эта информация пересылается в цент управления чтобы облегчить техническую поддержку пользователя.

Перевод: Денис Батранков

**Вывод: Proventia Desktop лучше, поскольку там есть реальный HIPS анализирующий сетевой трафик. Сервера защищать при помощи CSA нельзя.**