

Руководство
администратора

Outpost Network Security

Офисный брандмауэр от
Агнитум

О чем этот документ

Настоящий документ содержит сведения о развертывании Outpost Network Security в корпоративной сети. Кроме того, описывается общая последовательность настройки клиентского брандмауэра.

Подробное описание настройки клиентского брандмауэра приводится в **Руководстве пользователя Outpost Network Security Client**.

Содержание

Введение	4
Системные требования	6
Компоненты.....	6
Системные требования.....	6
Защита клиентских компьютеров: Шаг за шагом.....	7
Установка Outpost Network Security.....	7
Настройка обновлений для клиентских компьютеров	7
Развертывание Outpost Network Security Client на клиентских компьютерах.....	8
Настройка параметров защиты для клиентских компьютеров	8
Применение настроек к клиентским компьютерам	9
Установка Outpost Network Security.....	10
Настройка обновлений для клиентских компьютеров	11
Включение обновлений.....	11
Планирование обновлений.....	12
Настройка параметров соединения	12
Контроль статистики обновления	13
Развертывание Outpost Network Security Client на клиентских компьютерах	14
Открытие объекта групповой политики для редактирования.....	14
Использование политики установки программного обеспечения для развертывания Outpost Network Security Client.....	16
Привязка объекта групповой политики	17
Настройка параметров безопасности на клиентских компьютерах.....	18
Общие настройки	19
Правила для приложений	19
Контроль процессов.....	23
Глобальные правила	24
Параметры ICMP.....	25
Параметры LAN	25
Подключаемые модули	26
Очистка журнала.....	27
Пароль	28
Дополнительно	28
Применение настроек к клиентским компьютерам	30
Отслеживание статистики публикации.....	30
Управление группами компьютеров	31
Удаление брандмауэра с клиентских компьютеров	31

Введение

В наши дни, когда Интернет-угрозы увеличиваются экспоненциально, администраторам корпоративных сетей приходится уделять особое внимание защите рабочих станций пользователей. Корпоративные серверы могут быть защищены очень хорошо, но если на клиентских рабочих станциях остаются незащищенные входы, это может быть использовано для хищения внутренних данных или создания путаницы.

Администраторы фильтруют содержимое web-сайтов и блокируют сетевую рекламу, чтобы сократить сетевой трафик и сделать использование Интернета сотрудниками более управляемым.

Полагаться на то, что пользователи сами защитят свои рабочие станции, вообще говоря, не стоит, потому что большинство сотрудников не имеют достаточного технического образования, чтобы установить и поддерживать необходимый уровень защиты своих компьютеров, который предотвратил бы неавторизованный доступ к корпоративной сети.

Когда возникает необходимость защитить отдельные рабочие станции от вторжения и эпидемий вирусов, администратору приходится лично обходить все компьютеры, вручную устанавливать и настраивать брандмауэры в соответствии с корпоративной политикой безопасности. Почти всегда на всех рабочих станциях используются одинаковые средства защиты и одинаковые параметры безопасности. В сложных распределенных сетях администратору приходится тратить много времени на многократное повторение одних и тех же последовательностей операций. Более того, ему приходится вручную применять все изменения, внесенные каждым из пользователей.

После этого каждый пользователь должен самостоятельно загружать обновления к своему брандмауэру, что в масштабе корпоративной сети приводит к значительному избыточному Интернет-трафику.

До настоящего времени ни один брандмауэр не имел средств, обеспечивающих простую массовую установку на рабочие станции и последующую настройку. Outpost Network Security был разработан специально для того, чтобы облегчить администраторам защиту своих сетей от атак со всех возможных направлений. Эта система позволяет:

- Автоматически устанавливать на клиентские компьютеры и настраивать клиентский брандмауэр, основанный на Outpost Firewall Pro - наиболее популярном в мире брандмауэре. Благодаря этому вы получаете возможность защитить компьютеры своей сети от всех известных Интернет-угроз с помощью испытанных технологий Agnitum.
- Изменять конфигурации брандмауэров клиентов в соответствии с корпоративной политикой безопасности. Если пользователям разрешено вносить собственные изменения, Outpost Network Security позволяет перезаписывать эти изменения или сохранять их по вашему выбору.

- Централизованно управлять защитой отдельных рабочих станций (с сервера или выделенной рабочей станции), создавать и автоматически развертывать конфигурации защиты, а также устранять неполадки и контролировать процесс установки брандмауэра на каждом из компьютеров.
- Загружать одну копию обновления и устанавливать ее одновременно на все клиентские компьютеры, сокращая расходы на Интернет-трафик.

Системные требования

Компоненты

В состав Outpost Network Security, помимо клиентского брандмауэра, входят следующие средства администрирования:

- Командный центр Agnitum - основное средство администрирования, позволяющее контролировать установку клиентского брандмауэра по сети и управлять прочими компонентами продукта.
- Редактор конфигурации - средство, предназначенное для создания и изменения конфигураций клиентского брандмауэра.
- Agnitum Update Service - средство централизованного обновления брандмауэров клиентов (обновление загружается один раз и устанавливается на множество компьютеров).
- Agnitum Publisher Service - средство, обеспечивающее публикацию конфигураций брандмауэра и их передачу.

Системные требования

Outpost Network Security не обязательно устанавливать на сервер или контроллер домена. Для этого подойдет любая выделенная рабочая станция с Microsoft Windows 2000 или более поздней.

Клиентская часть Outpost Network Security может быть установлена на любом компьютере с Windows 98/2000/XP или Windows Server 2003.

Защита клиентских компьютеров: Шаг за шагом

Для настройки защиты рабочих станций при помощи Outpost Network Security необходимо выполнить перечисленные ниже операции. После этого сеть будет полностью защищена от всех известных Интернет-угроз.

Установка Outpost Network Security

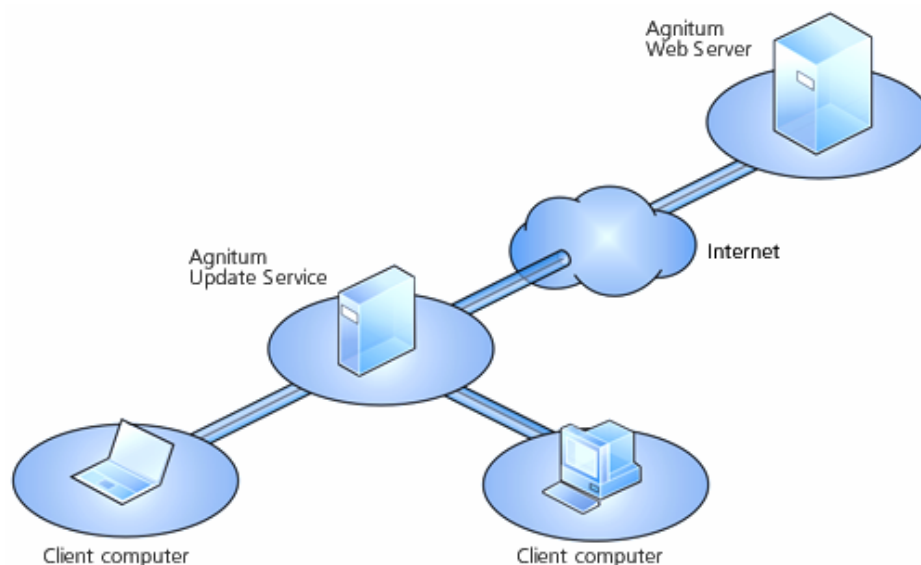
Первый шаг - установка средств администрирования и управления. Главное средство администрирования - Командный центр Agnitum - реализовано в виде оснастки ММС. С его помощью вы можете управлять установкой Outpost Network Security Client по сети и контролировать другие компоненты Outpost Network Security (Редактор конфигурации - средство создания и настройки параметров брандмауэров; Agnitum Update Service и Agnitum Publisher Service - службы обновления брандмауэров и публикации настроек). Командный центр Agnitum не обязательно устанавливать на сервер или контроллер домена. Его можно установить на любой выделенной рабочей станции, где будут работать Agnitum Update Service и Agnitum Publisher Service. Компьютер, на котором установлен Командный центр Agnitum, называется **консолью**.

Примечание: Outpost Network Security не осуществляет установки Outpost Network Security Client на консоль. Клиентский брандмауэр не может быть установлен на том же компьютере, что и Командный центр Agnitum.

Подробнее об установке Outpost Network Security рассказано в главе [Установка Outpost Network Security](#).

Настройка обновлений для клиентских компьютеров

После завершения установки Outpost Network Security вы можете настроить централизованные автоматические обновления таким образом, что при установке Outpost Network Security Client на пользовательских рабочих станциях все доступные обновления будут немедленно применяться, так что каждая рабочая станция и сеть в целом будут постоянно иметь максимальный уровень защищенности. Централизация обновлений сокращает сетевой трафик. Служба Agnitum Update Service обеспечивает автоматическую загрузку и установку всех доступных обновлений на всех компьютерах сети. При надлежащей настройке, служба загружает все необходимые файлы с web-сайта Agnitum по установленному расписанию и выдает эти файлы клиентам по их запросу. Когда клиент запрашивает обновление, оно автоматически загружается с консоли и устанавливается, благодаря чему экономятся мегабайты Интернет-трафика.



Служба Agnitum Update Service настраивается через Командный центр Agnitum. Подробнее об этом см. в главе [Настройка обновлений для клиентских компьютеров](#).

Развертывание Outpost Network Security Client на клиентских компьютерах

Следующий шаг состоит в развертывании Outpost Network Security Client на клиентских компьютерах в домене Active Directory (Windows 2000 и более поздних версий). Это можно сделать при помощи Групповой политики, используя политику установки программного обеспечения (**Software installation**). Поскольку политика применяется только к компьютерам, попадающим под действие объекта групповой политики (GPO), этот объект должен быть связан со всеми компьютерами, которые вы хотите защитить. В противном случае не будет применена политика и установлен Outpost Network Security Client. Созданную политику можно связать с любым компьютером, и она будет применена к нему при следующем перезапуске. Разрыв связи политики и компьютера может быть проведен как с удалением брандмауэра, так и без него.

Подробнее см. главу [Развертывание Outpost Network Security Client на клиентских компьютерах](#).

Настройка параметров защиты для клиентских компьютеров

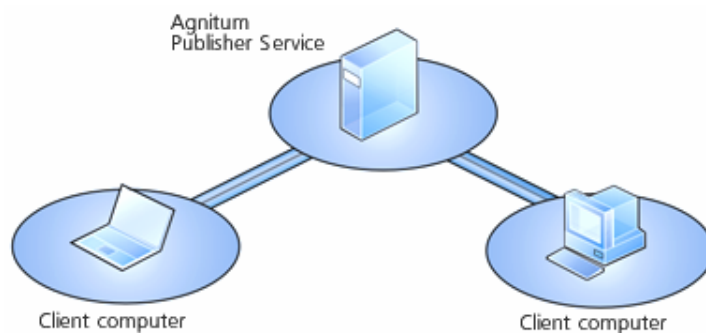
После установки Outpost Network Security Client на компьютерах пользователей можно приступить к настройке параметров безопасности. В состав Outpost Network Security входит специальное средство - Редактор конфигурации - которое позволяет указывать правила для приложений и глобальные правила, настройки обнаружения атак и все остальные параметры брандмауэра.

Подробнее об этом рассказывается в главе [Настройка параметров защиты для клиентских компьютеров](#).

Применение настроек к клиентским компьютерам

После того, как все нужные настройки будут установлены, их следует опубликовать, чтобы клиенты могли загрузить изменения в конфигурации, когда Outpost Network Security Client будет установлен на каждом компьютере.

Для этого используется служба Agnitum Publisher Service, которая управляется из Командного центра Agnitum. При публикации новой конфигурации Agnitum Publisher Service уведомляет все клиентские компьютеры о необходимости загрузить изменения в конфигурации. После загрузки конфигурация применяется без необходимости перезапуска компьютера.



Вы можете изменить конфигурацию брандмауэра и опубликовать ее для отдельных экземпляров Outpost Network Security Client в любой момент, как только в этом возникнет необходимость. Например, установив сетевое приложение на компьютерах пользователей, вы можете оперативно создать для него правило и применить его на всех клиентских компьютерах в своей сети.

Подробнее об этом см. в главе [Применение настроек к клиентским компьютерам](#).

Установка Outpost Network Security

Чтобы начать установку Outpost Network Security, запустите файл **setup.exe**. Процедура типична для большинства программ установки для Windows. Просто следуйте указаниям мастера, который установит все необходимые компоненты на вашем компьютере:

Командный центр Agnitum, Редактор конфигурации, Agnitum Update Service и Agnitum Publisher Service.

Примечание: Если вы хотите установить Командный центр Agnitum и службы на разные серверы, обратитесь к [Техническому руководству](#).

В процессе установки пакет Outpost Network Security Client будет скопирован в папку **C:\Program Files\Agnitum\Outpost Network Security\Command Center\oofclnt**, к которой автоматически открывается общий доступ, благодаря чему она становится доступна всем клиентам сети.

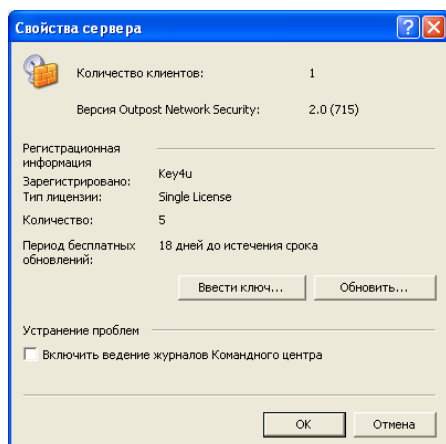
Примечание: Outpost Network Security не осуществляет установку Outpost Network Security Client на консоль. Клиентский брандмауэр не может быть установлен на том же компьютере, что и Командный центр Agnitum. Однако, если на консоли установлен какой-либо брандмауэр, убедитесь, что соединение с портом Agnitum Publisher Service не блокируется. В противном случае, клиентские компьютеры не смогут получить лицензионный ключ и нормально работать.

Важно: Для работы с Командным центром необходимы права администратора на компьютере-консоли. Убедитесь, что Вы обладаете необходимыми привилегиями.

После установки в окне **Свойства сервера** вы можете увидеть лицензионную информацию. Для открытия этого окна щелкните правой кнопкой мыши пункт **Командный центр Agnitum** и выберите **Свойства**.

Окно отображает информацию о текущей лицензии. Для обновления лицензии воспользуйтесь кнопкой **Обновить**. Вы будете перенаправлены на соответствующую страницу сайта компании Agnitum.

Вы можете также ввести новый ключ и зарегистрировать клиентские брандмауэры, щелкнув кнопку **Ввести ключ**. Новый ключ будет отправлен клиентским компьютерам вместе с файлами конфигурации, предоставленными Agnitum Publisher Service.

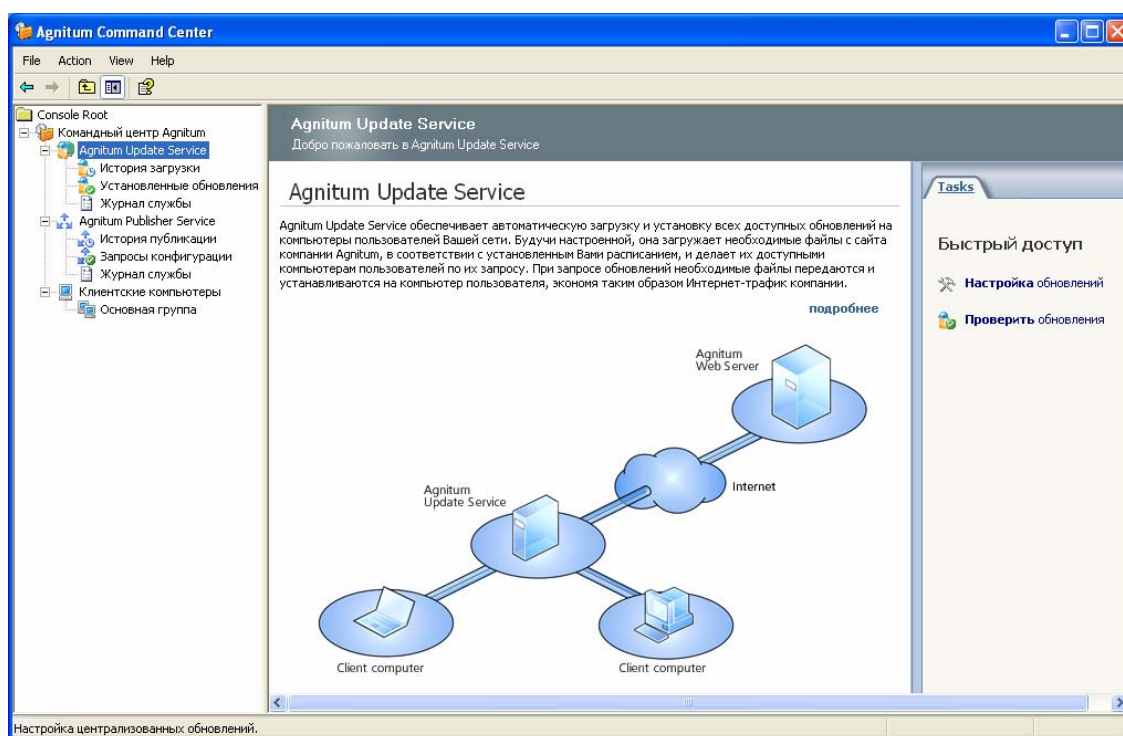


Примечание: Если не указан верный лицензионный ключ, брандмауэры на клиентских компьютерах не запускаются.

Кроме того, вы можете включить ведение журнала Командного центра, выбрав соответствующий флажок. В случае проблем при работе с продуктом, журналы могут быть предоставлены в службу технической поддержки компании Agnitum и помогут решить ваши проблемы.

Настройка обновлений для клиентских компьютеров

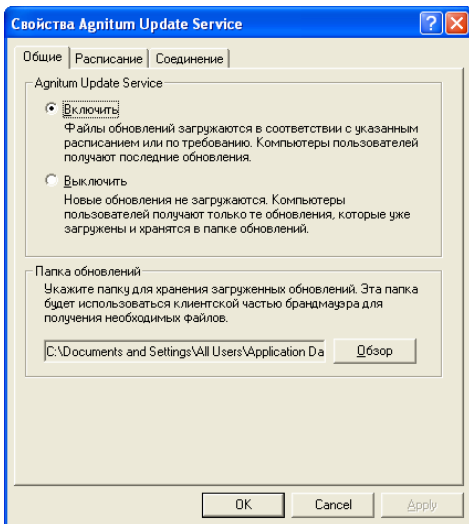
Изменение параметров обновления осуществляется через Командный центр Agnitum. Чтобы открыть оснастку центра, выберите пункт меню **Пуск > Программы > Agnitum > Outpost Network Security > Command Center**. В окне центра выберите пункт **Командный центр Agnitum > Agnitum Update Service** и щелкните **Настройка обновлений** в панели быстрого доступа.



Включение обновлений

Чтобы включить обновления, выберите пункт **Включить** на вкладке **Общие** диалогового окна **Свойства Agnitum Update Service**. Включение обновлений означает, что они будут автоматически загружаться ежечасно (если клиентский брандмауэр не работает в Режиме блокировки), в соответствии с установленным расписанием или по требованию, после чего будут передаваться на каждый клиентский компьютер и применяться к нему. Отключение обновлений означает, что новые обновления не будут загружаться и клиенты на свои запросы смогут получить только уже загруженные файлы.

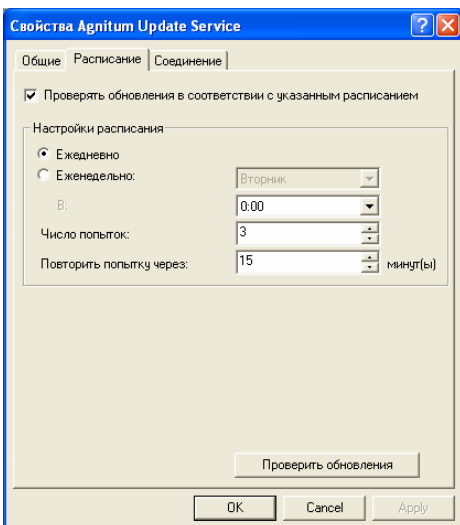
Примечание: Файлы обновлений могут быть переданы клиентам только после того, как они будут загружены полностью.



Вы можете указать папку для хранения загруженных обновлений.

Планирование обновлений

Чтобы запланировать загрузку обновлений в определенное время, переключитесь на вкладку **Расписание** и проверьте, что установлен флажок **Проверять обновления в соответствии с указанным расписанием**. Вы можете запланировать либо ежедневную, либо еженедельную загрузку обновлений и указать количество попыток и интервал между ними. Попытка считается успешной в том случае, если обновление загружается полностью.



Вы можете выполнить немедленную проверку наличия обновлений, щелкнув кнопку **Проверить обновления**.

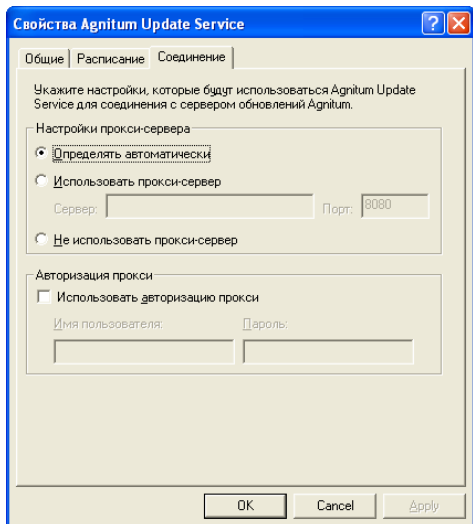
Настройка параметров соединения

Чтобы задать параметры соединения, которые будут использоваться службой Agnitum Update Service при подключении к серверу обновлений Agnitum, переключитесь на вкладку **Соединение**.

Если для подключения к Интернету используется прокси-сервер, установите переключатель **Определять автоматически**, чтобы включить автоматическое

определение параметров прокси-сервера. Можно выбрать переключатель **Использовать прокси-сервер** и указать адрес и порт прокси-сервера явным образом. Если прокси-сервер не используется, выберите переключатель **Не использовать прокси-сервер**.

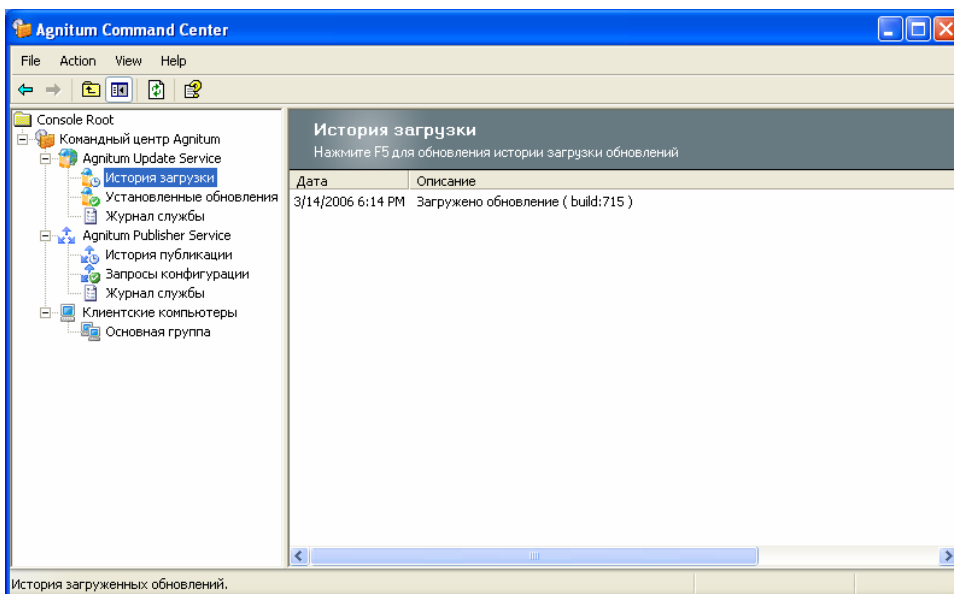
Если прокси-сервер требует авторизации, установите флажок **Использовать авторизацию прокси** и введите учетные данные для регистрации.



Контроль статистики обновления

Командный центр Agnitum позволяет администратору контролировать загрузку обновлений и их применение к определенным компьютерам.

Выберите пункт **История загрузки** в левой панели. При этом в правой панели будет отображен список всех загруженных обновлений с указанием даты и описанием. Узел **Установленные обновления** содержит список обновлений, примененных к конкретным компьютерам. **Журнал службы** содержит список событий, зарегистрированных службой.



Примечание: Обратите внимание, что обновления передаются на компьютер клиента и применяются только по его запросу. Если брандмауэр клиента отключен (не путать с

политикой **Режим бездействия**), он не будет обновляться до тех пор, пока не будет включен снова.

Развертывание Outpost Network Security Client на клиентских компьютерах

Если количество клиентских компьютеров невелико, вы можете установить Outpost Network Security Client на каждом из них вручную (файл с установочным пакетом клиентского брандмауэра называется **agnitum Outpost Network Security Client.msi** и находится в папке **C:\Program Files\Agnitum\Outpost Network Security\Command Center\oofclnt**, общий доступ к которой открывается в процессе установки; подробнее см. **Руководство по сопровождению Outpost Network Security Client**). Если компьютеров много, процесс установки можно автоматизировать. Как только установочный файл клиентского брандмауэра будет сделан доступным по сети, вы сможете воспользоваться политикой установки программного обеспечения (**Software installation**) для назначения этого установочного пакета нужным компьютерам. Для этого:

1. Откройте объект групповой политики для редактирования.
2. Установите брандмауэр при помощи политики установки программного обеспечения.
3. Свяжите объект групповой политики с нужными компьютерами.

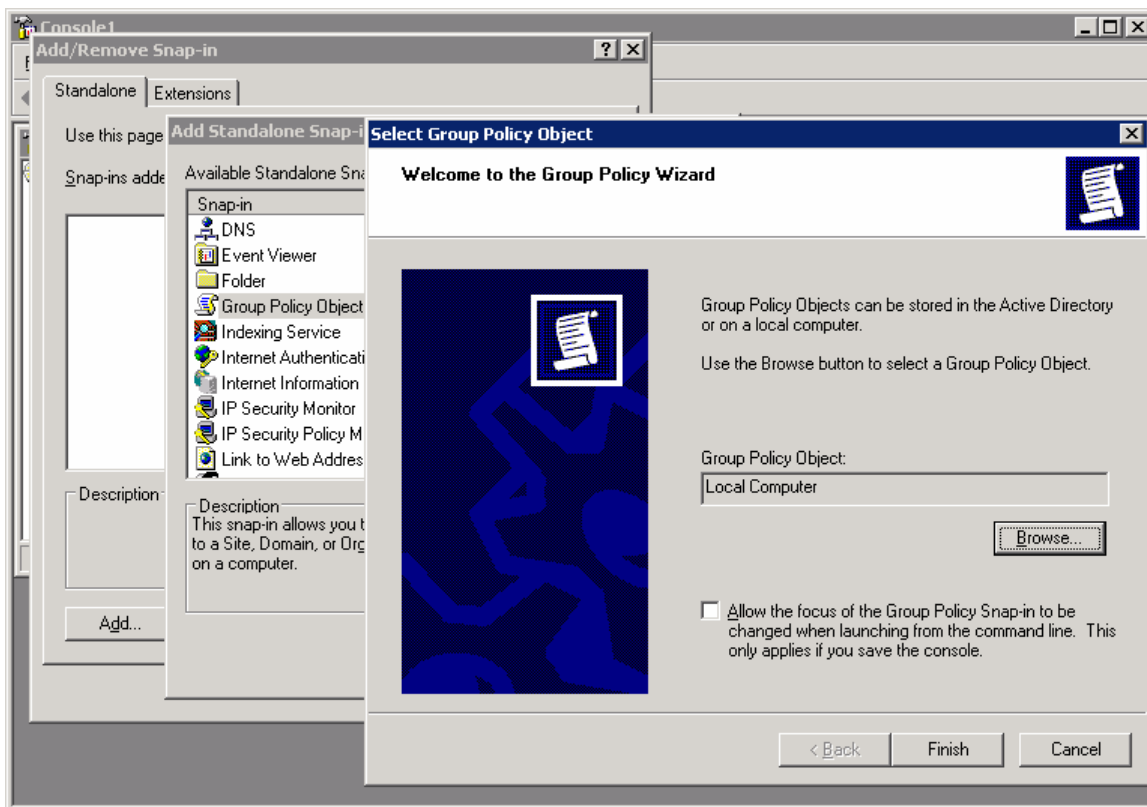
Ниже вы найдете подробное описание действий для каждого из трех перечисленных выше этапов.

Примечание: Предыдущие версии Outpost Firewall нужно обязательно удалить вручную со всех компьютеров, которые планируется защищать централизованно. Автоматический перенос конфигураций со старых версий в этом случае выполнен не будет. Кроме того, перед установкой Outpost Network Security Client убедитесь, что с компьютеров удалены все другие брандмауэры, и перезагрузите системы во избежание конфликтов между программами при попытке контроля сетевого доступа.

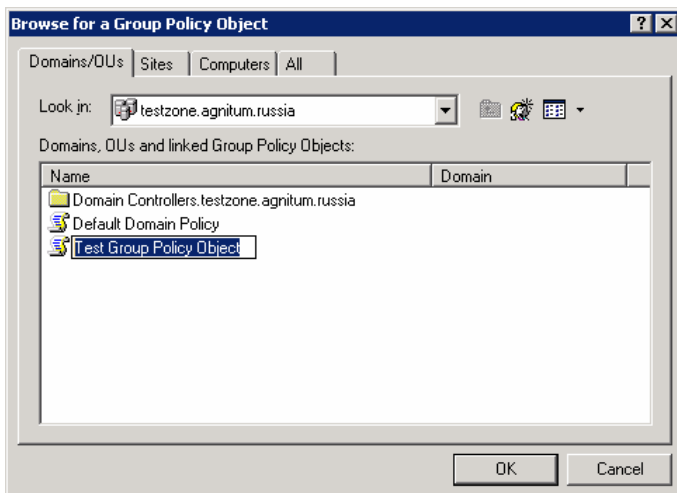
Примечание: О развертывании Outpost Network Security в доменах Windows NT и на клиентах с версиями Windows, младше, чем 2000, рассказывается в [Техническом руководстве](#).

Открытие объекта групповой политики для редактирования

Запустите консоль MMC (**Пуск > Выполнить > MMC > ОК**) и добавьте в консоль оснастку **Редактор групповой политики** (Group Policy Editor), для чего выберите пункт меню **Файл > Добавить/удалить оснастку**, щелкните кнопку **Добавить** и выберите из списка **Объект групповой политики**. Щелкните кнопку **Добавить**. После этого вам будет предложено выбрать объект групповой политики для редактирования.



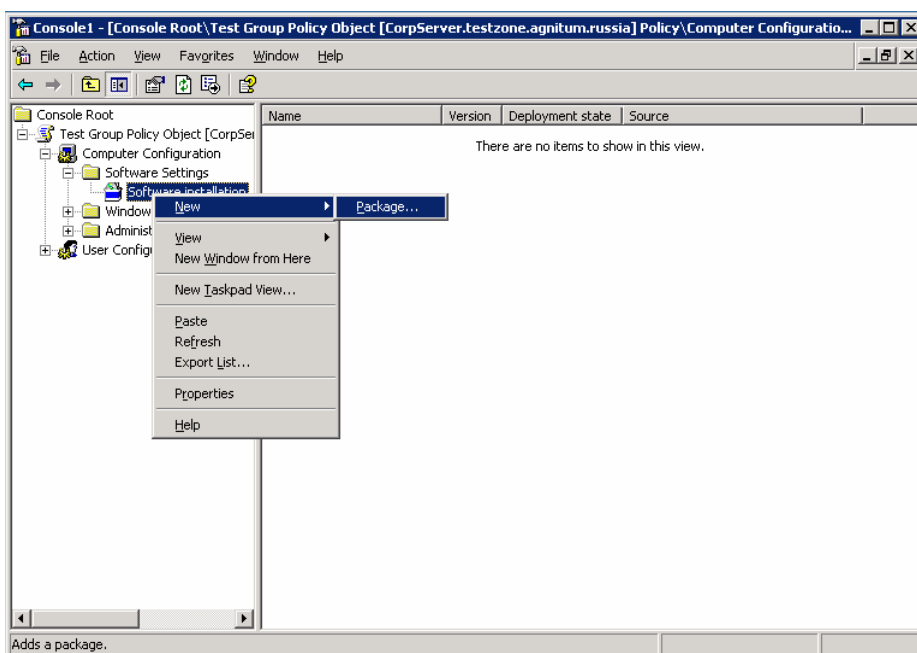
Щелкните кнопку **Обзор**, чтобы выбрать объект групповой политики. Вы можете создать новый объект, щелкнув на кнопке **Создать**, или выбрать существующий объект (например, **Default Domain Policy**).



Щелкните кнопку **ОК**, затем **Готово** и **Закреть**, чтобы закрыть открытые окна. После щелчка на кнопке **ОК** запускается редактор групповой политики, с помощью которого вы можете редактировать выбранный объект.

Использование политики установки программного обеспечения для развертывания Outpost Network Security Client

В процессе установки Outpost Network Security создается папка с установочными файлами клиентского брандмауэра, к которой открывается доступ по сети. Затем вы должны настроить политику установки программного обеспечения, чтобы назначить установку брандмауэра на выбранные компьютеры. Щелкните правой кнопкой мыши на узле **Установка программ** в разделе **Конфигурация компьютера > Конфигурация программ** и выберите пункт контекстного меню **Создать > Пакет**.

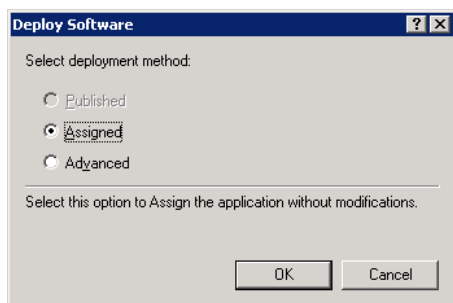


Перейдите в папку с установочными файлами (по умолчанию это папка `\\<ИмяКонсоли>\oofclnt`) и выберите установочный пакет клиентского брандмауэра.

Примечания: Вы должны указать путь универсальный (UNC) к установочному пакету, например, `\\server\ oofclnt`.

Если установочная папка размещена на томе NTFS, вы также должны установить соответствующие разрешения вручную, чтобы эта папка стала доступна клиентам. Убедитесь также, что клиенты имеют разрешение на чтение установочного пакета клиентского брандмауэра.

В диалоговом окне **Deploy Software** выберите переключатель **Назначить** и щелкните кнопку **ОК**.

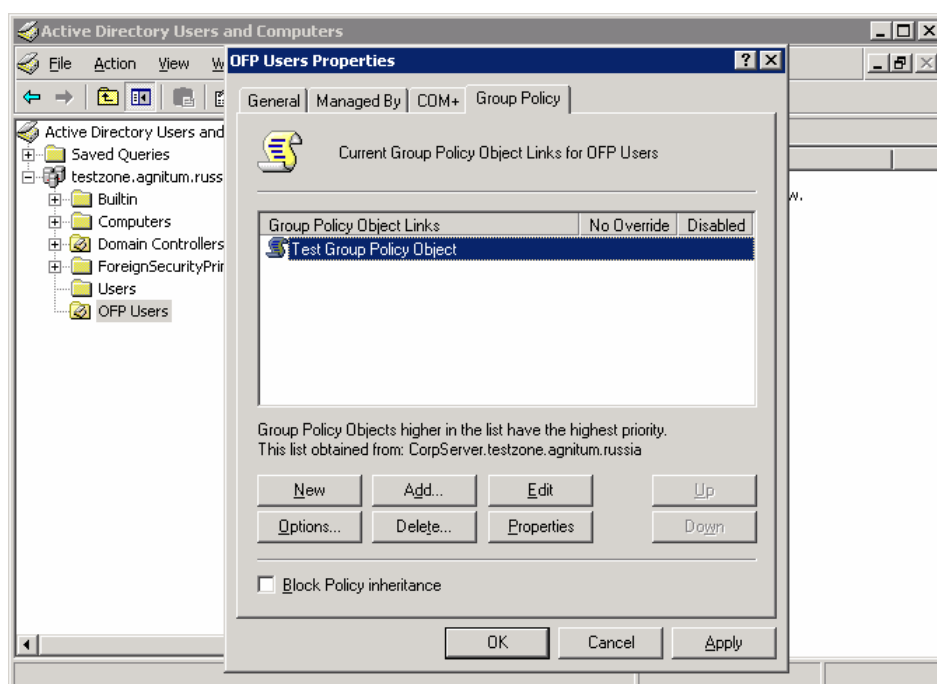


В правой панели консоли MMC вы увидите запись с установочным пакетом брандмауэра. Клиентский брандмауэр будет устанавливаться на выбранные компьютеры при их очередном включении, независимо от того, какой именно пользователь войдет в систему (если объект групповой политики связан с компьютером).

Примечание: Подробные сведения об управлении развертыванием программного обеспечения при помощи групповых политик читайте в документации, описывающей администрирование групповых политик.

Привязка объекта групповой политики

Привязка объекта групповой политики выполняется из оснастки *Active Directory Users and Computers* в том случае, если связь должна быть установлена с доменами или подразделениями (OU), или из оснастки *Active Directory Sites and Services*, если связь должна быть установлена с сайтами. Щелкните правой кнопкой на сайте, домене или подразделении, с которым должен быть связан объект групповой политики, и выберите пункт контекстного меню **Свойства**. На вкладке **Групповая политика** щелкните кнопку **Добавить** и выберите нужный объект групповой политики. После того, как вы дважды подтвердите свои действия, нажав кнопку **ОК**, объект групповой политики будет связан с выбранным объектом Active Directory.



Примечания: Подробнее о привязке объектов групповой политики и фильтрации их области применения читайте в документации, описывающей администрирование групповых политик.

Для привязки политики вы можете воспользоваться также консолью **Управление групповой политикой**. Для этого ваша учетная запись должна иметь права на **Управление ссылками групповой политики** для сайта, домена или подразделения.

Клиентский брандмауэр может быть развернут и при помощи сценариев входа в систему. Подробнее об этом см. в [Техническом руководстве](#).

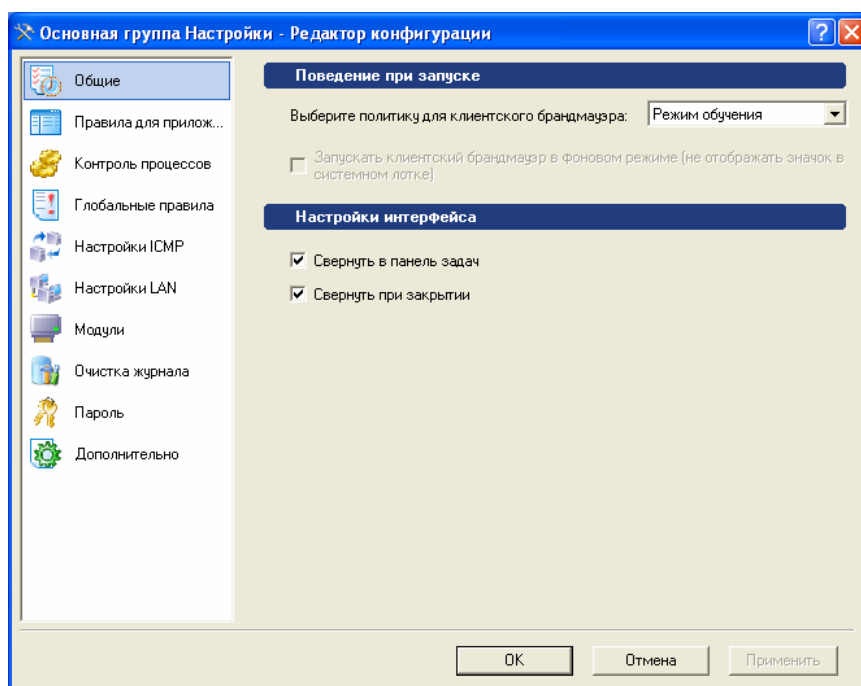
Настройка параметров безопасности на клиентских компьютерах

Информацию о клиентских компьютерах, зарегистрированных на консоли, вы можете увидеть, щелкнув узел **Клиентские компьютеры** в дереве Командного центра. Все клиентские компьютеры объединяются в группы под этим узлом. После установки клиент автоматически попадает в **Основную группу**.

Подробнее об объединении компьютеров в группы см. [Управление группами компьютеров](#).

Параметры брандмауэра на клиентских компьютерах настраиваются с помощью специального средства - **Редактора конфигурации**. Для его вызова щелкните группу правой кнопкой мыши и выберите **Настройки безопасности**.

С помощью этого средства вы получаете доступ ко всем параметрам Outpost Network Security Client на компьютерах выбранной группы, поэтому процесс покажется администраторам, знакомым с предыдущими версиями Outpost Firewall, простым и быстрым.



После установки всех параметров вы можете немедленно опубликовать созданную конфигурацию для всех компьютеров, щелкнув кнопку **Опубликовать**.

Все доступные параметры, включенные в удаленную конфигурацию, обсуждаются в последующих подразделах. Более подробное описание каждого из них вы можете найти в **Руководстве пользователя Outpost Network Security Client**.

Общие настройки

Эта вкладка позволяет вам выбрать политику, которая должна использоваться клиентскими брандмауэрами, а также режим, в котором они должны работать. По умолчанию брандмауэр работает в фоновом режиме, чтобы не беспокоить пользователей, экономить системные ресурсы. Кроме того, благодаря этому администратор может блокировать нежелательный трафик или содержимое незаметно для пользователя. По умолчанию используется политика **Режим разрешения**.

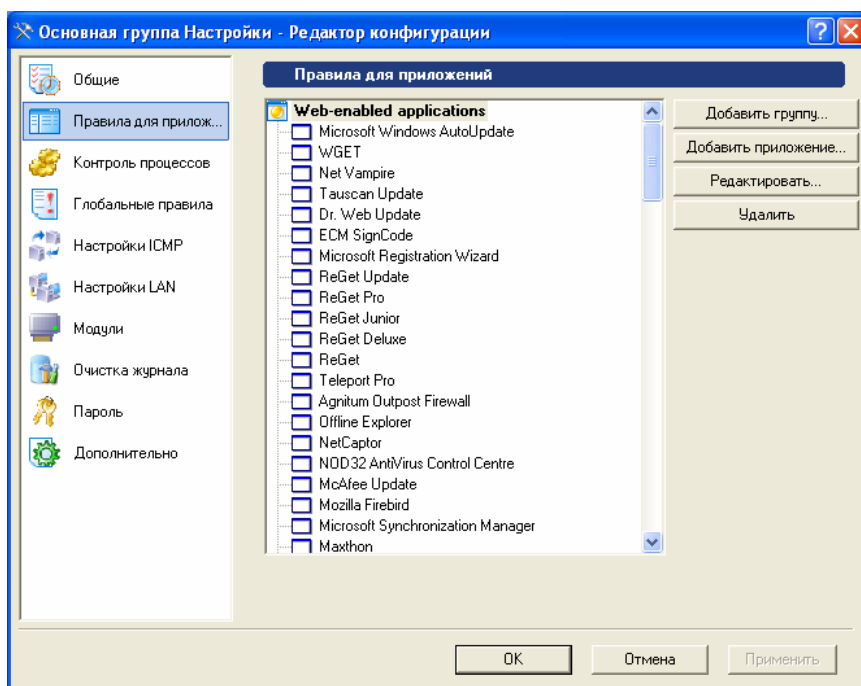
Если некоторые пользовательские приложения, требующие доступа к сети, при этом блокируются, а вы считаете пользователя достаточно опытным, чтобы правильно реагировать на все запросы, связанные с разрешением или запрещением доступа к сети, вы можете отключить фоновый режим и включить **Режим обучения** на компьютере этого пользователя.

Кроме того, вы можете сделать так, чтобы главное окно брандмауэра сворачивалось в значок в системном лотке.

Правила для приложений

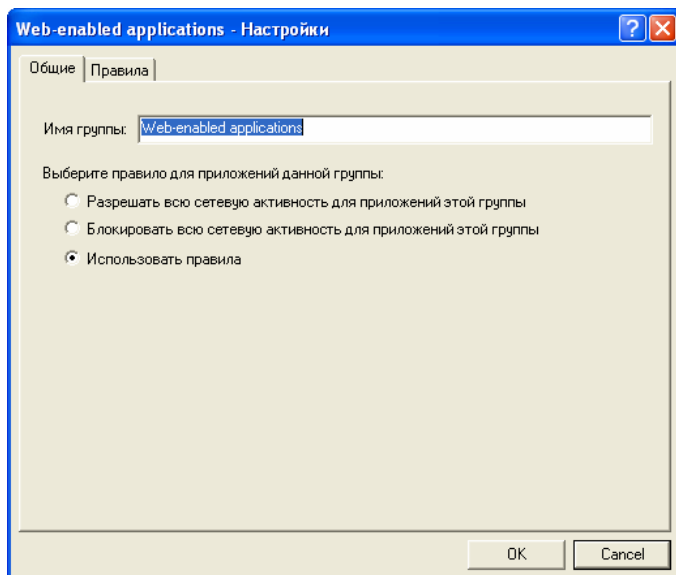
На странице **Правила для приложений** вы можете указать, какие приложения на компьютере пользователя могут иметь доступ к сети, а какие нет. Вы можете видеть список наиболее распространенных сетевых приложений, объединенных в группы по типу своей активности.

Во время применения конфигурации, Outpost Network Security Client сопоставляет приложения, установленные на компьютере пользователя, с указанными в конфигурации с помощью указанного критерия соответствия и при совпадении, создает соответствующие правила для приложения.



Редактор конфигурации предлагает предустановленные по умолчанию наборы правил для наиболее известных приложений, которые Вы можете изменять, добавляя новые правила для клиентских приложений и редактируя/удаляя существующие.

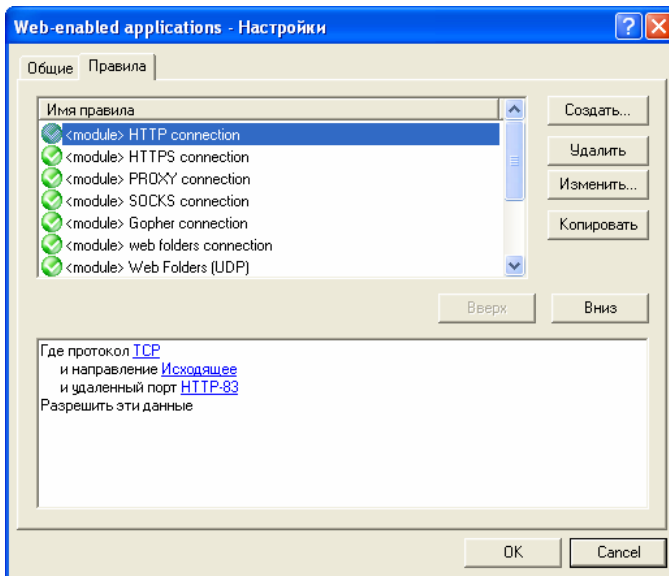
Выберите группу в списке и щелкните кнопку **Редактировать**. Откроется окно настроек группы, позволяя вам изменить правила для приложений данной группы.



На вкладке **Общие** вы можете указать имя группы и правило, в соответствии с которым приложениям данной группы на компьютере пользователя будет дан сетевой доступ. Вы можете:

- **Разрешить всю сетевую активность для этого приложения** – вся сетевая активность для данного приложения будет разрешена. Это правило рекомендуется только для приложений, которым вы полностью доверяете.
- **Блокировать всю сетевую активность для этого приложения** – вся сетевая активность для данного приложения будет заблокирована. Рекомендуется выбирать это правило для приложений, которым не требуется соединение с Интернет: текстовые редакторы, калькуляторы и т.д.
- **Создать правила** - Outpost Network Security Client будет разрешать доступ в сеть для этого приложения на основе созданных вами правил. Только указанная сетевая активность будет разрешена. Рекомендуется выбирать это правило для большинства ваших приложений.

Вкладка **Правила** позволит вам указать правила для приложений данной группы.

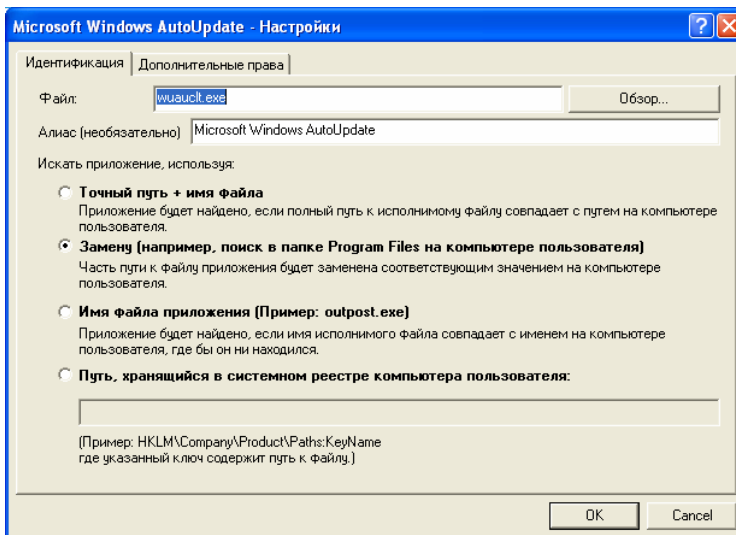


Редактирование правил осуществляется точно так же, как в Outpost Network Security Client. Подробнее о создании правил для приложений см. в **Руководстве пользователя Outpost Network Security Client**.

Щелкните **OK** для сохранения настроек группы после редактирования.

Примечание: Настройки групп **Доверенные** и **Заблокированные** изменить нельзя.

Для редактирования настроек приложения, выберите приложение в списке и нажмите **Редактировать**. Открывшееся окно позволит вам изменить критерий соответствия и дополнительные права для приложения.

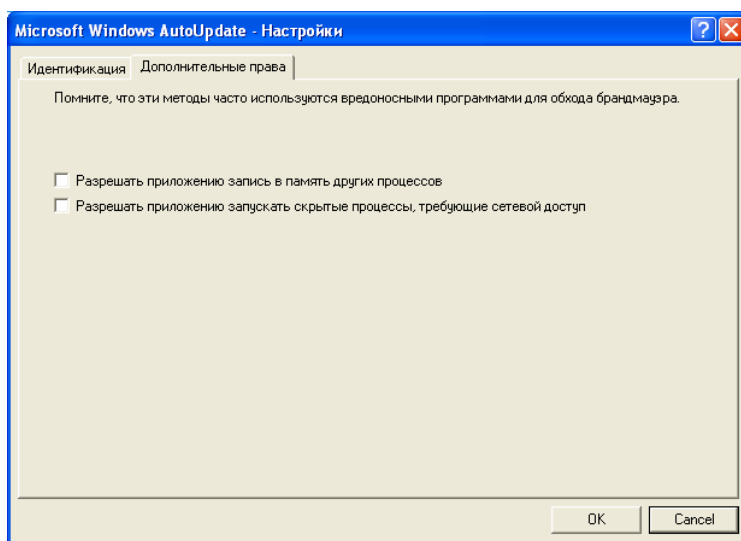


На вкладке **Идентификация** вы можете изменить имя и расположение исполнимого файла приложения, указать алиас, который будет использоваться вместо имени файла для

именования приложения и критерий соответствия для идентификации приложения на компьютере пользователя. Вы можете выбрать один из следующих критериев:

- **Точный путь + имя файла** – для поиска приложения по полному пути к его исполняемому файлу.
- **Замена** – если приложение установлено в одну из стандартных папок (например, **Program Files** или **Windows\System32**), путь к этой папке на консоли будет заменен на путь к аналогичной папке на клиентском компьютере.
- **Имя файла приложения** – поиск приложения будет вестись по имени файла приложения, где бы он ни находился на клиентском компьютере.
- **Путь, хранящийся в системном реестре компьютера пользователя** – путь к приложению будет взят из указанного ключа системного реестра на компьютере пользователя. Если ключ не указан, то поиск файла приложения ведется в ключе **HKLM\Software\Microsoft\Windows\ CurrentVersion\App Paths**.

На вкладке **Дополнительные права**, вы можете позволить приложению выполнять такие действия как запуск скрытых процессов и изменение памяти процессов. Однако, стоит помнить о том, что эти приемы могут быть использованы вредоносными программами для обхода защиты брандмауэра.



Подробнее об этих приемах см. Руководство пользователя **Outpost Network Security Client**.

Вы также можете создавать свои группы со своими приложения в соответствии с вашими требованиями. Для добавления новой группы/приложения щелкните **Добавить группу/Добавить приложение** и следуйте шагам мастера, указывая описанные выше настройки. Щелкнув **Готово**, вы увидите новую группу/приложение в списке. Приложения добавляются в выбранную в текущий момент группу.

Для перемещения приложения или всех приложений группы в другую группу используйте команды **Переместить в** и **Переместить приложения в** в контекстном меню приложения или группы соответственно.

Щелкните **Удалить**, чтобы удалить выбранное приложение или группу из списка.

Примечание: В зависимости от настроек на вкладке **Дополнительно**, правила из опубликованной конфигурации могут объединяться с правилами, существующими на клиентском компьютере, или заменять их. См. главу [Дополнительно](#).

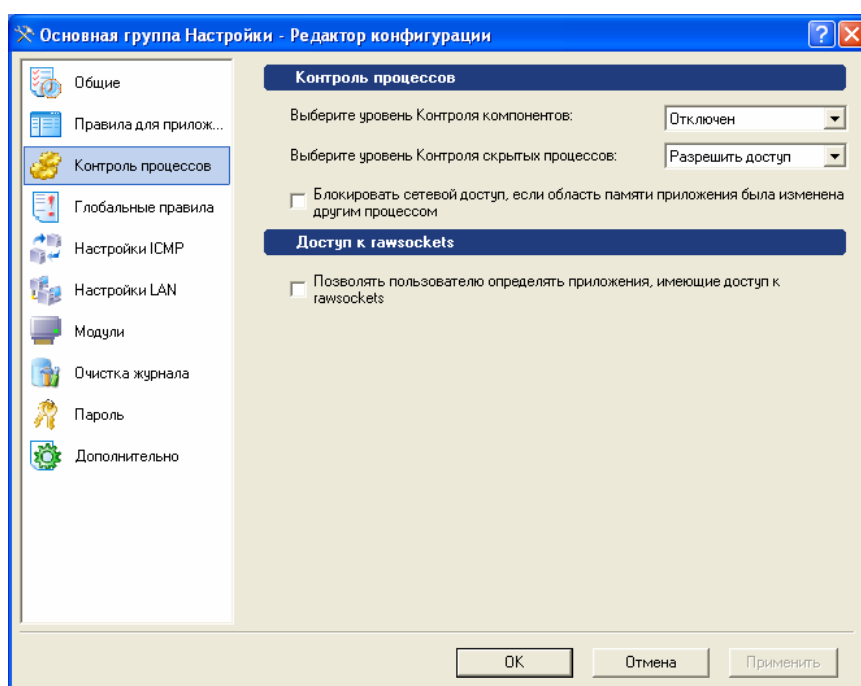
Контроль процессов

Вкладка **Контроль процессов** позволяет управлять дополнительными средствами защиты, входящими в состав Outpost Network Security Client, такими как Контроль компонентов, Контроль скрытых процессов и Open Process Control. Эта защита по умолчанию отключена, но если вы считаете пользователей достаточно опытными, чтобы справиться с огромным количеством запросов на обращение к сети, вы можете включить ее.

Контроль компонентов следит за компонентами каждого приложения, проверяя, чтобы вместо них не были загружены имитирующие их модули, написанные злоумышленниками. Установить требуемый уровень контроля за компонентами вы можете с помощью раскрывающегося списка.

Контроль скрытых процессов позволяет управлять процессами, которые запускаются от имени доверенного приложения, чтобы эти процессы не могли выполнять запрещенные действия. Вы можете выбрать требуемую политику для скрытых процессов при помощи соответствующего раскрывающегося списка.

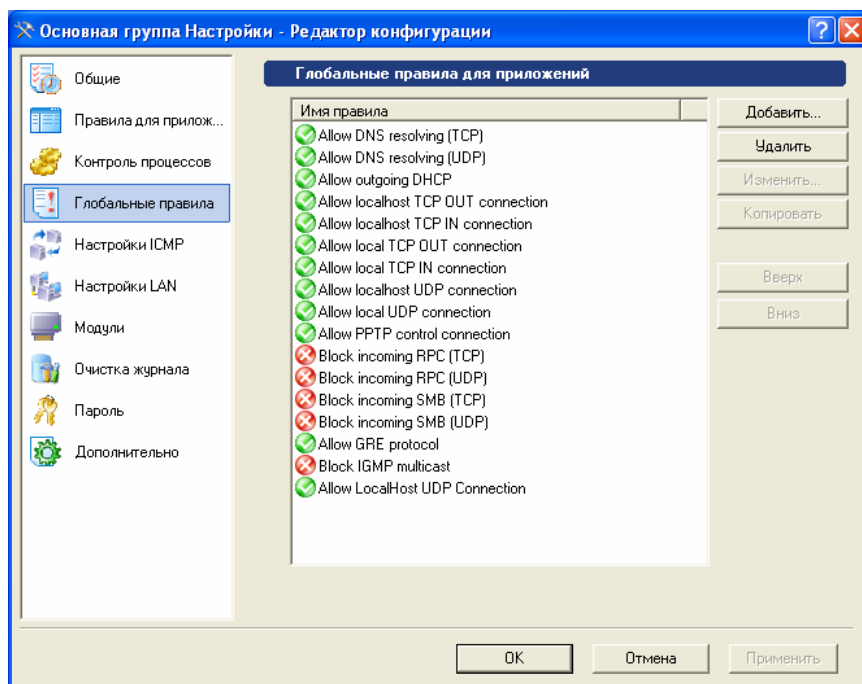
Open Process Control позволяет вам контролировать функции, которые могут использоваться для внедрения написанного злоумышленником кода в адресное пространство доверенного приложения, и тем самым предотвращает неконтролируемое изменение области памяти процесса другими процессами. Установите флажок **Блокировать сетевой доступ если область памяти приложения была изменена другим процессом**, чтобы включить эту технологию обеспечения сетевой безопасности.



Кроме того, имеется возможность позволить пользователю определять список приложений, которым разрешены вызовы функций для работы с rawsocket (это сокеты самого низкого уровня). Для этого установите соответствующий флажок.

Глобальные правила

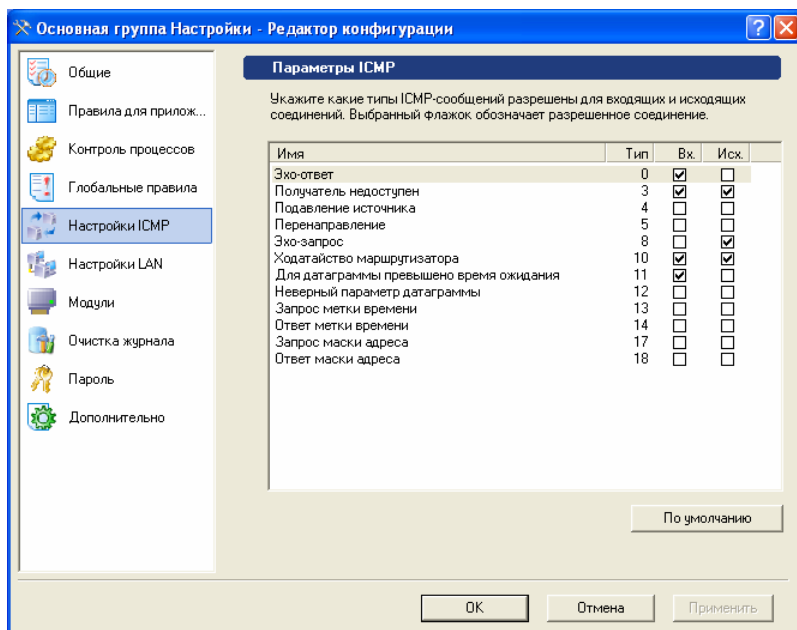
Вкладка **Глобальные правила** позволяет вам создавать глобальные правила, которые будут иметь высокий приоритет для всех приложений. Щелкните кнопку **Добавить**, чтобы создать новое правило, или **Изменить**, чтобы редактировать существующее. Правила применяются сверху вниз. Подробнее о редактировании глобальных правил читайте в **Руководстве пользователя Outpost Network Security Client**.



Примечание: В зависимости от настроек на вкладке **Дополнительно**, правила из опубликованной конфигурации могут объединяться с правилами, существующими на клиентском компьютере, или заменять их. См. главу [Дополнительно](#).

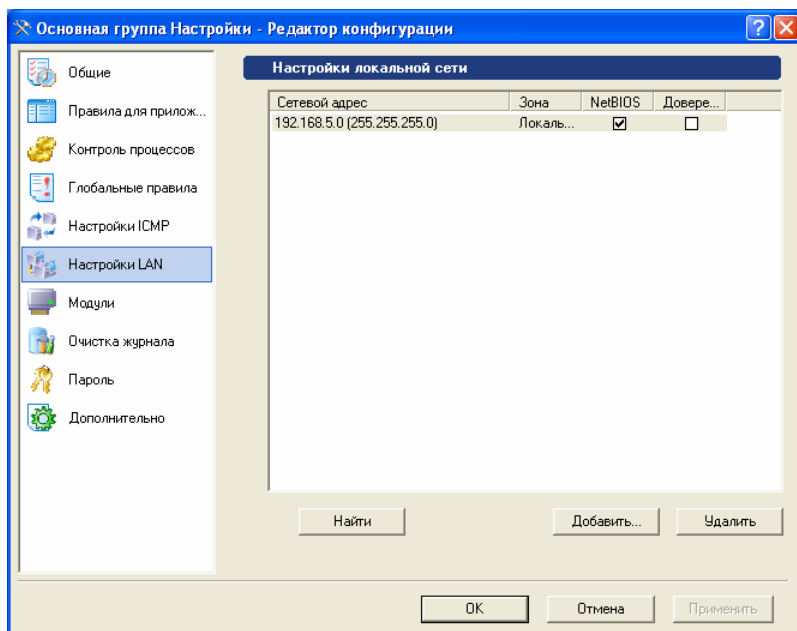
Параметры ICMP

Эти правила определяют разрешенные типы входящих и исходящих сообщений ICMP. Чтобы разрешить соединение, установите соответствующий флажок. Щелкните кнопку **По умолчанию**, чтобы вернуться к настройкам, установленным по умолчанию.

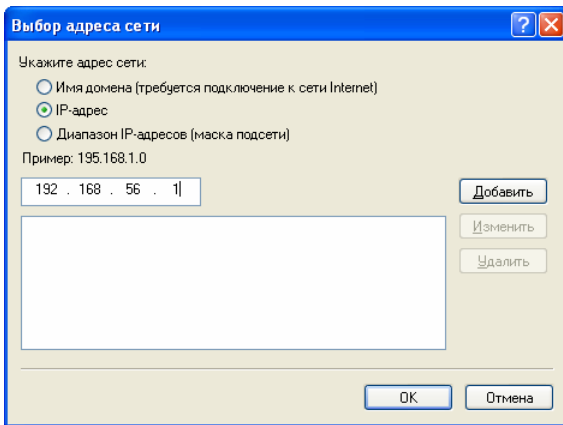


Параметры LAN

Эта вкладка позволяет вам изменять параметры локальной сети, к которой принадлежит компьютер пользователя, режим работы с NetBIOS, а также добавлять и удалять диапазоны доверенных IP-адресов.



С помощью кнопки **Найти** вы можете добавить в окно список сетей, к которым принадлежит консоль, если клиентские компьютеры принадлежат к тем же сетям. В противном случае вам придется добавлять сети, к которым принадлежат клиентские компьютеры, вручную, указывая доменное имя, IP-адрес или диапазон IP-адресов.

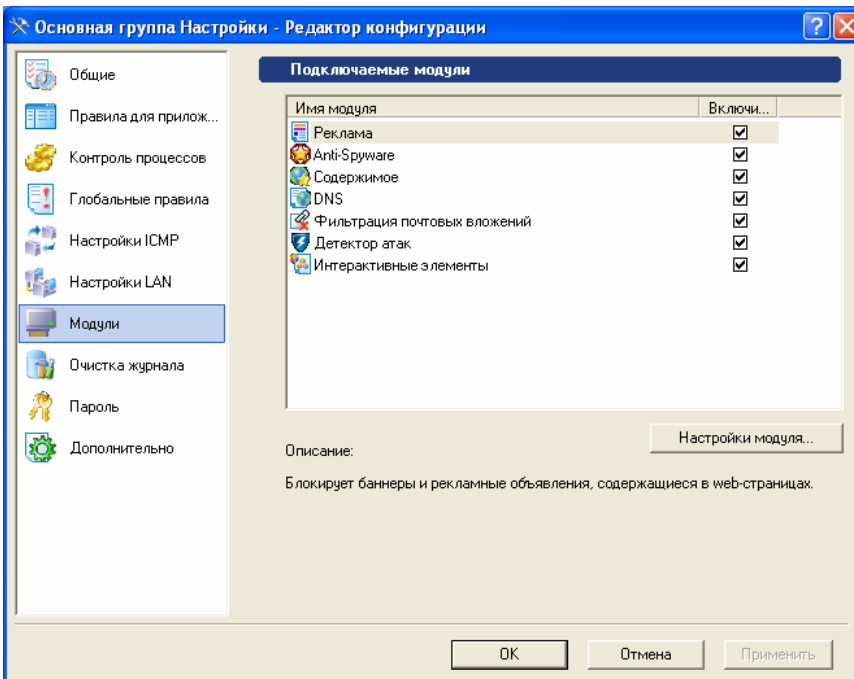


Если вы хотите разрешить все соединения для определенной сети, добавьте соответствующие сетевые адреса в список и установите соответствующий флажок в столбце **Доверенные**. Если же вы хотите удалить сетевой адрес из списка доверенных, снимите установленный около него флажок.

Если вы хотите разрешить все соединения по протоколу NetBIOS (связанные с конкретным сетевым адресом), убедитесь, что установлен флажок в столбце **NetBIOS**. Чтобы снять разрешение на взаимодействие с конкретной сетью, снимите флажки **NetBIOS** и **Доверенные**.

Подключаемые модули

Эта вкладка позволяет настраивать подключаемые модули Outpost Network Security Client на клиентских компьютерах. Выберите модуль, параметры которого вы хотите изменить, и щелкните кнопку **Настройки модуля**. Диалоговые окна параметров подключаемых модулей выглядят так же, как и в Outpost Network Security Client.

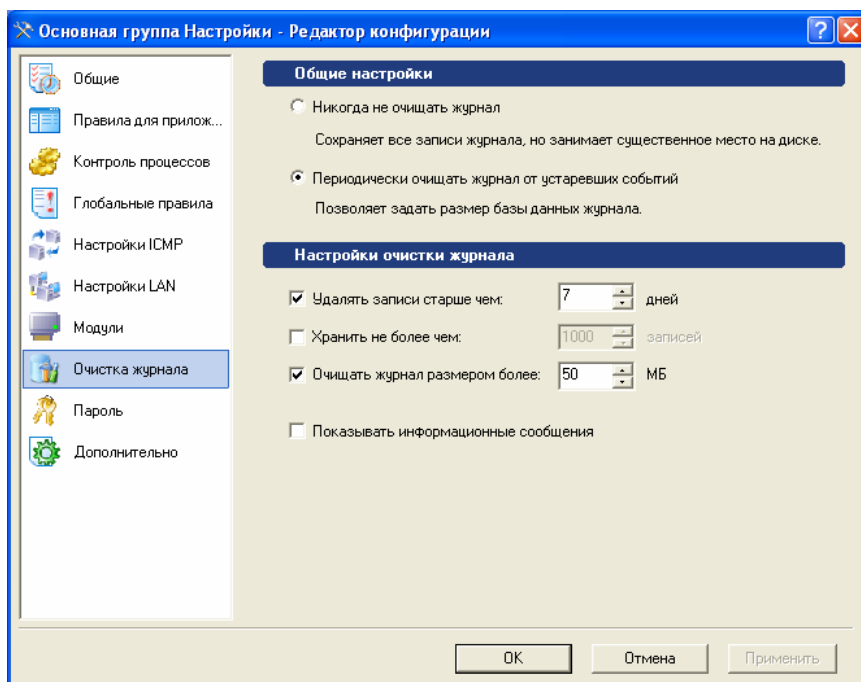


Очистка журнала

Чтобы указать параметры очистки журнала Outpost Network Security Client на клиентских компьютерах, перейдите на вкладку **Очистка журнала**. Выберите переключатель **Периодически очищать журнал от устаревших событий**, чтобы средство очистки журнала **Уборщик журнала** автоматически удаляло устаревшие записи из базы данных, или установите переключатель **Никогда не очищать журнал**, чтобы отключить Уборщик.

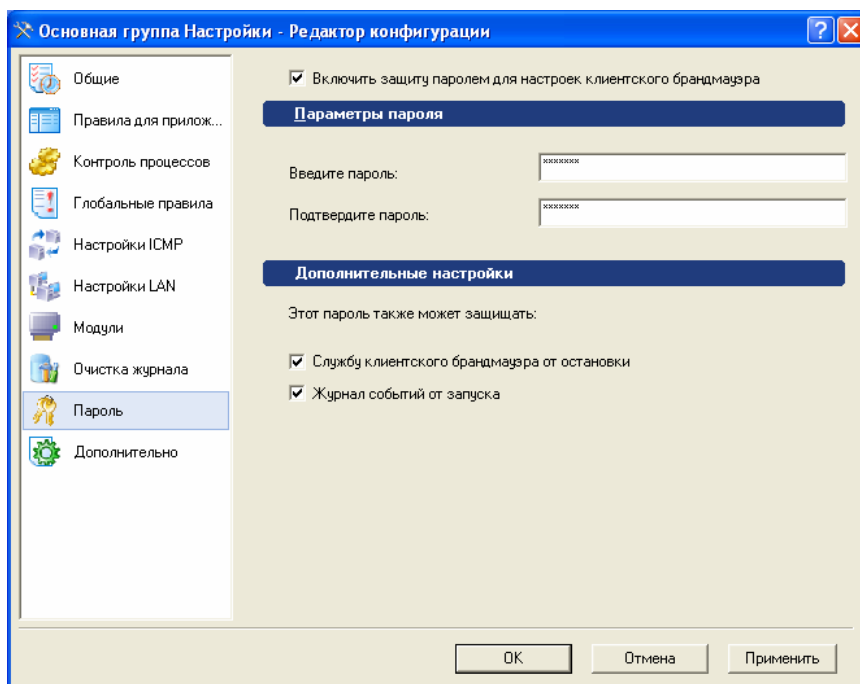
Укажите срок в днях, по истечении которого записи о событиях считаются устаревшими, а также максимальное количество свежих записей о событиях, которые должны храниться в журнале, и, наконец, **Очищать журнал размером более** - ограничение на размер базы данных Outpost Network Security Client в мегабайтах.

Установите флажок **Показывать информационные сообщения**, чтобы Уборщик отображал уведомления о процессе очистки.



Пароль

Вы можете задать пароль, чтобы помешать пользователям изменять настройки Outpost Network Security Client. Для этого перейдите на вкладку **Пароль**, выберите переключатель **Включить защиту паролем для настроек клиентского брандмауэра** и введите пароль в текстовом поле ввода. Подтвердите введенный пароль и укажите, должен ли он также использоваться для защиты службы Outpost Network Security Client от неавторизованной остановки, а также для запрета неавторизованного запуска Журнала событий.



Подробнее о том, как защитить от изменения отдельные настройки брандмауэра, см. раздел [Приоритеты](#) ниже.

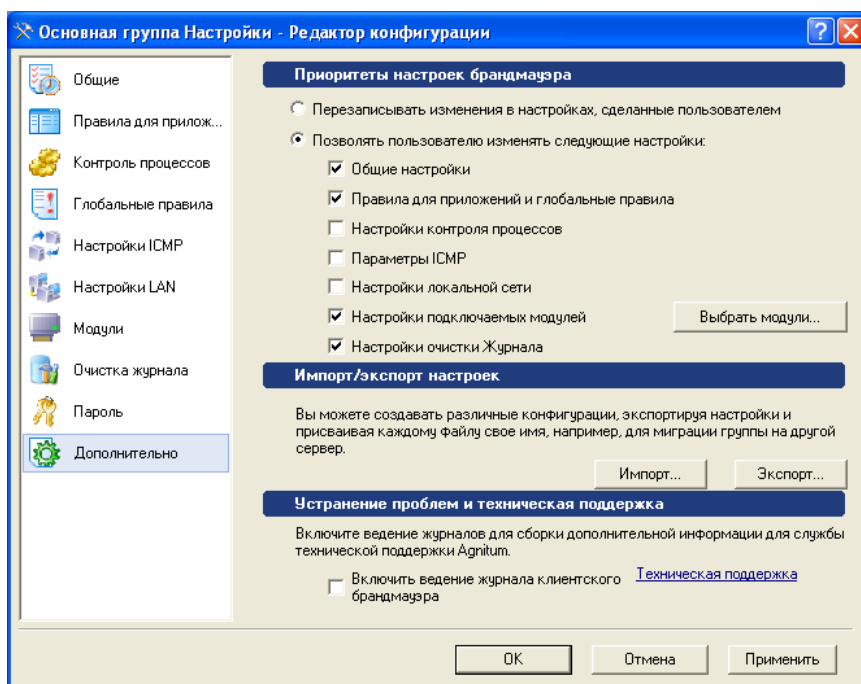
Дополнительно

Последняя вкладка позволяет указать могут ли пользователи изменять настройки брандмауэра или должны использоваться только опубликованные настройки, которые не могут быть изменены.

Выберете параметр **Перезаписывать изменения в настройках, сделанные пользователем**, если Вы не хотите, чтобы пользователи имели возможность изменять настройки брандмауэра. В этом случае, даже если настройки не защищены паролем и были изменены, они будут перезаписаны опубликованными настройками при следующем запросе конфигурации.

Если Вы хотите дать пользователям возможность влиять на настройки своих брандмауэров, выберите параметр **Позволять пользователю изменять следующие настройки** и укажите настройки, которые пользователь может изменять. Эти настройки не будут перезаписаны при применении опубликованной конфигурации.

Примечание: Если выбран флажок **Правила для приложений и глобальные правила**, правила из опубликованной конфигурации будут объединены с правилами, существующими на клиентском компьютере.



Клиент Outpost Network Security Client обладает множеством настроек. Конфигурация - это состояние, в котором находится Outpost Network Security Client в конкретный момент времени. Возможность сохранять несколько различных конфигураций позволяет вам:

- создавать разные конфигурации для клиентов;
- переключаться между этими конфигурациями;
- создавать резервные копии конфигураций.

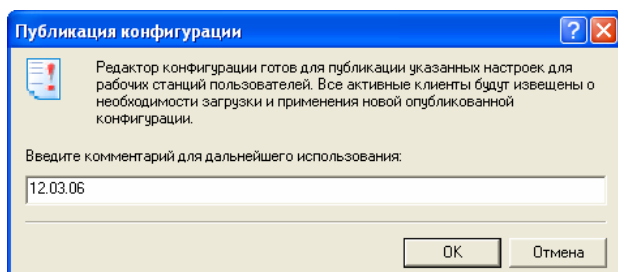
Чтобы создать несколько файлов конфигурации, достаточно дать им разные имена. Чтобы сохранить созданную конфигурацию, щелкните кнопку **Экспорт** и введите имя файла.

Для загрузки другой, заранее подготовленной, конфигурации щелкните кнопку **Импорт** и выберите нужный файл конфигурации.

Кроме того, в случае возникновения проблем при работе с продуктом Вы можете включить ведение журнала на стороне клиентского компьютера. Собранная информация может быть предоставлена в службу технической поддержки компании Agnitum для помощи при решении проблем.

Применение настроек к клиентским компьютерам

После того, как вы установили параметры клиентских брандмауэров, щелкните **ОК** в Редакторе конфигурации для публикации созданной конфигурации, чтобы клиентские компьютеры могли загрузить и применить ее. Введите комментарий к конфигурации и щелкните кнопку **ОК**. После этого клиенты будут уведомлены о новой конфигурации. Новые параметры будут загружены клиентом и применены без перезапуска компьютера.

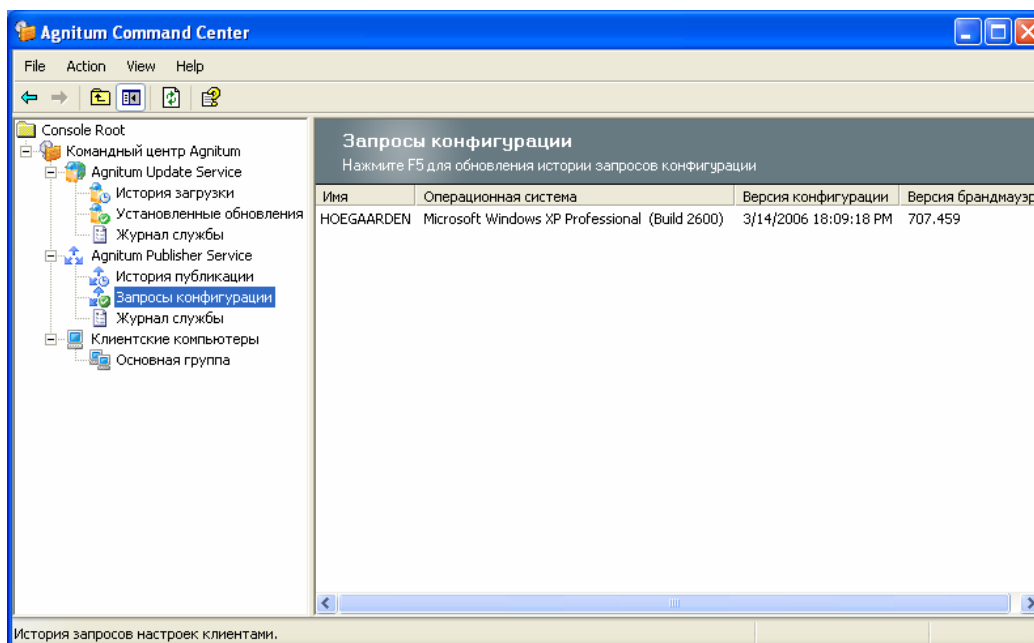


Примечание: При необходимости немедленно перезаписать все изменения, сделанные пользователем в конфигурации, воспользуйтесь командой **Перезаписать конфигурацию** в контекстном меню группы или компьютера. Вся конфигурация, независимо от настроек, будет заменена опубликованной.

Отслеживание статистики публикации

Командный центр Agnitum позволяет администратору отслеживать опубликованные конфигурации и определять, к каким компьютерам они были применены, а к каким - нет.

Выберите пункт **Agnitum Publisher Service > История публикации** в левой панели. После этого в правой панели будет выведен список всех конфигураций, которые были переданы клиентам, вместе с датой передачи и описанием. Узел **Запросы конфигурации** содержит описание текущих конфигураций отдельных компьютеров. Узел **Журнал службы** содержит журнал событий службы публикации.

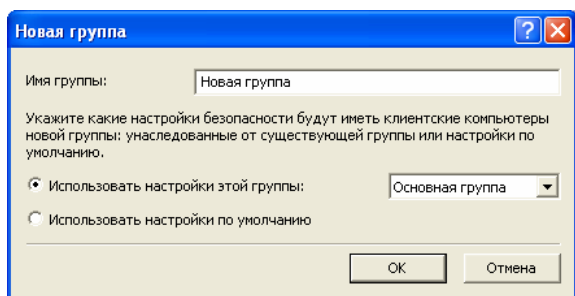


Примечание: Обратите внимание, если клиентский брандмауэр отключен (не путать с **Режимом бездействия**), клиент не сможет получить новую конфигурацию до тех пор, пока брандмауэр не будет включен снова.

Управление группами компьютеров

После регистрации на консоли все клиентские компьютеры помещаются в **Основную группу**. Если вам нужно задать различные настройки безопасности различным группам клиентских компьютеров, вы можете объединить их в группы в соответствии с вашими требованиями и назначить каждой группе отдельные настройки.

Для создания новой группы щелкните правой кнопкой мыши узел **Клиентские компьютеры** и выберите **Создать группу**. В окне **Новая группа** укажите имя новой группы, а также должна ли группа наследовать настройки безопасности от одной из существующих групп или ей должны быть назначены настройки по умолчанию.



После создания группы вы можете перенести в нее компьютеры из других групп, используя команду **Переместить** в контекстном меню компьютера. Все клиенты получат конфигурацию, опубликованную для их группы.

Удаление брандмауэра с клиентских компьютеров

Если в какой-то момент вы решите выключить защиту на одном или нескольких компьютерах, настройте групповую политику для удаления брандмауэра с клиентских машин, отсоединив объект групповой политики, отфильтровав его область применения или просто переместив учетные записи компьютеров в другой контейнер Active Directory.

Примечание: Подробнее о привязке объектов групповой политики и фильтрации их области применения читайте в документации, описывающей администрирование групповых политик.

Если брандмауэр был установлен на клиентский компьютер вручную, выберите **Выключить брандмауэр** в контекстном меню компьютера, чтобы выключить программу.