privacyware

Privatefirewall Version 7

Руководство Пользователя

(Kumga - http://forum.ru-board.com/)

http://forum.ru-board.com/topic.cgi?forum=5&topic=31543&start=660#1

Содержание

Использование Privatefirewall..... 3
Главное Меню 3
Приложения 10
Процесс Монитор 21
Обнаружение Процессов 26
Журнал Firewall 29
Отслеживание Портов 31

Настройки Privatefirewall..... 32
Основные Настройки 32
Стандартный режим Контроля……..33
Ручной режим Контроля…….. 33
Обнаружение Аномалий Email.... 39
Обнаружение Аномалий Системы 40
Обнаружение Процессов 42
Расширенные Настройки Приложения 44
Надежный Издатель 48

Обзор характеристик 48
Доступ Доверенного Издателя..... 48
Отключение Доверенного Издателя..... 49
Как работает Доверенный Издатель..... 50

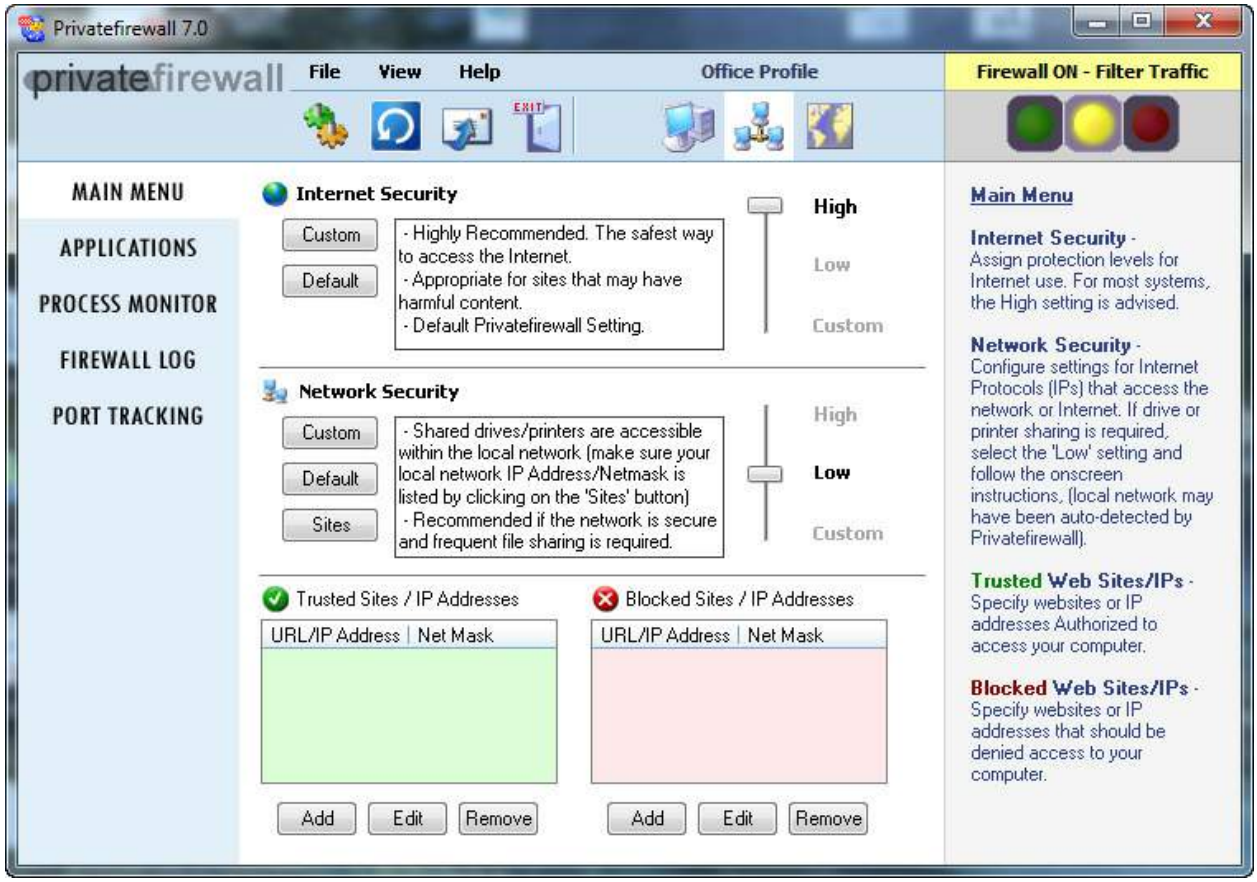
Меню и панели инструментов 57
Меню программы 57
Панель инструментов..... 61

Использование Privatefirewall

Главное Меню

(Доступно с Рабочего Стола. Нажмите кнопку Пуск /Programs/Privatefirewall 7.0/Privatefirewall 7.0)

Главное меню включают в себя элементы управления параметрами Интернет и сетевой безопасности, IP-адреса надежных сайтов и IP-адреса заблокированных сайтов. Кроме того могут поддерживаться три различных набора правил и параметров на основе текущего профиля брандмауэра, который может быть либо «Дом», «Сеть» или «Удаленный». Каждый профиль можно просмотреть, выбрав соответствующий значок профиля в верхней строке меню.



Фильтрация интернет-трафика (пакетов)

Privatefirewall контролирует входящий и исходящий Интернет-трафик. Этот трафик состоит из блоков данных, называемых «пакеты», которые могут перемещаться между любыми 2 компьютерами в Интернете или локальной сети. Пакеты могут быть разрешены, отфильтрованы или запрещены, в зависимости от желаемого уровня фильтрации.

Разрешить Интернет Трафик - это позволяет весь входящий и исходящий Интернет Трафик и обеспечивает наименьшую защиту.

Фильтр Интернет трафика (рекомендуется) – это позволяет доступ в Интернет при сохранении максимальной защиты от входящих вторжений

Примечание: Все правила по Интернет-безопасности, сетевой безопасности, и Настройки Приложения будут действовать только, если выбран этот параметр.

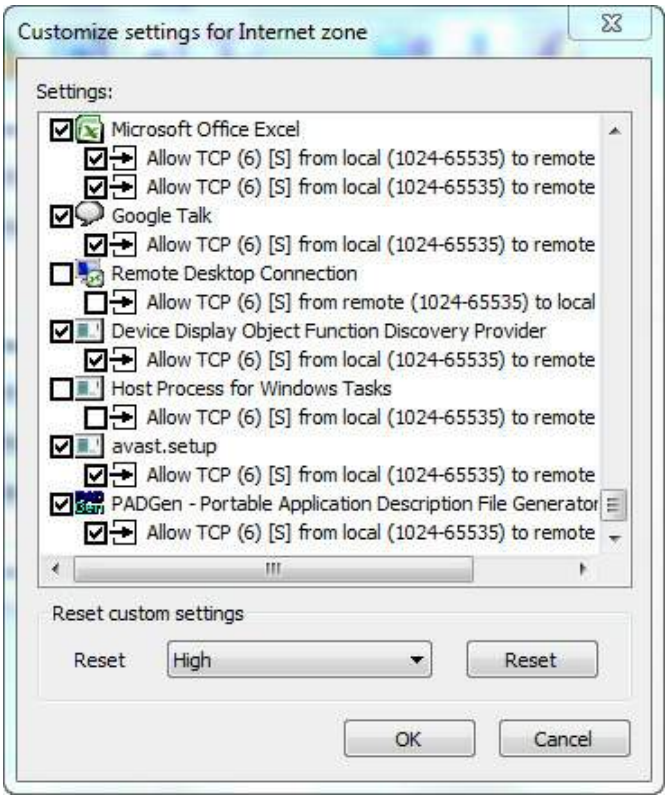
Запретить Интернет Трафик – это блокирует весь входящий и исходящий Интернет трафик и эффективно блокирует работу компьютера. Это полезно для компьютера с широкополосной связью, который остался без присмотра.

Системная безопасность (для Интернета и внутренней сети)

Интернет безопасность - можно задавать различные уровни защиты для доступа в Интернет. Для большинства пользователей уместен параметр «Высокий», поскольку он позволяет широкий доступ в интернет, обеспечивая высочайший уровень защиты брандмауэра. Параметр «Низкий» подходит только для самых доверенных сред, где не требуется полного доступа к системе.

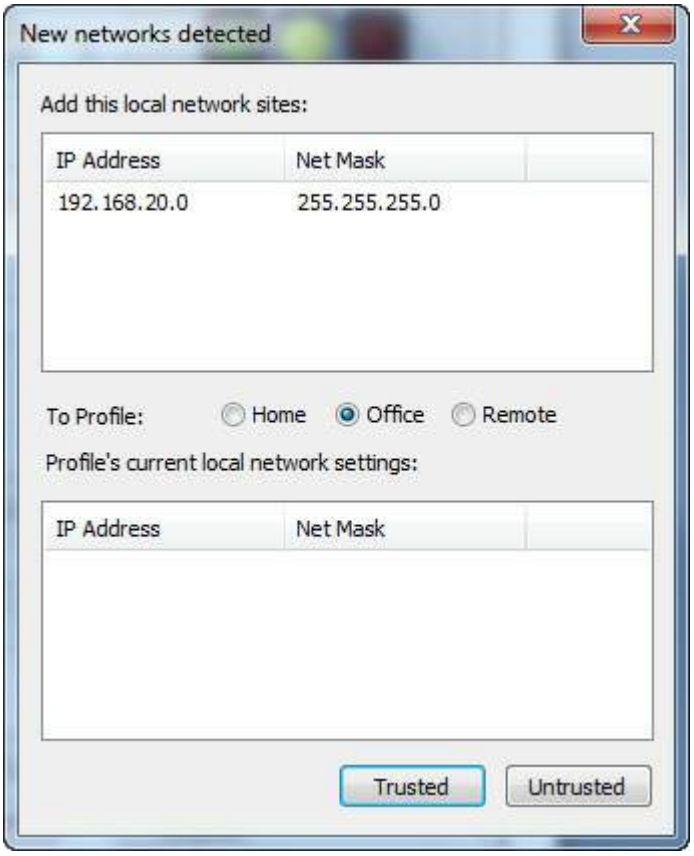
Сетевая безопасность - Могут быть указаны различные уровни защиты сети. Выбор Уровня зависит от типа сети, в которой находится компьютер. Для большинства пользователей подходит уровень "Низкий", так как позволяет доступ к файлам и принтерам в сети. При выборе уровня "Высокий" будут блокироваться все общие сетевые диски, принтеры и файлы. Этот уровень может быть задан при использовании сторонних или удаленных сетей.

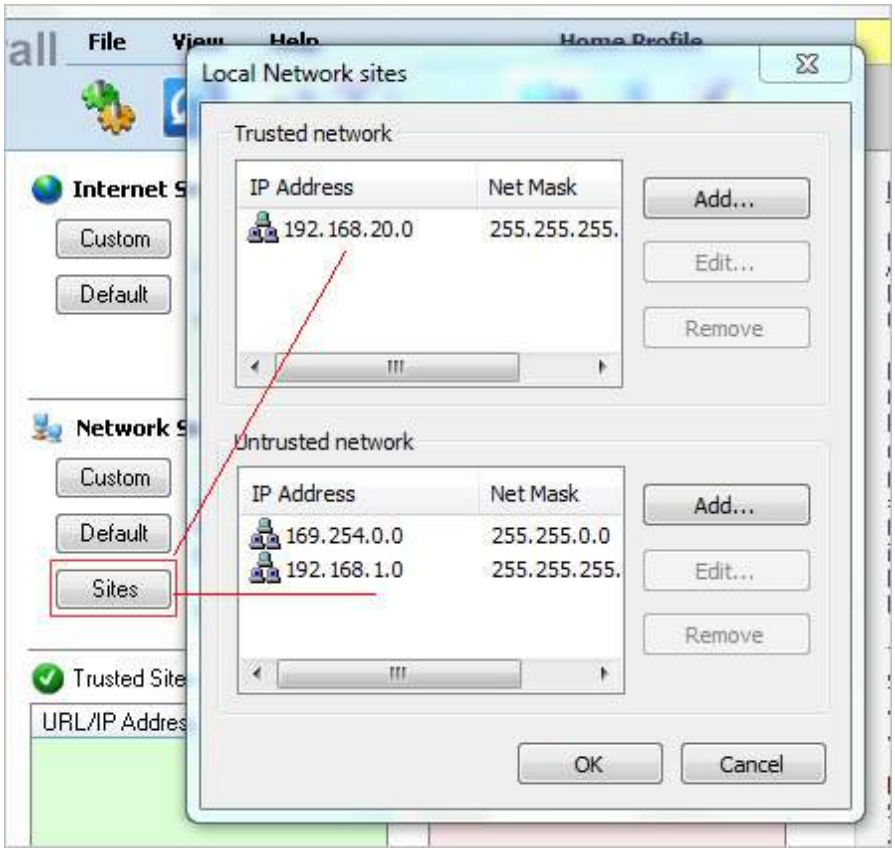
Пользовательский уровень безопасности – выбор кнопки Пользовательский в секции Интернет или Сетевой безопасности отображает диалоговое окно, которое позволяет установить настраиваемый набор правил для Интернет-безопасности путем выбора доступных правил, созданных автоматически или вручную пользователем.



IP-адреса Сети

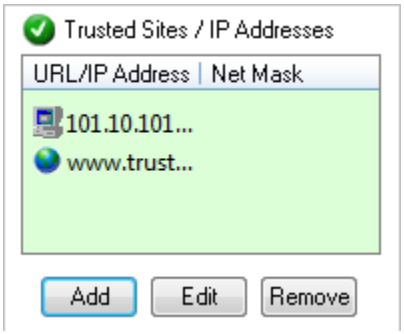
Новые локальные сети обнаруживаются автоматически. Локальная сеть, IP-адрес и Маска Сети могут быть установлены, как Доверенные или Ненадежные для профилей Дома, Офис или Удаленный (см. скриншот).





Все доверенные и ненадежные сети и сайты можно просматривать в любое время, выбрав кнопку Сайты в разделе Сетевая безопасность (см. скриншот)

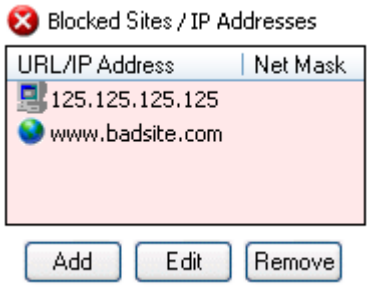
Интернет-сайты / IP адреса



С любого Интернет-сайта или IP-адреса может быть разрешен доступ к вашему компьютеру. Добавление узла в доверенные часто уменьшает количество всплывающих оповещений для этого определенного IP-адреса при доступе. Аналогично, если «www.trust...com» является доверенным веб-сайтом, пользователь может добавить этот сайт в надежные сайты. Эти дополнения помогут избежать в будущем любых, связанных с ними, всплывающих оповещений при доступе.

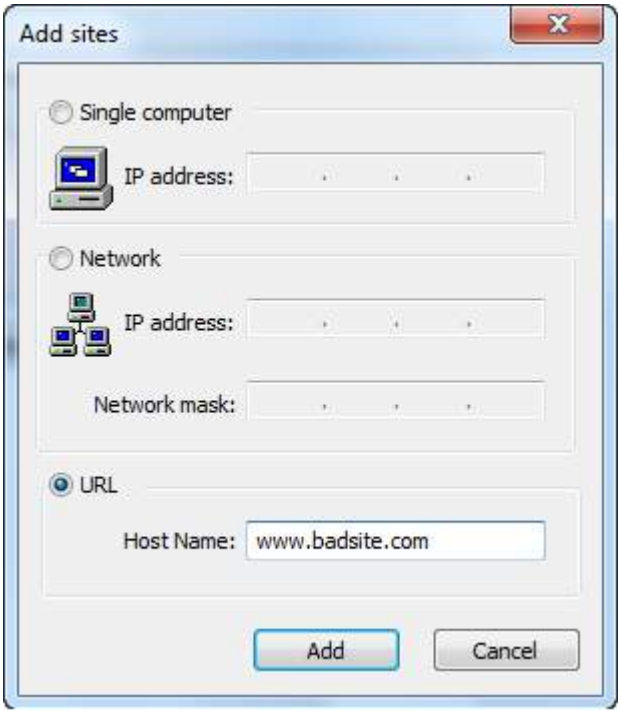
При работе в режиме ручного управления отображаются оповещения при блокировке входящих /исходящих пакетов, когда неизвестный (или ненадежный) IP-адрес пытается получить доступ к системе пользователя. Всплывающее предупреждение включает в себя дату, время, тип пакетов и IP адрес. Эти всплывающие окна могут быть отключены (информация будет продолжаться записываться/храниться в журнале брандмауэра). Также, может быть выбрана кнопка "Больше информации" для просмотра дополнительных сведений о пакете.

Аналогично, любой Интернет-сайт или IP-адрес может быть заблокирован для вашего компьютера, нажатием на кнопку Добавить в разделе Заблокированных сайтов / IP-адресов и вводом в окно соответствующего сайта / IP-адреса.



Добавление веб-сайтов / IP адресов

Надежные и заблокированные сайты / IP адреса можно добавить, нажав на кнопку Добавить в разделах доверенных или заблокированных сайтов / IP адресов в главном меню и введя соответствующую информацию. Все Локальные сети могут быть добавлены вводом корневого IP-адреса и Маски сети. Интернет-сайты могут быть добавлены после выбора раздела «URL» и ввода сайта в поле «Host Name».



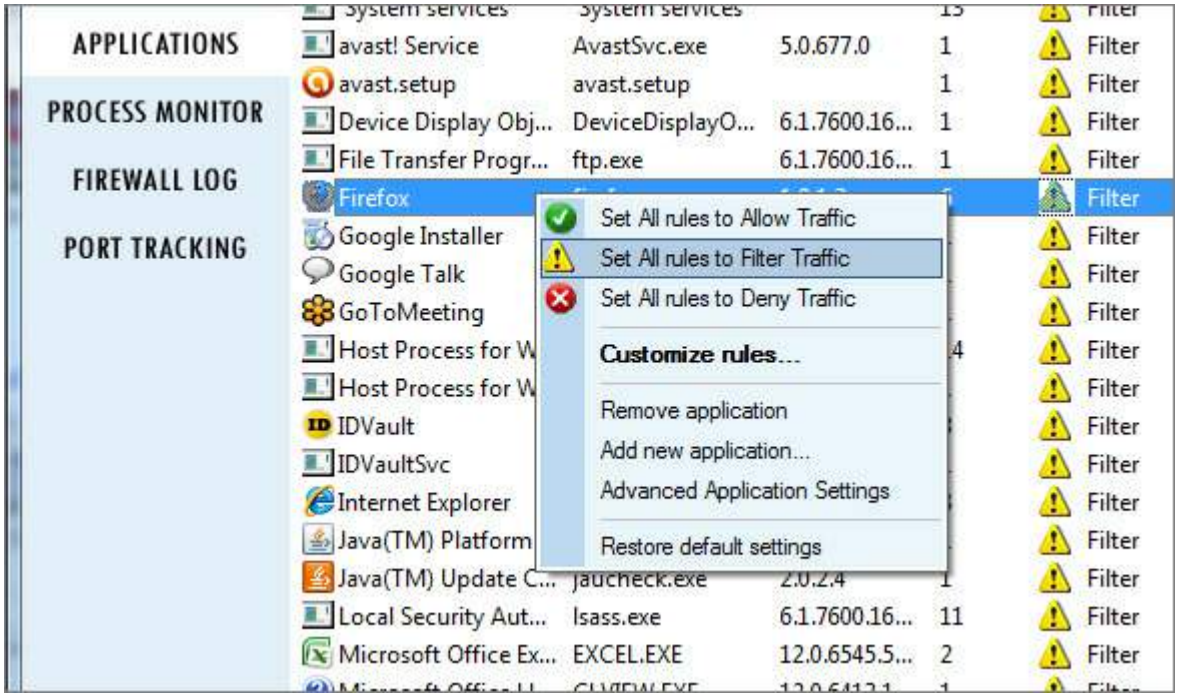
XMAS и NULL Сканирование

В то время как Privatefirewall не отображает специальный тип оповещений брандмауэра для XMAS и NULL сканирования/трафика, он обнаруживает, блокирует и записывает эти события как "XMAS сканирование обнаружено" и "NULL сканирование обнаружено" в журнал.

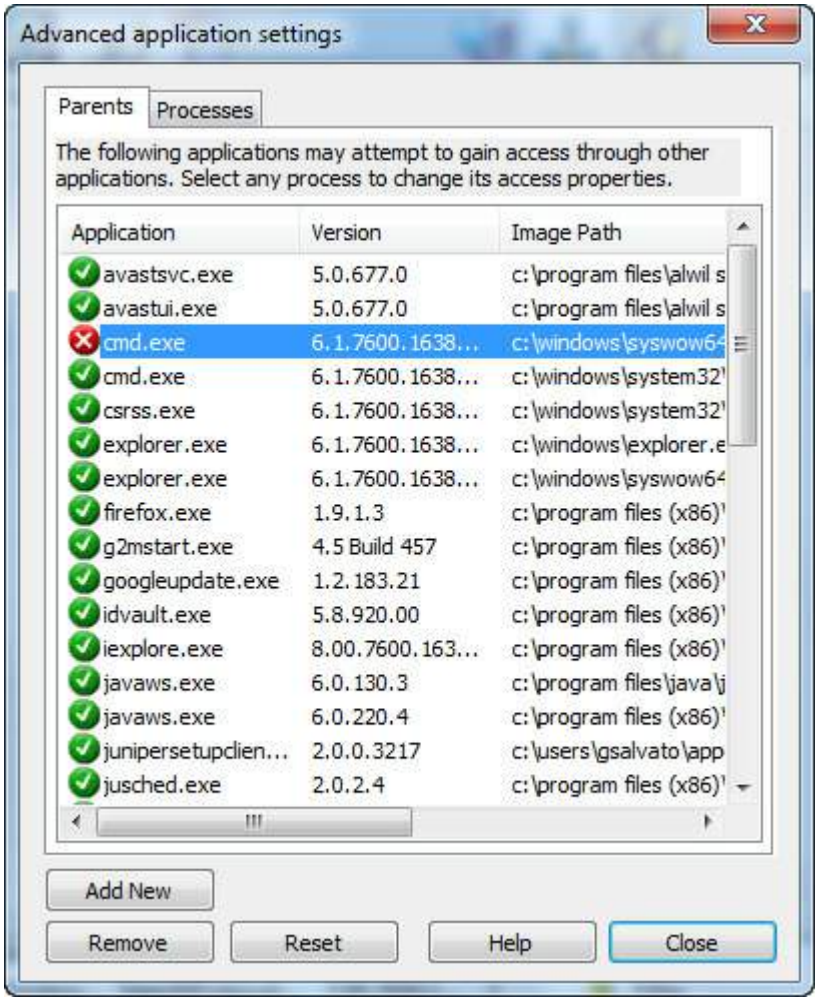
Оповещения экрана включены, когда Privatefirewall работает в режиме ручного контроля. При обнаружении уведомления фильтра пакетов отображаются с указанием конкретного номера порта, но без справки по XMAS или NULL сканированию.

Приложения

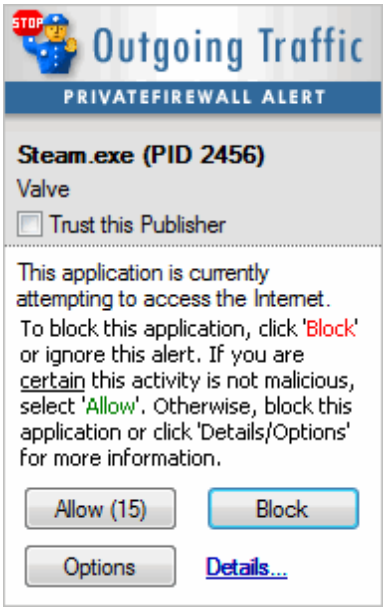
Окно настройки приложений состоит из всех правил брандмауэра, которые Privatefirewall применяет к перечисленным приложениям. Окно включает в себя имя приложения и исполняемый файл, номер версии, количество применяемых правил и классификацияю правил. Privatefirewall может разрешить или запретить входящий или исходящий трафик для каждой попытки доступа, или спросить разрешение при каждой попытке доступа.



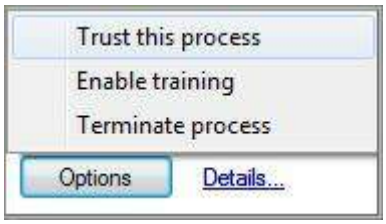
Расширенные параметры приложения (доступную из файл/параметры/расширенные настройки) Некоторые приложения позволяют другим приложениям контролировать свои действия, это означает, что 'основное' приложение может быть защищено, но может быть, что «вторичное» родительское приложение получит доступ к сети Интернет через основное приложение. В окне Расширенных настроек приложений перечислены эти «вторичные» родительские приложения, которые пытались получить доступ в Интернет или сети через «основное» доверенное приложение. Каждому приложению в списке доступ может быть разрешен или заблокирован.



Оповещения Обнаружения Приложения (Firewall)



Когда приложение впервые пытается получить доступ в Интернет, Privatefirewall будет отображать оповещение обнаружения приложений с запросом, чтобы разрешить или блокировать доступ (смотрите раздел этого руководства Параметры -> предупреждения системы безопасности и параметры управления угрозой для получения дополнительных сведений об оповещении о событии фильтрации).
Выбор кнопки Опции отобразит дополнительные варианты, позволяющие вам Доверять этому процессу, включить Обучение или прекратить процесс.



Опции – Доверять этому Процессу

Доверять этому Процессу в оповещении позволяет разрешить все действия, относящиеся к конкретной программе или процессу (вместо выбора "Разрешить" в оповещении, позволяющего только конкретную деятельность (т.е. открытие процессов, межпроцессное взаимодействие, и т.д.).

Опции - Включить Обучение

Включить Обучение через оповещение в трее или в **окне полной тревоги**:
Параметр Включить Обучение может быть выбран нажатием на кнопку Параметры/Расширенные настройки в Privatefirewall, при сообщении обнаружения процесс монитором и в окне полной тревоги (полный текст оповещения отображается в режиме Ручного контроля или вызова, при нажатии на кнопку «Подробнее...» в оповещении в трее). Выбор этого параметра активирует Обучение в течение 180 секунд и позволяет все действия (как и при нормальной инициализации режима Обучения), за исключением тех, которые были ранее заблокированы. Тренировочный период продлевается автоматически (перезапуск на вторые 180 сек) для каждого нового события, что происходит в течение первоначального или последующего связанного 180 секундного периода. Этот «временный» или «по требованию» период Обучения отключается, когда пользователь изменяет любые настройки через меню Файл | Параметры или после того, как истек второй период в 180 секунд.

Включение Обучения через меню в трее:
Обучение также доступно через меню в трее (для сценариев, где, например, пользователь устанавливает что-то новое и хотел бы обучить, таким образом, временной или конкретным видам деятельности). А флажок рядом с пунктом меню «Обучение» появляется, если параметр «Обучение» активируется вручную или через оповещение и остается активным, основываясь на той же логике, как при включение обучения через трей или окно полной тревоги.

Включение Обучения через Файл | Параметры | Дополнительно (для брандмауэра и Монитора Процессов). В отличие от включения Обучения через оповещения или меню в трее, включение Обучения через меню Файл | Параметры | Дополнительно (для брандмауэра и Монитора Процессов) будет активировать Обучение при условии, что флажок в окне установлен.

Во всех сценариях Обучения, Privatefirewall будет блокировать только ту деятельность, которая ранее была заблокирована (или настроена блокировка). Все новые активности будут разрешены и учтены, как законные. Вариант Обучения должен быть выбран только в том случае, когда вы абсолютно уверены, что процесс приложения является законным.

Опции – Завершить Процесс

Выбор опции **Завершить Процесс** остановит соответствующий процесс.

Нажатие кнопки «Подробнее» в оповещении в трее отобразит расширенное оповещение, которое предоставляет более подробную информацию о подозрительной активности и дополнительные опции управления угрозой (см. справа). Расширенное предупреждение содержит имя программы, номер версии, путь к файлу и другие детали. Если выбрана ссылка «Веб-поиск», поиск информации о процессе по имени исполняемого файла будет выполняться в браузере по умолчанию. Для процессов с действительной цифровой подписью будут активны дополнительные опции, которые позволят вам доверять издателю программного обеспечения и просматривать цифровые сертификаты издателей..

Примечание: В режиме Ручного управления, расширенное оповещение появится автоматически, а оповещение в трее отображаться не будет.

Опции управления расширенного оповещения

Нажатие на ссылку **Веб-поиск** предоставляет удобный способ поиска в Интернете, чтобы узнать больше информации о приложении. Функция будет начинать поиск в Интернете с помощью поисковой системы в браузере по умолчанию.

Просмотр сертификата - это может быть полезным и информативным для просмотра сведений об издателе программного обеспечения, прежде чем принять решение, что следует добавить издателя к списку доверенных издателей. Просто нажмите на ссылку Просмотр сертификата в расширенном оповещении для вызова диалогового окна, содержащего сведения о сертификате.

Доверять этому Издателю – отметьте этот чек_бокс для добавления издателя программного обеспечения в Список Доверенных Издателей.

Запомнить этот параметр – по умолчанию, правило, связанное с определенного типа деятельностью, запоминается только для текущей сессии (после перезагрузки правило больше не будет действующим). Чтобы помнить и применять правило для последующей деятельности, установите флажок в бокс Запомнить эти настройки. Соответствующие правила будут применяться к высокому и низкому уровням безопасности.

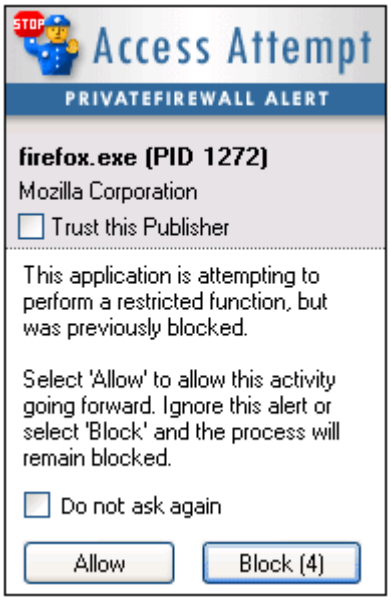
Применить для всех оповещений - устранит отображения дополнительных оповещений для этого процесса или приложения, рассматривая последующие действия на основании ответа на первоначальное предупреждение.
Примечание: Если предупреждение инициировано брандмауэром, ответ «Применить для всех оповещений» будет применяться для всех будущих оповещений брандмауэра. Если оповещение вызвано Монитором Процессов, ответ «Применять для всех оповещений» будет применяться для всех будущих предупреждений Монитора Процессов. В любом случае, соответствующие правила будут применяться к высокому и низкому уровням безопасности.

Разрешить – нажатие на кнопку Разрешить позволит конкретные действия, предпринимаемые программой. Выбор варианта Разрешить (без отмеченного чек_бокса "Запомнить этот параметр"), позволит деятельность, но только для текущей сессии (после перезагрузки правило больше не будет действительным). Соответствующие правила будут применяться к высокому и низкому уровням безопасности.

Обучить – нажатие этой кнопки будет вызывать режим Обучения.

Завершить - нажатие на кнопку Завершить остановит соответствующий процесс.

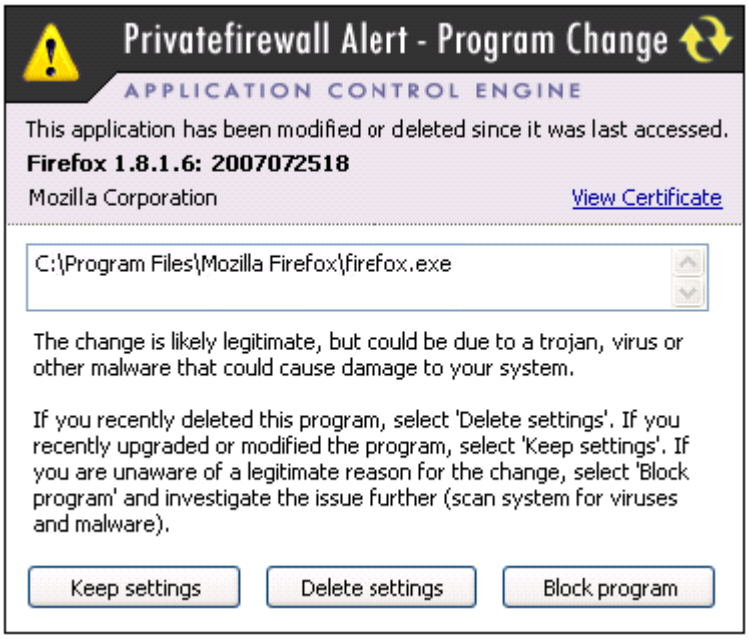
Блок – нажатие кнопки Блок будет останавливать конкретные действия, предпринимаемые программой. Выбор блока (без отмеченного чек_бокса "Запомнить этот параметр") будет блокировать активность, но только для текущей сессии (после перезагрузки правило больше не будет действительным). Соответствующие правила будут применяться к высокому и низкому уровням безопасности.



Если приложение пытается загрузить то, что было ранее проигнорировано или заблокировано, Privatefirewall будет генерировать оповещение с выбором Разрешить или Блокировать ранее заблокированную деятельность.

Изменения Программы

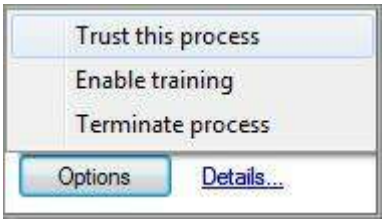
После того, как приложение установлено и добавляется в список программ, Privatefirewall будет отображать оповещение, если номер версии или программа были изменены.



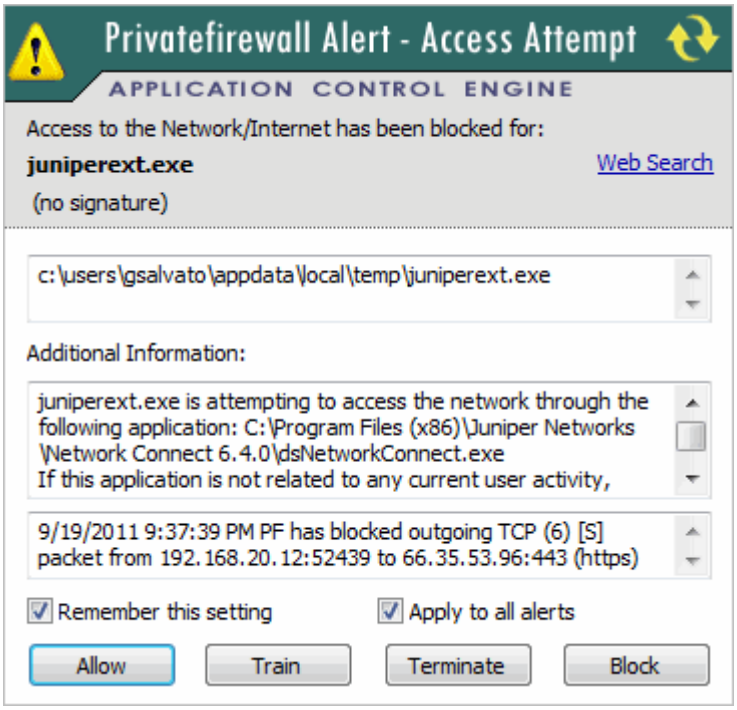
Имеется обычно один из 3 сценариев, когда отображается данное предупреждение:
1) Приложение было обновлено:
Это нормально для многих приложений, которые имеют частые обновления/модернизации. Если это так, нажмите кнопку «Сохранить параметры».
2) Приложение было удалено:
Это нормальная деятельность, когда многие приложения часто добавляются и удаляются. Если это так, выберите кнопку «Удалить параметры».
3) Приложение заменяется хакером/злоумышленником, использующим имя доверенного приложения для того, чтобы получить несанкционированный доступ.
Это часто упоминается как Троянский Конь. Хакер создает вредоносные программы, которые предназначены для причинения ущерба или извлечения ценной информации, и назначает общеизвестное имя программе (например: Internet Explorer обычно является именем iexplore.exe). Хакер, затем, пытается поместить эту программу в директорию, где обычно помещаются общеизвестные приложения (например: c:\program files\microsoft office). В случае успеха хакера, вредоносное приложение будет запущено в следующий раз, как Internet Explorer или iexplore.exe, пытаясь получить доступ. Если Privatefirewall установил изменение программы, он выдаст предупреждение. При этом, можно нажать кнопку «Запретить доступ», чтобы исследовать причину тревоги и принять решение.

Оповещение Доступа Программы

Метод широко используется хакерами для получения несанкционированного доступа для запуска доверенного приложения, чтобы получить доступ через него с помощью другого "вторичного" или родительского приложения. Тем не менее, эта деятельность является также функцией многих доверенных приложений, работающих нормально при доступе к сети Интернет. Если вы находитесь в процессе доступа к сети Интернет через Доверенное приложение, имя родительского приложения может быть не общее или узнаваемое, так что может быть трудно определить, какая осуществляется деятельность - нормальная или вредоносная. Если вы получите уведомление (см. справа) и указанное приложение относится к любой форме текущей деятельности, это скорее не вредоносная активность. Однако, если деятельность не связана с ним (наример: Если приложение даже не открыто, и т.д.), это может быть попытка атаки. При этом может быть принято решение Разрешить, Блокировать и выбраны другие опции по ссылке 'Подробнее ...' для исследования проблемы.

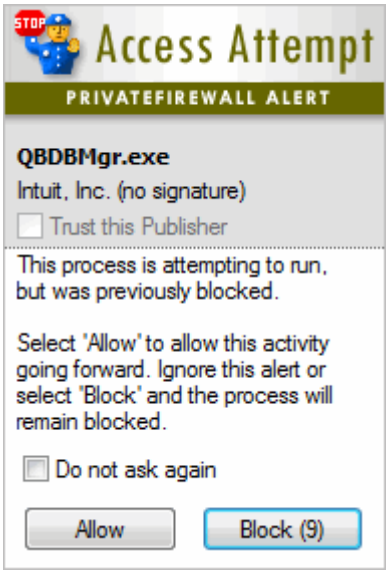


ПРИМЕЧАНИЕ: Privatefirewall будет отображать сообщение в трее 30 секунд. Если никаких действий не будет предпринято, время предупреждения истечет и деятельность будет заблокирована.

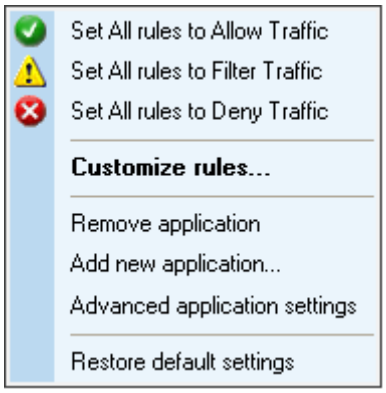


Нажмите "Подробнее / Опции" в окне Предупреждения для отображения расширенного оповещения, которое содержит более подробную Информацию о подозрительной активности и дополнительные опции управления угрозой. Данное предупреждение содержит имя программы, номер версии, дату, время и входящий / исходящий IP-адрес и Приложение "родитель", которое использовалось. В нем, также, будет указано, является ли трафик входящим или исходящим и предложено несколько вариантов реагирования. Если будет выбрана ссылка "Веб-поиск", поиск по имени исполняемого файла будет выполняться в вашем Браузере по умолчанию.

Если приложение пытается что-то загрузить или выполнить любые другие действия, которые ранее были проигнорированы или заблокированы, Privatefirewall сгенерирует специальное предупреждение - Попытка Доступа. Для просмотра списка всех этих типов приложений, обнаруженных Privatefirewall, нажмите на «Файл / Параметры / Расширенные настройки / Обнаруженные Приложения» в главном меню.



Настройка Правил Приложения



Privatefirewall предоставляет возможность вручную добавить, удалить или изменить правила для любого установленного приложения. Хакер может замаскировать программу под известный ресурс приложения и получить несанкционированный доступ. Privatefirewall обнаруживает ресурсы в каждом приложении, которые хакеры могут специально использовать и позволяет эти замаскированные ресурсы или попытки взлома блокировать. Щелкните правой кнопкой мыши любое приложение на странице Приложения и в «всплывающем окне приложения» появится меню (см. слева).

Разрешить/Фильтровать/Запретить трафик

Правила для Интернет-трафика, относящиеся к любому приложению могут корректироваться выбором пунктов 'Задать правила для Трафика..>Разрешить/Фильтровать/Запретить' во всплывающем меню приложения. Значение по умолчанию для любого набора правил, относящихся к приложению, является «Фильтровать трафик». Однако, эти правила могут быть отключены выбором либо "Разрешить" или "Запретить" трафик. Это может быть уместно, когда необходимы временный доступ или ограничение. Кроме того, правила, которые были созданы для этого приложения на вкладке "Настройка Правил" будут оставаться в памяти и будут по-прежнему применяться, если повторно выбрать пункт "Фильтровать трафик".

Удаление приложения

Приложение может быть удалено из списка приложений выбором пункта "Удалить приложение" из всплывающего меню приложения. Эта опция удалит всю защиту, которая применялась к выбранному приложению.

Добавление нового приложения

Новое приложение может быть добавлено вручную выбором пункта «Добавить новое приложение» во всплывающем меню приложения. Когда этот параметр выбран, необходимо выбрать исполняемый файл, который соответствует нужному приложению. Кроме того, все правила для приложения должны быть установлены вручную для того, чтобы Privatefirewall мог применять фильтрацию или защиту.

Расширенные настройки приложений

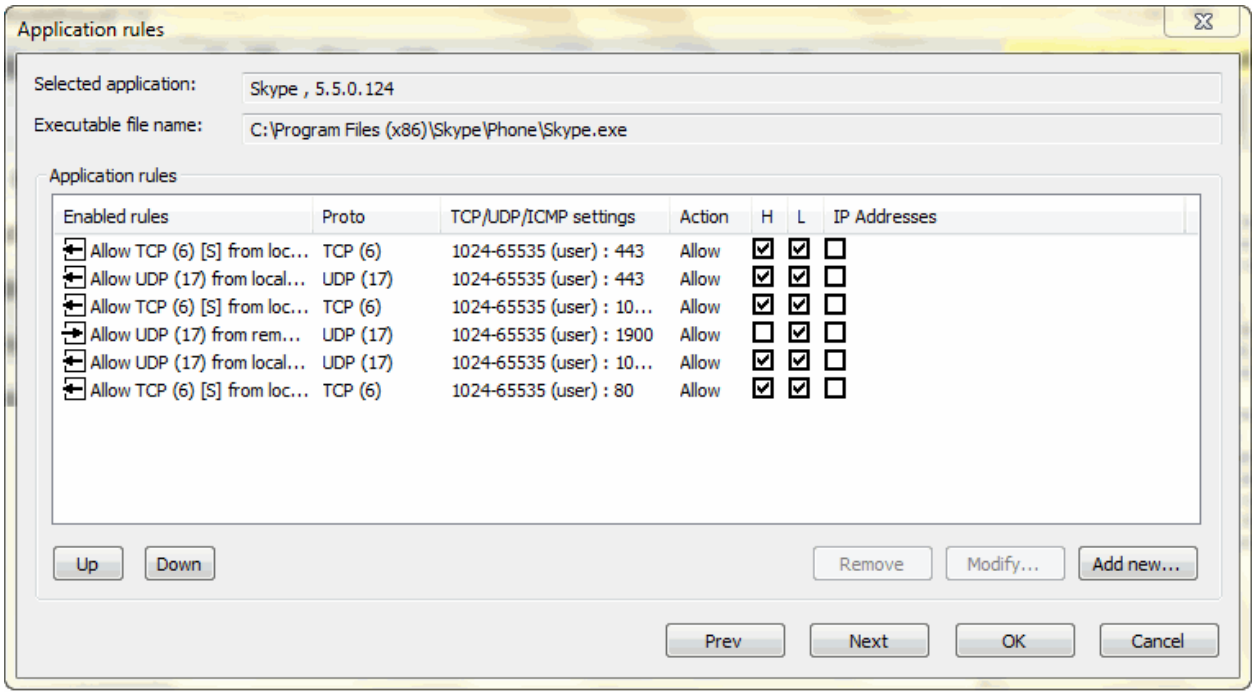
Окно "Расширенные настройки приложений" содержит списки приложений, которые пытались получить доступ в Интернет или сеть через другое доверенное приложение. Этот метод обычно используется хакерами, чтобы попытаться получить несанкционированный доступ.

Восстановление параметров по умолчанию

Восстановление настроек по умолчанию восстановит по умолчанию все приложения в списке приложений. Опция относится только к приложениям, которые предварительно загружены Privatefirewall. Опция будет неактивна (выделена серым цветом) для всех других приложений.

Настройка правил

Применяемые к приложениям правила, могут быть настроены выбором пункта "Настроить Правила ..." из всплывающего меню приложения. При выборе этого пункта, Privatefirewall отображает имя программы, имя исполняемого файла, номер версии программы, а также перечень правил для этого приложения (смотрите ниже). Правила могут быть добавлены, удалены или изменены щелчком правой кнопкой на любом правиле.



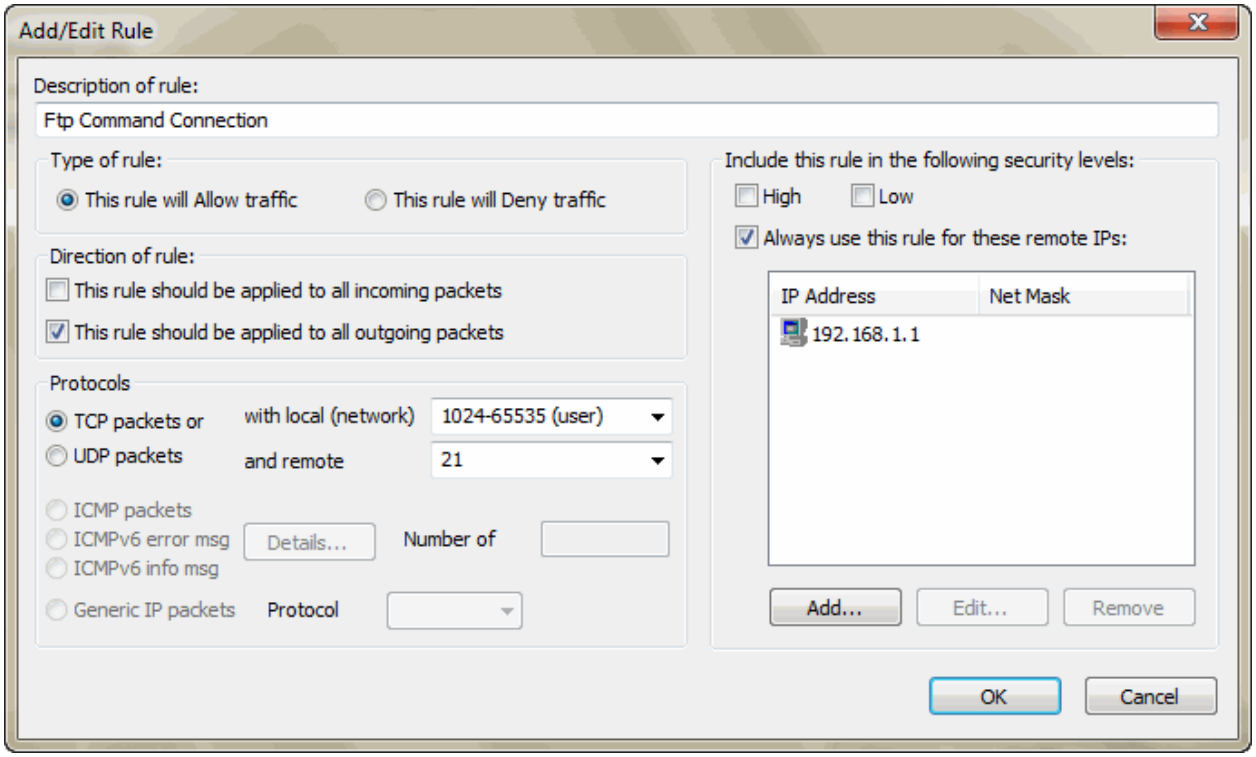
Перемещение правила

С помощью кнопок "вверх" и "вниз" можно изменить порядок применения правила, чтобы уделять первоочередное внимание выбранным по желанию пользователя.

Навигация по перечисленным приложениям
Навигация по другим перечисленным приложениям в окне "Правила Приложения" осуществляется выбором кнопок "Предыдущее" или "Следующее".

Удаление правила для приложения
Правило для приложений можно удалить из списка правил приложения, выделив правило приложения и нажав кнопку Удалить.

Добавить новые или изменить существующие правила для приложений



Диалог Добавления / Редактирования правил для приложений предусмотривает различные варианты конфигурации, которые включают IP-адреса, контроль уровня связи конкретного приложения. Используя эту функцию, можно разрешить доступ приложения только к/от определенных IP-адресов.

Примеры:
1) Ограничение для **ftp.exe:** Снять флажки в обоих зонах L и H. Выбрать "Всегда использовать это правило для этих удаленных IP-адресов". Добавить IP-адрес 192.168.1.1. Таким образом, **ftp.exe** сможет получить доступ только к IP-адресу 192.168.1.1. Все остальные будут заблокированы.

2) Ограничение для **RDP**: Для Системной Службы выбрать Включить правило для **RDP**. Снять флажки с L и H зоны. Выбрать "Всегда использовать это правило для этих удаленных IP-адресов". Добавить IP Адреса, которым подключение к вашегму компьютеру должно быть разрешено. Для всех других IP-адресов RDP порт будет полностью невидим.

В большинстве случаев, когда создается правило для конкретного типа деятельности / программы / IP адреса, H и L уровни безопасности, скорее всего, будут отменены, но есть сценарии, где можно было бы использовать комбинацию - например, вы можете проверять уровень безопасности L для управления связью по локальной сети одним из способов, в то время как FTP-доступ через конкретный IP-адрес. В этом случае, уровень безопасности L и правило "Всегда использовать это правило для этих удаленных IP-адресов" будут проверяться одновременно.

Privatefirewall обеспечивает гибкость в том, как правило может быть применено:

Используйте указанное правило для -
1) Любых узлов в зоне H, если выбрано
2) Любых узлов в зоне L, если выбрано
3) Перечисленных IPs, если выбрано

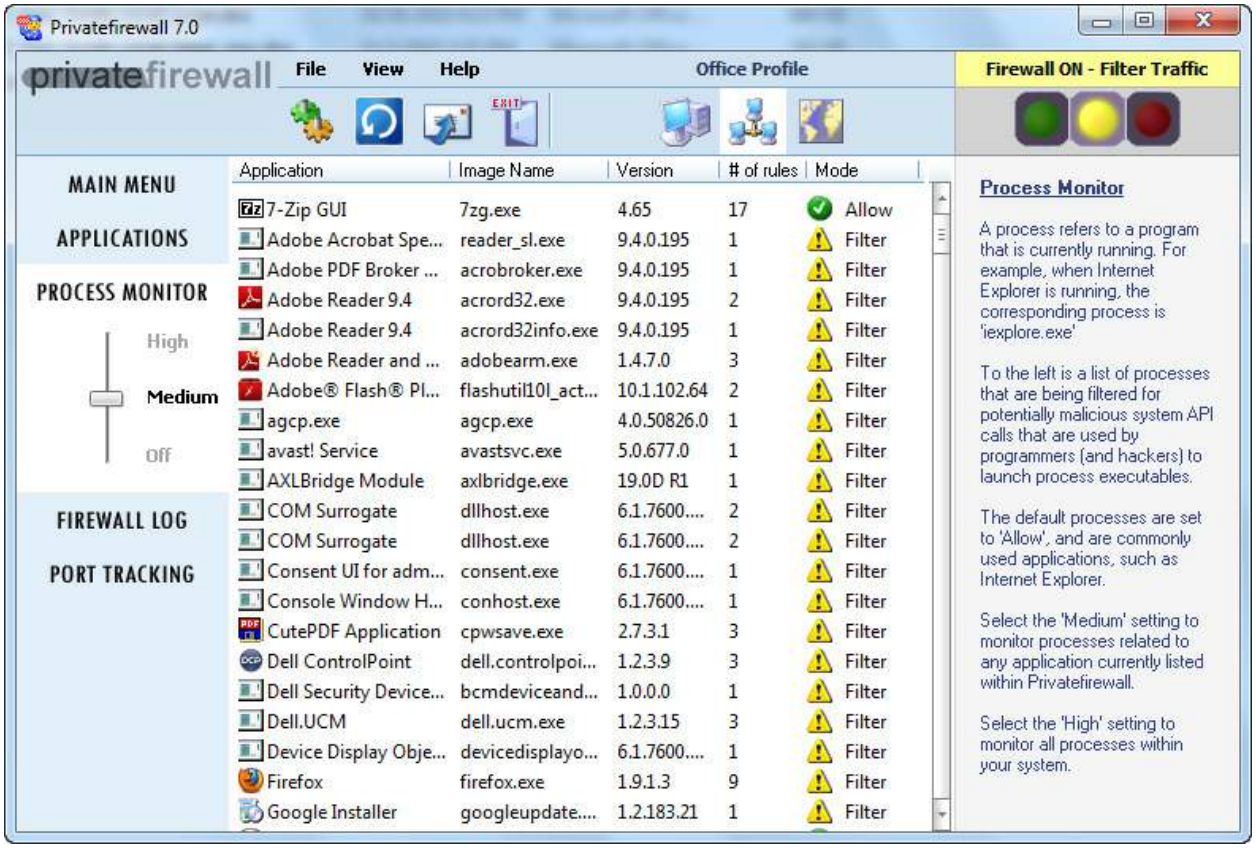
Контроль конкретных Портов Приложений.
Правила конкретного Порта могут быть определены для любого приложения, используя диапазоны доступных портов и портов, перечисленых в поле выпадающего списка. Введите вручную один или несколько номеров портов (то есть либо один порт, как 101 или один диапазон, как 101-204).

Безусловный Контроль Портов
- Задать порты (или диапазон), запрещающее правило для системных служб (приложений, служб, добавленных новых,...).

- Удалите любые конфликтующие разрешающие правила для конкретных приложений (они будут переопределять блок порта системной службы). Логика текущих правил для приложений по умолчанию работает следующим образом: 1) Проверка правила для приложения; если такое правило существует (чтобы запретить или разрешить трафик) дальнейшая обработка не выполняется; 2) Создание правила для системных служб, приложений и тренировка, где определяется, что конкретные правила приложений не находятся в противоречии/имеют приоритет.

Монитор Процессов

Процесс относится к программе, которая в данный момент выполняется. Например, когда Privatefirewall работает, соответствующие процессы "PFNet и PFGUI.exe" будут запущены (видно в Диспетчере Задач). Privatefirewall поддерживает список процессов, которые фильтруются на потенциально вредоносные вызовы API системы, и которые используется программистами и хакерми для запуска процесса на исполнение. Privatefirewall поддерживает набор процессов по умолчанию, которые связаны с часто используемыми приложениями, такими как Internet Explorer и устанавливает для них 'Разрешить'. Процессам не по-умолчанию, которые обнаружит Privatefirewall будет установлен режим 'Фильтровать', если они будут разрешены или «Запретить», если разрешены не будут.

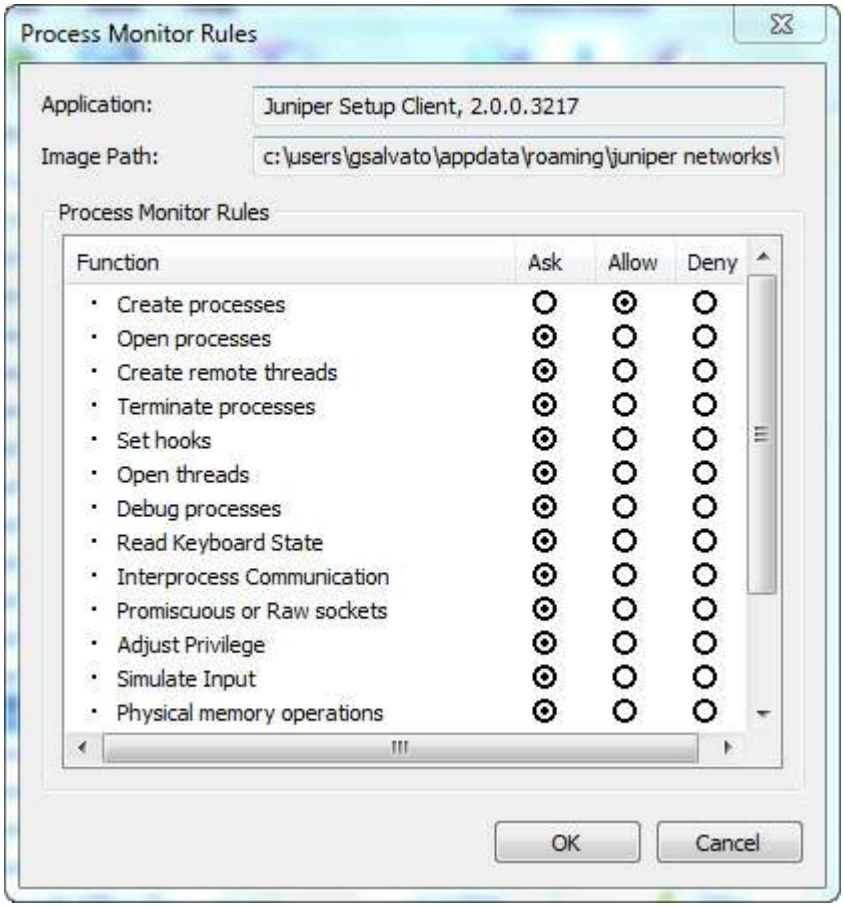


Монитору Процессов можно задать уровень работы либо 'Высокий', 'Средний' или «Выключено».

- Параметр «Высокий» будет контролировать все процессы, запущенные на вашем компьютере и разрешит только локальные / сетевые службы.
- Параметр «Средний» (по умолчанию) будет контролировать процессы, связанные с любыми приложениями, в настоящее время перечисленными в Privatefirewall, и разрешит службы, работающие под системной учетной записью.
- Параметр «Выключено» отключит Монитор Процессов, но не любую другую функцию Privatefirewall.

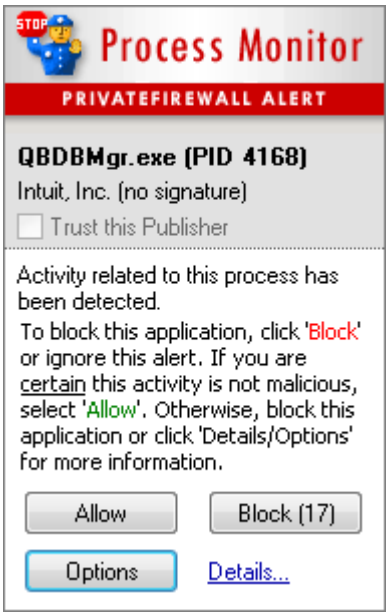
Правила Контроля Приложений

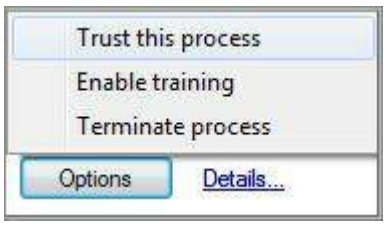
Сделайте двойной щелчок на любом процессе в окне Монитора Процессов для получения более детальной информации. Для каждого из перечисленных процессов, Privatefirewall контролирует функции WinAPI, перечисленные в колонке "функция" в окне "Правила Процесс Монитора". Для каждой функции WinAPI есть возможность задать условие, как "Спросить', 'Разрешить' или 'Запретить '. Если выбрано "Спросить', Privatefirewall спросит Пользователя должна ли выполняться конкретная функция процесса. Если выбрано "Разрешить", Privatefirewall позволит выполнить определенную функцию процесса без вмешательства пользователя. Если выбран параметр 'Запретить', Privatefirewall не позволит выполнить определенную функцию процесса. Приложениям по умолчанию (из набора общеизвестных часто используемых) будет задан для всех функций параметр «Разрешить».



Предупреждения Процесс Монитора

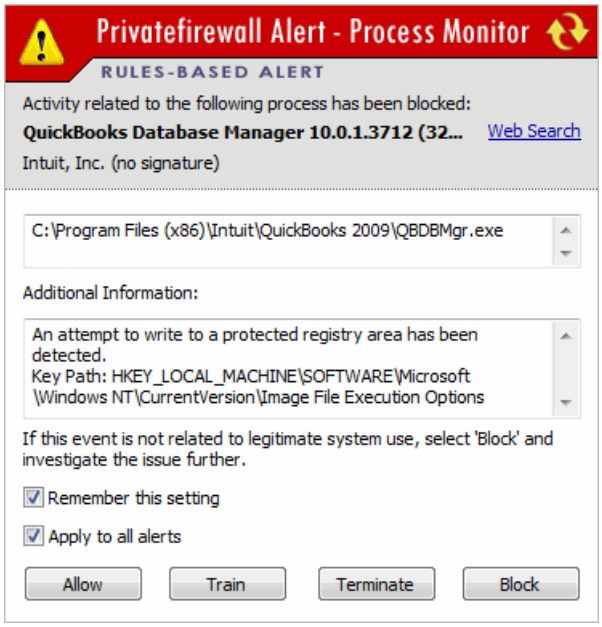
При обнаружении любой потенциально вредоносной деятельности, связанной с процессом, Privatefirewall будет отображать оповещение Процесс Монитора и предложит разрешить или блокировать доступ (смотрите справа). См. раздел данного руководства Privatefirewall-> Параметры-> предупреждения безопасности и варианты управления угрозами для получения дополнительных сведений о фильтрации событий и оповещениях. Выбор кнопки "Опции" отобразит список дополнительных вариантов действий, что позволит вам включить обучение или прервать процесс.

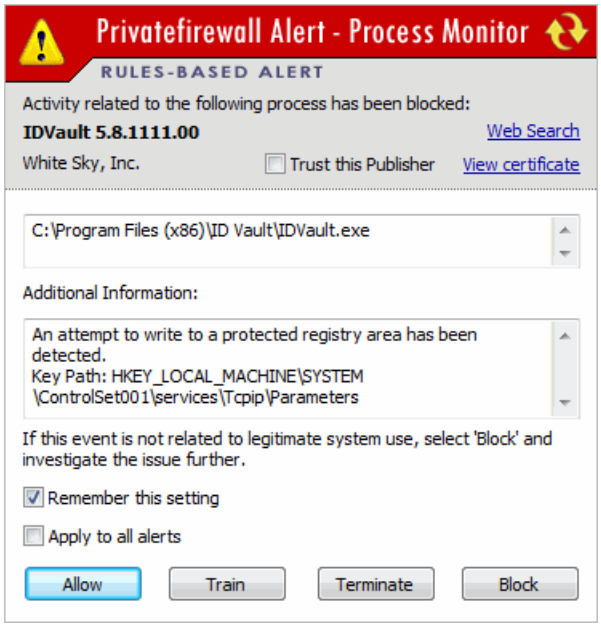




Примечание: Privatefirewall будет отображать оповещение в трее 30 секунд. Если никакие действия не предпринимаются и время истечет, то выявленная деятельность будет заблокирована.

Нажатие на ссылку «Подробнее...» в предупреждении отобразит окно расширенного оповещения, которое содержит более подробную информацию о подозрительной активности и дополнительные опции управления угрозой (см. ниже). В режиме Ручного Управления расширенное оповещение появляется автоматически, а в трее предупреждение отображаться не будет. Расширенное оповещение содержит имя программы, номер версии, путь к файлу и дополнительные детали. Если выбрана ссылка «Веб-поиск», то поиск по имени исполняемого файла процесса выполняется в браузере по умолчанию. Для процессов с действительный цифровой подписью активируются дополнительные опции, которые позволяют добавить Издателя программного обеспечения в доверенные и просмотреть его цифровой сертификат.





Существует несколько типов потенциально вредоносной деятельности, связанной с процессом, который будет генерировать оповещения. Например Процесс Монитор обнаруживает попытки создать или изменить ограничения объектов. Ниже приведены примеры оповещения, которые отображаются в этих случаях. Для всех оповещений,- если приложение или процесс связаны с любой законной деятельностью, в данный момент, осуществляемой на компьютере, то это скорее не вредоносная активность, однако, если это не связано с деятельностью (например: приложение или процесс даже не запускались пользователем т.д.), то это может быть вредоносной активностью и надо нажать кнопку «Блокировать» и исследовать этот вопрос.

Дополнительные Опции управления расширенного предупреждения

Веб-поиск - нажатие на ссылку Поиск в Интернете предоставляет удобный способ, чтобы узнать больше о приложении. Функция будет начинать поиск в Интернете с помощью поисковой системы браузера по умолчанию

Просмотр сертификата - это может быть полезным и информативным для просмотра сведений о программном обеспечении, прежде чем принять решение, что следует добавить издателя к списку доверенных издателей. Просто нажмите на ссылку Просмотр сертификата в окне расширенного оповещения для вызова диалогового окна, содержащего сведения о сертификате.

Доверять этому издателю - установите этот флажок, чтобы добавить издателя в список доверенных издателей.

Запомнить этот параметр – по умолчанию, правило, связанное с определенным типом деятельности запоминается только для текущей сессии (после перезагрузки правило больше не будет действительным в настоящее время). Чтобы применять правило для последующей деятельности, установите флажок "Запомнить этот параметр". Соответствующие правила будут применяться к высокому и низкому уровням безопасности.

Применить для всех оповещений - устранит отображения дополнительных оповещений для этого процесса или приложения, рассматривая последующие действия, на основании ответа на первоначальное предупреждение. Примечание: Если было предупреждение брандмауэра, ответ «Применить для всех оповещений» будет применяться для всех будущих предупреждений брандмауэра. Если оповещение было от Монитора Процессов, ответ «Применять для всех оповещений» будет применяться ко всем будущим оповещениям процесс мониторинга. В любом случае, правило будет применяться к уровням низкой и высокой безопасности.

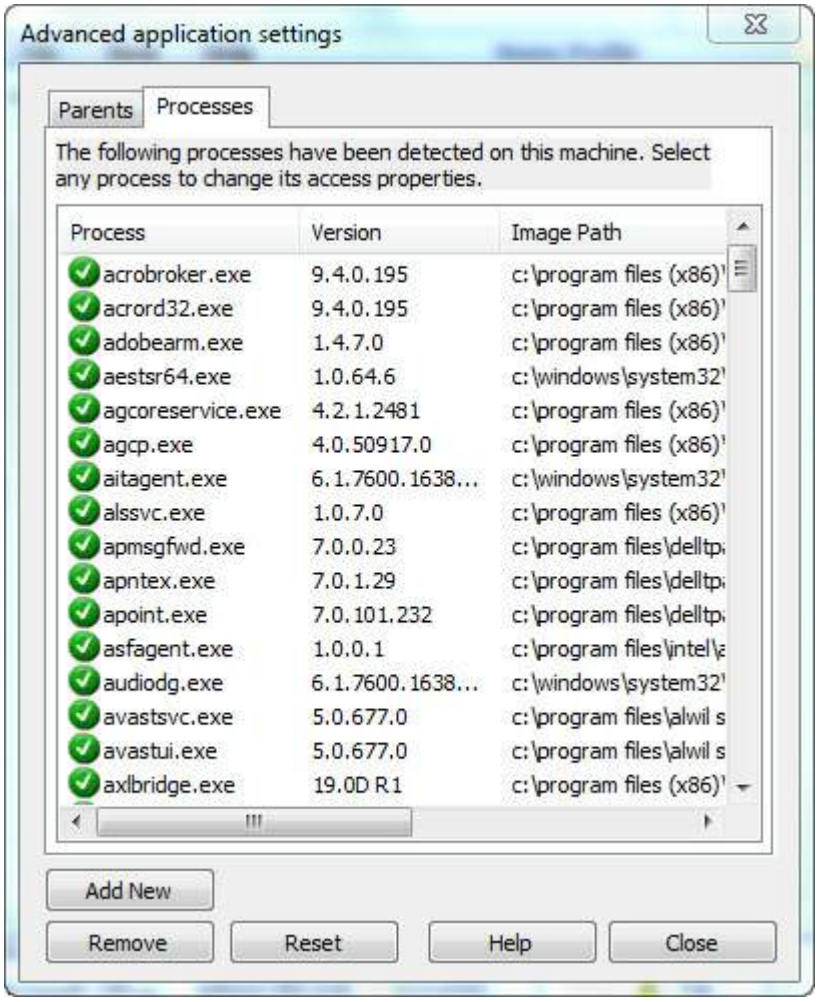
Разрешить – нажатие на кнопку "**Разрешить**" позволит конкретные действия, предпринимаемые программой. Выбор варианта разрешить ("Запомнить этот параметр" - не отмечено) позволит деятельность, но только для текущей сессии (после перезагрузки правило больше не будет действительным).
Соответствующие правила будут применяться к высокому и низкому уровням безопасности.

Обучить – нажатие на кнопку "**Обучить**" будет вызывать режим обучения.

Завершить - нажатие на кнопку "**Завершить"** остановит соответствующий процесс.

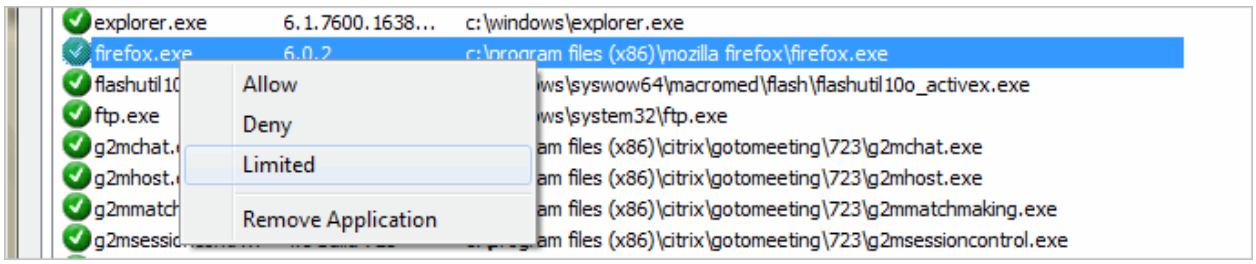
Блок – нажатие на кнопку "**Блок**" остановит конкретное действие, предпринимаемое программой. Выбор блока ("Запомнить этот параметр" - не отмечено) будет блокировать активность, но только для текущей сессии (после перезагрузки правило больше не будет действительным).
Соответствующие правила будут применяться к высокому и низкому уровням безопасности.

Обнаружение Процесса
В дополнение к фильтрации процессов на системные вызовы API, Privatefirewall также поддерживает список наиболее часто используемых процессов и обеспечивает предупреждение, когда запускается неизвестный процесс.



Управление Правами Процесса

Процессы могут быть запущены с ограниченными правами непосредственно через соответствующее оповещение в трее или в окне подробного оповещения. Также можно ограничить права процесса через вкладку "Расширенные Настройки Приложений". Выделите процесс и щелкните правой кнопкой мыши и выберите команду "Разрешить", "Отказать", "Удалить" или "Ограничить" права.



Дополнительная информация

Монитор Процессов, также, контролирует любые изменения в следующем:

Расширения Файлов
exe
dll
msi
ocx
com
vxd
sys
bat
cmd
pif
scr
hta
js
jse
lnk
reg
vbe
vbs
wsf
wsh

Системные Файлы
win.ini, system.ini, hosts

Пути
start menu\programs\startup

Ключи Реестра
shell\xxx\open (where xxx is any application)
software\microsoft\active setup\installed components
software\microsoft\windows\currentversion\explorer\sharedtaskscheduler
software\microsoft\windows\currentversion\shellserviceobjectdelayload
software\microsoft\windows\currentversion\explorer\shellexecutehooks
software\microsoft\windows\currentversion\shell extensions\approved
software\classes\folder\shellex\columnhandlers
software\microsoft\windows\currentversion\shellserviceobjectdelayload
software\microsoft\windows\currentversion\app paths
software\microsoft\windows\currentversion\run
software\microsoft\windows nt\currentversion\winlogon\shell
software\microsoft\windows nt\currentversion\winlogon\userinit
software\policies\microsoft\windows\system\scripts\startup
software\policies\microsoft\windows\system\scripts\logon
software\microsoft\windows\currentversion\policies\system\shell
software\microsoft\windows nt\currentversion\windows\load
software\microsoft\windows nt\currentversion\windows\run
software\microsoft\windows\currentversion\policies\explorer\run
system\currentcontrolset\control\session manager\bootexecute
system\currentcontrolset\services
software\microsoft\windows\currentversion\explorer\browser helper objects
software\microsoft\internet explorer\urlsearchhooks
software\microsoft\internet explorer\toolbar
software\microsoft\internet explorer\extensions
software\microsoft\windows nt\currentversion\image file execution options
software\microsoft\command processor\autorun

software\microsoft\windows nt\currentversion\windows\appinit_dlls
system\currentcontrolset\control\session manager\knowndlls
software\microsoft\windows nt\currentversion\winlogon\system
software\microsoft\windows nt\currentversion\winlogon\notify
software\microsoft\windows nt\currentversion\winlogon\ginadll
software\microsoft\windows nt\currentversion\winlogon\taskman
control panel\desktop
system\currentcontrolset\control\bootverificationprogram\imagename
system\currentcontrolset\control\print\monitors
software\pwi, inc.\privatefirewall

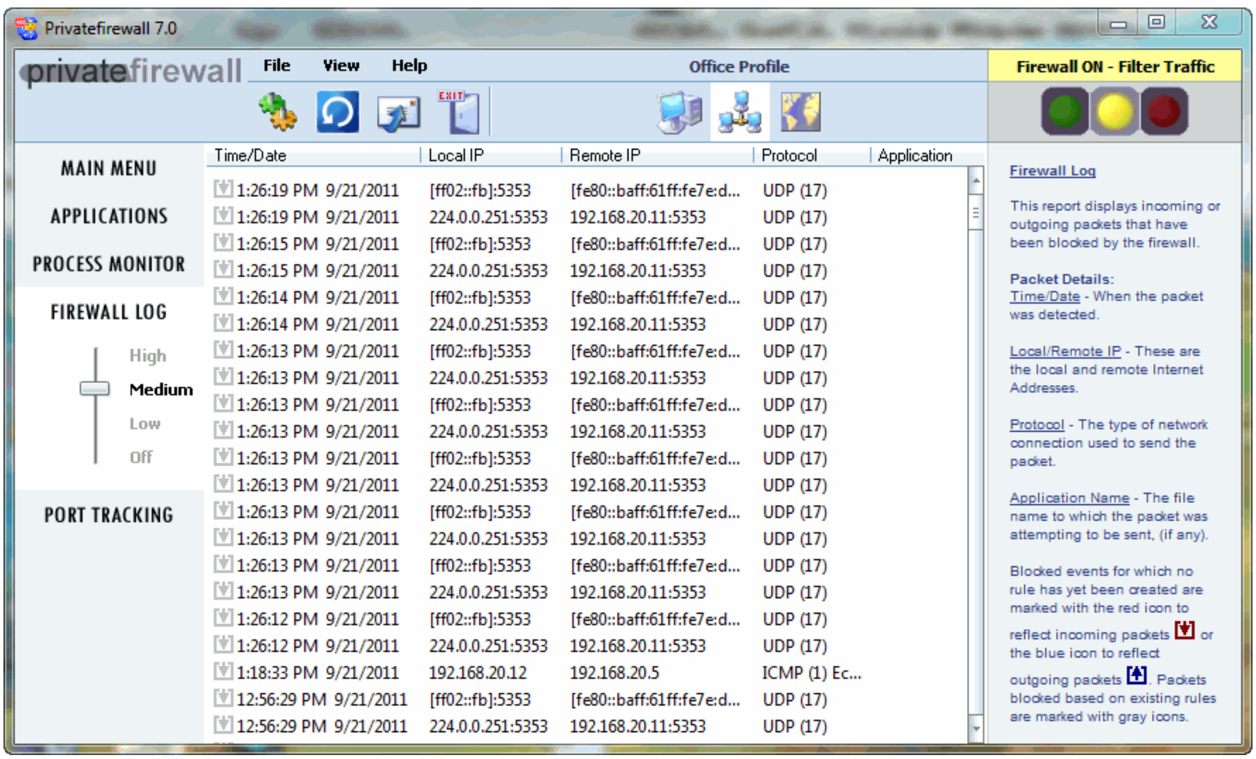
Журнал Firewall

В Журнал брандмауэра записываются входящие и исходящие пакеты, которые являются частью информации передающейся между источником и получателем в Интернете или любой другой сети; один из которых это ваш компьютер. Как показано на приведенном ниже снимке экрана, IP-адрес 192.168.0.2. является "домашним". **Примечание: Ваш IP-адрес может быть одним и тем же адресом во время каждого подключения к Интернету (так называемый "статический IP", используемый в большинстве T1/DSL-соединений). Или, ваш IP может измениться для каждого Интернет-соединения (так называемый «Динамический IP» используется в большинстве кабельных/Dial-Up соединений).**

Privatefirewall сообщает следующее:

Время/дата - когда пакет был обнаружен.
Локальный IP - адрес в Интернете, к которому пакет направляется.
Удаленный IP - адрес в Интернете, с которого пакет поступает.
Протокол - сетевой протокол или тип сетевого подключения, используемого для отправки пакета.
Приложение - имя приложения, к/от которого пакет отправляется (если таковые имеются).

Правый клик мыши на любой записи в журнале брандмауэра будет предоставлять следующие опции: Доверять Удаленному (IP), Блокировать Удаленный (IP), Копировать Удаленный IP(s) в буфер обмена, Копирование выделенное в Буфер Обмена, Очистить отчеты, Сохранить отчет как, или Полный (Расширенный) Отчет.



Уровень контроля Журнала можно задавать с помощью ползунка: Выкл, Низкий, Средний, Высокий. Уровень Низкий - (регистрируются только события, отмеченные красным/синим значком, т.е. которые не связаны с любым из существующих правил), Средний - (все события за исключением ограниченных IPs) и Высокий (регистрируются все события брандмауэра). Повторяющиеся записи не регистрируется.

Записи Журнала, в которых не указаны приложения (поле "Приложение" пустое), означает, что нет зарегистрированного приложения для этого порта или что управление осуществляет сама ОС (т.е. порт 137-139, 443), но не допускается текущим набором правил.

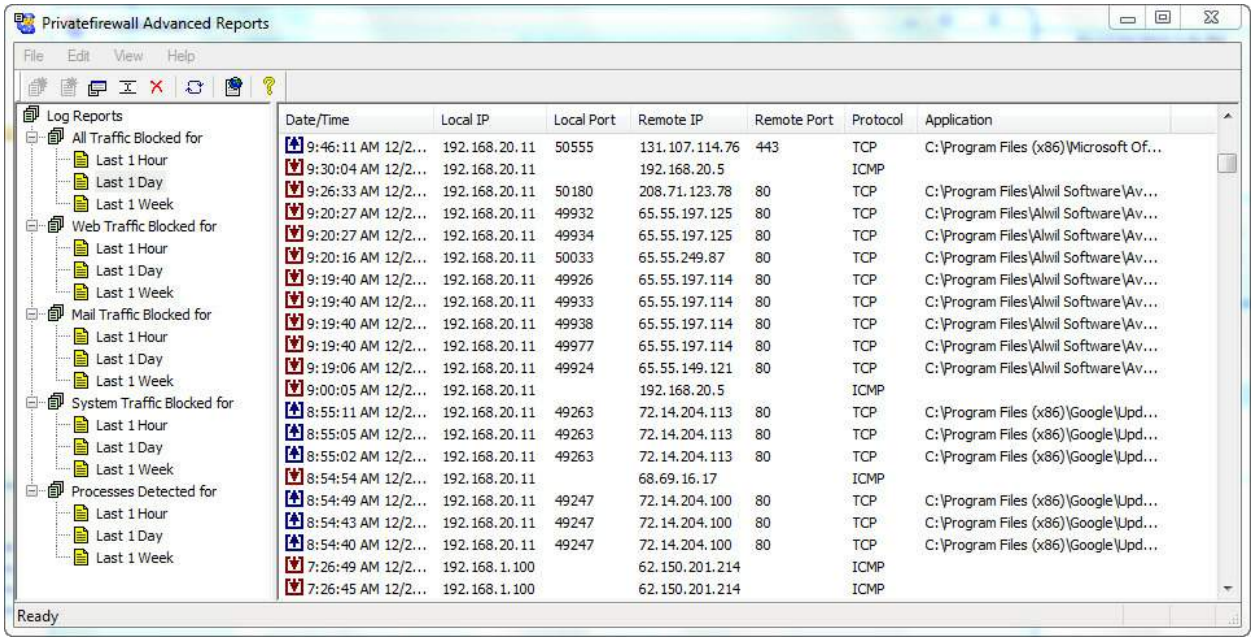
Полный (Расширенный) Отчет

Записи журнала брандмауэра можут быть отсортированы по типу и времени записи в Полный Отчет Privatefirewall. Этот отчет можно просмотреть из меню "Вид/Полный Отчет". Отчеты могут быть отсортированы по типу пакета - Интернет, электронная почта, или доступ системы. Каждый из этих отчетов можно также сортировать по времени, переходя обратно на 1 час, 1 день или 1 неделю.

Примечание: За последний прошедший 1 час принимается 3600 секунд, последний 1 день - 86400 секунд, чтобы отчеты могли отображать данные, охватывая более чем один календарный день, за последнюю 1 неделю принимается - последние 7*86400 секунд

Полный Отчет Privatefirewall содержит следующее:

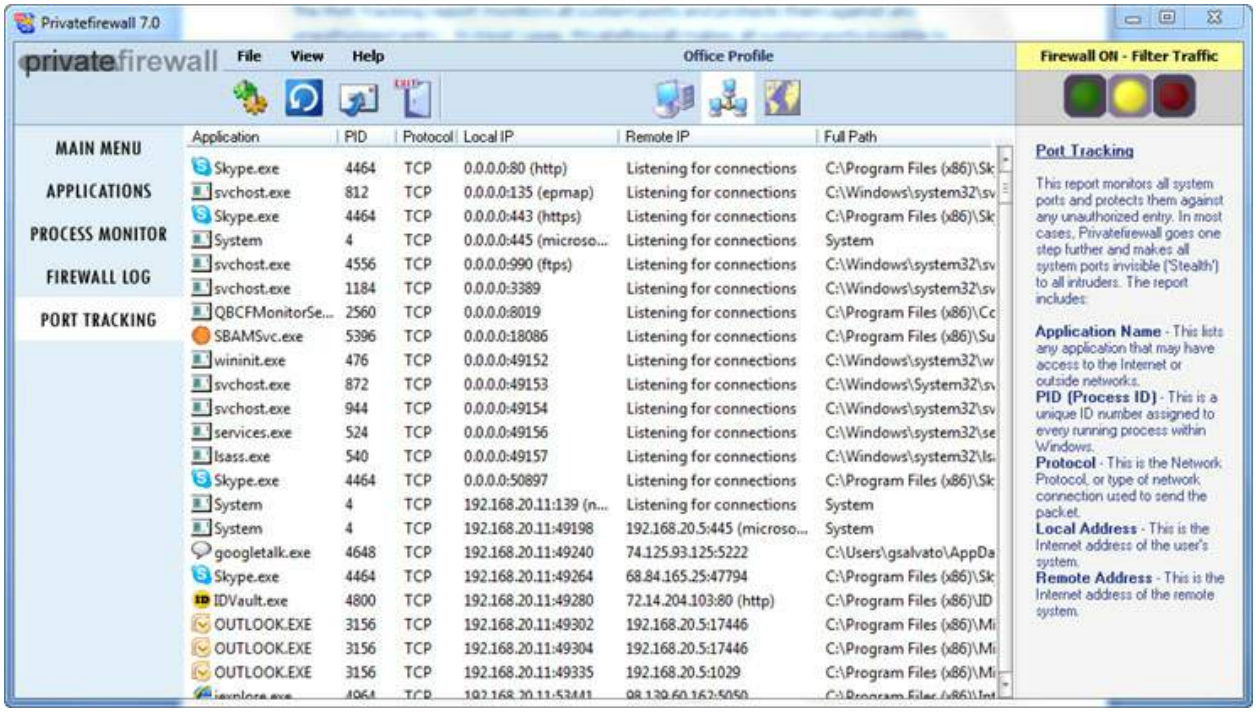
Дата и время - когда пакет был обнаружен.
Локальный IP (Интернет-адрес) - адрес в Интернете, из которого пакет поступает.
Локальный порт - порт локального компьютера, участвующего в попытке доступа.
Удаленный IP - адрес в Интернете, к которому пакет путешествует.
Удаленный порт - порт удаленного компьютера, участвующего в попытке доступа.
Протокол - сетевой протокол, или тип сетевого подключения, используемого для отправки пакета.
Приложения (если применимо) - имя приложения, к/от которому пакет отправляется (если таковые имеются).



Отслеживание Портов

Отчет на вкладке "Порты" содержит все отслеженные и защищенные от любого несанкционированного проникновения порты системы. Отчет Отслеживания Портов Privatefirewall включает следующие атрибуты:

Имя приложения - любое приложение, которое может иметь доступ к Интернету или внешней сети.
Процесс ID - уникальный номер для каждого запущенного процесса в среде Windows.
Протокол - сетевой протокол или тип сетевого подключения, используемого для отправки пакета.
Локальный адрес - IP-адрес вашей системы.
Удаленный адрес - это адрес в Интернете, где сформирован входящий пакет. Будет отображаться либо определенный IP-адрес или, если в настоящее время не обнаружен, статус (например, «прослушивание пакетов/соединения»).



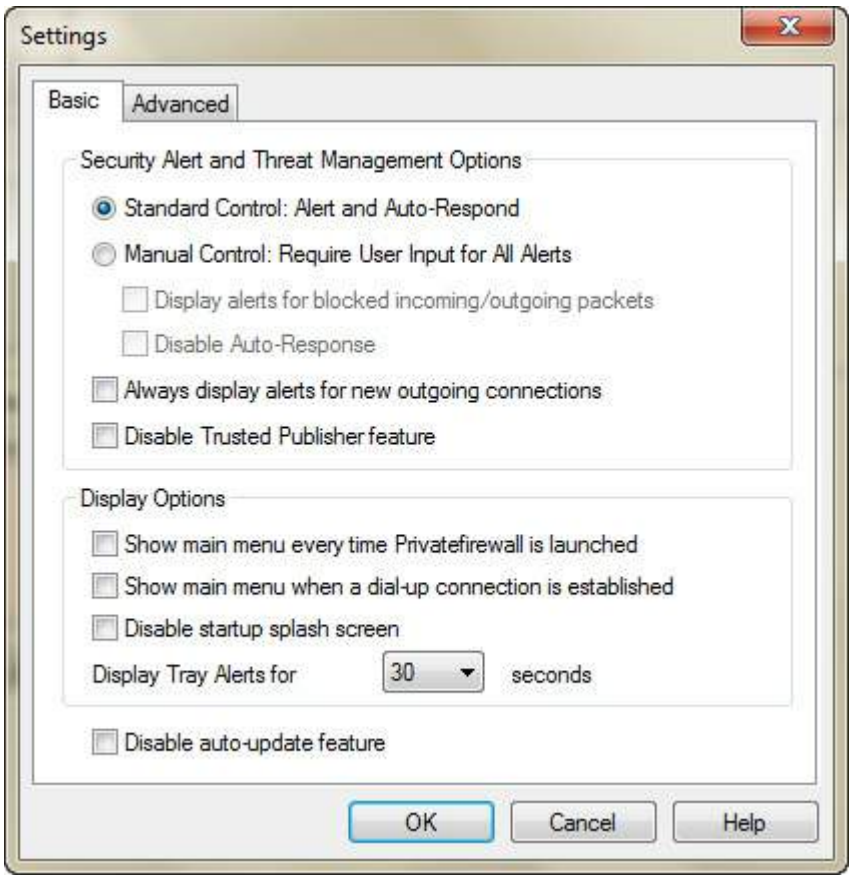
Настройки Privatefirewall

(Это меню можно вызвать, выбрав "Файл / Параметры" в главном меню)

Основные Настройки

Отображение главного меню/оповещений

Вкладка "Основные настройки" предоставляет пользователю выбрать предпочтительный режим контроля и предупреждений системы безопасности, режим управления угрозами и параметры отображения.



Стандартный режим управления

Privatefirewall предоставляет опции Предупреждения Системы Безопасности и Управления Угрозами. Стандартный Режим управления включен по умолчанию и предназначен для уменьшения частоты оповещений и автоматически управляет большей частью настроек, относящихся к безопасности.

В режиме Стандартного Контроля приложения и процессы с действительной цифровой подписью, независимо от PID, будут разрешены без генерации оповещения и добавятся в список Доверенных Издателей.

- **Исключение 1**: Для любого приложения/процесса будут создаваться оповещения (fw) для входящего трафика, что не был записан в период обучения. PF будет автоматически блокировать событие, если пользователь не разрешил его через сообщение в трее или в окне полного оповещения.

Все приложения/процессы, которые не прошли проверку подписи вызовут предупреждение и будут блокироватся по умолчанию, если не будут разрешены пользователем в таймаут оповещения (30 секунд), или путем выбора кнопки "Разрешить" в окне полного сообщения.

В режиме Стандартного Контроля, нажатие на кнопку "Разрешить" должно предотвратить, где возможно разрешить (см. Исключения), все другие оповещения, относящиеся к одному приложению. Эта логика применяется к обоим оповещениям - в трее или полном.

- **Исключение 2**: Оповещение будет возникать, если обнаружены изменения (размер, имя, версия, номер и т.д.) в файле процесса или приложения.

Ручной режим управления

Ручной режим управления предназначен для желающих иметь полный контроль над конфигурацией Privatefirewall. Большинство функциональных возможностей автоматического ответа из режима Стандартного Контроля - отключены, что требует от пользователя принятие решения по большему количеству предупреждений и настройки вручную конфигурации защиты относительно соответствующих приложений и процессов.

- Событие, формируемое процессами, перечисленными в списке Доверенных Издателей будет разрешено и не будет генерировать оповещение. По существу CAPICOM проверки не исключается создание Предупреждений в ручном режиме. Только события, инициированные программой издателя из актуального списка TP будут разрешены (и не вызовут генерацию сигнала тревоги).

- Процессы с действительной цифровой подписью, отправляющие/получающие пакеты через Интернет, независимо от PID, будут вызывать генерацию оповещения и будут разрешены по умолчанию (пользователь будет иметь опцию для блокировки события вручную через экран предупреждений).

- Процессы, которые не прошли проверку подписи вызовут генерацию оповещения и будут заблокированы по умолчанию (после окончания времени ожидания ответа в оповещении).

- Ручной режим управления обеспечивает возможность включения/отключения оповещений в трее о пакетах через пункт "Предупреждать о блокированных входящих и исходящих пакетах". Если в меню Файл-> Параметры-> Основные Настройки (режимы управления) в пункте «Предупреждать о заблокированных входящих/исходящих пакетах" флажок не установлен, межсетевой экран не отображает оповещения (для входящих/исходящих пакетов, для которых применяются правила блокирования брандмауэром, для подписанных или неподписанных приложений)

Если эта опция включена, отображается оповещение межсетевого экрана в трее, отражающее информацию о входящих/исходящих пакетах (для которых применяется правило блокировки брандмауэра для подписанных и неподписанных приложений).

Этот флажок разрешает оповещения, которые уведомляют пользователя о любом заблокированном трафике. Этот параметр не изменяет поведение больших/полных оповещений. Оповещения в трее предназначены для обеспечения видимости для всех выполняемых функций брандмауэра.

Разница между оповещением в трее и большим в том, что большие оповещения используются только, когда соответствующий пакет ассоциируется с определенным приложением на ПК (внешнее сканирование) и не был ранее заблокирован.

- Режим ручного управления предоставляет возможность отключения Авто-Реагирования вообще (Отключить Авто-Реагирование), что требует от пользователя разрешать всю деятельность, которая могла вызвать оповещение.

- Отключение Авто-Реагирования в режиме ручного управления, также, отключает Авто-Реагирование, связанное с функцией "Доверенный Издатель", и позволяет пользователю контролировать, какие приложения должны быть добавлены в TP список.

Всегда показывать предупреждения о новых исходящих соединениях
По умолчанию в стандартном и ручном режимах управления Privatefirewall авто-позволяет исходящие соединения для приложений, у которых цифровые подписи были проверены, или для приложений из списка доверенных издателей.

Параметр "Всегда показывать предупреждения о новых исходящих соединениях" переопределяет доверенных (и лежащие в их основе CAPICOM- на основе проверки цифровых сертификатов). Эта функция позволяет пользователю разрешить все новые исходящие соединения (но не распространяется на правила исходящих соединений, установленных вручную или в силу реагирования на предупреждение).

Существует функциональная разница между режимами Стандартный и Ручной Контроль. Стандартный режим предполагает, что если допускается одно исходящее подключение из приложения, то и все остальные должны допускаться.

Ручной режим позволяет пользователю влиять на правила для каждого типа соединения. В некоторых случаях, вы вручную можете разрешить доступ конкретному приложению, создающему очередь из нескольких исходящих соединений (часто аналогичных, но тем не менее разных) и, таким образом, будет получено множество предупреждений.

Privatefirewall позволяет использовать конфигурации, которые обеспечивают различные уровни управления, в зависимости от личных предпочтений, для безопасности и простоты использования.

Если используется режим Ручного Контроля и опция "Всегда отображать оповещения для новых исходящих соединений" включена, и не поставлена галочка "Запомнить этот параметр", правило связанное с определенным типом подключения будет применяться только для текущей сессии (после перезагрузки правило будет больше недействительным в настоящее время).
Независимо от того, какие оповещения безопасности и какой режим управления угрозами включен, заблокированные процессы будут оставаться в списке по пути Файл-> Параметры-> Расширенные Настройки-> Просмотр/редактирование Списка приложений, и пользователь может изменить для любого заблокированного процесса статус на "Разрешить", если это уместно.

На экране предупреждение будет отображаться немедленно как только обнаруживаются потенциальные угрозы. Оповещение предоставляет сведения о событии и варианты управления угрозой. Предупреждение в трее не будет отображаться при выборе этого параметра (Смотри раздел данного руководств Privatefirewall Настройки -> Оповещение системы безопасности и Опции управления угрозами для получения дополнительной информации о фильтрации событий и предупреждениях).

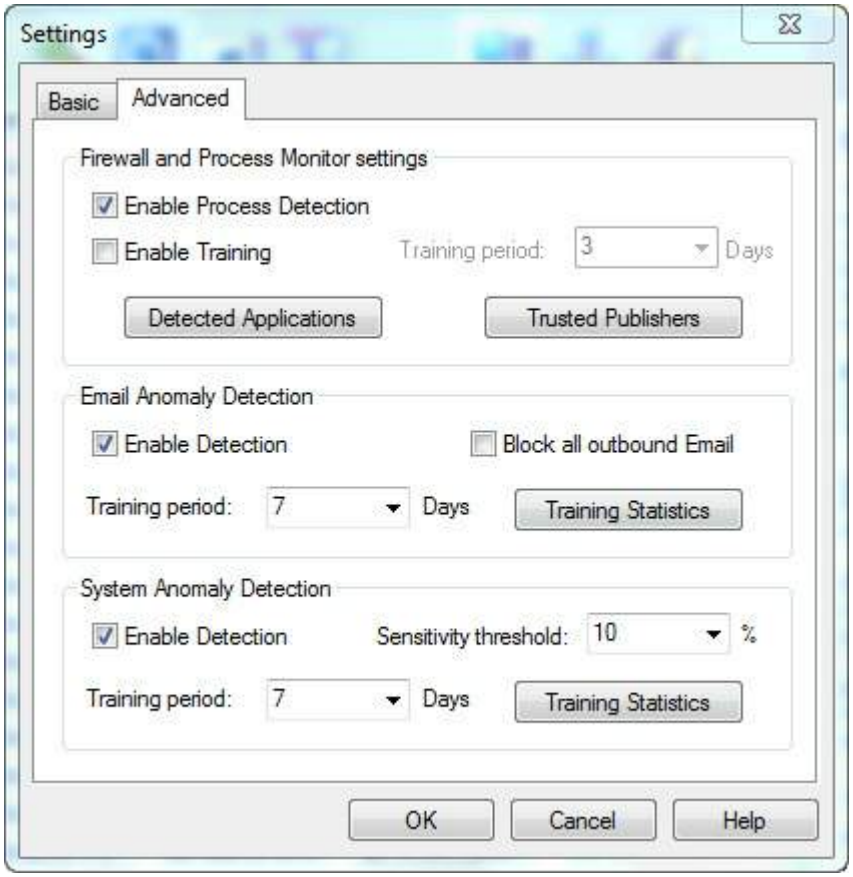
Настройки Межсетевого Экрана и Процесс Монитора

После установки Privatefirewall, вы сначала можете наблюдать многочисленные предупреждения Обнаружений Приложений и Процесс Монитора, пока Privatefirewall не установит правила для всех интернет-приложений и WinAPI, по мере обнаружения запущенных процессов. Если вы предпочитаете, можно задать период «Обучения» для этих типов предупреждений, так что правила будут устанавливаться без оповещения в период обучения. При завершении Обучения, частота оповещений будет уменьшена, так как будет создано много правил для набора часто используемых приложений и процессов. Предупреждение будет отображаться на экране сразу же, как обнаруживаются потенциальные угрозы. Предупреждение предоставляет сведения о событии и параметры управления угрозой. Оповещения в трее не будут отображаться, когда выбран этот параметр.

Примечание: Режим обучения не является необходимым, но может быть включен для уменьшения числа оповещений, когда, например, устанавливается новое программное обеспечение. В процессе обучения только приложения/процессы, которые не проходят проверку подписи и попытались отправить или получить пакеты через Интернет, будут вызывать генерацию оповещения и заблокируются по умолчанию, если не будут разрешены пользователем до окончания времени ожидания в оповещении (30 секунд) в трее или разрешены в окне полного оповещения.

Расширенные Настройки

Вкладка **Расширенные Настройки** диалогового окна Параметры позволяет включить или отключить обнаружение процесса, обнаружение системных и электронной почты аномалий, включить период Обучения, указать продолжительность обучения и порог чувствительности, содержит обзор и управление обнаруженными приложениями и список Доверенных Издателей.



Обнаружение Аномалий Электронной Почты

Эта функция отслеживает поведение исходящей электронной почты и предоставляет оповещения, если есть необычная деятельность. Механизм обнаружения аномалий электронной почты основан на поведении конкретного компьютера, при отправке электронной почты, во время периода обучения. Этот период может быть установлен в 7 (по умолчанию), 14 или 28 дней в меню настроек. Для того, чтобы начать обучение, должен быть установлен флажок «Включить обнаружение». Механизм обнаружения аномалий начнет работать сразу же после окончания учебного периода. Вы также можете просмотреть статистику обучения во время или после периода обучения.

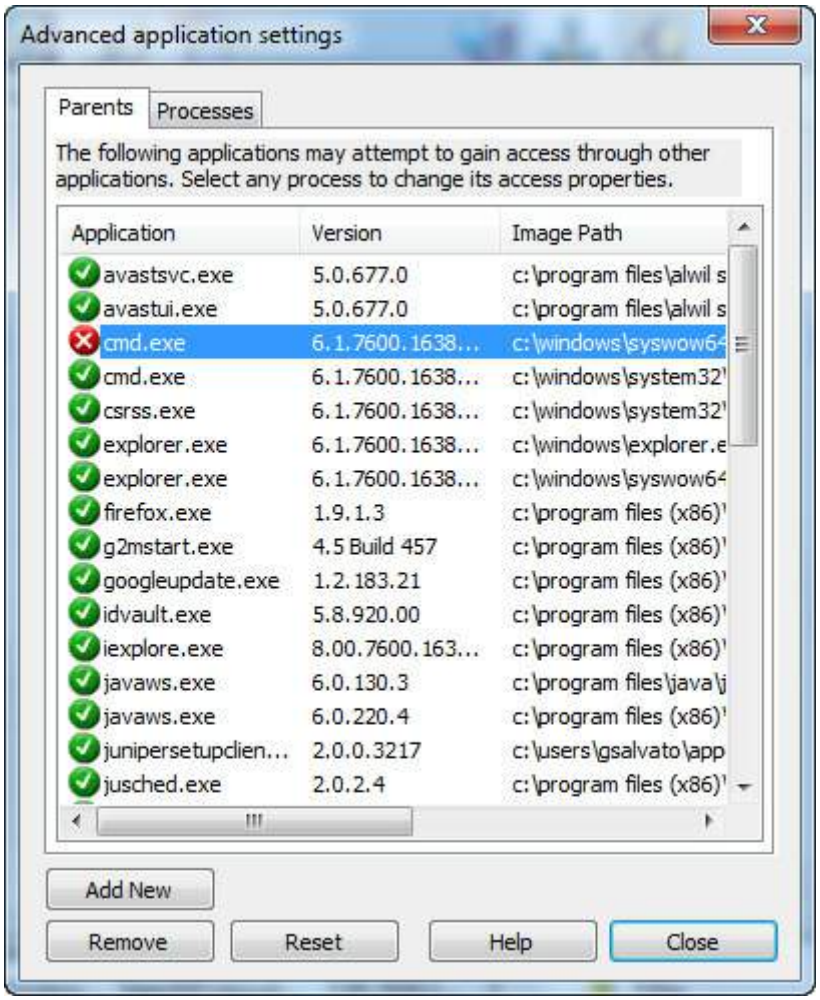
Примечание: В Privatefirewall в профилях исходящей почты заданы по умолчанию порты SMTP - 25 или 465. Если ваш сервер SMTP настроен на использование порта, отличного от 25 или 465, функция обнаружения аномалий электронной почты не будет работать.

Обнаружение Системных Аномалий

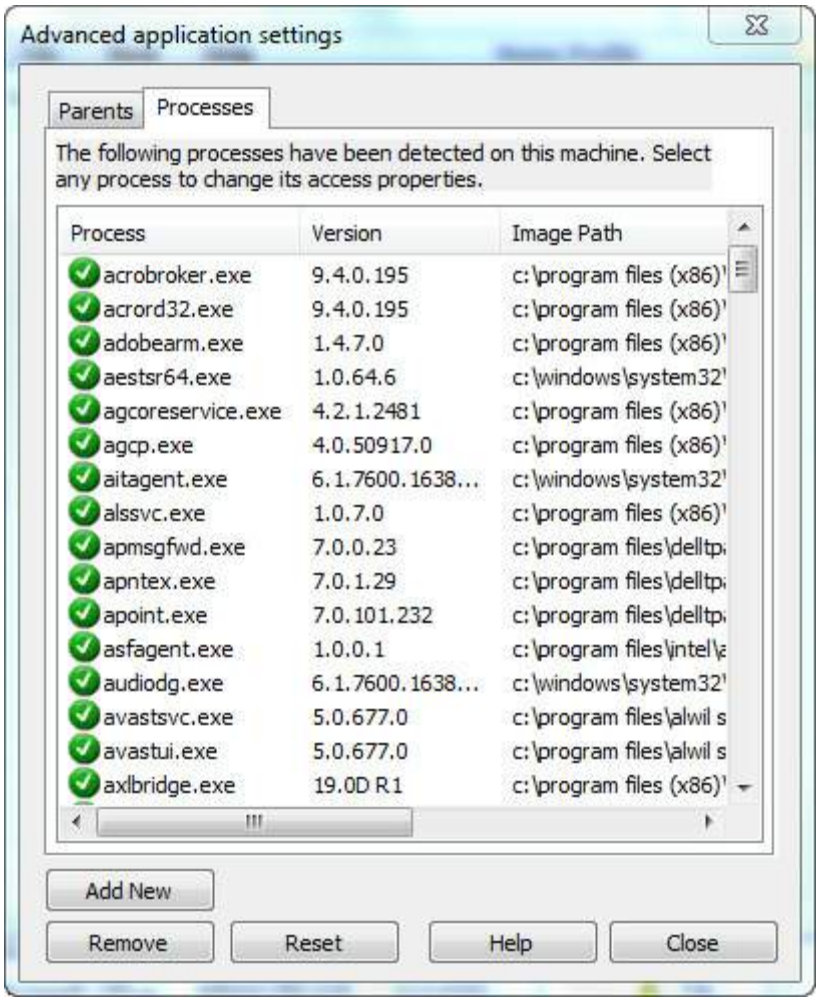
Эта функция анализирует закономерности нормального использования приложений и создает оповещения, когда обнаруживаются необычные действия. Механизм обнаружения аномалий системы применяет сложный алгоритм для установления базового уровня нормального использования системы, основанный на нескольких системных переменных, таких как использование CPU, количество потоков и других. Эти переменные наблюдаются в течение определенного периода времени обучения, который может быть установлен в 7 (по умолчанию), 14 или 28 дней в главном меню. Флажок «Включить обнаружение» должен быть установлен для активации обучения. Обучение в Privatefirewall включено по умолчанию и начинается сразу же после установки программы.

Обнаружение Приложений

Нажмите кнопку "Обнаруженные Приложения" для вызова на экран списка родителей. Все приложения, которые пытались получить доступ к Интернету или сети через другое доверенное приложение, перечисленны здесь. Вкладка содержит Имя приложения, Номер версии, путь к исполняемому файлу. Каждому приложению в списке можно задать параметр Разрешить или Запретить доступ.

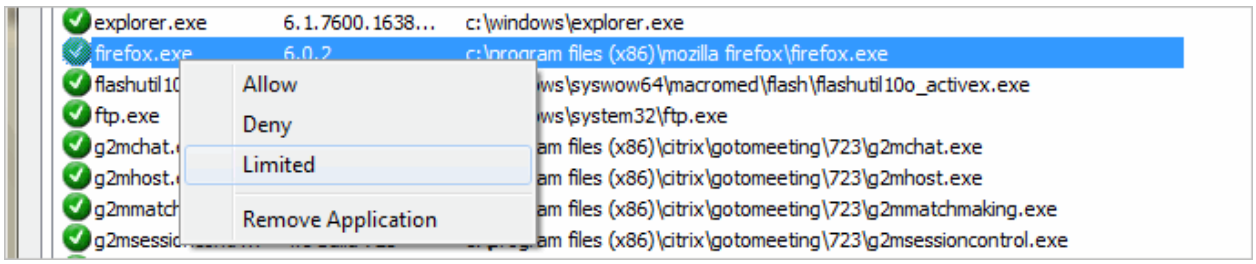


На вкладке Процессы перечислены часто используемые процессы. PF отображает оповещение, если неизвестный процесс пытается запуститься. Вкладка содержит Имя процесса, Номер версии и Путь к исполняемому файлу. Каждому приложению в списке может быть установлен параметр Разрешить или Запретить доступ.



Управление Правами Процессов

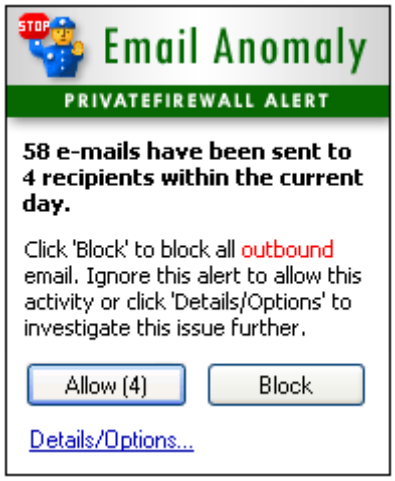
Процессы могут быть запущены с ограниченными правами непосредственно через соответствующее сообщение в трее или окно расширенного сообщения, но могут, также, управляться через вкладку Процессы в окне "Расширенные настройки приложений". Просто выделите процесс и, щелкнув правой кнопкой мыши, выберите "Разрешить", "Отказать", "Удалить" или "Работать с Ограниченными правами".



Обнаружение Аномалий Электронной Почты

Оповещения Обнаружений Аномалий Электронной Почты

Существует несколько предупреждений, которые могут быть отображены на основе типа и объема сообщений электронной почты в течение определенного периода времени. Если есть оповещение, а характер необычной активности электронной почты неизвестен, возможно, более разумно нажать кнопку "Блок" в рамке оповещения в трее, чтобы убедиться, что нет никаких червей или вирусов, вызывающих активность. Если характер деятельности определяется как безопасный, то параметр "Блокировать все исходящие сообщения электронной почты" должен быть отключен в меню настройки или в меню панели инструментов.

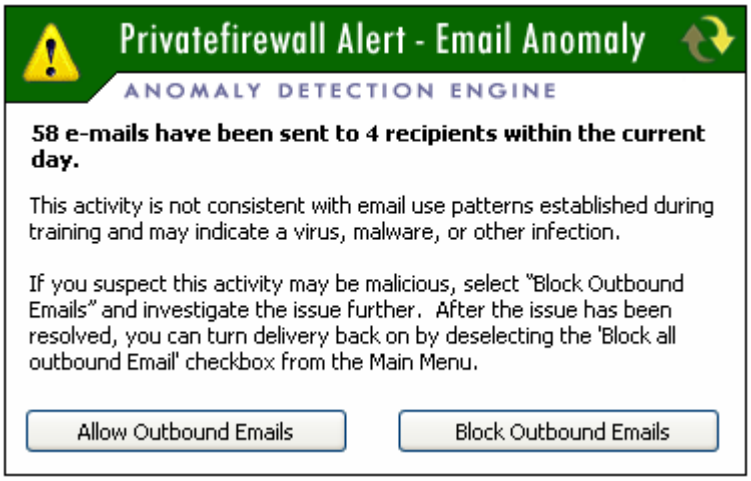


Разрешить доставку 

Блокировать доставку 

ПРИМЕЧАНИЕ: Privatefirewall будет отображать оповещение в трее 30 секунд. Если не принимать никаких мер, время предупреждения истечет и деятельность будет разрешена.

Нажмите кнопку «Подробно/Опции» в сообщении в трее для отображения расширенного оповещения, которое содержит больше подробной информации.

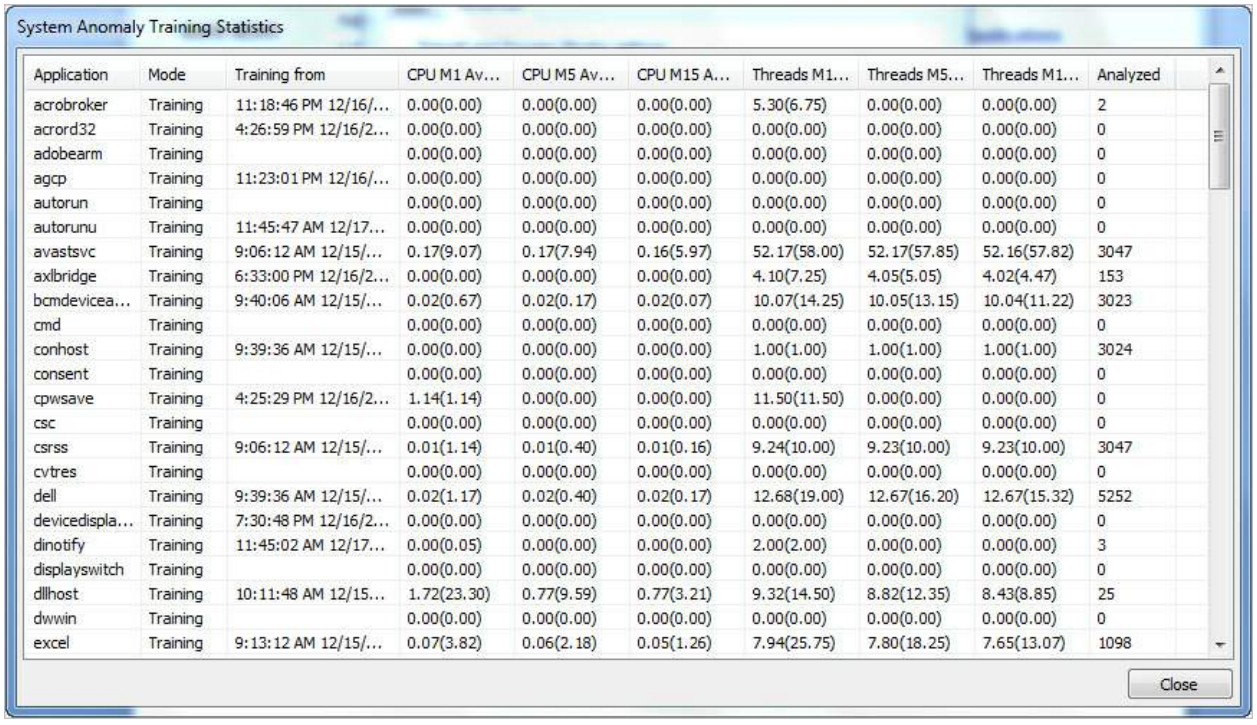


Примечание: Privatefirewall отслеживает исходящие незашифрованные сообщения электронной почты по умолчанию только через SMTP порты - 25 или 465. Для сообщений электронной почты, чтобы работала функция Обнаружение Аномалий, необходимо использовать один из этих портов, и чтобы сообщения электронной почты не передавались в незашифрованном виде.

Обнаружения Аномалий Системы

Функция Обнаружения Аномалий Системы анализирует закономерности нормального использования запущенных приложений и создает оповещения, когда обнаруживает необычные действия. Механизм обнаружения аномалий системы применяет сложный алгоритм для определения исходных условий нормальной эксплуатации на основе нескольких системных переменных, таких, как использование процессора, количество потоков и другие. Эти переменные отслеживаются за определенный период времени, называемый «Период обучения», который может быть равным 7 (по умолчанию), 14 или 28 дней и задается в главном меню. Флажок «Включить обнаружение» должен быть установлен, чтобы режим обучения был активным. После установки Privatefirewall по умолчанию обучение включено и начинается сразу же после установки.

Порог чувствительности: Обнаружение Аномалий Системы Privatefirewall создает оповещения, когда обнаруживает активность системы, которая отклоняется от нормальной. Чувствительность, с которой Privatefirewall реагирует, обнаружив аномалию системы, может быть настроена путем корректировки Порога чувствительности. Уменьшение порога увеличивает чувствительность, это означает, что небольшие отклонения будут генерировать предупреждения. Увеличение порогового значения позволит большее отклонение от обычной деятельности. По умолчанию, порог чувствительности обнаружения аномалий системы имеет значение 60%, что означает, что любая деятельность, откличающаяся более чем на 60% от нормальной, будет вызывать оповещение.

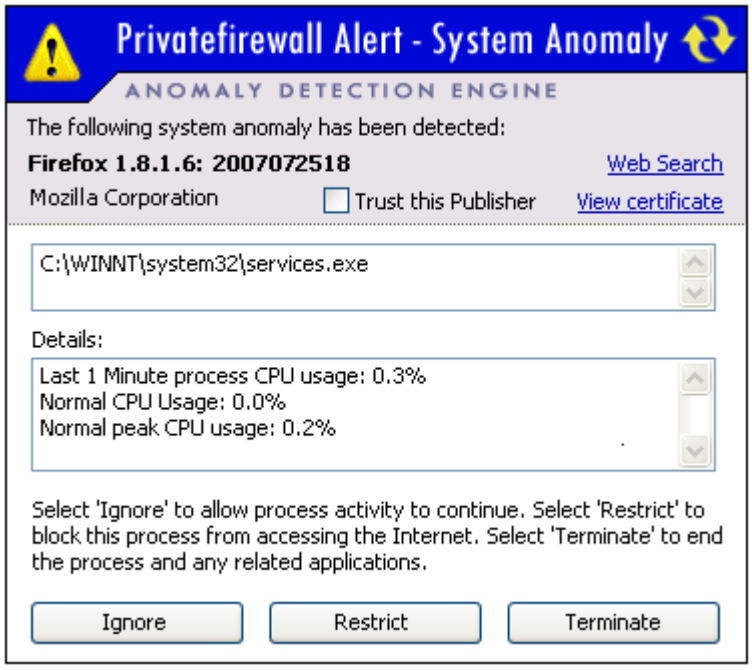


Application	Mode	Training from	CPU M1 Av...	CPU M5 Av...	CPU M15 A...	Threads M1...	Threads M5...	Threads M1...	Analyzed
acrobroker	Training	11:18:46 PM 12/16/...	0.00(0.00)	0.00(0.00)	0.00(0.00)	5.30(6.75)	0.00(0.00)	0.00(0.00)	2
acrord32	Training	4:26:59 PM 12/16/2...	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
adobearm	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
agcp	Training	11:23:01 PM 12/16/...	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
autorun	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
autorunu	Training	11:45:47 AM 12/17...	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
avastsvc	Training	9:06:12 AM 12/15/...	0.17(9.07)	0.17(7.94)	0.16(5.97)	52.17(58.00)	52.17(57.85)	52.16(57.82)	3047
axlbridge	Training	6:33:00 PM 12/16/2...	0.00(0.00)	0.00(0.00)	0.00(0.00)	4.10(7.25)	4.05(5.05)	4.02(4.47)	153
bcmdevicea...	Training	9:40:06 AM 12/15/...	0.02(0.67)	0.02(0.17)	0.02(0.07)	10.07(14.25)	10.05(13.15)	10.04(11.22)	3023
cmd	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
conhost	Training	9:39:36 AM 12/15/...	0.00(0.00)	0.00(0.00)	0.00(0.00)	1.00(1.00)	1.00(1.00)	1.00(1.00)	3024
consent	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
cpwsave	Training	4:25:29 PM 12/16/2...	1.14(1.14)	0.00(0.00)	0.00(0.00)	11.50(11.50)	0.00(0.00)	0.00(0.00)	0
csc	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
csrss	Training	9:06:12 AM 12/15/...	0.01(1.14)	0.01(0.40)	0.01(0.16)	9.24(10.00)	9.23(10.00)	9.23(10.00)	3047
cvtres	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
dell	Training	9:39:36 AM 12/15/...	0.02(1.17)	0.02(0.40)	0.02(0.17)	12.68(19.00)	12.67(16.20)	12.67(15.32)	5252
devicedispla...	Training	7:30:48 PM 12/16/2...	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
dinotify	Training	11:45:02 AM 12/17...	0.00(0.05)	0.00(0.00)	0.00(0.00)	2.00(2.00)	0.00(0.00)	0.00(0.00)	3
displayswitch	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
dllhost	Training	10:11:48 AM 12/15...	1.72(23.30)	0.77(9.59)	0.77(3.21)	9.32(14.50)	8.82(12.35)	8.43(8.85)	25
dwwin	Training		0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0.00(0.00)	0
excel	Training	9:13:12 AM 12/15/...	0.07(3.82)	0.06(2.18)	0.05(1.26)	7.94(25.75)	7.80(18.25)	7.65(13.07)	1098

Выбор кнопки "Статистика обучения" будет отображать сведения о поведении системы, собранные во время обучения. Они могут просматриваться во время или после периода обучения.

Механизм обнаружения аномалий начнет работать сразу после окончания учебного периода и будет генерировать предупреждение в трее (см. справа) всякий раз, когда есть какая-либо деятельность, не соответствующая модели использования системы, созданной в период обучения. Если есть оповещение и характер деятельности неизвестен, то может быть разумным выбор кнопки «Подробно/Опции» на оповещении в трее, чтобы открыть расширенное оповещение (см. ниже) и получить более подробную информацию о характере активности и дополнительные опции управления угрозой.

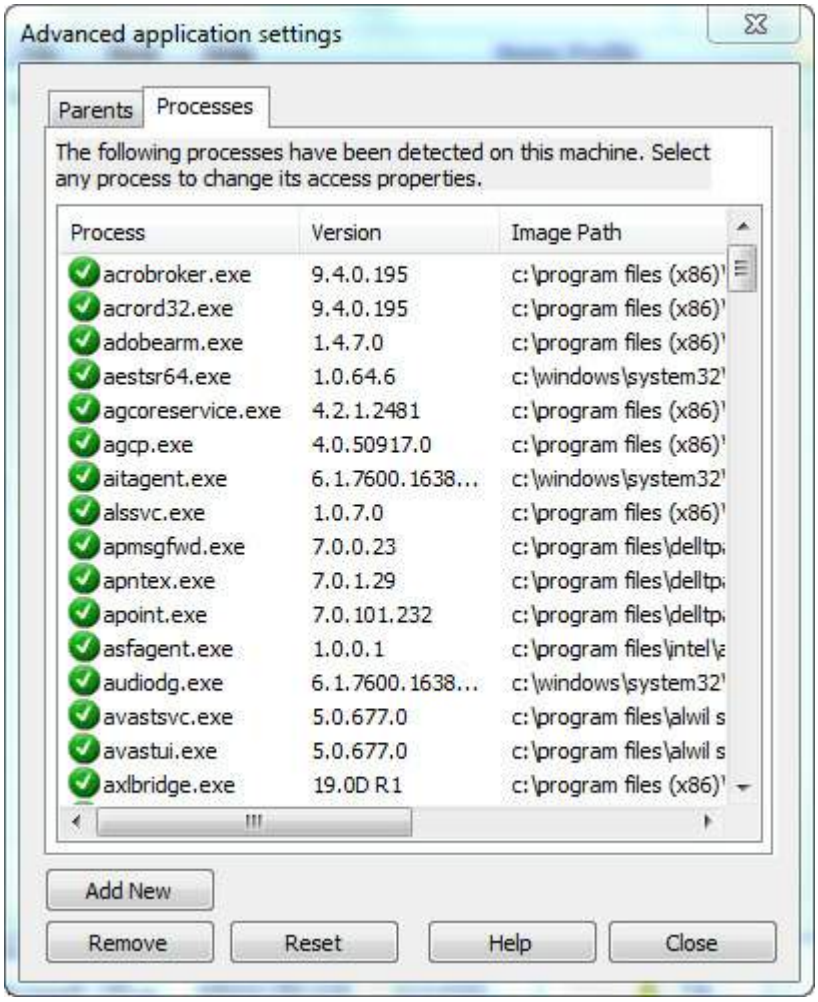
ПРИМЕЧАНИЕ: Privatefirewall будет отображать оповещение в трее 30 секунд. Когда время предупреждения истечет, деятельность будет допущена.



Если выбрана ссылка Веб-поиск, поиск по имени исполняемого файла ('Services.exe'в оповещении ниже) будет выполняться в браузере по умолчанию.

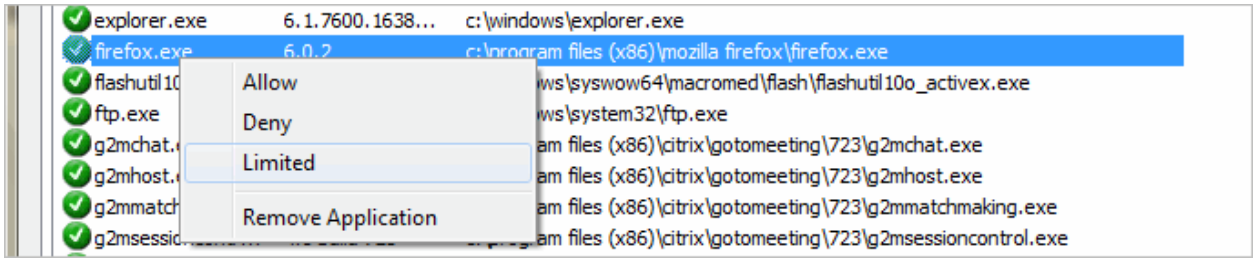
Обнаружение Процессов

Эта функция записывает все процессы, которые запускаются в период «Обучения», который может быть установлен в 1, 3 или 7 дней (см. раздел Дополнительные параметры). Обучение включено по умолчанию и начинается в течение десяти минут, сразу после установки. Расширенный период обучения продолжительностью 1, 3, 7 или 14 дней можно задать при необходимости. Перечисленные процессы можно просмотреть в любое время, выбрав вкладку «Процессы» в окне "Расширенные настройки приложений".

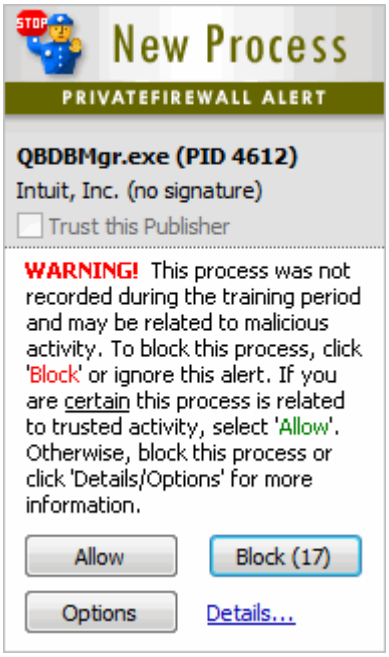


Управление Правами Процессов

Процессы могут быть запущены с ограниченными правами непосредственно через соответствующее оповещение в трее или полное оповещение, а также, через вкладку "Процессы" в окне "Расширенные настройки приложений". Просто выделите процесс и, щелкнув правой кнопкой мыши, выберите "Разрешить", "Отказать", "Удалить" или "Работать с ограниченными правами".

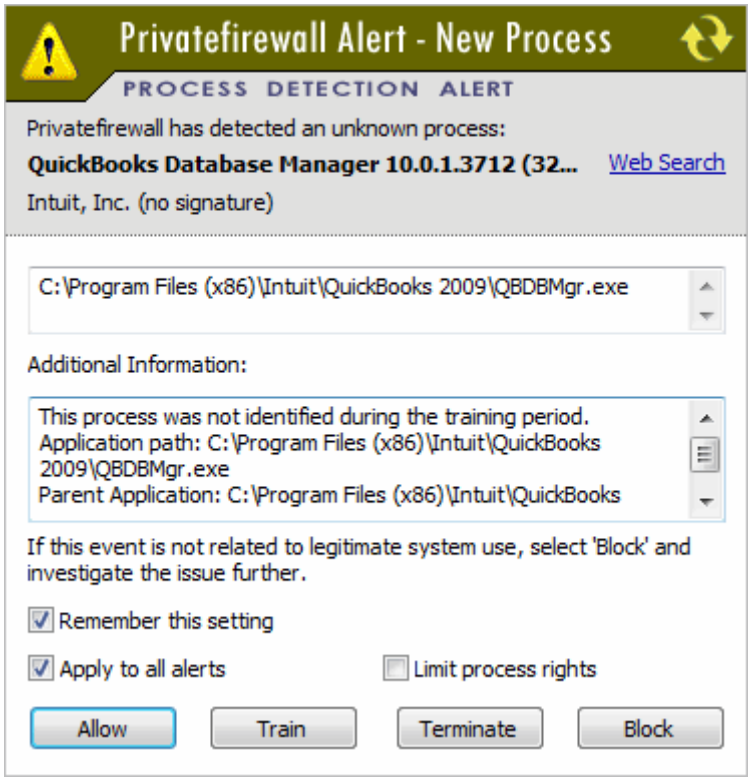


После завершения учебного периода, Privatefirewall будет генерировать предупреждение в трее (см. справа), когда любой процесс, который не был записан в период обучения, попытается запуститься. Если процесс связан с известной /доверенной деятельностью, этот процесс должен быть допущен и, затем, добавлен в список доверенных процессов.



Нажмите кнопку «Подробнее» в сообщении для отображения расширенного оповещения (см. ниже), которое содержит более подробную информацию о подозрительной активности и дополнительные опции управления угрозой. Если чек_бокс на вкладке главного меню "Параметры / Основные параметры" «По всем угрозам решение принимает пользователь» отмечен, расширенное оповещение будет появляться автоматически, а оповещение в трее не будет отображаться. Если выбрана ссылка «Веб-поиск», поиск по имени исполняемого файла будет осуществляться в вашем браузер по умолчанию.

ПРИМЕЧАНИЕ: Privatefirewall будет отображать сообщение 30 секунд. Если решение не принято, а время истечет, эта деятельность будет заблокирована.



При Ручном Управлении, если параметр “Всегда показывать предупреждения для исходящих соединений" включен, и бокс **"Запомнить этот параметр"** не отмечен, правило, связанное с этим особым типом соединения работает только для текущей сессии (после перезагрузки, правило не будет больше в силе в настоящее время).

Выбор опции "**Применить для всех оповещений**" исключит отображение дополнительных оповещений Процесс Монитора для этого приложения, реагируя на последующие действия на основанни ответа на первое предупреждение.

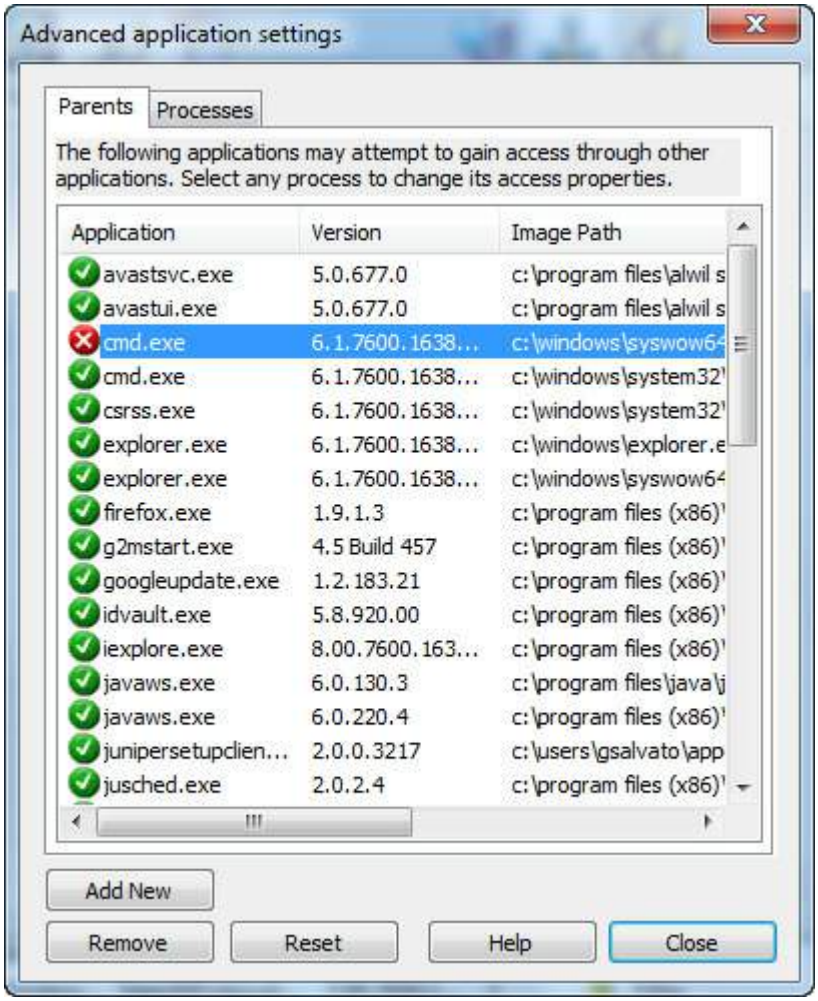
Выбор параметра "**Ограничить права процесса**" позволяет этому процессу выполняться с пониженными правами (эту установку можно измененить через клик правой кнопки мыши на процессе на вкладке "Расширенные настройки приложений / Процессы").

Если процесс пытается загрузить, что ранее было проигнорировано или заблокировано, Privatefirewall создаст оповещение с выбором действия "Разрешить" или "Блокировать" ранее заблокированную деятельность.

Расширенные Настройки Приложений

(Доступно из меню Файл/Параметры/Расширенные Настройки Приложений)

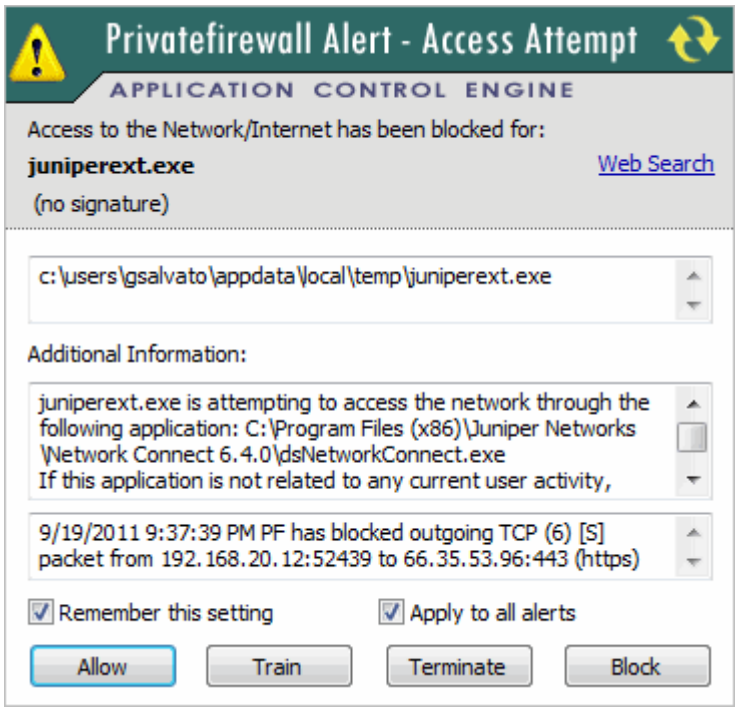
Некоторые приложения позволяют другим приложениям контролировать свои действия, это означает, что 'основное' приложение может быть защищено, но родительское приложения может получить доступ к сети Интернет через основное приложение. В окне "Расширенные настройки приложений" перечислены эти родительского приложения, которые пытались получить доступ к Интернету или сети через «основное» доверенное приложение. Каждму приложению в списке может быть присвоен параметр Разрешить или Заблокировать доступ.



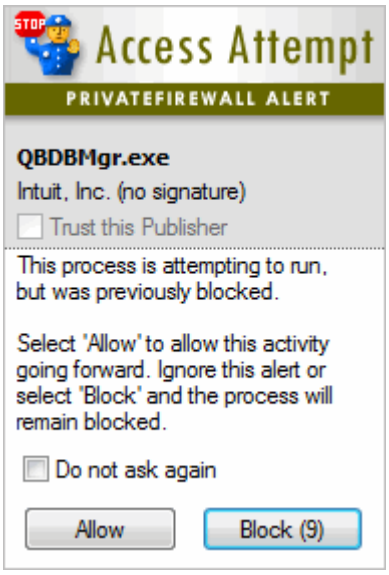
Хотя этот метод часто используется хакерами для получения несанкционированного доступа, он, также, является функцией многих «доверенных» приложений, работающих нормально при доступе к Интернет. Если вы находитесь в процессе доступа в Интернет с помощью приложения, имена 'вторичных ' или родительских приложений могут не быть общими или узнаваемыми, поэтому может быть трудно определить, является ли действие нормальным или вредоносным. Если вы получили оповещение и деятельность процесса связана с любой формой текущей активности, то это, скорее, не вредоносных деятельность. Однако, если она не связана (т.е. ссылка на приложение даже не открыта, и т.д.), это может быть попыткой несанкционированного доступа и надо нажать кнопку 'Блок', чтобы, таким образом, можно было исследовать вопрос.

ПРИМЕЧАНИЕ: Privatefirewall будет отображать тревогу 30 секунд. Если не принимать никаких мер, время истечет, и эта деятельность будет заблокирована.

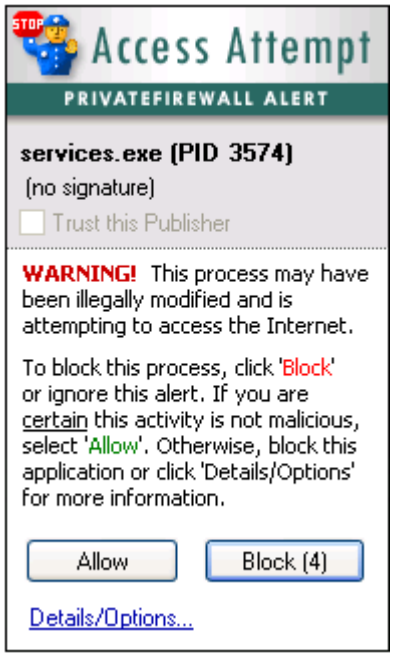
Нажмите кнопку «Подробно/Опции» в сообщении трея для отображения Расширенного оповещения, которое содержит более подробную Информацию о подозрительной активности и дополнительные опции управления угрозой. В данном предупреждении перечислены: имя программы, номер версии, дата, время, входящие/исходящие IP-адреса и родительское приложение, которое пытается получить доступ. В нем, также, будет указано, является ли трафик входящим или исходящим. Если выбрана ссылка 'Веб-поиск', поиск по имени исполняемого файла будет осуществляться в вашем браузере по умолчанию.



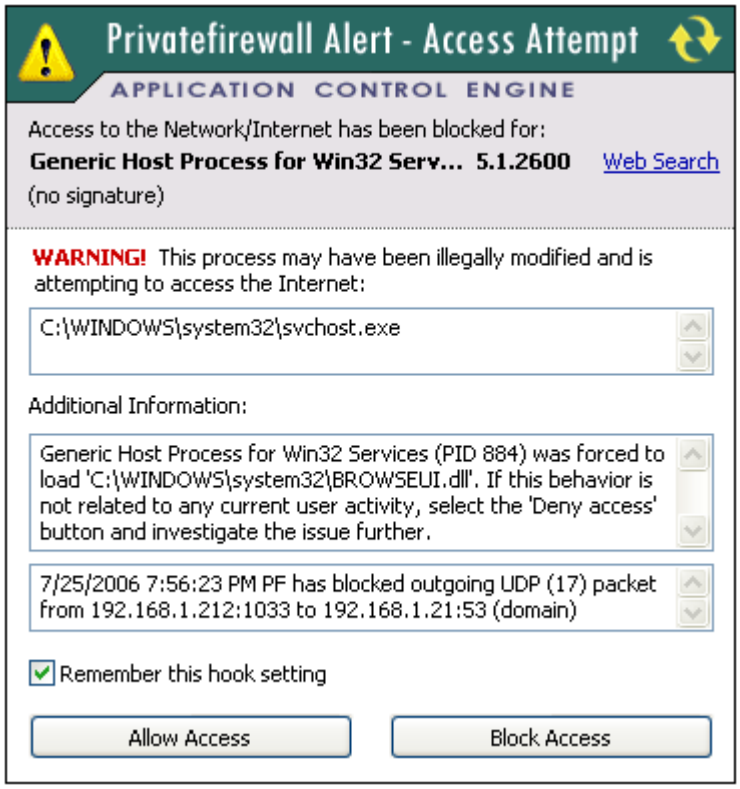
Если приложение пытается загрузить, что было ранее проигнорировано или заблокировано, Privatefirewall создаст следующее предупреждение.



Другой тип возможной атаки, когда процесс незаконно изменен и запущен и пытается получить доступ в Интернет. При этом будет создано иное предупреждение (см. справа). Если вы получаете такое предупреждение, действовать надо осторожно и тщательно расследовать этот вопрос, чтобы убедиться, что нет вредоносной деятельности.



Нажмите кнопку «Подробно/Опции» в окне тревоги для отображения расширенного предупреждения (см. ниже), которое содержит более подробную информацию о подозрительной активности и дополнительные варианты управления угрозой.



Надежный издатель

(Доступ Файл/Параметры/Доверенный Издатель)

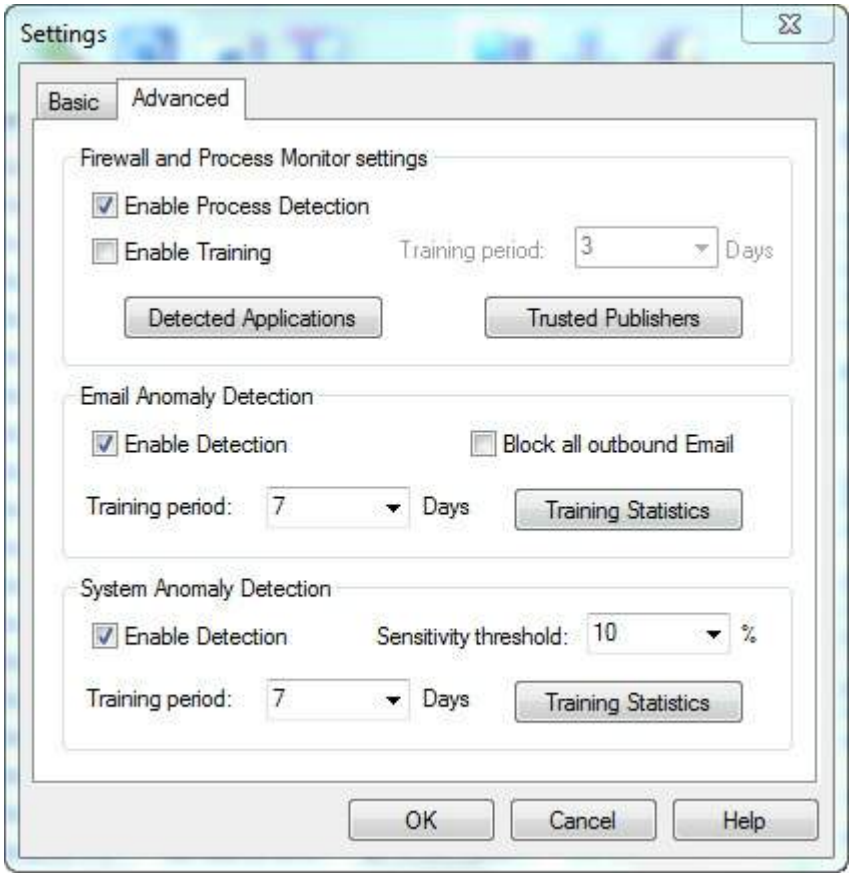
Обзор функций

Privatefirewall использует сочетание обычных и прогрессивных технологий (межсетевой экран, монитор процессов, системные и программные поведенческие профили, обнаружение аномалий и т.д.), чтобы обеспечить максимально возможный уровень безопасности для индивидуальных и корпоративных ПК. Для повышения безопасности и простоты использования, Privatefirewall предоставляет возможность составить (белый список) программного обеспечения от доверенных издателей – те, которые были предварительно утверждены и/или где цифровые подписи программного обеспечения были автоматически проверены Privatefirewall.

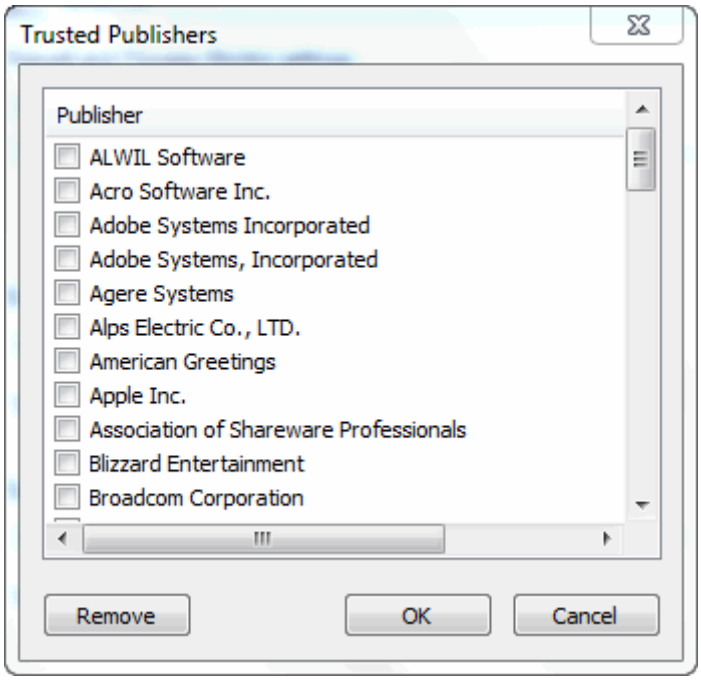
В Privatefirewall Доверенный Издатель включает в себя список предварительно утвержденных поставщиков популярных безопасных, производительных и других общеизвестных настольных приложений, но, главным образом, защитную функцию выполняет его белый список с помощью динамической проверки, когда новые приложения запускаются в первый раз. Когда первый раз издатель программного обеспечения (поставщик) был добавлен к списку, Privatefirewall позволит (без предупреждения или блокировки) любую программу, связанную с этим надежным издателем программного обеспечения, проверив сертификат.

Доступ к функции Доверенный Издатель

Для доступа к функции доверенного издателя, щелкните Файл/Параметры, выберите вкладку "Расширенные настройки" и щелкните кнопку Доверенные Издатели.



Окно Доверенных Издателей отображает список издателей программного обеспечения (по умолчанию добавленных после установки), для которых были предварительно проверены сертификаты. Одного или несколько издателей можно удалить из списка, выделив и нажав кнопку **Удалить.**



Отключение функции Доверенного Издателя

Доверенный издатель может быть отключен. Для этого щелкните файл > параметры и поставьте флажок в чек_бокс с надписью "Отключить функцию Доверенный Издатель" на вкладке Основные.

Как работает Доверенный Издатель

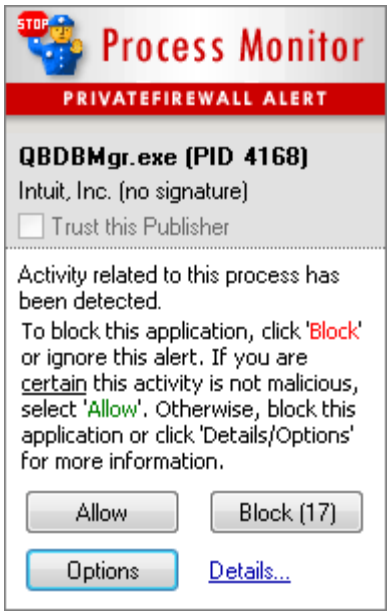
За исключением аномалий эл. почты, Privatefirewall будет подавлять предупреждения любого типа для издателей программного обеспечения, которые были добавлены (по умолчанию или во время запуска) в список доверенных издателей. Этот раздел будет описывать, как, в этом случае, Privatefirewall обеспечивает это через свою функцию Доверенного Издателя.

Оповещение в Трее

Когда Privatefirewall обнаруживает деятельность (доступ приложения в Интернет, новый процесс и т.д..), создаются один или несколько типов оповещений. Если Privatefirewall сможет проверить сертификат издателя программного обеспечения и подпись, связанные с приложением, которое вызвало оповещение Privatefirewall, функция Доверенного Издателя будет «активной», это означает, что чек_бокс слева от фразы "Доверять этому Издателю", можно отметить флажком (как показано в примере ниже).

Через окно оповещения конечный пользователь может просмотреть основную информация о событии, которое вызвало предупреждение и установить флажок Доверять этому Издателю, если он уверен в том, что деятельность приложения законная и что Издателю программного обеспечения можно доверять и далее. За исключением сообщений обнаружения аномалий электронной почты, Privatefirewall будет подавлять предупреждения любого типа для поставщиков программного обеспечения из списка доверенных издателей.

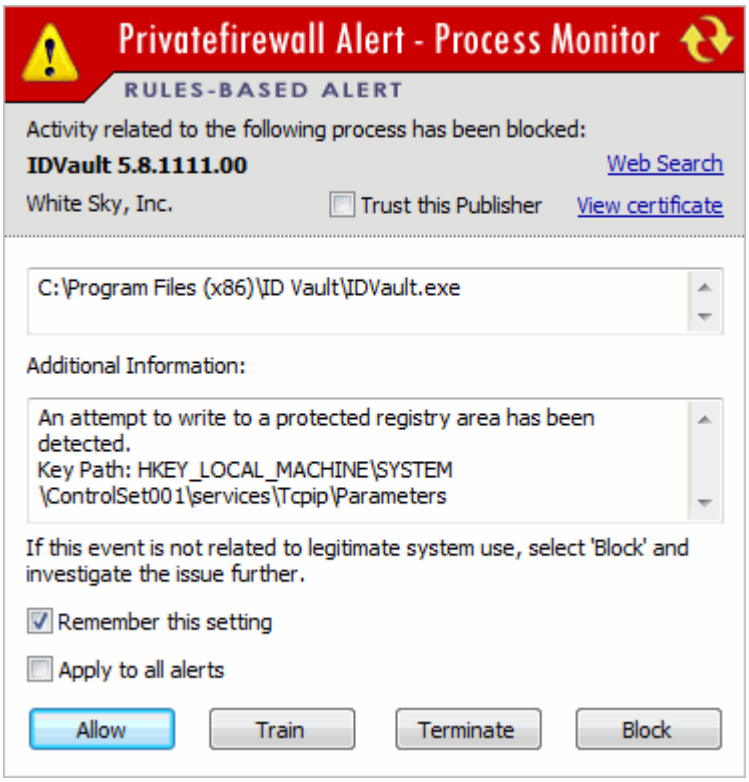
Дополнительные сведения о событии можно просмотреть, нажав на ссылку Подробно/Опции в левом нижнем углу оповещения в трее, которая вызывает окно полного оповещения. Обратитесь к разделу "Расширенное Оповещение" этого руководства за дополнительной информацией.

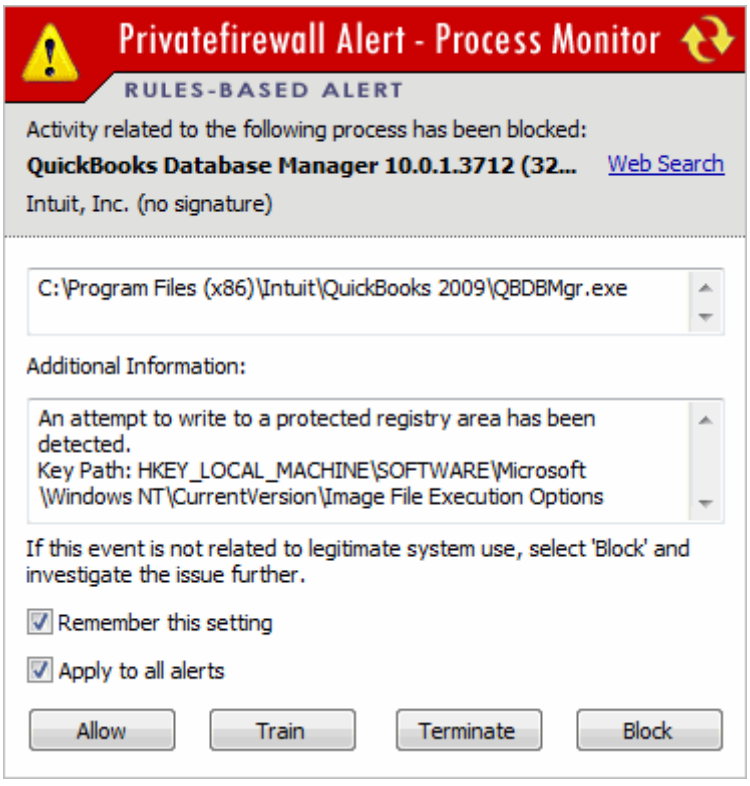


Если Privatefirewall не удается проверить сертификат издателя или может обнаружить сертификат издателя, но не в состоянии убедиться, что приложение было подписано, чек_бокс "Доверять этому Издателю" будет недоступен (отображается серым цветом).

Расширенное Оповещение

При клике на кнопку Подробно /Опции (ссылка в нижнем углу в окне трея), будет открыто Расширенное Оповещение, как показано в этом примере > В Расширенном Оповещении есть подробная информация о подозрительной активности и возможность проведения Web Поиска, чтобы узнать больше о процессе или приложении. Есть, также, возможность просмотра сертификата издателя программного обеспечения (смотреть сертификат)





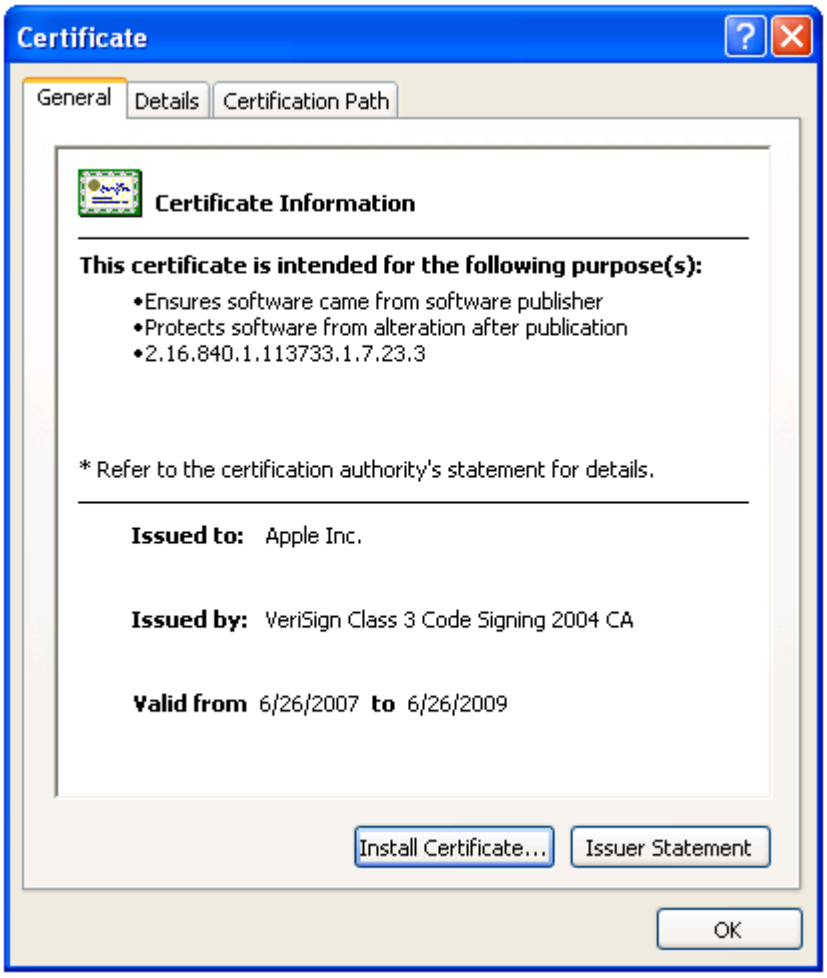
Если Privatefirewall не в состоянии проверить сертификат издателя программного обеспечения, в Расширенном Оповещении будет дополнительная информация и подробности, касающиеся события, а, также, возможность выполнить поиск в Интернете, но не будет ссылки на просмотр сертификата издателя программного обеспечения.

Веб-поиск

Как и предполагает название, нажатие на ссылку "**Веб-Поиск**" в Расширенном Оповещении будет вызывать поиск в Интернете через браузер по умолчанию для процесса, приложения или по другому вопросу, связанному с предупреждением. Эта функция упрощает получение четкого понимания событий, которые могут быть не знакомы. Выполнение быстрого поиска в Интернете часто помогает узнать является ли процесс или приложение вредоносным и требуется ли его блокировка, или они связаны с законным аспектом использования вашей вычислительной среды.

Просмотр Сертификата

Это может быть полезным и информативным, чтобы просмотреть сведения о сертификате издателя программного обеспечения, прежде чем принять решение о том, что издателя следует добавить в список "Доверенный Издатель". Просто нажмите на ссылку "Просмотр сертификата" в Расширенном Оповещении для вызова диалогового окна, содержащего сведения о сертификате.

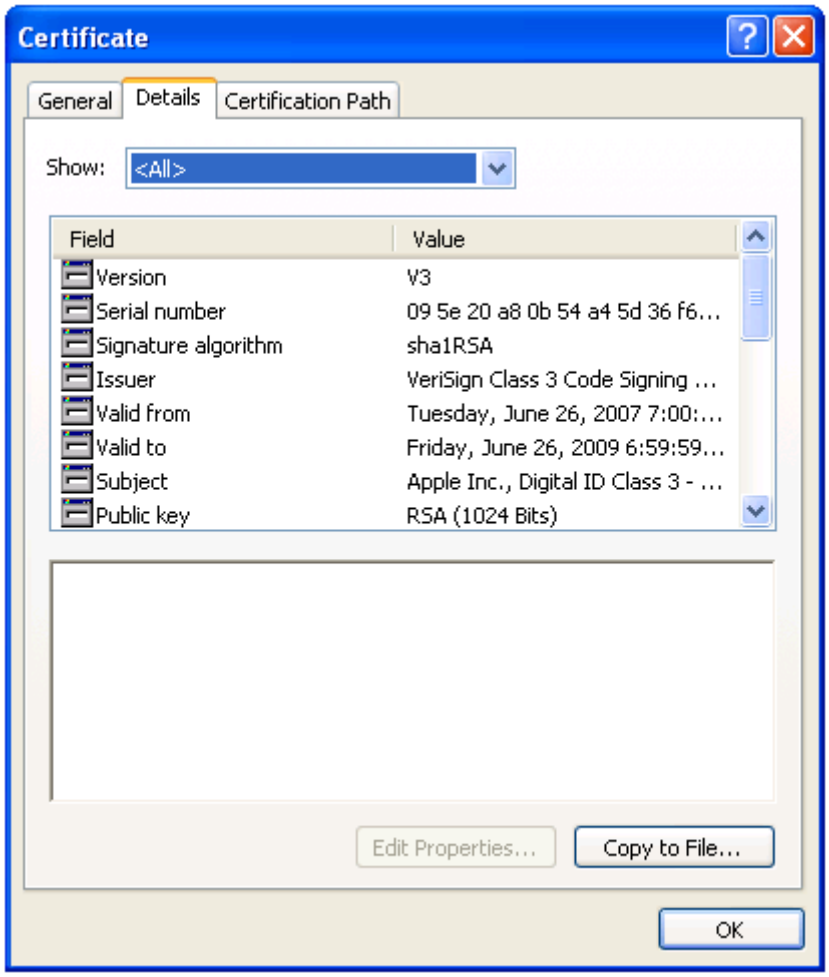


Вкладка Общие отображает разнообразную информацию, относящуюся к Сертификату, включая цель Сертификата, Эмитента и Диапазон дат, в котором сертификат является действительным.

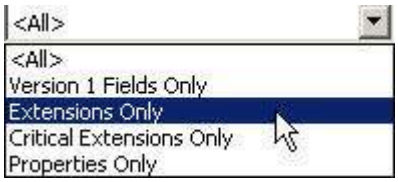
Сертификат может быть импортирован выбором "Установить сертификат", кнопка запустит Мастер импорта сертификата.

Заявление Поставщика сертификата можно просматривать, нажав кн."Заявление Эмитента".

На вкладке "Состав" приводятся подробные сведения относительно сертификата, например, открытый ключ, алгоритм подписи, серийный номер и другие атрибуты сертификата.

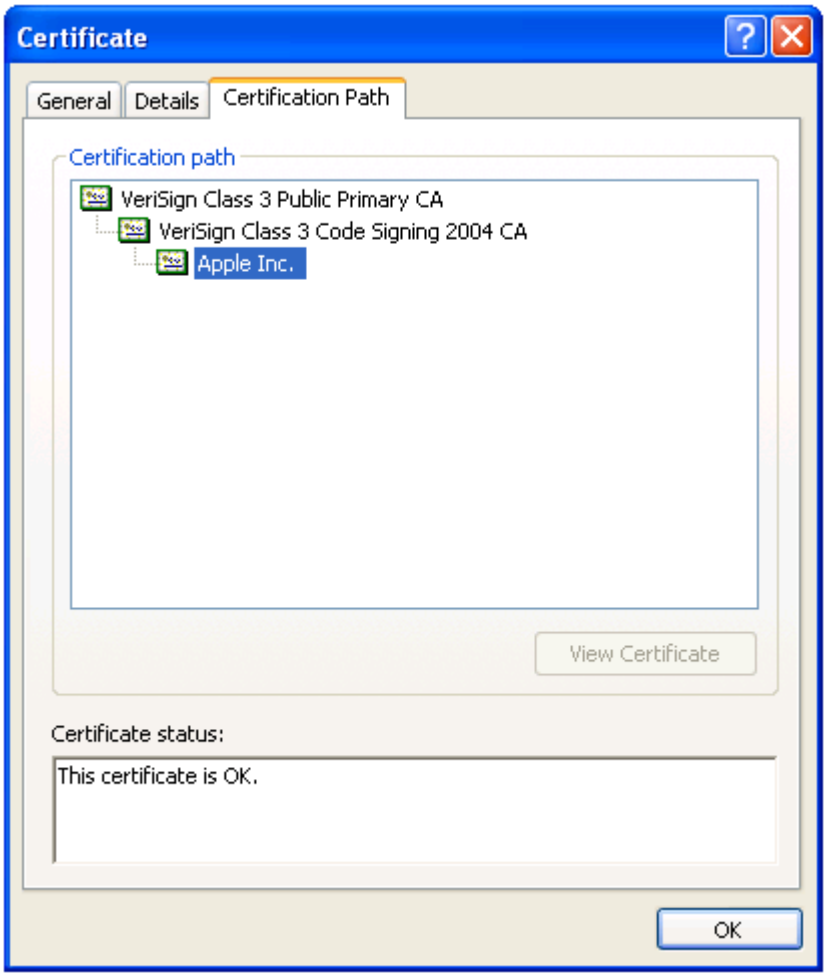


Представление сведений можно отфильтровать, нажав стрелку вниз, и в выпадающем списке окна указать, какие подробности сертификата вы хотите отобразить.



Информация о составе сертификата может быть скопирована в файл для последующего использования выбором кнопки "Копировать в Файл". Кнопка "Изменить Свойства" не активна.

Вкладка **Путь Сертификат**а отображает путь сертификата, который начинается с сертификата субъекта и проходит через ряд промежуточных сертификатов, вплоть до доверенного корневого сертификата, обычно, выданного доверенным Центром Сертификации (CA).

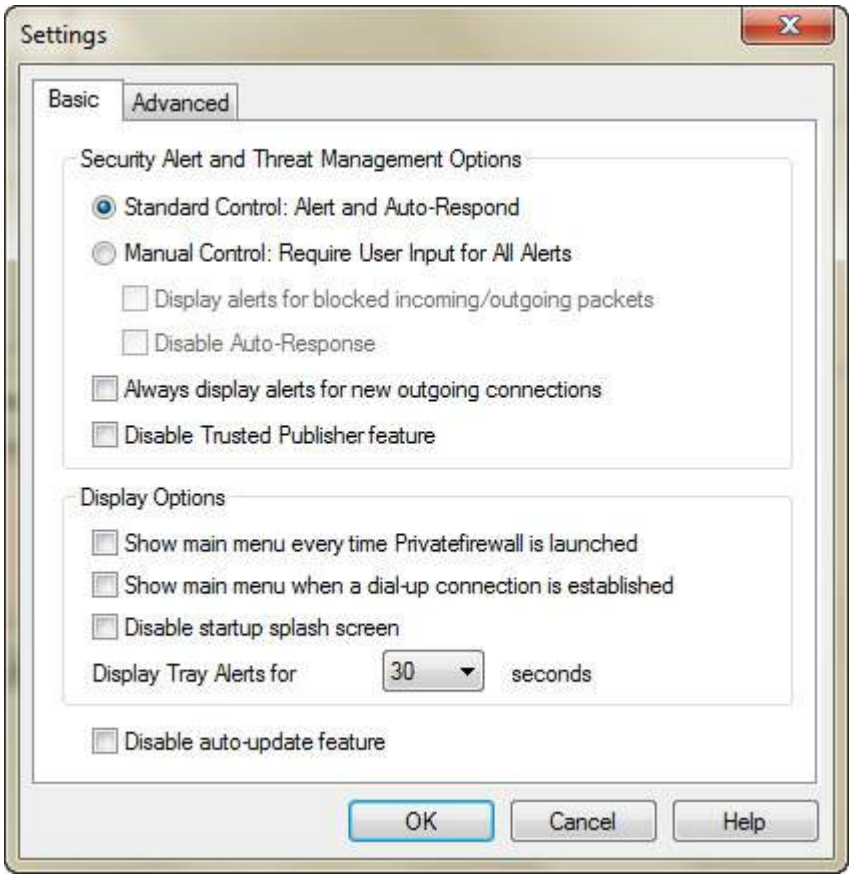


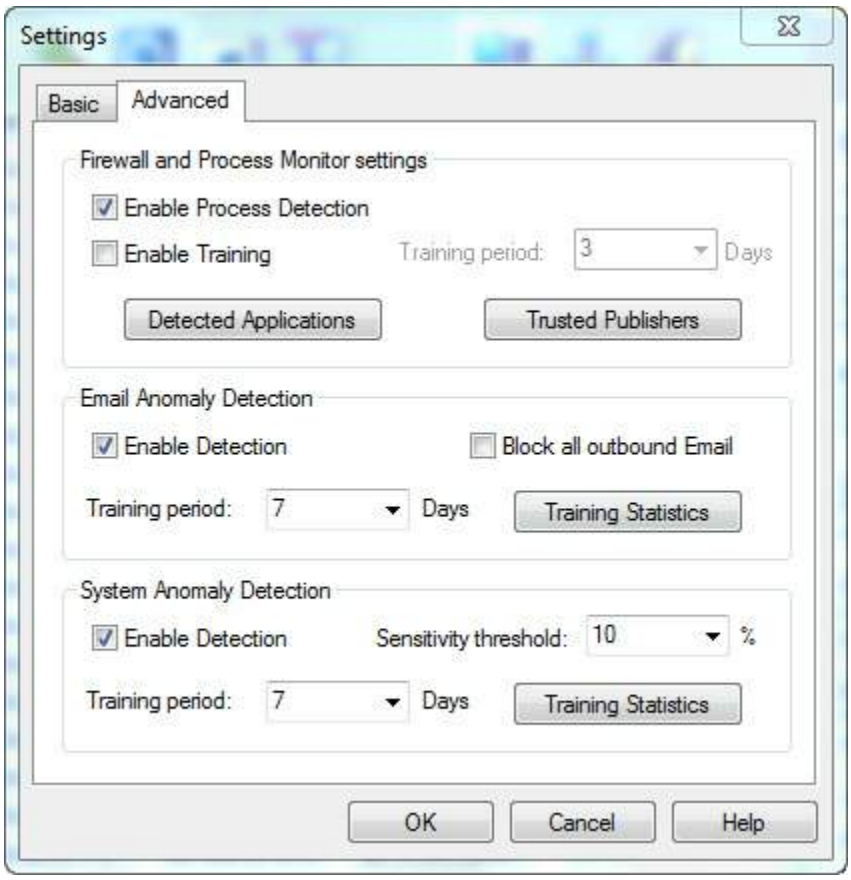
Меню и Панели Инструментов

Меню Программы

Файл/меню Параметры
(Это меню можно открыть, выбрав «Файл/Параметры» в Главном Меню)

В разделе **Параметры** можно настраивать меню/Отображение Предупреждений, Параметры Брандмауэра, Расширенные Настройки, список Обнаруженных Приложений и Обнаружения Аномалий.





Импорт/Экспорт Настроек

(Эта функция может вызываться выбором «Файл/Импорт или Экспорт Параметров» в Главном Меню)

В Privatefirewall пользовательские настройки и правила могут быть импортируемы или экспортируемы между системами в той же самой конфигурации (тот же путь установки приложения, включая использование системы).

Параметры, которые будут экспортированы в файл XML (PF-Settings.xml) включают в себя:
- Общие брандмауэра и настройки ПМ (режим, правила и т.д.)
- Параметры профиля (доверенные и ненадежные списки, режим, правила и т.д.)
- Список разрешенных родителей
- IPC правила для приложений
- Сетевые правила для приложений.

Меню Вид

(Это меню можно открыть, выбрав в главном меню «Вид»)

Скрыть Privatefirewall - этот параметр позволяет свернуть к минимуму Privatefirewall, при этом, отображается только иконка программы в трее.

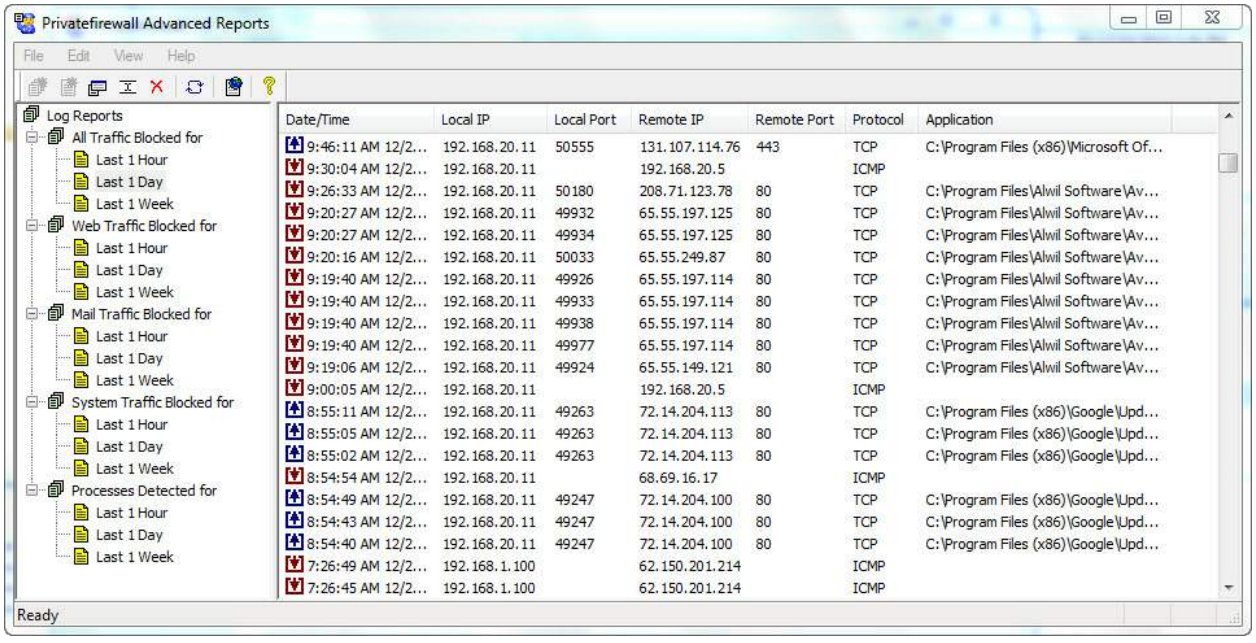
HTML отчет Отслеживание Портов - этот отчет идентичен отчету отслеживания портов в рамках Основного интерфейса, но в формате HTML, для более удобного просмотра. Отчет может быть соранен/просмотрен в формате *.txt, щелчком правой кнопкой мыши в любом месте в пределах окна отчетов отслеживания портов в главном интерфейсе и выбором опции "сохранить отчет как".

HTML Журнал брандмауэра - этот отчет идентичен журналу брандмауэра в главном интерфейсе, но в формате HTML для более удобного просмотра. Отчет, также, может быть сохранен/просмотрен в *.txt формате щелчком правой кнопкой мыши в любом месте в пределах журнала брандмауэра в основном интерфейсе и выбором опции «Сохранить отчет как...».

Полный Отчет - записи журнала брандмауэра могут быть отсортированы по типу и времени записи в Полный Отчет Privatefirewall. Отчеты могут быть отсортированы по попыткам доступа Web, Mail или системы. Каждый из этих отчетов, также, может быть отсортирован за последний 1 час, 1 день или 1 неделю.

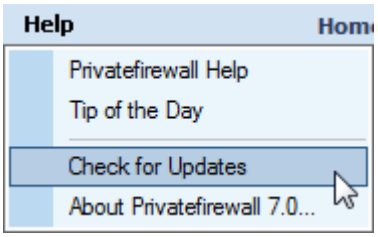
В Полном Отчете Privatefirewall содержится следующее:

Время/дата - когда пакет был обнаружен.
Локальный IP (Интернет-адрес) - адрес в Интернете, из которого поступает пакет.
Локальный порт - порт локального компьютера, участвующего в попытке доступа.
Удаленный IP - адрес в Интернете, который получает пакет.
Удаленный порт - порт удаленного компьютера, участвующего в попытке доступа.
Протокол - сетевой протокол или тип сетевого подключения, используемого для отправки пакета.
Приложение (если применимо) - имя приложения, которому отправляется пакет (если таковые имеются).



Меню Справка

(Это меню можно открыть, выбрав "Справка" в главном меню)



Privatefirewall в меню справки предлагает несколько информационных и функциональных параметров.

- **Privatefirewall Справка**: При выборе данного параметра запустится встроенное руководство пользователя Privatefirewall.

- **Совет дня**: При выборе этого варианта будет отображаться описание функций Privatefirewall, о которых вы можете не знать.

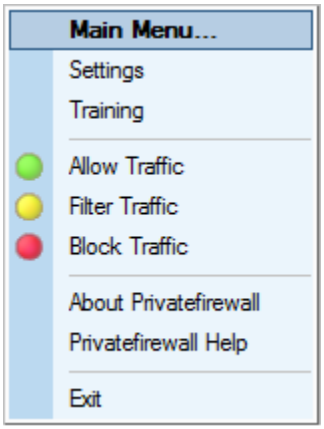
- **Проверить наличие Обновлений**: Эта опция позволит вам убедиться в том, что версия Privatefirewall, установленная на вашей системе, актуальна на данный момент, и загрузит сборку последней версии, если она имеется.
Примечание: Privatefirewall автоматически выполняет проверку версии каждые 24 часа, и после перезагрузки системы, на экране появится уведомление о новой версии и что инсталлятор доступен для скачивания. Эта функция была добавлена в версии 7.0.24.10 (опубликовано 18 июля 2011).

- **О Privatefirewall**: При выборе этого параметра будет отображаться номер версии Privatefirewall, которая, в настоящее время, установлена на вашей системе, а также уведомление об авторских правах и ссылка на страницу поддержки Privatefirewall.

Значок Меню Панели Задач

(Это меню можно получить, щелкнув правой кнопкой на значек Privatefirewall панели задач)

Privatefirewall работает автоматически, после установки в трее в правом нижнем углу должен появиться значек Privatefirewall  К Privatefirewall можно получить доступ, кликнув правой кнопкой мыши на значок на панели. Всплывающее окно (см. справа) содержит следующие параметры: Главное Меню, Справка, Параметры, Обучение, Разрешить, Фильтровать или Запретить интернет-трафик, сведения о Privatefirewall и выход из программы.



Панель Инструментов Privatefirewall

Основные Настройки Панели Инструментов

Параметры - будет отображаться меню настроек, которое состоит из различных основных меню и параметров отображения оповещений.

Сброс настроек по умолчанию - будут сброшены все параметры безопасности и приложения к заводским настройкам. Это полезно, когда применено правило "Разрешено" или "Заблокировано" по ошибке, и т.д..

Обнаружения аномалий исходящей эл. почты - будет разрешать или блокировать всю исходящую эл. почту, основываясь на информации, представленной функцией обнаружения аномалий эл. почты.

Выход – это свернет к минимуму Главное окно Privatefirewal, но не отключит Privatefirewall.

Параметры Профилей Панели Инструментов

Каждый профиль Privatefirewall может быть настроен и определяется путем настройки сети, Интернета и IP-параметров безопасности в рамках главного меню. Щелкните по соответствующему значку профиля межсетевого экрана, чтобы изменить правила/параметры профиля.

Домашний Профиль - профиль используется для дома или дома подключенного к среде сети без других существующих защит брандмауэра. Предлагаемые параметры: Сеть Интернет - Высокий для одного компьютера, Низкий для домашней сети.

Оффис (Сетевой) – этот профиль используется в сетевой среде, где присутствует существующий брандмауэр компании. Предлагаемые параметры: Интернет - Высокий, Сеть - Низкий; Обратитесь к администратору системы для подтверждения параметров.

Удаленный профиль – этот профиль используется при подключении к сети компании, где нет защиты брандмауэра, или локальной сети, где безопасность неизвестна. Предлагаемые настройки: Интернет - Высокий, Сеть - Высокий.

Один пример, где может быть полезным в «один-клик» переключение этих профилей. Полезно, когда компьютер используется для дома и офиса. Дома компьютер, вероятно, не подключен к сети и не может быть защищен аппаратным брандмауэром, и подключен через широкополосное или dial-up соединение. В офисе компьютер подключен к сети компании, которая требует, чтобы другие локальные пользователи имели доступ, используя company-wide брандмауэр, и имеет широкополосный доступ в Интернет. Эти два сценария могут потребовать от Privatefirewall настройки двумя разными способами.

Privacyware Privatefirewall

Version 7.0 – User Guide