Защита компьютера

Как за каменной стеной

Компьютеры, подключенные к Интернету, могут стать жертвами злоумышленников. Вероятность оказаться в такой ситуации зависит от сетевой активности и времени, проводимого в Сети. Но как бы вы ни пользовались Интернетом, защита нужна в любом случае.

Основное средство защиты от вторжения из Сети — брандмауэр. Персональные брандмауэры умеют не только блокировать определенные соединения и пакеты, но и обеспечивать защиту на прикладном уровне, не давая вредоносным воздействиям добраться до программ, установленных на компьютере пользователя.

Мы определили три варианта брандмауэров, в зависимости от того, насколько интенсивно человек пользуется Интернетом, и для каждого подобрали вариант защиты, который подходит для своей ситуации. В каждой описанной нами программе есть возможность блокировки рекламы и контроля активного содержимого, защиты личных данных. Все они следят за сетевой активностью приложений и их компонентов.

Agnitum Outpost Firewall Pro

Разработчик:	Agnitum, Ltd.
Сайт:	http://agnitum.com/ru
Условия распространения:	shareware
Цена: 499 руб.	(персональная лицензия)
Размер дистрибутива:	7,82 Мбайт

Для человека, использующего модемное соединение и в Сети появляющегося редко, подойдет Agnitum Outpost Firewall Pro. Это удобный в настройке, русифицированный и простой в использовании брандмауэр. Общее поведение брандмауэра определяется уровнями политики, которых всего пять: «брандмауэр выключен»; «блокировать все»; «блокировать все, что не разрешено»; «обучающий режим»; «разрешить все, что не заблокировано». В обучающем режиме, если осуществляется попытка соединения, для »

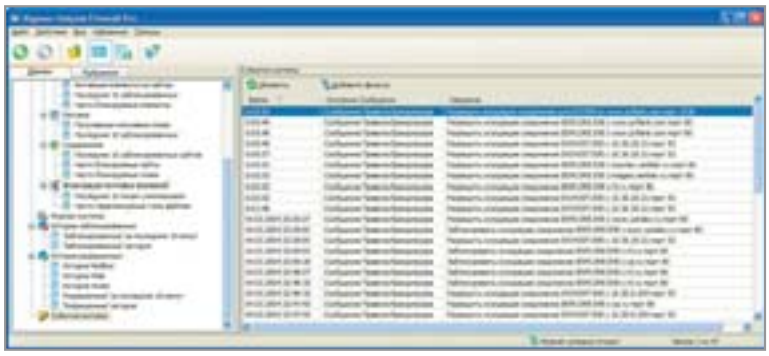
» которого нет правила, выбор действия предоставляется пользователю. В брандмауэре имеется детектор атак, который блокирует некоторые известные атаки, а также сканирование портов и DoS-атаки.

В брандмауэре используются два типа правил: общие и программные. При попытке какой-либо программы получить доступ к Сети сначала проверяются программные правила. Если приложения нет в списке или нет правила, соответствующего соединению или пакету, то проверяются общие. Приложение может находиться в одной из трех категорий: доверенные (весь трафик разрешен), запрещенные (весь трафик приложения блокируется) и пользовательские (для приложения применяются специальные правила). Обратите внимание: даже если для приложения нет соответствующего правила, но соединение разрешено общими правилами, то это соединение будет установлено.

В Outpost очень удобный журнал событий и применения правил, а также просмотр текущей сетевой активности. Настраиваемая блокировка рекламы осуществляется не только по URL, но и по размеру изображения.

Для Outpost не требуется особых настроек сразу после установки. Мастер автоматически создает правила для большинства известных программ. Для усиления безопасности можно добавить в конец списка общих правил блокировку всех входящих и исходящих UDP- и TCP-соединений или включить политику «блокировать все, что не разрешено». После окончательной настройки брандмауэра можно запускать его в фоновом режиме («Настройки» → вкладка «Общие» → тип запуска «Фоновый»). В этом случае будет запускаться только сервис Outpost, а графический интерфейс брандмауэра не будет виден.

▲ Окно с настройками Agnitum Outpost Firewall Pro



◂ Журнал работы Agnitum Outpost Firewall Pro

Symantec Norton Internet Security

Разработчик:	Symantec Corporation
Сайт:	http://symantec.com/region/ru
Условия распространения:	retail
Цена:	€80,84
Размер дистрибутива:	34,3 Мбайт

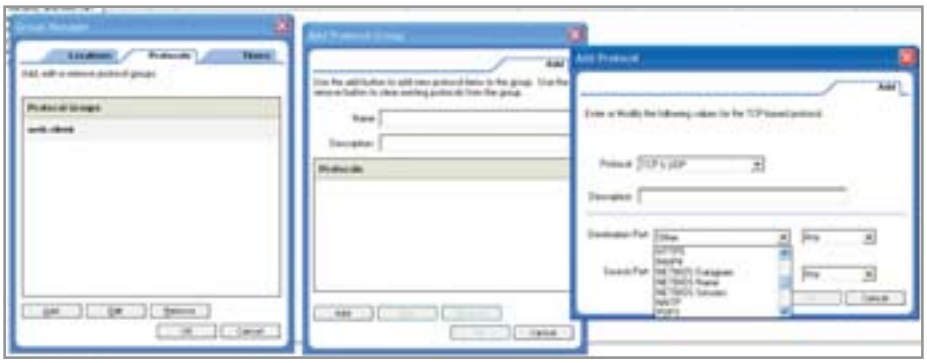
Теперь рассмотрим случай, когда компьютер постоянно подключен к сети и пользователь часто пользуется Интернетом. Например, через районную сеть. И даже если внешнего IP-адреса нет и соединение с Интернетом осуществляется через NAT, в локальной сети все равно найдется достаточное количество любителей запустить иногда какой-нибудь сканер или опробовать новую вредоносную программу. Для такого случая хорошо подходит Norton Internet Security от Symantec. Этот брандмауэр имеет логичную, простую в освоении систему настроек, позволяя при этом очень гибко регулировать сетевую активность персонального компьютера.

Брандмауэр имеет три уровня работы: «блокировать все, что не разрешено пользователем»; «блокировать только злонамеренные программы»; «пропускать все». Правила бывают трех типов: общие, для злонамеренных программ и для приложений. Сначала обрабатываются общие правила. Если после этого сетевая активность осталась незаблокированной, производится проверка на соответствие правилам приложений. Если в правилах для приложений не найдено подходящего правила, то в зависимости от настроек оповещения активность будет или заблокирована, или пользователь увидит запрос. После проверки правил для приложений проверяются правила для злонамеренных приложений. Это блокирующие правила, в основном, для защиты от известных троянских коней. Обычно эти правила не требуют вмешательства и обновляются автоматически.

Кроме этих трех типов правил имеются две области настроек, перекрывающие любые правила. Модуль определения вторжений (Intrusion Detection) защищает компьютер от известных типов атак. Действует как на пакетном уровне, так и на уровне соединений — отлавливает в трафике характерные для конкретных атак фрагменты (signatures) и блокирует соединение. Вторая область — раздел Home networking, где содержится два списка узлов: доверенные (Trusted) и запрещенные (Restricted). Все коммуникации с компьютерами, указанными в разделе Restricted, блокируются. Для списка компьютеров из раздела Trusted никакие правила вообще не проверяются. Разве что модуль Intrusion Detection проверяет все пакеты, исходящие в зону Trusted. Это сделано для того, чтобы пораженный компьютер не мог стать платформой для атаки.

Все основные настройки находятся в разделе «Status & Settings → Personal Firewall → Configure». Будем считать все узлы сети потенциальными врагами, поэтому в раздел Trusted добавлять никого не будем. В General Rules уже присутствуют почти правильные настройки, изменений потребуется минимум. Две настройки Bootp можно смело блокировать, если компьютер не получает IP-адрес с помощью DHCP. Также смело можно блокировать настройки NetBIOS, даже »

▲ Основные правила в Norton Internet Security



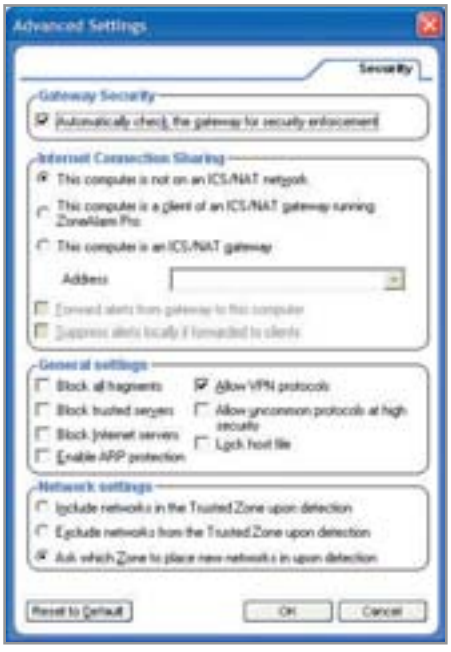
▲ Тонкая настройка Zone Alarm Pro

» если нужно использовать общие ресурсы (shared folders). Windows, начиная с версии 2000, умеет использовать протокол SMB без NetBIOS. В этом случае следует отключить правило «Default Block Microsoft Windows 2000 SMB». По умолчанию включено правило «Block access to secure sites», запрещающее устанавливать защищенное соединение по протоколу HTTPS. Но поскольку этот протокол часто используется на сайтах, где задействована ваша личная информация, правило лучше выключить. Если вы не планируется играть в различные онлайн-игры, можно смело создавать правило, блокирующее весь UDP-трафик и сделать его самым последним.

На вкладке Personal Firewall для настройки уровня безопасности нажимаем кнопку «Custom...» Пункт «Enable Access Controls Alerts» включает оповещения о том, что какая-то программа с вашего компьютера пытается получить доступ к Сети. Его лучше всегда держать включенным: так сразу будет видна нежелательная активность. Далее тонкий момент. Пункт «Alert when unused ports are accessed» включает предупреждения о том, что кто-то пытается установить соединение на закрытые порты. Таким образом, всякий раз при сканировании вашей машины будет появляться множество вопросов о том, что делать с этим соединением. Есть два пути решения проблемы: или выключить этот пункт и не видеть, кто и куда пытается установить входящее соединение, или добавить общее правило, запрещающее любые входящие TCP-соединения. Но следует помнить, что во втором случае будет невозможна работа FTP-клиента в активном режиме.

Для ручной настройки правил приложений нужно выключить пункт «Turn On Automatic Program Control», запустить по очереди все необходимые приложения и в предлагаемом способе настройки правил выбирать «Manually configure Internet access».

▲ Zone Alarm Pro: защита личной информации



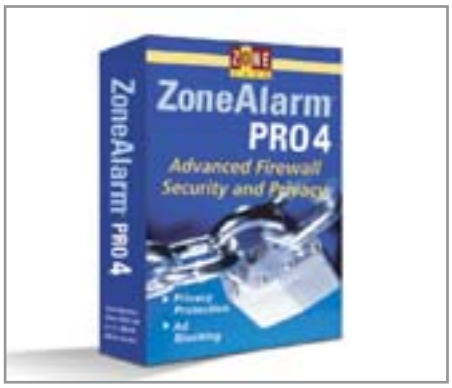
▲ Дополнительные настройки Zone Alarm Pro

ZoneAlarm Pro

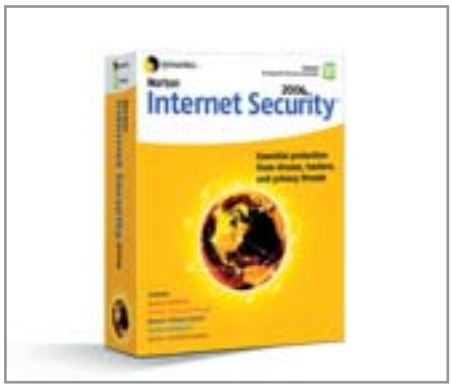
Разработчик:	Zone Labs
Сайт разработчика:	www.zonelabs.com
Условия распространения:	shareware
Цена:	$49,95 + 1 год поддержки
Размер дистрибутива:	4,67 Мбайт

Когда компьютер вообще не отключается от Интернета, Сеть используется активно и в довершение всего на машине установлена какая-нибудь интернет-служба, понадобится брандмауэр, обладающий широкими возможностями и тонкими настройками правил. Он же является и самым сложным в освоении. Это — ZoneAlarm.

Каждый узел, с которым происходит взаимодействие, находится в одной из трех зон: Trusted, Internet или Blocked. К зоне Trusted относятся узлы, с которых попытки несанкционированного доступа маловероятны. К зоне Internet — узлы с неизвестными намерениями. В Blocked — точно нежелательные. Все взаимодействия с зоной Blocked пресекаются. Брандмауэр может работать в трех режимах безопасности: Low, Medium и High. В режиме Low он практически выключен, работают только правила для программ. В режиме Medium по умолчанию разрешены некоторые часто используемые протоколы и доступ к общим ресурсам. В режиме High компьютер не видим в Сети и доступ к общим ресурсам запрещен. Для зон Trusted и Internet можно выбрать различные типы поведения брандмауэра в режимах High и Medium (раздел «Firewall» → вкладка «Main» → кнопка «Custom») — заблокировать или разрешить основные типы протоколов. Это так называемые Zone Rules — зонные правила. Тонкую же настройку обеспечивают Expert Rules. Они позволяют задать реакцию на соединение не только в »



▲ Zone Alarm Pro



▲ Norton Internet Security

» зависимости от входящего/исходящего порта и адреса, но и от текущего времени. Кроме того, есть возможность создавать группы из адресов, протоколов или временных промежутков, которые можно использовать сразу в нескольких правилах. Экспертные правила применяются перед зонными.

Раздел Program Control отвечает за доступ программ к Сети. Умеет отслеживать изменение исполняемого файла, использование программой различных компонентов и других для доступа к сети и даже попытки процессов управлять другими процессами при помощи функции OpenProcess. Program Control может быть или выключен, или работать в трех режимах. При установке «Low» Program Control работает в обучающемся режиме — запущенные программы автоматически добавляются в список разрешенных. При установке «Medium» программные правила включаются, но добавление их компонентов производится в обучающемся режиме. И, наконец, при установке «High» неразрешенная сетевая активность разрешается только с ведома пользователя. Для программ также можно задавать экспертные правила. Общие экспертные запрещающие правила имеют приоритет над любыми программными правилами.

Переходим к настройкам. В разделе «Firewall» на вкладке «Main» выставляем Internet Zone Security в режим «High». На вкладке «Zones» все найденные сети делаем типа Internet.

Для самых строгих настроек надо действовать следующим образом. Определяем типы трафика, который нужно разрешить, добавляем соответствующие правила в общие экспертные (например, исходящие запросы DNS, исходящие соединения HTTP и т. д.), а самым последним добавляем правило, блокирующее любой трафик. После этого для каждой используемой программы нужно разрешить доступ и настроить программные экспертные правила, разрешив только необходимые типы трафика. Последним же правилом для каждой программы добавить опять-таки «блокирующее все». При этом нужно помнить, что некоторым программам требуется разрешение взаимодействия с localhost (IP-адрес 127.0.0.1). Также не забываем о том, что большинство интернет-приложений используют доступ к службе DNS.

ZoneAlarm имеет множество дополнительных возможностей, среди которых поддержка VPN (виртуальные частные сети), Internet Connection Sharing (стандартная служба Windows для общего доступа к сетевому подключению), защита личной информации и электронной почты. Privacy Control различает все виды cookies, блокирует баннеры, активное содержимое, заголовки HTTP, внедренные объекты. Причем все это настраивается отдельно для каждого сайта. Есть возможность экспорта настроек ZoneAlarm в XML-файл.

Брандмауэры различаются функциональностью, сложностью настроек и удобством управления. Мы надеемся, что каждый может подобрать себе подходящую программу для защиты собственного компьютера.

■ ■ ■ **Дмитрий Солошенко**

Ликбез

Правила для брандмауэров

Все брандмауэры действуют на основе правил. Правило состоит из условия и действия, которое будет произведено в случае, если условие выполнено. В условие входит направление пакета или соединения, порты и адреса источника и отправителя, протокол взаимодействия. Также возможны дополнительные параметры: текущее время, нестандартный тип протокола и т. д. Обычно правила просматриваются брандмауэром в некотором порядке (в зависимости от приоритета). Если встречается правило, условия которого удовлетворяют рассматриваемому трафику, то действие, указанное в правиле, выполняется, и дальнейший просмотр правил прекращается.

Конкретному приложению в зависимости от его функций требуется доступ к различным видам трафика. Браузерам требуется не только возможность исходящего TCP-соединения на 80-й порт (HTTP). Нужен доступ к службе DNS — возможность обмениваться пакетами UDP с 53-м портом DNS-сервера. Кроме того, иногда может потребоваться соединение на 443-й порт (HTTPS) для работы в защищенных сессиях. Часто браузеры работают также в качестве FTP-клиентов. FTP-клиенты в «активном» режиме (то есть когда соединение данных инициирует FTP-сервер) требуют разрешения входящего TCP-соединения с 20-го порта сервера почти на любой порт (так как FTP-клиент выбирает его произвольно и сообщает серверу). В пассивном же режиме (когда соединение данных инициирует FTP-клиент) достаточно исходящего TCP-соединения на порт 21 и любой порт с номером больше 1024. Почтовые клиенты требуют разрешения исходящих TCP-соединений на порты 110 (POP3), 25 (SMTP), 143 (IMAP). Для некоторых типов авторизации может потребоваться входящее TCP-соединение на порт 113. ICQ-клиенты, если между ними не установлена прямая связь, требуют исходящего TCP-соединения на порт 5190 — именно так они соединяются со своими серверами. 80-й порт нужен не для нормальной работы клиента, а для загрузки рекламы.