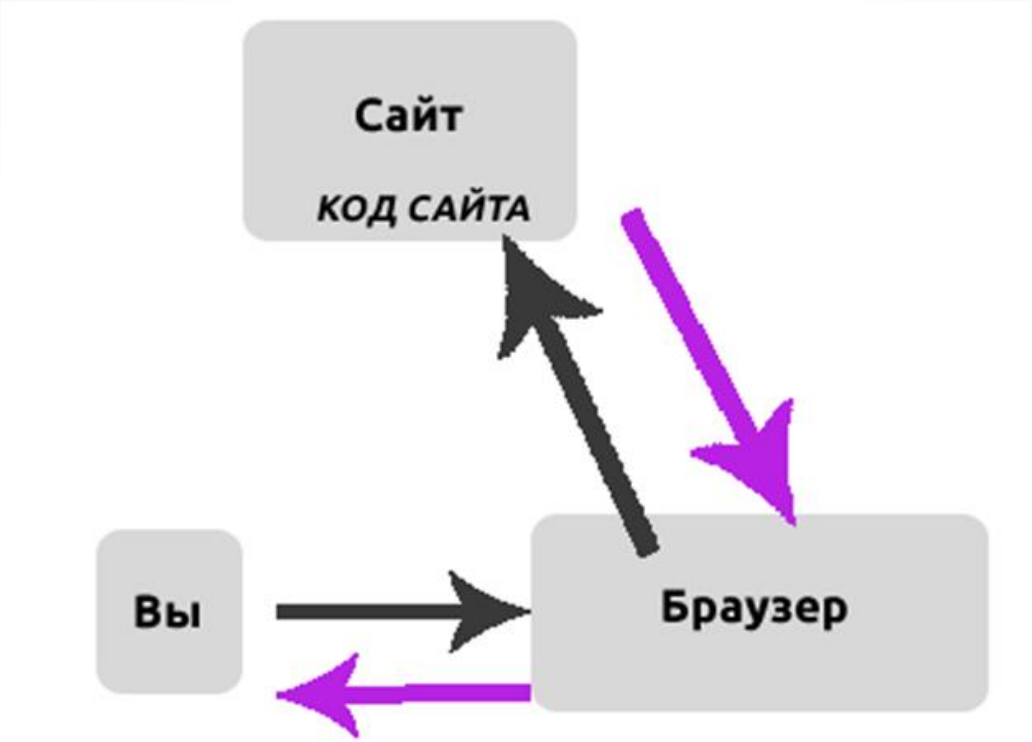
Лекция 6 Инструменты Internet

Лектор

Ст. преподаватель Купо А.Н.

То есть происходит такая картина:



Она означает следующее:

- **Вы заходите в браузер и переходите на сайт.**
- **После этого, браузер читает код сайта и показывает вам всё, что он прочитал, но не в виде кода, а уже нормальным человеческим языком, который обычный пользователь может легко прочитать (разумеется, если он умеет читать)**

Mozilla Firefox. Распространяется совершенно бесплатно, находится в свободном доступе. Мозила работает не только с Windows, но и с некоторыми дистрибутивами Linux, один из них — Ubuntu. Простой в использовании браузер с большим количеством плагинов (расширений), которыми легко и просто управлять (убирать и добавлять новые). Его можно назвать самым гибким.

Opera. Бесплатна, начиная с версии 8.50. Имеет встроенный почтовый клиент, удобную службу Opera Link, которая сохраняет настройки, пароли и позволяет вам использовать их на разных компьютерах. Благодаря другой службе (Opera Unite) можно смотреть видео и слушать музыку потоком. Opera считается высокоскоростным браузером и работает практически со всеми интернет-технологиями. Про этот браузер можно сказать, всё в одном.

Internet Explorer. Старый добрый Internet Explorer. Когда-то он был самым распространённым для рядовых пользователей, так как входит в комплект операционной системы Windows. В чём его отличительная черта от других, так это в том, что с IE работают серьёзные компании. Например, многие интернет-банки, в которые можно зайти с использованием электронно-цифровой подписи. Только Internet Explorer поддерживает такую функцию. Стандартный, простой браузер. Его последние версии стали более скоростными.

Safari. Разработан корпорацией Apple. Работает на операционных системах Mac OS и MS Windows. Имеет оригинальный дизайн и является одним из самых современных.

Google Chrome (бесплатен). Наиболее простой в использовании, скорее даже самый простой. Он имеет встроенный флеш-плеер. То есть, например, для просмотра видео на You-tube вам не придётся его постоянно скачивать или обновлять. Также Хром первым ввёл возможность поиска прямо из адресной строки, что очень удобно.

Защита компьютера интернет-пользователя: системный брандмауэр, персональный файрвол

Что такое брандмауэр?

- Политика безопасности брандмауэра
- Версии брандмауэра

Персональный файрвол

- Файрволы ОС
- Возможности файрвола

Межсетевой экран

- Типичные возможности
- Проблемы, не решаемые файрволом

Что такое брандмауэр?

Брандмауэр — это программное обеспечение или оборудование, которое препятствует злоумышленникам и некоторым типам вредоносных программ получать доступ к компьютеру по сети или через Интернет. Для этого брандмауэр проверяет данные, поступающие из Интернета или по сети, и блокирует их или разрешает передачу на компьютер.

Брандмауэр отличается от антивирусной и антивредоносной программы. Брандмауэр защищает от червей и злоумышленников, антивирусные программы защищают от вирусов, а антивредоносные программы защищают от вредоносных программ. Необходимо использовать все три типа защиты. Можно воспользоваться Защитником Windows(эта антивирусная и антивредоносная программа поставляется вместе с системой Windows 8) или использовать другое приложение для защиты от вирусов и вредоносных программ. На компьютере должно работать только одно приложение брандмауэра. Наличие нескольких приложений брандмауэра на компьютере может вызывать конфликты и проблемы.

Брандмауэр Windows входит в комплект Windows и по умолчанию включен.

Брандмауэр создает барьер между Интернетом и компьютером

Рекомендуется использовать следующие параметры брандмауэра по умолчанию.

Брандмауэр включен для всех типов сетей (частные, публичные и доменные).

Брандмауэр включен для всех сетевых подключений.

Брандмауэр блокирует все входящие подключения, кроме явно разрешенных пользователем.

Политика безопасности брандмауэров

- Целостность системы

Для предотвращения неавторизованной модификации конфигурации брандмауэра должна иметься некоторая форма гарантий целостности. Обычно для рабочей конфигурации системы вычисляются контрольные суммы или криптографические хэш-функции, которые хранятся потом на защищенном носителе.

- Документация

Важно, чтобы правила работы с брандмауэром и параметры его конфигурации были хорошо документированы, своевременно обновлялись и хранились в безопасном месте. Это будет гарантировать, что при невозможности связаться с администратором брандмауэра, другой опытный человек сможет после прочтения документации быстро осуществить администрирование брандмауэра.

- Физическая безопасность брандмауэра

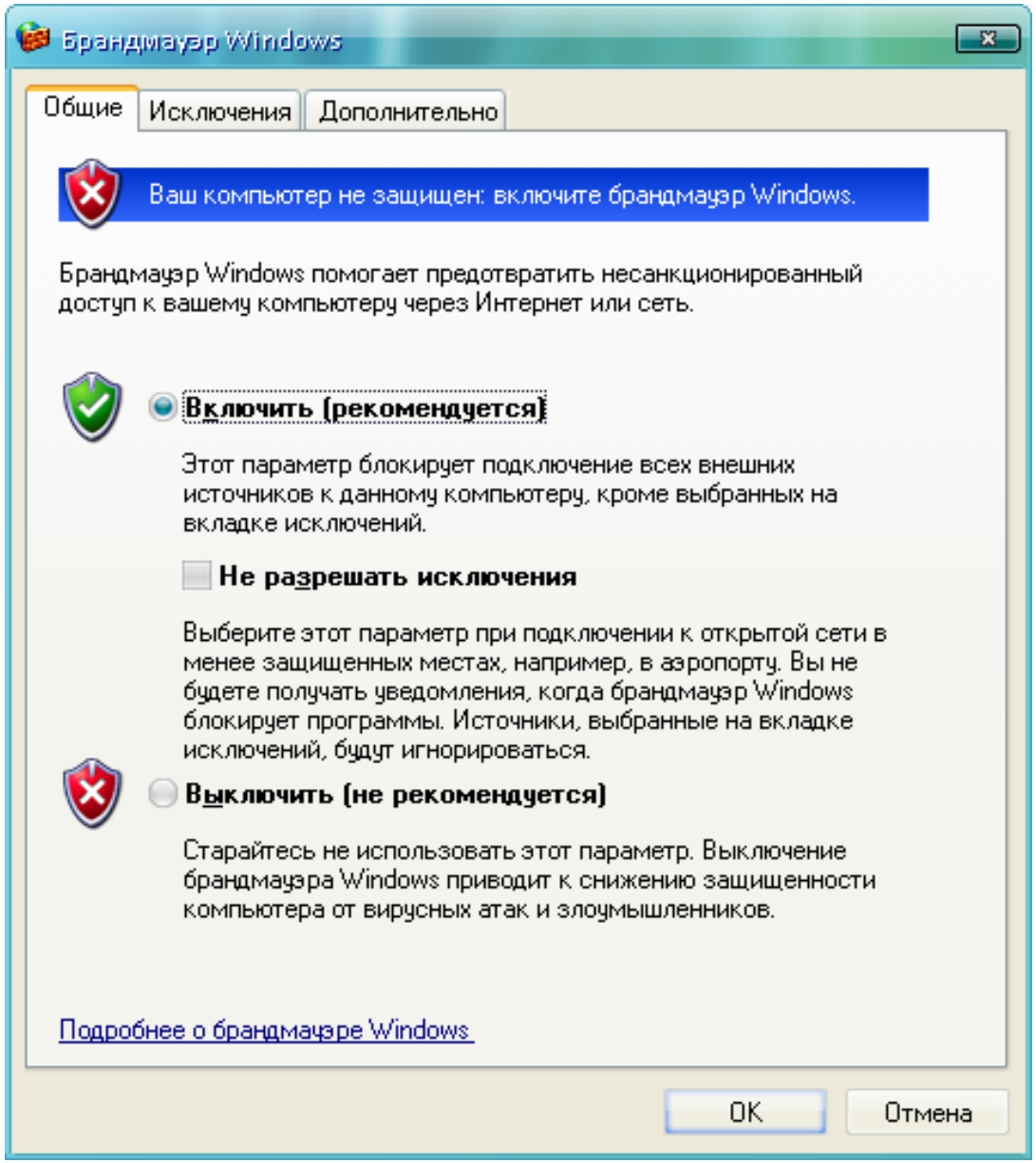
Физический доступ к брандмауэру должен строго контролироваться во избежание несанкционированных изменений конфигурации брандмауэра или его состояния, а также для того, чтобы нельзя было наблюдать за работой брандмауэра. Кроме того, должна иметься система создания архивных копий, позволяющие гарантировать бесперебойную работу брандмауэра.

Версии брандмауэра

Windows XP

Брандмауэр Windows был выпущен в составе Windows XP Service Pack 2. Все типы сетевых подключений, такие как проводное, беспроводное, VPN по умолчанию фильтруются через брандмауэр (с некоторыми встроенными исключениями, разрешающими соединения для машин из локальной сети). Это устраняет проблему, когда правило фильтрации применяется лишь через несколько секунд после открытия соединения, создавая тем самым уязвимость. Системные администраторы могут настраивать фаервол, используя групповую политику. Брандмауэр Windows XP не работает с исходящими соединениями (фильтрует только входящие подключения).

Брандмауэр Windows под Windows XP

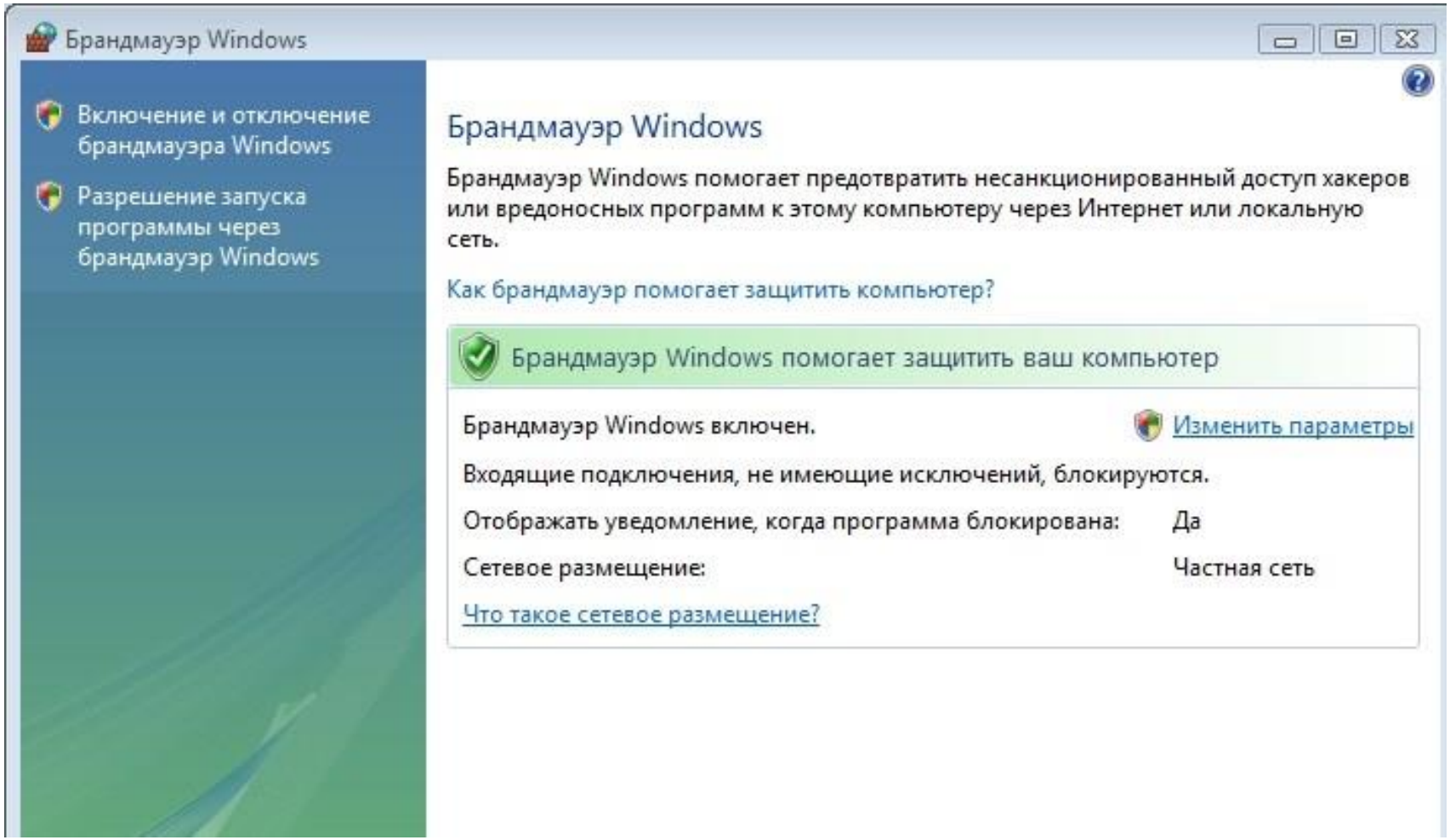


Версии брандмауэра

Windows Vista добавляет в брандмауэр новые возможности, улучшающие его развёртывание в корпоративной среде:

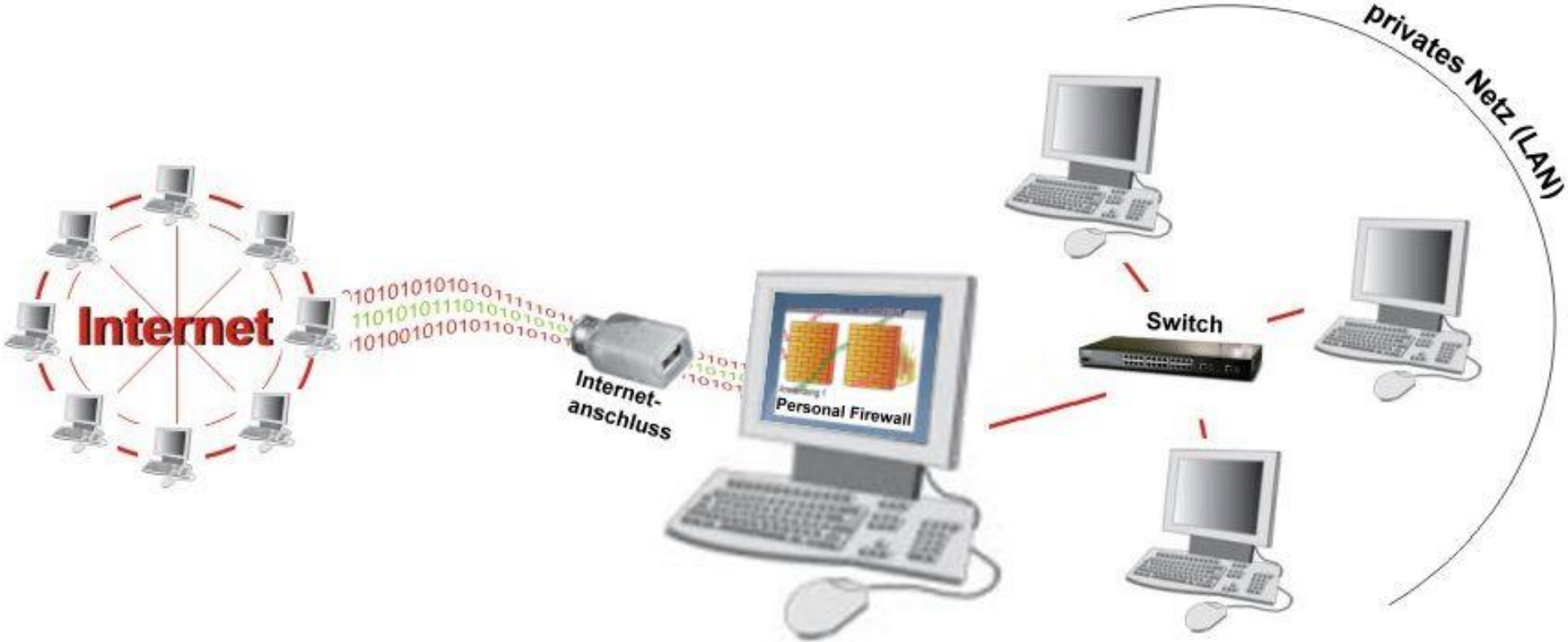
- Фильтр соединений IPv6.
- Фильтрация исходящего трафика, позволяющая бороться с вирусами и шпионским ПО. Настроить фильтрацию можно, используя консоль управления MMC.
- Используя расширенный фильтр пакетов, правила можно применять к определённым диапазонам IP-адресов и портов.
- Правила для служб можно задавать, используя имена служб из списка без необходимости указывать полное имя службы.
- Улучшено управление сетевыми профилями (возможность создавать разные правила для домашних, рабочих и публичных сетей). Поддержка создания правил, обеспечивающих соблюдение политики изоляции домена и сервера.

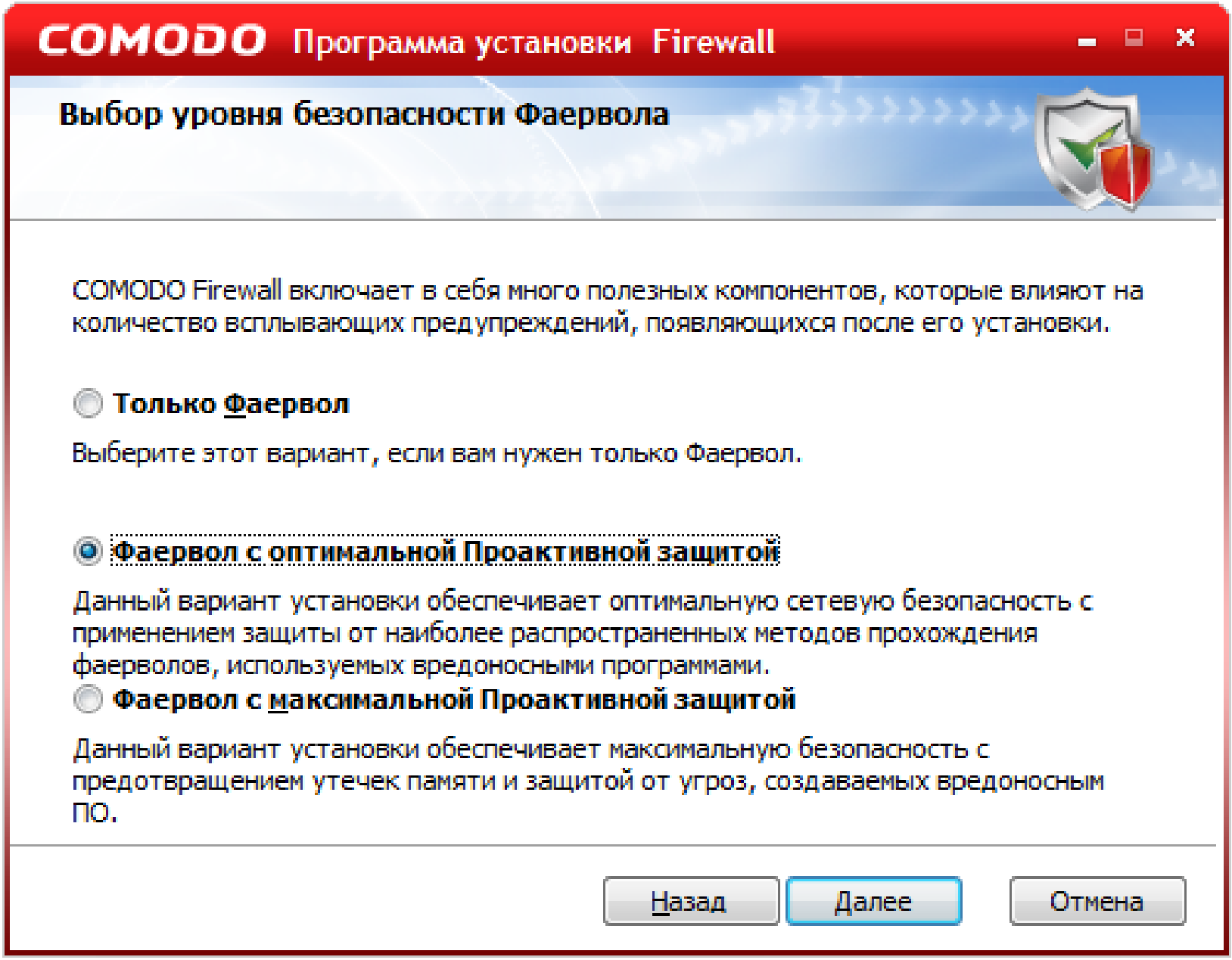
Брандмауэр Windows под Windows Vista

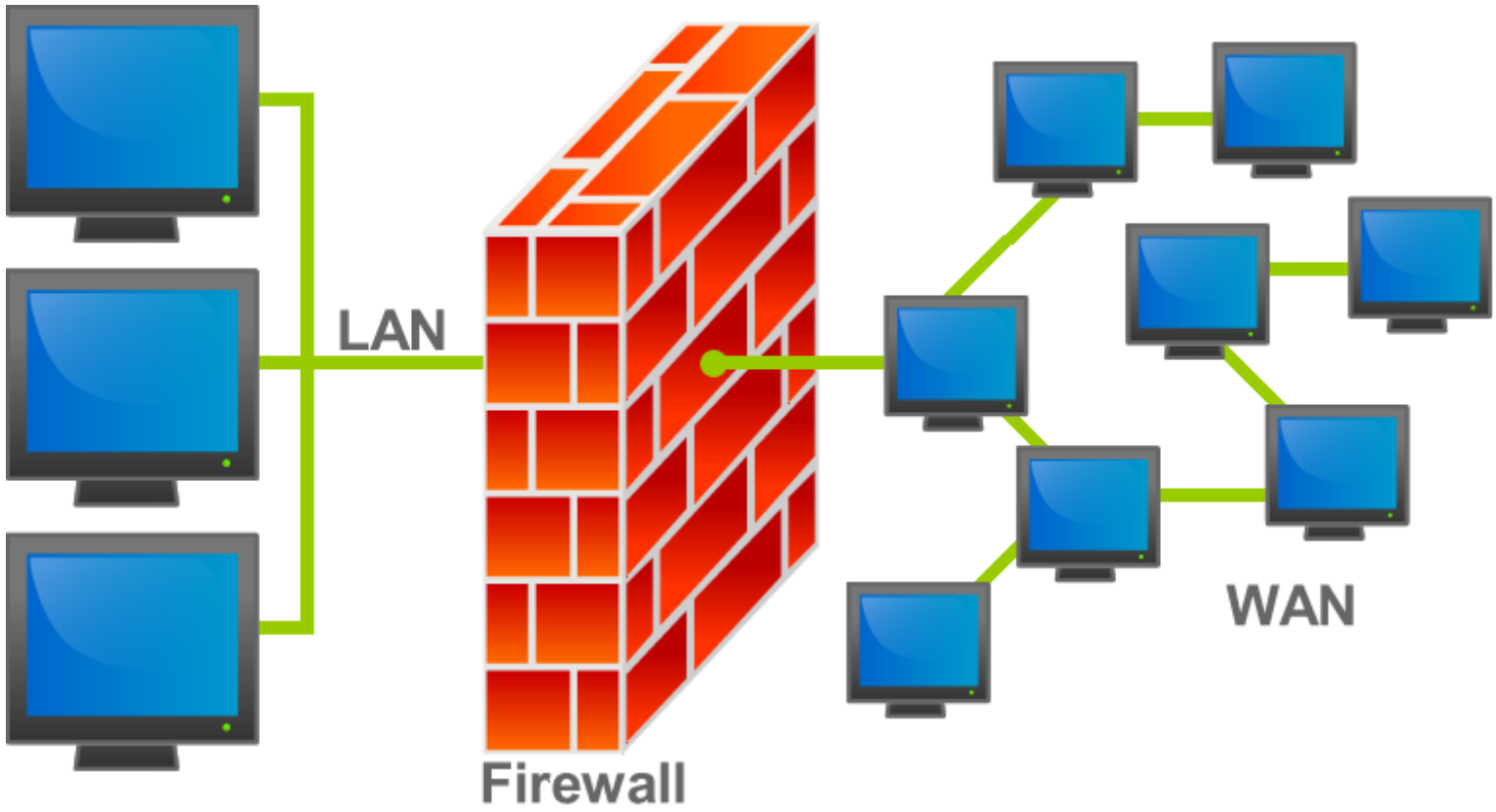


Персональный файрвол

Персональный файрвол — программное обеспечение, осуществляющее контроль сетевой активности компьютера, на котором он установлен, а также фильтрацию трафика в соответствии с заданными правилами. В отличие от межсетевого экрана, персональный файрвол устанавливается непосредственно на защищаемом компьютере.




COMODO Программа установки Firewall
Выбор уровня безопасности Фаервола
COMODO Firewall включает в себя много полезных компонентов, которые влияют на количество всплывающих предупреждений, появляющихся после его установки.
Только Фаервол
Выберите этот вариант, если вам нужен только Фаервол.
Фаервол с оптимальной Проактивной защитой
Данный вариант установки обеспечивает оптимальную сетевую безопасность с применением защиты от наиболее распространенных методов прохождения фаерволов, используемых вредоносными программами.
Фаервол с максимальной Проактивной защитой
Данный вариант установки обеспечивает максимальную безопасность с предотвращением утечек памяти и защитой от угроз, создаваемых вредоносным ПО.
Назад
Далее
Отмена


LAN
Firewall
WAN

Возможности:

- Фильтрация входящего трафика
- Фильтрация исходящего трафика
- Проверка целостности приложения
- Шифрование данных
- Сокрытие вашего присутствия
- Создание отчетов / Ведение логов
- Защита электронной почты от вирусов
- Блокирования всплывающих (Pop-up) рекламных окон
- Слежение за cookie
- Защита от шпионского ПО
- Защита ноутбука

Целостность приложения

Если главное приложение изменилось со времени последнего использования, при том, что ни пользователи, ни администраторы на выполняли его модернизацию, это может служить "красным флагом" файрволу, означающим что данное приложения могло быть инфицировано. Во многих случая предупреждение возникнет вследствие того, что вы только что модернизировали приложение. Однако в некоторых случая причиной предупреждения может быть злонамеренная программа, которая без вашего ведома управляла и изменила приложение.

Уведомления пользователя

В некоторых файрволах есть уведомления пользователя в определяемом или всплывающем окне, которые предупреждают пользователя о запросах на входящие или исходящее соединение. Можно наблюдать за каждым соединением, но после первых пятнадцати минут использования нового файрвола новинка надоедает, и большинство пользователей находит, что контролировать постоянный поток запросов это мучения. Настройка автоматического принятия и отклонения некоторых типов запросов является оправданной в большинстве случаем и позволяет пользователю избежать постоянной игры роли привратника.

Файрволы операционной системы

Windows' Internet Connection Firewall:

Встроенные возможности файрвола XP слабы, но это лучше, чем ничего. Важно обратить внимание на то, что у данного файрвола нет возможности фильтрования исходящего трафика или любых других дополнительных возможностей. По умолчанию файрвол в XP выключен, но лучше проверьте это перед установкой другого ПО межсетовой защиты. Обратите внимание, никогда не должно использоваться большего одного программного файрвола одновременно.

Mac OS X Firewall:

Встроенный в Mac OS X файрвол, подобен другим, основанным на Unix, поэтому это влечет за собой расширенную форму мониторинга портов. Он прост для понимания и настройки, но также, подобно файрволу Windows XP, выключен по умолчанию. В родном средстве межсетевой защиты нет никаких расширенных возможностей, но нужно отметить, что в последней версии MacOSX, Panther, включая версию Safari, браузер блокирует всплывающие окна и осуществляет защиту cookie.

Популярные файерволы

Kerio Personal Firewall 2:

Бесплатен для домашнего использования. В дополнение к возможности создавать собственные правила Kerio имеет предварительно загружаемый набор правил. Есть одна особенность - идентификация файла по цифровой сигнатуре. Файлы не зашифрованы файрволом, но он использует криптографию как средство контроля целостности приложений.

Outpost Firewall, by Agnitum:

Это хороший, надежный и бесплатный файрвол, но так или иначе имеющий небольшое признание. Удобен в использовании, блокировании баннеров, вирусов и контроле cookie.

Zone Alarm, by ZoneLabs:

Вероятно самый известный бесплатный файрвол на рынке PC, Zone Alarm прост в установке и настройке. Подобно другим бесплатным и коммерческим продуктам, он фильтрует входящий и исходящий трафик.

Межсетевой экран

Межсетевой экран или **сетевой экран** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Типичные возможности

- фильтрация доступа к заведомо незащищенным службам;
- препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
- контроль доступа к узлам сети;
- может регистрировать все попытки доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети;
- регламентирование порядка доступа к сети;
- уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран;

Проблемы, не решаемые фаерволом

Межсетевой экран сам по себе не панацея от всех угроз для сети. В частности, он:

- не защищает узлы сети от проникновения через «люки» (англ. *back doors*) или уязвимости ПО;
- не обеспечивает защиту от многих внутренних угроз, в первую очередь — утечки данных;
- не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;

Для решения последних двух проблем используются соответствующие дополнительные средства, в частности, антивирусы. Обычно они подключаются к файрволу и пропускают через себя соответствующую часть сетевого трафика, работая как прозрачный для прочих сетевых узлов прокси, или же получают с файрвола копию всех пересылаемых данных. Однако такой анализ требует значительных аппаратных ресурсов, поэтому обычно проводится на каждом узле сети самостоятельно.