Контроль и управление доступом в Интернет

(pfSense, m0n0wall, untangle)

PfSense - представляет собой программно-аппаратный комплекс позволяющий защитить локальную сеть от вторжений извне, а также провести мероприятия по управлению доступом пользователей к ресурсам локальной сети, корпоративным ресурсам и к сети Интернет с возможностью учета и сохранения информации об использованном трафике.

Система построена на основе операционной системы с открытой лицензией FreeBSD

Возможности:

- **Контроль и управление доступом в Интернет**
- Персональный полноценный доступ в Интернет для каждого сотрудника. Авторизация по логину и паролю, авторизация по IP адресу и по MAC адресу.
- Контроль доступа к ресурсам Интернет, вся информация о действиях пользователя сохраняется
- Возможность иерархической группировки пользователей (например, структурные

единицы), назначение ответственных лиц для управления этими группами.

- Разграничение доступа пользователей к Интернет (например, одной группе пользователей разрешен доступ только к корпоративным сайтам, другой - к корпоративным сайтам и ICQ, третьей – Интернет банк, и т.д.).
- Content фильтр. Возможность запрета по типу скачиваемых файлов (например, mp3, avi), блокирование рекламы, протоколов по ключевым словам.

- **Учет трафика по пользователям, планирование и ограничение расходов**
- Планирование и ограничение расходов (лимитирование) по пользователям отделам, всему предприятию (например, установка квот для пользователей на определенный период – 20Мб/день, или 400Мб/месяц и т.д.).
- Подсчет статистики в реальном времени, автоматическое предупреждение без отключения, либо отключение пользователя при превышении лимита.
- Статистика посещения ресурсов Интернет (статистика за период по всей организации/ за период по конкретному пользователю/за период по конкретному IP). Статистика может быть представлена в текстовом или в графическом виде. Просмотр статистики можно разрешить только определенному пользователю.
- Возможность экономии на трафике за счет кеширование Интернет контента (часть редко меняющегося контента сохраняется на сервере локально, что позволяет экономить на трафике от 5 до 10 процентов).

- Защита, межсетевой экран Firewall
- Защита компьютеров от атак из Интернет с использованием технологий NAT и встроенного Firewall.
- Блокирование IP адресов и протоколов по заданным условиям.
- Защита от сканеров сети, защита от DOS –атак и блокирование чрезмерной активности.
- Разграничение доступа к корпоративным ресурсам, создание общих и закрытых серверов сети.
- Ограничение скорости Интернет трафика для отдельных пользователей, компьютеров, или протоколов.
- DNAT portmapper. Возможность прозрачной переадресации адресов и портов на

другой адрес (например, для прозрачного прокси, или для публикации внутреннего веб-сервера).

- Удаленное подключение сотрудников и подразделений
- Доступ сотрудников к сети предприятия из дома или командировки по защищенному каналу.
- Возможность создать закрытые корпоративные серверы для ограниченного круга сотрудников.
- Возможность объединения удаленных подразделений в общую сеть на единой платформе по шифрованным протоколам VPN.

- Интеллектуальная приоритезация трафика (QoS)
- Возможность вручную расставлять приоритет трафика по скорости и типу (резервирование полосы пропускания для важных приложений).
- Равномерное распределение канала между пользователями и приложениями.

- DHCP- сервер
- Автоматическое распределение IP адресов в локальной сети.

- DNS – сервер
- DNS обеспечивает удобную работу с Интернетом, т.к. для соединения с узлом необходимо указание его IP-адреса, а большинству людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например, HTTP-сервера, различая их по имени запроса.

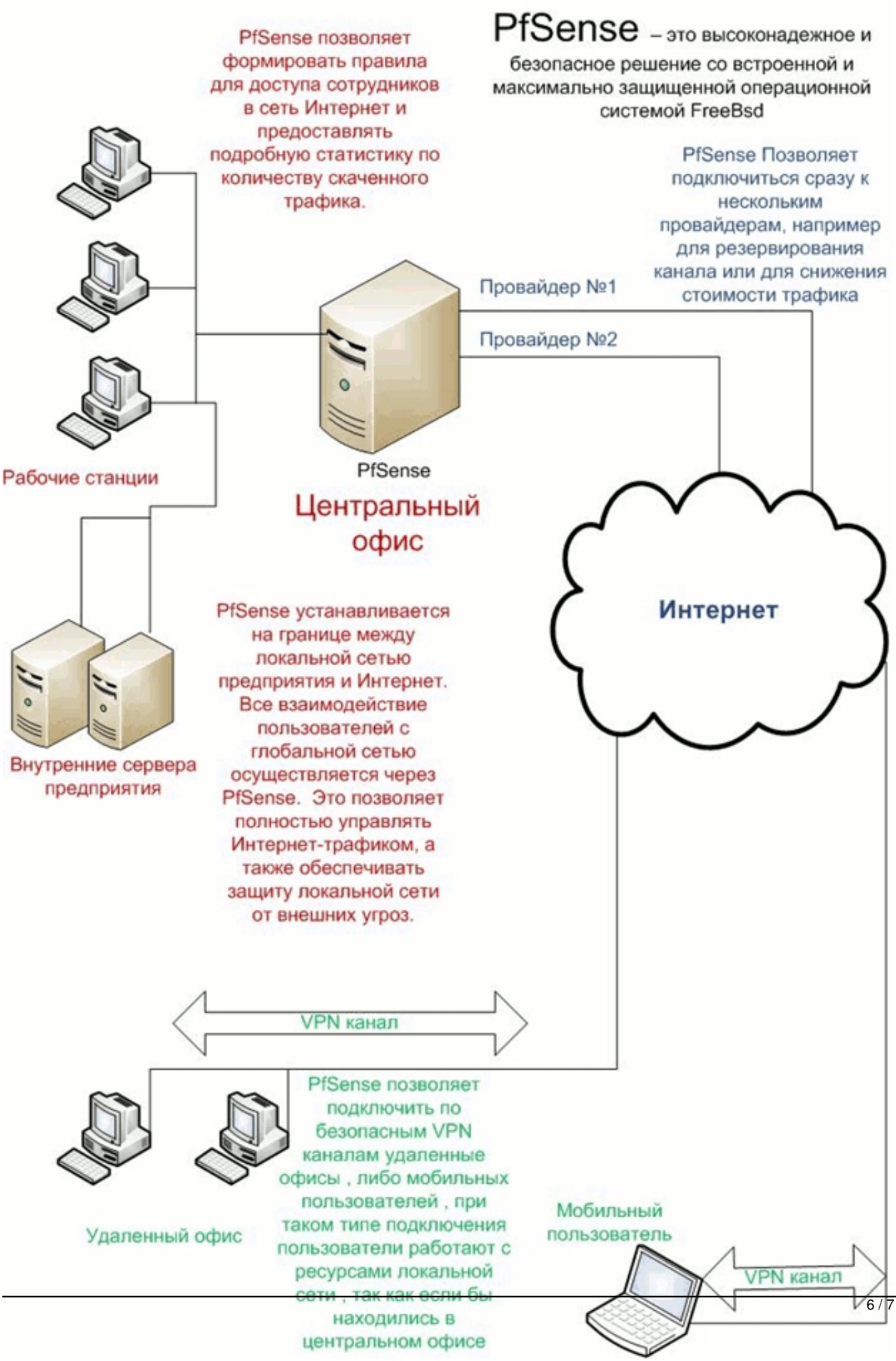
- Полноценный маршрутизатор
- Поддерживает множество интерфейсов (как локальных, так и внешних).
- Возможность указать маршруты по источнику, что позволяет экономить на цене трафика при наличии нескольких провайдеров путем перенаправления трафика в разные подсети.

- Подключение к провайдерам, резервирование каналов
- Поддержка нескольких провайдеров и нескольких внешних сетей.
- Возможность полного разделения пользователей для выхода в Интернет через разных провайдеров.
- Автоматическая проверка связи с провайдером и переключение на альтернативного провайдера в случае необходимости.

- FTP – сервер
- Возможность хранения общих документов и прочих файлов.
- Возможность доступа к серверу как снаружи, так и из локальной сети.
- Возможность анонимного и авторизованного входа.

- Создание закрытой и публичной части.
- Возможность ограничения скорости скачивания.

- WEB – сервер


PfSense – это высоконадежное и безопасное решение со встроенной и максимально защищенной операционной системой FreeBsd
PfSense позволяет формировать правила для доступа сотрудников в сеть Интернет и предоставлять подробную статистику по количеству скаченного трафика.
PfSense Позволяет подключиться сразу к нескольким провайдерам, например для резервирования канала или для снижения стоимости трафика
Провайдер №1
Провайдер №2
PfSense
Рабочие станции
Центральный офис
Интернет
PfSense устанавливается на границе между локальной сетью предприятия и Интернет. Все взаимодействие пользователей с глобальной сетью осуществляется через PfSense. Это позволяет полностью управлять Интернет-трафиком, а также обеспечивать защиту локальной сети от внешних угроз.
Внутренние сервера предприятия
VPN канал
PfSense позволяет подключить по безопасным VPN каналам удаленные офисы , либо мобильных пользователей , при таком типе подключения пользователи работают с ресурсами локальной сети , так как если бы находились в центральном офисе
Удаленный офис
Мобильный пользователь
VPN канал

{jcomments on}