Снова * * * **22.2 Статус системы**

Основная страница системы pfSense -это страница Статус системы (Status >> System, показанная на рисунке 22.2, "Статус Системы"). Она содержит некоторую информацию о базовой системе, например имя маршрутизатора, версию pfSense, платформа (Раздел 1.6, "Платформы"), время работы, размер таблицы состояния (Раздел 4.5.9.6, "Firewall Maximum States"), использование MBUF, использование CPU, использование памяти, использование своп пространства и использование диска. Счётчики на странице обновляются автоматически, каждые несколько секунд, потому нет необходимости в обновлении страницы.

Рисунок 22-2

22.3 Статус интерфейсов

Статус сетевых интерефйсов можно наблюдать на странице Status >> Interfaces. ...

продолжение следует...
Метки: pfsense, нЭмного пА РусскЕ

Догонялки... Из-за отсутствия домашнего интернета (очередная финансовая пропасть в которую можно падать вечно) все дела застопорились. Сегодня выкладываю небольшой перевод в продолжение 22 главы pfSense TheDefinitiveGuide.

***

22.1.3 Удалённое журналирование с использованием Syslog

Прочие опции меню Status >> Systems Logs на закладке Settings необходимы для настройки демона syslog, позволяющего копировать записи журналов на удалённый сервер. Поскольку журналы хранимые pfSense на самом маршрутизаторе имеют конечный (и достаточно малый) размер, их копирование на syslog-сервер обеспечивает, как возможность поиска и устранения неисправностей, так и возможность длительного хранения записей в случае необходимости. Журналы марщрутизатора очищаются при перезагрузке, а наличие удалённой копии журналов позволяет диагностировать события происходящие непосредственно перед перезагрузкой. Некоторые корпоративный и законодательные политики определяют, сколько времени должны храниться файлы журналов брандмауэров или аналогичных устройств. Если ваша организация требует долгосрочного хранения журналов, вам придётся заняться конфигурирование syslog-сервера.
Для запуска удалённого журналирования, установите Enable sysloging для удалённого

syslog-сервера и заполните IP адрес для вашего syslog-сервера Remote Syslog Server. Если вы хотите отключить локальное журналирование, вы можете отметить Disable writing log files to the local ram disk, но обычно этого делать не рекомендуется.
Обычно, syslog-сервер, это сервер напрямую связанный с локальным интерфейсом системы pfSense. Журналирование может осуществляться на сервер через VPN, но для этого могут потребоваться некоторые дополнительные настройки (смотрите раздел 13.4.4 "Трафик инициируемый pfSense и IPsec"). Вы не должны передавать данные syslog непосредственно через WAN интерфейс, поскольку эти данные являются простым текстом и могут содержать значимую информацию.
Установите флаги для типов записей, которые вы хотите копировать на syslog-сервер. Вы можете выбрать удалённую регистрацию системных событий, событий брандмауэра, событий службы DHCP, аутентификации, события VPN либо все виды событий сразу. Убедитесь, что нажали кнопку Save после изменения настроек.
Если у вас нет syslog-сервера, его достаточно просто установить. Смотрите раздел 24.3 "Syslog-сервер для Windows с использованием Kiwi Syslog". Практически любой UNIX или его клон могут использоваться в качестве syslog-сервера. FreeBSD syslog-сервер описан в следующем разделе, для иных систем настройки могут несколько отличаться.

22.1.3.1 Конфигурирование syslog-сервера на базе FreeBSD

Установка syslog-сервера на основе FreeBSD потребует буквально пары шагов. В следующих примерах, замените192.168.1.1 на IP адрес вашего брандмауэра, замените exco-rtr именем хоста брандмауэра и замените exco-rtr.example.com полным именем хоста и доменом вашего брандмауэра. Я использовал в данных примерах 192.168.1.1, поскольку рекомендуется работать с внутренним адресом вашего маршрутизатора, а не интерфейм WAN.
Во-первых, вам понадобится запись в /etc/hosts, содержащая адрес и имя вашего брандмауэра, например:

192.168.1.1 exco-rtr exco-rtr.example.com

Затем, вам необходимо настроить флаги запуска syslogd, чтобы принимать сообщения syslog от брандмауэра. Отредактируйте /etc/rc.conf и добавьте следующую строку:

syslogd_flags ="-a 192.168.1.1"

И, наконец, вам необходимо добавить некоторые строки в /etc/syslog.conf которые будут описывать захват записей для нашего узла. В конец файла необходимо добавить:

```
! *
+*
+exco-rtr
*.* /var/log/exco-rtr.log
```

Эти строки сбрасывают программу и фильтры хостов, а затем установят фильтр хоста для вашего брандмауэра (используя его краткое наименование как описано в /etc/hosts). Если вы знакомы с syslog, вы можете рассмотреть /etc/syslog.conf на маршрутизаторе pfSense.

После внесения изменений необходимо перезапустить syslogd. На FreeBSD это действие выполняется одной командой:

 # /etc/rc.d/syslogd restart

Теперь вы можете наблюдать log-файл на syslog сервере и видеть, что он заполняется записями действий производимых брандмауэром.

Продолжение следует...

Метки: pfsense, нЭмного пА РусскЕ pfSense 1.2.3 Глава 22 Начало **п.п. Не удалось перейти к первой главе - приходится выполнять актуальный перевод. Потому перехожу к главе 22.**

Глава 22 Системный мониторинг

Столь же важной частью, как и предоставление основных сервисов, является информация и данные о текущих процессах и состоянии системы, которые предоставляет pfSense. Иногда кажется, что коммерческие маршрутизаторы стараются максимально скрывать от пользователей значительную часть информации, но pfSense позволяет предоставить пользователю практически любой объём информации.

22.1 Системные журналы

По умолчанию, pfSense регистрирует довольно малый объём данных, который позволяет избежать переполнения хранилища маршрутизатора. Журналы можно обнаружить на вкладке Status >> System Logs в web интерфейсе, и в каталоге /var/log файловой системы. Некоторые компоненты, такие как DHCP и IPsec генерируют достаточно объёмную информацию, поэтому вынесены на отдельные вкладки, в целях улучшения читаемости журналов и поиска требуемой информации. Чтобы увидеть эти журналы, выберите вкладку соответствующей подсистемы.

Журналы pfSense ведутся в циркулярном бинарном логе или в clog-формате. Они имеют фиксированные размеры и никогда не разрастаются. Как следствие - журнал содержит только определённое количество записей, и устаревшие записи удаляются из журнала с приходом новых. Если для вас это проблема - можно скорректировать поведение журнала, позволив копировать записи на удалённый syslog-сервер, где они могут храниться постоянно и ротироваться с меньшей скоростью. Смотрите раздел 22.1.3 "Удалённое журналирование с syslog" более подробно рассматривающий настройки данной возможности.

22.1.1 Просмотр системных журналов

Системные журналы могут быть найдены на вкладке Status >> System Log, меню System. Они содержат записи журнала, непосредственно сгенерированные узлом, некоторыми службами и пакетами, которые не перенаправляются на другие вкладки

системного журнала. Как показано на рисунке 22.1 "Пример записей системного журнала" здесь есть записи демона SSH, пакета avahi и клиента динамического DNS. Здесь же регистрируются и множество других систем, но большинство сервисов не будет загружать системный журнал. Обычно, если служба ведёт объёмный журнал, она перемещает его на собственную вкладку.

Обратите внимание, что журналы сконфигурируются и позволяют отображать записи в порядке их обновления - т.е. новые записи появляются в вершине списка. Смотрите следующий раздел, который расскажет о конфигурировании журналов.

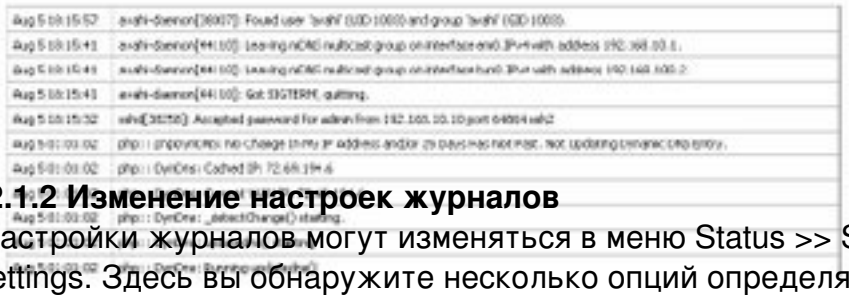


Рисунок 22.1

22.1.2 Изменение настроек журналов

Настройки журналов могут изменяться в меню Status >> System Logs на вкладке Settings. Здесь вы обнаружите несколько опций определяющих, как журналы будут отображаться на экране. Первая опция <Показать записи журналов в обратном порядке> (Show log entries in reverse order), управляет порядком, в котором записи журнала выводятся на экран. Установка этой опции приводит к тому, что новые записи журнала выводятся ввеху. При отключении этой опции новые записи будут выводится в низ журнала. Многие пользователи считают что оба метода вывода информации полезны в различных ситуациях.

Следующая опция <Число отображаемых записей журнала> (Number of log entires to show), позволяет задать число выводимых записей журнала на каждой из вкладок. Фактически, журналы могут содержать больший объём данных и данная опция позволяет ограничить или расширить визуальную информативность журнала.

Обычно, каждый пакет блокированный правилом по умолчанию брандмауэра подлежит регистрации в журнале. Если вы не хотите видеть эти записи, снимите флаг <Вести журнал блокировки пакетов правилом по умолчанию> (Log packets bloked by rule).

Опция <Показывать журнал raw-фильтра> (Show raw filter logs) контролирует вывод закладки журнала <Брандмауэр> (Firewall). Когда она установлена, вывод журнала не будет интерпретироваться синтаксическим парсером, а будет осуществляться в необработаном (сыром) формате. Иногда, это позволяет легче идентифицировать неисправность, либо предоставит службе поддержки больший объём информации, чем предоставляет стандартный вывод брандмауэра. Сырые журналы более сложно читать и интерпретировать и в большинстве случаев опция остаётся неиспользованной.

После изменения настроек нажмите Save. Оставшиеся опции мы обсудим в следующем разделе.

продолжение скорее всего вечером... Метки: pfsense, НЭмного пА РусскЕ pfSe

nse 1.2.3 Глава 14 - Окончание

14.8 Перенаправление PPTP

Перенаправление PPTP позволяет передавать трафик PPTP предназначенный вашему WAN IP адресу на внутренний PPTP сервер. Чтобы задействовать эту функцию, выберите <Перенаправление входящего PPTP соединения> (Redirect incoming PPTP connections) и введите IP адрес вашего внутреннего сервера в строку ввода . Функционально, это действие эквивалентно добавлению записи перенаправления порта 1723 и GRE протокола к вашему внутреннему PPTP серверу, который вы предпочитаете использовать. Существование данного функционала - историческое наследие m0n0wall, в котором базовый IP фильтр не поддерживал передачу протокола GRE. Возможность была сохранена, поскольку многие пользователи привыкли пользоваться этой функцией и многие предпочитают использование одной записи вместо двух прямых прописываний портов. Правила брандмауэра для протокола GRE и порта 1723 добавляются автоматически для WAN. Вам нет необходимости вводить правила брандмауэра при использовании перенаправления PPTP, если у вас не отключено опция <Отключать все авто добавления правил VPN> (Disable all auto-added VPN rules) в меню System >> Advanced.

14.9 Проблемы PPTP.

Этот раздел рассматривает диагностику проблемных ситуаций возникающих при использовании PPTP.

14.9.1 Невозможно установить соединение

Для начала убедитесь, что клиентский компьютер соединён с интернетом. Если это верно, обратите внимание на ошибки, которые выдаёт клиент. Windows (кроме Vista) информирует кодом ошибки, который поможет локализовать проблемы. Windows Vista такой информации не предоставляет, и следовательно, затрудняет диагностику отказов соединения, но к счастью, эта проблема решена в Windows 7. Проводить поиск и устранение неисправностей в Vista не рекомендуется. Для тех кто использует не Windows клиенты диагности проблем примерно такая же, но со своими подходами.

14.9.1.1 Error 619

Ошибка 619 сообщает о том, что происходит повреждение GRE трафика. Практически всегда это результат работы брандмауэра за которым находится клиент. Если клиент находится так же за pfSense, убедитесь, что ни один из сценариев описанных в разделе 14.4 "Ограничения PPTP" не имеет место. Если брандмауэр, за котором находится клиент представляет собой какой-то другой продук или оборудование, возможно требуется специальная настройка. В некоторых случаях, например при использовании беспроводных провайдеров 3G, клиентам присваиваиваются частные IP адреса, и вам придётся выбрать другую форму VPN.

14.9.1.2 Error 691

Данная ошибка вызывается недопустимым именем пользователя или паролем. Это

означает, что пользователь ввёл некорректное имя или пароль для клиента PPTP. Исправьте имя и/или пароль в соответствии с конфигурацией пользователя в базе данных PPTP или на RADIUS сервере.

14.9.1.3 Error 649

Проходя аутентификацию на RADIUS сервере Microsoft Windows с использованием IAS можно встретить ошибку 649. Она означает, что учётная запись не имеет разрешения набора и вероятной причиной этого может быть:

1. Установка "Deny access" на разрешение набора - в свойствах пользовательского аккаунта Active Directory Users and Computers на владке Набор (Dial-in). В зависимости от требуемой конфигурации IAS вы можете установить разрешение доступа (Allow access) или предоставить доступ через политику удалённого доступа (Control access through remote access policy).
2. Истёк срок действия пароля пользователя - соответственно пользователь не может использовать PPTP.
3. Неправильная конфигурация IAS - возможно вы неверно сконфигурировали правила политик и пользователи не могут соединится.

14.9.2 Соединение PPTP не передаёт трафик

Убедитесь, что вы добавили правила брандмауэра для интерфейса VPN PPTP как было описано в разделе 14.5.5 "Конфигурирование правил брандмауэра для клиентов PPTP". Так же, следует убедится, что удалённая подсеть работающая через VPN отличается от лакальной подсети. Если вы пытаетесь соединиться с сетью 192.168.1.0/24 через VPN, а локальная подсеть клиента имеет адресацию 192.168.1.0/24, трафик предназначенный для удалённой сети никогда не будет пересекать VPN, поскольку находится в окальной сети. Именно поэтуму следует выбирать заведомо несвязанную подсеть при использовании VPN, о чём уже говорилось в разделе 4.2.4 "Конфигурация LAN интерфейса".

14.10 Хитрости марсшрутизации PPTP

Если вы хотите, чтобы выбранные подсети маршрутизировались через туннель PPTP, это можно сделать путём маршрутизации на клиенте. Следующие методы работают на Windows XP, Vista и Windows 7, и возможно могут работать на любой другой платформе. Предполагается, что уже сконфигурировали клиентскую часть не передавать весь трафик через соединение (т.е. не использовать удалённый шлюз).

Во-первых, клиенту PPTP должен быть присвоен статический адрес в профиле пользователя. Это можно сделать используя встроенную аутентификацию, или посредством RADIUS. Статический адрес должен находится за пределами общего пула адресов. Данный способ должен направить трафик предназначенный для удалённых подсетей к адресу присвоенному PPTP. Мы заставим трафик для этих подсетей двигаться по туннелю на другой стороне. Способ не ограничивается подсетями, которые сразу достижимы с другой стороны, поскольку могут использоваться любые подсети. Это весьма удобно, если вы хотите пткрыть доступ к стороннему сайту через тунель VPN. Команды могут быть введены в командной строке, но в нашем примере мы запишем их в командный файл:

@echo off
route add 192.168.210.0 mask 255.255.255.0 192.168.1.126
route add 10.99.99.0 mask 255.255.255.0 192.168.1.126
route add 172.16.1.0 mask 255.255.252.0 192.168.1.126
pause

В этом примере, 192.168.1.126 - статический IP, присвоенный пользователю клиента PPTP. Команды направляют три указанных подсети через PPTP соединение, дополнительно к подсети соединённой непосредственно. Пауза опциональна, но она может помочь убедится, что все маршруты добавлены успешно. Пакетный файл должен выполняться каждый раз при установлении соединения.

NOTE
На Windows VIsta и WIndows 7, эти команды должны выполняться с правами администратора. Если вы создали ярлык на данный пакетный файл, измените его свойства предоставив ему эти права. Аналогично щёлкнув правой кнопкой на файле вы можете выбрать опцию <Выполнить в роли администратора>.

14.11 Логи PPTP
Запись событий авторизации и выхода пользователей хранятся в Status >> System Logs, закладка PPTP.

Рисунок 14.35

Как вы можете видеть на рисунке 14.35 "Журнал PPTP", каждый вход и выход пользователя записываются с указанием метки времени, имени пользователя и IP адресом присвоенным клиенту PPTP.

Продолжение следует ... вечерком Метки: pfsense, НЭмного пА РусскЕ pfSense 1.2.3 Глава 14 - продолжение

14.5.2 Аутентификация
Можно производить аутентификацию пользователей по локальной базе пользователей, или посредством RADIUS-сервера. RADIUS позволяет соеденяться с другим сервером в вашей сети, для целей аутентификации. Такая возможность может использоваться для аутентификации пользователей PPTP с помощью Microsoft Active Directory (см. раздел 24.1 "Аутентификация RADIUS с Windows Server"), или другими RADIUS совместимыми серверами. Для использования RADIUS, установите флаг <Использовать сервер RADIUS> (Use a RADIUS server) и заполните поля во вкладках и . Для аутентификации с использованием локальной базы данных пользователей, снимите данный флаг. Если вы используете RADIUS вам не нужно вам не нужно добавлять пользователей на вкладке Users VPN >> PPTP. Смотрите раздел 14.5.6, "Добавление пользователей" более подробно рассматривающий встроенную систему

аутентификации.

14.5.3 Необходимость 128 битного шифрования.

Используйте 128 битное шифрование везде где это возможно. Большинство клиентов PPTP поддерживают 128 битное шифрование, таким образом, оно прекрасно работает в большинстве сетевых сред. PPTP достаточно слабо защищён даже при использовании 128 битного шифрования и тем более при 40 и 56 битном. Если специальных требований нет, недопустимо использовать шифрование ниже чем 128 бит для PPTP.

14.5.4 Сохранение изменений для запуска PPTP сервера

После заполнения вышеописанных настроек, нажмите Save. При этом ваша конфигурация будет сохранена и PPTP сервер запустится. Если вы аутентифицируете своих пользователей по локальной базе, перейдите на вкладку Users и введите данные своих пользователей.

14.5.5 Конфигурирование правил брандмауэра для клиентов PPTP

Открываем Firewall >> Rules и выбираем закладку PPTP VPN. Эти правила управляют трафиком клиентов PPTP. Пока вы не добавите правила брандмауэра, весь трафик инициируемый клиентами PPTP будет блокироваться. Трафиком исходящим от внутреннего LAN до клиентов PPTP управляют правила брандмауэра LAN. Для начала можно добавить правило разрешающие весь трафик, как показано на рисунке 14.2, "Правила брандмауэра VPN PPTP", но после тестирования работы следует ввести более жёсткие ограничения на данные правила.

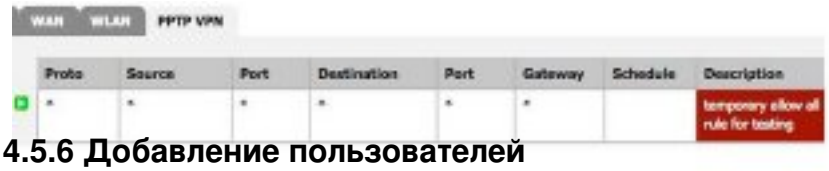


Рисунок 14.2

14.5.6 Добавление пользователей

Добавление пользователей для сервера RADIUS может меняться от версии к версии. Эта процедура выходит за рамки контекста этого раздела, и рассматривается в документации на RADIUS сервер.

Добавление пользователей во встроенную базу pfSense производится достаточно просто. Во-первых, выберите VPN >> PPTP и перейдите на вкладку Users. Вы увидите пустую таблицу пользователей показанную на рисунке 14.3, "Вкладка Пользователи PPTP". Нажмите кнопку для добавления пользователя.

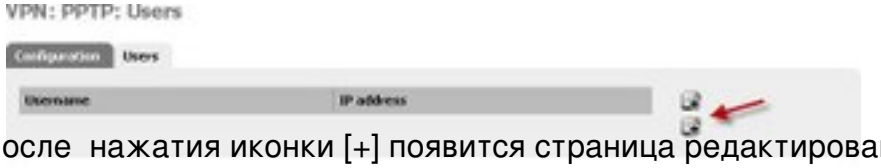


Рисунок 14.3

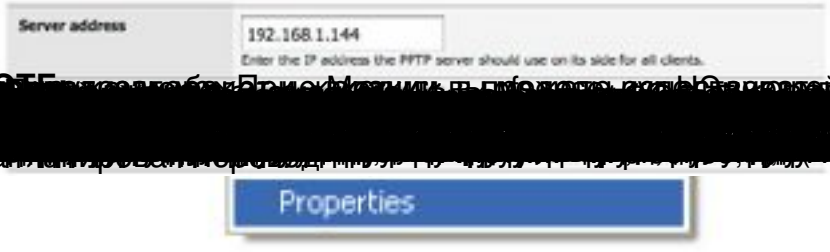
После нажатия иконки [+] появится страница редактирования пользователя. Заполните имя и пароль пользователя как показано на рисунке 14.4 "Добавление пользователя PPTP". При желании можно ввести статический IP присваиваемый пользователю.


VPN: PPTP: User: Edit
Username
Password
VPN: PPTP: Users
The PPTP user list has been modified.
You must apply the changes in order for them to take effect.
Warning: this will terminate all current PPTP sessions!
Apply changes
Configuration
Users
Username
IP address

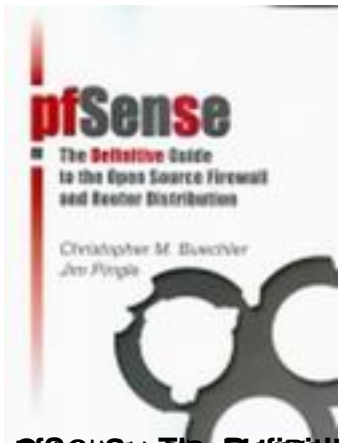

VPN: PPTP: Users
The changes have been applied successfully. You can also monitor the filter reload progress.
Configuration
Users


Network Tasks
Create a new connection


ExampleCo
Disconnected, Firewalled
Connect
Status
Set as Default Connection


Server address
192.168.1.144
Enter the IP address the PPTP server should use on its side for all clients.
Properties

Автор:
30.12.10 09:26 - Последнее обновление 12.09.11 08:09



Guide to the pfSense

http://iboxio.livejournal.com/tag/pfsense