Автор:
02.04.12 10:08 - Последнее обновление 02.04.12 10:12

Руководство по pfSense 2.0. Часть 22

Часть 22 Системный мониторинг

оглавление

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.

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.

Просмотр 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 региструются 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.

Aug 5 18:15:57	avahi-daemon[38307]: Found user 'avahi' (UID 1003) and group 'avahi' (GID 1003).
Aug 5 18:15:41	avahi-daemon[44110]: Leaving mDNS multicast group on interface em0.IPv4 with address 192.168.10.1.
Aug 5 18:15:41	avahi-daemon[44110]: Leaving mDNS multicast group on interface tun0.IPv4 with address 192.168.100.2.
Aug 5 18:15:41	avahi-daemon[44110]: Got SIGTERM, quitting.
Aug 5 18:15:32	sshd[38258]: Accepted password for admin from 192.168.10.10 port 64864 ssh2
Aug 5 01:01:02	php: : phpDynDNS: No Change In My IP Address and/or 25 Days Has Not Past. Not Updating Dynamic DNS Entry.
Aug 5 01:01:02	php: : DynDns: Cached IP: 72.69.194.6
Aug 5 01:01:02	php: : DynDns: Current WAN IP: 72.69.194.6
Aug 5 01:01:02	php: : DynDns: _detectChange() starting.
Aug 5 01:01:02	php: : DynDns: updatedns() starting
Aug 5 01:01:02	php: : DynDns: Running updatedns()

Рисунок 22.1

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 вверху. 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 необработанном (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.

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 увас 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.

Конфигурирование syslog-сервера на базе FreeBSD

Установка syslog-сервера на основе FreeBSD потребует буквально пары шагов. В следующих примерах, замените 192.168.1.1 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.

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, поэтому нет необходимости в обновлении страницы.

System information	
Name	pfsense-123test
Version	**1.2.3-RC2** built on Thu Jul 23 17:25:52 EDT 2009
Platform	pfSense
Uptime	4 days, 15:47
State table size	7/10000 Show states
MBUF Usage	420 /1290
CPU usage	0%
Memory usage	7%
SWAP usage	0%
Disk usage	2%

Рисунок 22.2 Статус системы

Статус интерфейсов

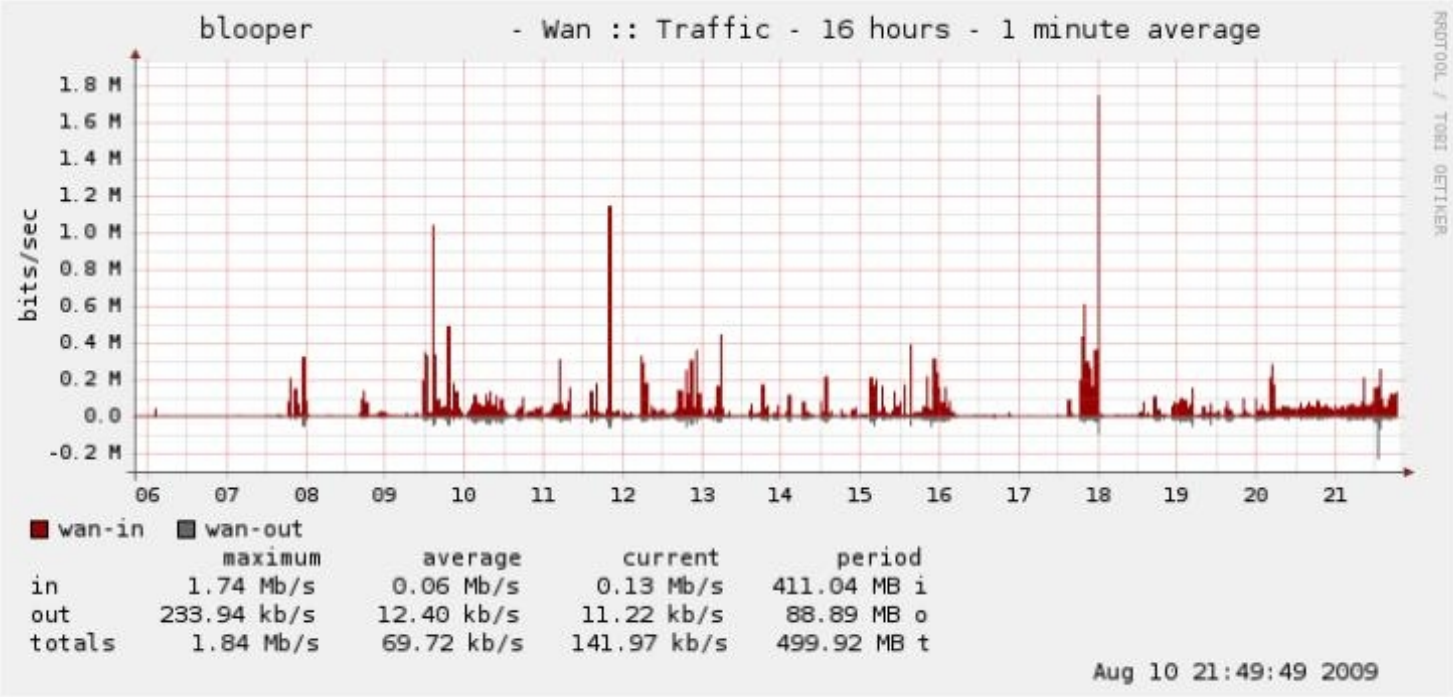
Статус сетевых интерефйсов можно наблюдать на странице Status >> Interfaces. В первой части Рисунка 22.3 "Состояние интерфейсов" показано PPPoE WAN соединение и можно наблюдать данные о его IP адресе, DNS и прочих параметрах. Так же вы можете увидеть MAC адрес сетевого интерфейса, тип среды передачи, число входящих/исходящих пакетов, ошибки и коллизии. Для динамических типов соединений, таких как PPPoE и PPTP доступна кнопка [Disconnect] когда соединение установлено и [Connect] - когда соединение разорвано. Для интерфейсов получающих IP адрес от DHCP сервера доступна кнопка [Release] когда аренда адреса активна, и [Renew] - в противном случае. В нижней части рисунка Вы видите информацию по LAN соединению. Поскольку, это нормальный интерфейс со статическим адресом, для него отображается стандартный набор элементов. Если статус интерфейса указан как "no carrier" обычно, это означает что кабель интерфейса не подключен, либо на другом конце кабеля устройство работает некорректно. Если показаны какие либо ошибки, они обычно имеют чисто физическую природу - либо кабельное соединение либо ошибки порта. Наиболее часто это проблема кабелей, соответственно и решение проблемы простое и дешёвое.

Статусы сервисов

Состояние множества демонов различных систем и служб отражены на странице Status >> Services. Каждый сервис отображается с собственным именем, описанием и состоянием, как показано на рисунке 22.4 "Статусы сервисов". Состояние сервиса обычно представляется как Выполняется (Runnung) или Остановлена (Stopped). С этой страницы вы можете перезапустить или остановить сервис. Обычно нет необходимости прямого управления сервисами, но иногда, в целях диагностики это может быть удобно.

Service	Description	Status
avahi	Not available.	Running
dnsmasq	DNS Forwarder	Running
ntpd	NTP clock sync	Running
dhcpd	DHCP Service	Running
bsnmpd	SNMP Service	Running
miniupnpd	UPnP Service	Running
racoon	IPsec VPN	Running

[redacted]



[redacted]

tcp	192.168.10.10:53650 -> 72.69.194.6:41047 -> 168.143.168.68:443	FIN_WAIT_2:FIN_WAIT_2
udp	224.0.0.251:5353 <- 192.168.10.17:5353	NO_TRAFFIC:SINGLE
tcp	207.45.186.18:80 <- 192.168.10.11:1289	ESTABLISHED:ESTABLISHED
tcp	192.168.10.11:1289 -> 72.69.194.6:52740 -> 207.45.186.18:80	ESTABLISHED:ESTABLISHED

[redacted]