Автор:
30.03.12 14:15 - Последнее обновление 30.03.12 14:21

Руководство по pfSense 2.0. Часть 2

Часть 2 Аппаратные средства

оглавление

Одно из главных преимуществ pfSense над другими программными маршрутизаторами, это поддержка любых аппаратных средств, которые поддерживает ОС FreeBSD на платформе i386 и amd64. Такие платформы как MIPS, PowerPC и ARM на данный момент не поддерживаются. Возможно в будущем и появятся версии pfSense для embeded-систем, но на данный момнет такая возможность недоступна. С релизом версии 2.0RC1 появилась поддержка 64-битных систем, хотя и раньше версия для 32-битных прекрасно себя чувствовала на таких системах. Использование 64-битной версии приносит пользу только в системах сетевой защиты с большим объемом памяти (больше 3ГБ).

Аппаратная совместимость

Самый надежный способ для определения совместимости Ваших аппаратных средств с той или иной версией pfSense это FreeBSD Hardware Notes (Список поддерживаемых аппаратных средств ОС FreeBSD). Например, версия pfSense 1.2.3 имеет в качестве

базы ОС FreeBSD версии 7.2, следовательно нужно смотреть hardware notes для этой версии. Такая информация может быть найдена на официальном сайте FreeBSD - http://www.freebsd.org/releases/7.2R/hardware.html
?. В pfSense версии 2.0 используется база FreeBSD версии 8.2, следовательно информацию о поддержке нужно искать http://www.freebsd.org/releases/8.2R/hardware.html
?. Далее мы рассмотрим руководство по выбору аппаратных средств, имеющих лучшую поддержку в области сетевой защиты и маршрутизации.

Сетевые адаптеры

pfSense поддерживает практически любые сетевые адаптеры (далее NIC), но не все NIC одинаково полезны. В зависимости от производителя аппаратные возможности чипа могут сильно различаться. Наиболее рекомендуемым является использование адаптеров Intel Pro 100/1000, так как они имеют наилучшую поддержку во FreeBSD и драйвера написаные специалистами Intel. Наиболее распространенными являются NIC от компании Realtek серии rl8139, и хотя это оборудование чрезвычайно популярно, оно имеет наихудшее качество. Вот небольшой отрывок комментария из текста драйвера для данного чипа, который говорит о многом: "Realtek 8139 PCI NIC определяется как "low end". Вероятно, это самый плохой контроллер Ethernet из когда либо сделанных". Множество производителей используют данный чип в погоне за уменьшенной себестоимостью производимого оборудования. Так же Вы обнаружете чипсет 8139 во множестве встроенных устройств и в принципе они работают, но могут возникнуть значительные неполадки. Например VLAN может не работать должным образом или не работать вообще. Если Вы планируете создание качественной сети с высокой пропускной способностью - не стоит экономить на сетевом оборудовании. Так же, если Вы планируете использование VLAN - убедитесь, что покупаете оборудование поддерживающее VLAN на аппаратном уровне. Подробнее об этом, мы расскажем в части 10 "Виртуальные LAN; VLAN.

Программный маршрутизатор pfSense так же поддерживает USB NIC-адаптеры, и хотя они прекрасно работают на рабочих станциях и домашних компьютерах, их

использвоние в крупных сетях с высокой надежностью крайне не рекомендуется.

Беспроводные адаптеры широко поддерживаются. Рекомендации по выбору такого адаптера мы приведем в части 18.

Минимальные требования к оборудованию

Далее мы рассмотрим минимальные требования к оборудованию для разворачивания pfSense версии 2.0. Стоит так же сказать, что минимальные требования не являются подходящими для всех сред, подробнее смотрите далее в "Руководстве по определению оборудования".

Наиболее общие требования для всех платформ pfSense - центральный процессор - 100 МГц или больше; - оперативная память - 128 Мб или больше.

Требования определённые для конкретных платформ следующие:

LiveCD

- привод CD-ROM

- USB флэш или привод флоппи дисков для хранения файла конфигурации

Полная инсталляция

- привод CD-ROM

- 1Гб или более на жёстком диске

Встроенная NanoBSD

- 512 Мб или большая карта Compact Flash

- Серийный порт для консоли

- нуль-модемный кабель для соединения с консольным портом

Оборудование

По своей натуре, ОС из семейства OpenSource частенько вызывают проблемы с аппаратной совместимостью. Некоторе оборудование может поддерживаться системой в целом, но некоторые функции будут недостпуны. Бывает отказывются работать вместе различные комбинации оборудования, даже если по отдельности они полностью функционаровали. Системы, которые поддерживают полноценную работу в Windows, зачастую вообще не могут работать с Linux или BSD. Некоторые проблемы совместимости можно решить, если Вы столкнетесь с проблемами связанными с оборудованием - часть 3 данного руководства, поможет Вам в поиске решения

некоторых проблем.

Предотвращение аппаратных проблем

Этот раздел предлагает некоторые советы по решению проблем с оборудованием.

Ряд производителей предоставил свое оборудование нашим разработчикам и при его использвании Вы гарантируете себе, что данное решение полностью протестировано. Посетите http://www.pfsense.org/vendors для получения свежей информации о рекомендуемом оборудовании.

Руководство по определению оборудования

Подбирать оборудование для инсталляции pfSense следует учитывая требуемую пропускную способность системы и особенности ее использования. Далее мы постараемся более подробно разобрать этот вопрос.

При разворачивании брандмауера с ожидаемой пропускной способностью менее 10 Мбит/с, Вы можете ииспользовать минимальные требования к системе, а при необходимости более высоких скоростей мы рекомендуем обратиться к данному руководству, осноманному на нашем длительном опыте использования системы. Самое существенное влияние на пропускную способность оказывает выбор сетевого адаптера, а также мощность Вашего ЦП. Таблица 2.1 "Зависимость максимальной пропускной способности от процессора"? показывает максимальную достижимую пропускную способность при использовании двух PCI NIC Realtek 8139 в сравнении с двумя PCI адаптерами Intel Pro/1000 GT Desktop.?

Сетевые адаптеры Realtek гораздо сильнее расходуют ресурс Вашего ЦП, в отличии от качественных адаптеров Intel. При использовании адаптеров Realtek, ЦП станет первым узким местом в производительности брандмауера. Мощность процессора может быть использована значительно ьолее эффективно, что и показывает таблица 2.1

Таблица 2.1 Зависимость максимальной пропускной способности от процессора

Процессор	Адаптер на борту максимальная пропускная способность (Mbps)	Realtek максимальная пропускная способность (Mbps)	Intel Pro/1000 максимальная пропускная способность (Mbps)
Pentium MMX 200MHz	-	25 Mbps	40 Mbps
WRAP-266 MHz Geode	24 Mbps	-	-
ALIX-500 MHz Geode	85 Mbps	-	-
VIA 1GHz	93 Mbps	-	-
Netgate Hamakua (1GHz Celeron)	250 Mbps	-	-
Pentium II 350MHz	-	51 Mbps	64 Mbps
Pentium III 700MHz	-	84 Mbps	217 Mbps
Pentium 4 1.7GHz	-	93 Mbps	365 Mbps

При развертывании гигабитной сети, необходимо определить, какая именно пропускная способность реально нужна, весь 1 Гбит/с или только 200-300 Мбит/с. Если Вам будет достаточно производительности в 200Мбит/с, то любая 1ГГц система с качественным сетевым адаптером справится с такой нагрузкойю, а для производительности в 400-500 Мбит/с будет достаточно 2-3ГГц ЦП.

Числа в таблице 2.1. остановились на относительно низком уровне, поскольку это достаточно разумные значения для лабораторного тестирования. Тестирование мультигигабитной системы требует серверов и систем способных к формированию 1Гбит. Мы не имели адекватного оборудования для данного масштаба. Но это не

позволяет сказать, что pfSense не подходит для данной среды; реально pfSense может использоваться в подобных системах. При выборе оборудования для мультигигабитных систем основным фактором является число пакетов в секунду, а не гигабиты в секунду. Вы будете попадать в рамки ограничений FreeBSD и самых быстрых четырёх-ядерных серверов - 500,000 пакетов в секунду (pps). Пропускная способность зависит от вашей сетевой среды, и в некоторой степени может определяться справочной информацией из таблицы 2.2. "Пропускная способность 500,000 pps для различных размеров кадров".

Для развёртывания системы со скоростью 1Гбит/с между двумя интерфейсами может быть использован Pentium 4 с частотой 3ГГц или более быстрый ЦП с PCI-X или PCI- e адаптером. Использование PCI позволяет вам достигать скорости в несколько сотен Мбит/с, однако ограничения шины PCI будут препятствовать повышению производительности между двумя 1Гбитными адаптерами. Если вы подбираете оборудование для системы реализующей гигабитный обмен на множестве интерфейсов, следует позаботится о современном сервере с четырёх-ядерным процессором и PCI-e адаптерами. Если вам необходимо превысить предел в 500,000 пакетов в секунду, вам может не хватить возможности дешёвого оборудования (commodity PC hardware) для передачи пакетов.

Таблица 2.2. Пропускная способность 500,000 pps для различных размеров кадров

Размер кадра	Пропускная способность 500Kpps
64 байта	244Мбит/с
500 байт	1.87 Гбит/с
1000 байт	3.73 Гбит/с
1500 байт	5.59 Гбит/с

Особенности

Вообще особенности использования той или иной установки pfSense не сильно сказываются на выборе оборудования, однако есть и такие, которые могут оказать на

это существенное влияние.

Одна из таких особенностей это "Таблица состояний брандмауера", используемая для отслеживания текущих активных сетевых подключений, при этом каждое подключение исполбзует одо состояние. Подробнее о состояниях читайте в Части 6 "Межсетвая защита". Сети содержащие большое количество одновременных соединений требуют увеличенных объемов оператиной памяти, так как каждое состояние занимает около 1Кбайта RAM. В Таблице 2.3 "Потребление оперативной памяти таблицами состояний"? показана информация о требуемых объемах памяти для больших таблиц состояний. Имейте ввиду, что другие компоненты pfSense так же требуют дополнительной оперативной памяти, минимум 32-48Мбайт и больше, опять же в зависимости от особенностей использования.

Таблица 2.3. Потребление оперативной памяти таблицами состояний

Состояния	Требуемый объём оперативной памяти
100000	~97 Мб
500000	~488 Мб
1000000	~976 Мб
3000000	~2900 Мб

VPN (все типы)

При выборе оборудования для построения VPN важна требуемая пропускная способность. Шифрование и дешифрование трафика для всех типов VPN? очень сильно нагружает ЦП. В pfSense представлено шесть видов шифрования при использовании IPsec: DES, 3DES, Blowfish, CAST128, AES и AES 256.? Алгоритмы шифрования работают по разному, и максимальная производительность вашего брандмауэра зависит от типа используемого шифрования. 3DES широко используется из-за его функциональной совместимости практически со всеми устройствами IPsec, однако он является самым медленным алгоритмом поддерживаемым pfSense в отсутствии аппаратных криптоакселераторов. Аппаратные криптоакселераторы, такие

как платы Hifn, значительно увеличивают максимальную производительность VPN?. Таблица 2.4. "Производительность IPsec с различными алгоритмами шифрования" демонстрирует максимальную производительность для оборудования PC Engines ALIX(500 МГц Geode), с крипто ускорителем Soekris vpn1411 Hifn и без.

Таблица 2.4. Производительность IPsec с различными алгоритмами шифрования

Шифрующий протокол	Максимальная производительность (Мбит/с)	Максимальная производительность с Hifn (Мбит/с)
DES	13.7	34.6
3DES	8.4	34.3
BlowFish	16.5	не ускоряет (без изменений)
CAST 128	16.3	не ускоряет (без изменений)
AES	19.4	34.2
AES 256	13.5	34.2

Таблица 2.5. "Производительность ЦП с IPsec" показывает максимальную производительность IPsec с алгоритмом шифрования Blowfish, в зависимости от используемого ЦП, иллюстрируя тем самым сравнительную мощность процессоров.

Таблица 2.5. "Производительность ЦП с IPsec"

Центральный процессор	Производительность BlowFish (Мбит/с)
Pentium II 350МГц	12.4
ALIX 500МГц	16.5
Pentium III 700МГц	32.9
Pentium 4 1.7ГГц	53.9

Аппаратные криптоакселлераторы, вроде Hifn, должны использоваться там, где требуется повышенная производительность IPsec, однако они неуместны при использовании двух и четырех-ядерных процессоров, так как данные процессоры обеспечивают более эффективное шифрование, нежели криптоакселлераторы

работающие на шине PCI.

Пакеты

Некоторые пакеты используемые в pfSense оказывают большое влияние на выбор оборудования.

Например Snort, система обнаружения вторжений, может требовать существенного объема оперативной памяти. В качестве разумного минимума рассматривается 256 Мбайт, однако некоторые конфигурации могут требовать и 1 Гбайт оперативной памяти.

Squid, кеширующий HTTP-прокси сервер, довольно требователен к дисковой системе Вашего оборудования, которая определяет производительность кеша программы. Для небольшой сети, даже при работе Squid'a, будет достаточно обычного жесткого диска любой скорости. Для более крупной сетевой среды (>200 пользователей) следует рассматривать жесткие диски повышенной производительности 10000 RPM (оборотов в минуту). SAS и SCSI диски с 15000 RPM рекомендованы к использованию в особо крупных сетевых средах. Так же pfSense поддерживает большинство аппаратных RAID-контроллеров. Использование RAID 10 позволит повысить производительность Squid и может быть рекомендовано для развёртывания системы с тысячами пользователей?.?

оглавление

{jcomments on}

//