Автор:
02.04.12 10:01 - Последнее обновление 02.04.12 10:06

Руководство по pfSense 2.0. Часть 21

Часть 21 Сервисы.

оглавление

В базовой установке, pfSense поставляется с набором сервисов добавляющих некоторую фундаментальную функциональность и гибкость присущую системе брандмауэра. Как следует из названия, данные опции будут предоставляться маршрутизатором клиентам, или другим маршрутизаторам. Данные сервисы включают DHCP адресацию, разрешение имён DNS и динамический DNS, SNMP, UPnP и многие другие. Эта глава рассматривает сервисы доступные в базовой системе. Кроме того существое большое число сервисов которые могут быть добавлены в базовую систему с помощью установки дополнительных пакетов.

Сервер DHCP

Сервер DHCP назначает IP адреса и связанные параметры конфигурации клиентским компьютерам вашей сети. Этот сервис включен по умолчанию на LAN интерфейсе с IP 192.168.1.1 и выделенным диапазоном адресов 192.168.1.10-192.168.1.199. В стандартной конфигурации, pfSense присваивает этот LAN IP в качестве шлюза по умолчанию и DNS сервера, если включена опция DNS Forwarder. WEB GUI позволяет настраивать множество опций данной конфигурации.

Чтобы изменить поведение DHCP сервера, перейдите на страницу **Services -> DHCP Se rver**
. Здесь вы можете изменить настройки DHCP сервера, статические сопоставления IP адресов и связанные с ним опции, такие как статические ARP.

На странице настройки DHCP есть вкладки для каждого HE-WAN интерфейса. Каждый интерфейс имеет свой собственный DHCP сервер, со своей конфигурацией, которые могут работать независимо друг от друга. Прежде чем вносить изменения, убедитесь что вы находитесь на вкладке нужного интерфейса.

Первая опция на каждой вкладке сообщает pfSense следует ли обрабатывать DHCP запросы на данном интерфейсе. Для включения DHCP на интерфейсе, отметьте флажок **Enable DHCP** для имени интерфейса. Для отключения сервиса DHCP снимите данный флаг. Обычно, DHCP сервер отвечает на запросы с любого клиента на аренду адресов. В большинстве сред это нормальное и приемлемое поведение, но в более ограниченной или более безопасной среде такое поведение нежелательно. С установленной опцией **Deny unknow clients**, аренду адресов будут получать только клиенты со статическим распределением, что конечно более безопасно, но менее удобно.

Примечание: *Таким образом можно реализовать защиту от пользователей с низким уровнем знаний и случайно подключенных устройств. Однако имейте в ви ду, что пользователь знающий в вашей сети постоянный IP адрес, маску подсети, шлюз и DNS может получить доступ. Он может изменить MAC адреса дабы соответствовать реальным клиентам сети и получить их арендные адреса. Где это возможно, объедините эту опцию со статическими записями ARP, контролем доступа к коммутатору, которые будут ограничивать доступ MAC*

*адресов
к
определённым портам коммутатора
в целях повышения
безопасности, а также включите
или отключите
переключение
известных неиспользуемых
портов.*

Кроме того, отображается IP адрес и маска подсети для настраиваемого интерфейса. Ниже отображается доступный диапазон IP адресов для маски подсети, что может помочь определить попадание начального и конечного адресов диапазона в пул DHCP.

Два поля диапазона сообщают pfSense первый и последний адрес пула DHCP. Первый адрес должен быть меньше второго. Например, по умолчанию для LAN диапазон DHCP базируется на подсети для IP адреса по умолчанию LAN. Это 192.168.1.10 - 192.168.1.199. Диапазон может изменяться в зависимости от ваших требований, но он должен находится в рамках подсети интерфейса.

Могут быть определены два WINS сервера (Windows Internet Name Server) . Если у вас один или несколько WINS серверов, здесь следует ввести их адреса. Фактически сервера не обязаны находится в той же подсети, но следует убедится, что существуют соответствующие правила маршрутизатора и брандмауэра, позволяющие их достичь. Если оставить это поле пустым WINS не будет передаваться клиентам.

В зависимости от ваших настроек, вы можете и не указывать DNS серверы. Если вы используете для обработки DNS форвардер встроенный в pfSense, оставьте эти поля пустыми и pfSense будет автоматически назначать себя как сервер DNS для клиентских хостов. Если DNS форвардинг отключается, и эти поля оставляются пустыми, pfSense действует основываясь на DNS серверах указанных в общих параметрах на странице **System->General setup**. Если вы хотите использовать специфические DNS сервера а не выбранные автоматически, следует заполнить указанные поля как минимум двумя значениями IP адресов (смотрите раздел 24.2. "Свободная фильтрация контента с использованием OpenDNS"). В сетях серверов ОС Windows, особенно при наличии AD, рекомендуется

использовать эти сервера для клиентов DNS. При использовании DNS форвардера в сочетании с CARP, укажите в этих полях CARP IP для этого интерфейса.

Опция Gateway может быть пустой, в случае, если pfSense является шлюзом для локальной сети. Если это не так, необходимо заполнить IP адрес шлюза который будет использоваться клиентами данного интерфейса. В случае использования CARP, здесь следует указать CARP IP для данного интерфейса.

Время аренды по умолчанию и максимальный период времени аренды указывают максимальную длительность аренды адреса DHCP. Время аренды по умолчанию используется в случае если клиент не запрашивает специфического времени истечения. Если клиент указывает, как долго он желает использовать аренду адреса, максимальное время аренды позволит ограничить данный запрос разумными пределами. Значения задаются в секундах, по умолчанию установлено 7200 секунд (2 часа) для параметра по умолчанию и 86400 секунд (1 день) для максимального времени аренды.

Если данная система является частью отказоустойчивого развёртывания, такого как кластер CARP, введите в данное поле IP адрес соседа системы. Это должен быть реальный IP адрес другой системы в данной подсети, а не общий CARP адрес.

Флаг **Enable Static ARP** работает аналогично отказу неизвестным MAC адресам в получении аренды, но позволяет сделать ещё один шаг в направлении ограничения любых неизвестных машин при подключении их к pfSense. Это позволит ограничить потенциальных нарушителей и закрыть им обход DHCP.

Замечание: *Будьте осторожны при использовании статических ARP, гарантируйте, что все системы
которые должны общаться
с маршрутизатором
перечислены
в статическом
списке перед
активацией данной опции, особо это касается системы, используемой для подключения к WEB
GUI.*

Динамический DNS (Dynamic DNS)

Для настройки динамического DNS нажмите кнопку Advanced справа от данного поля. Для включения данной опции установите флаг , а затем заполните доменное имя для имени хоста DHCP. Если вы используете DNS форвардер pfSense, вы можете оставить данный параметр пустым и настроить параметры в рамках DNS форвардера.

Для указания NTP серверов нажмите кнопку Advanced справа от данного поля и введите два IP адреса NTP серверов.

Для того что-бы включить установки загрузки по сети, нажмите кнопку Advanced справа от данного поля. Теперь вы можете установить флажок включения данной функции и ввести IP адрес, с которого будут доступны загрузочные образы, а так же указать имя файла загружаемого образа. Оба эти поля должны быть заполнены для нормального течения процесса загрузки по сети.

Сохранение настроек (Save Settings)

После внесения всех изменений не забудьте нажать кнопку Save, прежде чем создавать статические сопоставления. Настройки будут утеряны, если вы покинете страницу без сохранения.

Статическое сопоставление DHCP позволяет выделить предпочтения выделения IP адреса данному компьютеру, основываясь на его MAC адресе. В тех сетях где ограничиваются неизвестные клиенты, это позволяет иметь список "известных" хостов, которым позволено получать аренду адресов и статические ARP. Статические сопоставления могут быть добавлены двумя способами. Во-первых, на текущем экране вы можете нажать [+] и получить форму для статического сопоставления. Другой способ - добавление сопоставлений из обзора аренды DHCP, который мы рассмотрим далее. Из четырёх предоставленных полей необязатеьным является только MAC адрес. Ввод только MAC адреса позволяет добавить его в список известных клиентов в случае использования опции запрета неизвестных клиентов (Deny unknow clients).

Существующая ссылка рядом с полем MAC адреса позволяет копировать MAC адрес компьютера в список доступа к WEBGui. Это сделано для удобства работы по сравнению с другими более сложными путями, получения адреса.

Примечание: *На большинстве систем MAC адрес можно получить непосредственно из к омандной строки. В ОС UNIX или подобных, в том числе и на Mac OS X, введя команду "ifconfig-a" вы увидите MAC адреса для каждого интерфейса. В Windows MAC адреса можно получить используя команду "ipconfig /all". В большинстве случаев, MAC адреса можно обнаружить на наклейках сетевых карт либо рядом с ними (для случая интегрированого адаптера). Для хостов одной подсети, MAC можно пределить путём пингования IP адреса хоста и дальнейшим использованием команды "ARP -a".*

Поле IP адреса необходимо если используется статическое сопоставление IP, а не только как информация DHCP серверу о валидности клиента. Данный IP адрес должен быть реальным, а не резервируемым. Назначенный здесь IP адрес не будет мешать использованию этого же адреса в другом контексте. Если данный IP адрес используется в клиентских запросах аренды, он будет получен из главного пула адресов. По этой причине, WebGUI pfSense не позволяет назначать статические IP находящиеся внутри пула адресов DHCP. Может быть установлено имя хоста (HOSTNAME), и оно не обязательно должно совпадать с фактическим именем установленым на клиенте. Имя хоста установленное здесь будет использовано при регистрации адреса в DHCP в DNS форвардере. Описание (Description) является косметическим, и позволяет вводить любую дополнительную информацию о данной записи. Это может быть имя человека использующего ПК, описание функциональности или нечто другое. Вы можете оставить это поле пустым. Нажмите Save чтобы закончить редактирование статического сопоставления и вернуться к странице конфигурирования DHCP сервера.

Статус

Вы можете найти статус сервиса DHCP сервера на вкладке **Status -> Services**. Если он включен, его статус должен быть Running, как показано на рисунке 21.1. "Статус сервиса DHCP демона". Кнопка с правой стороны позволяет вам перезапустить или остановить службу DHCP сервера. Перезагрузка никогда не используется, поскольку pfSense автоматически перезапускает службу в случае изменений конфигурации, которые требуют перезагрузки. Остановка службы тоже скорее всего никогда не понадобится, если вы отключите все экземпляры DHCP сервера.

Service	Description	Status
dnsmasq	DNS Forwarder	Running
dhcpd	DHCP Service	Running

Рисунок 21.1. "Статус сервиса DHCP демона"

Аренда

Вы можете просмотреть текущее назначение аренды на странице **Diagnostics -> DHCP l eases**
. Этот экран показывает назначенные IP адреса, MAC адреса связанные с ними, имя хоста (если есть), начало и окончание срока аренды для активных клиентов, активность аренды, истечение или статическую регистрацию.

По умолчанию отображаются только активные и статические аренды, но вы можете просматривать все аренды, в том числе и истёкшие, нажав кнопку Show all configured leases. Для возврата к нормальному виду , нажмите кнопку Show active and static leases only.

Если вы нажмёте на MAC адрес, или кнопку Wake on LAN справа от аренды, pfSense передаст пакет Wake on LAN соответсвующему хосту. Более детельно Wake on LAN рассматривается в разделе 21.8 "Wake on LAN (Пробуждение по сети)".

Чтобы превратить динамическую аренду в статическое сопоставление, нажмите кнопку [+] справа от аренды. Вы попдете на экран **Edit static mapping** с предварительно заполненным MAC адресом хоста. Вам необходимо будет добавить желаемый IP адрес, имя хоста, описание и нажать Save. Любые существующие аренды для данного MAC адреса будут удалены из файла аренды при сохранении новой записи.

В процессе просмотра аренды вы можете вручную удалять неактивные или истёкшие аренды, нажав кнопку [x] в конце строки. Данная возможность недоступна для активных или татических аренд, только для автономных или истёкших.

Демон DHCP ведет логи своей активности доступные на странице **Status -> System Logs** , закладка DHCP. Отображается каждый запрос и ответ DHCP, наряду с другими статусами и сообщениями об ошибках.

DHCP-relay

DHCP запросы являются широковещательным трафиком. Широковещетельный трафик ограничивается широковещательным доменом где он инициируется. Если вам необходимо предоставить службу DHCP на сегменте сети без DHCP сервера, вы используете DHCP релей для направления этих запросов на определённый сервер в другом сегменте сети. Невозможно запусть DHCP сервер и DHCP релей одновременно. Чтобы включить DHCP релей, необходимо отключить DHCP сервер для каждого из интерфейсов. После того, как DHCP сервер отключен, перейдите на страницу **Services -> DHCP Relay** . Как и у DHCP сервера, здесь существует вкладка для каждого интерфейса. Нажмите на интерфейс, на котором планируете запустить DHCP релей, а затем установите флаг на Enable DHCP relay on [name] interface . Если вы отметите Append circuit ID и agent ID to request ,

DHCP
релей будет добавлять
circuid
ID
(в
pfSense
номер интерфейса) и
agent
ID
для запроса
DHCP
. Это может быть затребовано DHCP сервером на другой стороне, или может помочь определить источник запросов. Опция Proxy requests to DHCP server на подсети WAN делает именно то о чём она говорит. если опция установлена, она позволяет DHCP запросы с клиентов на этом интерфейсе к DHCP серверу который ассоциирован с IP адресом на WAN интерфейсе. Кроме того, вы можете заполнить IP адрес сервера DHCP для которого запросы должны проксироваться.

DNS форвардер

DNS форвардер в pfSense - это кеширующий DNS резольвер. Он включен по умолчанию, и использует DNS сервера сконфигурированные на странице **System -> General Setup** , или те сервера которые получены от ISP для динамически конфигурируемых WAN интерфейсов (DHCP, PPPoE и PPTP). Для статического IP WAN, необходимо ввести DNS сервера на странице System -> General Setup или в процессе установки мастера для функций DNS форвардера. Так же, вы можете использовать статически настроенные DNS сервера для динамически конфигурируемых WAN интерфейсов сняв флаг "Allow DNS
server
list
to
be
overridden
by
DHCP
/
PPP

on
WAN
" на странице
System
->
General
Setup
. В ранних версиях, pfSense первоначально пытался использовать первый сконфигурированный DNS сервер для разрешения имён, и переходил к последующим серверам если попытка не удавалась. Это могло приводить к длительным задержкам, если один или несколько серверов были недоступны. В pfSense 1.2.3. это поведение было изменено на одновременный опрос всех DNS серверов, и только первый ответ использовался и помещался в кэш. Результатом стало ускорение работы службы DNS и сглаживание проблемы медленной работы DNS серверов и их высокой латентности.

Конфигурирование DNS форвардера производится на странице **Services -> DNS Forwarder** .

Включение DNS форвардера

Отметьте этот флаг для включения DNS форвардера, или снимите его если вы хотите отключить данную функциональность.

Если вы хотите, чтобы ваши внутренние имена хостов для DHCP клиентов разрешались в DNS, отметьте этот флаг. Это работает только для машин которые определяют имя хоста в своих DHCP запросах.

Работает аналогично опции п. 21.3.1.2., кроме того, что регистрируются статические сопоставления DHCP.

Первый раздел в нижней части экрана DNS форвардера - здесь вы можете задать переопределение для DNS разрешения имён хостов. Вы можете настроить разрешить определённое имя хоста иным образом чем через DNS серверы, используемые для DNS форвардера. Это бывает полезно для для раздельной конфигурации DNS (см. раздел

7.5.2. "Разделение DNS") и в качестве полумеры блокирования доступа к некоторым специфическим web сайтам. Рисунок 21.2. "Пример переопределения DNS" иллюстрирует переопределение DNS для внутреннего web сервера (example.com и www.example.com), а так же пример блокирования доступа к myspace.com и www.myspace.com
.

Host	Domain	IP	Description
	example.com	192.168.1.100	www override
	myspace.com	127.0.0.1	hack block
www	myspace.com	127.0.0.1	hack block
www	example.com	192.168.1.100	www override

Рисунок 21.2. Пример переопределения DNS

Примечание: *Не рекомендуется использовать функциональность переопределения DNS как основное средство блокирования доступа к определённым сайтам. Есть огромное число способов обойти эту проблему. Этот метод может*

остановить технически не подготовленных пользователей, но может быть легко нейтрализован даже при незначительных знаниях.

Переопределение домена находится в нижней части экрана DNS форвардера. Эта возможность позволяет указать другой DNS сервер для разрешения специфического домена. Одним из примеров применения данной опции являются сети малого бизнеса с единственным внутренним сервером AD (Active Directory), как правило на базе Microsoft Small Business Server. DNS запросы для домена AD могут разрешаться с использованием внутренней функциональности Windows Server. Добавление переопределений для домена AD, указывающих на IP адрес внутреннего сервера Windows гарантирует, что эти записи будут разрешены верно для клиентов использующих pfSense в качестве DNS сервера или для самого Windows сервера. В среде AD, ваши системы всегда должны использовать ваш Windows DNS сервер в качестве основного DNS сервера. В средах с единственным Windows DNS сервером вы должны включить DNS форвардер с переопределением для вашего домена AD и использовать pfSense как вторичный DNS сервер для ваших внутренних хостов. Это гарантирует, что разрешение DNS (за исключением AD) не будет иметь единой точки отказа, и потеря одного сервера не будет означать полного отключения Интернет. Потери одного сервера в такой среде, как правило, имеют значительные последствия, но пользователи будут вас меньше донимать с решением проблемы если у них будет возможность проверить собственные ресурсы в интернете, такие как MySpace, Facebook и пр. Другое общее использование переопределения DNS заключается в разрешении внутренних доменов DNS на удалённых узлах с помощью сервера DNS на основном сайте доступном через VPN. В таких условиях обычно требуется разрешать все DNS запросы на центральном узле в целях централизованного контроля над DNS, однако некоторые организации предпочитают позволить интернет DNS с pfSense на каждом сайте и только переадресация запросов для внутренних доменов на сервере центрального DNS. Обратите внимание, что вам необходим статический маршрут для этой функции через IPsec. Смотрите раздел 13.4.4. "Трафик инициированный pfSense и IPsec" для получения большей информации.

Динамический DNS

Клиент динамического DNS в pfSense позволяет вам регистрировать IP адрес WAN интерфейса различных поставщиков сервиса динамического DNS. Это полезно когда желаете получить удалённый доступ к динамическим IP соединениям и используется, чаще всего для подключения к VPN, веб серверам или почтовым серверам.

Примечание: *Клиент работает только на первичном WAN интерфейсе. Любые интерфейсы OPT не могут использовать встроенного клиента динамического DNS. Кроме того, вы можете зарегистрировать только одно имя динамического DNS. pfSense 2.0 подерживает множество различных динамических DNS, позволяя регистрировать IP адреса WAN OPT, а так же регистрацию вашего реального публичного IP в среде где pfSense получает приватный IP для WAN и NAT апстрима.*

pfSense позволяет регистрировать девять различных провайдеров динамического DNS, и начиная с версии 1.2.3. вы можете увидеть список доступных поставщиков, нажав на выпадающий список Service type. Вы можете узнать больше о провайдерах перейдя на их сайты. Большинство провайдеров предлагает базовый уровень обслуживания на безвоздмезной основе, некоторые предлагают дополнительную функциональность за дополнительную плату. Как только вы выбрали провайдера, посетите его сайт и зарегистрируйтесь. Процедуры настройки на провайдера различны для каждого поставщика, но в большинстве случаев на сайте имеется соответствующая инструкция. После настройки на сайте провайдера вы можете настроить pfSense на соответствующего поставщика.

MX запись почтовых серверов на которые будет доставляться почта для вашего домена. Некоторые провайдеры динамического DNS позволяют вам настроить эту опцию вашего клиента. Если это возможно, введите имя хоста почтового сервера который будет получать электронную почту для вашего домена.

Включение шаблонов DNS на динамическом DNS означает, что все запросы имени хоста будут разрешаться в IP адрес с вашим DDNS именем хоста. Например, если имя хоста example.dyndns.org, включение шаблона типа *.example.dyndns.org (a.example.dyndns.org, b.example.dyndns.org) разрешается так же как

example.dyndns.org.

SNMP

Демон **Simple Network Management Protocol** [http://en.wikipedia.org/wiki/Snmp] (SNMP) позволит вам удалённо контролировать некоторые системные параметры pfSense. В зависимости от выбранного варианта, вы можете контролировать сетевой трафик, потоки, очереди pf, и основные системные параметры, такие как использование процессора, памяти и дисков. Реализация SNMP используемая в pfSense - **bsnmpd**, включающая только базовые функции управления информационной базы MIB, которые могут расширяться засчёт подгружаемых модулей. Кроме SNMP демона, есть возможность передавать ловушки SNMP серверу для определённых событий. Возможности могут варьироваться в зависимости от загруженных модулей. Например, состояние сетевого линка будет генерировать ловушку если вы загрузите модуль MIB II. Службу SNMP можно настроить перейдя на страницу **Services -> SNMP**. Самый простой способ увидеть, какие данные будут доступны для запуска snmpwalk на pfSense - осуществить доступ с другого компьютера с net-snmp или эквивалентной инсталляции. Плная информация о базе MIB выходит за рамки данной книги, но существует достаточное количество электронных и печатных изданий описывающих SNMP, а некоторые ветви MIB рассмотрены в RFC. Например Host Resources MIB определён в RFC 2790.

SNMP демон (SNMP daemon)

Данные параметры определяют каким образом будет работать демон SNMP. Для включения демона SNMP отметьте Enable. После включения данного флага вы сможете изменить прочие параметры демона.

SNMP соединения используют UDP и клиенты SNMP по умолчанию используют UDP порт 161. Этот параметр позволяет сменить порт прослушиваемый демоном. Соответственно SNMP клиент или агент должны работать на соответствующем порту.

Это текстовое поле определяет, какие строки будут возвращены при запросе расположе ния системы посредством SNMP. Вы можете следовать соглашению принятому в вашей организации. Для некоторых устройств может подойти название города или провинции, а для некоторых номер стойки и местоположение устройства.

Контактная система представлена текстовым полем, которое может быть заполнено в соответствии с вашими требованиями. Это может быть информация о имени, адресе электронной почты, номера телефонов.

В SNMP данный параметр действует как своеобразная пара логин/пароль. SNMP клиенты должны использовать эту строку при проведении опроса. Обычным значением по умолчаию является "public", поэтому вам следует рассмотреть вопрос по изменению этой строки в дополнение к ограничениям доступа SNMP сервиса в службах брандмауэра.

Ловушки SNMP (SNMP Traps)

Для уведомления демона SNMP передвать ловушки SNMP, отметьте Enable. После установки данного флага можно изменить другие параметры настройки.

Сервер ловушек это имя хоста илиIP адрес куда должны направляться SNMP ловушки.

По умолчанию, ловушки SNMP используют UDP порт 162. Если ваш приёмник ловушек SNMP настроен на другой порт, соответствующим образом измените этот параметр.

UPnP

Universal Plug and Play [http://en.wikipedia.org/wiki/Upnp] (UPnP) - сетевой сервис, позволяющий взаимодействие некоторого ПО и устройства в целях взаимной настройки при подключении к сети. В функции сервиса включается создание порта NAT форвардера и ассоциация правил брандмауэра. Сервис UPnP pfSense можно найти на странице **Services -> UPnP**, и он включает автоматические разрешения трафика для клиентских компьютеров и других устройств, например игровых консолей. Существует множество программ и систем поддерживающих UPnP, например таких как Skype, Utorrent, MIRC, различные интернет пейджеры, PlayStation 3 и Xbox 360. UPnP использует Simple Service Discovery Protocol (SSDP) для исследования сети и работает на порту UDP 1900. Демон UPnP, miniupnpd, используемый в pfSense кроме того использует порт TCP 2189. В правилах брандмауэра понадобиться разрешить доступ для данного сервиса, особенно, если вы уалили правила по умолчанию LAN-to-any, или в конфигурации моста.

Сервис UPnP представляет собой классический пример копромисса "Безопасность - Удобство". По своей природе, UPnP является небезопасным сервисом. Любая программа в сети может позволить направление любого трафика - потенциальная угроза безопасности. С другой стороны, это может быть весьма удобно для введения и поддержки порта NAT форвардера и связанных с ним правил, особенно в случаи с наличием игровых консолей. Существует много догадок и проведено много исследований в области поиска требуемых портов и настроек, но UPnP работает достаточно просто и требует минимум административного внимания. Использование сервиса в большинстве случаев черезмерно пространственно и потенциально сервис предоставляет множество услуг, которые не должны быть открыты из сети Интернет. В конфигурации сервиса UPnP присутствует контроль доступа, который позволяет управлять правами внесения изменений. Кроме встроенных элементов управления доступом, можно управлять доступом посредством правил брандмауэра. При правильной настройке, UPnP может быть более безопасным.

Конфигурация

Настройка сервиса UPnP производится на странице Services -> UPnP. Для включения сервиса установите флаг Enable UPnP. Когда вы закончите вносить любые необходимые изменения, описанные в оставшейся части данного раздела, нажмите

Save. Сервис UPnP запустится автоматически.

Интерфейсы(Interfaces)

Этот параметр позволит вам выбрать интерфейсы на которых разрешена работа сервиса UPnP. Можно выбрать более одного интерфейса путём удержания клавишы Ctrl и выборе дополнительных интерфейсов. Отмена выбора работает аналогично. Если интерфейс соединяется с другим интерфейсом, UPnP должен выбираться только для "родительского" интерфейса, а не соединямого. Например, если у вас есть OPT1 соединяемый с LAN, следует включить UPnP только на LAN.

Максимальныескорости (MaximumSpeeds)

Начиная с версии pfSense 1.2.3. вы можете установить максимальные скорости загрузки и выгрузки для портов открытых UPnP. Эти скорости задаются в kBit/sec, поэтому например для ограничения скорости загрузки в 1,5Mbit/sec, необходимо ввести 1536 в поле MaximumDownloadSpeed.

Переопределение WANадреса (Override WAN address)

По умолчанию, сервис UPnP будет настраивать порт форвардера и правила брандмауэра для WAN адреса. Эта настройка позволит вам ввести альтернативный IP адрес, например вторичный WAN адрес или общий CARP адрес.

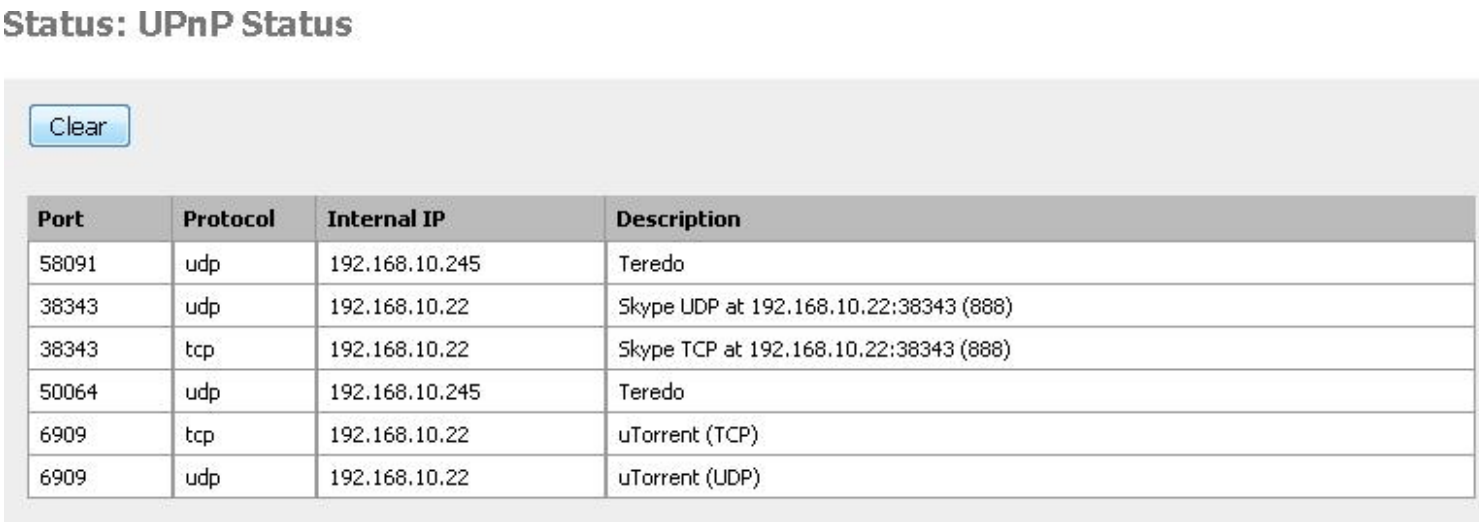
Очередь формированиятрафика(Traffic Shaping Queue)

По умолчанию, правила созданные UPnP не назначают трафик в очередь формирования. Вводя имя очереди в данное поле вы определите очередь в котрую будет попадать трафик проходящий в соответствии с правилом созданным UPnP. Выбирайте мудро, поскольку любое UPnP устройство и программа будут использовать

эту очередь. Это может быть Bittorent или игровая консоль, так что выбирайте очередь имеющую приоритет который лучше всего подходит для ожидаемого трафика.

Статус(Status)

Статус сервиса UPnP может быть найден на странице **Status -> Service**. Он показывает, состояние сервиса и позволяет остановить, запустить или перезапусть сервис. Все операции обрабатываются атоматически но могут выполняться и вручную. список текущих портов и клиентов похож на показанный на рисунке 21.3. "Экран статуса UPnP", может быть найден на странице
Status
->
UPnP
.



Port	Protocol	Internal IP	Description
58091	udp	192.168.10.245	Teredo
38343	udp	192.168.10.22	Skype UDP at 192.168.10.22:38343 (888)
38343	tcp	192.168.10.22	Skype TCP at 192.168.10.22:38343 (888)
50064	udp	192.168.10.245	Teredo
6909	tcp	192.168.10.22	uTorrent (TCP)
6909	udp	192.168.10.22	uTorrent (UDP)

Рисунок 21.3. "Экран статуса UPnP"

Когда сервис работает, он должен отображаться при просмотре сети с использованием системы поддерживающей UPnP, такой как Windows 7 или Windows Vista, как показано на рисунке 21.4. "pfSense с точки зрения Windows 7 при работе в сети". Вы можете щёлкнуть правой кнопкой на иконке маршрутизатора и нажать View device webpage для открытия WebGUI маршрутизатора в браузере по умолчанию. Если щёлкнуть правой кнопкой на маршрутизаторе и выбрать пункт Свойства, вы сможете увидеть версию pfSense и IP адрес маршрутизатора.

Рисунок 21.4. "pfSense с точки зрения Windows 7 при работе в сети"

Поиск неисправностей

Большинство проблем UPnP, как правило, связаны с мостами. В данном случае важно иметь конкретные правила брандмауэра позволяющие работу порта UDP 1900. Поскольку это многоадресный трафик, назначать следует широковещательный адрес для подсети. Обратитесь к журналу вашего брандмауэра на странице Status -> System Logs закладки Firewall, для просмотра трафика который блокируется. Обратите особое внимание на адрес назначения, поскольку он может оказаться иным чем вы ожидали. Решение проблем с игровыми приставками может быть устранено за счёт перехода на ручное конфигурирование исходящего NAT и включение статического порта (Static

Port). Смотрите раздел 7.6.2., "Статический порт" для получения большей информации.

OpenNTPD

OpenNTPD [http://www.openntpd.org/] - сервис предоставлемый демоном Network Time Protocol

[http://en.wikipedia.org/wiki/Network_Time_Protocol] (NTP), который принимает запросы от клиентов и даёт возможность синхронизировать локальные часы с работой pfSense. Запуск локального сервера NTP и использовании его клиентами позволяет снизить нагрузку на сервера времени нижнего стратума и позволит гарантировать, что ваши клиенты получат доступ к серверу времени. Прежде чем делегировать эту задачу системе pfSense, разумно убедиться, что её системные часы работают нормально. OpenNTPD сервер имеет небольшое количество настроек, которые доступны на странице
Services
->
OpenNTPD
. Сначала отметьте флаг Enable, выберите интерфейсы на которых сервис будет слушать входящие запросы и нажмите кнопку Save. Может быть выбран более чем один интерфейс путём удерживания клавиши Ctrl и щёлчком на дополнительных интерфейсах. Отмена выбора дополнительных интерфейсов работает аналогично. Сервис запускается автоматически, однако, существует некоторая задержка между запуском и началом обслуживания NTP-запросов. Журналы OpenNTPD находятся на странице
Status
->
System
Logs
, на закладке OpenNTPD. Сервис имеет небольшие журналы и если никаких проблем нет, записи генерироваться не будут.

Wake on Lan (Пробуждение по сети).

Wake on LAN [http://en.wikipedia.org/wiki/Wake_on_lan] (WOL) доступный на странице Services -> Wake on LAN может быть использован для пробуждения компьютеров находящихся в выключенном состоянии путём передачи им специальных "магических пакетов" (Magic Packets). Сетевая плата компьютера-клиента должна поддерживать режим WOL и должна быть правильно настроена. Обычно существую настройки BIOS позволяющие включить WOL, а для не интегрированных адаптеров кроме того требуется специальный кабель WOL связывающий сетевой адаптер с материнской платой. WOL имеет множество потенциальных возможностей применения. Как правило, рабочие станции и сервера постоянно находятся в рабочем состоянии из-за специфики предоставляемых ими услуг, файлов, общих принтеров или просто для удобства использования. WOL позволяет им оставаться включёнными, одновременно позволяя экономить энергию. Если требуется какой либо сервис, система может быть разбужена когда это необходимо. Другим вариантом может стать случай удалённого доступа к системе выключенной пользователем. WOL не обеспечивает собственной реализации безопасности. Любая система 2-го сетевого уровня может передать WOL пакет, который будет принят и исполнен. Лучший вариант, настроить WOL только на тех клиентах где его использование целесообразно, и отключить в BIOS на всех остальных. Существует несколько производителей, которые реализуют расширение безопасности WOL, однако универсального решения не существует.

Чтобы пробудить одну машину, следует выбрать интерфейс, посредством которого она может быть достигнута, ввести MAC адрес системы в формате XX:XX:XX:XX:XX:XX. После нажатия Send, pfSense будет передавать магические пакеты WOL на выбранный интерфейс, и если всё нормально, указанная система должна проснуться. Имейте в виду, что системе требуется некоторое время для загрузки.

Для хранения MAC адресов, в целях последующего использования, нажмите [+] на списке сохранённых MAC адресов и увидите пустой экран редактирования. Выберите интерфейс через который может быть достигнут хост и введите MAC адрес в формате XX:XX:XX:XX:XX:XX. Кроме того, вы можете ввести произвольное описание хоста. Нажмите кнопку Save для сохранения и вы вернётесь на главную страницу WOL. Ваша новая запись должна появиться в нижней части страницы. Управление записями аналогично другим задачам pfSense: нажмите [e] для редактирования и [x] для удаления записи.

Чтобы отправить магический пакет WOL системе, которая была сохранена, нажмите не её MAC адрес в списке сохранённых систем. Вы попадёте на страницу WOL с уже заполненными параметрами пробуждаемой машины. нажмите кнопку Send для отправки магического пакета.

На странице WOL есть кнопка [w] которая используется для отправки магических пакетов WOL всем хранимым системам. Нажмите её и запросы будут переданы без каких либо дополнительных действий.

Для отправки пакета WOL из окна просмотра DHCP аренды, перейдите на страницу Diagnostics -> DHCP leases, нажмите MAC адрес в списке аренд. Ссылка WOL существует только у активных систем, со статусом offline. Вы попадёте на страницу WOL с заполненными данными системы. Нажмите кнопку Send для отправки магического пакета.

Вы можете скопировать MAC адрес для новой записи сопоставления WOL при просмотре DHCP аренды на экране Diagnostics -> DHCP leases. Нажмите кнопку [w] в конце строки и вы попадёте на предварительно заполненный экран редактирования WOL. Добавьте описание и нажмите кнопку Save.

Сервер PPPoE

pfSense может выступать в качестве PPPoE сервера и производить аутентификацию PPPoE соединений от клиентов на локальном интерфейсе, выступая в качестве концентратора доступа. Эта возможность может быть использована для аутентификации пользователей перед получением доступа к сети или иного контроля требующего аутентификации. Конфигураация PPPoE производится на странице Services -> PPPoE Server. Как вы можете убедится, конфигурация очень похожа на конфигурацию PPTP VPN сервера (Глава 14 "PPTP VPN"). Для активации данной функциональности, отметьте флаг Enable PPPoE server. Затем выберите интерфейс, на котором будет работать данный сервис. Установите маску подсети (Subnet Mask), относящуюся к клиентам PPPoE и количество пользователей PPPoE (Number of PPPoE

Users to allow). Теперь, введите адрес сервера (Server Address) который является IP адресом который pfSense будет передавать клиентам PPPoE для использования в качестве шлюза. Введите IP адрес в поле Remote Address Range и совместно с маской подсети они будут использоваться для определения сети клиентов PPPoE. Остальные опции предназначены для аутентификации посредством RADIUS. Если вы хотите передавать запросы на аутентификацию на сервер RADIUS, заполните информацию в нижней части экрана. если вместо этого будет использована локальная аутентификация, нажмите Save setting и щёлкните на закладке Users для добавления локальных пользователей. Нажмите IP address для добавления пользователя и заполните имя пользователя и пароль. Для получения дополнительной информации смотрите раздел 24.1. "Аутентификация RADIUS с использованием Windows Server".??

оглавление

{jcomments on}