Автор: Administrator
19.10.10 14:08 - Последнее обновление 03.11.10 16:13

Установка и настройка Wi-FI HOT-SPOT

системы на примере программного роутера PfSense 2.0.

В этой серии статей я расскажу - как имея «на руках» компьютерное железо не самой последней конфигурации в виде системного блока, точку доступа, диск с дистрибутивом PfSense 2.0 и немного терпения, в кратчайшие сроки организовать и настроитьhot-spot систему по раздачи Wi-Fi интернета в какой-нибудь небольшой организации или кафе.

Для начала определимся с «железом», а именно с аппаратной частью системного блока и точкой доступа. Разработчики дистрибутива рекомендуют следующие минимальные требования к железу, чтобы все «завелось»:

CPU - 100 MHz Pentium

RAM - 128 MB

Requirements specific to individual platforms follow.

Live CD

CD-ROM drive

USB flash drive or floppy drive to hold configuration file

Hard drive installation

CD-ROM for initial installation

1 GB hard drive

Embedded

128 MB Compact Flash card

Serial port for console

Сами понимаете эта конфигурация более чем скромная и такое железо нужно еще поискать, поэтому системный блок с конфигурацией четырехлетней давности будет «просто летать».

Для тестов я взял системный блок со следующими параметрами:

CPU AMD Athlon(tm) XP 1800+

RAM 512Mb

HDD 10Gb

2xLan

Теперь на счет точки доступа: здесь все схоже — минимум подойдет любая точка начиная от самых бюджетных, но и сами понимаете с некоторыми ограничениями в виде мощности антенны(1-2dbi) и пропускной способности. Вообще здесь лучше не экономить и если сегодня точка справляется с 5-10 клиентами в прямой видимости в радиусе 20метров, то завтра если вам захочется расширить охват территории где на пути сигнала от точки будут попадаться препятствия, а клиентов будет в разы больше, нужно взять решение по дороже, ориентированное минимум на малый бизнес и усилением антенны в 5dbi. Возможен и другой вариант, если нужно покрыть площадь из 2-4 помещений, а тратить время и деньги на замеры уровня сигнала, места расположения точки и ее покупку нет желания, то можно приобрести по точке из бюджетного сегмента

в каждое из помещений, а соединить их с сервером Hotspot с помощью свитча. SSID каждой из точек лучше назначить такой, который бы ассоциировался с местом ее расположения(например: banket_zal, bar и т.д.).

Подробно установку Pfsense я описывать не стану, с ней все интуитивно понятно, а отправлю вас к подробному скринкасту:

http://thin.kiev.ua/index.php?option=com_content&view=article&id=246:inst&catid=50:pfsense&Itemid=81

http://forum.pfsense.org/index.php/topic,7356.0.html

Если же возникнут вопросы по установке, то добро пожаловать в комментарии, обязательно подскажу.

Итак после инсталляции Pfsense мы имеем два сетевых интерфейса — WAN который смотрит на провайдера, ADSL модем, в другой маршрутизатор и т.д. И принимает входящий интернет трафик, а так-же LAN интерфейс, который и будет раздавать интернет трафик нашим клиентам по средсвам подключенной к нему точки доступа.

Подключаемся с помощью патчкорда к интерфейсу LAN и в адресной строке вводим адрес веб-панели маршрутизатора (по умолчанию 192.168.1.1) и попадаем в админ-панель.(логин по умолчанию -admin, пароль – pfsense) Запустится мастер первичной настройки где нужно задать все необходимые параметры, которые "спросит мастер".

Итак, мы должы были получить работоспособный шлюз, который "раздает" трафик на интерфейс LAN к которому можно уже подключить через свитч дюжену ПК или точку доступа и вполне комфортно пользоваться услугами маршрутизатора, но наша цель не много шире, а именно – организация hot-spot с раздачей интернет трафика с учетом по времени беспроводным клиентам путем выдачи ваучеров(кодов доступа).

Наши пользователи будут получать доступ к интернету через страницу Captive Portal, где они будут вводить код доступа и собственно получать этот доступ лимитированный по времени. Для настройки "портала" переходим в веб-интерфейсе по следующему пути **Services- Captive Portal**. Для включения страницы аутентификации отмечаем галчкой **E nable captive portal**
, интерфейс выбираем
LAN
.

Пройдемся по настройкам Captive Portal:

Для начала его необходимо включить, установив галочку в положение enable и применить к сетевому интерфейсу, на котором "портал" будет запущен, в нашем случае это LAN.

***Maximum concurrent connections* –** максимальное число клиентов Captive Portal, которые могут получить доступ к странице аутентификации одновременно с одного IP адреса(по умолчанию четыре соединения, максимально 16 соединений). Не путать общеее число возможных подключений через Captive Portal с возможностью одновременной аутентификации через страницу, как в данном случае. Я не изменял этот параметр и оставил его по умолчанию.

***Idle timeout* –** клиенты будут отключены от шлюза в результате бездействия после времени указанного в этом параметре. Чем поезен это параметр для клиента – после отключения от шлюза не используемое время клиента замораживается на отметке оставшегося. Здесь имеет смыл поиграться с нужным параметром, но нет смысла ставить его больше 30минут. Пустое поле свидетельствует об отключении этого параметра.(после отключения пользователя по тайм-ауту бездействия пользователю будет необходимо ввести свой ваучер(код доступа) на странице аутентификации Captive Portal повторно)

***Hard timeout* —** клиенты отключаются от шлюза принудительно, не зависимо бездействуют они или находятся «в сети», чтобы не включать этот параметр оставьте это поле пустым.

Pass-through credits allowed per MAC address — этот параметр позволяет проходить аутентификацию определенное количество раз на основе только MAC адреса. После истечения указанного количества аутентификаций, клиент сможет подключиться только на основе валидных аутентификационных данных. Для эффективного использования данного параметра рекомендуется использовать в связке с параметрами hard timeout и/или idle timeout. (ввести число подключений на MAC адрес клиента, 0 или пусто означают, что параметр не задан)

Waiting period to restore pass-through credits — в этом параметре задается время после которого счетчик подключений из предыдущего параметра восстанавливается, этот параметр следует выставлять отличным от 0 если Pass-through credits allowed per MAC address отличен от 0.

Reset waiting period on attempted access - Enable waiting period reset on attempted access — если включить данный параметр, то по исчерпании количества подключений сквозной аутентификации на основе MAC(см. Выше), счетчик сбрасывается не выждав установленного времени в параметре Waiting period to restore pass-through credits.

Logout popup window — включить или отключить всплывающее окно ручного включения или отключения своей сессии для клиента.(клиент сам может(не полагаясь на шлюз) прервать или возобновить свою сессию) — может блокироваться браузером клиента.

Redirection URL — вписав в это поле URL нужного ресурса, клиенты после удачного логина будут автоматически перенаправлены на этот адрес, не зависимо от того на какой адрес они пытались попасть изначально.

Concurrent user logins - Disable concurrent logins активация данного параметра позволяет контролировать подключаемых пользователей. Только последняя сессия по одному ваучеру будет активной, все предыдущие сессии по этому же ваучеру будут прерваны..

MAC filtering - Disable MAC filtering установка этого параметра отключает фильтрацию по MAC адресам. Это значит, что не будет отслеживаться неизменность MAC адрес клиентов с момента первого логина. Если эта опция включена, RADIUS MAC-аутентификация не может быть использована. Хоть и подделка MAC адреса достаточно не тривиальная задача, лучше эту опцию не включать, если конечно клиенты находятся в одной подсети со шлюзом(PfSense).

Pass-through MAC Auto Entry **:**

Enable Pass-through MAC automatic additions – Если задействовать эту опцию запись MAC адреса клиента успешно аутентифицированного автоматически добавляется в доверенные. Если MAC адрес этого клиента останется не измененным, ему не придется каждый раз подключаясь проходить аутентификацию. Удалить эту запись можно из административной панели во вкладке Pass-through MAC или отправив POST запрос из другой системы. Если эта опция включена, RADIUS MAC-аутентификация не может быть использована. Кроме того окно выхода (если вы установили параметр *Logout popup window)* отображено не будет.

Enable Pass-through MAC automatic addition with username – Если задействовать эту опцию, данные (имя и MAC пользователя) будут автоматически сохранены на время действия ваучера, чтобы не приходилось вводить код доступа повторно. Записи удаляются во вкладке Pass-through MAC или путем отправки POST запроса из другой системы.

Per-user bandwidth restriction — задействовав эту опцию опцию, можно регулировать полосу пропускания каждого клиента, поставив ограничения на скорость скачки и закачки. В настройках RADIUS сервера можно переопределить параметры по умолчанию. Чтобы отключить ограничения, либо снимите галочку в поле включения

параметра, либо выставите значения 0 или «пусто» в полях установки скорости полосы пропускания. В большинстве случаев для более или менее комфортного веб-серфинга достаточно выставить ограничения 128-256кбит(все зависит от общей полосы предоставляемой вам провайдером интернета).

Authentication **–** здесь как не сложно догадаться выбирается тип аутентификации, всего их три: No Authentication(без аутентификации), Local User Manager (аутентификация основанная на базе локальных пользователей), RADIUS Authentication (аутентификация на сервере аутентификации RADIUS). В нашем случае следует выбрать Local User Manager, поэтому отмечаем этот тип.(Все настройки связанные с аутентификацией на RADIUS сервере пропускаем).

HTTPS login — параметр отвечающий за шифрование передаваемой серверу аутентификационной информации(в нашем случае код ваучера). В самом простом варианте этот параметр можно оставить пустым, но коды доступа будут «летать» в открытом виде, а можно и обезопасить соединение передачи аутентификационной информации активировав данный параметр. Единственным недостатком, на мой взгляд, включения шифрования будет «паника» браузера клиента на сертификат сервера не подписанный авторизованными центрами сертификации. Здесь приходит в голову три варианта:

-

Настроить точку доступа как открытую и не включать параметр HTTPS login, недостатками данной конфигурации будет отсутствие всяческого шифрования клиентского трафика и постоянная «сигнализация» ОС клиента ссылающаяся на не безопасную Wi-Fi сеть, кого то из клиентов это как минимум может насторожить.

-

Включить уровень защиты на точке доступа WPA2 с шифрованием трафика по алгоритму AES. HTTPS login можно не задействовать. Недостатком данного метода может быть настройка клиентом до аутентификации на странице hotspot wi-fi адаптера на работу с WPA2. И еще одним недостатком данного метода может быть желательная периодичность смены ключа шифрования(PSK) точки доступа.

-

Оставить точку доступа открытой, но задействовать параметр HTTPS login, недостатком этого метода по мимо «сигнализации» ОС по поводу не безопасной сети Wi-Fi будет еще «сигнализация» по поводу само подписанного сертификата HotSpot.

Самым щадящим для клиента, на мой взгляд, будет второй метод, а если вы все таки активируете параметр HTTPS login, то вам нужно будет сгенерировать самоподписанный сертификат, заполнив поля ниже. Сгенерировать сертификат можно на странице Cert Manager.

Portal page contents – здесь вы можете загрузить альтернативную страницу аутентификации разработанную под вашу компанию. Самую простую страницу можно сделать по аналогии:

```
<form method="post" action="$PORTAL_ACTION$">

<html>
<head>
<title>pfSense captive portal</title>
</head>
<body>
<center>
<h2>Портал Аутентификации</h2>
Добро пожаловать в Wi-Fi На этой странице введите свой код доступа, чтобы начать пользоваться сетью INTERNET.
<p>
 <input name="auth_voucher" type="text">
 <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
 <input name="accept" type="submit" value="Continue">
</form>
```

Authentication error page contents - в этой форме загружаются собственные HTML / PHP страницы, которые будут выведены клиенту при неудачной аутентификации. В эти станицы вы также можете включить "$ PORTAL_MESSAGE $", в результате чего все ошибки RADIUS сервера, если таковые имеются также будут отображены.

Logout page contents – если вы активировали параметр *Logout popup window* для всплывающей страници отвечающей за ручное отключение от hotspot, здесь эту страницу можно загрузить.

Применяем параметры, нажав SAVE.

Вкладка Pass-through MAC отображает данные пользователей, которым разрешен доступ «мимо» страници аутентификации. Здесь можно задать MAC адрес компьютера и ограничение полосы пропускания для данного MAC. Можно добавлять, редактировать и удалять как вручную, так и с помощью параметров указанных в предыдущей вкладке Enable Pass-through MAC automatic additions, Enable Pass-through MAC automatic addition with username. Поскольку доступ по MAC достаточно легко обойти, к этой вкладке и добавлению клиентов которым разрешен доступ автоматом на основе их MAC нужно относиться с осторожностью.

Вкладка allowed IP addresses позволяет добавлять правила для IP адресов к которым и от которых разрешены соединения минуя страницу аутентификации. Это может быть применено в отношении Web сервера на котором хранятся изображения для страници аутентификации или DNS-сервера из другой подсети.

any x.x.x.x All Все соединения до IP-адреса разрешены

x.x.x.x any Al Все соединения с IP-адреса разрешены

All connections Все соединения с и до IP-адреса разрешены

Вкладка Vouchers:

Первым делом включаем режим ваучеров, отметив пункт Enable Vouchers.

Voucher Rolls — «Виртуальные рулоны» ваучеров(кодов доступа) здесь мы позже будем выписывать коды доступа, пока оставляем этот пункт не тронутым.

Voucher public key, Voucher private key — в эти поля нужно вставить или сгенерировать автоматически (нажав на ссылку
Generate
new key расположенную под каждом из полей) RSA публичный и приватные ключи в формате PEM, на основе этих ключей будут шифроваться и дешифроваться ваучеры.

Character set - символы используемые при генерации ваучеров, не рекомендуется использовать символы 0/O и I/1.

# of Roll Bits — объем в битах для хранения каждого рулона. Допустимый диапазон: 1 .. 31. Сумма Roll+Ticket+Checksum должна быть на один бит меньше, чем размер ключа RSA. (мое значение 16)

# of Ticket Bits — объем в битах для хранения каждого ваучера. Допустимый диапазон: 1 .. 16. Использование 16 бит позволяет создать рулон до 65535 ваучеров. Битовый массив, хранящиеся в оперативной памяти и в конфигурации, используется для определения, используемых ваучеров. Массив для 65535 ваучеров требует 8 Кб оперативной памяти. (у меня здесь стоит значение 10).

# of Checksum Bits — зарезервированное место в каждом ваучере для хранения контрольных сумм всего рулона и кода доступа. Допустимый диапазон 0 .. 31. (мой вариант 5)

Magic Number — число сохраняемое в каждом ваучере. Проверяется в ходе проверки ваучера. Проверка числа зависит от количества свободного места в битах используемых на хранения информации о рулоне, коде доступа и контрольной сумме, если свободного места не осталось, то использование и проверка Magic Number осуществляться не будет.

Save Interval — список активных и используемых ваучеров сохраняется в конфигурации каждые X минут на случай перебоя в подачи электроэнергии. При отсутствии новых активаций сохранения не происходят. Вы можете ввести 0, чтобы никогда не создавать XML конфиг.

Invalid Voucher Message – сообщение об ошибке отображается при активации недействительного ваучера ($ PORTAL_MESSAGE $).

Expired Voucher Message — сообщение об ошибке при активации истекшего ваучера у которого закончился срок действия.

Подраздел Voucher database synchronization в контексте данной статьи я рассматривать не буду, хотя здесь все ясно и понятно, он отвечает за синхронизацию с удаленной базой данных с ваучерами.

Жмем SAVE и переходим к генерации «рулонов»(Roll) с ваучерами. Для этого в пункте Voucher Rolls все той же вкладки Vouchers нужно нажать кнопку «+»(add Voucher) и перейти непосредственно к созданию самих рулонов с ваучерами. Пройдемся по форме заполнения информацией для создания кодов доступа:

Roll# - здесь вводится номер рулона с ваучерами, допустимое значение 0 .. 65535.

Minutes per Ticket — время в минутах действия каждого ваучера в рулоне, отсчет начинается с момента активации ваучера.

Count — количество ваучеров в рулоне. Изменение этого числа в уже созданном рулоне приведет к тому, что все использованные ваучеры будут активны снова и готовы к активации.

Comment — комментарии к созданному списку ваучеров.

Заполняем все вышеназванные поля и жмем SAVE.

Теперь на вкладке Vouchers в пункте Voucher Rolls мы можем видеть информационную таблицу о созданных списках(рулонах) с ваучерами. Чтобы сгенерировать и скачать список на компьютер для последующей распечатки и нарезки кодов доступа, жмем кнопку с буквой «i» справа от нужного информационного поля в таблице и сохраняем на компьютер.

Вкладка File Manager:

Любые файлы загруженные через этот файловый менеджер будут доступны в корневом каталоге портала аутентификации HTTP (S) сервера. Вы можете включать их прямо в html код страницы аутентификации. Например с помощью файлового менеджера вы загрузили изображение 'captiveportal-test.jpg', теперь вы можете включить его путем вставки в html код следующим образом:

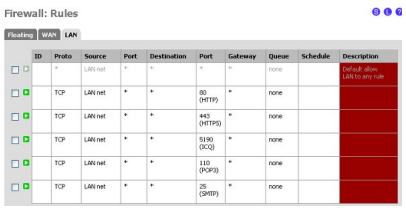
<img src="captiveportal-test.jpg" width=... height=...>

Кроме того вы можете загружать php файлы и исполнять их используя подобный код в странице аутентификации:

Acceptable usage policy

Максимальный размер для всех файлов **1,00 МБ.**

С настройками Captive Portal мы разобрались, перейдем к конфигурации **firewall (Firewall – Rules – LAN)**
, здесь все просто — разрешаем доступ из LAN по стандартным портам, все остальное запрещаем. На скрине ниже примерная конфигурация, которая в большинстве случаев подойдет всем:



В заключении рассмотрим еще одну вкладку Pfsense относящуюся к captive portal – Status- Captive Portal. Вкладка носит информативный характер, бегло пробежимся по информационным параметрам отображаемым здесь.

Active Users – пользователи, которые в данный момент находятся online, здесь мы видим IP адрес пользователя, MAC адрес сетевой карты через которую подключен пользователь, код ваучера используемый данным пользователем и дата активирования пользовательской сессии.

Active Vouchers – список ваучеров активных в данный момент времени. По каждому из ваучеров можно получить следующую информацию — код активного ваучера, номер рулона к которому относится данный ваучер, дата активации ваучера, время через которое истекает срок действия ваучера, дата и время истечения срока действия кода доступа.

Voucher Rolls – список рулонов с подробной информацией о каждом. Здесь мы видим — номер рулона, срок действия каждого ваучера в этом рулоне, количество ваучеров в рулоне, комментарии к рулону, использовано ваучеров, активно в данный момент ваучеров из этого рулона, готовых к активации(не использованных).

Test Vouchers - Введите несколько ваучеров через пробел или символ новой строки. После нажатия на Submit можно видеть оставшееся время по каждому из введенных ваучеров, если таковое имеется.

На этом все, если я что-то упустил, есть вопросы или замечания, прошу в комментарии, но и не забываем, что я описывал настройку Pfsense 2.0 Betta4 , а betta, как известно еще не стабильная версия.

Автор: Э_L_A_Y http://bruteforcer.ru

оригинал:
1
2
3

вся статья: тут

тема на форуме: тут

{jcomments on}