Глава 19 Каптивный портал

Функциональность pfSense называемая каптивным порталом (Captive Portal) позволяет создать публичную сеть на одном из интерфейсов брандмауэра, т.е. даёт возможность реализовать общественную точку беспроводного доступа - хотспот или зону публичного доступа. Первоначально, пользователь попадает на web-страницу с которой он может получить доступ в интернет после нажатия какой либо кнопки или после прохождения аутентификации. Наиболее популярно использование данного функционала в качестве hot spot или как дополнительная аутентификация для разрешения использования клиента беспроводного доступа к внутренней сети. Функционал может использоваться и с проводными клиентами, если это необходимо.

19.1. Ограничения

Реализация каптивного портала в pfSense имеет некоторые ограничения. В данном разделе мы рассмотрим эти ограничения и общие моменты работы.

19.1.1. Может работать только на одном интерфейсе.

Вы можете использовать каптивный портал только на одном интерфейсе вашего брандмауэра. Для сред где множество IP подсетей требуют функционал каптивного портала, вам необходимо использовать маршрутизатор внутри каптивного портала установленый как показано на рисунке 19.1. "Каптивный портал на множестве подсетей."

19.1.2 Отсутствует возможность обратного портала

Использование обратного портала, требующего аутентификации для трафика входящего в вашу сеть из интернет НЕ ВОЗМОЖНО.

19.2. Конфигурация портала без аутентификации

Для создания простого портала, без аутентификации, всё что вам необходимо - установить флаг [Enable captive portal], выбрать интерфейс и загрузить HTML страницу с содержимым вашего портала как описано в разделе 19.5.12 "Содержимое страницы портала". По желанию, вы можете указать дополнительные опции конфигурации как указано в разделе 19.5 "Опции конфигурации".

19.3. Конфигурация портала с использованием локальной аутентификации

Для установки портала с локальной аутентификацией, отметьте флаг [Enable captive portal], выберите интерфейс, выберите локальную аутентификацию, и загрузите HTML страницу с содержимым вашего портала, как описано в разделе 19.5.12, "Содержимое страницы портала". Дополнительные опции конфигурации детально описаны в разделе 19.5 "Опции конфигурации". Теперь сконфигуруйте ваших локальных пользователей на закладке Users страницы Services >> Captive Portal.

19.4. Конфигурация портала с использованием RADIUS-аутентификации

Для установки портала с использованием RADIUS-аутентификации, сначала сконфигурируйте ваш RADIUS сервер, затем следуйте тем же процедурам, которые использовались при установки портала с локальной аутентификацией, заполняя соответствующую информацию для вашего RADIUS-сервера. Следующий раздел рассматривает информацию по опциям конфигурирования .

19.5. Опции конфигурирования

Этот раздел описывает каждую из опций конфигурирования каптивного портала.

19.5.1. Интерфейс

Здесь вы выбираете интерфейс на котором запускается каптивный портал. Учтите, что в качестве интерфейсов НЕ МОГУТ использоваться интерфейс моста и любые WAN

или OPT WAN интерфейсы.

19.5.2. Максимальное число параллельных соединений (Maximum concurrent connections)

Это поле определяет максимальное число параллельных соединений на IP адрес. По умолчанию задано значение 4, которое будет достаточным для большинства сред. Данное ограничение существует для предотвращения захвата одним хостом всех ресурсов брандмауэра, намеренно или неумышленно. Одним из примеров такой проблемы может стать хост заражённый вирусом червём. Тысячи подключений заставляют многократно генерировать страницу портала если хост уже не аутентифицирован, что приведёт к мощной загрузке вашей системы.

19.5.3. Таймаут неактивности (Idle timeout)

Если вы хотите отключать неактивных пользователей вам следует заполнить данное поле. Пользователи будут иметь возможность немедленного входа.

19.5.4. Жёсткий таймаут (Hard timeout)

Чтобы форсировать выход пользователя через определённый период времени введите значение жёсткой блокировки времени. Вы должны ввести значение жёсткого таймаута, таймаута неактивности или оба значения для гарантированного удаления сеансов не вышедших пользователей. Пользователи смогут немедленно использовать обратный вход после истечения жёсткого таймаута, при условии, что их мандатные данные всё ещё действительны (для локальных акаунтов не истёкших, а для RADIUS аутентификации - пользователь может подтвердить подлинность на RADIUS-сервере).

19.5.5. Всплывающее окно выхода из системы (Logout popup window)

Отметьте этот флаг для включения всплывающего окна выхода. К сожалению, поскольку большинство браузеров блокирует всплывающие окна, данная функция может не работать у большинства пользователей, если вы не администрируете их компьютеры и может быть заблокирована.

19.5.6. Перенаправление URL (Redirection URL)

Если вы вводите в это поле URL, после аутентификации или входа через портал, пользователи будут автоматически перенаправлены к данному URL, а не туда куда они пытались обратится первоначально. Если поле оставить пустым перенаправление работать не будет.

19.5.7. Параллелльный вход пользователей (Concurrent user logins)

Если данный флаг отмечен, разрешается только один вход с одной учётной записью пользователя. Все попытки нового входа с той же учётной записью будут отброшены.

19.5.8. Фильтрация MAC (MAC filtering)

Эта опция позволяет использовать по умолчанию фильтрацию MAC. Это необходимо в случае множественных подсетей за маршрутизатором использующим портал, как показано на рисунке 19.1. "Каптивный портал для множества подсетей", поскольку все пользователи за маршрутизатором отображаются MAC адресами.

19.5.9. Аутентификация

Данный раздел описывает конфигурирование системы аутентификации, если это необходимо. Если вы выбираете [No authentication] (без аутентификации), пользователям досточно пройти на страницу портала. Если требуется аутентификация, вы можете использовать локальное управление пользователями или аутентификацию с помощью RADIUS. Конфигурирование локальных пользователей производится на закладке Users страницы Services >> Captive Portal. Пользователи RADIUS определяются на RADIUS-сервере.

Для сетевой инфраструктуры использующей Microsoft Active Directory, RADIUS может использоваться для аутентификации пользователей каптивного портала из вашего AD используя Microsoft IAS. Более подробно данная процедура описана в разделе 24.1. "RADIUS аутентификация с Windows Server". Могут использоваться и другие RADIUS-сервера. Управление аккаунтами RADIUS может быть включено для передачи информации для каждого пользователя RADIUS-сервера. Вам следует обратится к руководству по вашему RADIUS серверу для получения большего объёма информации.

19.5.10. HTTPS логин (HTTPS login)

Отметьте этот флаг при использовании HTTPS для страницы портала. Если вы это сделали вам необходимо ввести сертификаты и личные ключи.

19.5.11. HTTPS имя сервера (HTTPS server name)

Данное поле - место где вы определяете полное имя домена (имя хоста+домен) для использования HTTPS. Это необходимо для соответствия общего имени (Common Name - CN) вашего сертификата, с целью предотвращения получения пользователями ошибок в браузере.

19.5.12. Содержимое страницы портала

Здесь описана структура HTML страницы вашего портала, которую увидят пользователи при попытке выхода в интернет и прохождением аутентификации или без оной.

19.5.12.1. Страница портала без аутентификации

Портальная HTML страница не использующая аутентификация формируется следующим образом:

```
<html>
<head>
<title>Welcome to our portal</title>
</head>
<body>
<p>Welcome to our portal</p>
<p>Click Continue to access the Internet</p>
<form method="post" action="$PORTAL_ACTION$">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<input name="accept" type="submit" value="Continue">
</form>
</body>
</html>
```

19.5.12.2. Страница портала с аутентификацией

Структура страницы портала с аутентификацией

```
<html>
<head>
<title>Welcome to our portal</title>
</head>
<body>
<p>Welcome to our portal</p>
<p>Enter your username and password and click Login to access the Internet</<form method="post" action="$PORTAL_ACTION$">
<input name="auth_user" type="text">
<input name="auth_pass" type="password">
```

```
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<input name="accept" type="submit" value="Login">
</form>
</body>
</html>
```

19.5.13. Содержимое страницы ошибки аутентификации

Здесь вы можете загрузить HTML страницу которая будет отображаться в случае ошибки аутентификации. Ошибка аутентификации происходит в том случае, если пользователь вводит неверное имя или пароль, либо, в случае RADIUS аутентификации потенциально недостижимый RADIUS-сервер.

19.6. Диагностика каптивного портала

Данный раздел содержит информацию по устранению общих ошибок в работе каптивного портала.

19.6.1. Ошибки аутентификации

Ошибки аутентификации - обычно результат ошибки пользователей, вводящих неверные логины и/или пароли. В случае использования RADIUS аутентификации ошибки могут происходить из-за проблем связи с вашим RADIUS-сервером или проблем возникших на самом RADIUS-сервере. Проверьте журналы RADIUS-сервера для определения отказов доступа, и устраните проблемы связи брандмауэра с RADIUS-сервером.

19.6.2. Не загружается страница портала или любая другая страница.

По нашим данным это бывает при использовании каптивного портала на VLAN, когда родительский интерфейс VLAN так же ассоциируется с другим интерфейсом pfSense. Например, если vlan0 - VLAN 10 на fxp1, вы не можете ассоциировать fxp1 с любым другим интерфейсом, его нужно оставлять неиспользованным. Для всех случаев - это рекомендуемая конфигурация, и одна из причин разумно следовать советам.