Построение защищенной беспроводной сети IEEE 802.11 (Wi-Fi) с использованием SoftPI RADIUS

Существует несколько технологий безопасности беспроводной сети, поддерживаемых практически всеми точками доступа:

- WEP;
- WPA Personal/Enterprise;
- WPA2 Personal/Enterprise.

В настоящий момент наиболее надежная защита сети достигается при использовании технологии WPA2 Enterprise. Рассмотрим настройки SoftPI Radius сервера при работе с точками доступа, работающими по технологии WPA2 Enterprise. В таком варианте беспроводная точка доступа будет блокировать все подключения к беспроводной сети до тех пор, пока вводимые пользователем имя и пароль не пройдут проверку на сервере аутентификации. Если пользователя нет в базе данных RADIUS сервера, то он не сможет подключиться к беспроводной сети. Дополнительно при использовании сертификатов осуществляется взаимная аутентификация клиентов и сервера, что исключает возможность создания работающих «ложных» точек доступа.

Для работы данной схемы аутентификации необходима настройка следующих компонентов:

- В качестве RADIUS сервера используем сервер SoftPI RADIUS.
- Точка доступа 802.11 с поддержкой WPA2 Enterprise.
- Клиентский компьютер.

Настройка сервера SoftPI RADIUS

Сервер SoftPI RADIUS выполняет проверку пользователей, подключающихся к точке доступа (аутентификация), проверяет, имеет ли право данный пользователь подключаться к точке доступа в текущий момент (авторизация), и ведет учет всех сессий пользователей (аккаунтинг).

Первым делом нужно в "Консоли управления RADIUS" сервера настроить параметры сервер доступа. Сервером доступа в данном случае будет точка доступа Wi-Fi. Необходимо ввести IP адрес точки доступа и общий секрет. Общий секрет – это пароль, используемый при обмене данными между сервером RADIUS и точкой доступа. Использование данного пароля исключает возможность появления неавторизованной точки доступа. RADIUS-сервер будет игнорировать все запросы от сервера доступа, если ему неизвестен IP-адрес или общий секрет сервера. Пример добавления сервера доступа приведен на рисунке 1.

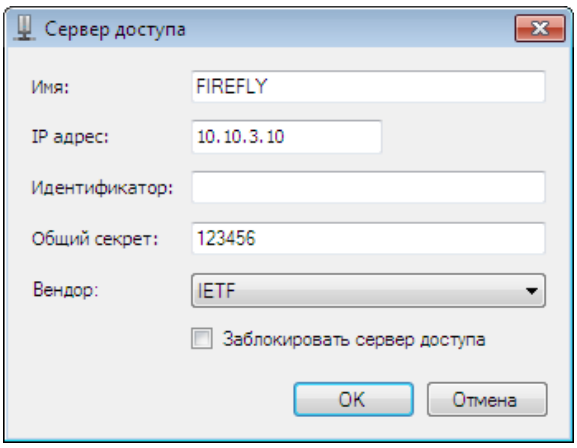

Рисунок 1

Далее необходимо создать одного или нескольких пользователей, которые будут иметь право подключаться к точке доступа. Для добавления пользователя необходимо использовать режим "Консоли настройки RADIUS-сервера": "Пользователи/Группы" → "Пользователи". Для пользователя обязательно следует указать имя пользователя и пароль. Также можно указать группу атрибутов, разрешенное время входа, и ряд других параметров.

Окно добавления пользователя приведено на рисунке 2.

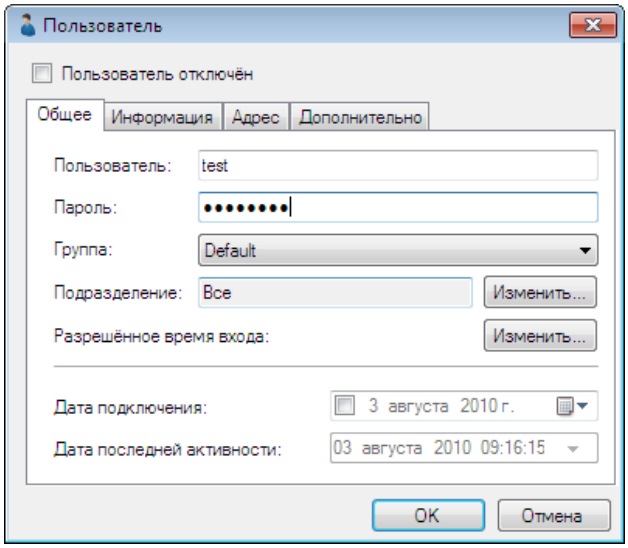

Рисунок 2

После создания пользователя при необходимости задайте атрибуты. Атрибуты, отправляемые авторизованному клиенту, необходимо отмечать типом "Отправлять в Access-Accept".

Для задания выдаваемого пользователю IP адреса можно добавить пользователю атрибут Framed-IP-Address и в качестве значения указать требуемый IP адрес (рисунок 3).

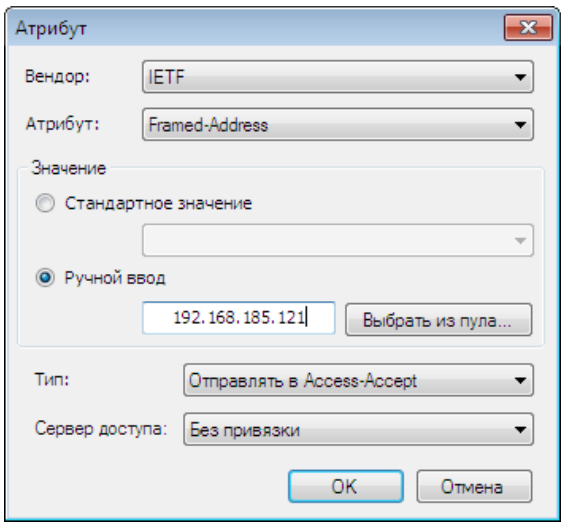

Рисунок 3

Для ограничения времени сессии пользователя следует воспользоваться атрибутом Session-Timeout, который задаёт максимальную длительность сессии в секундах.

Аналогичным образом можно создать нужное количество логинов пользователей. Кроме ручного создания пользователей поддерживается также импорт данных из Active Directory или другого каталога, поддерживающего LDAP протокол.

Настройка точки доступа

Для того, чтобы точка доступа выполняла проверку подключений пользователей средствами RADIUS сервера, необходимо выполнить настройку параметров безопасности устройства Wi-Fi. В зависимости от типа устройства настройка может отличаться.

Выберете режим безопасности “WPA2 Enterprise” (Поддерживаются также WPA Enterprise и WEP RADIUS, однако они значительно более уязвимы), укажите IP адрес RADIUS сервера, и введите общий секрет, заданный в настройках RADIUS сервера. Пример настройки точки доступа приведен на рисунке 4.

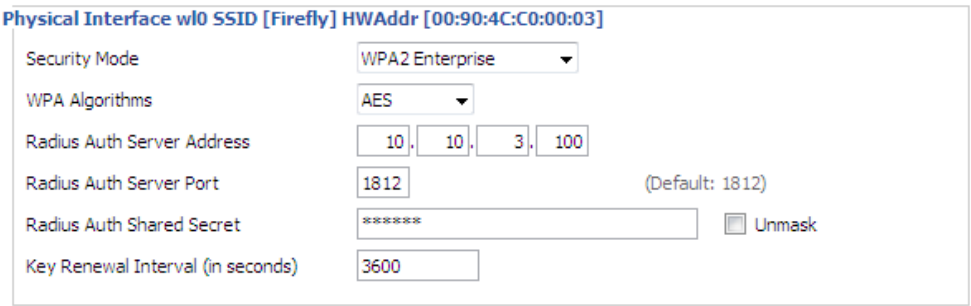

Рисунок 4

Настройка на стороне клиента

Ниже приведена инструкция по созданию и настройке беспроводного подключения на клиенте с операционной системой Windows 7.

Создадите новый профиль подключения (рисунок 5).

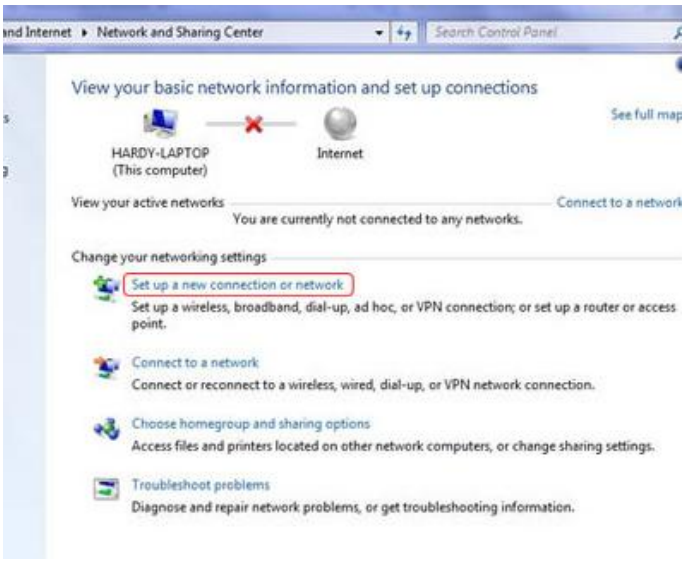

Рисунок 5

Выберите подключение по беспроводной сети (рисунок 6).

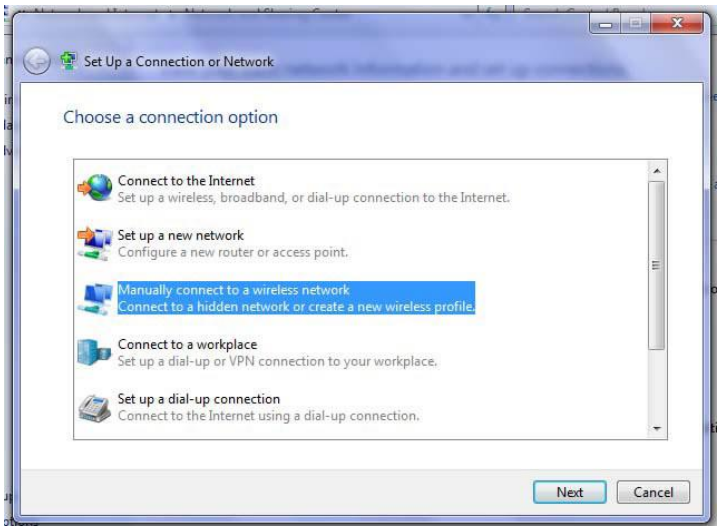

Рисунок 6

Введите имя SSID беспроводной сети, выберите тип безопасности WPA2 Enterprise и тип шифрования AES (рисунок 7).

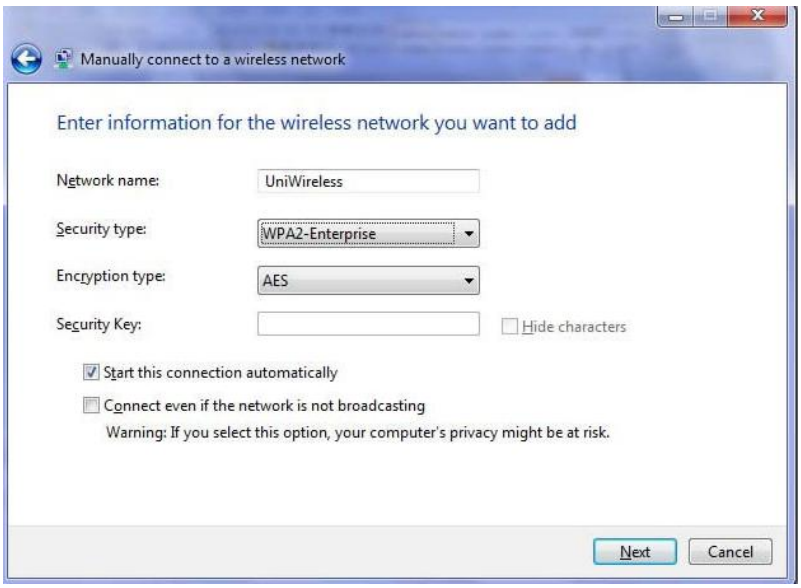

Рисунок 7

Откройте дополнительные настройки подключения (рисунок 8).

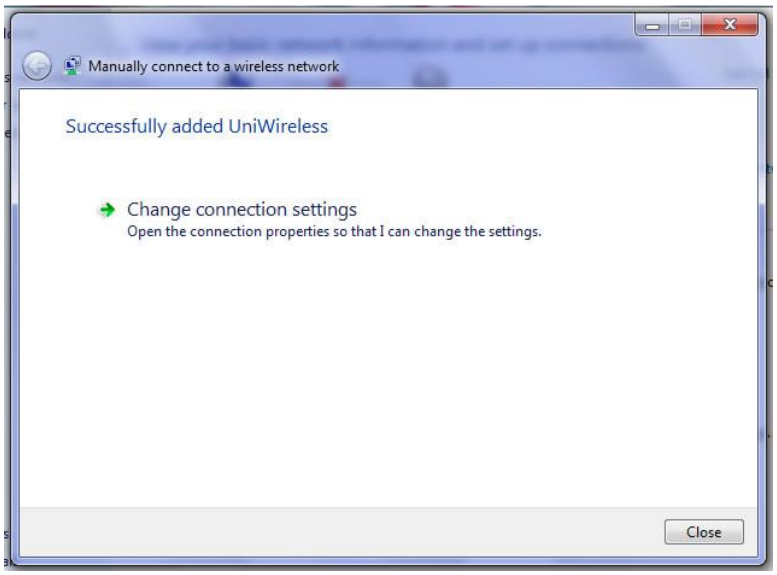

Рисунок 8

Выберите вкладку «Безопасность». Из списка методов аутентификации следует выбрать ***Microsoft: Protected EAP (PEAP)***. После этого нажмите кнопку «*Настройки*» (рисунок 9).

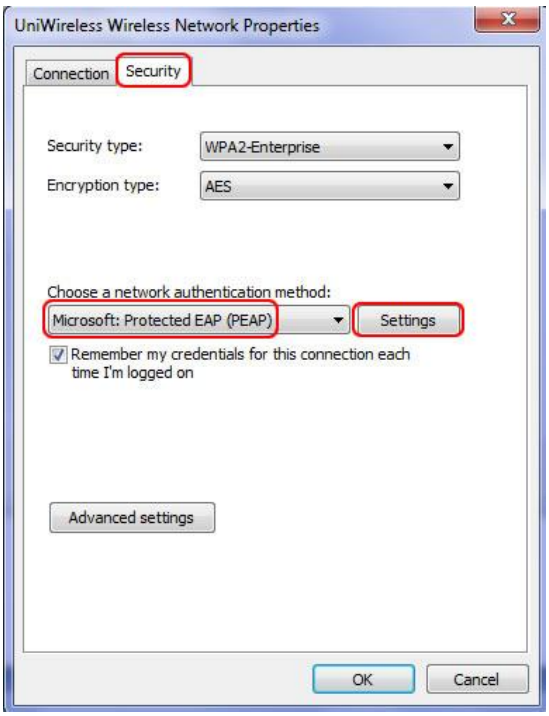

Рисунок 9

Все клиенты PEAP должны проверять сертификат RADIUS сервера, поэтому в настройках необходимо выбрать опцию «*Проверять сертификат сервера*», а в списке доверенных центров сертификации надо отметить SoftPI Radius сервер.

В списке методов аутентификации должен быть выбран «***Secured password (EAP-MSCHAP v2)***». Далее следует отключить опцию быстрого переподключения и щелкнуть по кнопке «*Configure*» (рисунок 10).

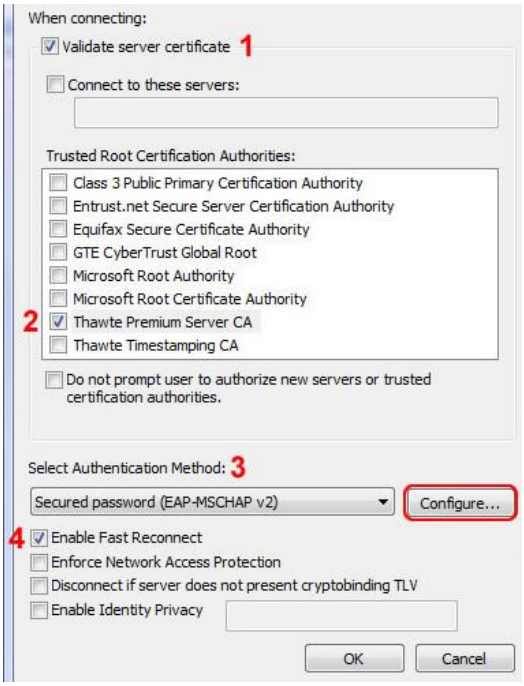

Рисунок 10

В диалоговом окне снимите флаг у пункта «Автоматически использовать имя входа и пароль Windows (и имя домена, если существует)» (рисунок 11).

Рисунок 11

Щелкните по кнопке «*ОК*» для закрытия всех диалоговых окон.
Щелкните «Закрыть» для закрытия мастера создания сетевого подключения.

Для подключения выберите в списке доступных беспроводных подключений созданное ранее подключение и щелкните по кнопке «*Подключиться*». В открывшемся окне введите имя пользователя и пароль, настроенные для пользователя в "Консоли настройки SoftPI RADIUS".