

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.

📱 Сервер доступа	
Имя:	FIREFLY
IP адрес:	10.10.3.10
Идентификатор:	
Общий секрет:	123456
Вендор:	IETF 🔹
	🔲 Заблокировать сервер доступа
	ОК Отмена

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.

Пользователь от Общее Информац	ключён ия Адрес Л	Ополнительно	
Пользователь:	test	·	
Гароль: Группа:	Default		٦
Подразделение:	Bce		Ізменить
Разрешённое вре	мя входа:		1зменить
Дата подключени	R:	🔲 3 августа 2010	г. 🔲 🔻
Дата последней а	ктивности:	03 августа 2010 09	:16:15 👻
		ОК	Отмена

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).

Атрибут	
Вендор:	IETF 🔹
Атрибут:	Framed-Address 🔹
Значение	
🔘 Стандар	тное значение
	
🔘 Ручной в	вод
	192. 168. 185. 121 Выбрать из пула
Тип:	Отправлять в Access-Accept 🔹
Сервер дост	упа: Без привязки 💌
	ОК Отмена
	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.

Physical Interface wl0 SSID [Firefly] HWAddr [00:90:4C:C0:00:03]	
Security Mode	WPA2 Enterprise 🔹	
WPA Algorithms	AES 👻	
Radius Auth Server Address	10. 10. 3. 100	
Radius Auth Server Port	1812	(Default: 1812)
Radius Auth Shared Secret	******	Unmask
Key Renewal Interval (in seconds)	3600	

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).

Choose a connection option	
Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Internet.	
Set up a new network Configure a new router or access point.	
Manually connect to a wireless network Connect to a hidden network or create a new wireless profile.	
Connect to a workplace Set up a dial-up or VPN connection to your workplace.	
Set up a dial-up connection Connect to the Internet using a dial-up connection.	

Рисунок 6

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

Enter information	for the wireless network you want to add	
Network name:	UniWireless	
Security type:	WPA2-Enterprise	
Enc <u>r</u> yption type:	AES 🔹	
Se <u>c</u> urity Key:	Hide characters	
Start this conne	ction automatically	
Connect even if Warning: If you	the network is not broadcasting select this ontion, your computer's privacy might be at risk.	
	server and a server server a prince of might be at lists	

Рисунок 7

Откройте дополнительные настройки подключения (рисунок 8).

Manually connect to a wireless network	
Successfully added UniWireless	
 Change connection settings Open the connection properties so that I can change the settings. 	
	Close

Рисунок 8

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

AES	•
hoose a network authentication method:	
Aicrosoft: Protected EAP (PEAP)	Ins
Remember my credentials for this connection each time I'm logged on	
Advanced a 195-20	
Advanced settings	
Advanced settings	
Advanced settings	

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).

	Connect to these servers:
Tr	usted Root Certification Authorities:
	Class 3 Public Primary Certification Authority
	Entrust.net Secure Server Certification Authority
	Equifax Secure Certificate Authority
	GTE CyberTrust Global Root
	Microsoft Root Authority
	Microsoft Root Certificate Authority
	Thawte Premium Server CA
	Do not prompt user to authorize new servers or trusted
Seler	Do not prompt user to authorize new servers or trusted certification authorities.
Selec	Do not prompt user to authorize new servers or trusted certification authorities. It Authentication Method: 3 ured password (EAP-MSCHAP v2) Configure.
Selec Sec E E D E E	Do not prompt user to authorize new servers or trusted certification authorities.

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

	vz rioperae	3	_
When conne	ecting:		
Automa	atically use my	Windows logon na	ame and
passwe		ir ii di iy).	
	OV	Crearl	1

Щелкните по кнопке «*OK*» 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".