

# Настройка аутентификации VPN с использованием сервера SoftPI RADIUS

## Настройка SoftPI RADIUS сервера

Сервер SoftPI RADIUS (далее RADIUS сервер) 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 программе "Консоль управления RADIUS" сервера настроить параметры сервера доступа, в качестве которого будет выступать VPN сервер.

Необходимо ввести его IP адрес и общий секрет. Общий секрет – это пароль, используемый при обмене данными между сервером RADIUS и VPN сервером. Использование этого пароля исключает возможность появления неавторизованного VPN сервера. 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 ввести параметры пользователей, которые будут иметь право подключаться к VPN серверу. Для добавления пользователя следует 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.

После создания пользователя при необходимости следует задать ему атрибуты. Для отправки атрибутов авторизованному пользователю, необходимо в параметре "Тип" выбрать значение: "Отправлять в Access-Accept".

👗 Пользователь 💽 💌			
🔲 Пользователь от	ключён		
Общее Информац	ия Адрес Д	ополнительно	
Пользователь:	test		
Пароль:	•••••		
Группа:	Default		•
Подразделение:	Bce		Изменить
Разрешённое время входа:			Изменить
Дата подключения Дата последней а	я: ктивности:	<ul> <li>З августа 20</li> <li>03 августа 2010</li> </ul>	10 r. ■▼ 09:16:15 ▼
		OK	Отмена

Рисунок 2

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

Атрибут	<b>—</b> ×
Вендор:	IETF 🔹
Атрибут:	Framed-Address 🔹
Значение	
🔘 Стандартн	юе значение
[	-
Ручной вво	д
	192. 168. 185. 121 Выбрать из пула
Тип:	Отправлять в Access-Accept 🔹
Сервер доступ	а: Без привязки 💌
	ОК Отмена

Рисунок 3

Для ограничения времени сессии пользователя средствами сервера доступа (если такая возможность есть), можно воспользоваться атрибутом Session-Timeout (или другим, который поддерживается конкретным сервером доступа), который задаёт максимальную длительность сессии в секундах.

Аналогичным образом можно создать нужное количество логинов пользователей.

Кроме ручного создания пользователей, SoftPI Radius поддерживает также импорт данных из Active Directory или другого каталога, поддерживающего протокол LDAP.

Сервер доступа (VPN сервер) может поддерживать и другие атрибуты, которые можно задать для пользователя и/или группы пользователей.

## Настройка сетевого сервера доступа (Network Access Server - NAS)

В зависимости от типа VPN сервера настройка может иметь отличия. Для настройки аутентификации и авторизации по протоколу RADIUS необходимо указать:

- 1. IP адрес сервера аутентификации RADIUS.
- 2. Номер порта аутентификации (по умолчанию 1812).
- 3. Общий секрет, введенный ранее в настройках RADIUS сервера.
- 4. При необходимости ведения учета предоставленных услуг следует указать IP адрес биллингового сервера.

### Настройка компьютера клиента VPN (Пример настройки для WindowsXP)

- 1. Создание нового подключения.
  - 1.1 Откройте окно «Сетевые подключения» и выберите пункт «Создание нового подключения».
  - 1.2 Создайте новое подключение для подключения с использованием VPN (рисунки 4 7).

Мастер новых подключений		
Тип сетевого подключения Выберите одну из следующих возможностей.		
<ul> <li>Подключить к Интернету</li> <li>Подключить к Интернету для просмотра веб-узлов и чтения электронной почты.</li> <li>Подключить к сети на рабочем месте</li> </ul>		
Подключить к рабочей сети (используя удаленный доступ или VPN), чтобы можно было работать из дома, удаленного офиса или другого места.		
О <u>У</u> становить домашнюю сеть или сеть для малого офиса		
Подключить к существующей сети малого или домашнего офиса или установить новую сеть.		
Установить прямое подключение к другому компьютеру Подключить напрямую к другому компьютеру с помощью последовательного, параллельного или инфракрасного порта, или настроить данный компьютер, позволив другим компьютерам подключаться к нему.		
< <u>Н</u> азад Далее > Отмена		

Рисунок 4

Мастер новых подключений	
Сетевое подключение Каким образом вы хотите подключиться к сети на своем рабочем месте?	S)
Создать подключение:	
Подключение удаленного доступа	
Подключаться, используя модем и обычную телефонную линию, либо телефонную линию ISDN.	
Подключение к виртуальной частной сети Подключение к сети с использованием подключения к виртуальной частной сети (Virtual Private Network - VPN) через Интернет.	
< <u>Н</u> азад Далее>	Этмена

Рисунок 5

Мастер новых подключений		
Имя подключения Укажите имя для этого подключения к рабочему месту.		
Введите в следующем поле имя для этого подключения. <u>О</u> рганизация		
SoftPi Test		
Например, можно ввести имя рабочего места или имя сервера, к которому будет выполняться подключение.		
<ul> <li><u>Назад</u>алее &gt; Отмена</li> </ul>		

Рисунок 6

Мастер новых подключений
Публичная сеть Windows может сначала установить подключение к публичной сети.
Выберите, надо ли автоматически подключаться к Интернету или иной общей сети перед установлением виртуального подключения.
Не набирать номер для предварительного подключения.
Набрать номер для следующего предварительного подключения:
< <u>Н</u> азад Далее > Отмена

Рисунок 7

1.3 Укажите IP адрес VPN сервера (рисунок 8).

Мастер новых подключений	
<b>Выбор VPN-сервера</b> Укажите имя или адрес VPN-сервера	I)
Введите имя узла или IP-адрес компьютера, к которому осуществляется подключение. <u>И</u> мя компьютера или IP-адрес (например, microsoft.com или 157.54.0.1):	
192.168.185.1	
Далее > ()	Этмена
< <u>Назад</u> алее> (	Этмена

Рисунок 8

- 2. Настройка VPN подключения.
  - 2.1 Откройте созданное подключение, введите имя пользователя и пароль, а затем выберите «*Свойства*» (рисунок 9).

Подключение	: SoftPi Test	? 🗙
C		
По <u>л</u> ьзователь:	test	
П <u>а</u> роль:	•••	
С <u>о</u> хранять и только д для л <u>ю</u> б	имя пользователя и пароль: иля меня ого пользователя	
Подключение	Отмена Свойства Сп	равка

Рисунок 9

2.2 Во вкладке "Безопасность" выберите опцию "Дополнительные" и щелкните по кнопке "Параметры" (рисунок 10).

🗢 Soft	Pi Test Свой	ства		? 🛛
Общие	Параметры	Безопасность	Сеть	Дополнительно
Пара	аметры безопа	сности		
	Јб <u>ы</u> чные (реко) При проверке (	мендуемые пара использиется:	метрыј	
	при проверке і	используется.		~
	<u>И</u> спользова из Windows Tpe <u>б</u> уется и	ать автоматическ (и имя домена, є шифрование данн	ки имя в) Эсли сущ ных (инач	кода и пароль ествует) не отключаться)
0	Дополнительны	ые (выборочные г	араметр	ы
	Применение эт знания протоко безопасности.	гих параметров т олов обеспечени:	ребует я	Параметры
			Пара	метры I <u>P</u> Sec
			OK	Отмена
		Рисунок 1	10	

2.3 В окне "Дополнительные параметры безопасности" выберите протокол(ы) для проверки подлинности (рисунок 11).

Дополнительные параметры безопасности 🛛 🕐 🔀
Шифрование данных:
обязательное (отключиться если нет шифрования) 🛛 💌
с Безопасный вход
<ul> <li>Протокол расширенной проверки подлинности (ЕАР)</li> </ul>
Защищенные ЕАР (РЕАР) (шифрование включенс 🗸
Своўства
О Разрешить следующие протоколы
<u>Н</u> езашифрованный пароль (РАР)
Протокол проверки пароля Shiva (SPAP)
Пр <u>о</u> токол проверки пароля (СНАР)
ротокол проверки пароля Microsoft (MS-CHAP)
Разрешить старый протокол MS-CHAP для Windows 95
Прото <u>к</u> ол проверки пароля Microsoft (MS-CHAP v2)
Для протоколов на основе MS-CHAP автоматически использовать имя входа и пароль Windows (и имя домена, если существует)
ОК Отмена

Рисунок 11

Наиболее защищённый протокол из представленных — ЕАР. Дополнительные настройки для протокола РЕАР описаны далее в соответствующем разделе. Для использования в локальной сети может быть достаточно протокола MS-CHAPv2. Не рекомендуется использовать протоколы РАР/СНАР в виду их слабой защищённости.

Настройки для протокола РЕАР.

При выборе опции «Протокол расширенной проверки подлинности (EAP)» становится доступным список протоколов, из которого необходимо выбрать протокол PEAP. По нажатию кнопки «Свойства» отобразится диалог «Дополнительные параметры безопасности» для задания настроек PEAP. В диалоге следует выбрать опции проверки сертификата RADIUS сервера или отключить проверку сертификатов. При включённой опции «Проверять сертификат сервера» на компьютере клиента, в хранилище сертификатов, должен быть установлен корневой сертификат SoftPI RADIUS сервера. Этот сертификат должен быть выбран в списке «Доверенные корневые центры сертификации». Другие опции следует задать, как показано на рисунке 12.

Защищенные свойства ЕАР 🛛 💽 🗙
При подключении:
Проверять сертификат сервера
Подклю <u>ч</u> ение к серверам:
Доверенные корневые центры сертификации:
C&W HKT SecureNet CA Root
Certiposte Classe A Personne
Certisign - Autoridade Certificadora - AC2
Certisign - Autoridade Certificadora - AC4
Не требовать авторизовать новые серверы или
доверенные центры сертификации.
<u>В</u> ыбор метода проверки подлинности:
Безопасный пароль (EAP-MSCHAP v2) 🛛 🖌 <u>Н</u> астроить
Включить быстрое переподключение
Включить проверки в <u>к</u> арантине
ОК Отмена

Рисунок 12

На рисунке 13 показан вид окна свойств метода проверки подлинности EAP-MSCHAP v2.

Защищенные свойства ЕАР	<b>?</b> ×	
При подключении:		
Проверять сертификат сервера		
Подклюцение к серверам:		
При подключении:		
Автоматически использовать имя входа и	_	
существует)		
	~	
ОК Отмена		
доверенные центры сертификации.		
Выбор метода проверки подлинности:		
Безопасный пароль (ЕАР-МSCHAP v2) 🗸 Настро	ить	
Включить быстрое переподключение		
Включить проверки в карантине		
ОК Отм	ена	

Рисунок 13

## Пример настройки для Windows Vista/Windows 7

Порядок действий по созданию и настройке подключения через VPN канал для операционных систем Windows Vista и Windows 7 аналогичный инструкциям для Windows XP. На рисунках, приведенных ниже, показаны основные шаги настройки для Windows 7.

Откройте режим "Панели управления" Windows, позволяющий создать VPN подключение (рисунки 14, 15).



Далее необходимо открыть мастер создания подключения, как показано на рисунке 16.



Выберете тип подключения «Подключение к рабочему месту» (VPN) (рисунок 17).

<b>Веспрово</b>	ение к Интернету дное, скоростное или те	елефонное подключе	ение к Интернету.	
Set Up a N Configure	letwork a new router or access pe	oint.		
Настройк Подключ	а телефонного подключ ение к Интернету через	<b>чения</b> телефонное подклю	чение.	
Подключ	ение к рабочему месту			
Настройк	а телефонного или VPN	-подключения к раб	очему месту.	

Рисунок 17

Для создания нового подключения выбираем тип подключения «Подключение к сети с помощью виртуальной частной сети (VPN)» (рисунки 18 - 19).

<u>Отзывы</u> Отзывы	и предложения
Использовать имеющееся подключение?	
<ul> <li>Нет, создать новое подключение</li> <li>Да, выбрать существующее подключение</li> </ul>	
Подключение по локальной сети WAN Miniport (PPTP)	
	Next Cancel

Рисунок 18

Отзывы и предложения	×
Как выполнить подключение?	
Использовать мое подключение к Интернету (VPN) Подключение через Интернет с помощью виртуальной частной сети (VPN).	\$
💐 — 🎱 — 🕪	
Использовать прямой набор номера Прямое подключение к телефонному номеру без выхода в Интернет.	
🔍 — 🦫	
Что такое VPN-подключение?	
Ca	ncel

Рисунок 19

Далее следует выбрать параметр «Отложить настройку подключения к Интернету», т.к. не все параметры еще установлены (рисунок 20).

Отзывы и предложения 📼 📼 🔀	
Настроить подключение к Интернету перед продолжением?	
Для использования подключения виртуальной частной сети (VPN) требуется подключение к Интернету.	
Установить подключение к Интернету	
Отложить настройку подключения к Интернету	
Cancel	

Рисунок 20

Введите адрес или доменное имя сервера VPN, и произвольное имя создаваемого подключения (рисунок 21).

	Отзывы и предложения
🕒 📠 Подключение к рабоч	ему месту
Введите адрес Инте	рнета для подключения
Этот адрес можно получи	ть у сетевого администратора.
<u>А</u> дрес в Интернете:	vpn.server.com
<u>И</u> мя местоназначения:	vpn - Internet
Использовать сма	от-карту
🛞 📃 <u>Р</u> азрешить исполь	зовать это подключение другим пользователям
Этот параметр поз компьютеру, испо	воляет любому пользователю, имеющему доступ к этому льзовать это подключение.
Не подключаться с	ейчас, только выполнить установку для подключения в будущем
	Next Cancel

Рисунок 21

Введите логин и пароль (рисунок 22).

Введите имя пользов	зателя и пароль	
<u>П</u> ользователь:	Ваш Логин/Имя пользователя	
Паро <u>л</u> ь:	Ваш Пароль	
	Отображать вводимые знаки	
	Запомнить этот пароль	
Домен (не обязательно):		

Рисунок 22

	Отзывы и предложения
🚱 🔚 Подключение к рабочему месту	
Подключение готово к использованию	
· · · · · · · · · · · · · · · · · · ·	<b>I</b> P
Прежде чем продолжить, необходимо уст Интернету.	тановить подключение к
	Закрыть

Рисунок 23

После создания подключения следует перейти к его свойствам и настроить параметры безопасности. Настройка аналогична настройке для Windows XP.