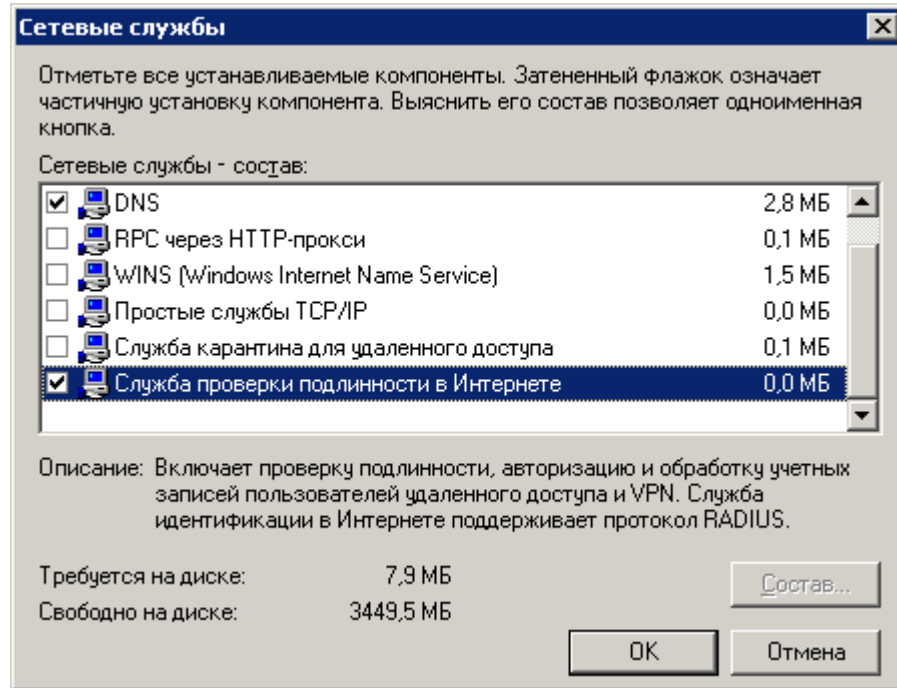
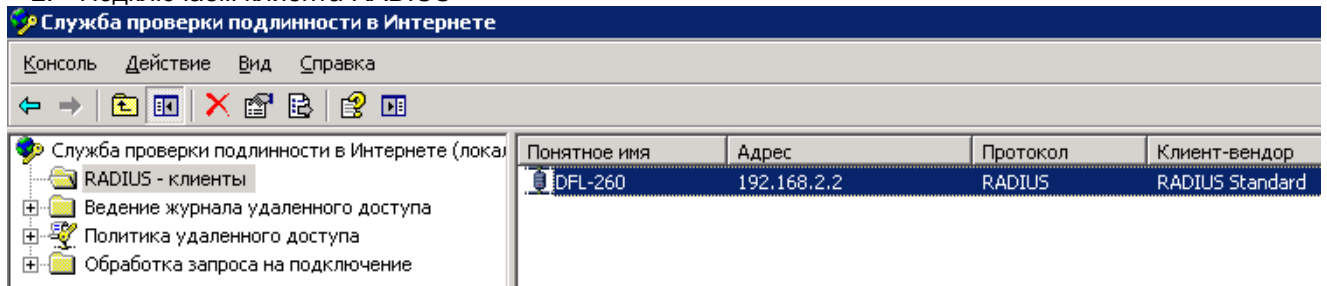


1. Устанавливаем RADIUS

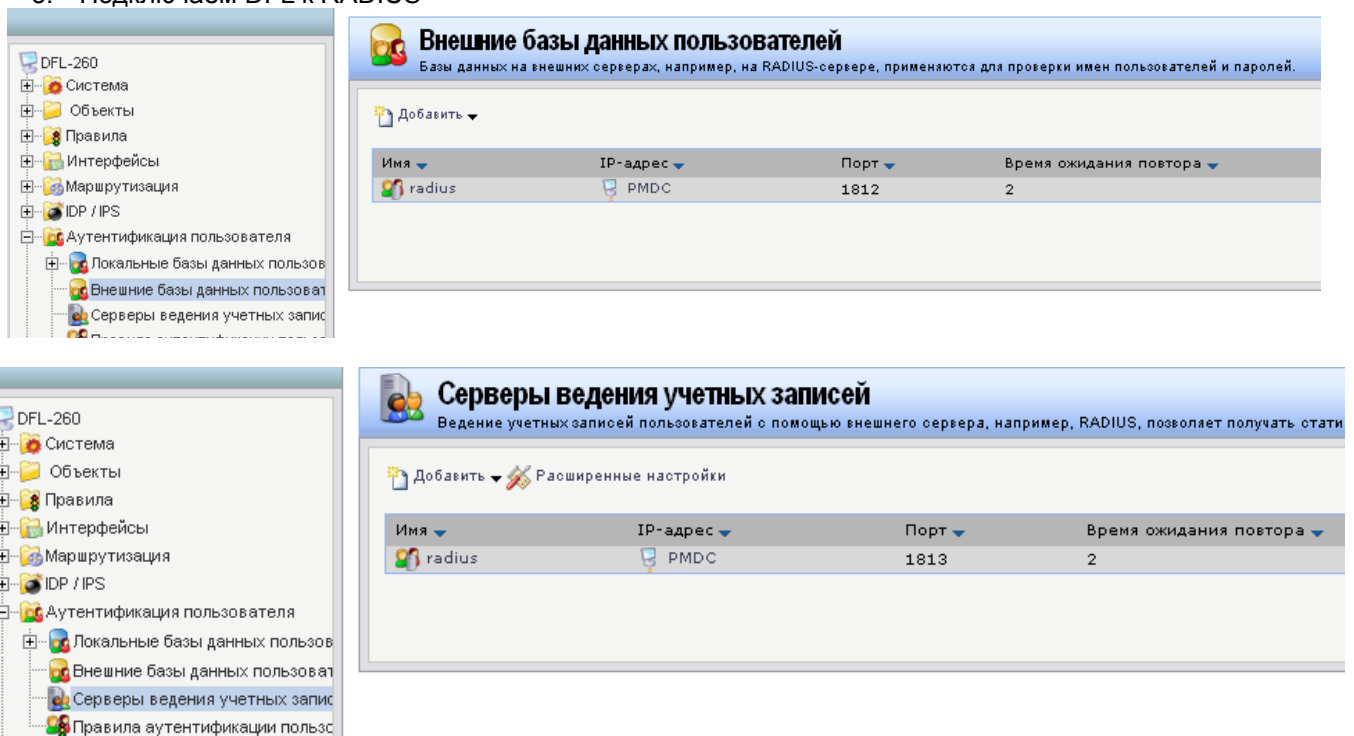


2. Подключаем клиента RADIUS



Вводим Общий секрет (пароль для «общения» с DFL), галку Запрос должен содержать атрибут проверки подлинности сообщения не ставим.

3. Подключаем DFL к RADIUS



Общий секрет — такой же, как и на RADIUS

4. Настраиваем правило аутентификации для HTTP:

The screenshot shows the 'Общие' (General) tab of a configuration window. It contains several fields for setting up an authentication rule:

- Имя: http-auth
- Агент: HTTP
- Источник аутентификации: RADIUS
- Интерфейс: lan
- IP-адрес источника: lannet
- IP-адрес терминатора: (None)

Below these fields is a note: 'Для XAuth и PPP IP-адрес источника для туннеля.' (For XAuth and PPP, the source IP address for the tunnel).

The screenshot shows the 'Опции аутентификации' (Authentication Options) tab. It includes instructions: 'Выберите один или более серверов аутентификации. Также выберите метод аутентификации, используемый для шифрования.' (Select one or more authentication servers. Also select the authentication method used for encryption).

Under 'Radius-сервер (-ы):' (Radius server(s)), there are two lists: 'Доступные' (Available) and 'Выбрано' (Selected). The 'Выбрано' list contains 'radius'. Between the lists are '>>' and '<<' buttons. Below the lists are 'Переместить вверх' (Move up) and 'Переместить вниз' (Move down) buttons.

Below the lists, there are two dropdown menus:

- Метод Radius: Нешифрованный п. (Unencrypted p.)
- Локальная база данных пользователя: (None)

The screenshot shows the 'Ведение учетных записей' (Accounting) tab. It includes instructions: 'Выберите один или более серверов учетных записей. Также выберите статистику для аутентификации.' (Select one or more accounting servers. Also select statistics for authentication).

Under 'Сервер(ы) учетных записей:' (Accounting server(s)), there are two lists: 'Доступные' (Available) and 'Выбрано' (Selected). The 'Выбрано' list contains 'radius'. Between the lists are '>>' and '<<' buttons. Below the lists are 'Переместить вверх' (Move up) and 'Переместить вниз' (Move down) buttons.

Below the lists, there is a section titled 'Статистика пользователя' (User statistics) with several checkboxes:

- ☒ Отправленные байты
- ☒ Полученные байты
- ☒ Отправленные пакеты
- ☒ Полученные пакеты
- ☒ Время сессии
- ☐ Поддержка Временного учета
- ☐ Управляемое сервером значение

At the bottom, there is a field for 'Временное Значение:' (Temporary Value) set to '600' and a unit selector set to 'Секунды' (Seconds).

Общие | Настройки Журнала | Опции аутентификации | Ведение учетных записей | Опции HTTP(s)-агента

Общие

Тип логина:

Строка:

Сертификаты

Сертификат хоста:

Сертификат корня:

Общие | Настройки Журнала | Опции аутентификации | Ведение учетных записей | Опции HTTP(s)-агента | Опции PPP-агента | Ограничения

Таймауты

Время ожидания: секунды

Таймаут сессии:

☐ Использовать таймауты, полученные от сервера аутентификации.

Если таймауты не были получены ИЛИ данная опция не была выбрана, будут использоваться вышеуказанные настройки.

Разрешить использование нескольких регистраций на имя пользователя

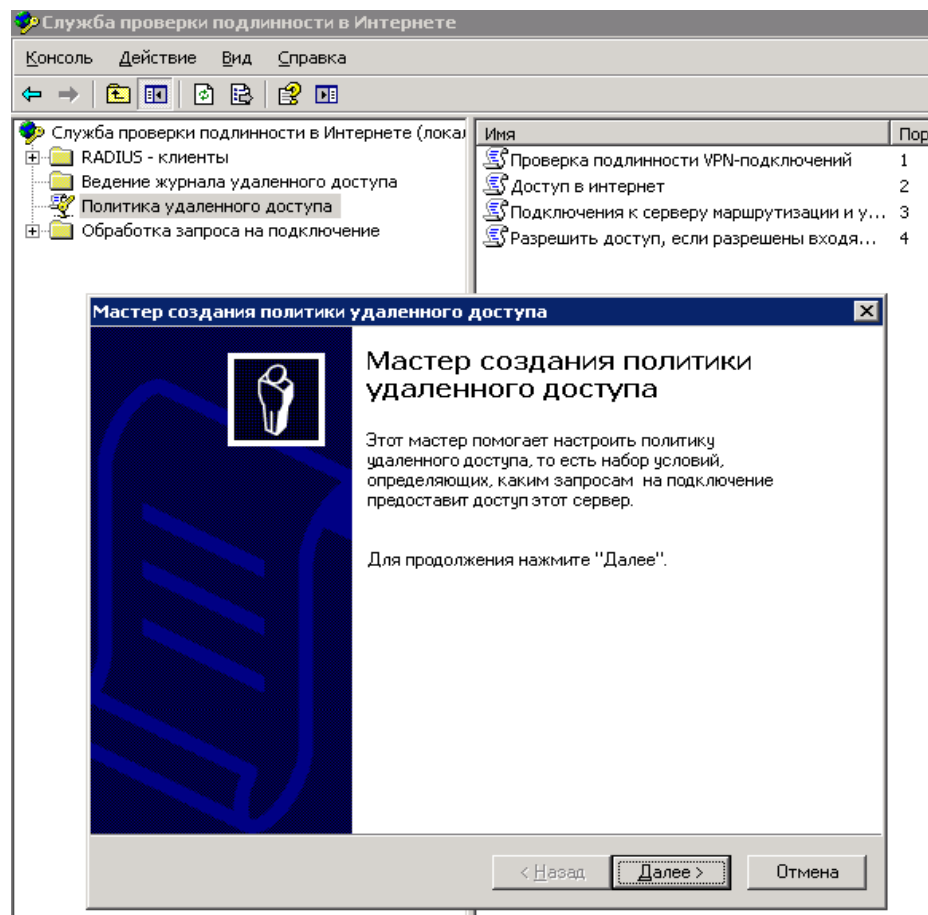
☒ Разрешить несколько Логинов на имя пользователя

☐ Разрешить один логин на имя пользователя и запретить обратное.

☐ Разрешить один логин на имя пользователя

Заменить существующего пользователя, если ожидание длится больше, чем секунды

5. Настраиваем правила, как указано тут <http://dlink.ru/ru/faq/85/574.html> . В п. 1 у объекта lan-auth на закладке Аутентификация пользователя ставим галку Не заданы допуск. П. 4 и п. 6 опускаем за ненадобностью.
6. Настраиваем Политики удаленного доступа на RADIUS:



Мастер создания политики удаленного доступа

Метод настройки политики

Этот мастер может создать обычную (шаблонную) политику, либо можно создать свою собственную.

Каким образом следует установить эту политику?

☐ Использовать мастер для установки типовой политики общего сценария

☒ Выбрать особую политику

Введите имя, описывающее эту политику.

Имя политики:

Пример: Проверка подлинности всех VPN-подключений.

< Назад Далее > Отмена

Мастер создания политики удаленного доступа

Условия политики

Чтобы пройти проверку на подлинность запросы на подключение, должны удовлетворять указанным условиям.

Укажите условия, которым должен соответствовать запрос на подключение, чтобы получить доступ или отказ в получении доступа.

Условия политики:

Windows-Groups соответствует "LIDER\Inet_Users"

Добавить... Изменить... Удалить

< Назад Далее > Отмена

Мастер создания политики удаленного доступа

Разрешения
 Политика удаленного доступа может либо назначать, либо запрещать права доступа пользователям, которые удовлетворяют определенным условиям.

Если запрос на подключение удовлетворяет указанным условиям:

☒ Предоставить право удаленного доступа

☐ Отказать в праве удаленного доступа

< Назад Далее > Отмена

На следующей странице после Условий политики жмем изменить профиль

Изменение профиля коммутируемых подключений

IP Многоканальное подключение

Ограничения по входящим звонкам

Проверка подлинности Шифрование Дополнительно

Выберите методы проверки подлинности, которые хотите разрешить для данного подключения.

Методы EAP

☐ Шифрованная проверка (Microsoft, версия 2, MS-CHAP v2)
☒ Разрешить смену пароля по истечении срока действия

☐ Шифрованная проверка подлинности Microsoft (MS-CHAP)
☒ Разрешить смену пароля по истечении срока действия

☐ Шифрованная проверка подлинности (CHAP)

☒ Проверка открытым тестом (PAP, SPAP)



Доступ без проверки

☐ Разрешить подключение клиентов без согласования метода проверки подлинности.

OK Отмена Применить

Все.

DFL теперь показывает доменные учетки:

 Статус аутентификации пользователя Отображает список всех аутентифицированных пользователей.					
 Общие					
Имя пользователя	IP-адрес	Интерфейс	Таймаут сессии	Время ожидания	Зарегистрирован как
domain_user	192.168.0.33	dmz		29m	ANY AUTHENTICATED
domain_user	192.168.0.203	dmz		29m	ANY AUTHENTICATED
domain_user	192.168.0.21	dmz		29m	ANY AUTHENTICATED
domain_user	192.168.0.26	dmz		29m	ANY AUTHENTICATED
domain_user	192.168.0.62	dmz		29m	ANY AUTHENTICATED
domain_user	192.168.0.41	dmz		29m	ANY AUTHENTICATED

Просмотр системных событий на RADIUS также может дать дополнительную информацию:

Пользователю "domain_user" предоставлен доступ.

Полное-имя-пользователя = lider.local/Структура/УК ЛИДЕР/ОИТ/Белов Евгений

NAS-IP-адрес = <нет данных>

NAS-идентификатор = Clavister

Понятное-имя-клиента = DFL-260

IP-адрес-клиента = 192.168.2.2

Идентификатор-вызывающей-станции = <нет данных>

Тип-NAS-порта = <нет данных>

NAS-порт = 2

Имя-политики-прокси = Использовать проверку подлинности Windows для всех пользователей

Поставщик-проверки-подлинности = Windows

Сервер-проверки-подлинности = <не определено>

Имя-политики = Доступ в интернет

Тип-проверки-подлинности = PAP

EAP-тип = <не определено>

!Тип проверки подлинности PAP предполагает передачу пароля в открытом виде!