Лабораторная работа 2.

Аутентификация и авторизация с помощью RRAS RADIUS роутеров.

VPN PPTP сервер на роутере Cisco.

Часть 1.

Настройка RADIUS сервера на Windows Server для использования AAA сервисов при входе на устройства Cisco.

Задание 1.

Cборка и настройка схемы.

1. Собрать схему в GNS согласно рисунку 1:

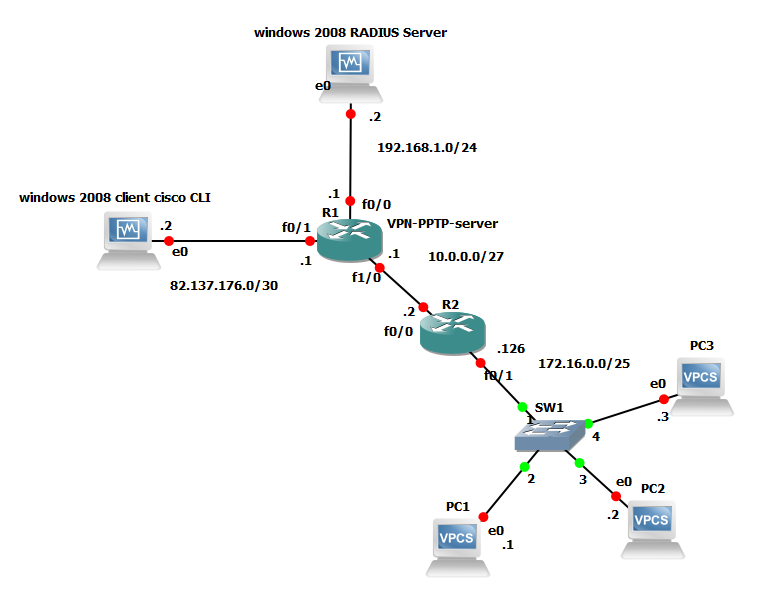


Рисунок 1.

В данной схеме используются две ВМ на основе Windows 2008 Server. Одна из них в качестве VPN/SSH/Telnet клиента, вторая в качестве внешнего RADIUS сервера, на основе роли RRAS в составе Windows Server.

Разумеется в роутере R1, не будет хватать 1-го слота Ethernet, его надо будет добавить.

1. Настроить сетевые интерфейсы устройств согласно адресному плану, указанному на схеме.

Подсказки:

1. После импорта ВМ Windows 2008 Server, перед подключением их в GNS, нужно перевести 1-й сетевой интерфейс из типа NAT в тип “Не подключен”, иначе GNS выдаст соот. ошибку.
2. В ВМ Windows Client cisco CLI надо будет перед включением ее в схеме GNS запустить самим VirtualBox и скачать из интернета или с сетевого диска \\app.sstu.ru\soft программу Putty, с помощью которой будет осуществляться консольный доступ к маршрутизаторам R1 и R2. После чего ее можно включить в схему, переведя интерфейс в тип “Не подключен” и запускать уже из под GNS. Если вы все таки уже включали ее из GNS, чтобы не сбивать сетевые настройки нужные для работы ВМ в GNS. Выключите ВМ и активируйте второй интерфейс как NAT, далее запустить самим VirtualBox и скачать из интернета или с сетевого диска \\app.sstu.ru\soft программу Putty.
3. Между роутерами R1 и R2 настроить маршрутизацию RIPv2, не забыв отключить авто суммуризацию сетей, для всех подключенных к ним Directly-connected сетей, кроме сети 82.137.176.0/30 на маршрутизаторе R1.
4. Проверить связь в локальной сети между PC1/PC2/PC3 c R1 и сервером RADIUS, а так же межу R1 и сервером RADIUS (ВМ windows 2008 RADIUS Server). Связь должна быть успешной.
5. Проверить связь во внешней сети между ВМ Windows Client cisco CLI и R1. Связь должна быть успешной.

Примечание:

Именно сегмент сети между ВМ Windows Client cisco CLI и R1 является эмуляцией внешнего подключения к ЛВС, специально для чего им выделены адреса из маршрутизируемого в сети интернет диапазона 82.137.176.0/30.

Задание 2.

Настройка RADIUS сервера на Windows Server.

*Пункты 1-5 настройка клиентов RADIUS сервера.*

1. Зайти на ВМ windows 2008 RADIUS Server и установить роль Службы политики сети и доступа (RRAS). В качестве службы ролей установите – Сервер политики сети.
2. После успешной установки запустить оснастку – Сервер политики сети.

Теперь нужно будет настроить RADIUS клиенты, а это в нашем случае роутеры R1 и R2, а так же сетевые политики, с помощью которых мы сможем подключать одних пользователей с административными правами, а других с правами оператора, на роутерах cisco, соответственно уровни привилегий 15 и 1.

1. Перед тем как производить настройку RADIUS сервера, нужно создать пользователей и группы, которые будут использоваться для входа на роутеры Cisco. В нашем случае, так как не используется контроллер домена AD, надо открыть оснастку управления локальными пользователями и группами и создать два пользователя для административного доступа - admin-1 и admin-2 с аналогичными паролями. А так же два пользователя для доступа к роутерам с правами операторов – operator-1 и operator-2 с аналогичными паролями.

Так же для них нужно создать группы cisco-admins и cisco-operators и не забыть внести этих пользователей в эти группы.

1. Выберете пункт RADIUS клиенты и создайте нового RADIUS клиента, рисунок 2:

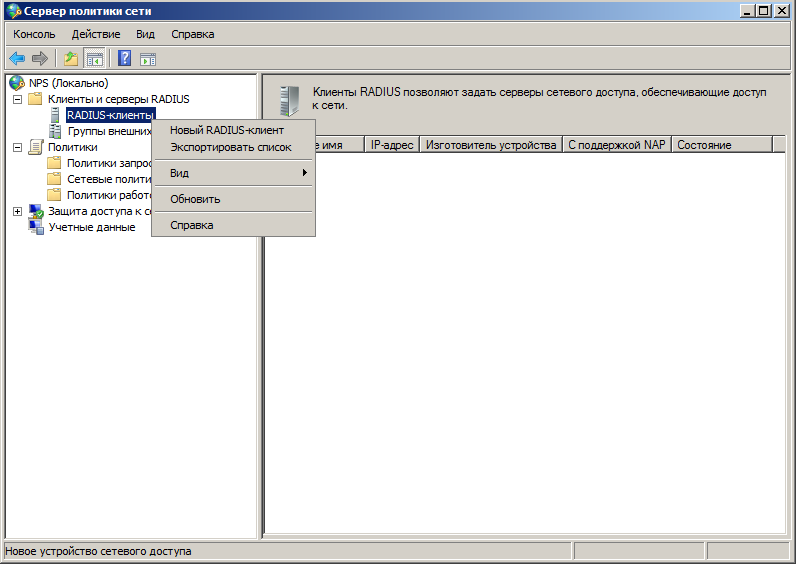


Рисунок 2.

При создании RADIUS клиента указать его имя, для роутера R1 – Cisco Router R1, его IP адрес. В качестве имени поставщика выбрать – Cisco. Далее надо придумать парольную фразу (Общий секрет), которая будет так же настроена на роутере R1. Пусть это будет password-1.

После чего настройку клиент Radius для роутера R1 можно считать выполненной, рисунок 3:

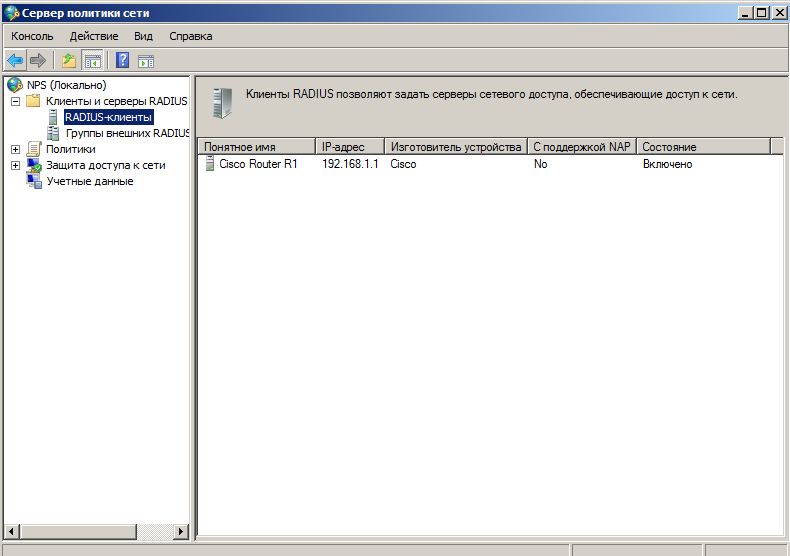


Рисунок 3.

1. По аналогии настроить Radius клиент для роутера R2.

*Пункты 6-7 настройка сетевых политик доступа пользователей для группы администраторов и операторов*

1. Выбрать пункт - Сетевые политики, и создать Новый документ, рисунок 4:

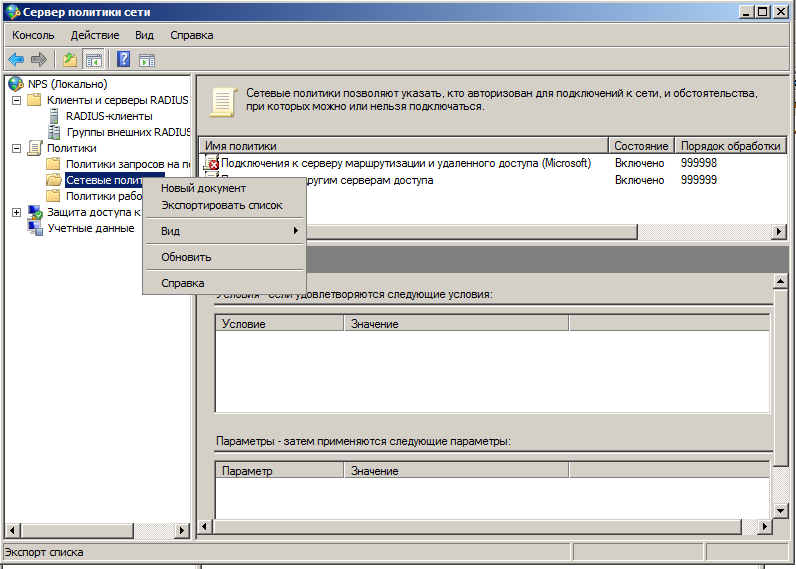


Рисунок 4.

Далее нужно указать имя политики сети и тип подключения. В качестве имени задать – Connect to Cisco Router’s Admins, тип сервера и доступа к сети оставить – Не определен. Данная политика будет действовать для пользователей обладающих административными правами на маршрутизаторе cisco.

После чего в качестве условия надо задать группу пользователей, в нашем случае это будет группа cisco-admins.

В окне настройки доступа, оставьте все по умолчанию, то есть – Доступ разрешен.

В окне “Настройка методов проверки подлинности” оставить выбранным только – Проверка открытым текстом (PAP, SPAP).

В окне Настройка ограничений можно выставить настройки таймаута простоя и таймаута сеанса 15 и 30 минут соответственно.

В окне настройка параметров выбрать вкладку Стандарт и в ней удалить атрибуты Framed-Protocol и Service-Type, после чего нажать на кнопку Добавить и выбрать пункт Service-Type, в его настройке выбрать “Значение атрибута” – Другие как “login”, рисунок 5:

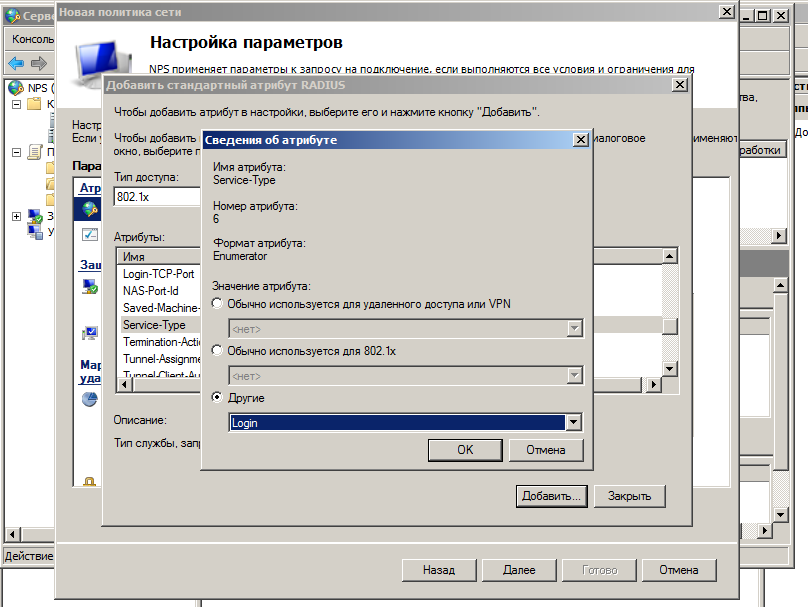


Рисунок 5.

В том же окне “Настройка параметров”, выбрать вкладку параметров – Зависящие от поставщика и нажать на кнопку - Добавить. Далее в выпадающем списке выбрать пункт Vendor-Specifir, в нем выбрать поставщика сервера удаленного доступа – Cisco, чуть ниже в пункте соответствия спецификация RADIUS RFC выбрать пункт – Да, Соответствует. После того как атрибут будет добавлен, нужно нажать на кнопку – Изменить и выбрать “Назначенный поставщиком номер атрибута” = 1, “Формат атрибута” – строковый, “Значение атрибута” – priv-lvl=15, рисунок 6:

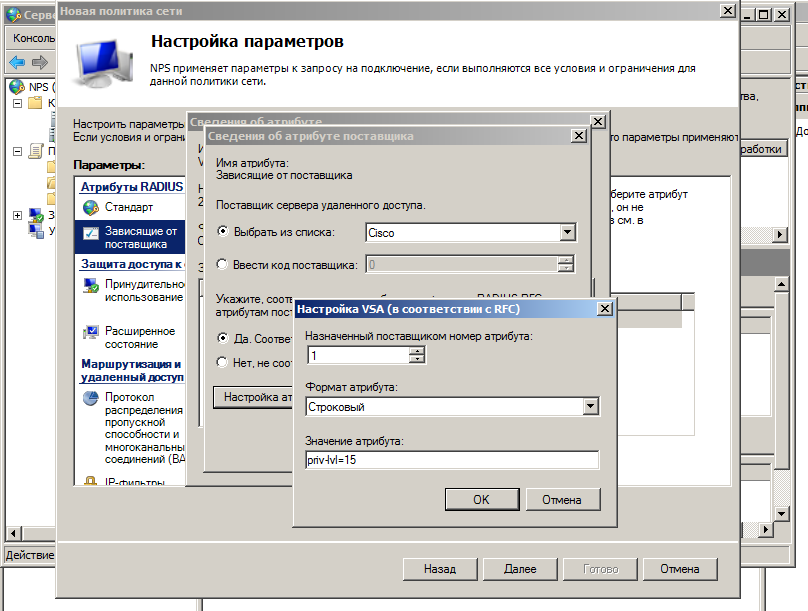


Рисунок 6.

То есть мы для группы cisco admins настроили доступ к клиентам Radius с уровнем привилегий 15, то есть административный.

Итогом правильно настроенный политики сети для административного доступа к роутерам cisco, станет окно с отчетом, рисунок 7:

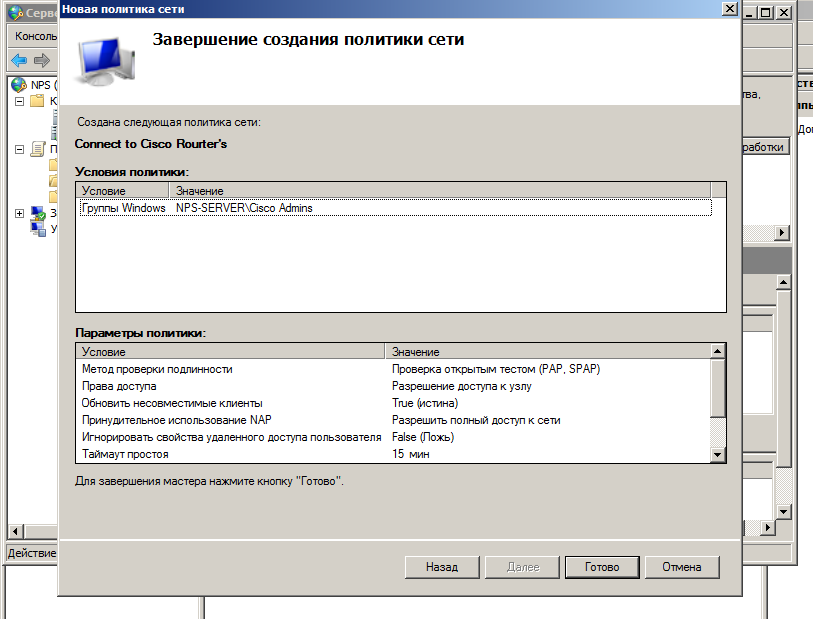


Рисунок 7.

1. По аналогии создать политику для доступа к роутерам cisco с правами операторов, уровень привилегий 1, для группы cisco- operators.

Итогом правильно настроенный политики сети для пользовательского доступа к роутерам cisco, станет окно с отчетом, рисунок 8:

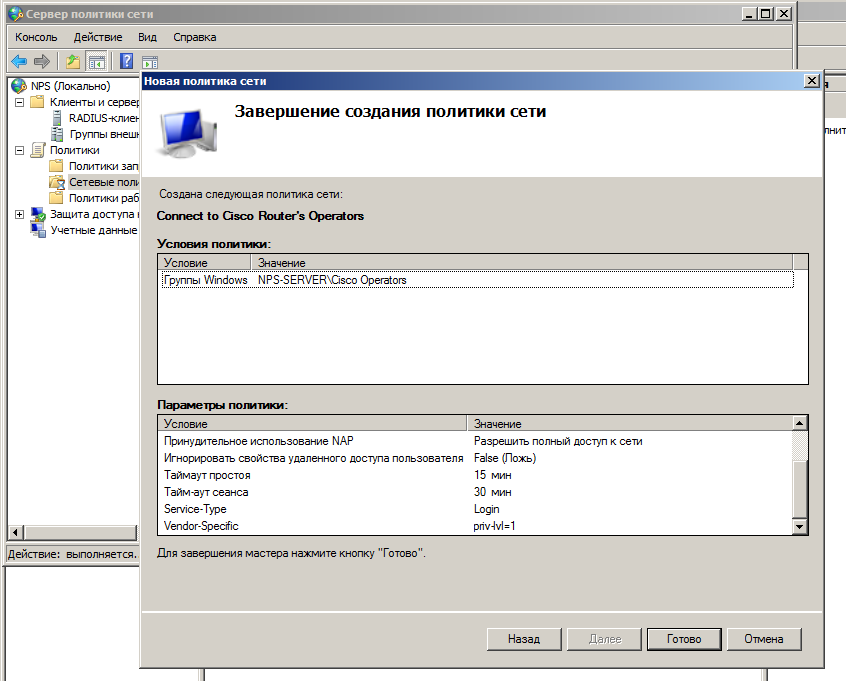


Рисунок 8

Задание 3.

Настройка роутеров cisco R1 и R2 для работы с внешним сервером RADIUS на основе Windows 2008 Server.

Чтобы маршрутизатор cisco начал работать с помощью аутентификации, авторизации и учета посредством RADIUS или TACACS+ сервера необходимо включить новую модель аутентификации командой aaa new-model. Но перед этим шагом надо обезопасить себя от того что сервер RADIUS по какой то причине не сможет ответить на запрос аутентификации и будет использоваться локальный процесс аутентификации и авторизации на роутере. То есть для этого надо задать локального пользователя с уровнем привилегий 15.

**Шаг 1.** Шифрование всех паролей **service password-encryption**. Да лучше создать пароль используя команду secret в результате которой пароль будет зашифрован лучше. Но во второй части работы мы с вами настраиваем PPTP сервер, а он с паролями заданными командой secret не работает.

**Шаг 2.** Создание локального пользователя:

username root privilege 15 password password-1

В качестве пароля зададим все тот же password-1.

**Шаг 3.** Включаем новую модель аутентификации, авторизации и учета:

**aaa new-model**

*Примечание: данная команда в принципе аналогична действию команды login local, то есть разрешает использование локальных учетных записей (если не указана radius аутентификация), а не просто настроить пароль на console 0 и VTY линии. Но ее возможности шире, и поэтому главным образом ее используют для работы с RADIUS, а когда просто нужно использовать локальные учетные записи, по старинке используют команду login local.*

**Шаг 4.** Создаем профиль аутентификации под названием **Login-Radius** и задаем его для группы radius серверов (да у нас он один, но может быть несколько в качестве обеспечения избыточности). Так же в качестве резервного метода указываем local, который будет использовать для аутентификации локальную БД пользователей, у нас это пользователь **root**.

Так же стоит отметить, что до данного пункта процесс выбора методов аутентификации доберется, только если RADIUS сервер не ответит три раза подряд. Разумеется если посылать на Radius сервер неправильные логин-пароль, то это не будет считаться неудачной попыткой аутентификации с RADIUS сервером:

**aaa authentication login Login-Radius group radius local**

Так же не забываем создать профиль авторизации на запуск команд - **Auth-Radius-exec**:

**aaa authorization exec Auth-Radius-exec group radius local**

**Шаг 5.** Теперь надо разрешить доступ по виртуальным консолям vty 0 15 для работы с AAA. Для чего зайти в режим конфигурации линий vty 0 15 и включить профили аутентификации и авторизации настроенные на предыдущем шаге:

**login authentication Login-Radius**

**authorization exec Auth-Radius-exec**

**Шаг 6.** Настроим тайм аут простоя рабочей сессии для всех виртуальных консолей, 15 минут, второе значение позволяет выставлять тайм аут в секундах:

**exec-timeout 15 0**

**Шаг 7.** Настроим тайм аут простоя сессии входа длительностью 180 секунд, если пользователь не введет логин-пароль по прошествии которых сессия отключится:

**timeout login response 180**

**Шаг 8.** Разрешим работу на VTY консолях только протоколов telnet и SSH:

**transport input telnet ssh**

Сервер SSH на роутерах еще не настроен, его мы настроем позже, а пока будем пробовать работу RADIUS AAA сервиса с помощью службы telnet.

**Шаг 9.** Так же надо указать в настройках роутеров, IP адрес сервера, который мы будем использовать в качестве RADIUS, в нашем случае это 192.168.1.2:

**radius-server host 192.168.1.2**

По идее далее надо указать порты которые RADIUS сервер использует для процесса аутентификации и аккаунтинга, но Cisco IOS укажет их в автоматическом режиме, если посмотреть получившуюся конфигурацию, мы увидим более развернутое написание данной команды:

**radius-server host 192.168.1.2 auth-port 1645 acct-port 1646**

То есть CISCO IOS сама добавила нужные порты.

**Шаг 10.** Укажем максимальное число неправильно введенных паролей, скажем равное двум. Почему двум, ну потому что если бы мы использовали для хранения учетных записей пользователей MS AD, как и следует делать, а не хранить все учётные записи на NPS RADIUS сервере, то скорее всего мы бы столкнулись с блокировкой учетной записи на 30 минут после 3-х неудачных попыток ввода пароля. Это дефолтовая настройка политики безопасностей паролей MS AD, если конечно ее не изменить для всего домена или для групп пользователей cisco вручную.

**radius-server retransmit 2**

Шаг 11. Ну и самое главное - укажем общий секрет (общую парольную фразу), которую мы задавали при настройке клиентов RADIUS в задании 2:

**radius-server key password-1**

Задание 4.

По аналогии с заданием 3 настроить роутер R2 для работы с внешним сервером RADIUS на основе Windows 2008 Server. Как для пользователей административной группы, так и для пользовательской. Аутентификация и получение соответствующих группе пользователей прав должна осуществляться успешно.

Задание 5.

Проверка работы RADIUS аутентификации на роутере R1 с помощью ВМ windows 2008 client cisco CLI. Проверка работы RADIUS аутентификации на роутере R2 с помощью роутера R1. Как для пользователей административной группы, так и для пользовательской. Аутентификация и получение соответствующих группе пользователей прав должна осуществляться успешно.

Задание 6.

Включение на роутерах R1 и R2 безопасной консоли SSH.

Если CISCO IOS поддерживает шифрование, то есть в ее названии присутствуют индекс k8 или k9, значит помимо расширенных возможностей по шифрованию трафика, можно на нем настроить безопасную консоль, то есть сервер SSH.

**Шаг 1.** Задать имя роутера:

**hostname имя\_роутера**

Оно у нас и так задано, так что пропускаем этот шаг.

**Шаг 2.** Укажем имя домена, оно необходимо для генерации связки открытого и закрытого ключей RSA:

**ip domain-name ФИО\_латиницей.ru**

***Пример:***

***ip domain-name ivanovii.ru***

**Шаг 3.** Генерируем связку открытый-закрытый ключей RSA:

**crypto key generate rsa general-keys modulus 2048**

**Шаг 4.** Включаем использование SSH сервера версии 2:

**ip ssh version 2**

**Шаг 5.** На линиях VTY у нас разрешено использование SSH и Telnet, выключим Telnet:

**transport input ssh**

**Шаг 6.**  Проверить доступность маршрутизатора R1 через SSH подключение с ВМ windows 2008 client cisco CLI.

**Шаг 7.** Проверить доступность маршрутизатора R2 через SSH подключение с R1. Для чего использовать команду:

**ssh -l имя\_пользователя ip\_адрес\_R2**

**ssh -l admin-1 10.0.0.2**

Часть 2.

VPN PPTP сервер на роутере Cisco c аутентификацией через RADIUS сервер на основе Windows Server.

На всех роутерах Cisco имеющими IOS k9 версии 12.1 и выше есть возможность запуска службы vpdn, с помощью которой можно быстро и просто организовать PPTP либо L2TP VPN сервер.

В топологи в качестве клиентов внешней сети которые подключаются к корпоративной сети через R1 маршрутизатор, посредством канала VPN-PPTP будем использовать сеть 82.137.176.0/30. В качестве внутренней сети к которой мы подключаем клиента используем адресный диапазон 10.0.0.0/27.

В данной работе в качестве клиента VPN будет использоваться ВМ на Oraсle VirtualBox - Windows 2008 Server, но можно использовать и Linux с установленным VPN-PPTP клиентом. Из коробки такой клиент установлен в Linux Ubuntu 15.04 Desktop.

Задание 7.

Настройка PPTP сервера на роутере Cisco

1. Так как для упрощения мы не пользуемся dhcp сервером, то будем раздавать IP адреса vpn pptp клиентам из пула созданного для этих целей, то есть без настройки dhcp:

**R1(config)#ip local pool VPN-PPTP-POOL** **10.0.0.3 10.0.0.30**

То есть используем все оставшиеся адресное пространство сети 10.0.0.0/27 для реализации 28 подключений VPN.

1. Включить службу vpdn, командой **vpdn enable**, в глобальном режиме конфигурации.
2. Далее надо создать и настроить VPDN-группу. Отвечающей за включение сервера VPN PPTP. Здесь мы должны разрешить маршрутизатору отвечать на входящие запросы PPTP, и указать специально созданный виртуальный шаблон (virtual template), необходимый для клонирования интерфейса и использования его в качестве основного шлюза для подключающихся клиентов:

**R1(config)#vpdn-group *VPN-PPTP***

**R1(config-vpdn)#accept-dialin**

**R1(config-vpdn-acc-in)#virtual-template *1***

**R1(config-vpdn-acc-in)#protocol pptp**

**R1(config-vpdn-acc-in)#exit**

По идее мы можем активировать сервер типа L2TP или даже PPPoE, так как служба vpdn поддерживает их все. По сути она является аналогом роли RRAS в Windows Server, если говорить о подключении виртуальных каналов. Но настройка L2TP сильно отличается от PPTP и в данной лабораторной работе не рассматривается.

1. Переходим к последнему этапу настройки: необходимо создать виртуальный шаблон, который позволит клонировать интерфейс, а так же укажет, какие параметры для подключения необходимо использовать:

Создаём интерфейс virtual-template 1:

**R1(config)#interface virtual-template *1***

Включаем инкапсуляцию PPP:

**R1(config-if)#encapsulation ppp**

Адреса для подключающихся берем из созданного ранее пула **VPN-PPTP-POOL**:

**R1(config-if)#peer default ip address pool VPN-PPTP-POOL**

Указываем внешний интерфейс роутера, к которому будут подключаться VPN клиенты:

**R1(config-if)#ip unnumbered FastEthernet0/1**

Отключаем механизм keepalive, для устранения проблем при поднятие VPN-PPTP сессии:

**R1(config-if)#no keepalive**

Включаем шифрование. Некоторые версии IOS с урезанными функциями шифрования могут не поддерживать данную команду, как собственно и PT, это печально, ибо в этом случае будет просто создаваться VPN PPTP канал, но шифрования пользовательского трафика, которое как бы и подразумевает технология VPN не будет! И хотя как будет видно позже при анализе пакетов передаваемых в VPN PPTP канале с помощью Wireshark, в явном виде трафик будет от нас скрыт, с помощью дополнительных утилит получить доступ к нему не представляется сложным.

Некоторые ISP делают так же, то есть не включают функцию шифрования PPTP и L2TP трафика, если данные от клиентов идет через собственные каналы связи. Они считаются достаточно надежными и тратить аппаратные ресурсы VPN сервера на стороне провайдера не имеет смысла, так же это позволяет увеличить производительность трансфера на клиентах провайдера, если они используют маршрутизаторы с слабым аппаратным обеспечением.

**R1(config-if)#ppp encrypt mppe auto**

Включаем все возможные виды аутентификации:

**R1(config-if)#ppp authentication pap chap ms-chap ms-chap-v2**

Примечание: хотя мы активировали все возможные виды аутентификации есть одна важная особенность связанная с работой VPN клиента в Windows. По умолчанию настройка безопасности показана на рисунке 9. Обратите внимание на пункт “Требуется шифрование данных (иначе отключаться)”. Так вот так как мы хотим непременно использовать шифрование трафика mppe, нам необходимо использовать в качестве аутентификации ms-chap-v2, если попытаться через дополнительные параметры безопасности в созданном VPN подключении использовать PAP, выдаться ошибка, рисунок 10.

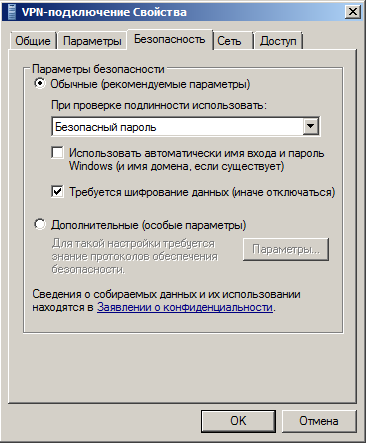


Рисунок 9

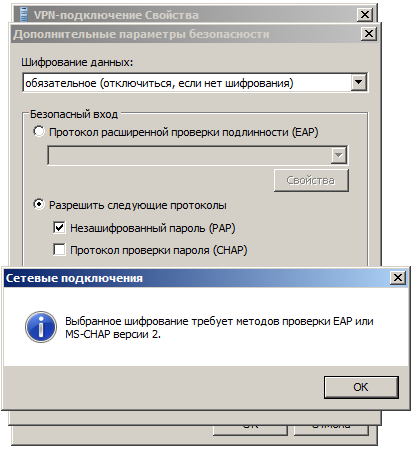


Рисунок 10

Так что по идее если нам 100% шифрование трафика, то нет особого смысла указывать все типы аутентификации, так как при них на этапе проверки подлинности произойдет сбой и VPN туннельное соединение не поднимется.

В нашем случае правильнее настроить так:

**R1(config-if)#ppp authentication ms-chap-v2**

1. Для того чтобы наш VPN-PPTP сервер мог проходить процедуру аутентификации и авторизации на RADIUS, надо в глобальном режиме конфигурации указать это двумя командами:

**aaa authentication ppp default group radius local**

**aaa authorization network default group radius local**

Первая команда позволяет пройти аутентификацию согласно настроенному для VPN политики безопасности, которую мы настроили на RADIUS сервере Windows Server.

Но если мы забудем вписать вторую команду у нас не будет происходить получение IP адреса из пула. Так как не будет согласование методов шифрования указанных на маршрутизаторе R1 и политике подключения для VPN на RADIUS сервере, а именно использование mppe.

1. Чтобы работало без RADIUS сервера необходимо просто настроить локального пользователя для доступа к VPN, с уровнем доступа 0. Создаем VPN пользователей, для упрощения, просто в локальной БД. Хотя можно создать их и на RADIUS/TACACS+ сервере, если есть такая необходимость.

Уровень привилегий задаем 0, чтобы этот пользователь случайно не смог подключится к самому маршрутизатору.

**R1(config)#username test privilege 0 password 123456**

***Обратите внимание***, что если использовать при задании пароля команду secret, чтобы пароль хранился в running-config в сложно зашифрованном виде, нам на предыдущем шаге нужно было настроить тип аутентификации только pap. Дело в том, что некоторые версии IOS неправильно работают при паролем зашифрованном как secret при всех видах аутентификации, кроме PAP. А как было сказано чуть выше при использовании аутентификации PAP невозможно настроить Windows VPN клиент для поднятия туннеля с зашифрованным трафиком с помощью типа шифрования mppe. По этой причине пароль резервного локальный логина root, на роутерах, задается командой password, а шифруется легким типом шифрования с помощью сервиса service password-encryption.

Задание 8.

Настройка пользователей VPN и политики сети на RADIUS сервере Windows Server

1) Зайти на ВМ windows 2008 RADIUS Server открыть оснастку управления локальными пользователями и создать пользователя vpn-user. Для него создать группу vpn-group и добавить пользователя в нее.

2) Открыть оснастку “Сервер политик сети” и создать новую политику сети с названием VPN. В окне выбора условий подключения, выбрать группу vpn-group. В окне в качестве ограничений, методы проверки подлинности оставить по умолчанию (для дефолтовой настройке vpn клиента в windows нужна аутентификация ms-chap-v2). В настройка шифрования убрать пункт “Без шифрования”. Все остальные пункты оставить по умолчанию.

Задание 9.

Настройка клиента VPN-PPTP

1. Настроить VPN подключение на ВМ windows 2008 client cisco CLI, в качестве IP адреса сервера, указать IP адрес Fa0/0 интерфейса роутера R1, логин и пароль согласно предыдущему заданию.
2. Установить VPN-PPTP канал связи.
3. Проверить доступность хостов PC1, PC2 и PC3. Разумеется связь должна быть успешной.
4. Подключится по SSH к роутеру R2.