Министерство образования Республики Беларусь
Учреждение образования «Полоцкий государственный университет»

Факультет информационных технологий
Кафедра технологий программирования

Методические указания
к выполнению лабораторной работы №8

по дисциплине «**Компьютерные системы и сети**»
для специальности 1-40 01 01 Программное обеспечение информационных технологий

на тему «**Настройка VPN-клиента и VPN-сервера на Linux Ubuntu Server**»

Новополоцк, 2018 г.

Название: «Настройка VPN-клиента и VPN-сервера на Linux Ubuntu Server».

Цель работы: Изучить настройки службы PPTPD и VPN. Настроить VPN-клиента и VPN-сервера на Linux Ubuntu Server.

Теоретическая часть

VPN (англ. Virtual Private Network – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений).

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети – PPTP, причём используемую зачастую не для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол – IP (такой способ использует реализация PPTP – Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» на постсоветском пространстве для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в Сети.

Ход работы

Настройка VPN-сервера

Установка пакета pptpd выполняется командой:

apt-get install pptpd

Настройка службы выполняется путем редактирования двух файлов:

/etc/pptpd.conf

/etc/ppp/pptpd-options

Файл **pptpd.conf** описывает настройки и содержит ссылку на файл с опциями **/etc/ppp/pptpd-options:**

option *файл_опций*

Используются следующие основные опции:

Для включения широковещательного режима (отправляется клиентам все широковещательные пакеты, принятые на внутреннем интерфейсе сервера) применяется опция ***bcrelay внутренний_интерфейс.***

localip указание_ip – описывает один или несколько IP-адресов для использования на локальном конце туннелей PPP-каналов между сервером и клиентом. Если задан только один адрес, этот адрес используется для всех клиентов. Иначе, должен быть задан один адрес на каждого клиента, а если свободные адреса отсутствуют, то любые новые клиенты будут отброшены.

remoteip указание_ip – список IP-адресов для назначения удалённым PPTP-клиентам. Каждый подключенный клиент должен иметь разный адрес, поэтому в списке должно быть по меньшей мере столько адресов, сколько одновременных клиентов. Предпочтителен некоторый запас, поскольку вы не сможете изменить этот список без перезапуска pptpd. Если пул IP-адресов будет исчерпан, в syslog(3) будет отправлено предупреждение.

Вышеописанные указания (для опций localip и remoteip) могут быть списком IP-адресов (например, 192.168.0.2, 192.168.0.3), диапазоном (например, 192.168.0.1-254 или 192.168.0-255.2) или их сочетанием (например, 192.168.0.2, 192.168.0.5-8). Правильными парами могут быть (в зависимости от использования VPN):

localip 192.168.0.1
remoteip 192.168.0.2-254
или
localip 192.168.1.2-254
remoteip 192.168.0.2-254

В файле **/etc/ppp/pptpd-options** используются следующие настройки:

auth – требовать у партнёра подтвердить свою подлинность перед разрешением отправки и приёма сетевых пакетов. Если система имеет маршрут по умолчанию, то эта опция используется по умолчанию. Если не указана ни эта опция, ни опция noauth, pppd разрешит партнёру использовать только такой IP-адреса, к которому система на данный момент не имеет маршрута.

name имя – использовать при аутентификации name в качестве имени локальной системы. Это привилегированная опция. При аутентификации pppd будет использовать секрет из той строки в файле секретов, у которой во втором поле указано имя name. Если имя, заданное этой опцией, не было заменено с помощью опции user, то оно будет отправлено партнёру для аутентификации локальной системы (Использовать имя = pptpd).

domain имя_домена – определяет имя домена, в который включается клиент.

refuse-chap – при использовании этой опции pppd не согласится аутентифицировать себя по протоколу CHAP.

refuse-mschap – при использовании этой опции pppd не согласится аутентифицировать себя по протоколу MS-CHAP.

refuse-mschap-v2 – при использовании этой опции pppd не согласится аутентифицировать себя по протоколу MS-CHAPv2.

refuse-eap – при использовании этой опции pppd не согласится аутентифицировать себя по протоколу EAP.

refuse-pap – при использовании этой опции pppd не согласится аутентифицировать себя по протоколу PAP.

require-chap – требовать партнёра аутентифицировать себя используя аутентификацию CHAP

Необходимо выставить требование аутентификации по протоколу **mschap-v2.**

ms-dns ip_адрес – если pppd работает в качестве сервера для клиентов Microsoft Windows, эта опция позволяет pppd предоставлять клиентам один или два адреса DNS (серверов доменных имён). Первый экземпляр этой опции указывает адрес первичного DNS; второй экземпляр (если задан) указывает адрес вторичного DNS. (Эта опция в некоторых старых версиях pppd имела имя dns-addr.)

ms-wins ip_адрес – если pppd работает в качестве сервера для клиентов Microsoft Windows или Samba, эта опция позволяет предоставлять клиентам адреса одного или двух серверов WINS (Winows Internet Name Services). Первый экземпляр этой опции указывает адрес первичного WINS; второй экземпляр (если задан) указывает адрес вторичного WINS.

proxyarp – запись о клиенте в таблицу ARP.

nodefaultroute – запрещает замещение маршрута по умолчанию на клиенте.

lock – указывает, что pppd должен создать для последовательного устройства файл блокировки в стиле UUCP, чтобы быть уверенным в эксклюзивном доступе. По умолчанию pppd не создаёт файл блокировки.

logfile путь_к_файлу лога – путь к файлу лога.

Более полный список настроек содержится в файле «pppd Команды системного администрирования.mht».

Перезапуск демона pptpd производится командой:

service pptpd restart

Список пользователей VPN храниться в файле **/etc/ppp/chap-secrets** в следующем виде:

имя_пользователя сервер пароль выдаваемый_ip

сервер определяет с какого удаленного сервера выполняется подключение (можно заменить на *).

выдаваемый_ip определяет ip-адрес который будет выдаваться данному клиенту (можно заменить на *).

Разрешение маршрутизации

Для разрешения переадресации пакетов необходимо заменить содержимое файла **/proc/sys/net/ipv4/ip_forward** на «1».

Практическая часть

Содержание задания

В рамках задания требуется настроить службу DHCP на две подсети. Подключить два клиента, один Windows, второй Linux, находящиеся в разных подсетях. Настроить PPTPD и VPN-сервера. По результатам работы составить отчет.

Порядок выполнения работы

1 Ознакомиться с теоретической частью.

2 Настроить DHCP-сервер на две подсети, с различными ip-адресами подсетей (*последняя цифра в IP-адресе сервера – это номер студента в списке группы*).

3 Настроить PPTPD-сервер.

4 Настроить VPN-клиент на Windows.

5 Проверить работоспособность (клиент Windows должен «увидеть» клиента Linux, находящийся в другой подсети).

6 Составить отчёт о проделанной работе.

7 Показать выполненную работу и отчёт преподавателю.

Содержание отчёта

1 Титульный лист.

2 Цель работы.

3 Краткие теоретические сведения.

4 Основные результаты по каждому пункту хода выполнения работы.

5 Описание проверок функционирования служб со скриншотами результатов.

6 Выводы о проделанной работе.

Защита работ проводится индивидуально.