Документация программного обеспечения «сервер доступа к локальной сети по L2TP (L2TP Network Server)», предоставленного для экспертной проверки

Установка программного обеспечения

Содержание

1. Общие положения

В данном Документе приведено описание процедуры установки ПО **«L2TP Network Server, сервер доступа к локальной сети по L2TP (на базе ACCEL-PPP)»,** (далее - **L2TP сервер**).

Важно! Пользование данной инструкцией подразумевает, что используется аппаратный сервер, с предустановленным Proxmox VE на операционную систему Debian (версия 11) со стандартным набором утилит.

В системе Proxmox должна быть создана виртуальная машина (ВМ) для установки ПО L2TP сервера.

Минимальные требования, предъявляемые к машинным ресурсам для отдельной виртуальной машины LNS:

Процессор	Оперативная память	Жесткий диск
Минимум 2 ядра. Частота минимум: От 2 ГГц на ядро	Тип не ниже DDR3. Объем не менее: 2 гигабайт	Тип HDD/SSD. Объем не менее: 10 Гбайт

2. Установка L2TP-сервера

ПО представляет собой VPN/IPoE сервер для Linux. На его базе будет функционировать ВМ сервер L2TP.

2.1 Установка ПО L2TP-сервера

Установка подразумевается на ВМ с ОС Debian (версия 11).

Перед компиляцией и сборкой пакета необходимо установить необходимые зависимости командой:

```
apt-get install -y build-essential cmake gcc linux-headers-`uname -r` libpcre3-dev libssl-dev liblua5.1-0-dev
```

Где:

- cmake — система с открытым исходным кодом, управляющая процессом сборки
- gcc — Коллекция компиляторов GNU (GCC) — система компиляторов.
- linux-headers-`uname -r` - исходный код текущего установочного ядра linux, необходимого для сборки модулей ipoe и vlan_mon. Если не нужны эти модули, можно их не устанавливать.
- libpcre3-dev - исходный код pcre lib, accel-ppp нужен для использования reg-выражения
- libssl-dev - исходный код pcre lib, accel-ppp нужен для использования регулярных выражений
- liblua5.1-0-dev - это необходимо для создания пользовательского имени пользователя (IPoE) из пакета. Скрипт написан на языке lua.

После установки зависимостей загрузить исходный код accel-ppp с предоставленного внешнего диска.

На диске должны быть представлены исходные коды в архиве **l2tp-server.tgz**

Разархивировать архив дистрибутива на ВМ с ОС Debian 11. Для этого

1. Создать нужную папку:

```
mkdir /opt/accel-ppp-code
```

2. Перейти в этот каталог

```
cd /opt/accel-ppp-code
```

3. Ввести команду разархивации напрямую с CD (нужно учесть, что привод должен быть монтирован в ОС):

```
tar zxvf /CD_path/l2tp-server.tgz
```

Где ***CD_path*** – путь к CD-приводу.

Создать каталог для исходного кода сборки и перейти в этот каталог.

```
mkdir /opt/accel-ppp-code/build
cd /opt/accel-ppp-code/build/
```

Для построения кода следует установить следующие параметры командой:

```
cmake -DBUILD_IPOE_DRIVER=TRUE -DBUILD_VLAN_MON_DRIVER=TRUE -DCMAKE_INSTALL_PREFIX=/usr -DKDIR=/usr/src/linux-headers-`uname -r` -DLUA=TRUE -DCPACK_TYPE=Debian11 ..
```

Где:

- -DBUILD_IPOE_DRIVER=TRUE включает модуль IPoE. Этот модуль необходим, требуется использовать accel-ppp в качестве общего интерфейса.
- -DBUILD_VLAN_MON_DRIVER=TRUE включить модуль мониторинга vlan. Если необходимо автоматически создавать vlan при анализе заголовков IP с регулярным выражением, установленным в файле конфигурации accel-ppp. (Доступно для IPoE и PPPoE).
- -DKDIR=/usr/src/linux-headers-`uname -r` устанавливает путь к исходному коду ядра Linux. Нужен только для сборки IPOE, VLAN-MON.
- -DCMAKE_INSTALL_PREFIX=/usr путь для установки исполняемого кода. Если собирается пакет DEB, не рекомендуется изменять это.
- -DCPACK_TYPE=Debian11 это аргументы для сборки пакета DEB для Debian 11.

Примечание*: символы .. устанавливают путь к исходному коду accel-ppp, а не удаляют его! Символы можно заменить полным путем к accel-ppp-code, например, /opt/accel-ppp-code/*

Далее скомпилировать командой:

```
make
```

Создать DEB-пакет:

```
cpack -G DEB
```

Установить пакет:

```
dpkg -i accel-ppp.deb
```

Если пакет успешно установлен, переименовать файл конфигурации в accel-ppp.conf:

```
mv /etc/accel-ppp.conf.dist /etc/accel-ppp.conf
```

Отредактировать accel-ppp.conf при необходимости (см. Приложение 1).

После установки следует разрешить запуск accel-ppp при старте системы командой:

```
systemctl enable accel-ppp
```

2.2 Системные настройки

После установки выполнить рекомендации по включению пересылки пакетов и увеличению размера кэша ARP, изложенные ниже.

Чтобы включить пересылку пакетов, нужно отредактировать **/etc/sysctl.conf** и добавить или раскомментировать следующее:

```
net.ipv4.ip_forward=1
```

Установить следующие значения кэша ARP в **/etc/sysctl.conf**:

```
net.ipv4.neigh.default.gc_thresh1 = 4096
net.ipv4.neigh.default.gc_thresh2 = 8192
net.ipv4.neigh.default.gc_thresh3 = 12288
```

Чтобы применить установленные значения, ввести команду:

```
sysctl -p
```

3. Сетевые настройки сервера

В настройках подразумевается, что на одной ВМ присутствует один оператор. В данной инструкции приведены настройки для одного оператора. Перед запуском сервера ACCEL следует выполнить изложенный ниже ряд шагов.

3.1 Установка alias на интерфейс

ens18 **192.168.254.132** - основной интерфейс

ens18.0 **172.0.0.3/32**

Важно! *Интерфейсы и адресация, помеченные* ***красным шрифтом****, на каждом разворачиваемом сервере должны отличаться от приведенных здесь и соответствовать актуальным проектным значениям.*

Для этого отредактировать файл интерфейсов **/etc/network/interfaces**, который должен выглядеть, как приведено в примере ниже:

```
# The loopback network interface
```

```
auto lo ens18
iface lo inet loopback
auto ens18
allow-hotplug ens18
iface ens18 inet static
        address 192.168.254.132/24
        gateway 192.168.254.1

# test LNS
auto ens18:0
iface ens18:0 inet static
        address 172.0.0.3
        netmask 255.255.255.255
```

3.2 Установка и настройка брандмауэра

Установить пакет iptables:

```
# apt-get install
    iptables
        # update-alternatives --set iptables /usr/sbin/iptables-legacy
```

Отредактировать файл **/etc/rc.local** и внести строки:

```
#!/bin/sh

/sbin/iptables -F

/sbin/iptables -A FORWARD -i ppp+ -p all -d 1.2.3.0/24 -j ACCEPT
/sbin/iptables -A FORWARD  -i ppp+ -p all -d 192.168.176.0/28 -j ACCEPT
/sbin/iptables -A FORWARD  -i ppp+ -p all -j DROP
```

После редактирования следует ввести команду для разрешения доступа к файлу **/etc/rc.local**:

```
chmod 755 /etc/rc.local
```

Следует разрешить запуск *rc.local* при старте системы командой:

```
systemctl enable rc-local
```

3.3 Установка FRR OSPF

Установить служебную программу командной строки cURL командой:

apt-get install curl

Для работы cURL установить необходимый пакет apt-transport-https, позволяющий получить доступ к apt репозиториям через https протокол, командой:

apt-get install apt-transport-https

После этих действий установить FRR. Процесс установки пакета FRR указана на сайте: https://deb.frrouting.org/

3.4 Настройка конфигурационных файлов FRR

Для окончательных настроек в файле **/etc/frr/daemons** следует оставить **ospfd=yes**, все остальные параметры **no.**

Файл **/etc/frr/vtysh.conf** оставить незаполненным.

В файл **/etc/frr/frr.conf** должно быть вписано следующее:

```
frr version 8.0.1
frr defaults traditional
hostname Megafon
log syslog informational
no ipv6 forwarding
!
password zebra
enable password zebra
!
router ospf
 ospf router-id 192.168.254.132
 redistribute kernel
 redistribute connected
 network 192.168.254.0/24 area 0.0.0.1
 exit
!
line vty
 exec-timeout 0 0
!
```

3.5 Конфигурация L2TP-сервера

Следующим шагом является приведение конфигурационного файла ACCEL-PPP /etc/accel-ppp.conf к виду, указанному в Приложении 1 к данной Инструкции.

3.6 Запуск сервера

После всех настроек, следует запустить сервер командой:

/etc/init.d/accel-ppp start

Далее необходимо перезагрузить ВМ.

Проверка корректной работы сервера приведена в п.п. 4.2.

4. Первичная проверка работоспособности

Пункты проверки должны быть пройдены один раз после завершения всех вышеуказанных действий в Инструкции и еще один раз после контрольной перезагрузки сервера.

4.1 Проверка состояния UDP-соединений

UDP-соединения проверяются с помощью утилиты netstat командой:

 # netstat -lpun

Корректный вывод (пример):

```
active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address   Foreign Address   State   PID/Program name
udp        0      0 172.0.0.1:1701          0.0.0.0:*
                     1801/accel-pppd
udp        0      0 10.0.0.1:3799           0.0.0.0:*
                     1801/accel-pppd
```

4.2 Поиск работающего процесса accel

Поиск осуществляется с помощью команды:

/etc# ps auxww|grep accel

Корректный вывод (пример):

```
root      1801  0.0  0.0  88792  5520 ?        Ssl  09:30   0:00 /usr/sbin/accel-pppd -d -p
/var/run/accel-pppd.pid -c /etc/accel-ppp.conf
```

4.3 Проверка логирования

Убедиться, что в логфайлах **/var/log/accel-ppp/core.log** и **/var/log/accel-ppp/emerg.log** отсутствуют записи об ошибках.

4.4 Проверка работы брандмауэра

Вывести цепочки брандмауэра командой:

```
iptables –nvL
```

Корректный вывод (пример):

```
Chain INPUT (policy ACCEPT 3 packets, 879 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  ppp+   *       0.0.0.0/0            1.2.3.0/24
    0     0 ACCEPT     all  --  ppp+   *       0.0.0.0/0            192.168.176.0/28
    0     0 DROP       all  --  ppp+   *       0.0.0.0/0           0.0.0.0/0

Chain OUTPUT (policy ACCEPT 3 packets, 156 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Приложение 1

Конфигурационный файл /etc/accel-ppp.conf (пример)

```
[modules]
log_file
l2tp
auth_chap_md5
auth_pap
radius
ipset_manage

[core]
log-error=/var/log/accel-ppp/core.log
thread-count=4

[common]
check-ip=0

[ppp]
verbose=0
min-mtu=1280
mtu=1480
mru=1480
ccp=0
accomp=deny
pcomp=deny
mppe=prefer
ipv4=require
ipv6=deny
lcp-echo-failure=3
lcp-echo-timeout=120
unit-cache=10000
unit-preallocate=1

[l2tp]
verbose=0
bind=172.0.0.3
dictionary=/usr/share/accel-ppp/l2tp/dictionary
host-name=test.rors
hide-avps=0
avp_permissive=1
dataseq=allow
ppp-max-mtu=1492
secret=password
hello-interval=120
rtimeout=5
reorder-timeout=100

[dns]
dns1=8.8.8.8

[radius]
verbose=0
dictionary=/usr/share/accel-ppp/radius/dictionary
nas-ip-address=192.168.254.132
gw-ip-address=172.0.0.3
server=192.168.254.109,password,auth-port=1812,acct-port=1813,req-limit=0,fail-timeout=0,max-
fail=10,weight=1
dae-server=192.168.254.132:3799,testing123
timeout=5
max-try=3
acct-timeout=120
sid-in-auth=1
```

```
nas-identifier=LNSTest

[auth]
any-login=0
noauth=0

[authproxy]
auth=1

[log]
log-file=/var/log/accel-ppp/accel-ppp.log
log-emerg=/var/log/accel-ppp/emerg.log
log-fail-file=/var/log/accel-ppp/auth-fail.log
copy=1
level=2

[client-ip-range]
disable

[cli]
verbose=1
tcp=127.0.0.1:2001
```