УДК: 004.7.056.53

РАЗВЕРТЫВАНИЕ СЕРВЕРА УДАЛЕННОГО ДОСТУПА PPTP НА БАЗЕ ЭВМ УНИВЕРСАЛЬНОГО НАЗНАЧЕНИЯ И ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX FEDORA CORE

А. Ю. Телков, Н. А. Семенов

Воронежский государственный университет

Поступила в редакцию 20.03.2012 г.

Аннотация. Рассмотрена задача организации безопасного удаленного подключения сотрудников к локальной сети предприятия через Интернет. Описан процесс установки и конфигурирования сервера удаленного доступа на базе ЭВМ универсального назначения и операционной системы Linux Fedora Core, использующего протоколы PPTP (Point-to-Point Tunneling Protocol) и MPPE-128 (Microsoft Point-to-Point Encryption) для шифрования данных и протокол MS-CHAPv2 для аутентификации пользователей. Рассмотрены особенности настройки модуля iptables при решении задач маршрутизации и транзитной передачи трафика в различных направлениях.

Ключевые слова: сервер удаленного доступа, PPTP, iptables, файрвол, Linux.

Annotation. The problem of implementation of safe remote network access to company's local network via the Internet for company's employees is considered. The installation and configuration processes of general-purpose host-based Network Access Server, driven by Linux Fedora Core operating system, utilizing PPTP and MPPE-128 protocols for data encryption and MS-CHAPv2 protocol for user authentification, are described. Features of iptables module configuration for solving tasks of traffic transition in different directions were reviewed.

Keywords: network access server, PPTP, iptables, firewall, Linux.

ВВЕДЕНИЕ

Традиционной задачей обеспечения доступа к ресурсам является задача подключения «удаленных» и «домашних» пользователей, находящихся вне локальной сети центрального офиса предприятия, к ресурсам этой сети.

Задача создания удаленного соединения на практике может решаться с применением аппаратных средств [1]. Однако, в ряде случаев, развертывание сервера удаленного доступа удобно произвести на ЭВМ универсального назначения. Это относится к ситуациям, когда в организации уже имеется Linux сервер, выполняющий сетевые функции, например, прокси-сервера, файлового сервера, сервера резервного копирования, сервера печати [2]. Немалым преимуществом создания сервера удаленного доступа на базе многофункциональной ЭВМ с платформой Linux является независимость стоимости маршрутизатора от количества необходимых подключений удаленного доступа. Стоимость аппаратных маршрутизаторов, как правило, растет с увеличением максимального числа подключений удаленного доступа, которые те могут обеспечить.

Отметим, что функции сервера удаленного доступа на практике зачастую реализуют на сетевом устройстве, выполняющем функции обычного маршрутизатора, поэтому вопрос создания сервера удаленного доступа уместно рассматривать вместе с вопросом реализации обычного маршрутизатора на этом же устройстве. Реализация связки маршрутизатор + сервер удаленного доступа на Linux наталкивается на определенные трудности (неработоспособность протоколов исходящих из локальной сети подключений по протоколам PPTP и FTP в Интернет, недоступность узлов локальной сети удаленным пользователям после подключения и авторизации на сервере удаленного доступа и др.). Для исключения указанных трудностей необходимо производить дополнительную настройку конфигурационных файлов сервера, о которой пойдет речь ниже.

Таким образом, основными задачами данной работы являются:

1. Описание процесса сборки Linux сервера и настройки на нем базовых правил маршрути-

зации iptables, обеспечивающих, с одной стороны, возможность работы пользователей локальной сети предприятия в сети Интернет, и, с другой стороны, возможность подключения к Linux серверу извне по протоколу PPTP (Point-to-Point Tunneling Protocol).

2. Описание процесса установки и настройки на Linux сервере роли PPTP сервера на основе пакетов PPP и PoPToP, описание создания рабочей конфигурации для процессов, соответствующих этим пакетам.

3.Обсуждение реализации типовых задач, связанных с ограничением средствами Linux сервера числа возможных протоколов, работающих между локальной сетью и сетью Интернет и замечаний относительно конфигураций соседнего с Linux сервером сетевого оборудования.

2. НАСТРОЙКА МАРШРУТИЗАЦИИ ПАКЕТОВ НА СЕРВЕРЕ LINUX

Будем считать, что наш Linux сервер изолирован от сети Интернет (WAN) пакетным маршрутизатором, который реализует функции трансляции сетевых адресов (NAT), функции трансляции (проброса) портов и базовые функции защиты (межсетевого экранирования), то есть является так называемым пакетным фильтром. Linux-сервер подключен к указанному маршрутизатору через сетевой интерфейс Eth1. Кроме того, будем считать, что интерфейс Eth0 Linux сервера подключен к коммутатору локальной сети. Допускается, что локальная сеть может быть сегментирована, изолирована от Linux сервера дополнительным сетевым оборудованием, мы эти варианты не рассматриваем, работу с ними нетрудно построить, основываясь на обсуждаемом варианте сетевой топологии.

Процесс установки операционной системы Linux рассмотрен в [3]. Особенности установки, связанные с рассматриваемой задачей, практически отсутствуют. Далее рассмотрим настройку [4] процесса маршрутизации на Linux сервере средствами пакета iptables.

Предполагается, что перечисленные ниже команды набираются с клавиатуры в консоли с правами суперпользователя (root):

```
# iptables -F
# iptables -t nat -F
# iptables -P INPUT ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD DROP
# export LAN=eth0
# export WAN=eth1
# iptables -I INPUT 1 -i ${LAN} -j ACCEPT
# iptables -I INPUT 1 -i lo -j ACCEPT
# iptables -A INPUT -p UDP --dport bootps -i ! ${LAN} -j REJECT
# iptables -A INPUT -p UDP --dport domain -i ! ${LAN} -j REJECT
```

Разрешаем доступ к ssh-серверу из сети Интернет:

```
# iptables -A INPUT -p TCP --dport ssh -i ${WAN} -j ACCEPT
```

Разрешаем доступ к pptp-серверу из сети Интернет:

```
# iptables -A INPUT -p TCP --dport 1723 -i ${WAN} -j ACCEPT
```

Разрешаем работу протокола GRE на всех интерфейсах:

```
# iptables -A INPUT -p gre -j ACCEPT
```

Отбрасываем все TCP/UDP-пакеты, обращающиеся к привилегированным портам:

```
# iptables -A INPUT -p TCP -i ! ${LAN} -d 0/0 --dport 0:1023 -j DROP
# iptables -A INPUT -p UDP -i ! ${LAN} -d 0/0 --dport 0:1023 -j DROP
# iptables -I FORWARD -i ${LAN} -d 192.168.0.0/255.255.255.0 -j DROP
# iptables -A FORWARD -i ${LAN} -s 192.168.0.0/255.255.255.0 -j ACCEPT
# iptables -A FORWARD -i ${WAN} -d 192.168.0.0/255.255.255.0 -j ACCEPT
# iptables -t nat -A POSTROUTING -o ${WAN} -j MASQUERADE
# echo 1 > /proc/sys/net/ipv4/ip_forward
# for f in /proc/sys/net/ipv4/conf/*/rp_filter ; do echo 1 > $f ; done
# /etc/init.d/iptables save
```

Указываем значение переменной, отвечающей за включение маршрутизации в системном файле:

```
# nano /etc/sysctl.conf
```

Добавим строки:

```
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
```

Добавляем iptables в список модулей, загружаемых операционной системой при старте маршрутизатора:

```
# chkconfig iptables on
```

На этом завершается начальная настройка маршрутизатора iptables на Linux сервере. На этом этапе при правильных настройках сетевого оборудования и рабочих станций пользо-

ватели локальной сети могут работать в сети Интернет.

3. НАСТРОЙКА УДАЛЕННОГО ДОСТУПА НА СЕРВЕРЕ LINUX

Для реализации возможности удаленного доступа на linux-сервер необходимо установить соответствующее программное обеспечение. Нами использовалась операционная система Linux Fedora Core 14, пакеты ppp-2.4.5-17.0.fc14.i686.rpm и pptpd-1.3.4-2.fc14.i686.rpm, которые устанавливались в систему в графическом режиме. После установки производились изменения в конфигурационных файлах, отвечающих за работу PPP (Point-to-Point Protocol) сервера и его расширения - протокола PPTP (Point-to-Point Tunneling Protocol).

Указываем, что настройки pptpd находятся в файле /etc/ppp/options.pptpd:

option /etc/ppp/options.pptpd

Включаем запись событий процессов pppd и pptpd в журнал /var/log/messages:

debug

TAG: logwtmp

logwtmp

Ограничиваем число одновременных соединений VPN значением 100:

connections 100

Определяем локальный адрес нашего VPN-сервера и диапазон выдачи сетевых адресов VPN-клиентам:

localip 10.11.12.1

remoteip 10.11.12.11-100,10.11.12.101

Изменяем содержимое файла /etc/ppp/pptpd.conf на следующее:

имя процесса, который будет производить аутентификацию:

name pptpd

Требуем ms-chap-v2 аутентификацию, все остальное отклоняем:

refuse-pap

refuse-chap

refuse-mschap

require-mschap-v2

Требуем шифрование mppe-128:

require-mppe-128

Сети и маршрутизация: предполагаем, что наш маршрутизатор может пересылать DNS запросы вышестоящим серверам, поэтому указываем его в качестве DNS сервера.

ms-dns 10.11.12.1

Считаем, что в локальной сети у нас есть wins сервер с адресом 192.168.0.25:

ms-wins 192.168.0.25

Включаем ARP (Address Resolution Protocol):

proxyarp

Включаем журнализацию подключений и отключений удаленного доступа:

debug

Для устойчивой связи на плохих каналах связи уменьшаем размер пакета (< 1500):

lock

mtu 1400

mru 1400

Отключаем использование BSD-Compress сжатия:

nobsdcomp

Выключаем Van Jacobson сжатие (нужно для некоторых сетей Windows 9x/ME/XP):

novj

novjccomp

И, наконец, опишем, кто может подключаться к нашему Linux-серверу, и какие адреса сервер при этом будет выдавать своим клиентам. Укажем, что это может быть пользователь User1 с паролем User1_strongpassword. Для этого приведем конфигурационный файл /etc/ppp/chap-secrets к виду, приведенному ниже:

Secrets for authentication using CHAP

client server secret IP addresses

User1 pptpd User1_strongpass 10.11.12.21

Добавляем в список модулей, загружаемых операционной системой при старте PPTP-сервер:

chkconfig pptpd on

На этом завершается этап настройки сервера удаленного доступа PPTP на Linux-сервере. При правильных настройках сетевого оборудования удаленные пользователи могут на своих рабочих станциях настроить VPN подключение к этому серверу удаленного доступа, например, средствами операционных систем. [5]

4. ТОНКАЯ НАСТРОЙКА МАРШРУТИЗАЦИИ ПАКЕТОВ НА СЕРВЕРЕ LINUX

На этом этапе, без дополнительной настройки конфигурационных файлов процессов, обеспечивающих требуемый функционал, мы будем иметь следующие промежуточные результаты:

1. Пользователи локальной сети могут работать в сети Интернет по протоколам HTTP, DNS, POP3, SMTP и пр.

2. Не работает загрузка и выгрузка данных в локальную сеть/из локальной сети в сеть Интернет по протоколу FTP.

3. Исходящие подключения из локальной сети к серверам в Интернет по протоколу PPTP невозможны.

Для преодоления указанных недостатков следует подключить дополнительные модули и отредактировать конфигурационные файлы.

Во-первых, отредактировать конфигурационный файл /etc/sysconfig/iptables-config, а именно модифицировать строку, содержащую IPTABLES_MODULES=" ", привести ее к виду:

IPTABLES_MODULES="ip_conntrack_ftp ip_nat_ftp ip_conntrack_pptp ip_nat_pptp";

Во-вторых, отредактировать конфигурационный файл /etc/sysconfig/iptables, добавить в него правила, разрешающие маршрутизацию пакетов между удаленными VPN-клиентами и LAN и между удаленными VPN-клиентами и WAN. Поскольку в данной работе процесс начальной конфигурации iptables уже описывался выше, мы приведем только конечный вид конфигурационного файла /etc/sysconfig/iptables,который будет таким:

```
# Generated by iptables-save v1.4.9 on Mon Aug 15 15:06:42 2011
*nat
:PREROUTING ACCEPT [27:4266]
:OUTPUT ACCEPT [207:12738]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -o eth1 -j MASQUERADE
COMMIT
# Completed on Mon Aug 15 15:06:42 2011
# Generated by iptables-save v1.4.9 on Mon Aug 15 15:06:42 2011
*filter
:INPUT ACCEPT [1293:896272]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [1287:149133]
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth0 -j ACCEPT
-A INPUT ! -i eth0 -p udp -m udp --dport 67 -j REJECT --reject-with icmp-port-unreachable
-A INPUT ! -i eth0 -p udp -m udp --dport 53 -j REJECT --reject-with icmp-port-unreachable
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 1723 -j ACCEPT
-A INPUT -i eth1 -p gre -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 0:1023 -j DROP
-A INPUT -i eth0 -p udp -m udp --dport 0:1023 -j DROP
-A FORWARD -d 192.168.0.0/24 -i eth0 -j DROP
-A FORWARD -s 192.168.0.0/24 -i eth0 -j ACCEPT
-A FORWARD -d 192.168.0.0/24 -i eth1 -j ACCEPT
-A FORWARD -s 10.11.12.0/24 -d 192.168.0.0/24 -j ACCEPT
-A FORWARD -s 192.168.0.0/24 -d 10.11.12.0/24 -j ACCEPT
-A FORWARD -s 10.11.12.0/24 -j ACCEPT
-A FORWARD -d 10.11.12.0/24 -j ACCEPT
COMMIT
# Completed on Mon Aug 15 15:06:42 2011
```

Современные системы безопасного удаленного доступа должны обладать способностью журнализации событий, связанных с их работой. Отметим, что в нашем случае такая возможность обеспечивается. Факты успешных (и неуспешных) входов в систему записываются в файл /var/log/messages в виде подобном показанному ниже:

```
Aug 15 17:25:21 LXLAB pptpd[2689]: CTRL: Client 192.168.0.110 control connection started
Aug 15 17:25:21 LXLAB pptpd[2689]: CTRL: Starting call (launching pppd, opening GRE)
Aug 15 17:25:21 LXLAB pppd[2690]: Plugin /usr/lib/pptpd/pptpd-logwtmp.so loaded.
Aug 15 17:25:21 LXLAB pppd[2690]: pptpd-logwtmp: $Version$
Aug 15 17:25:21 LXLAB pppd[2690]: pppd 2.4.5 started by root, uid 0
Aug 15 17:25:21 LXLAB pppd[2690]: Using interface ppp0
Aug 15 17:25:21 LXLAB pppd[2690]: Connect: ppp0 <--> /dev/pts/0
Aug 15 17:25:24 LXLAB pptpd[2689]: CTRL: Ignored a SET LINK INFO packet with real ACCMs!
Aug 15 17:25:24 LXLAB pppd[2690]: Unsupported protocol 'IPv6 Control Protocol' (0x8057) received
Aug 15 17:25:24 LXLAB kernel: [ 110.245799] PPP MPPE Compression module registered
Aug 15 17:25:24 LXLAB pppd[2690]: MPPE 128-bit stateless compression enabled
```

Aug 15 17:25:25 LXLAB pppd[2690]: Cannot determine ethernet address for proxy ARP

Aug 15 17:25:25 LXLAB pppd[2690]: local IP address 10.11.12.1

Aug 15 17:25:25 LXLAB pppd[2690]: remote IP address 10.11.12.21

Aug 15 17:25:25 LXLAB pppd[2690]: pptpd-logwtmp.so ip-up ppp0 User1 192.168.0.110

Aug 15 17:26:15 LXLAB pulseaudio[2391]: ratelimit.c: 7 events suppressed

Aug 15 17:28:20 LXLAB pppd[2690]: pptpd-logwtmp.so ip-down ppp0

Aug 15 17:28:20 LXLAB pppd[2690]: Connect time 3.0 minutes.

Aug 15 17:28:20 LXLAB pppd[2690]: Sent 0 bytes, received 141776 bytes.

Aug 15 17:28:20 LXLAB pppd[2690]: Modem hangup

Aug 15 17:28:20 LXLAB pppd[2690]: Connection terminated.

Содержимое данного фрагмента показывает, что время попытки входа, факт входа, время соединения, IP адрес, ID удаленного пользователя записываются в журнал событий.

ЗАКЛЮЧЕНИЕ

Таким образом, рассмотрена задача организации безопасного удаленного подключения сотрудников предприятия к локальной сети предприятия через Интернет. Описан процесс установки и конфигурирования сервера удаленного доступа на базе ЭВМ универсального назначения и операционной системы Linux Fedora Core, использующего протоколы PPTP (Point-to-Point Tunneling Protocol) и MPPE-128 для шифрования данных и протокол MS-CHAPv2 для аутентификации пользователей. Сделан акцент на конфигурации маршрутизатора iptables, работающего на том же сервере, благодаря которой возможны подключения из локальной сети предприятия к удаленным PPTP серверам, находящимся в сети Интернет.

СПИСОК ЛИТЕРАТУРЫ

1. *Браун С.* Виртуальные частные сети VPN / С. Браун . – М.: Лори, 2001. – 480 с.

2. *Телков А. Ю.* Сборка маршрутизатора с функцией прокси-сервера на аппаратной основе многофункциональной ЭВМ и программной платформе LINUX // Вестник Воронежского института ФСИН России : сборник научных трудов . — Воронеж, 2009. — Вып. 2 (2009). – С. 183–187.

3. *Колесниченко Д. Н.* Linux-сервер своими руками / Д. Н. Колесниченко. – СПб. : Наука и техника, 2006. – 587 с.

4. Руководство по развертыванию домашнего маршрутизатора. // Документация Gentoo Linux. URL:http://www.gentoo.org/doc/ru/home-router-howto.xml (дата обращения 15.02.2012).

5. Удаленный доступ и VPN. // Администрирование сетей Microsoft Windows XP Professional. URL: http://www.intuit.ru/department/os/winadmin/14/7.html (дата обращения 15.02.2012).

Телков Александр Юрьевич – доцент кафедры электроники Воронежского государственного университета, кандидат физико-математических наук. Тел.: 8-919-243-81-83. E-mail: telkov@dpo-it.ru

Семенов Николай Александрович – Магистрант 1 года обучения кафедры электроники физического факультета ВГУ. Тел.: 8-960-120-93-11. E-mail: nick-89@inbox.ru

Telkov Aleksander Yurievich – The Assistant professor of chair of Electronics, Voronezh State University. Candidate of sciences (physics and mathematics). Tel.: 8-919-243-81-83. E-mail: telkov@dpo-it.ru

Semenov Nikolay Aleksandrovich – First-year student of master's program of chair of Electronics,Voronezh State University. Tel.: 89601209311. E-mail: nick-89@inbox.ru,