ProFTPd — FTPs, sFTP и виртуальные пользователи

Задача сделать доступ виртуальным пользователям каждому в свою домашнюю директорию (т.е. chroot) по FTP, FTPs и sFTP.

```
# yum install proftpd proftpd-utils
```

Разрешаем сервис и запускаем его:

```
$ sudo systemctl enable proftpd
$ sudo systemctl start proftpd
```

Firewall:

```
# iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED --dport 20:21 -j ACCEPT
# iptables -A INPUT -p tcp -m state --state NEW --dport 40900:40999 -j ACCEPT
```

Открываем конфиг /etc/proftpd.conf добавляем туда строки:

```
ServerName "FTP SERVER"
ServerType standalone
DefaultServer on

Port 21
Umask 022

DefaultAddress 192.168.0.1 192.168.1.41
SocketBindTight on
RequireValidShell off
AuthUserFile /etc/proftpd.d/ftpd.passwd
UseIPv6 off
IdentLookups off
PassivePorts 40900 40999

MaxInstances 30
CommandBufferSize 512

User nobody
```

```
Group nobody
LangEngine on
LangPath /usr/share/locale.
UseEncoding UTF-8 WINDOWS-1251

DefaultRoot ~
AllowOverwrite on

# Bar use of SITE CHMOD by default
<Limit SITE_CHMOD>
  AllowAll
</Limit>
<Directory ~>
  AllowOverwrite on
  AllowStoreRestart on
 <Limit Write>
    AllowAll
 </Limit>
 <Limit READ>
    AllowAll
 </Limit>
</Directory>
<Global>
   PassivePorts 40900 40999
   AuthUserFile /etc/proftpd.d/ftpd.passwd
   #RequireValidShell off
   MaxLoginAttempts 6
   LangEngine on
   UseEncoding UTF-8 WINDOWS-1251
   DefaultRoot ~ !admins
   # Добавляем возможность перезаписи файлов
   AllowOverwrite on
</Global>
```

Добавляем пользователя

```
# adduser imp -s /sbin/nologin -d /home/imp
```

Проверяем

```
# vipw
imp:x:1002:1003::/home/imp:/sbin/nologin
```

Добавляем в группу

```
# usermod -aG www-data imp
```

Смотрим uid/gid

```
# id imp
uid=1002(imp) gid=1003(imp) группы=1003(imp),1001(www-data)
```

Создаем пару Логин-Пароль

```
# mkdir /etc/proftpd.d/
#  ftpasswd  --passwd  --file=/etc/proftpd.d/ftpd.passwd  --name=imp  --uid=1002  --gid=1001  --home=/home/imp  --shell=/sbin/nologin
```

Эту же процедуру повторяем для всех пользователей.

Сменить пароль можно командой

```
#  ftpasswd  --passwd  --file=/etc/proftpd.d/ftpd.passwd  --name=imp --change-password
```

Проверяем и перечитываем конфигурацию

```
# proftpd -t
# proftpd -s reload
```

Настройка ProFTPD на использование TLS/SSL протокола

```
# mkdir /etc/proftpd.d/ssl/
```

```
# openssl req -x509 -days 3650 -nodes -newkey rsa:1024 -keyout /etc/proftpd.d/ssl/proftpd.key                    -out /etc/proftpd.d/ssl/proftpd.crt
Country Name (2 letter code) [XX]:UA
State or Province Name (full name) []:Kiev
Locality Name (eg, city) [Default City]:Kiev
Organization  Name  (eg,  company)  [Default  Company Ltd]:OfficeLTD
Organizational Unit Name (eg, section) []:IT
Common  Name  (eg,  your  name  or  your  server's  hostname) []:ftp.domen.com
```

```
Email Address []:postmaster@domen.com

# chmod 600 /etc/proftpd.d/ssl/proftpd.key
```

Добавляем в proftpd.conf

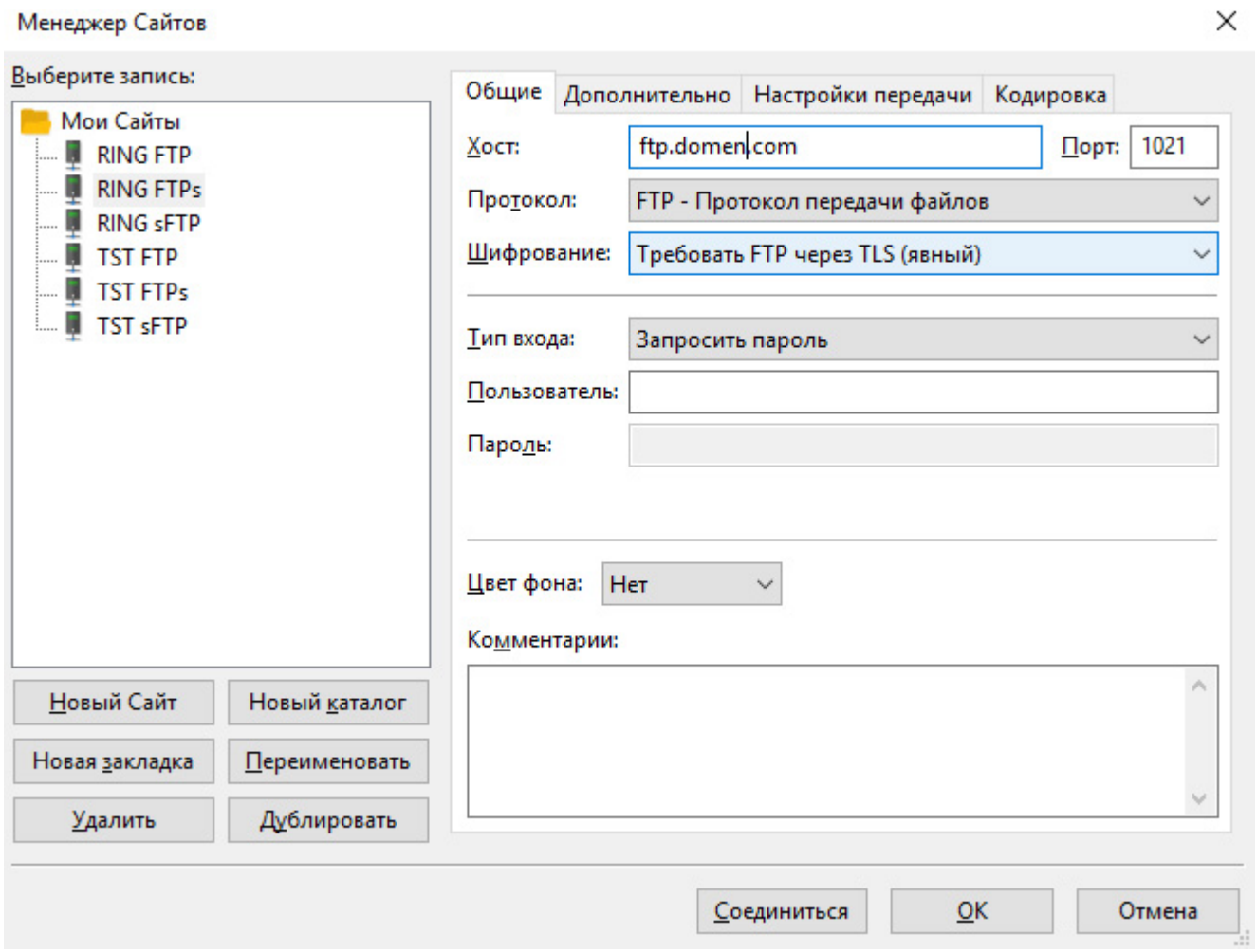
```
# nano /etc/proftpd.conf

#LoadModule mod_tls.c.
<VirtualHost 192.168.1.41>
  MasqueradeAddress ftp.domen.com
  TLSEngine on
  Port 1021
  TLSLog /var/log/proftpd/tls.log
  TLSProtocol SSLv23
  TLSRequired auth
  #TLSOptions NoCertRequest
  TLSRSACertificateFile /etc/proftpd.d/ssl/proftpd.crt
  TLSRSACertificateKeyFile /etc/proftpd.d/ssl/proftpd.key
  TLSVerifyClient off
</VirtualHost>
```

Разрешаем порт 1021 в iptables:

```
# iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED --
dport 1021 -j ACCEPT
# iptables -A INPUT -p tcp -m state --state NEW --dport
40900:40999 -j ACCEPT
```

Пробуем соединиться например клиентом FileZila с такими настройками:



Доступ по sFTP

Добавляем в /etc/proftpd.conf после секции <Global></Global>

```
LoadModule mod_sftp.c
<VirtualHost 192.168.1.41>
  MasqueradeAddress ftp.domen.com
  SFTPEngine on
  Port 8022
  #SFTPHostKey /etc/ssh/ssh_host_ed25519_key
  SFTPHostKey /etc/ssh/ssh_host_rsa_key
  SFTPHostKey /etc/ssh/ssh_host_ecdsa_key
  SFTPLog /var/log/proftpd/sftp.log
  SFTPCompression off
</VirtualHost>
```

Разрешаем порт 8022 (или любой другой незанятый, желательно выше 1024)

```
# iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED --
dport 8022 -j ACCEPT
```

Проверяем и перечитаем конфигурацию

```
# proftpd -t
# proftpd -s reload
```

Если такая ошибка:

```
proftpd[15477]: fatal: SFTPHostKey: unable to use
'/etc/ssh/ssh_host_rsa_key' as host key, as it is group- or
world-accessible on line 78 of '/etc/proftpd.conf'
```

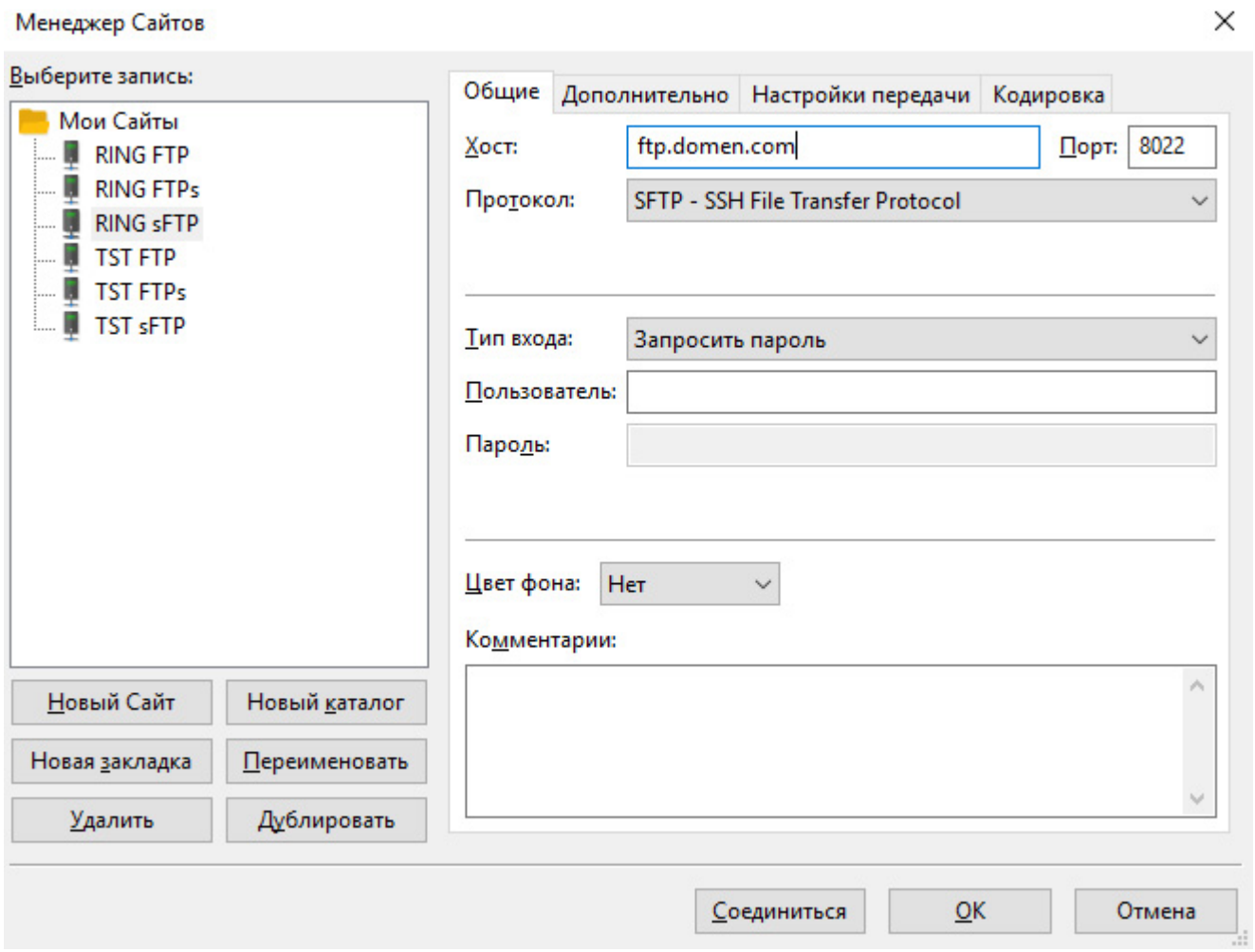
Меняем права доступа

```
# chmod 600 /etc/ssh/ssh_host_rsa_key
```

И для ключа юзера выполнить (не уверен):

```
# ssh-keygen -f /etc/ssh/ssh_host_dsa_key -N '' -t dsa
```

Пробуем соединиться:



Пасивный режим и iptables

Необходимо загрузить модуль ip_conntrack_ftp для iptables. В RedHat/CentOS достаточно в файл /etc/sysconfig/iptables-config добавить ссылку на загрузку модуля ip_conntrack_ftp:

```
# nano /etc/sysconfig/iptables-config
IPTABLES_MODULES="ip_conntrack_ftp"
```

Добавить:

```
#nano /etc/sysconfig/proftpd
PROFTPD_OPTIONS="-DTLS"
```

nano iptables (у меня присутствует и NAT):

```
# Load needed modules
modprobe ip_conntrack_ftp
```

```
modprobe ip_nat_ftp
....
# FTP, sFTP, FTPs
iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED --
dport 20:21 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED --
dport 8022 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW,ESTABLISHED --
dport 1021 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW --dport
40900:40999 -j ACCEPT
....
```

Логирование

Создаем файлы:

```
# touch /var/log/proftpd/{proftpd,xfer,access,auth}.log
```

Настраиваем логирование ftp:

```
# cat /etc/proftpd.conf
....
SystemLog /var/log/proftpd/proftpd.log
TransferLog /var/log/proftpd/xfer.log
ExtendedLog /var/log/proftpd/access.log WRITE,READ write
ExtendedLog /var/log/proftpd/auth.log AUTH auth
DebugLevel 9
.....
```

Отладка

Есть шикарный механизм отладки. Прежде чем запустить его, нужно остановить сервис:

```
# service proftpd stop
```

Режим DEBUGa (-d – выбор уровня логирования)

```
# proftpd -n -d 9 -c /etc/proftpd.conf
```

Защита

Добавим защиту в fail2ban. Создаем клетку и правим фильтр:

```
cat /etc/fail2ban/jail.d/proftpd.conf
[proftpd]
enabled = true
filter = proftpd
logpath = /var/log/proftpd/proftpd.log
maxretry = 3
ignoreip = 127.0.0.1/8 192.168.0.0/24
#backend = polling
port = ftp,ftp-data,ftps,ftps-data
#logpath = %(proftpd_log)s
#backend = %(proftpd_backend)s
backend = gamin
```

```
cat /etc/fail2ban/filter.d/proftpd.conf
[Definition]
failregex = USER \S+: no such user found from \S* ?\[<HOST>\]
to \S+\s*$
ignoreregex =
```

Перезапускаем и проверяем:

```
# service proftpd restart
# service fail2ban restart
# fail2ban-client status proftpd
```

Итог

Мы создали FTP сервер с возможностью подключения виртуальных пользователей по FTP, sFTP, FTPs, при этом каждый из пользователей не попадет выше своей директории.

Источники

https://www.dmosk.ru/instruktions.php?object=proftpd-centos7
https://sys-adm.in/os/nix/539-centod-install-proftpd.html
http://unixblog.org.ua/proftpd/install-proftpd-centos-7-auth-via-authuserfile/

Iptables и пассивный режим FTP
https://www.homeless.su/linux-tipstricks/iptables-i-passivnyj-rezhim-ftp/

Log
https://sys-adm.in/os/nix/496-loggining-proftpd-in-centos.html