Лабораторная работа №2
Настройка FTP сервера

Цель работы

Познакомиться с безопасной настройкой серверов работающих по протоколу FTP (**VsFtpd**). Изучить особенности настройки сервера для предоставления общего доступа анонимным и аутентифицированным пользователям.

Задания

1. Установить сервер `vsftpd` с помощью системных команд установки ПО
2. Произвести настройку сервера для выполнения необходимых условий
3. Создать необходимые каталоги на файловой системе
4. Проверить функциональность созданной конфигурации

Теоретические сведения

FTP протокол

FTP (File Transfer Protocol — протокол передачи файлов) — стандартный протокол, предназначенный для передачи файлов по TCP-сетям. Для установки управляющего соединения использует 21 порт. FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, и даже до TCP/IP, в 1971 году. На сегодняшний день **FTP** используется достаточно активно, например, используется для загрузки документов на сервера хостинга, распространения дистрибутивов Linux и т.д.

Протокол построен на архитектуре ”клиент-сервер”и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером. Пользователи FTP могут пройти **аутентификацию**, передавая логин и пароль открытым текстом, или же, если это разрешено на сервере, они могут подключиться **анонимно**. Для этого пользователи обычно входят в систему как «anonymous» в качестве имени пользователя, в качестве пароля пользователей просят прислать адрес их электронной почты, однако никакой проверки фактически не производится.

Протокол определён в RFC 959. Особенностью протокола FTP является то, что он использует множественное (как минимум — **двойное**) подключение. При этом один канал является **управляющим**, через который поступают команды серверу и возвращаются его ответы (обычно через TCP-порт 21), а через остальные происходит собственно передача данных, по одному каналу на каждую передачу. Поэтому в рамках одной сессии по протоколу FTP можно передавать одновременно несколько файлов, причём в обоих направлениях. Для каждого канала данных открывается свой TCP порт, номер которого выбирается либо сервером, либо клиентом, в зависимости от режима передачи.

FTP может работать в двух режимах:

- **Активном**
  Клиент создаёт управляющее TCP-соединение с сервером и отправляет серверу свой IP-адрес и произвольный номер клиентского порта, после чего ждёт, пока сервер запустит TCP-соединение с этим адресом и номером порта. Если клиент находится за брандмауэром, то вероятнее всего настройки брандмауэром не позволяют принять входящее TCP-соединение, то тогда может быть использован пассивный режим.
- **Пассивном**
  В этом режиме клиент использует поток управления, чтобы послать серверу команду PASV, и затем получает от сервера его IP-адрес и номер порта, которые затем используются клиентом

для открытия потока данных с произвольного клиентского порта к полученному адресу и порту. Первые клиентские FTP-приложения были интерактивными инструментами командной строки, реализующими стандартные команды и синтаксис, т.е. для загрузки/выгрузки файлов на/с ftp-сервера небоходимо было знать набор команд ftp-сервера. После этого были разработаны графические пользовательские интерфейсы для многих используемых по сей день операционных систем. Среди таких ftp-клиентов можно отметить как универсальные программы доступа к файлам (проводник в Windows, менеджеры файлов в графических системах Linux, **TotalCmd**, **MC**), а также веб-браузеры(FireFox, Chrome, Opera), так и специализированные FTP-клиенты (например, CuteFTP, FileZilla) и программы для доступа к файлам на удалённых серверах (**WinSCP**).

Пример взаимодействия клиента и сервера:

```
220 FTP server ready.
USER ftp
230 Login successful.
PASV
227 Entering PassiveMode (192,168,254,253,233,92)
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD incoming
250 Directory successfully changed.
PASV
227 Entering PassiveMode (192,168,254,253,207,56)
STOR gyuyfotry.avi
150 Ok to send data.
226 File receive OK.
QUIT
221 Goodbye .
```

Недостатки FTP

FTP является одним из старейших прикладных протоколов, появившимся задолго до TCP/IP, в 1971 году. Это одна из причин его слабой адаптированности к современным требованиям. В частности к недостаткам протокола относят:

- Его слабую защищенность от атак: скрытые атаки (bounce attacks), спуфинг-атаки (spoof attacks), метод грубой силы (brute force attacks)
- Отсутствие встроенной поддержки шифрования трафика, что приводит к:
  * возможности перехвата логина и пароля, т.к. они передаются в открытом виде
  * возможности перехвата передаваемых данных и кражи ценных сведений
  * возможности внедрения злоумышленником своих данных в передаваемый поток
- Для борьбы с предыдущим недостатком используют решения, которые не являются частью само-го протокола и не являются полностью стандартизированными, что приводит лишь к частичной их поддержке ftp-клиентами.
- Отсутствие возможность сжатия передаваемых данных

Надёжный FTP

К методам повышения надёжности протокола относят:

- **FTPS** — расширение стандарта FTP, добавляющее возможность шифрования в протокол. Может быть двух видов:

    * **Явный FTPS**, добавляющий команду «AUTH TLS», которую сервер может принять (и то-гда дальнейший обмен происходит в шифрованном виде) или отклонить.
    * **Неявный FTPS** — устаревший стандарт для FTP, требующий использования SSL- или TLS-соединения. Этот стандарт должен был использовать отличные от обычного FTP пор-ты.
- **SFTP** — на самом деле, никак не связан с FTP, однако иногда ошибочно его считают подвидом FTP. **SFTP** — это способ передачи файлов по протоколу **SSH**.
- **FTP через SSH** — туннелирование обычного FTP посредством протокола **ssh**.

FTP сервера́

На сегодняшний день FTP сервера существуют под все распространённые платформы и распространяются под различными лицензиями, например, **FileZilla Server** является свободным (бесплатным) ПО для ОС Windows, CrushFTP Server — платный ftp-сервер для всех платформ, **ProFTPD** — сервер с открытым исходным кодом для *nix-систем.

К критериям выбора ftp-серверов относится:

- Поддержка защищённого FTP: SFTP, FTPS, SCP
- Поддержка других протоколов: HTTP, WebDAV, XTP
- Возможности по аутентификации: LDAP, ActiveDirectory, DB, по сертификатам
- Кластеризация и балансировка нагрузки

Vsftpd

Одним из наиболее популярных ftp-серверов для Linux является Vsftpd (**V**ery **S**ecure **FTP D**aemon) — FTP-сервер с поддержкой IPv6 и SSL.

Является FTP-сервером по умолчанию многих операционных систем(Ubuntu, CentOS, Fedora, Slackware, NimbleX и RHEL), и обслуживает официальные репозитории ftp.debian.org , ftp.redhat.com, ftp.openbsd.org, ftp.freebsd.org. Также используется на официальном FTP ядра Linux.

Вся конфигурация сервера находится в файле `/etc/vsftpd.conf` К наиболее часто используемым конфигурационным директивам относится (см. страницы man):

- anonymous_enable, local_enable, write_enable
- anon_upload_enable, anon_mkdir_write_enable, anon_other_write_enable
- idle_session_timeout, data_connection_timeout, accept_timeout, connect_timeout
- anon_max_rate, local_max_rate
- chroot_local_user, chroot_list_enable, chroot_list_file
- guest_enable
- listen
- pasv_enable, pasv_min_port, pasv_max_port

Порядок выполнения работы

1. Установите сервер `vsftpd` с помощью системных команд установки ПО в вашем дистрибутиве Linux
   Проверить что сервер успешно запустился можно с помощью команды `netstat` :

```
# netstat nptl
Active Internet connections (only servers)
Proto Recv Q Send Q Local Address Foreign Address
State PID/Program name
```

```
tcp        0      0 0.0.0.0:21              0.0.0.0:*
LISTEN      22468/vsftpd
```

2. Создайте корневую папку ftp сервера `/home/ftp/`
   В ней создайте несколько директорий и разместите в них файлы для демонстрации публично доступных файлов фтп сервера
3. Произведите настройку `vsftpd` для выполнения следующих требований:
   - Корневая директория сервера: `/home/ftp/`
   - Анонимный доступ (без аутентификации по логину и паролю) к корневой директории (и поддиректориям) ftp сервера только на чтение.
   - Запись анонимным пользователям разрешён только в каталог `/incoming/` и созданные ими подкаталоги. Пользователи не могут удалить файлы из этого каталога.
   - Аутентифицированные пользователи получают доступ в свой домашний каталог
   - Пользователю `guest2` доступ запрещён
   - **Обратите внимание:** реализация некоторых из указанных пунктов требует не только настройки конфигурационного файла, но и прав доступа к директориям файловой системы
4. Выполните проверку выполнения всех указанный условий подключившись к вашему ftp серверу, например, используя ftp-клиент в встроенный в `mc` .

Контрольные вопросы

1. Какие команды используются для установки нового ПО в вашем дистрибутиве Linux?
2. С помощью какой команды осуществляется (пере)запуск **vsftpd** сервера?
3. Какой файл используется для основной конфигурации фтп сервера? Для ограничения доступа аутентифицированных пользователей?
4. Для чего используется команда `chmod +t <filename>` ?

Основная литература

1. Страницы man
   (a) `man vsftpd`
   (b) `man vsftpd.conf`

Дополнительная литература

1. Заяц, А.М. Администрирование информационных систем [Электронный ресурс]: учебное пособие / А.М. Заяц. — Электрон. дан. — Санкт-Петербург: СПбГЛТУ, 2011. — 140 с. — Режим доступа: https://e.lanbook.com/book/45448. — Загл. с экрана.

Информационно-справочные и поисковые системы

1. http://wiki.qemu.org/Manual
2. https://www.debian.org/doc/
3. http://vsftpd.beasts.org

VSFTPD.CONF

ФОРМАТ

Каждая строка это коментарий # или директива. Командные строки начинающиеся с символа # игнорируются. Директивы имеют формат опция=значение. Важным фактом является пробел между опцией или значением, что приведет к ошибке. Каждое значение по умолчанию может быть изменено в конфигурационном файле.

СПОСОБЫ ЗАПУСКА

listen
Если опция включена сервер стартует в независимом от inetd/xinetd режиме "standalone mode". В этом случае он сам заботится о прослушивании и определении входящих соединений.
Default: NO

listen_ipv6
Тоже самое что listen, за исключением того что vsftpd слушает IPv6 протокол включительно.Этот параметр и listen взаимно исключаемые.
Default: NO

background
При включении, vsftpd стартуя в режиме listen, работает в фоновом режиме. Т.е. контроль передается той оболочке в которой был запущен vsftpd.
Default: NO

listen_port
Если запущен в standalone mode, указанный порт прослушивается на предмет входящих FTP соединений.
Default: 21

listen_address
Если запущен в standalone mode, обычно слушает все адреса (или все локальные интерфейсы). Что может быть отменено указанием определенных ip адресов в этой строке.
Default: (none)

listen_address6
Тоже что и listen_address, но прослушивает адреса соединений на основе IPv6 протокола (который используется если выбрана опция listen_ipv6), формат в виде стандартного IPV6 адреса.
Default: (none)

max_clients
Если vsftpd находится в standalone_mode, это максимальное количество клиентов, которые могут быть подключены. Попытки подключения сверх указанного количества,получат сообщение об ошибке.
Default: 0 (unlimited)

max_per_ip
Если vsftpd находится в standalone mode, эта опция указывает максимально возможное количество клиентов с одинаковыми ip адресами. Клиентские подключения пытающиеся превысить этот лимит, получат сообщение об ошибке.
Default: 0 (unlimited)

run_as_launching_user
Включите для возможности запуска vsftpd от пользователя vsftpd. Это полезно когда root доступ недопустим. Важное предупреждение! Не разрешайте эту опцию если вы полностью не уверены что вы делаете, наивное использование этой опции

может создать множество проблем связанных с безопасностью. В особенности, vsftpd не может использовать chroot технологию для разграничения доступа к файлам (даже если при этом сервер запущен от root). В некоторой степени можно ограничить доступ при помощи параметра deny_file, указав шаблон запрещенных файлов, такой как {/*,*..*}, но надежность этого не сравнима с chroot, поэтому не стоит возлагать на это больших надежд. С использованием этой опции, также проявляются ограничения в других опциях. Для примера, в опциях требующих привилегии, не анонимные входы, изменение владельца закачанных
на сервер файлов, подключение по 20 порту и прослушивание портов менее 1024. Возможно и другие опции пересекаются с включением этой опции.
Default: NO

ПРАВИЛА ДЛЯ АНОНИМНЫХ ПОЛЬЗОВАТЕЛЕЙ

anonymous_enable
Разрешает или запрещает вход анонимных пользователей. Если разрешено, пользователи с именами ftp и anonymous распознаются как анонимные пользователи.
Default: YES

anon_max_rate
Максимальная допустимая скорость передачи данных для анонимных
пользователей, выражена в байтах
в секунду .
Default: 0 (unlimited)

anon_root
В этой строке указывается каталог, в который vsftp будет переводить
анонимных пользователей после входа. При неудаче просто игнорируется.
Default: NO

no_anon_password
Если опция установлена, vsftp не спрашивает пароль у анонимных
пользователей, позволяя им подключаться сразу.
Default: NO

anon_mkdir_write_enable
Включение этой опции, позволяет анонимным пользователям создавать новые каталоги в соответствии с определенными для этого условиями. Для того чтобы это работало опция write_enable должна быть включена, и анонимный пользователь должен иметь права на запись в данном каталоге.
Default: NO

anon_other_write_enable
Если выбрано YES, анонимные пользователи могут выполнять операции записи отличные от
загрузки на сервер и создания каталогов, такие как удаление и переименование. Это обычно
не рекомендуется, но все таки такая возможность присутствует для полноты.
Default: NO

anon_upload_enable
Включение этой опции позволяет анонимным пользователям загружать файлы на сервер, в соответствии с определенными для этого условиями. Для того чтобы это работало опция write_enable должна быть активирована, и анонимный ftp пользователь должен иметь права на запись в каталоге для загрузки. Включение опции также необходимо для предоставления возможности загружать на сервер файлы виртуальным пользователям; по умолчанию виртуальные пользователи имеют одинаковые привилегии с анонимными пользователями
(т.е. максимально ограниченные привилегии).
Default: NO

anon_world_readable_only
При включение этой опции, анонимным пользователям будет разрешено скачивать только видимые ими из мира файлы. Предполагается полезным, если пользователи могут загружать на сервер и хранить на нем собственные файлы.
Default: YES

deny_email_enable
Активация опции, позволяет использовать список анонимных паролей типа e-mail, при использовании которых попытки подключения будут отвергнуты. По умолчанию, файл содержащий этот список располагается в /etc/vsftpd.banned_emails, но имеется возможность изменить путь, указав альтернативный путь в banned_email_file.
Default: NO

banned_email_file
Эта опция указывает имя файла в котором содержится список анонимных e-mail паролей не принимаемых сервером. Сервер сверяется с этим файлом если опция deny_email_enable включена.
Default: /etc/vsftpd.banned_emails

guest_enable
Если опция включена, подключения всех не анонимных локальных пользователей рассматриваются как "гостевые" ("guests"). "Гостям" назначаются параметры указванные в опции guest_username.
Default: NO

guest_username
Опция содержит имя "гостевого" пользователя, определяющее его домашнюю директорию.Работает при включенной guest_enable.
Default: ftp

secure_email_list_enable
Активируйте опцию, если хотите разрешать вход анонимным пользователям только на основе проверки паролей указанных в e-mail листе. Это простой путь ограничения доступа к низко безопасному содержимому без необходимости в виртуальных пользователях. При включении, анонимные входы блокируются если пароль не содержится в файле указанном опцией email_password_file. Формат файла - один пароль на строку. По умолчанию файл располагается в /etc/vsftpd.email_passwords.
Default: NO

email_password_file
Эта опция может быть использована для предоставления альтернативного пути файла используемого secure_email_list_enable опцией.
Default: /etc/vsftpd.email_passwords

anon_umask
Значение накладываемой маски на создаваемые анонимными пользователями файлы. Замечание! Если вы решили указать цифровое значение, надо помнить о нулевом "0" префиксе, иначе значение будет рассмотрено как десятизначное.
Default: 077

ftp_username
Имя назначаемое анонимным пользователям. Пользователи с назначенным именем привязаны к своему домашнему каталогу, который является корневым каталогом анонимного пространства FTP.
Default: ftp

ПРАВИЛА РАБОТЫ С ПОЛЬЗОВАТЕЛЯМИ

local_enable
Разрешает или запрещает вход для локальных пользователей. Если включено

обычные пользовательские акаунты в /etc/passwd могут быть использованы для входа. Должно быть включено для разрешения любых не анонимных входов, включая вход виртуальных пользователей.
Default: NO

local_root
Эта опция указывает каталог в который vsftpd должен перевести пользователя после локального не анонимного входа. В случае неудачи просто игнорируется.
Default: (none)

user_config_dir
Эта опция позволяет задавать дополнительные параметры относительно к отдельным пользователям. Например если в user_config_dir выбрать /etc/vsftpd_user_conf, тогда вход пользователя "chris", означает что vsftpd будет использовать настройки из конфигурационного файла /etc/vsftpd_user_conf/chris для этой сессии. Обратите внимание, не все настройки применимы к отдельным пользователям, например listen_address, banner_file, max_per_ip, max_clients, xferlog_file, и другие.
Default: (none)

chroot_local_user
Если выбрано локальные пользователи будут (по умолчанию) перенесены в chroot () "заточение" в их домашнем каталоге после входа. Внимание: эта опция имеет смысл быть включенной из соображений безопасности, особенно если пользователи имеют права позволяющие загрузку файлов на сервер, или shell доступ. Включать только если вы действительно уверены что знаете зачем вам это нужно. Заметим что эта опция безопасности в системах класса unix, характерна не только для vsftpd, используется и в других FTP серверах.
Default: NO

passwd_chroot_enable
Работает при включенном параметре chroot_local_user. Пользователи помещаются в свои домашние директории, которые указаны в файле /etc/passwd. Точное указание пути /./ указывает что пользователь будет перемещен при входе в директорию в этом пути.
Default: NO

chroot_list_enable
Если включить, вы можете использовать список локальных пользователей помещаемых в chroot() заточение в их домашнем каталоге после входа. Если используется совместно с включенным chroot_local_user означает список пользователей которые не помещаются в chroot() заточение. По умолчанию список содержится в файле /etc/vsftpd.chroot_list, но можно указать любой другой путь к файлу используя опцию chroot_list_file.
Default: NO

chroot_list_file
Опция является дополнением к chroot_list_enable указывает альтернативный путь к файлу содержащему список локальных пользователей которые будут перемещены в chroot() заточение в их домашние каталоги при входе. Эта опция уместна только при разрешенной chroot_list_enable. Если опция chroot_local_user включена, наоборот указывает файл списка пользователей не помещаемых в chroot() заточение.
Default: /etc/vsftpd.chroot_list

chmod_enable
Включение этой опции разрешает использование SITE CHMOD команд устанавливающих права доступа для файла. ВНИМАНИЕ! Применимо только к локальным пользователям. Анонимные пользователи никогда не используют SITE CHMOD команды.
Default: YES

check_shell
Замечание! Опция эффективна только для non-PAM сборок vsftpd. Если запрещена,

vsftpd не проверяет файл /etc/shells на допустимость пользовательских shell оболочек для локальных входов.
Default: YES

virtual_use_local_privs
Если включено, виртуальные пользователи будут использовать одинаковые с локальными пользователями привилегии. По умолчанию, виртуальные пользователи используют одинаковые с анонимными пользователями привилегии, предполагающие большие ограничения, (особенно условия доступа на запись).
Default: NO

user_sub_token
Используется для автоматической генерации домашнего каталога виртуального пользователя базируясь на шаблоне. К примеру, если домашний каталог реального пользователя указанного в guest_username это /home/virtual/$USER, и в user_sub_token выбрать $USER, тогда при входе виртуального пользователя fred, он будет направлен, (обычно в chroot) директорию /home/virtual/fred. Эта опция также работает если local_root содержит user_sub_token.
Default: (none)

local_max_rate
Максимальная скорость передачи данных, выраженная в байтах в секунду, для локально аутентифицированных пользователей.
Default: 0 (unlimited)

local_umask
Значение маски назначения прав доступа к файлам созданным локальными пользователями. Помните! Если вы хотите указать параметр в качестве цифрового значения, указывайте "0" (нулевую) приставку, иначе значение будет определено как целое десятизначное.
Default: 077

session_support
session_support
Эта опция определяет, будет ли vsftpd поддерживать установленные соединения. Если vsftpd поддерживает сессии, он будет пытаться обновить utmp и wtmp. Он также откроет pam_session, если используется PAM аутентификация и закроет соединение только после отключения. Можно отключить эту опцию, если не требуется журналирование сессии и есть желание предоставить vsftpd больше возможностей для запуска с меньшими привилегиями. Замечание - utmp и wtmp поддерживаются только в сборках с включенным PAM.
Default: NO

userlist_enable
Если разрешено, vsftpd загружает список имен пользователей, из файла указанного userlist_file параметром. Если пользователь пытается войти используя имя взятое из этого файла, вход будет отклонен перед запросом пароля. Это может быть полезно для предотвращения передачи пустого поля в качестве пароля. Смотри также userlist_deny.
Default: NO

userlist_file
Этот параметр указывает путь к файлу списка пользователей, загружаемому если userlist_enable параметр включен.
Default: /etc/vsftpd.user_list

userlist_deny
Эта опция работает если userlist_enable включен. Если выбрано значение NO, значит вход пользователей будет отклонен если они не найдены в файле указанном usrlist_file. Если вход отклоняется, отказ производится перед тем как у пользователя будет запрошен пароль.
Default: YES

КОМАНДЫ

dirlist_enable
Если выбрать NO, все команды листинга каталогов будут запрещены.
Default: YES

async_abor_enable
При включении, специальные FTP команды известные как "async ABOR" будут разрешены. Только плохо продуманные FTP клиенты используют эту функцию. В добавок эта функция неудобна в управлении, поэтому отключена по умолчанию. К сожалению, некоторые FTP клиенты могут зависать в момент отмены передачи, если эта функция выключена. Если это происходит можно попробовать включить эту функцию.
Default: NO

write_enable
Разрешает FTP команды изменяющие файловую систему. Такие команды как: STOR, DELE, RNFR, RNTO, MKD, RMD, APPE, SITE.
Default: NO

ls_recurse_enable
При включении, разрешает рекурсивный листинг "ls -R". Включение немного рискованно исходя из соображений безопасности, так как выполнение "ls -R" в верхнем уровне большого сайта может поглощать много ресурсов.
Default: NO

mdtm_write
Если включить, разрешает обновления времени модификации файла через MDTM ftp команды.
Default: YES

cmds_allowed
В этой опции указывается список разделенных запятыми команд разрешенных FTP (post login. USER, PASS и QUIT pre-login всегда разрешены). Другие команды запрещены. Пример: cmds_allowed=PASV,RETR,QUIT
Default: (none)

DOWNLOAD/UPLOAD

file_open_mode
Маска файлов назначаемая при загрузке файлов на сервер. При желании возможно изменить на 0777 если есть необходимость сделать исполняемыми загружаемые на сервер файлы.
Default: 0666

ascii_download_enable
Если включить, ASCII режим передачи данных будет разрешен при download.
Default: NO

ascii_upload_enable
Если включить, ASCII режим передачи будет разрешен при uploads.
Default: NO

chown_uploads
Если включить, у всех анонимно закачанных файлов на сервер будут изменены владельцы на пользователя в указанного в chown_username. Это может быть полезно при администрировании, и возможно из соображений безопасности.
Default: NO

chown_username
В этом параметре указывается имя пользователя, назначаемого хозяином анонимно загруженных на сервер файлов. Эта опция уместна только при включенной опции chown_uploads.

Default: root

download_enable
Если выбрано значение NO, все запросы на скачивание файлов с сервера будут отклонены.
Default: YES

lock_upload_files
При включении опции, все загрузки на сервер происходят с блокировкой записи загружаемого файла. Все загрузки с сервера совершаются с общей блокировкой чтения скачиваемых файлов.
Default: NO

ОСНОВНЫЕ ПРАВИЛА

tcp_wrappers
Если включено, и vsftpd был скомпилирован с поддержкой tcp_wrappers, входящие соединения контролируются через tcp_wrappers. Этот механизм предоставляет возможность контролировать соединения по ip адресам, назначая конкретному подключению отдельный конфигурационный файл vsftpd. Параметры tcp_wrappers устанавливаются в конфигурационных файлах /etc/hosts.allow и /etc/hosts.deny, среди них есть переменная окружения VSFTPD_LOAD_CONF, указывающая на месторасположения файла с альтернативными vsftpd.conf параметрами для определенного правила (ip адреса) напротив которого она указана.
Default: NO

idle_session_timeout
Временной промежуток в секундах указывающий для удаленного клиента максимальное время которое он может бездействовать не выполняя FTP команды. Если время исчерпано, соединение отбрасывается.
Default: 300

data_connection_timeout
Максимальный временной промежуток в секундах, разрешенного замирания процесса передачи данных. Если перерыв превышен, соединение с удаленным клиентом отбрасывается.
Default: 300

accept_timeout
Максимальное время в секундах для выделения подключения с PASV стилем передачи данных.
Default: 60

connect_timeout
Максимальное время в секундах, отведенное на выделение соединения PORT стиля передачи данных.
Default: 60

deny_file
Эта опция может быть использована для выбора шаблона имен файлов к которым необходимо ограничить доступ. Обозначенный в шаблоне элемент не скрывается, но любая попытка сделать с ним что нибудь (скачать, изменить и др.) будет отклонена. Эта опция очень проста и не должна использоваться для серьезного контроля доступа. Может быть использована с настройками виртуальных пользователей. Пример: deny_file={*.mp3,*.mov,.private}
Default: (none)

hide_file
Эта опция может быть использована для выбора шаблона имен файлов и каталогов которые должны быть скрыты от просмотра. Несмотря на то что они скрыты, они остаются полностью доступными для клиентов которые знают их имена. Элементы будут скрыты если их имена содержат строки заданные в hide_file или если их шаблоны указаны в hide_file.

Пример: hide_file={*.mp3.,.hidden,hide*,h?}
Default: (none)

banner_file
Эта опция указывает на имя банер-файла содержащего текст выводимый на экран клиента при подключении к серверу. Если выбрано, отменяет банер-строку предоставленную ftpd_banner опцией.
Default: (none)

ftpd_banner
В этой опции можно указать банер-строку выводимую на экран клиента при подключении к серверу.
Default: (none - default vsftpd banner is displayed)

dirmessage_enable
Если разрешено, при входе в каталог пользователям показывается сообщение из файла .message. По умолчанию, директория сканируется на наличие сообщения в файле .message, что можно изменить задав имя другого файла параметром message_file.
Default: NO (but the sample config file enables it)

message_file
Эта опция указывает на имя файла в котором содержится сообщение показываемое пользователям при входе в каталог. Работает только если опция dirmessage_enable включена.
Default: .message

use_localtime
При включении, vsftpd производит листинг каталогов с отображением времени лично вашей временной зоны. По умолчанию в листинге отображается GMT временная зона. Времена обновляемые MDTM командами также затрагиваются этой опцией.
Default: NO

force_dot_files
Если включено, файлы и каталоги имена которых начинаются с "." будут показаны при листинге каталогов, даже если флаг "a" не был использован клиентом.
Default: NO

text_userdb_names
По умолчанию в полях листинга каталогов пользователей и групп отображаются цифровые ID. Включив эту опцию можно задать текстовые отображения. Это выключено по умолчанию по причине производительности.
Default: NO

hide_ids
Включение скрывает информацию о именах владельцев файлов и группах, при листинге отображается как "ftp".
Default: NO

secure_chroot_dir
Эта опция указывает на имя пустого каталога. Также, каталог не должен быть записываемый для ftp пользователя. Этот каталог используется как безопасный chroot(), когда vsftpd не нужен доступ к файловой системе.
Default: /var/run/vsftpd

delay_failed_login
Время ожидания в секундах, перед выводом отчета о неудачном входе.
Default: 1

delay_successful_login
Время ожидания в секундах, перед разрешением успешного входа.
Default: 0

connect_from_port_20
Включение этой опции указывает исходящим с сервера соединениям использовать 20 порт. Из соображений безопасности, некоторые клиенты могут настаивать на этом значении. Отключение этой опции позволяет vsftpd стартовать с немного меньшими привилегиями.
Default: NO (but the sample config file enables it)

ftp_data_port
Указывается порт для входящих соединений с сервером (пока connect_from_port_20 включен).
Default: 20

port_enable
Отключите при желании запретить PORT метод организации соединения.
Default: YES

port_promiscuous
При включении выключается PORT security check гарантирующий что исходящие соединения могут быть установлены только с клиентами. Включайте только если действительно знаете что делаете!
Default: NO

one_process_model
Начиная с ядра Linux 2.4, возможно использование различных моделей безопасности, так включение этой опции позволяет использовать только один процесс на одно пользовательское подключение. Обычно нет нужды включать это если вы точно не уверены что делаете, и сайт не поддерживает большое количество одновременно подключенных пользователей.
Default: NO

setproctitle_enable
При включении, vsftpd будет показывать информацию о статусе сессии в списке системных процессов. Другими словами, в списке процессов будут подробно отображаться события происходящие с vsftpd (скачивания и др.)
Default: NO

max_login_fails
Количество неудачных попыток входа, после которых сессия прекращается.
Default: 3

pasv_max_port
Значение указывает максимальный порт до которого размещены порты для PASV стиля передачи данных. Может быть использовано для указания подробного размещения портов помогая файрволлингу.
Default: 0 (use any port)

pasv_min_port
Значение номера порта начиная с которого размещаются порты для PASV стиля передачи данных. Может быть использовано для указания подробного размещения портов помогая файрволлингу.
Default: 0 (use any port)

pasv_address
Этой опцией задается ip адрес для ответа на запрос PASV команды. Адрес указывается в цифровом виде, если не включен pasv_addr_resolve. По умолчанию, берётся адрес сокета входящего соединения.
Default: (none - the address is taken from the incoming connected socket)

pasv_addr_resolve
Необходимо включить если вы хотите использовать имя хоста (вместо ip адреса) в pasv_address опции.
Default: NO

pasv_enable
Отключите, если вы хотите запретить PASV метод соединения.
Default: YES

pasv_promiscuous
Включите, если хотите запретить PASV security check, контролирующую подключения с одинаковыми ip адресами. Включайте это, только если вы знаете что делаете! Используется в некоторых туннельных соединениях, возможно в FXP.
Default: NO

use_sendfile
Внутренняя настройка используемая для определения пользы использования sendfile().
Default: YES

trans_chunk_size
Вы возможно не хотите менять это, но можете попытаться выбрать что нибудь наподобие 8192 для более плавного ограничения полосы пропускания.
Default: 0 (let vsftpd pick a sensible setting)

tilde_user_enable
При включении, vsftpd распознает имена каталогов с тильдой "~" в начале как папки пользователей, папки будут распознаны только если файл /etc/passwd находится в _current_ chroot().
Default: NO

nopriv_user
Указывает имя пользователя под которым работает сервер, когда ему не нужны привилегии. Для этого предпочтительней выделить отдельного пользователя, чем использовать nobody.
Default: nobody

pam_service_name
В этой строке можно указать имя PAM сервиса который будет использоваться для vsftpd.
Default: vsftpd

SSL ШИФРОВАНИЕ ДАННЫХ

ssl_enable
Если включено, и vsftpd был скомпилирован с поддержкой OpenSSL, vsftpd будет поддерживать безопасность соединения с помощью SSL.
Это позволяет контролировать соединения (включая входы в систему) и также передачу данных. Для этого также необходим клиент с поддержкой SSL.
Замечания!! Включайте, если это действительно вам необходимо.
Надо понимать тот факт, что vsftpd не может гарантировать безопасность OpenSSL библиотек. Включая эту опцию вы доверяете безопасность установленной OpenSSL библиотеке.
Default: NO

ssl_sslv2
Разрешено только при включенной ssl_enable. Включение этой опции делает возможными подключения по протоколу SSL v2.
TLS v1 подключения оптимальны.
Default: NO

ssl_sslv3
Разрешается только при включенном ssl_enable. Если разрешено, эта опция позволяет подключения по протоколу SSL v3.
TLS v1 подключения оптимальны.
Default: NO

ssl_tlsv1
Разрешено только если ssl_enable включено. Если разрешено, эта опция разрешает соединения по протоколу TLS v1 который является оптимальным.
Default: YES

allow_anon_ssl
Разрешено только если ssl_enable включено. При включении этой опции, анонимным пользователям также будет разрешено использование безопасных SSL соединений.
Default: NO

force_anon_data_ssl
Разрешено только если ssl_enable включено. При включении, все анонимные подключения будут использовать SSL безопасные соединения для приема и передачи данных.
Default: NO

force_anon_logins_ssl
Разрешено только при включенном ssl_enable. При включении, все анонимные подключения будут использовать безопасные SSL соединения при посылке паролей.
Default: NO

force_local_data_ssl
Разрешено только если ssl_enable активно. При включении, все не анонимные подключения используют безопасные SSL соединения для приема и передачи данных.
Default: YES

force_local_logins_ssl
Разрешено только если ssl_enable включено. При включении, все не анонимные подключения используют безопасное SSL соединение при передачи паролей.
Default: YES

dsa_cert_file
Эта опция указывает местонахождение DSA сертификата для использования в SSL зашифрованных соединениях.
Default: (none - an RSA certificate suffices)

dsa_private_key_file
Эта опция задает расположение личного DSA ключа для использования в SSL зашифрованных соединениях. Если эта опция не выбрана, сертификат предусматривается как личный ключ.
Default: (none)

rsa_cert_file
Эта опция задает расположения RSA сертификата для использования в SSL зашифрованных соединениях.
Default: /usr/share/ssl/certs/vsftpd.pem

rsa_private_key_file
Эта опция задает расположения личного RSA ключа для использования в SSL зашифрованных соединениях.
Если эта опция не выбрана, сертификат предусматривается как личный ключ.
Default: (none)

ssl_ciphers
Эта опция может быть использована для выбора того, какие SSL шифры будут разрешены для шифрования SSL соединений. Смотрите страницу man ciphers для детального ознакомления. Заметьте, такие ограничения шифров могут использоваться в целях предосторожности,предотвращая использования отдаленными сторонами шифра с которым были обнаружены проблемы.
Default: DES-CBC3-SHA

ЖУРНАЛИРОВАНИЕ

syslog_enable
При включении, все выводы журнала направляемые ранее в /var/log/vsftpd.log будут направляться в системный журнал вместо этого.
Default: NO

no_log_lock
Если включено, запрещает vsftpd блокировку файла журнала при записи в него. Этот параметр обычно не разрешен.
Default: NO

log_ftp_protocol
При включении, все FTP запросы и ответы журналируются, включение с опцией xferlog_std_format запрещено. Используется для выявления ошибок.
Default: NO

dual_log_enable
При включении, два файла с журналами генерируются параллельно, по умолчанию они располагаются в /var/log/xferlog и /var/log/vsftpd.log. Первый генерируется
в стиле журнала wu-ftpd, анализируемый стандартными средствами.
Другой в стиле журнала vsftpd.
Default: NO

xferlog_enable
Если включено, журнал будет включать детальные отчеты о закачках на сервер, и закачках с сервера (uploads, downloads). По умолчанию, этот файл будет располагаться в /var/log/vsftpd.log, но расположение может быть изменено используя опцию vsftpd_log_file.
Default: NO (but the sample config file enables it)

xferlog_std_format
Если включено, запись в журнал производится в стандартном wu-ftpd стиле, xferlog формата. Полезно при желании использования уже существующих привычных способов генерации статистики. Однако с другой стороны, формат используемый по умолчанию лучше читается. Расположение журнала по умолчанию /var/log/xferlog, что может быть изменено при
помощи опции xferlog_file.
Default: NO

xferlog_file
В параметре этой опции можно указать альтернативный путь к файлу журнала записываемому в стиле wu-ftpd. Запись в этот журнал производится только при включенной xferlog_eneble опции, включительно с xferlog_std_format. Также журнал ведется если включена опция dual_log_enable.
Default: /var/log/xferlog

vsftpd_log_file
В этой строке можно указать альтернативный путь к файлу журнала, записываемому в стиле vsftpd. Этот журнал ведется если опция xferlog_enable включена, и xferlog_std_format остается не выбрана. Также журнал ведется если включена опция dual_log_enable. Важно не забыть, при включенной syslog_enable опции, этот файл не записывается и вывод вместо этого напрвляется в системный журнал.
Default: /var/log/vsftpd.log