Очень хороший материал с примерами и описанием

Взято: http://www.bog.pp.ru/work/vsftpd.html

vsftpd (Very Secure Ftp Daemon) разрабатывался Chris Evans, недовольным уровнем безопасности, производительности и сложностью настройки как "классического" FTP-сервера wu-ftpd , так и ProFTPD . Бесплатен (GPL). Текущая версия - 2.0.5 (июль 2006). Настраивается с помощью одного очень простого файла конфигурации (можно иметь несколько экземпляров, привязанных к разным адресам и/или портам). Возможен запуск в автономном режиме или через inetd/xinetd. Поддерживается SSL, IPv6, виртуальные пользователи, управление трафиком, настройки в зависимости от имени и IP адреса пользователя.

Настройка vsftpd 2.0.1

Сам сервер (/usr/sbin/vsftpd) имеет ровно один параметр - имя файла конфигурации.

Файл конфигурации (обычно /etc/vsftpd/vsftpd.conf) состоит из директив. Каждая директива располагается на отдельной строке. Строка, начинающаяся с "#", является комментарием. Директива состоит из имени опции и значения, разделённых символом "=" без пробелов. Опции делятся на логические (NO, YES), строчные и неотрицательные целые:

- режимы работы и общие параметры
- listen NO (автономная работа без inetd/xinetd)
- listen_ipv6 NO
- listen_address
- listen_address6

- listen_port 21 (в автономном режиме)
- ftp_data_port 20
- background NO (перейти в фоновый режим при автономном запуске)
- async_abor_enable NO
- connect_from_port_20 NO (при включении исходящие с сервера соединения исходят с порта 20, при выключении сервер может работать с несколько меньшими привилегиями)
- ascii_download_enable NO
- ascii_upload_enable NO
- one_process_model NO (один процесс на пользователя вместо 2, быстрее, но менее безопасно)
- pasv_enable YES (разрешить режим PASV)
- pasv_min_port 0
- pasv_max_port 0
- pasv_promiscuous NO (не делать проверок параметров PASV)
- pasv_address (по умолчанию, для PASV берётся адрес сокета)
- port_enable YES (разрешить режим PORT)
- port_promiscuous NO (не делать проверок параметров PORT)
- run_as_launching_user NO (сервер будет работать от имени запустившего пользователя)
- tcp_wrappers NO (переменная VSFTPD_LOAD_CONF в /etc/hosts.allow задаёт имя конфигурационного файла vsftpd)
- use_sendfile YES (использовать sendfile() для ускорения работы)
- nopriv_user nobody (под этим пользователем сервер работает, когда ему не нужны никакие привилегии, лучше завести специального пользователя)
- secure_chroot_dir /usr/share/empty (сюда сервер делает chroot, когда ему не нужен доступ к файловой системе)

- аутентификация и права входа
- local_enable NO (использовать /etc/passwd для аутентификации пользователей)
- userlist_enable NO (пользователи из файла, заданного опцией userlist_file, не допускаются до запроса пароля)
- userlist_deny YES (если задать NO, то будут допускаться только пользователи, указанные в файле, имя которого задаётся опцией userlist_file)
- userlist_file (имя файла содержащего имена запрещённых или допустимых пользователей)
- check_shell YES (проверять /etc/shells при попытке входа локальных пользователей)
- guest_enable NO (все неанонимные входы рассматриваются от имени гостевого пользователя; это позволяет производить аутентификацию с помощью PAM (pam_userdb) относительно файла имён виртуальных пользователей)
- guest_username ftp
- no_anon_password NO (не запрашивать пароль анонимных пользователей)
- secure_email_list_enable NO (пароли анонимных пользователей задаются в файле /etc/vsftpd.email_passwords)

- email_password_file /etc/vsftpd.email_passwords (имя файла, содержащего пароли анонимных пользователей)
- virtual_use_local_privs NO (виртуальные пользователи будут иметь привилегии локальных пользователей вместо анонимных)
- pam_service_name ftp
- user_config_dir (позволяет задавать часть параметров в зависимости от имени пользователя; из этого каталога читается файл с именем пользователя, который рассматривается как дополнение к файлу конфигурации)
- user_sub_token (генерация имени домашнего каталога для виртуальных пользователей (см. guest_enable) по шаблону, например с использованием $USER)

- авторизация общая
- cmds_allowed (список допустимых команд протокола FTP)
- deny_file (шаблон имён запрещённых файлов, "deny_file={*.mp3,*.mov,.private}")
- hide_file (шаблон невидимых файлов)
- download_enable YES (позволять чтение файлов)
- dirlist_enable YES (позволять листинг каталогов)
- force_dot_files NO (показывать в листинге каталогов имена файлов, начинающиеся с '.')
- hide_ids NO (скрывать имена владельцев файлов и группы)
- ls_recurse_enable NO
- text_userdb_names NO (показывать текстовые имена пользователей и групп в листинге)
- use_localtime NO (использовать локальное время вместо UTC)
- write_enable NO (позволять команды STOR, DELE, RNFR, RNTO, MKD, RMD, APPE, SITE)
- tilde_user_enable NO (разрешать в именах файлов конструкции "~" и "~имя-пользователя")

- права локальных пользователей
- chroot_list_enable NO (в файле /etc/vsftpd.chroot_list задаётся список пользователей, при аутентификации которых деляется chroot в их домашний каталог)
- chroot_list_file /etc/vsftpd.chroot_list
- chroot_local_user NO (при аутентификации всех локальных пользователей деляется chroot в их домашний каталог, в этом случае chroot_list_enable задаёт список исключений)
- passwd_chroot_enable NO (имя каталога для chroot извлекается из /etc/passwd по строке "/./")
- chmod_enable YES (SITE CHMOD для локальных пользователей, анонимные пользователи не могут в любом случае)
- local_umask 077
- local_root (в какой каталог переходить для локальных пользователей)

- права анонимных пользователей
- anonymous_enable YES
- anon_world_readable_only YES
- anon_upload_enable NO
- anon_umask 077
- anon_mkdir_write_enable NO
- anon_other_write_enable NO (удаление, переименование и др.)
- chown_uploads NO (владелец анонимно загруженного файла устанавливается параметром chown_username)
- chown_username root
- anon_root (в какой каталог переходить для анонимных пользователей)
- ftp_username ftp (с правами какого пользователя обрабатывать анонимные запросы, домашний каталог этого пользователя будет корнем доступа)

- журналы и сообщения
- xferlog_enable NO (журнал загрузок и записей в /var/log/vsftpd.log)
- xferlog_std_format NO (записывать журнал в формате wu-ftpd в /var/log/xferlog)
- dual_log_enable NO (записывать оба журнала: /var/log/xferlog и /var/log/vsftpd.log)
- syslog_enable NO (журнал выводится через syslog , подсистема FTPD)
- vsftpd_log_file /var/log/vsftpd.log (имя журнала в формате vsftpd)
- xferlog_file /var/log/xferlog (имя журнала в формате wu-ftpd)
- log_ftp_protocol NO
- no_log_lock NO
- session_support NO (поддержка сессий: запись в utmp и wtmp; pam_session)
- setproctitle_enable NO (состояние сессии показывается в списке процессов)
- banner_file (файл с текстом приветствия)
- ftpd_banner (текст приветствия)
- dirmessage_enable NO (при входе в каталог пользователь получает сообщение из файла .message)
- message_file .message (позволяет задать имя файла с сообщением в каталоге)

- SSL
- ssl_enable NO
- ssl_sslv2 NO
- ssl_sslv3 NO
- ssl_tlsv1 YES
- allow_anon_ssl NO (разрешать анонимным пользователям пользоваться SSL)
- force_local_data_ssl YES
- force_local_logins_ssl YES
- dsa_cert_file
- rsa_cert_file /usr/share/ssl/certs/vsftpd.pem
- ssl_ciphers DES-CBC3-SHA

- интервалы ожидания (в секундах)
- accept_timeout 60 (для PASV)
- connect_timeout 60 (для PORT)
- data_connection_timeout 300 (замирание в процессе передачи данных)
- idle_session_timeout 300

- управление трафиком (в байтах в секунду) и нагрузкой
- anon_max_rate 0
- local_max_rate 0
- max_clients 0
- max_per_ip 0
- trans_chunk_size 0

Установка vsftpd 2.0.5 в Fedora 7 для доступа в домашний каталог (хост для стенда)

Устанавливал из пакета vsftpd-2.0.5-17.fc7 (i386). Требуется пустой каталог /usr/share/empty/ и отдельный пользователь (я взял пользователя ftp, в качестве домашнего каталога /var/ftp, пользователь ftp не является его владельцем, /sbin/nologin). В состав пакета входят скрипт запуска (/etc/rc.d/init.d/vsftpd, для каждого файла конфигурации /etc/vsftpd/*.conf запускается свой экземпляр сервера), /etc/pam.d/vsftpd (/etc/vsftpd/ftpusers используется как запретительный список) и настройка ротации журналов (/etc/logrotate.d/vsftpd.log).

Настройка /etc/vsftpd/vsftpd.conf:

- listen=YES
- listen_port=21
- ftp_data_port=20
- listen_ipv6=NO
- async_abor_enable=YES
- connect_from_port_20=YES
- ascii_upload_enable=YES
- ascii_download_enable=YES
- pasv_enable=YES

- # соответственные правила в iptables
- pasv_min_port=от
- pasv_max_port=до
- pasv_promiscuous=NO
- port_enable=YES
- port_promiscuous=NO
- tcp_wrappers=NO
- nopriv_user=ftp
- #
- local_enable=YES
- userlist_enable=YES
- userlist_deny=NO
- # сюда список допущенных к своим домашним каталогам
- userlist_file=/etc/vsftpd/user_list_enable
- check_shell=NO
- guest_enable=NO
- pam_service_name=vsftpd
- #
- download_enable=YES
- dirlist_enable=YES
- force_dot_files=YES
- hide_ids=NO
- ls_recurse_enable=YES
- text_userdb_names=YES
- use_localtime=NO
- write_enable=YES
- tilde_user_enable=NO
- #
- chroot_list_enable=NO
- # домашний каталог будет выглядеть как корень
- chroot_local_user=YES
- chmod_enable=YES
- local_umask=022
- #
- anonymous_enable=NO
- anon_world_readable_only=YES
- anon_upload_enable=NO
- anon_mkdir_write_enable=NO
- anon_other_write_enable=NO
- chown_uploads=NO
- anon_root=/tmp
- ftp_username=ftp
- # патронов не жалеть
- xferlog_enable=YES
- xferlog_file=/var/log/xferlog.log
- xferlog_std_format=YES

- dual_log_enable=YES
- syslog_enable=YES
- vsftpd_log_file=/var/log/vsftpd.log
- log_ftp_protocol=YES
- no_log_lock=NO
- session_support=YES
- setproctitle_enable=YES
- ftpd_banner=Welcome to ... FTP service.
- dirmessage_enable=NO
- #
- ssl_enable=NO
- #
- accept_timeout=60
- connect_timeout=60
- data_connection_timeout=300
- idle_session_timeout=300

Настройка iptables в /etc/sysconfig/iptables

-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport от:до -j ACCEPT

Запуск:

service vsftpd start # смотрим в журнал syslog
chkconfig --level 345 vsftpd on

Проблема с SELinux : как обычно, политика ограничивающая права процесса vsfdpd неправильная. Эту политику можно править , но проще тупо скопировать /usr/sbin/vsftpd в /usr/sbin/vsftpd2 (и поменять /etc/init.d/vsftpd).

Установка vsftpd 2.0.5 в CentOS 5.0 для анонимного доступа (репозитарий)

Устанавливал из пакета vsftpd-2.0.5-10.el5 (x86_64). Требуется пустой каталог /usr/share/empty/ и отдельный пользователь (я взял пользователя ftp, в качестве домашнего каталога /var/ftp, пользователь ftp не является его владельцем, /sbin/nologin). Предполагаемый каталог для раздачи: /var/ftp заменён на /mirror/anonftp. В состав пакета входят скрипт запуска (/etc/rc.d/init.d/vsftpd, для каждого файла конфигурации /etc/vsftpd/*.conf запускается свой экземпляр сервера), /etc/pam.d/vsftpd

(/etc/vsftpd.ftpusers используется как запретительный список) и настройка ротации журналов (/etc/logrotate.d/vsftpd.log).

Настройка /etc/vsftpd/vsftpd.conf:

- anonymous_enable=YES
- local_enable=NO
- write_enable=NO
- anon_upload_enable=NO
- anon_mkdir_write_enable=NO
- anon_other_write_enable=NO
- xferlog_enable=YES
- connect_from_port_20=YES
- xferlog_std_format=YES
- nopriv_user=ftp # ?
- async_abor_enable=YES
- ascii_download_enable=YES
- ftpd_banner=текст приглашения
- ls_recurse_enable=YES
- pam_service_name=vsftpd
- userlist_enable=YES
- listen=YES
- listen_address=IP-адрес
- tcp_wrappers=YES
- hide_ids=YES
- syslog_enable=YES
- # соответственные правила в iptables
- pasv_min_port=от
- pasv_max_port=до
- anon_root=/mirror/anonftp
- local_root=/mirror/anonftp
- guest_enable=NO
- anon_world_readable_only=YES

Настройка iptables в /etc/sysconfig/iptables

```
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport от:до -j ACCEPT
```

Запуск:

service vsftpd start # смотрим в журнал syslog
chkconfig --level 345 vsftpd on

Проблема с SELinux : в CentOS 5 имеется политика ограничивающая права процесса vsfdpd. Эту политику можно править , но я тогда об этом не знал и предпочёл тупо скопировать /usr/sbin/vsftpd в /usr/sbin/vsftpd2 (и поменять /etc/init.d/vsftpd).

Установка vsftpd 2.0.1 в CentOS 4.5 для анонимного доступа (репозитарий)

Устанавливал из пакета vsftpd-2.0.1-5.EL4.5. Требуется пустой каталог /usr/share/empty/ и отдельный пользователь (я взял пользователя ftp, в качестве домашнего каталога /var/ftp, пользователь ftp не является его владельцем, /sbin/nologin). Предполагаемый каталог для раздачи: /var/ftp заменён на /mirror/anonftp. В состав пакета входят скрипт запуска (/etc/rc.d/init.d/vsftpd, для каждого файла конфигурации /etc/vsftpd/*.conf запускается свой экземпляр сервера), /etc/pam.d/vsftpd (/etc/vsftpd.ftpusers используется как запретительный список) и настройка ротации журналов (/etc/logrotate.d/vsftpd.log).

Настройка /etc/vsftpd/vsftpd.conf:

- anonymous_enable=YES
- local_enable=NO
- write_enable=NO
- anon_upload_enable=NO
- anon_mkdir_write_enable=NO
- anon_other_write_enable=NO
- xferlog_enable=YES
- connect_from_port_20=YES
- xferlog_std_format=YES
- nopriv_user=ftp # ?
- async_abor_enable=YES
- ascii_download_enable=YES
- ftpd_banner=текст приглашения
- ls_recurse_enable=YES
- pam_service_name=vsftpd
- userlist_enable=YES
- listen=YES

- listen_address=IP-адрес
- tcp_wrappers=YES
- hide_ids=YES
- syslog_enable=YES
- # соответственные правила в iptables
- pasv_min_port=от
- pasv_max_port=до
- anon_root=/mirror/anonftp
- local_root=/mirror/anonftp
- guest_enable=NO
- anon_world_readable_only=YES

Настройка iptables в /etc/sysconfig/iptables

-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport от:до -j ACCEPT

Запуск:

service vsftpd start # смотрим в журнал syslog
chkconfig --level 345 vsftpd on