www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

FTP services

Setting up FTP services on today's servers is straight forward.

A few rules I use for most setups:

1) If you have a VM farm, use a separate virtual machine for FTP. It's not worth the security concerns by putting this on your main web server or application server.
2) Configure Passive FTP. This way, you are controlling the firewall issues and can open ports on the firewall to create a problem free user experience
3) KISS – Keep it simple Sam/Sally, FTP services have a lot of configuration options. Keep it to a bare minimum of changes needed for your environment.

To setup a basic non-authenticated ftp service, it's as simple as:

- Apt-get install vsftpd
- Modify /etc/vfstab.conf to update configurations

```
# Enable passive ftp and assign 10 ports available for data transfer
 pasv_enable=YES
 pasv_min_port=11000
 pasv_max_port=11010

#Ensure users are chroot to their local home directory
# Setup a list of exceptions so
chroot_local_user=YES

#Explicitly list the users that can go outside their home directory
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list

#Change the banner to something meaningful for users
ftpd_banner=Welcome to blah FTP service.

# Uncomment this to allow local users to log in.
local_enable=YES

# Uncomment this to enable any form of FTP write command.
write_enable=YES
```

- Restart the service
  - Service vsftpd start

www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

- Add local users
  - Add a single user as the administrator that isn't chroot'ed to their own home directory. This should be a trusted admin that can access all data.
    - Edit the file: etc/vsftpd.chroot_list and add 1 user as the administrator

The server is now setup to run FTP with local users that are define in /etc/passwd. Now, we need to ensure that the Firewall doesn't get in the way.

Firewall Configurations

For our configuration, we're using a Netscreen firewall. First you need to setup the ability to connect into the different ports. Since we did passive FTP, there's the main channel port on 21 plus back-end ports from 11001 to 11010.

```
#Define custom services for ports 11001 to 11010
set service "ftp-passive1" protocol tcp src-port 0-65535 dst-port 11001-11001
set service "ftp-passive2" protocol tcp src-port 0-65535 dst-port 11002-11002
set service "ftp-passive3" protocol tcp src-port 0-65535 dst-port 11003-11003
set service "ftp-passive4" protocol tcp src-port 0-65535 dst-port 11004-11004
set service "ftp-passive5" protocol tcp src-port 0-65535 dst-port 11005-11005
set service "ftp-passive6" protocol tcp src-port 0-65535 dst-port 11006-11006
set service "ftp-passive7" protocol tcp src-port 0-65535 dst-port 11007-11007
set service "ftp-passive8" protocol tcp src-port 0-65535 dst-port 11008-11008
set service "ftp-passive9" protocol tcp src-port 0-65535 dst-port 11009-11009
set service "ftp-passive10" protocol tcp src-port 0-65535 dst-port 11010-11010

#Configure pinholes in the firewall for both port 21 and the backend ports:
set interface ethernet3 vip  204.5.5.5 + 21 "FTP" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11001 "ftp-passive1" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11002 "ftp-passive2" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11003 "ftp-passive3" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11004 "ftp-passive4" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11005 "ftp-passive5" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11006 "ftp-passive6" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11007 "ftp-passive7" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11008 "ftp-passive8" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11009 "ftp-passive9" 10.10.10.10
set interface ethernet3 vip 204.14.50.213 + 11010 "ftp-passive10" 10.10.10.10

#Define the services
set service "FTP"
set service "ftp-passive1"
set service "ftp-passive2"
set service "ftp-passive3"
set service "ftp-passive4"
set service "ftp-passive5"
```

www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

set service "ftp-passive6"
set service "ftp-passive7"
set service "ftp-passive8"
set service "ftp-passive9"
set service "ftp-passive10"

Test the site

1) Ensure Anonymous access works. Try it from a web page and ensure it's working
2) Test a standard user and ensure they are chrooted to their home directory and can only see files in that directory.
3) Test the Administrator and ensure it can see both that directory and any other directory on the site