**INSTALLING AND CONFIGURING SecureFTP (ftp over ssh traffic)**

* Create ftp group: #Sudo groupadd <user\_group>
* Create ftp user: #useradd <user\_name>
* Add user to group: #usermod –G <user\_group> <user\_name>
* Verify user info: #id <user\_name>
* Edit /etc/ssh/sshd\_config and replace the following line:

Subsytem sftp /usr/libexec/openssh/sftp-server

Whith the following:

Subsystem sftp internal-sftp

* Add the following to end of the same file above:

Match Group <user\_group>

X11Forwarding no

ChrootDirectory /home

ForceCommand internal-sftpid subaru

Save and exit

* Restart ssh service.

**HARDENING PORT SECURITY OF SFTP**

In order to secure the sftp traffic we need to separate the sftp port to be other port than the ssh port 22.

This is done by adding one more interface and configure ssh to listen to each interface on ssh to other ports (on interface will listen for example to port 990 only for sftp users traffic and the and one will listen to port 22 to regular ssh sessions.

To accomplish this do the following:

* Edit the file sshd\_config as following:

If exist line of ListenAddress comment it.

* Create new lines as following:

ListenAddress x.x.x.x:22 #listening to regular ssh sessions

ListenAddress y.y.y.y:990 #listening to sftp sessions

* Restart ssh service

To add:

Create public and private key in the user home directory as the user

ssh-keygen -t rsa

create authorized\_keys and paste the public certificate

create ppk file from the private key and connect