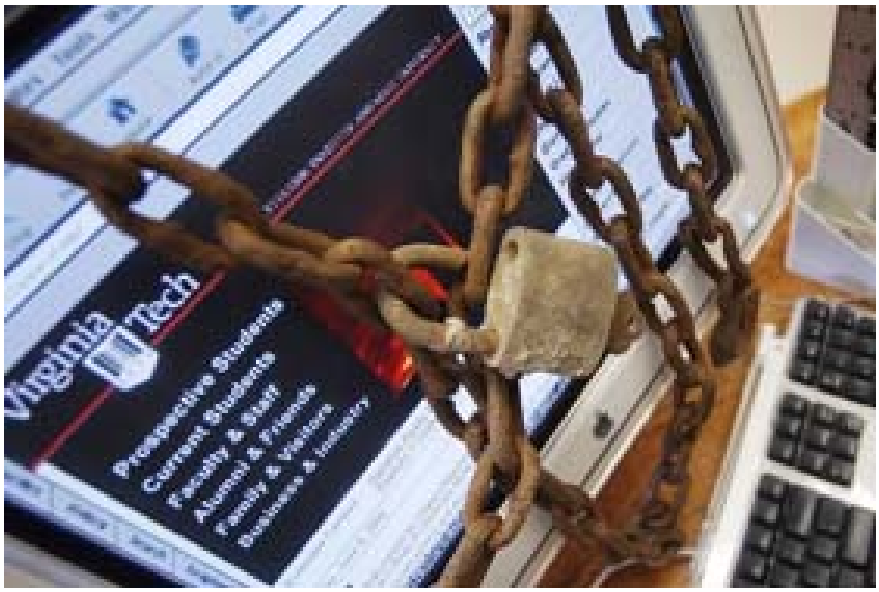
Use rssh to restrict user access

rssh, can be used to solve the situation of providing services that require shell access but does not actually allow users to gain access.



Network Administration - There will be times when you want to provide services that require *shell* access but do not actually allow users to access this. At this point, the shell is limited, rssh, can be used to solve this situation for you .

At first it seems to be quite contradictory, but there will be times when a system administrator has a legitimate need to provide access-based shell services to users that are indeed normal. Do not allow them this access on the system. Providing shell access to users, especially if they are untrusted users, can be a serious security issue for system administrators.

An example is using OpenSSH to provide SFTP accounts so that users can transfer files to and from secure servers. OpenSSH requires shell access to provide SFTP access. However, we still have a limited shell called rssh that can provide shell access to servers such as OpenSSH but does not provide an interactive shell environment to be abused by user.

The rssh tool is available in the software repository of Unix-like open source systems, such as Debian GNU / Linux and FreeBSD. Debian's apt-cache search command has something to say about it:

rssh - Restricted shell allows only scp, sftp, cvs, rsync and / or rdist

You can find more information about the program at its home page.

After installing it with the original software management tools of the Linux or BSD Unix system, calling and working with the tool is a very simple task. Just create an account that you want to use rssh with your system's standard account creation utilities, then set its default shell to rssh. When this is done, you can test the account's configuration by logging it via ssh. The connection will be closed before login is complete, with a message explaining that the account has been restricted with rssh.

However, for those who want to allow the default account to be able to do something, it will prevent other ways of using the account such as SFTP by default. To allow SFTP, rssh needs to be explicitly configured to do so. Finding the rssh.conf file, its location will depend on the specific system where you installed it, but usually it is still /usr/local/etc/rssh.conf, then edit it to contains the following line, its purpose is to allow SFTP connections:

permissionftp

Similar configuration options are available in other tools that rssh supports, and you can also provide users with access to specific resources on the system without having to provide them. they are able to log in directly with an interactive shell.