Restricting users to specific folders via SFTP

677 Jisna Joseph April 20, 2025 Features & Functionalities, Security Compliances 5535

How to Restrict SFTP Connections to Specific Ports?

Overview: This article explains how to restrict SFTP connections to specific ports using SSH configuration, chroot directories, and user group settings to enhance security.

SFTP, or Secure File Transfer Protocol, is a subsystem of SSH used for securely accessing, managing, and transferring large files of data. **Chroot** or **change root** is a security feature that restricts users to a certain directory and prevents them from accessing locations outside of their specified directory. To restrict SFTP connections to specific ports you can have another **ssh daemon running on a different port** and force **internal sftp** for users connecting on that port alone.

Step 1: Create a separate directory for Ezeelogin gateway users for file transfer.

```
root@gateway:~# mkdir -p /sftp/ezadmin
```

Step 2: Apply suitable permissions for the '**/sftp**' directory.

```
root@gateway:~# chmod -R 755 /sftp/
```

Step 3: Edit the SSH configuration file, and add the following lines at the end.

```
root@gateway:~# vim /etc/ssh/sshd_config

Port 22
Port 2244

Subsystem sftp internal-sftp
Match LocalPort 2244 Group ezuser
  ChrootDirectory /sftp/%u
  ForceCommand internal-sftp
```

Step 4: After making changes to the SSH configuration file, restart the SSH service for the changes to take effect.

```
root@gateway:~# systemctl restart sshd
```

From the above configuration users connecting to the port **22** via **ssh** would be assigned to the **ezsh shell** and provide **SFTP** access for specific users under the group "**ezuser**" on a custom port, **2244** which ensures that the users under the group **ezuser** is limited to their home directory under '**/sftp**'. This chrooting mechanism increase security by limiting users access to their specified directories and prevent them from navigating to other directories outside of their specified directory.

```
root@AD-LAPHP-06:~# ssh admin@192.168.1.66 -p 2244
admin@192.168.1.66's password:
This service allows sftp connections only.
Connection to 192.168.1.66 closed.
root@AD-LAPHP-06:~#
```

```
root@AD-LAPHP-06:~# sftp -P 2244 admin@192.168.1.66
admin@192.168.1.66's password:
Connected to 192.168.1.66.
sftp>
sftp>
```

Related Articles:

Is there solution to show users only desired folders as they can see all other folders while using SFTP?

How to copy files from desktop to Gateway servers using WinSCP

Online URL: https://www.ezeelogin.com/kb/article/restricting-users-to-specific-folders-via-sftp-677.html