# **Threat Modeling**

We will be performing a threat modeling of the Secure File Transfer Protocol (SFTP) using the STRIDE framework.

## **Assumptions:**

The following assumptions are made regarding the below network architecture.

* The network contains two SFTP servers. One in the DMZ and another in the internal network to prevent direct access to the internal network from external attackers.
* Third party vendors are not trusted.
* Third party vendors cannot push files into the server. The SFTP server in the DMZ pulls files from the third party vendors.
* When files are pulled from third party vendors they’re stored into the internal SFTP server in plain text.
* Stored files are not scanned for any maliciousness.
* The scope of this threat model is concerned only with SFTP and assets that directly impact it.

# **What is SFTP?**

SFTP (FTP over SSH) a secure FTP protocol that sends files over SSH. Providing a high level of protection for file transfers. It also offers several ways to authenticate a connection – with a user ID and password, SSH key, or a combination of a password and SSH key – for organizations that require stronger authentication.

SFTP is slower but speed shouldn’t be the ultimate factor as it is only slightly slower. SFTP is firewall friendly since it only uses one port for communication (port 22).

The encrypted tunnel between the user and the SFTP server, protects all the sensitive data, user ID, passwords and commands.

You can connect your SFTP GoAnywhere to your AD, or LDAP to simplify account creation.

### **SFTP Server includes:**

* detailed audit logs of all SFTP sessions. (User ID, commands, IP addresses, and names of Files transferred).
* The activities can be viewed through on-demand reports. (which is either automatically generated, or scheduled).
* Event Triggers can monitor when transfers occur and automatically process files or send email notifications when files are uploaded or downloaded.
* There is an integrated key management system for SSH keys. You can create public and private keys and key length up-to 4096 bits.

GoAnywhere can be installed in a private network without opening any inbound ports when paired with goanywhere gateway in the DMZ. It can also be installed in a cluster for load balancing and redundancy to ensure maximum availability.

SFTP provides compliance for (PCI-DSS, HIPAA, Privacy laws, and Sarbaness-Oxley).

### **Two-Factor authentication using SSH Keys:**

1. Import the trading partner’s SSH public key into the key vault.
2. Configure the web user authentication type. (configure the web to use both password and SSH key).

### **Tips and tricks for securing SFTP.**

* Use strong encryption algorithm and disable the weak ones.
* use strong hash/mac algorithms to verify the integrity of the transmission. Like the SHA-2 family.
* Move files and user credentials and keys into the private network (private SFTP server). A control channel is opened between the private and the gateway, and the session that the third party vendor has is sent by the SFTP GW server over the control channel.
* Implement IP blacklist/whitelist. Auto-blacklist attacks like DoS attack.
* Good account management
* Strong password.