

# Introduction

General introductory topics about Syncplify R2FS!

- [What is Syncplify R2FS!?](#)

# What is Syncplify R2FS!?

**Syncplify R2FS!** (Remote-Reverse File System) is an optional component of **Syncplify Server!** designed to securely expose internal storage to your SFTP transfer server without opening inbound network access.

## The Core Idea

Traditional architectures require the server in the DMZ to initiate inbound connections toward backend storage. R2FS! inverts this model: **the storage side initiates and maintains an outbound, secure connection to the server.**

This “reverse” approach dramatically reduces the attack surface and simplifies firewall rules.

## How It Fits In

R2FS! integrates with the Virtual File System (VFS) of Syncplify Server!. To users accessing Syncplify Server! via its protocol-handlers (SFTP, FTPS, HTTPS), remote storage appears as a normal file-system path, even though it physically resides in a protected network.

## Why It Matters

- **No inbound firewall ports** required toward internal storage (subnet)
- **Strong authentication** using mutual TLS and or PSK
- **Clear network separation** between DMZ and private/subnet infrastructure
- **Compliance-friendly design** for regulated and highly-regulated environments
- **Scales naturally**, supporting multiple R2FS! nodes and high-availability setups

## Typical Use Case

An organization runs Syncplify Server! in a DMZ, while file data remains on internal systems in a separate and isolated subnet. R2FS! allows secure access to that data without exposing the internal network nor relaxing firewall policies.

## In Short

Syncplify R2FS! provides a secure, modern way to bridge DMZ-hosted file transfer services with internal storage by reversing the direction of trust and connectivity.