



Enterprise-Grade, Secure File Transfer

CrushFTP Technologies Overview

Overview

Put simply, CrushFTP is a secure high speed file transfer server that runs on almost any OS. It handles a wide array of protocols, and security options. It gives the server administrator the ability to customize, monitor, and control every aspect of the server's operations.

CrushFTP is stand alone and self contained. It doesn't run on top of another vendors' server code, or rely on another vendors application container. The HTTP server isn't based on Tomcat, or others. This means that when vulnerabilities are discovered for Tomcat, you don't have to go run and patch your server to keep it secure. CrushFTP maintains its own security stack, which is comprised of industry standard, enterprise-grade technologies. This also means that the protocol engines are designed from the ground up for file transfer. It's not an after thought where you have to see if the engine in the product can handle a large file, or protect against PHP exploits or other script vulnerabilities. CrushFTP does not run server side scripts as a web application server may do. CrushFTP specializes in file transfer, and does it very well. The HTTP engine in CrushFTP understands when a large file is being uploaded and avoids checking every incoming byte to look for the "end of file" signature that web browsers send. It knows it doesn't need to check for this until the file transfer is almost done. This saves on CPU usage considerably, and allows for faster transfers.

File Transport & Encryption

CrushFTP supports all the main file transfer protocols (FTP, FTPS, FTPES, SFTP, SCP, HTTP, HTTPS, AS2). It allows you to limit the usage of protocols on a global server level, or even on a per-user level. You may want to allow anonymous access to some general publications, but all protected files require a login, and you can refuse the logins if they are not sent over a secure protocol. You have control over the individual encryption ciphers used in encrypted protocols too. You may only want AES 256 encryption, and block less secure ciphers. You have that control. The encryption CrushFTP implements applies to both in stream data, and data at rest. File data is written to disk in encrypted form, and is only decrypted when the file is downloaded again by an appropriate user. AES or PGP based encryption can be used for data at rest. Additional security options include global & per-user IP address restrictions, and policies restricting activity during specific days of the week and time of day.

DMZ Options

CrushFTP offers the ability to act as a DMZ Gateway to other servers. You can put a secure CrushFTP in your DMZ giving access to legacy FTP servers on the other side. Data is not stored on the DMZ server, it is always streamed across so there are no store and forward operations. If people attempt to abuse the server, they are only reaching CrushFTP, and it detects abuse with its own intrusion detection mechanism, which bans a user's IP automatically to protect itself from robots and hack attempts. CrushFTP is also doing protocol conversion, so you can provide a SFTP server in front of your internal FTP server, or even a full featured web interface in front of the FTP server. If the internal server is another CrushFTP server, you can configure one way socket connections. This allows you to keep your firewall locked down, and the internal CrushFTP will connect outgoing to the DMZ CrushFTP to handle the incoming requests.

Auditing & Reporting

Every action taken in CrushFTP is audited. There is a detailed log file tracking changes to all settings, and actions that users take. You can see attempted and successful actions. You can see which administrator makes a change to the user's IP restrictions as the change is logged with before and after results. Additionally, a statistics database is tracking logins and file transfers allowing for reports to be run against this data. Built-in reports can be automated and emailed on a schedule in both HTML and CSV formats. The interface allows real-time monitoring of what is going on. You can see how many users are connected, and see their individual session transcripts, file transfers, time remaining, etc. You can see what your server is really doing.

User Management

User management in CrushFTP is separate from the OS users, and extremely granular. Individual settings can be inherited from other template users. The virtual file systems from multiple users can be merged together into a single file system that the user sees. This simplifies management as you can make a change in one location, and everyone inheriting that setting instantly gets the change applied to them as well. The individual folders and files a user has access to can all be controlled. Allow uploads to one folder, downloads to another, set a quota on another, etc. User management and server administration is entirely web based. Regulatory compliance is easy to do in CrushFTP. You can limit the server to only secure protocols, preventing users from ignoring security considerations. The file at rest encryption can be globally enabled, and only high strength cryptography allowed.

Bandwidth Control and Acceleration

Bandwidth utilization is available on the main interface of CrushFTP. You can limit bandwidth globally for the entire server, or at an individual user level. You can also accelerate transfers to use your full bandwidth regardless of your network latency or distance. This acceleration is done over HTTPS and does not require special ports, or UDP allowances. Its pure, accelerated TCP/IP HTTPS transfers are built into the web interface. The acceleration is not based strictly on files either. You can take an unsecured FTP connection and tunnel it through the HTTPS acceleration giving users much greater speeds for their file transfer. Some other protocols can be tunneled and accelerated too as the bandwidth acceleration works in stream. If a connection breaks, it's automatically reconnected, and transfers continue uninterrupted. Full speed transfers around the world, using up to all the bandwidth you have available. Stand alone CrushTunnel instances can be used as well creating dedicated acceleration gateways. A single gateway can handle as many connections as you want, combining and accelerating them all in stream at the same time.

WebInterface

The web interface of CrushFTP is one of the more powerful file transfer areas. Since the HTTP engine in CrushFTP is self contained, and tightly controlled, it's designed for speed. Users can view file listings, see thumbnails of files, preview slideshows of images, upload, download, rename, and delete. Downloads can be zipped so the users can retrieve an entire folder at one time, and save on bandwidth. Uploads can also be zipped, and entire folders can be uploaded all from the browser as well. Zipped uploads are transparently zipped in the browser as they are being uploaded, and unzipped by the server as they are being received. Users can track keywords on files, search the files they have access to, and even share the files with colleagues. Shared files self expire after a specified amount of time. Users can temporarily grant access to one of their own folders, and monitor and manage that access they have granted. You as the server administrator can control if the user can do this, and you can of course override the shares they may have created. This is real ad hoc file transfer, with email notifications going out with a unique URL to access the share, and if you choose, event notifications when the recipient downloads, or uploads files back to you.

Process Automation

Job scheduling, monitoring and editing can all be done in the web interface as well. Jobs can do almost an unlimited number of tasks. Finding files on a remote SFTP server, pulling them down to your server, renaming them, zipping them, PGP encrypting them with a user's public key, then uploading them off to three other servers all at the same time across multiple threads, and finally emailing a user letting them know they are there. If an error occurs, alternate steps can be taken, or HTTP service POSTS and notifications sent. Folder Monitor is a special module that allows the server admin to monitor any number of directories, and implement a 'move' or 'delete' policy based on the age and/or filename. Folder Monitor can also perform tasks once file age & filename conditions are met. With all of that completing in what jobs can do, you can see in a live visual flow of the progress of the job, what it's working on, a live view of its log file, and more. Jobs will resume where they left off if the server is restarted, or a clustered server can take over the job if the primary goes offline.

Virtual File Systems

Each user can have a complex filesystem referencing local folders, and remote locations. They could be pointed to a UNC location, SMB, FTP, SFTP, and many other protocols including Amazon S3 buckets. To the end user, they don't really know where they're working from, or the complexities of how that file system works, they just see a standard view in their client or WebInterface. Gigabit speed transfers with an Amazon S3 bucket are now possible with the accelerated S3 VFS engine too.

Remote Sync & Replication

CrushSync can be used for real time file synchronization with CrushFTP. End users can run CrushSync and link it to a folder. Any changes made to that folder are replicated to the CrushFTP server. Anyone else synced with that folder than immediately receives those changes, and changes they make can work in reverse. Delta based changes are sent whenever possible so large files sync very quickly after a change. End users can use encryption in their client so that the server's data is encrypted in a format the server admin can never access, only the end user clients have their own keys to their data. This all works with bandwidth acceleration for long distance transfers too. Clients in Europe can be synchronized with clients in the US with a backup of all data on a centralized server, including revisions of files. Conflict changes are handled and managed too. Another use is dropping a file in a folder, and all your subscribed clients instantly get that file distributed to them. When you're done with the file, delete it, and it's removed from all the subscribed clients. The subscribed clients can be read only, so any changes they make, don't replicate back to the server. Only the master user can control the distributions and actions in the subscribed folder.