CIODIVE

OPINION

Real risks of using file transfer protocol

By Chandra Shekhar

Published July 30, 2018

Editor's note: The following is a guest article from Chandra Shekhar, technology analyst at Adeptia Inc.

Today's businesses primarily function on data — facts, figures, values. However, the same data becomes a nasty drain clog when it stockpiles. Enterprises face significant financial losses if they can't bring data to the right place at the right time.

File transfer protocol (FTP), the standard protocol for data sharing, solves less than half of this problem. This protocol doesn't scale beyond 30 connections and its failure rate of 8% is too expensive. Apart from costs surrounding this protocol, there are several reliability, security, auditing and flexibility issues associated with it.

What is FTP?

FTP is an application layer protocol used for the transfer of files between a client and server. It was developed 30 years ago in 1971 on a client-server model architecture. This protocol supports only three data structures: file structure, record structure and page structure.

It is not considered as a secured protocol per today's standards. Users don't get the ability to encrypt and protect data.

FTP is an ideal file sharing platform for small to medium-size enterprises which have basic file transfer requirements. It doesn't scale to support enterprise integration needs like any-to-any data transfer, large file ingestion, etc.

Downsides of FTP

The saying, "If something sounds too good to be true, it probably is" can be applied to FTP solutions laced with hidden cost.

In the beginning, FTP solutions look cost effective and straightforward. However, the total cost of ownership expands when the underlying codes gain volume. For instance, a lot of coding goes into the background for the creation of scripts, notifications and events. As these codes continue to pile up, updating them becomes a massive effort.

Here are some other downsides of FTP solutions:

Weak IT security

FTP exposes data transmissions to many vulnerabilities because they don't offer capabilities for data encryption. Users refer proxy FTP whenever there's a slow network, which sets a direct transmission between two servers. A hacker can use a PORT command to access ports and gain access to data by disguising himself as a middleman.

FTP is also vulnerable to brute force attack which can break down weak and repeatedly used passwords. Hacker can use packet capture techniques to capture transmitted data packets and decode them. Networks adhering to federal compliance norms such as PCI DSS, HIPAA and GLBA cannot rely on it.

Absence of IT governance

FTP lacks controls for data management. Teams don't have a clear idea about who owns the data and how long it is usable. It is not a cutting-edge solution for extreme file movements. Sending gigabytes of files on an outdated UI can be really painful. Setting up FTP solutions is a nightmare as thousands of developers work independently on different interfaces to write codes.

No reporting feature

FTP solutions don't provide any status about information sent or received upon transmission of data. The users don't get to know about disruptions or problems occurring to data transmission. Tracking high volume or multiple file transfers can be daunting with FTP solutions.

Lack of automation

FTP solutions cannot be automated and customized for high volume file transfer workflows. FTP servers don't have process management framework to automate operations across multiple servers. Lengthy lines of coding needs to be generated for scheduling file transfers, applying routing triggers or changing passwords and IP.

Alternatives to FTP

FTP has become over 30 years old and it is not suitable for high-volume transactions and multiple requirements.

Here are some top alternatives to FTP:

SFTP

Also known as Secure FTP Secure, SFTP is a Shell (SSH) based program to transfer files. It enables SSH encryption for ensuring

secure data exchange over an unsecured network. SSH is an advanced encryption technique that scrambles data and provides access to only those users who have appropriate keys.

Modern-day SFTP solutions leverage 256-bit advanced encryption techniques to safeguard data as much as possible. Moreover, next-generation SFTP also provides dedicated IP support to cloud-based solutions. However, there are snags attached with SFTP too:

- Heavy developer support is needed for installing, configuring and using SFTP software.
- Many SFTP deployments use OpenSSH/SFTP protocols, which do not ban a user for invalid authentication.
- SFTP doesn't maintain a log of user activity.

Hypertext transfer protocol (HTTP)

Another good alternative to FTP which makes file transfers fast and smooth is HTTP. The advantage with HTTP is that it can work on popular web browsers. File transfers can be enabled and managed through Chrome and Firefox.

A browser-based HTTP connection is used for sending and receiving HTTP commands, and any user with a browser can exchange files. A popular example of HTTP is webpage where information is fetched from remote web server to a browser. However, HTTP file transfer also suffers from unique disadvantages:

- A new connection needs to be established for transferring files which is not a technically feasible option for large file data exchange where there are thousands of partners.
- Specialized tools like curl or wget are needed for heavy uploads.
- HTTP connection on the web can breached by hackers.

MFT: All industry-standard protocols at one place

The newest technology for B2B data exchange is managed file transfer (MFT) protocol. MFT is an industry best secure communications framework which supports multiprotocol managed file transfers.

It provides the ability to transport and replicate data from one location to another in simple steps. This approach ensures timely delivery of data to partners and customers. It allows synchronization, orchestration and validation of data within and outside the firewall.

MFT enables secure, standards-based exchange of EDI, EDIFACT and HL7 messages with trading partners and customers. It is a unified multi-protocol solution that ensures connectivity, reliability, security and ease of use during file transfers.

How MFT works

Managed File Transfer is not a protocol, it is a software and a service (SaaS) based technology platform. This platform enables data security, operational efficiency, governance and compliance.

MFT provides a single run-time engine or Enterprise File Transfer Command Center to manage all enterprise file transfers internally or externally. This command center automates the entire process of sending and receiving files. This platform allows users to exchange data with stringent security standards. A digital dashboard enables users to monitor and control file electronic data transfers across all open platforms.

Enterprise File Transfer Command Center provides access to logs of every data transfer taking place at local or central level. User can generate detailed reports of those transfers for compliance. Real-time alerts notify users about data failures or errors as and when

they happen. High-level clustering provides foundational support to fail-over activities.

Previously, only employees in an organization were generating data. However, in the present scenario smart machines, sensors and gadgets are also generating data for enterprises. Gartner predicts that enterprises will generate nearly 40 zettabytes of data by 2020. The average file size is expected to grow by 40 GB.

Conventional solutions like FTP and SFTP will be outmoded to manage and share this colossal amounts of data. Enterprises will need an MFT solution for sharing this data in a multi-dimensional network and ensuring continued success from their B2B operations.