International Journal
Information Technology Applications (ITA)

Volume 9, Number 2, December 2020

EVOLUTION OF MANAGED FILE TRANSFER IN BUSINESS TO BUSINESS

Shiva Prasad Paudel, Frank Schindler

Abstract:

In an era of digital world, data have became import part of our life. Every single day a tons of data are being exchanged over the internet. As of 2020, everyday 2.5 quintillion bytes of data are being produced and exchanged over internet. A2A, B2B, C2G and G2C rely on huge data exchange. Traditional transfer protocols like FTP, HTTP are not sufficient as they do not comply with security standards and hence a managed centralized system is necessary that not only can exchange data as traditional transfer protocols do but also can perform several other tasks like sending an SMS, sending an email, record activity so that data can be made available for analysis purpose and provide security requirement for authentication for example DFA and MFA. To fulfil the demand of modern world a managed system was created and the system is named as Managed File Transfer. This article describes evolution of MFT and importance of MFT in IoT, B2B and C2G.

Keywords:

Managed file transfer (MFT), B2B, C2G, G2C, A2A, FTP, HTTPS, SFTP, cloud.

ACM Computing Classification System:

Managed file transmission, business 2 business, consumer 2 government.

Introduction

Digitalization created a challenge to computer engineers to innovate technology day by day. In mid 90s people were hardly using computers and internet. Since 2000, internet users started increasing drastically and with the rise of smartphones, usage of internet got quadrupled [1]. Today, there is hardly any household that does not have internet connection. People started communicating digitally with their family, friends and public sectors. Digitalization in one hand made the life easier but on other hand, it raised concerns over data security and data piracy. Internet started being unsafe from data pirates, who were spying on every activity that we exchange. Identifying pirates was not easy so an approach was required to safe transfer of data. Organizations like NIST and PCI-DSS came with an approach and set certain standards that a corporation or an organization should comply with if it is exchanging sensitive data with its consumers. This standard became a must to financial and government sectors. Gigantic companies like IBM, Axway, Google took this opportunity and started developing a software/application. Software was developed to be compatible with both traditional protocols and new security standards and named the system as Managed File Transfers or MFT.

1 Traditional Protocols

Term traditional protocols refers to protocols that were developed in 4th quarter of 20th century and beginning of 21st century. Most common protocols used in transfer of files were FTP, HTTP, SFTP.

1.1. FTP

File Transfer Protocol or commonly abbreviated as FTP is a very common protocol. This protocol was developed in 1971 [2]. FTP is a client-server protocol that means a computer that initiates an FTP connection is called as client and the computer that receives request to establish a session is called as server. FTP requires two ports to transfer data. One port is control port to exchange command between client and server and the other port is data port. Default control port is 21 but data port is dynamic and based on type of mode these ports are agreed in advance before exchanging data.

1.1.1. Active mode

FTP transfer in active mode is controlled by a client machine. At the time of communication between host A to host B, client (host A) sends server (host B) information about data port that will be used by for data exchange. Server on other side checks the port and if the port is not in conflict with other clients, it acknowledges the port and deliver data to client on specified port. Active mode is useful when client and server do not reside behind the firewall, but this raises a concern when Network Addresses Translation (NAT) and firewall are in place. Since client randomly chooses data port, firewall would block the port and that could lead to ftp transmission failure.

1.1.2. Passive mode

FTP transfer in passive mode provides flexibility to the server to decide which port will be used by client for data transfer. Server chooses a random port from its port range and tells client to connect to that port. This is a very practical way of transfer because a port range (range of 100 ports) may be defined on server side and firewall rules may be enabled on both client and server to allow communication only to defined range. This provides an extra flexibility to a corporation to adhere with strict security and compliance rules. Both client and server machine may reside behind firewalls and still communicate with each other under strict security measures.

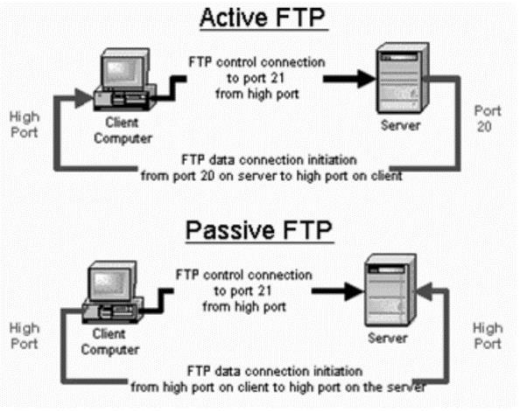

Fig.1. Active and passive FTP flow [3].

1.2. HTTP

Hypertext transfer protocol is an application layer protocol used widely by World Wide Web (WWW). This protocol was invented by Tim Berners-Lee and teams [4]. An HTTP functions as a request-response protocol. Request is initiated by a client machine and response is provided by a server. Client machine initiates a request for contents of a web page via web browsers (internet explorer, Mozilla, safari, opera etc.) and server in response provides the contents. Web page available in server may be of static type (HTML, CSS, JavaScript) or dynamic type (PHP, PERL, PYTHON, etc.).

1.2.1. Static web page

Static web pages use static contents like HTML, CSS and JavaScript. Static content means that data on page does not change. Static pages are simple in nature. Static pages are faster in getting response. These web pages do not use database to fetch data. Example of static website is www.nepslov.sk.

1.2.2. Dynamic web page

Dynamic web pages are written in complex language like PHP, ASP.NET, etc. Dynamic contents are first interoperated at server side and only after that data get fetched on client's browser. Dynamic web page uses database to fetch and store data from client's machine. Example of dynamic website is facebook.com.

1.3. SFTP

SSH File transfer protocol was discovered to ease file transfers from local to remote computer. Traditional FTP raised concerns over security and FTPS implementation was not easy for every user as it requires subscription to digital certificates. To tackle with these problems SSH FTP (SFTP) was invented. SFTP, though in beginning was not as popular as FTP but now a days it is one of the most used protocols. SFTP has replaced FTPS in many commercial and financial sectors. Unlike FTP/FTPS which use two different ports for communication i.e., one for control and one for data channel, SFTP uses only one port and whole communication between client and server is secured via secure channel. Hence, it gained more popularity in corporation where client and server reside behind firewall.

SSH File transfer uses keypairs (private/public) for authentication [5]. Private key resides on machine itself whereas public key is distributed and stored on remote server. When a client initiates a session to the server, server checks if the client's key is in its database or not and if not, session is aborted. If server finds a key in database, it sends a random text by encrypting it to the client. Client on other side decrypts the string using its corresponding private key. If client successfully decrypts the message, then server allows client to establish a session and transfer data. Whole communication between client and server is secured by using cipher suites. Cipher suites comprises these items:

1.3.1. Encryption algorithm

Encryption is a method of converting plain text string to the random string that cannot be decrypted by unauthorized person or computer. There are two types of encryption algorithms which are used in computer science and they are symmetric and asymmetric.

- Symmetric encryption - symmetric encryption uses the same key to encrypt and decrypt data between source and destination. HTTPS browsers use symmetric keys to encrypt/decrypt data between client's browser and web server. DES, DES3 and AES are symmetric encryption methods.
- Asymmetric encryption - asymmetric encryption uses different key to encrypt and decrypt data. SFTP uses asymmetric keys to encrypt and decrypt data between client and server. RSA and ECC are asymmetric encryption methods.

1.3.2. Key exchange algorithm

Key exchange algorithm is an algorithm that allows two machines residing in different location over internet to communicate by sharing a secret key over non-secure channel and allowing those machines to decrypt the secret key via symmetric or asymmetric keys. Diffie Hellman group DH group1, DH group 14 are KEX algorithms.

1.3.3. Message authentication algorithm

Message authentication key is used to check the data integrity. MAC algorithm determines if data received on the other side were manipulated or not. SHA1, SHA2 are MAC algorithms.

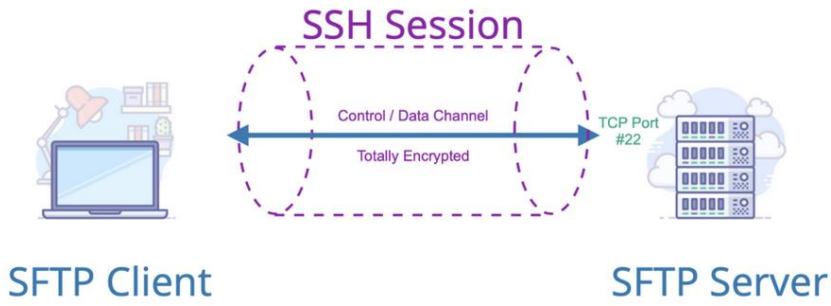

Fig.2. SFTP transfer flow [6].

1.4. FTPS

FTP + SSL or FTPS is an enhanced feature of FTP that is more secure than FTP itself. FTP transfers data in a plain text format and hence poses a security risk when it comes to transfer of sensitive data. To prevent sensitive data from man in the middle, FTP was enhanced with SSL/TLS protocol to encrypt data. TLS protocol uses digital certificates authorized by Certificate Authority (CA) as an identification mechanism. FTP alone is rarely used today and has been replaced by FTPS.

1.5. HTTPS

HTTP+SSL or HTTPS is an enhanced feature of HTTP. HTTP being a non-secure protocol, HTTPS was developed. Like FTPS, HTTPS also secures data by using SSL/TLS protocol. HTTPS uses digital certificate to identify a client and a server. Data between client and server are encrypted via secure channel that guarantees data integrity during entire session.

1.6. SSL/TLS

Secure socket layer also called as Transport Layer Security is a security protocol used by protocols like FTP and HTTP on the top of their own protocol to secure data, that are transferred over the internet. SSL/TLS protocol uses cipher suites and digital certificates (verified by Certificate authority or self-sign certificates). When a client initiates a session with server it provides a list of cipher suites supported by itself. Server checks the list of provided ciphers and checks in its system if it supports those cipher suites and if yes then it agrees with client to use certain cipher suites. Along with cipher suites, server presents its digital certificate to client to validate itself at client's side. Client checks if the public part of digital certificate from server is in its database. If it finds, session is established else session is aborted. Initial communication between client and servers are performed using asymmetric ciphers and once both hosts agree then communication begins with symmetric ciphers.

- Symmetric encryption - symmetric encryption uses the same key to encrypt and decrypt data between source and destination. HTTPS browsers use symmetric keys to encrypt/decrypt data between client's browser and web server. DES, DES3 and AES are symmetric encryption methods.
- Asymmetric encryption - asymmetric encryption uses different key to encrypt and decrypt data. SFTP uses asymmetric keys to encrypt and decrypt data between client and server. RSA and ECC are asymmetric encryption methods.

2 Managed File Transfer

Managed File Transfer or MFT is a software or application that not only consists of and support all traditional protocols but also many other features that traditional protocols were lacking. An organization may have multiple partners that use different set of protocols to transfer files or data. If the organization would use only one protocol it would have difficulties to compete in modern world as today users and organization have flexibility to choose the best and suitable protocols for them and they do not have to limit to one protocol only.

Managed files application developed by different organization support different protocols and different tasks but most common MFT used by financial sectors are Axway Gateway from Axway corporation and Sterling File Gateway from IBM corporation. These applications are not limited to transfer files only and they perform various other tasks that help an organization to compete with partners. Managed file system provides a centralized system to manage files, create report, monitor an events or transfer.

Every organization following ITIL process wants to have a track of number of incidents, problems and changes. Managed file transmission provides a real time analysis of number of incidents that occurred in a certain interval of time. This helps an organization to identify possible cause of those incidents.

Similarly, MFT also provides statistical reports to higher management as per their requirement. Managed file transmission monitors critical files that has Service Level Agreement (SLA) and alerts an admin via email or SMS, if the SLA has been breached. This prevents an organization from paying huge penalty.

Fig.3. MFT centralized system [6].

1.7. SSL/TLS

An admin is a person that is responsible to manage managed file transmission application. This role has a right to add partners, remove partners, configure application, configure monitoring and various tasks that can be setup in MFT application.

1.8. Secure File Transfer

Secure File Transfer is a system that consists of various traditional protocols that are supported by Managed File Transfer system. As an standard, MFT supports FTP, FTPS, HTTP, HTTPS, SFTP and various other protocols. MFT from IBM corporation also support NDM/CD protocol that are useful to transfer data between distributed operation systems like Windows and Linux to mainframe computers and vice-versa.

1.9. Analytics and Reports

Analytics and reports are very crucial to a company to track its system and flow. These reports help an organisation to keep track of incidents, problems, SLA breaches and overall availability of the system. This report serve management to plan revenue and onboard new partners.

1.10. Schedule Task and Automation

Schedule task are tasks that are setup by admin and are configured to run at a particular time. Schedule task can be referred to a SLA check for a file that is supposed to be delivered or received at a certain time interval. Schedule tasks also can be configured for generation of reports to higher management based on requirement. Automation is a task that is configured to execute automatically. If a file has to be received from client A at a certain time and deliver the file to client B, then automation task performs these tasks without manual intervention.

1.11. Database Management System

Unlike traditional protocols, MFT transfers are recorded in Database. Each entry is logged into database. Since each activity is audited, it is very easy to monitor and audit the system.

Any manipulation in system can be easily tracked. Files are stored in DB or data storage servers like Network File Share/Samba Share. Based on archiving policy of an organization, stored file can be easily retrieved at any point of time as per requirement.

Conclusion

Safety of data play an important role for an organization to have trust among clients. It is very crucial for such organization to have a modern and safe system to handle sensitive data of its clients. Traditional protocols do perform the task to transfer files but do not provide safety that is required by NIST or PCI DSS and hence Managed File Transfers systems are the best choice. There are many vendors and many types of MFT systems. An organization can choose an appropriate MFT system based on budget and requirements.

References

[1] CHAFFEE, I. (2018). USCNews, *Internet use at home soars to more than 17 hours per week* [online]. 20. Jan. 2018 [cit. 05. May 2021]. Available on: <https://news.usc.edu/134580/internet-use-at-home-soars-to-more-than-17-hours-per-week>

[2] BHUSHAN, A. (1971). Network Working Group, A File Transfer Protocol, RFC 114[online]. 16 Apr. 1971 [cit. 05. May 2021]. Available on: <http://www.faqs.org/rfcs/rfc114.html>

[3] DIGITALHACKING, All About FTP, [online]. 28 Dec. 2013 [cit.24-04-2021]. Available on: <http://digitalhacking.blogspot.com/2013/12/all-about-ftp.html>

[4] BERNERS-LEE, T. (1999). Network Working Group, Hypertext Transfer Protocol -- HTTP/1.1, RFC 2616 [online]. June 1999. Available on: <http://www.faqs.org/rfcs/rfc2616.html>

[5] BARRETT, DANIEL J., SILVERMAN, RICHARD E. May 2005, SSH, The Secure Shell: The Definitive Guide. USA: O'Reilly Media, 2005. ISBN 0-596-00895-3

[6] CONKLIN, K. (2018), IPSWITCH, Managed File Transfer - What Is it? [online]. 21 May 2018 [cit. 05 May 2021]. Available on: <https://blog.ipswitch.com/just-what-is-managed-file-transfer>

Authors

Shiva Prasad Paudel
Faculty of Informatics
Pan-European University, Tomášikova 20, 821 02 Bratislava
paudel1989221@gmail.com
Student of Pan-European University with focus in Applied Informatics

Prof. RNDr. Frank Schindler, Ph.D.
Faculty of Informatics
Pan-European University, Tomášikova 20, 821 02 Bratislava
frank.schindler@paneurouni.com
Professor and Head of Institute of Applied Informatics