

Managed File Transfer

Insights & Best Practices

Dave Butcher, PMP CSDP

May 1, 2008



Tumbleweed Snapshot

File Transfer Overview

- Evolution
- Challenges & Drivers

What is Managed File Transfer?

Best Practices

Q&A

Tumbleweed Communications



Company

- Founded in 1993, HQ in Redwood City, CA
- Focused purely on secure content delivery
- Global leader in managed file transfer & email encryption
- Over 3,200 customers
- Strengths in ease of use & flexible integration
- Offices in the US, Europe, Asia

Gartner

Best Email Encryption Solution



Products

Secure Transport™



Secures all data exchanges between organizations with secure managed file transfer

Secure Messenger™



Encrypt email at the gateway or desktop, automatically or manually

MailGate™



Protects email with comprehensive inbound and outbound security

Customers

Multi-Nationals



Fortune 500



Government



Financial Services



File Transfer – The Evolution



Early Connectivity

- Dial-up connections – Async, Bisync
- Dedicated links – FrameRelay
- Value Added Networks - VANs

Enter the Internet

- FTP becomes the de facto standard for file transfer
- Available on every platform, easy to code into scripts
- The tool of choice for application-to-application connectivity

Evolving Solutions

- Variety of enhanced secure file transfer products
- Open standards / open protocols
 - ✓ FTP, HTTP, SSL/TLS, SSH, PGP, S/MIME, EDIINT AS2 and AS3.
- Managed File Transfer Solutions

FTP – The De Facto Standard



File Transfer Protocol - Wikipedia, the free encyclopedia - Microsoft Internet Explorer

Address: <http://en.wikipedia.org/wiki/Ftp>

Sign in / create account

Your continued donations keep Wikipedia running!

File Transfer Protocol

From Wikipedia, the free encyclopedia
(Redirected from Ftp)

This article is about the File Transfer Protocol standardised by the IETF. For other file transfer protocols, see [File transfer protocol \(disambiguation\)](#). "FTP" redirects here. For other uses, see [FTP \(disambiguation\)](#).

FTP or File Transfer Protocol is used to transfer data from one computer to another over the Internet, or through a network.

Specifically, FTP is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol (such as the Internet or an intranet). There are two computers involved in an FTP transfer: a server and a client. The FTP server, running FTP server software, listens on the network for connection requests from other computers. The client computer, once connected, the client can do a number of things: download files from the server, rename files, and create new files. A programmer is able to create FTP programs for every computer platform supports FTP. FTP can be used over any network to manipulate files on and off the network (if the computers permit FTP). FTP servers can be setup anywhere be...

The five-layer TCP/IP model

5. Application layer

DHCP • DNS • FTP • Gopher • HTTP • IMAP4 • IRC • NNTP • XMPP • MIME • POP3 • SIP • SMTP • SNMP • SSH • TELNET • RPC •

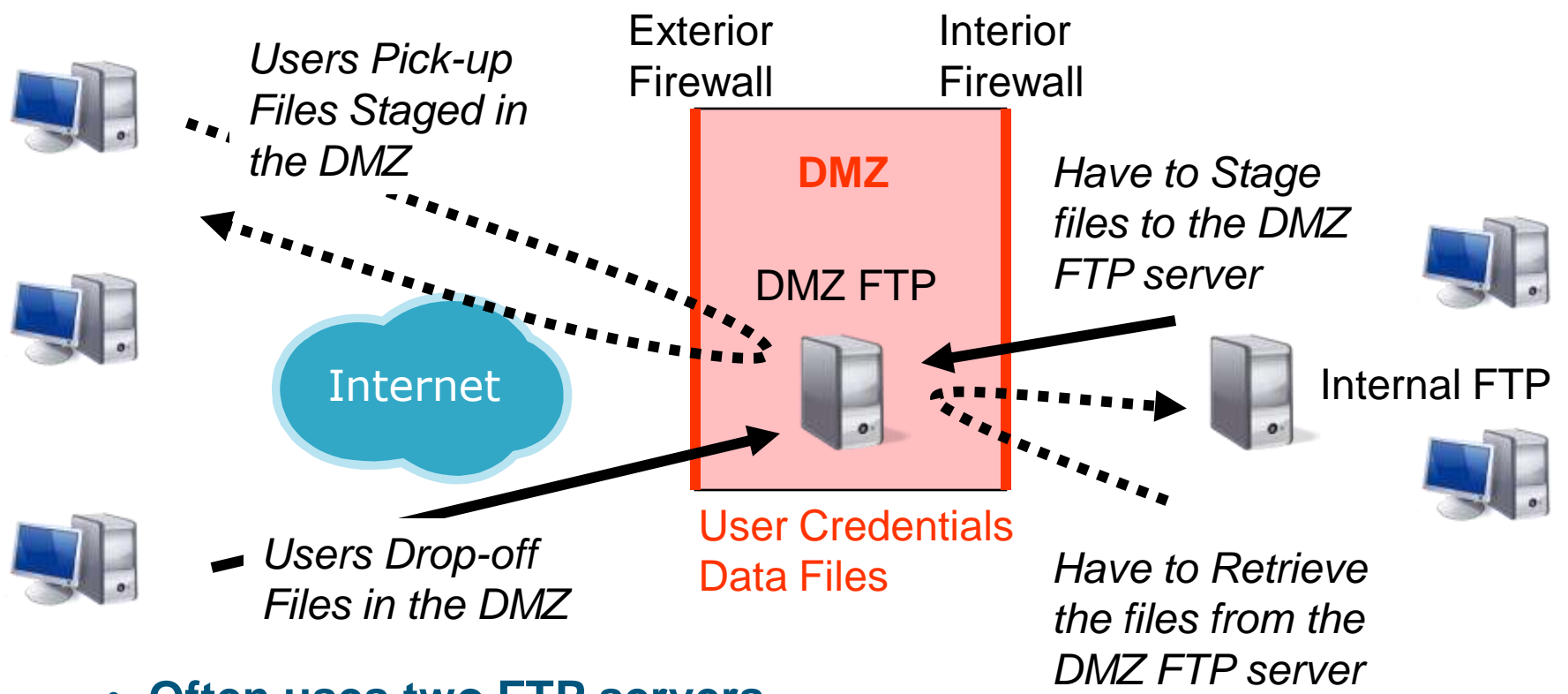
- Most Common Internet File Transfer Method
- Client / Server Architecture
 - ✓ Client initiates all connections
- Many Variations Of FTP, (Vendor Customizations)
- FTP Problems
 - ✓ No Encryption
 - ✓ User Names and Passwords Are In The Clear
 - ✓ No Integrity Checking
 - ✓ No Checkpoint Restart
 - ✓ No Tracking
 - ✓ No Management
 - ✓ FTP Scripting

Contents [hide]

- 1 Overview
- 2 Criticisms of FTP
- 3 Security problems
- 4 FTP return codes
- 5 Anonamous FTP
- 6 Data format
- 7 FTP and web browsers
- 8 FTP and NAT devices
- 9 FTP over SSH
- 10 References
- 11 See also

Homegrown FTP

The DMZ Issue



- Often uses two FTP servers
- User credentials and files stored in the DMZ
- Files maybe left unprotected for long periods of time
- Scripted jobs move the files between FTP servers
- Coordination nightmare

File Transfer – Other Tools



FTP/S

- FTP over SSL/TLS

SSH – Secure Shell

- SFTP – SSH File Transfer Protocol or Secure FTP
- SCP Is Command Line Only
- Leverages SSH Protocol
- Encryption and Authentication

AS2

- AS2 - Applicability Statement 2
- HTTP Based, Can Use SSL
- Encryption, Data Integrity, Signatures, Receipts
- Server initiates all connections
- Associated With EDIINT – Can Send Any Data

File Transfer Business Challenges



Data Volume & File Sizes Are Increasing

Paper-based Processes Are Inadequate

Regulatory Mandates Are Increasing

Markets Are Moving Faster

Management of Disparate Systems is challenging

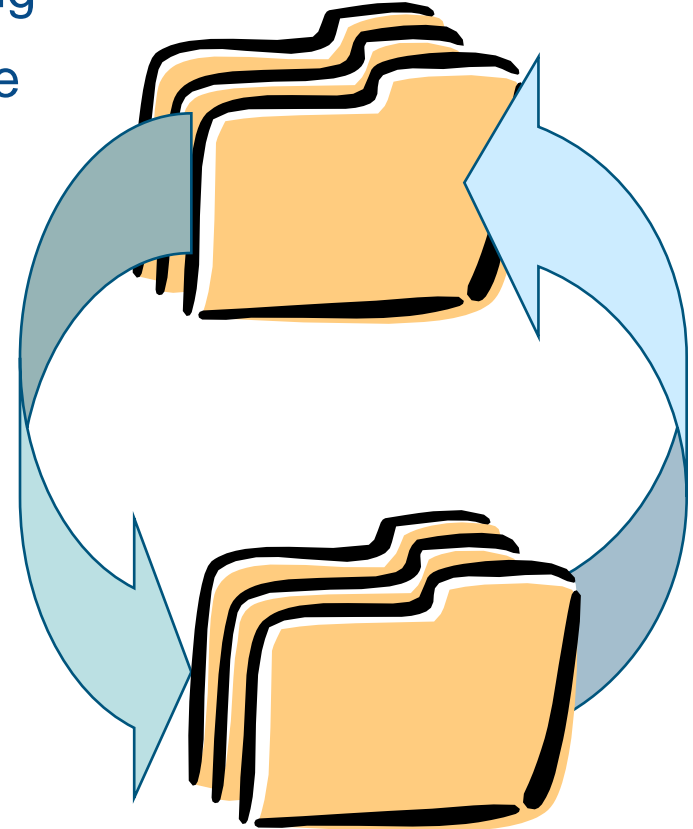
- Rogue FTP Servers

Desire To Reduce Costs

- Streamline operations
- Fewer systems to manage
- Internet Perceived As “Free”

Expand Business Community

- Access To Many Trading Partners
- Trade Worldwide
- Accommodate Partner Technology

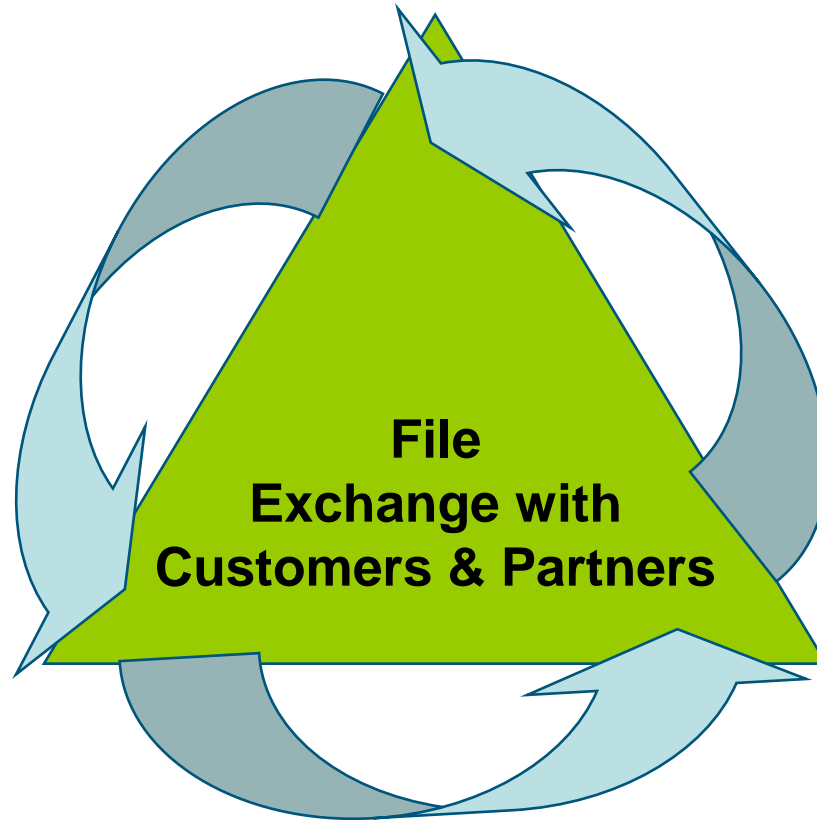


File Transfer Drivers



**Data Protection
and Security**

**Regulations and
Compliance**



**Outgrown/Limited
Existing Systems**

File Transfer Drivers

Data Protection & Security



Disney subcontractor caught selling customer data

Stolen credit card numbers and other account information sold
July 2007, Computer World

T.J. Maxx hack exposes consumer data

computers hacked, putting shoppers at risk of identity fraud
January 2007 — CNET news

Western Union reveals customer data theft

Thousands of customers' personal information was stolen by hackers.
July, 2007 Earth Times

Data Theft Affected Most in Military

Stolen information included data on 2.2 million active troops
June, 2006 — Washington Post

Merrill Lynch ID Theft May Affect 33,000 Employees

August, 2007 — CNBC

Credit agency suffers 'misappropriation' of 2.3 million consumer records

July, 2007 CNET News

Payroll hole exposes dozens of companies

February, 2005 — CNET News.com

Johns Hopkins Loses Data On 135,000 Patients. Employees

47 percent of financial firms reported their network or data is targeted by organized criminals.

SC Magazine Jan 2008

File Transfer Drivers

Regulations & Compliance



GLBA



HIPAA

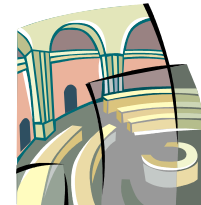


**SEC 17a-4 &
NASD 3010**



SOX

External regulations
driving some need for file
transfer, *but...*



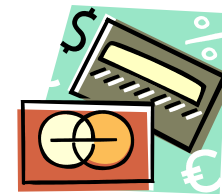
CA SB 1386



**FDA 21 CFR
Part 11**



USA Patriot Act



**Payment Card
Industry (PCI) Data
Security Standard**

File Transfer Drivers

Outgrown Existing/Limited Systems



Existing file transfer infrastructure constructed of too many “fragile” components

- Complex with little visibility
- Too many moving parts

Expensive, proprietary legacy systems

Inadequate security and confidentiality

Rampant “rogue” (unmanaged) FTP

- Risk management issues
- Need to support auditing, SOX compliance

Inflexible – inability to address future needs

- Speed of business continually increasing
- Larger files, more frequently, to more partners in shorter timeframes

Variable Scalability, Reliability, Performance



Internal Constituents & Partners

Driving Need for MFT



Internal

Increasing scrutiny from Chief Security Officer (CSO)

- Facilitates need to prove data exchange activity/ security with reporting, logging and auditing

Physical medium file transfers are gone

Corporate reputation – remember TJX

Enforcement of corporate policies

Each business unit deploying point solutions

Efficiency – savings achieved through automation & consolidation

Partners

Partners and customers require electronic transfers

SLA enforcement

- Did our partner/vendor deliver the data on schedule?
- 67% of CIOs surveyed reported more than 20% of their file transfers are tied to SLAs – SC Magazine (Jan. 2008)

Managed File Transfer (MFT)

According to Gartner



The Gartner “Managed File Transfer Suites: Technology Overview” report identifies a managed file transfer suite as having the following functionality:

- **Secure Communications:** This entails a collection of commonly used protocols and technologies used for transporting and ensuring the authentication, privacy, non-repudiation and authorization of data between two or more entities.
- **Management:** This is the ability to monitor and control the data (regardless of size) throughout the file transfer.
- **Integration functionality:** Adapters or exposed application programming interfaces.
- **Streaming input /output:** This capability enables the MFT Suites to overcome physical hardware limitations and operating environment limitations.
- **Checkpoint/restart capabilities:** This capability lets the user resume incomplete file transfers as a result of interrupted transmissions, accidental or otherwise.

Best Practices

Understanding the File Transfer Needs



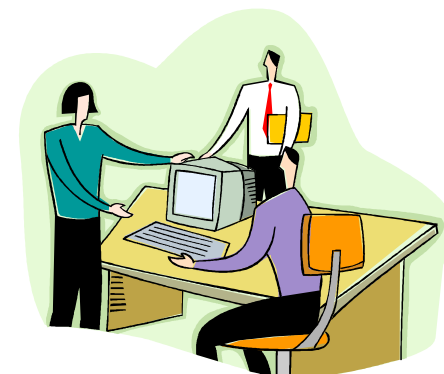
Know your stakeholders and their file transfer roles

- Information Technology
 - ✓ Owners of IT policy
 - ✓ Caretakers of IT systems
- Corporate Security
 - ✓ Charged with protecting data, knowing what is leaving the enterprise and if it is authorized and secure
- Business Units
 - ✓ Owners of the data being transferred
- Partners

Understand your stakeholders file transfer needs and requirements

Implement the security architecture to meet these needs/requirements

- Answer key questions
- Consider security architect best practices
- Investigate MFT solutions



Best Practices

File Transfer Needs – Key Questions



What are you currently using for File Transfer?

Does your file transfer environment have many components that have evolved over time?

Are you planning to leverage the Internet for your file transfers?

What protocols do you currently use to communicate with your trading partners?

Do you feel pressure to comply with regulatory requirements for your file transfers?

Do you stage or store data in your DMZ? Is it stored in plain text?

Do you have HA requirements for your business critical file transfers?

Do you have trading partners with PGP encryption requirements?

Do you have very large files you need to transfer? Would a checkpoint restart capability be of interest?

Are delivery receipts with non-repudiation important to you?

Do you have file transfer integration requirements?

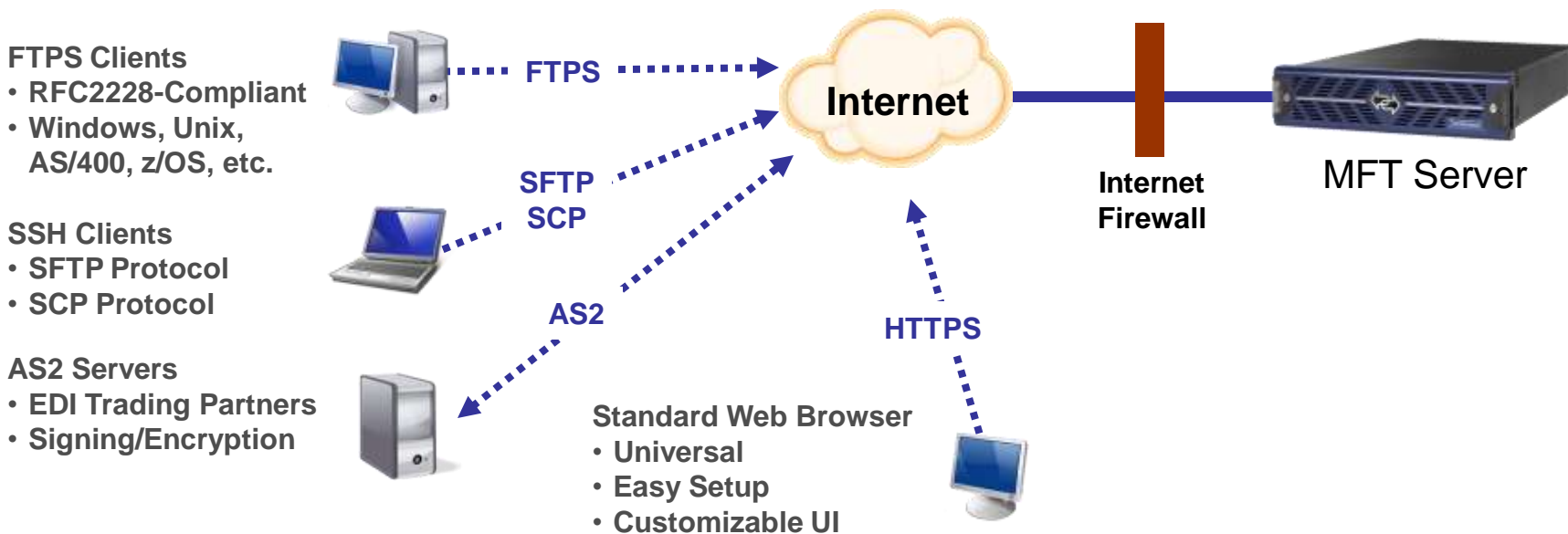
Best Practices

Flexible Protocol Support



Support multiple protocols – avoid client side changes

- HTTP/HTTPS – browser clients
- FTP/FTPS
- SFTP/SCP
- AS2
- Proprietary – Large files (checkpoint restart, integrity)



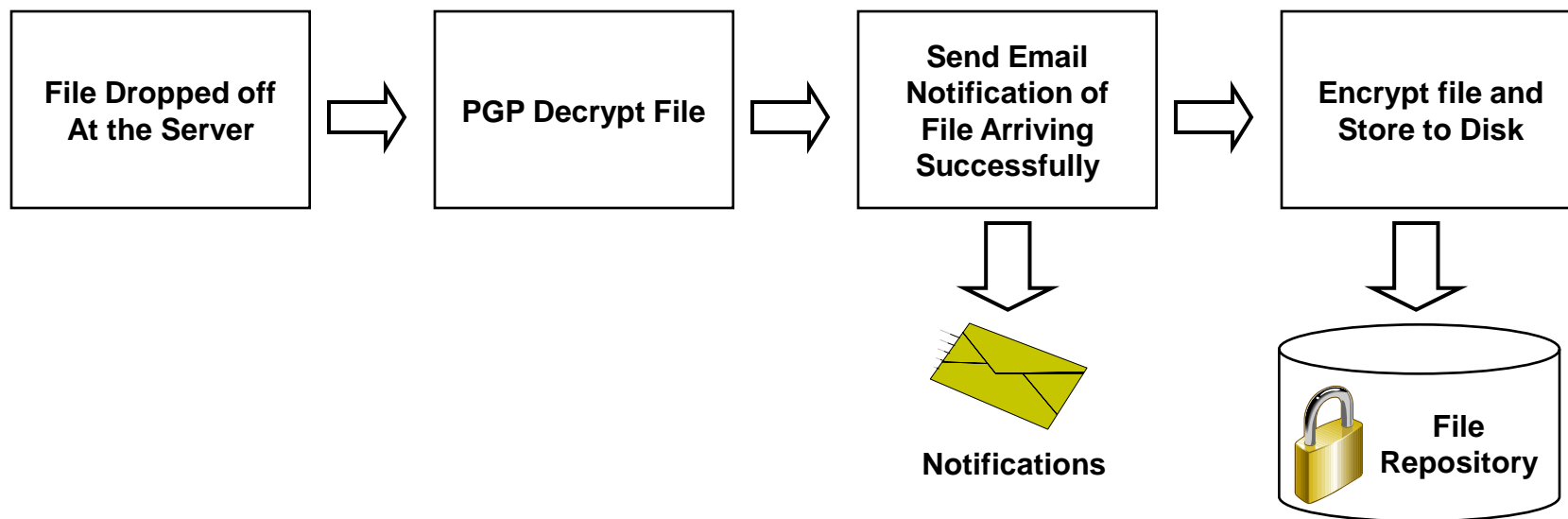
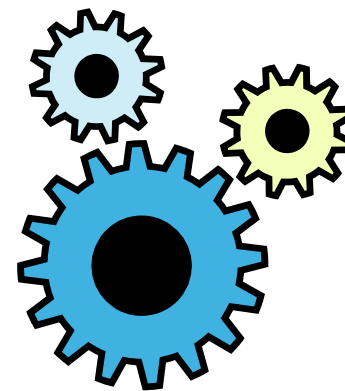
Best Practices

Automation Support



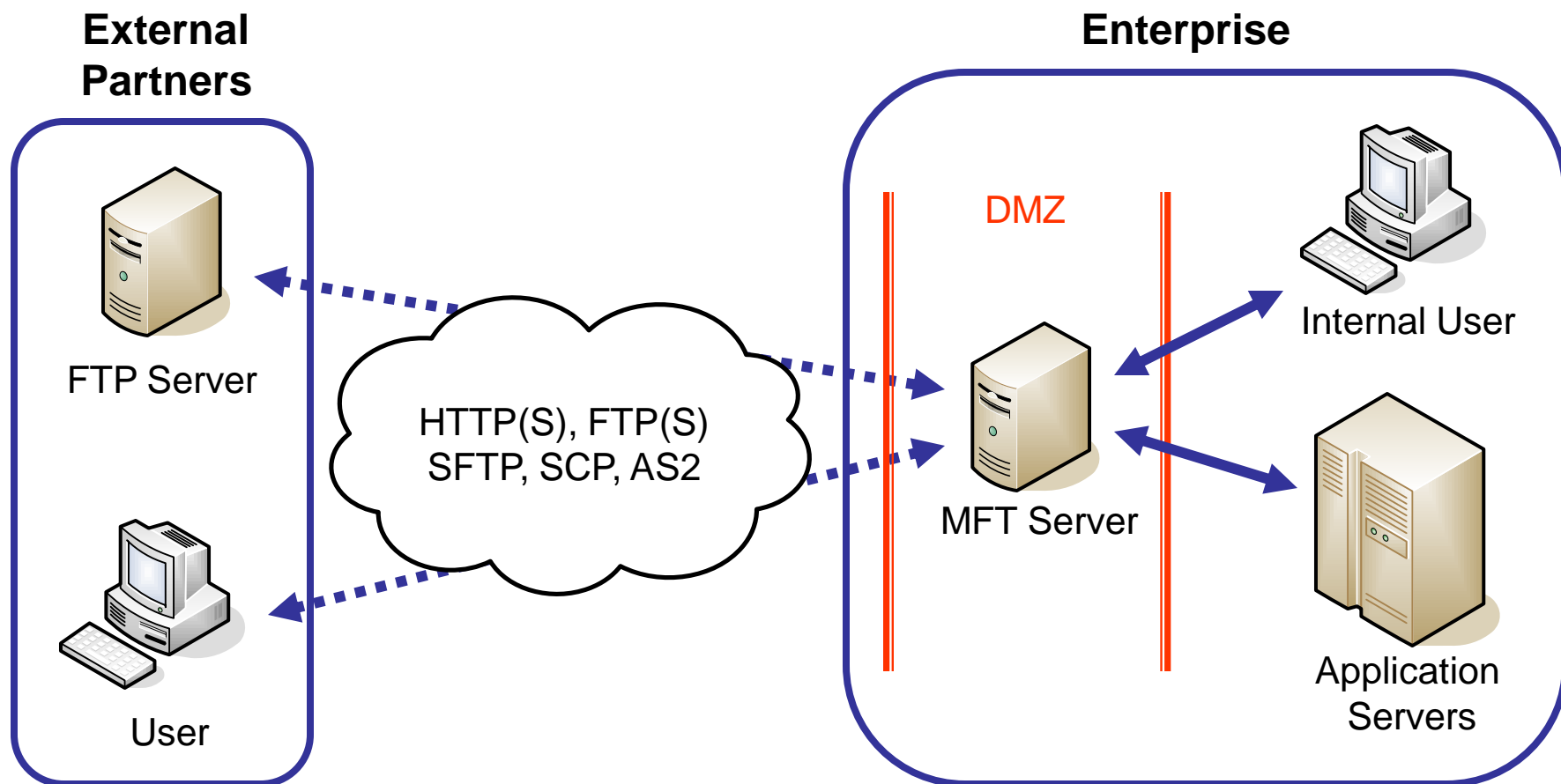
Back end automation – getting the data to the systems that are consuming it and from the systems that produce it

- File moves and copies
- File level encryption
 - ✓ PGP during transport
 - ✓ Encrypted file system during storage
- Email notifications on successful transfers and failures
- Framework for custom transforms – event drive



Best Practices

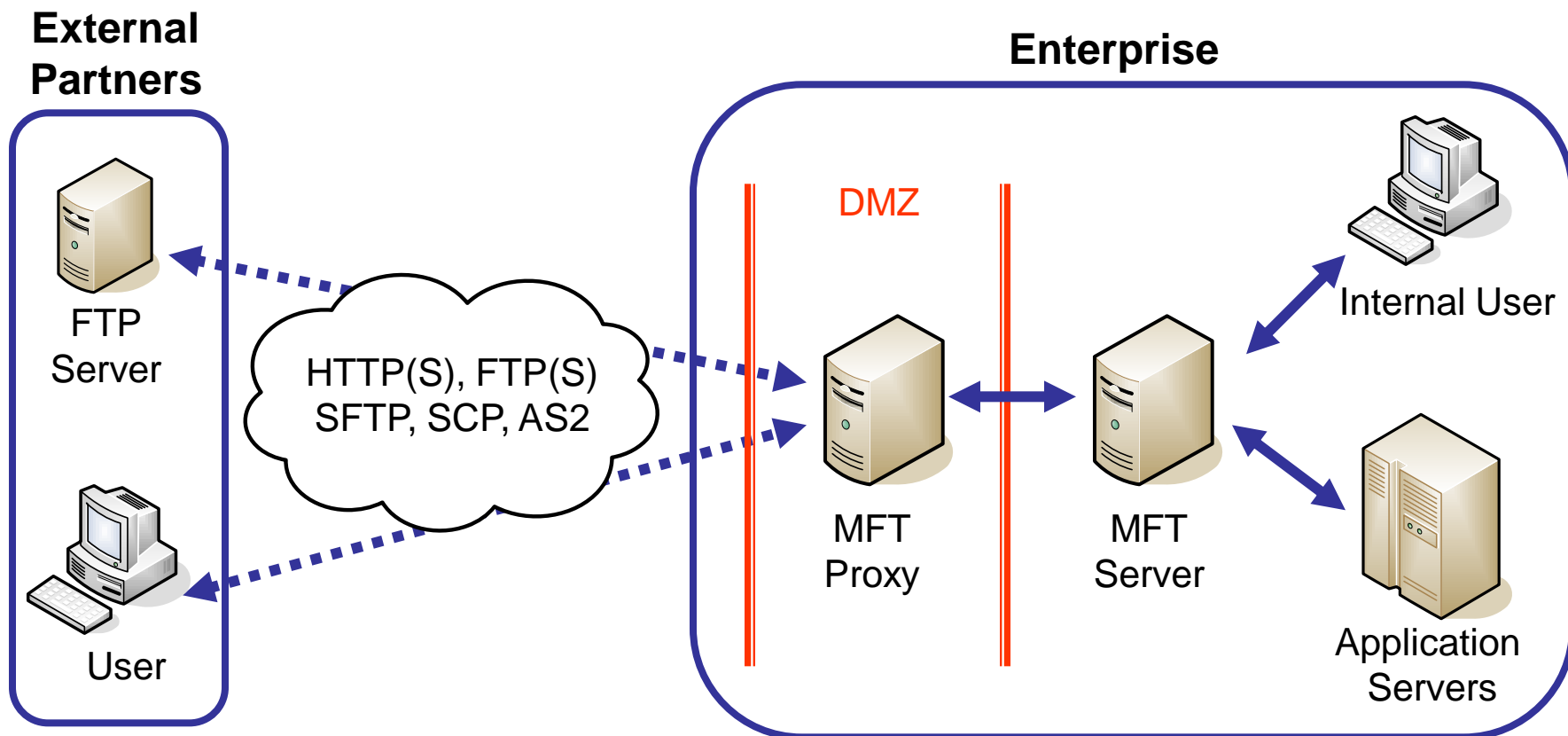
MFT Enterprise Gateway



- All file movement is centralized through the MFT server
- Firewalls are locked down to prevent circumventing the server

Best Practices

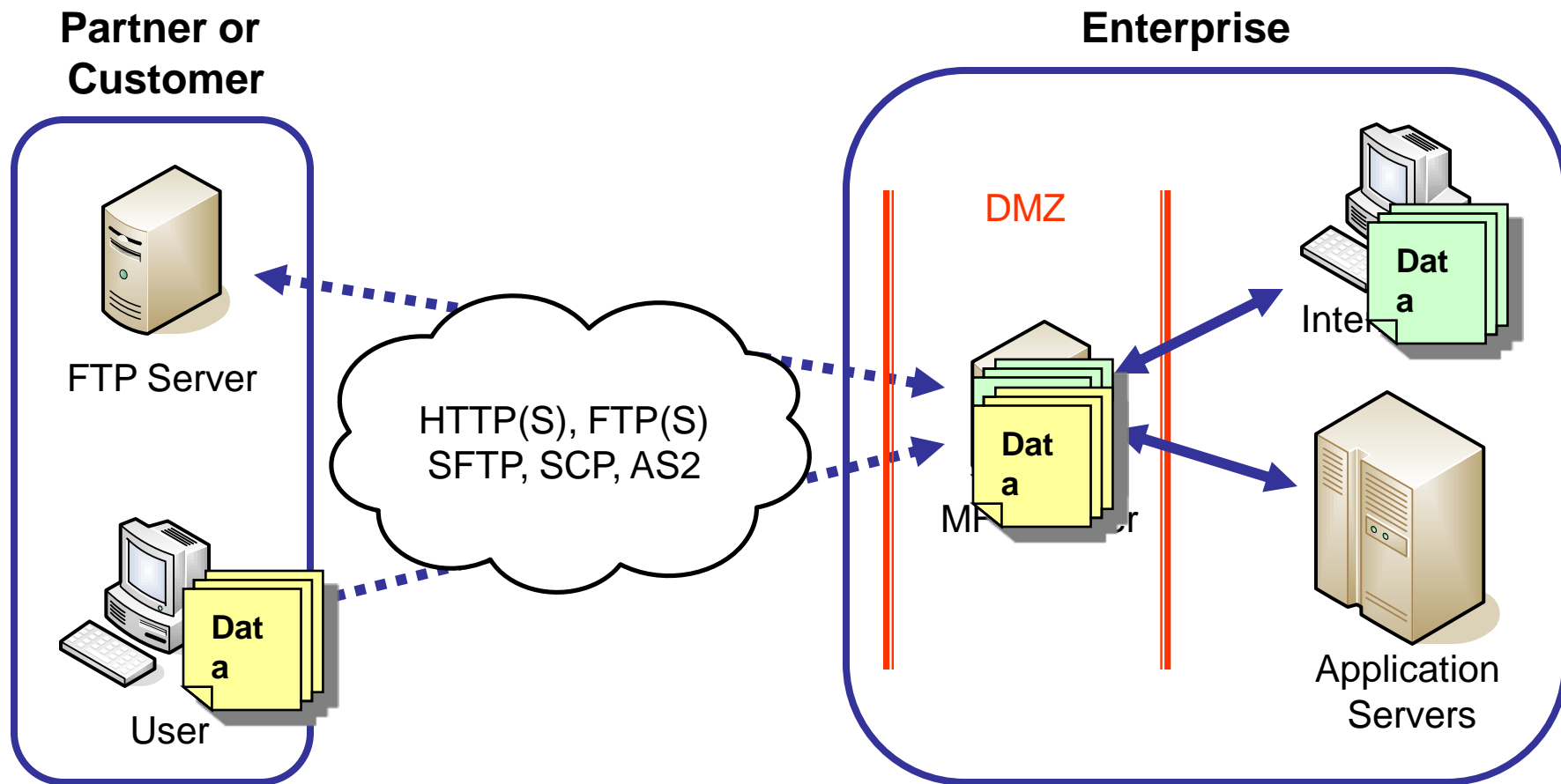
Two Tier Deployment



- Nothing stored in the DMZ
- No user data or credentials
- Eliminates data staging and retrieval issues

Best Practices

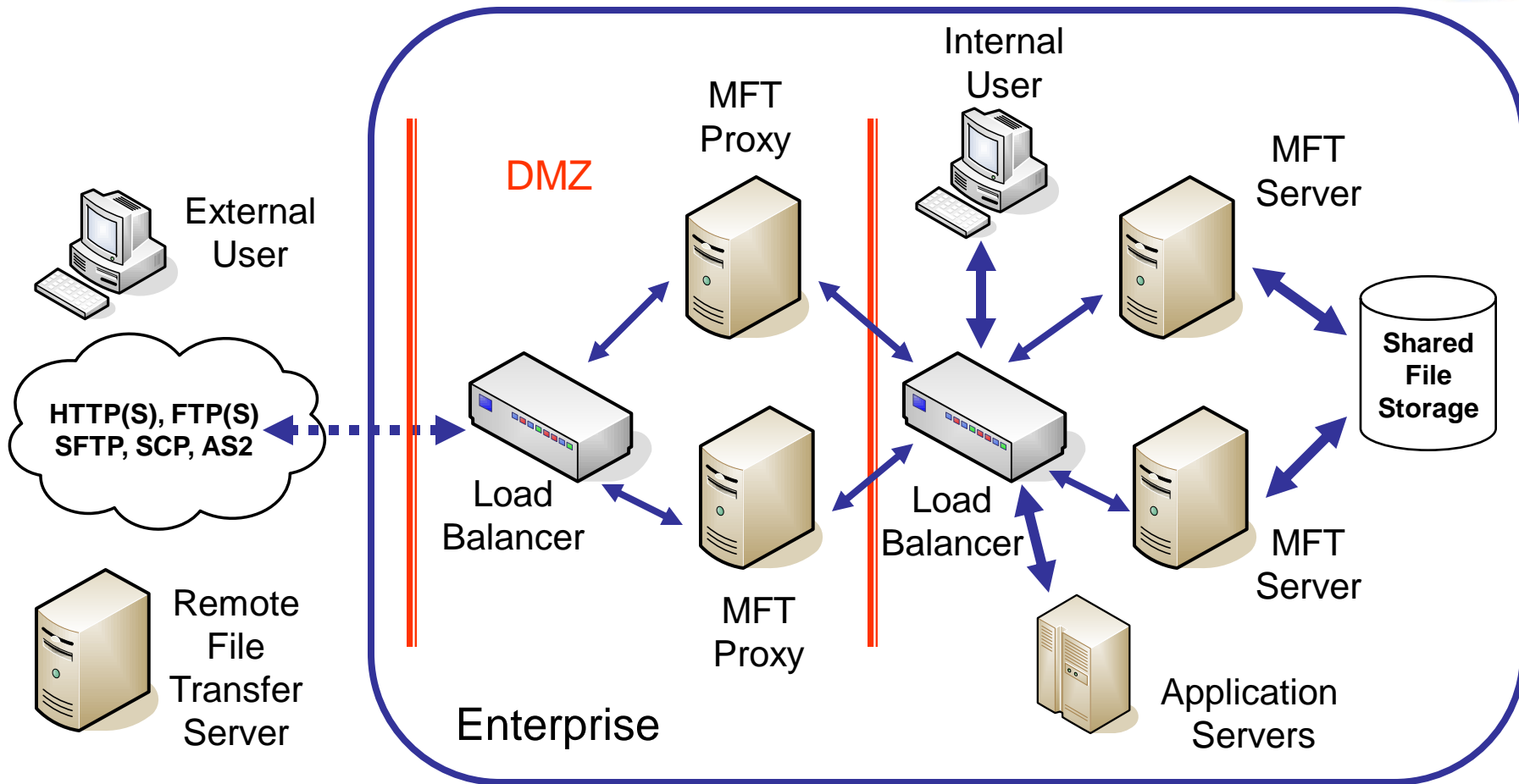
Centralized File Transfer



- All file movement is centralized through the MFT server
- Firewalls are locked down to prevent circumventing the server

Best Practices

High Availability



- Avoid Single Points of Failure
- Need for Scalability and Failover Support

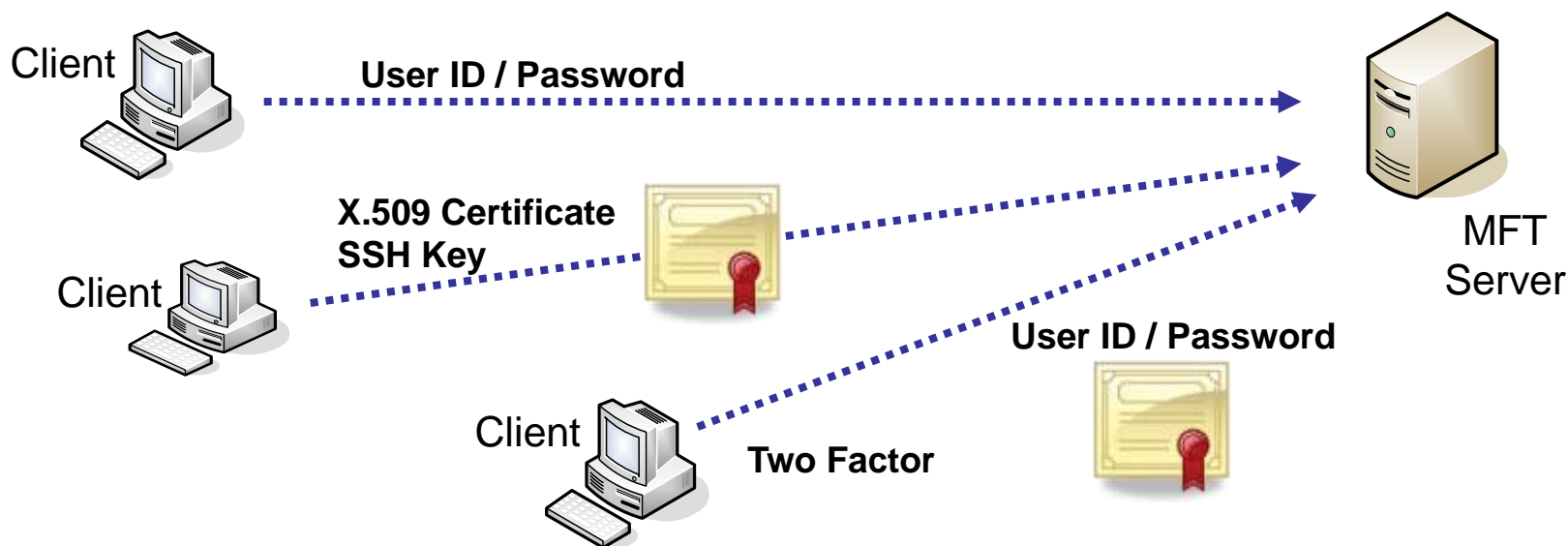
Best Practices

Multiple Authentication Methods



Authentication

- Single factor
 - ✓ Passwords
 - ✓ Certificates
- Multi factor
- Authentication database local to solution
- Integrating with existing authentication databases (LDAP/AD/SSO)



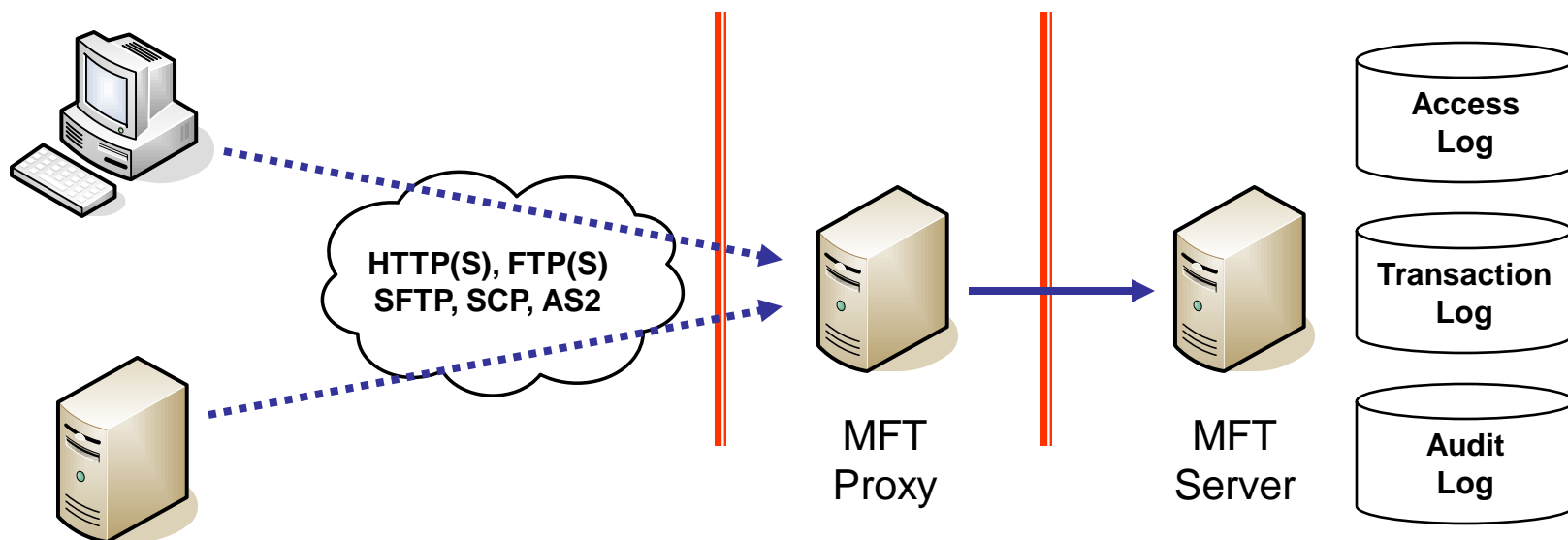
Best Practices

Record Keeping



Logging

- Granular
 - ✓ All file transfers recorded – who, what and when
 - ✓ All access recorded
- Integrity
 - ✓ Protected from outsiders – out of the DMZ
 - ✓ Protected from insiders – digitally signed



Best Practices

Investigate MFT Solutions



Ask your trading partners what solutions they are using with their other vendors

Seek third-party recommendations on MFT solutions

- Gartner
- SC Magazine
- Etc.

Go to the source

- Explore MFT vendor websites
- Review informative white papers, webinars, etc.
- Request a demo / eval
- Ask for references



Questions/Discussion



For More Information



www.tumbleweed.com

info@tumbleweed.com

877 282-7390