Secure IT/OT File Transfer

DMZ-based architectures for network file exchange between IT and OT

OT Security Learning Series

Document 841 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Network-based file transfer between IT and OT networks requires careful architectural design. A properly implemented DMZ-based file transfer system provides secure, auditable exchange while maintaining network segmentation and preventing direct connectivity between zones.

Common file transfer requirements include:

- Software patches and updates from IT to OT
- Production data export from OT to IT (historians, reports)
- Configuration files and documentation
- Vendor files received via email or download
- Backup data replication

This document covers secure network-based file transfer architectures and procedures for IT/OT environments.

2 Architecture Overview

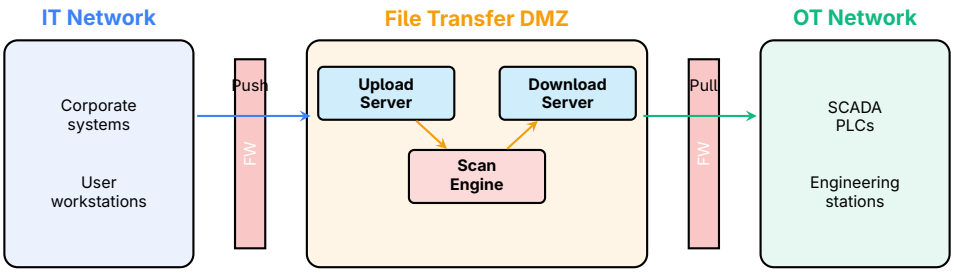

Figure 1: DMZ-Based File Transfer Architecture

2.1 Key Design Principles

Secure File Transfer Principles

- **No direct connectivity** – IT and OT never communicate directly
- **Defense in depth** – Multiple security layers (firewalls, scanning, access control)
- **Pull model for OT** – OT retrieves files; nothing pushed into OT
- **Scan everything** – Multi-engine AV and content inspection
- **Audit trail** – Complete logging of all transfers
- **Least privilege** – Minimal permissions at each stage

3 DMZ Components

3.1 Upload Server (IT-Facing)

Receives files from IT network:

- Web portal for manual uploads
- SFTP/SCP for automated transfers
- User authentication (AD integration optional)
- File size and type restrictions
- Quarantine storage pending scan

3.2 Scanning Engine

Processes all incoming files:

- Multiple AV engines (minimum 2-3 vendors)
- Content Disarm and Reconstruction (CDR)
- File type validation (magic numbers, structure)
- Signature updates via one-way channel
- Sandboxing for suspicious files (optional)

3.3 Download Server (OT-Facing)

Provides clean files to OT:

- Separate server from upload (defense in depth)
- Pull-only access from OT network
- File integrity verification (hashes)
- Automatic expiration of unclaimed files
- Notification system for available files

Protocol	Direction	Use Case	Security
SFTP	IT→DMZ	Automated uploads	Encrypted, key auth
HTTPS	IT→DMZ	Web portal uploads	TLS, cert validation
SCP	DMZ→OT	Pull from OT	Encrypted, key auth
SMB/CIFS	Internal	Windows shares	Requires Kerberos

Table 1: Recommended Transfer Protocols

4 Transfer Protocols

Warning

Avoid These Protocols:

- FTP (unencrypted credentials and data)
- Telnet (unencrypted)
- HTTP (unencrypted)
- NFS without Kerberos (weak authentication)

5 Firewall Rules

5.1 IT to DMZ Firewall

Source	Dest	Port	Purpose
IT Users	Upload Server	443/tcp	HTTPS portal
IT Systems	Upload Server	22/tcp	SFTP uploads

Table 2: IT→DMZ Firewall Rules

5.2 DMZ to OT Firewall

Source	Dest	Port	Purpose
OT Systems	Download Server	22/tcp	SFTP pull
OT Systems	Download Server	443/tcp	HTTPS download

Table 3: DMZ→OT Firewall Rules (OT Initiates)

Key Point

Key Point: OT systems initiate connections to the DMZ. The DMZ never initiates connections into OT. This prevents attackers who compromise the DMZ from directly accessing OT systems.

6 Content Disarm and Reconstruction

CDR Technology

CDR sanitizes files by deconstructing them, removing potentially malicious active content, and rebuilding clean versions. This neutralizes threats that bypass signature-based detection.

6.1 CDR Capabilities

- **Office documents** – Remove macros, embedded objects, OLE
- **PDFs** – Strip JavaScript, forms, embedded files
- **Images** – Flatten layers, remove metadata, steganography
- **Archives** – Extract, scan contents, repackage
- **Conversion** – Convert to safe formats (e.g., PDF/A)

6.2 File Type Policies

File Type	Action	Notes
.exe, .msi, .bat	Block or quarantine	Require approval workflow
.pdf, .docx	CDR processing	Strip active content
.csv, .xml, .txt	Allow after scan	Low risk
.zip, .7z	Extract and scan	Recursive scanning
.bin, .hex (firmware)	Manual review	High-risk, requires approval

Table 4: File Type Processing Policies

7 Workflow and Approval

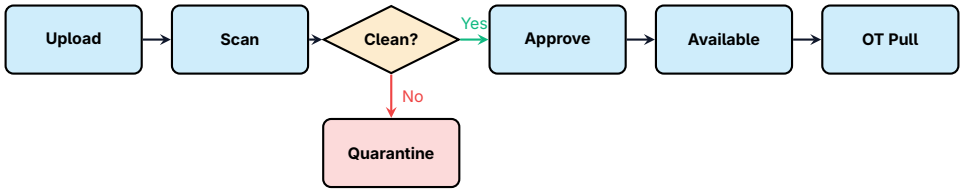

Figure 2: File Transfer Workflow

7.1 Standard Workflow

1. User uploads file via portal or SFTP
2. File quarantined, scan initiated
3. Multi-AV scan and CDR processing

4. Clean files queued for approval (if required)
5. Approver reviews and approves
6. File moved to download area
7. OT user notified, retrieves file
8. Unclaimed files expire after defined period

7.2 Approval Requirements

- **Automatic approval** – Low-risk file types (text, CSV, sanitized docs)
- **Single approval** – Standard files (patches, configs)
- **Dual approval** – High-risk files (executables, firmware)
- **Emergency bypass** – Documented exception with senior approval

8 Data Diode Integration

For high-security environments, data diodes provide hardware-enforced one-way transfer:

- **Inbound diode** – IT→OT for patches and updates
- **Outbound diode** – OT→IT for historian data, logs
- Eliminates any possibility of reverse channel
- Requires protocol proxies for TCP-based applications

Warning

Data diodes require careful protocol handling. TCP acknowledgments cannot traverse the diode, so proxy applications must handle protocol conversion.

9 Logging and Monitoring

All file transfers must be logged with:

- Timestamp and unique transfer ID
- Source user/system identity
- File metadata (name, size, hash before/after)
- Scan results from all engines
- Approval workflow (who, when)

- Destination (who retrieved, when)
- Any alerts or anomalies

Key Point

SIEM Integration: Forward file transfer logs to your security monitoring platform. Alert on failed scans, unusual file types, high volumes, or after-hours transfers.

10 Operational Procedures

10.1 Patch Tuesday Process

1. IT downloads patches from vendor
2. Upload to file transfer system
3. Scan and CDR processing
4. OT team reviews and approves
5. Files staged for maintenance window
6. OT retrieves and tests in lab
7. Deploy to production during outage

10.2 Emergency File Transfer

- Pre-approved emergency contacts authorized to bypass
- Documented justification required
- Post-incident review mandatory
- Scan still performed (blocking only bypassed)

11 Summary

Key Takeaways

- **Use a DMZ** – Never allow direct IT/OT file transfer
- **Pull model** – OT retrieves files; nothing pushed to OT
- **Scan everything** – Multiple AV engines plus CDR
- **Strict firewall rules** – Minimal ports, OT initiates only
- **Approval workflows** – Human review for sensitive files
- **Complete audit trail** – Log all transfers for forensics
- **Consider data diodes** – Hardware-enforced for high security

12 Further Reading

Standards and Guidelines

- **IEC 62443-3-3** – System security requirements for IACS
  https://webstore.iec.ch/publication/7033
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA – Securing Industrial Control Systems**
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS – Network Security Monitoring**
  https://www.sans.org/cybersecurity-focus-areas/industrial-control-systems-security

Books

- Knapp, E. & Langill, J. – *Industrial Network Security* (Syngress)
- Macaulay, T. & Singer, B. – *Cybersecurity for Industrial Control Systems* (CRC Press)

Part of the OT Security Learning Series