Link-s Enterprise-Grade Point-to-Point File Encrypted Transmission and Precise Sharing Solution

Facilitate Secure and Efficient Data Circulation, Reconstruct the Security Boundary of Enterprise File Transmission

Link-S is a brand-new enterprise-grade file sharing and transmission solution dedicated to addressing three core challenges in cross-regional large-file transmission: transmission efficiency, data security, and industry compliance. Supporting full private deployment, it boasts such core strengths as stability and reliability, high-speed transmission, full-process encryption, and precise sharing control, providing secure and controllable file transmission and sharing services for customers across government, finance, military industry, manufacturing, and other sectors. The personal version is available for free.

I. Cross-Regional Large-File Transmission: Dual Industry Pain Points of Efficiency and Security

For the transmission and cross-departmental sharing of files such as dozens of GB or even hundreds of GB of database backups, code repositories, design source files, confidential business data, and system logs, traditional solutions have exposed obvious shortcomings:

• Unstable transmission and poor sharing experience: Network fluctuations are prone to cause transmission interruptions, repeated transmissions greatly reduce efficiency, and team sharing permissions cannot be finely controlled.

• Weak encryption system and prominent security risks: Traditional cryptography such as RSA/ECC is still used, which is difficult to resist the risk of cracking by future quantum computing; no perfect forward secrecy, once the key is leaked, all historical transmission data can be decrypted; lack of session-level isolation protection; some solutions even transmit in plaintext, and there are hidden dangers of interception, tampering, and leakage when files are transferred through third parties.

• Difficulty in meeting compliance requirements: Requirements include data not leaving the domain, refined permissions, auditable sharing behaviors, and secure and reliable national cryptographic algorithms (SM4), etc.

Link-s enterprise-level solution is a security solution tailored to the above dual pain

points of "transmission + sharing".

II. Core Technical Highlights: Point-to-Point Encryption + Resumable Transmission + Private Deployment

1. Point-to-Point Encrypted Transmission, No Data Landing

Link-s adopts a point-to-point invitation mechanism to establish a temporary encrypted tunnel. Files are directly transmitted from the sender to the receiver without passing through any third-party intermediate servers. The transmission adopts a hybrid encryption system of Kyber-768 post-quantum encryption + AES-256/SM4-CTR. Keys are only generated and stored at the sending and receiving ends, and the server cannot obtain the keys or decrypt the file content. Whether it is transmission or sharing with designated members, end-to-end security is guaranteed.

2. Resumable Transmission + Automatic Reconnection to Cope with Complex Networks

Built-in resumable transmission and automatic reconnection mechanisms after network disconnection. After transmission interruption, it can continue transmission from the interrupted position without starting from scratch, significantly improving the success rate and efficiency of large-file transmission.

3. Full-Stack Private Deployment to Safeguard Data Sovereignty

For institutions with strict requirements on data sovereignty, it provides complete private deployment capabilities: signaling services, relay services, and audit platforms can all be deployed in the enterprise intranet to realize data not leaving the domain, easily meeting level protection, classified protection and industry compliance requirements.

4. Precise Sharing: Fine-Grained Control Based on Files and Contacts

Abandoning the inefficient sharing mode of traditional "public links" or "visible to all", Link-s provides dual sharing control capabilities at the contact level and file level:

Authorization by contact: When sharing files or folders, you can accurately check the visible contacts, and unauthorized users cannot see the content in "Discovered Files".

III. Hierarchical Technical Architecture, Stable,

Reliable and Easy to Maintain

Link-s adopts a standardized hierarchical architecture, with five core components performing their respective duties, balancing performance, security and manageability:

Hierarchy	Core Components	Core Responsibilities
Access Layer	Multi-Platform Client	Supports Windows/Mac/Linux and domestic operating systems, green and non-installable
Control Layer	Signaling Service Cluster	Connection negotiation, user identity authentication, transmission session management
Forwarding Layer	Relay Service Cluster	Cross-network data forwarding, supporting horizontal expansion
Security Layer	IP Management Module	Illegal device interception, access control
Management Layer	Audit Web Background	Global log audit, account permissions, full-process control of file circulation

IV. Highly Scalable Architecture: Cluster Deployment, No Single Point of Failure

1. Decentralized Signaling Cluster

The signaling service adopts a decentralized distributed cluster architecture, and any node can access the global service; session status and user information are automatically synchronized between nodes to eliminate single points of failure; single node failure switches automatically to ensure uninterrupted service, and the cluster can be horizontally expanded infinitely.

2. Relay Service Cluster

Relay services support cluster deployment with no upper limit on the number of nodes, which can be elastically expanded with business volume; during cross-network transmission, the optimal relay node is automatically and intelligently allocated to ensure transmission availability and stability.

3. Global Audit, Highly Controllable Management

The audit platform realizes full-dimensional control: account management, forced logout, file sharing and download permission control, blacklist and whitelist management, etc., to meet the refined operation and maintenance needs of enterprises.

V. Powerful Transmission Capabilities, Balancing Speed and Security

• P2P Direct Connection: Establish point-to-point direct connections through LDC, WDC, and DHC with no speed limit. Files do not pass through the server.

• Resumable Transmission: Interruption resumption + network disconnection reconnection, greatly saving large-file transmission time

• Stream Encryption: Encrypt while transmitting, decrypt while receiving, no need to wait for the complete file transmission before processing

• Multi-Thread Parallelism: Large files are automatically split into blocks, and multi-thread concurrent transmission is used to make full use of network bandwidth

Four Intelligent Connection Methods, Adapting to All-Scenario Networks

• L-DC: LAN P2P Direct Connection

• W-DC: LAN and Public Network Direct Connection

• DH-DC (P2P Hole Punching): Public Network Penetration Direct Connection

• Relay: Cross-Network Relay Forwarding

Comprehensively covering various scenarios such as enterprise intranet collaboration, server-client transmission, and cross-regional remote collaboration.

VI. In-Depth Private Deployment to Meet High Compliance Requirements

Enterprises can independently deploy the entire set of service components in the intranet:

• Signaling Control Server: Connection negotiation, user authentication, session scheduling

• Relay Server: Cluster deployment to ensure stable cross-network transmission

• Audit Management Platform: Log traceability, user management, blacklist and whitelist policies

It truly realizes data not leaving the domain, controllable permissions, and auditable behaviors, perfectly adapting to institutions such as government, finance, military industry, and energy that have extremely high requirements for data security and compliance.

VII. Solution Summary

Link-s enterprise-level point-to-point file encrypted transmission system takes no speed limit, no file size limit, full-link encryption, and private deployment as its core advantages. It adopts AES-CTR+ML-KEM end-to-end encryption technology to ensure full-process encrypted transmission, keys only stored at the sending and receiving ends, and servers cannot decrypt. At the same time, it supports four connection modes: LAN direct connection, public network direct connection, P2P hole punching, and relay forwarding, achieving the optimal balance between security, stability, and speed. It is an ideal choice for enterprises to securely transmit large files across regions.