Kiteworks

Securing Data in Motion With SFTP

Unlocking Robust Security and Compliance for Your File Transfer Needs

What Is SFTP?

Secure File Transfer Protocol (SFTP) is a network protocol that provides secure file transfers over SSH (Secure Shell). It encrypts data in transit and allows secure authentication, protecting information as it is transferred over insecure networks.

SFTP is widely used as a secure alternative to File Transfer Protocol (FTP) to exchange sensitive data between organizations. It enables transfer of files between a client and server over an encrypted SSH session. All file operations like uploading, downloading, renaming, deleting files, etc. are performed securely over this encrypted channel.

Brief History of SFTP

The origins of SFTP can be traced back to the creation of the SSH protocol in 1995. SSH was developed as a secure replacement for insecure remote login protocols like Telnet and rlogin. It allowed secure remote access by encrypting data over an insecure network.

In 1997, SSH File Transfer support was added to the SSH protocol, allowing secure file transfers. This gave rise to the first version of SFTP.

Over the years, SFTP has undergone improvements by incorporating stronger encryption algorithms, improved error handling, caching for better transfer speeds, and more functionality like directory listings and file permissions. Today, SFTP is an Internet Engineering Task Force (IETF) standard, defined in RFC 913. It is the preferred method for securely transferring files over the internet.

How SFTP Works

The SFTP protocol works by establishing a secure SSH session between the client and server before initiating any file transfers. Steps involved include:

1. Client connects and authenticates to the SFTP server over SSH. This establishes an encrypted session.
2. Server and client negotiate encryption algorithms to use for the session.
3. Authentication happens over the encrypted channel. This is usually public key-based.
4. Once authenticated, all file transfer operations are performed over the encrypted channel.
5. After the file transfer is complete, the SSH session is terminated.

This ensures all data including file contents, file names, and commands are securely encrypted during the transfer. Integrity mechanisms like hash verifications are used to prevent tampering of transferred files.

Why Organizations Use SFTP: 6 Reasons

There are several key reasons why organizations use SFTP for file transfer:

1 Improved Security Over Regular FTP

SFTP offers better security compared to regular FTP. FTP has no encryption, meaning data can be intercepted in transit by attackers. SFTP encrypts all traffic, preventing unauthorized access to sensitive data. Encrypting data in motion is critical to prevent man-in-the-middle attacks. SFTP uses strong AES and RSA encryption algorithms to provide robust encryption security.

2 Encryption Protects Data in Transit

All data including file contents, file names, and commands are encrypted before being transmitted. The encrypted data can only be decrypted by the intended recipient. Even if the encrypted SFTP traffic is intercepted, attackers cannot decrypt the data without the encryption keys. This preserves confidentiality of the transferred data.

3 Strong Authentication Mechanisms

SFTP uses public key cryptography for strong authentication. Users authenticate with private keys rather than plaintext passwords. This prevents password brute-forcing attacks. Certificate-based authentication is also used to verify identities and establish trust between parties before transferring sensitive data.

4 Integrity Checks Ensure Data Is Not Modified

Integrity checks like checksums and hash algorithms are used to verify that files are not altered during transfer. This guarantees data integrity, preventing tampering of sensitive information by malicious actors. If any discrepancies in integrity checks are found, the transfer is aborted, preventing loss of data integrity.

5 Widely Adopted Open Standard

SFTP is an open IETF standard supported by all major operating systems. This interoperability provides flexibility to transfer files between diverse and incompatible systems that support SFTP. Open standards have greater adoption. By using SFTP, organizations can avoid vendor lock-in and seamlessly exchange data between various partners, contractors, and third-party agencies.

6 Supports Regulatory Compliance

Data security regulations like HIPAA, PCI DSS, and GDPR often mandate the use of secure transfer protocols. SFTP checks the boxes for data encryption in transit and other security controls required for compliance. Detailed logging and audit trails provide evidence of regulatory due diligence. This simplifies compliance audits for protected data.

Key Requirements for SFTP

For SFTP deployments to provide robust security, there are some key requirements related to encryption standards, access controls, compliance, and more.

Security Requirements for SFTP

1 Encryption Algorithms

SFTP allows negotiation of symmetric ciphers to encrypt session data. AES is the recommended standard that comes in key lengths of 128, 192, or 256 bits. AES-256 is preferred for utmost security.

2 Hashing Algorithms

Secure hashing algorithms like SHA-256, SHA3-256, or SHA-512 are used for data integrity and authenticity checks. SHA-1 is now considered obsolete.

3 Public Key Infrastructures

A public key infrastructure (PKI) is essential for managing user keys and certificates. A trusted Certificate Authority (CA) provides the root of trust for authentication.

4 User Access Controls for SFTP

Configuring least-privilege permissions as per zero-trust model is advised. Users must have granular folder/file level access without excessive privileges. Reviewing access regularly is also recommended.

5 Hardened Virtual Appliance

Using a hardened virtual appliance designed specifically for high security provides layered protection. Features like IP blacklisting, deactivated ports and protocols, and tuned OS parameters help secure SFTP servers.

Governance Requirements for SFTP

Governance is also a critical requirement for SFTP, consisting of the following:

1 Centralized Management

Centralized control of configurations, policies, user permissions, etc. instead of fragmented management is required. This provides unified visibility and administration.

2 Detailed Audit Logs

Comprehensive logging of all access requests, file transfers, and user activities is essential for security monitoring and forensics.

3 User and Access Monitoring

Ongoing monitoring of onboarding/offboarding, sudden increase in user permissions, and suspicious access patterns help identify risky events.

4 Policy Enforcement

Enterprise data policies for external sharing, retention periods, and restricted destinations must be enforced on the SFTP server for governance.

Compliance Requirements for SFTP

SFTP enables organizations to comply with various security standards and data privacy regulations, including:

1 Regulatory Requirements

Data privacy regulations often prescribe specific technical safeguards for transferring sensitive data. SFTP deployment must conform to applicable compliance requirements.

2 Encryption Standards

Mandated encryption strength and algorithms for data in transit must be implemented.

3 Audit Logs

Comprehensive activity logs that capture access, transfers, and violations are required as evidence of due diligence during audits.

4 Integration With Security Stack

The SFTP server should integrate with existing security tools like data loss prevention (DLP), advanced threat protection (ATP), and content disarm and reconstruction (CDR), among others. The hardened virtual appliance protecting the SFTP should have an embedded network firewall, WAF, antivirus, and intrusion detection.

Use Cases by Industry

SFTP provides a versatile solution for securely transferring files across numerous industry verticals.

Healthcare

Healthcare organizations use SFTP for:

- Securely transferring electronic health records between facilities. Patient privacy is protected.
- Allowing medical image sharing between practitioners for improved diagnostics through collaborative examination.
- Securely sending prescriptions to pharmacies from e-Prescription apps. Encryption prevents diversion of controlled substances.

Financial Services

Financial institutions use SFTP for:

- Secure transfer of payment data like card numbers, account information, etc. between financial networks. Encryption protects sensitive customer data.
- Sharing confidential financial reports, statements, transaction documents, etc. with auditors and regulators in a secure manner.
- Money transfers between banks domestically and internationally. File encryption safeguards the transmission.

Technology

Technology companies use SFTP for:

- Software and patch distribution from development teams to systems across the organization in a secure manner.
- Transferring source code between globally distributed developers and building servers to securely synchronize code.
- Allowing log file sharing between servers/applications and centralized log analysis systems. Encryption preserves the integrity of log data.

Government

Government agencies use SFTP for:

- Securely sharing classified documents between authorized personnel with appropriate security clearances.
- Secure collaboration between federal agencies and external contractors that require access to sensitive government data.
- Securely transferring files between various field offices of law enforcement and intelligence agencies.

Manufacturing

Manufacturing companies use SFTP for:

- Securely transferring design files, CAD drawings, and blueprints between facilities and external contractors. Encryption protects intellectual property.
- Sharing production schedules, inventory reports, and supply chain data with suppliers and vendors to coordinate operations.
- Allowing OEMs to send software updates and patches to machines and devices at customer sites to improve performance.

Legal

Legal firms use SFTP for:

- Securely collaborating with clients on case files, contracts, confidential documents, etc.
- Transferring sensitive client documents between attorneys working across multiple locations.
- Sharing information securely with external counsel, courts, regulators, and opposing counsel.

Pharmaceuticals and Life Sciences

Pharmaceutical and life sciences companies use SFTP for:

- Secure transfer of intellectual property like drug formulas, clinical trial data, and lab research between sites.
- Sharing patient information, test results, and medical records with doctors, hospitals, and CROs for clinical trials.
- Securely providing regulatory submission documents to government health agencies.

Professional Services

Professional services firms use SFTP for:

- Securely transferring client proposals, analysis, and confidential reports between engagement teams.
- Allowing remote consultants to securely access internal databases and collaboration folders.
- Securely sharing deliverables, findings, and results with clients upon project completion.

Government Contractors

Government contractors use SFTP for:

- Secure collaboration with government agencies on sensitive classified projects that require high security.
- Securely sharing progress reports, military project data, intelligence documents, etc.
- Allowing distributed teams to access classified files from multiple locations while preserving security protocols.

Higher Education

Higher education institutions use SFTP for:

- Secure transfer of student records between schools, colleges, universities, etc. while maintaining FERPA compliance.
- Sharing research work, lab results, dissertations, etc. between faculty and external research partners.
- Allowing faculty to access instructional materials, lecture notes, etc. remotely in a secure manner.

Why Kiteworks SFTP Is an Optimal Choice

Kiteworks offers a robust SFTP solution designed to keep enterprise requirements for security, governance, and compliance in mind.

1 Hardened Virtual Appliance

The Kiteworks SFTP server is deployed as a hardened virtual appliance with extensive security protections like IP blacklisting, an embedded network firewall, WAF, antivirus, intrusion monitoring, and detection. This creates an isolated environment, securing SFTP.

2 Flexible Deployment Options

Organizations can choose to deploy Kiteworks SFTP either on-premises, hosted on the Kiteworks cloud, or on their preferred cloud like AWS and Azure for flexibility aligned with business needs.

3 Comprehensive Monitoring and Logging

Kiteworks logs all SFTP activity such as logins, transfers, errors, and more in granular detail. Live feeds into SIEM allow security analytics. Summary reports aid compliance audits.

4 Easy Folder Management for Business Users

Business users can easily manage SFTP folders, add external partners, and set access permissions without IT help. This improves productivity while IT retains administrative control.

5 Scalability for Growing Transfer Loads

The Kiteworks SFTP architecture is designed to be highly scalable, using load balancers and high-availability configurations to handle increasing business demands seamlessly.

6 Integrates With Existing Workflows

Kiteworks SFTP integrates into organizations' existing scripts, applications, and automation workflows. There is no need for business process disruptions due to technology change.

7 Expert Support Services

Kiteworks provides stellar customer support and technical guidance spanning solution architecture, custom integrations, and optimizations. Customers can rely on expert assistance.

EBOOK

Secure, Reliable, Compliant SFTP

SFTP offers a secure and reliable means to protect sensitive data in transit. For comprehensive protection, organizations must implement SFTP solutions that provide robust encryption paired with strong access controls, detailed logging, scalability to meet growing demands, and more. Kiteworks helps organizations realize the full potential of SFTP deployments with an enterprise-class SFTP solution combining airtight security, seamless governance, and compliance capabilities tuned to your needs.

Kiteworks

www.kiteworks.com

October 2023