Why PGP is an extremely bad choice for a file server's at-rest encryption, and how to do it right

Pretty Good Privacy (PGP and all of its variants) is a well-known encryption program that provides cryptographic privacy and authentication for data communication. While PGP is excellent for securing emails and their attachments, using it for at-rest file encryption on a file server is not advisable. This article explains why PGP is unsuitable for this purpose and why a streaming encryption method is a better alternative.

Limitations of PGP for At-Rest File Encryption

Performance Overhead

PGP is designed for encrypting and decrypting individual files (like an email attachment, for example) or messages. When used for at-rest encryption on a file server, it introduces significant performance overhead. Each file must be encrypted and decrypted in its entirety, which can be time-consuming and resource-intensive, especially for large files or a high volume of files.

Scalability Issues

File servers often handle large amounts of data and numerous files. PGP's approach of encrypting files individually does not scale well in such environments. The process of encrypting and decrypting each file separately can lead to bottlenecks, reducing the overall efficiency of the file server.

Complex Key Management

PGP relies on a system of public and private keys for encryption and decryption. Managing these keys for a large number of files on a file server can become complex and cumbersome. Ensuring that the correct keys are used and securely stored adds an additional layer of complexity.

Lack of Real-Time Encryption

PGP does not support real-time encryption and decryption. Files must be fully written to disk before they can be encrypted and fully read before they can be decrypted. This lack of real-time processing can lead to security vulnerabilities, as files are temporarily stored in an unencrypted state.

Not Post-Quantum Secure

PGP relies on cryptographic algorithms like RSA and DSA, which are not considered secure against potential quantum computing attacks. Quantum computers could potentially break these algorithms, rendering the encrypted data vulnerable. In contrast, other encryption methods, such as AES-256 GCM, are considered resistant to quantum crypto-analytic attacks.

The Need for Streaming Encryption

Real-Time Encryption and Decryption

Streaming encryption methods allow for real-time encryption and decryption of data as it is written to or read from storage. This ensures that data is never stored in an unencrypted state, significantly enhancing security.

Improved Performance

Streaming encryption is designed to handle data in a continuous flow, which reduces the performance overhead associated with encrypting and decrypting entire files. This approach is more efficient and better suited for environments with high data throughput.

Scalability

Streaming encryption methods are inherently more scalable than PGP. They can handle large volumes of data and numerous files without the performance bottlenecks associated with PGP. This makes them ideal for use on file servers that need to manage extensive data storage.

Simplified Key Management

Many streaming encryption solutions use symmetric key encryption, which simplifies key management. A single key can be used to encrypt and decrypt data streams, reducing the complexity of managing multiple keys for individual files.

Conclusion

While PGP is a robust tool for securing individual files and communications, it is not suitable for at-rest file encryption on a file server. The performance overhead, scalability issues, complex key management, and lack of real-time encryption make it an impractical choice. Instead, streaming encryption methods provide real-time encryption and decryption, improved performance, scalability, and simplified key management, making them the ideal solution for securing data on a file server.

How Syncplify Server! does it 🗝️

At-rest encryption for a file server, and more specifically for an SFTP/FTP(E/S) server, is typically an Enterprise need; for such reason the Ultimate edition of Syncplify Server! has built-in top-notch at-rest streaming encryption at VFS level. This uses the **AES-256** algorithm (which is found to be post-quantum secure, unlike PGP) in **GCM** mode, which has also the added benefit of being **"*authenticated encryption*"** meaning it gives you the absolute certainty your data streams cannot be tampered with during the reading or writing operations.

Revision #4
Created 27 June 2024 10:47:45 by DevTeam
Updated 15 July 2024 19:34:49 by DevTeam