Avere FlashCloud Security Overview

Introduction

The Avere FXT Edge Filer with FlashCloud enables the use of cloud storage platforms as a core filer. In its beta iteration, this is done exclusively with Amazon Simple Storage Service (Amazon S3). Objects stored in a public cloud need to be kept confidential and their integrity must be protected. Objects are encrypted by the edge filer before being sent to the public cloud. This document addresses the security of data as it leaves the local premises.

Encryption

The Avere FXT cluster uses Amazon's REST API over HTTP or HTTPS to communicate with AWS S3. All objects written to the cloud are encrypted using 256-bit AES (Advanced Encryption Standard) in CBC (Cipher Block Chaining) mode. Each object stored in the cloud is encrypted using a randomly generated Data Encryption Key (DEK), which is unique per object. The DEK is encrypted with a Key Encrypting Key (KEK) which is known as Key Wrapping (RFC 3394). The wrapped DEK is stored along with the object. During decryption, the DEK is first unwrapped using the KEK, and then the object payload is decrypted using the DEK.

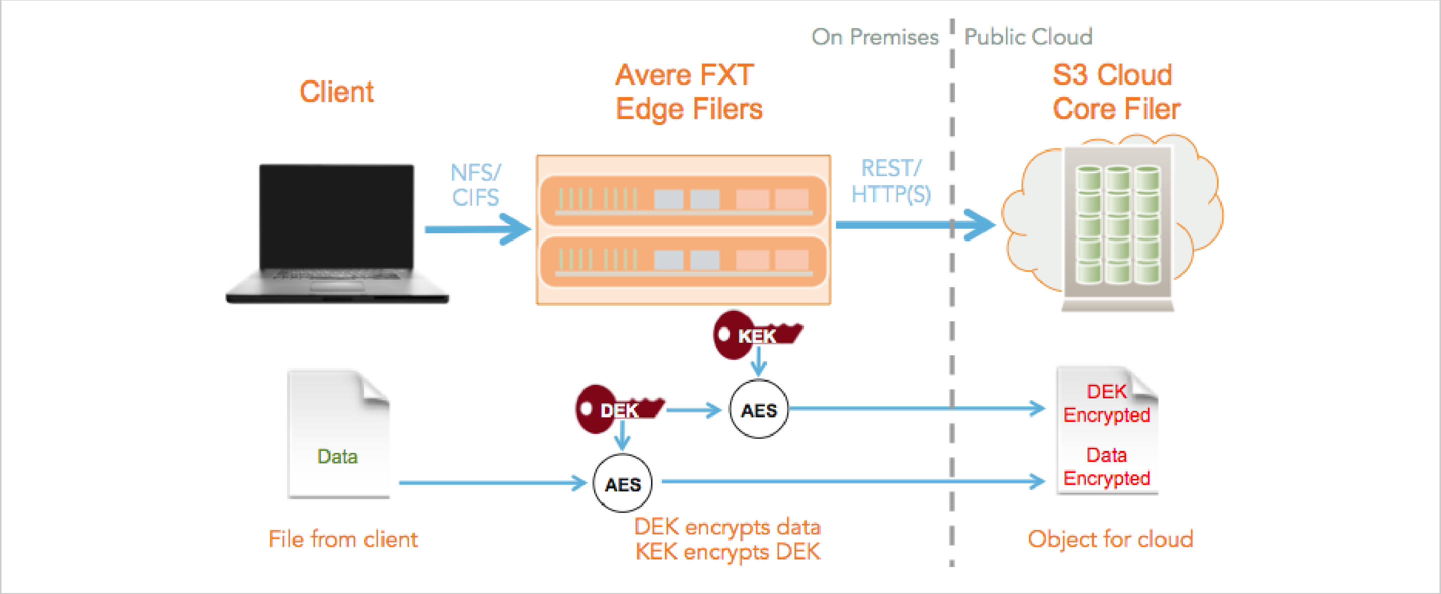

Figure: Encryption of cloud objects and Key Wrapping using the FXT Edge Filer

Integrity Protection

After encrypting the object, a Hashed Message Authentication Code (HMAC) using SHA-512 is calculated over the encrypted object, and the resulting code is appended to the object. For HMAC calculation, a separate randomly generated key is used, which is also wrapped with the KEK and stored with the object.

Key Management

A key database for each cloud core filer stores the current as well as all previous KEKs ever used. For key rotation, a new KEK can be generated any time. The key database can be downloaded by the cluster administrator, but it must first be encrypted with a user-supplied passphrase. The encrypted key database is downloaded at the time of KEK creation. It is the cluster administrator's responsibility to securely backup the key database and provide the passphrase for recovery.