redstor™

Technical White Paper

Backup Pro V8 and later: An overview of the security implementation

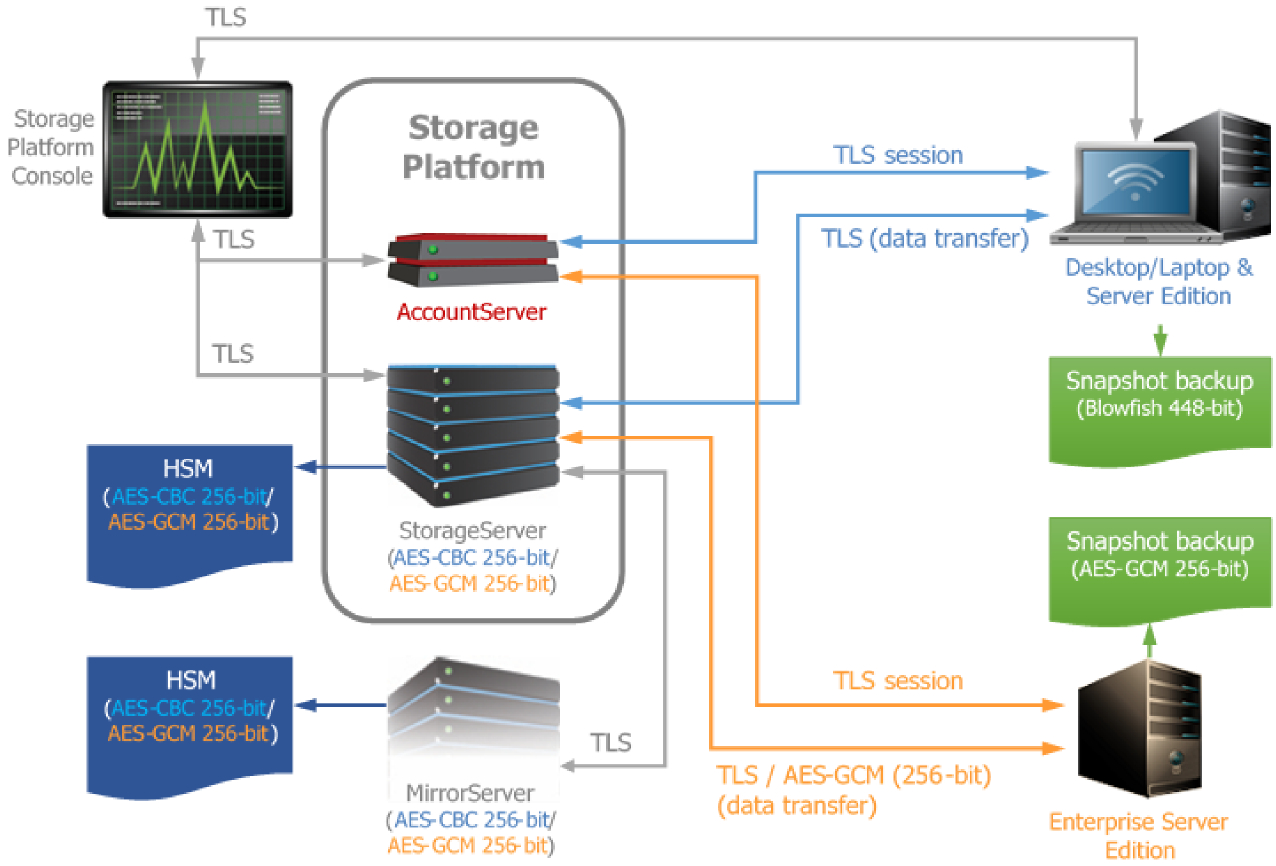
Contents

Summary

Backup Pro uses state-of-the-art security techniques, including TLS protocols and AES encryption to ensure the complete safety of all data that it protects. Backup Pro provides the security needed to confidently recover lost data in almost any situation.

Introduction

The graphic below illustrates a typical Backup Pro implementation with data being transferred either over LAN or to the cloud.


TLS
Storage Platform Console
TLS
TLS
Storage Platform
AccountServer
StorageServer (AES-CBC 256-bit/ AES-GCM 256-bit)
HSM (AES-CBC 256-bit/ AES-GCM 256-bit)
HSM (AES-CBC 256-bit/ AES-GCM 256-bit)
MirrorServer (AES-CBC 256-bit/ AES-GCM 256-bit)
TLS
TLS session
TLS (data transfer)
Desktop/Laptop & Server Edition
Snapshot backup (Blowfish 448-bit)
Snapshot backup (AES-GCM 256-bit)
TLS session
TLS / AES-GCM (256-bit) (data transfer)
Enterprise Server Edition

1. Storage Platform

- For releases V8 R3 and earlier, the Storage Platform allows Backup Client connections that use SSL up to SSL 3.0 and TLS 1.0 but would not be able to communicate through TLS 1.1 and 1.2 connections.

- Since release V8 R4, the Storage Platform only allows Backup Client connections that use TLS (1.0, 1.1 and 1.2) but TLS 1.2 is preferred since its cipher suites are the most secure.

Note: *Depending on the operating system configuration, the Backup Client will use SSL or TLS cipher suites. Since cipher suite selection cannot be controlled by Backup Pro, insecure connections are merely blocked at the Storage Platform (since release V8 R4). In addition, and to further improve security on the Storage Platform itself, a daily log message will appear about insecure cipher suites still accessible to the SP's operating system (as mentioned in Knowledge Base article 588)*

2. Desktop/Laptop and Server Editions

- TLS is used for authentication and to create a secure session for the data transfer between the DL/SE Backup Client and the SP.

  Note: *The Backup Pro components will only initiate communications on the configured ports if the Redstor certificates are installed and valid.*
- When creating Snapshot backups and restores as well as HSM archiving, the data is encrypted using the Blowfish 448-bit encryption algorithm.
- Backup data on the SP is stored in encrypted form using 256-bit Advanced Encryption Standard (AES) operating in Cipher-block Chaining (CBC) mode.

3. Enterprise Server Edition

- TLS is used to authenticate the data transfer and to create a secure session between the ESE Backup Client and the SP. Data is also encrypted using the 256-bit AES in Galois Counter Mode (GCM) encryption algorithm prior to being transferred.

  Note: *The Storage Platform components will only accept or initiate communications on the configured ports if the Redstor certificates are installed and valid.*
- When creating Snapshot backups and restores as well as HSM archiving, the data is encrypted using the 256-bit AES (GCM) encryption algorithm.
- Backup data on the SP is stored in encrypted form using 256-bit AES (GCM).

Further Reading

Also Refer to Redstor's Knowledge Base article 584 for Storage Platform configuration best practices.

Vulnerabilities

RC4

To secure the server where the StoragePlatform is installed against a vulnerability with the RC4 cipher, RC4 should be disabled. Please see Knowledge Base article 556 for more information.

POODLE

The POODLE vulnerability is a man-in-the-middle exploit that affects SSL 3.0. To secure the server where the StoragePlatform is installed, Redstor recommends disabling SSL 3.0 on Windows Server operating systems. Please see Knowledge Base article 556 for more information.