IBM Cloud
Data sheet

Aspera FASP Security Model

Comprehensive built-in security for business-critical digital assets

Key benefits

- Standards-based open-source cryptographic libraries are used to implement encryption with best-practices
- Encryption in transit and at rest helps ensure maximum security of business-critical digital assets
- Data integrity verification guards against man-in-the-middle, replay, and UDP denial-of-service attacks

Key features

- Built-in transport security uses the OpenSSL toolkit
- Sessions are securely initiated over an SSH control-channel
- User/endpoint authentication with native file system access control supports all major operating systems
- Data encryption in transit uses AES-CFB or AES-GCM cipher modes
- Data encryption at rest is supported as an option
- Data integrity verification is used for each transmitted datagram

Included in all IBM Aspera® software and hosted services, the patented Aspera FASP® protocol offers built-in security for data transfers using the standard open-source OpenSSL toolkit. The OpenSSL cryptographic library is used without modification in order to take full advantage of standards-based best practices implementation.

The security model enables each transfer session to establish a secure control-channel that can exchange a randomly-generated per-session key for data encryption and secure authentication of the transfer endpoints. In addition, the Aspera FASP protocol provides on-the-fly data encryption, and integrity verification for each transmitted datagram.

The transfer preserves the native file system access control attributes between all supported operating systems.

Secure session establishment

Each transfer job begins by establishing a secure, encrypted session between the endpoints, using a standard Secure Shell (SSH) control channel.

Once the secure session channel is established, the transfer endpoints authenticate using SSH. Both password and public-key authentication with passphrase-protected keys are supported.

Data encryption

Once SSH authentication has completed, the Aspera FASP transfer session performs a three-way handshake during which the client endpoint generates a random per-session AES key for data encryption (supporting sizes of 128, 192, and 256 bits), and sends these keys to the server endpoint over the secure SSH channel. A new encryption key is generated for each Aspera FASP transfer session, and the key is never stored on disk.

The Aspera FASP transport encryption includes support for both AES-CFB and AES-GCM cipher modes. Each mode can be independently configured in server configuration files as well as through the command-line client. Both AES-CFB and AES-GCM include data-integrity verification.

Firewall considerations

Each Aspera transfer server runs one SSH server on a configurable TCP port (22 by default; 33001 is often used). The firewall on the server side must allow this one TCP port to reach the Aspera server. No servers are listening on UDP ports. When a transfer is initiated by an Aspera client, it opens an SSH session to the SSH server on the designated TCP port and negotiates the UDP port (33001 by default) over which the FASP transport data will travel.

To allow the UDP session to start, the firewall on the Aspera server side must allow port UDP 33001 to reach the Aspera server. In cases where corporate firewalls disallow direct outbound connections (typically using proxy servers for web browsing):

- Allow outbound connections from the Aspera client on the TCP port and on the UDP port
- Allow either:
  - inbound UDP traffic responding to the outbound UDP (this is default on most firewalls)

  or
  - inbound UDP traffic on port 33001 (on non-standard firewall configurations)
- In the case of point-to-point deployments of Aspera products, the endpoints accepting incoming connections act as servers, and, therefore, their firewalls must allow TCP port 22 and UDP port 33001 (both configurable) to access the Aspera machine.

Concurrent transfer considerations

Transfers on Aspera transfer servers with multiple concurrent clients will:

- Share the same UDP port on UNIX and UNIX-like operating systems
- Require a range of UDP ports (e.g., 33001-33100) to be allowed on Windows because the operating system does not allow the Aspera FASP protocol to reuse the same UDP port for multiple connections. Incoming client connections will auto-increment to use the next available port in the range.

Support for FIPS 140-2

The National Institute of Standards and Technology (NIST), part of the United States Department of Commerce, provides the Federal Information Processing Standard (FIPS 140-2) for cryptographic modules. Aspera's core transfer technology supports FIPS 140-2 capabilities via an embedded FIPS 140-2 validated cryptographic module. This module comes from the OpenSSL toolkit and can be activated using the available FIPS mode configuration setting in the IBM Aspera High-Speed Transfer Server.

About IBM Aspera

IBM Aspera offers next-generation transport technologies that move the world's data at maximum speed regardless of file size, transfer distance and network conditions. Based on its patented, Emmy® award-winning FASP® protocol, Aspera software fully utilizes existing infrastructures to deliver the fastest, most predictable file-transfer experience. Aspera's core technology delivers unprecedented control over bandwidth, complete security and uncompromising reliability. Organizations across a variety of industries on six continents rely on Aspera software for the business-critical transport of their digital assets.

For more information

For more information on IBM Aspera solutions, please visit ibm.com/products/aspera or contact aspera-sales@ibm.com.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
December 2019

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on the specific configurations and operating conditions. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM product and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Please Recycle