IBM Aspera FASP Proxy

High-speed transfers in highly restrictive networks

Key benefits & capabilities

- Provides secure communication channel for FASP transfers to and from internal Aspera transfer servers and clients within highly restrictive networks
- Keeps corporate networks secure, using DNAT to hide internal IP addresses
- Allows only authorized internal client users to initiate FASP transfers through proxy
- Preserves key characteristics of FASP transfers such as maximum transfer speeds, data encryption and retry and resume of failed transfers

IBM® Aspera® FASP® Proxy protects your organization's network and business-critical digital assets while enabling secure, high-speed transfers within highly restrictive network environments. Designed for FASP-powered performance, it allows transparent pass-through of FASP transfer sessions across secure DMZs without impeding transfer speeds or compromising the security of your internal network.

Able to function as a forward or a reverse proxy, Aspera FASP Proxy consolidates FASP transfers in and out of a corporate network and enables precise control over which users can initiate FASP transfers with Aspera transfer servers. Proxy runs on select Linux versions and in the latest version supports load balancing and failover, as well as configurable security policies. With support for Aspera FASP Proxy built into all Aspera desktop and browser-based transfer clients, it is simple to configure, making it easy to use by all users within an organization.

Secure access in highly restrictive networks

Aspera FASP Proxy provides access to Aspera transfer servers located outside of the corporate network while protecting internal users' IP addresses. Optional user authentication helps control which clients are allowed access to outside Aspera transfer servers.

Scalable, enterprise-grade protection for internal resources

Functioning as a reverse proxy within a corporate DMZ, Aspera FASP Proxy protects the security of Aspera transfer servers deployed within the internal network. Using Dynamic Network Address Translation (DNAT), it enables Aspera clients to access the servers from outside without having to give away the servers' IP addresses to outside users. Options such as high-availability deployment and forwarding rules enable flexible and highly scalable architecture for the most demanding high-volume enterprise scenarios.

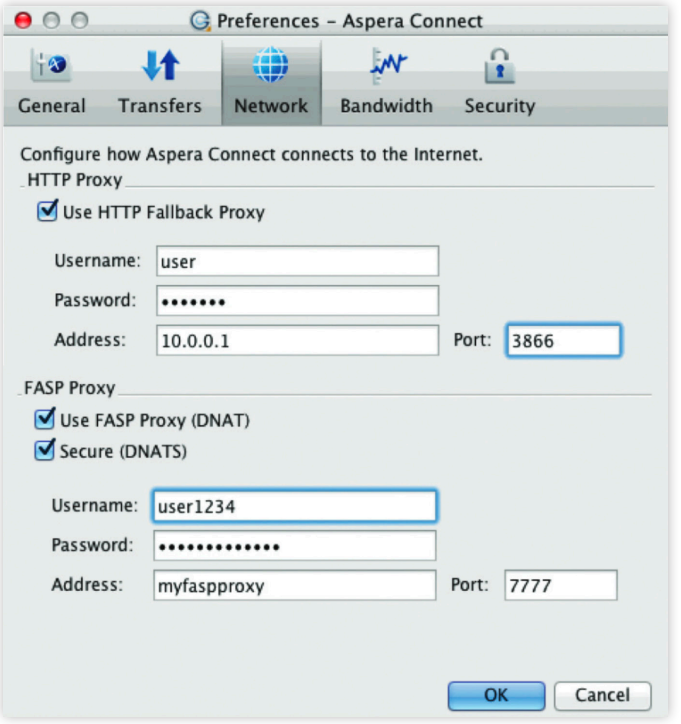

Figure 1: Configuration settings for Aspera FASP Proxy

Built for FASP performance

By using kernel-level packet forwarding to deliver high-speed transfer performance, Aspera FASP Proxy preserves key characteristics of FASP transfers such as speed, security, and 100 percent reliability found in all Aspera software products.

Easy-to-use client interface

With native support for Aspera FASP Proxy built into all desktop and browser-based Aspera clients, there are no special add-ons to install or scripts to run. A simple configuration within the client settings UI helps ensure seamless deployment and adoption by client users.

Key features

- Support for forward and reverse proxy deployments helps protect internal instances of Aspera transfer clients and servers.
- Kernel-level packet forwarding makes sure that FASP packets do not slow down, fully maintaining FASP transfer speeds.
- Dynamic Network Address Translation (DNAT) helps secure Aspera transfer servers and clients located behind corporate DMZ.
- Support for high-availability deployments.
- Fowarding rules enable load balancing.
- Allows client user authentication, enabling control over which internal users can perform FASP transfers.
- APIs enable secure, transparent proxying of FASP transfer sessions.
- Built-in support for Aspera FASP Proxy in all Aspera desktop and browser clients makes it easy to deploy across the enterprise.

Supported platforms

Limited-use Internet access

- Linux (RedHat or Debian) with kernel 2.4+

Aspera server software

- IBM® Aspera® Enterprise or Connect Server (v3.0+).
- Proxy-enabled and node-enabled server license.

Aspera client software

- IBM® Aspera® Desktop or Point-to-Point Clients (v3.0+).
- Aspera Connect (v3.0+).
- IBM® Aspera® Embedded Client (v3.0+)

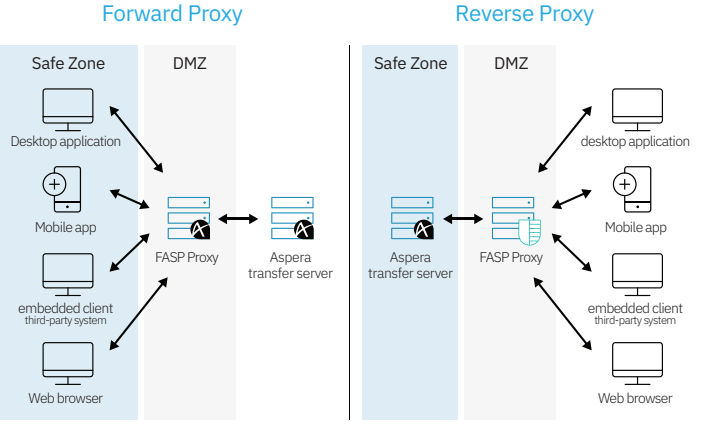

Figure 2: Aspera FASP Proxy environment

Use cases

Limited-use Internet access

Limited Internet access for internal users can affect the FASP protocol even if used for legitimate business needs. Aspera FASP Proxy provides secure access to the outside Aspera transfer servers without exposing users' IP addresses. It also enforces strict user authentication for Aspera clients that initiate connections to the outside servers.

Consolidate and control transfers

If you need to establish control and security around FASP transfers in and out of your network, Aspera FASP Proxy can fulfill your requirements without impeding end users' experience. It provides a single point through which all FASP transfers flow, hiding internal IP addresses and enabling control over which users can initiate transfers.

Protect internal transfer servers

To provide security for business-critical assets, it is often not an option to expose an Aspera transfer server by deploying it in the DMZ. To prevent direct connections, Aspera FASP Proxy can be deployed in the enterprise DMZ to hide the server's IP address, handle incoming connections and manage FASP sessions between outside Aspera clients and the server.

Features and benefits

Secure access to outside Aspera transfer servers

- Provides secure communication channel for FASP transfers between internal users within highly restrictive networks and outside Aspera transfer servers.
- Keeps corporate networks secure by using DNAT to hide internal clients' IP addresses.
- Controls which users can perform FASP transfers with optional client authentication.
- Provides APIs for secure, transparent proxying of FASP transfer sessions.

Scalable, enterprise-grade protection for internal Aspera transfer servers

- Protects internal servers using DNAT to forward FASP traffic.
- Supports high-availability deployments via multiple instances on a server cluster.
- Runs on select Linux versions and in the latest version supports load balancing and failover, as well as configurable security policies. tunneling to Aspera nodes, per-user encryption settings and enforceable encryption-at-rest policies.

Uncompromising FASP performance

- Uses kernel-level packet forwarding to make sure that FASP packets do not slow down, fully maintaining FASP transfer speeds.
- Preserves key characteristics of FASP transfers such as encryption, data integrity verification, and retry and resume of failed transfers.

Comprehensive administration

- Load balancing and failover capability for fronting multiple Aspera hosts.
- Includes configuration options for IP addresses, port numbers, cleanup and keep-alive intervals, timeout period and authentication.
- Supports proxy client accounts to make sure that only authorized client users can initiate FASP transfers through the proxy.

Easy-to-use client interface

- All Aspera desktop and browser clients provide built-in support for Aspera FASP Proxy.
- Simple configuration user interface requires minimal information and can be easily set up by non-technical users.

About IBM Aspera

Aspera, an IBM company, is the creator of 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

On IBM Aspera solutions, please visit us at https://www.ibm.com/cloud/high-speed-data-transfer or contact aspera-sales@ibm.com.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
November 2018

Please Recycle

KUD12394-USEN-01