Progress® MOVEit®

Ipswitch® Gateway

Multi-layer Security for MOVEit® Managed File Transfer

Ipswitch Gateway provides a DMZ proxy function that enables deployments of MOVEit Transfer within secured networks (behind the firewall) to meet the advanced compliance requirements often associated with data protection regulations such as GDPR, HIPAA and PCI-DSS.

SECURITY BENEFITS

- Facilitates compliance with mandates such as PCI DSS requirement §1.3.7 that protected data not be stored in the DMZ network.
- Eliminates the need to expose secured networked resources, authentication services such as AD or auditing data to the DMZ network risking public access

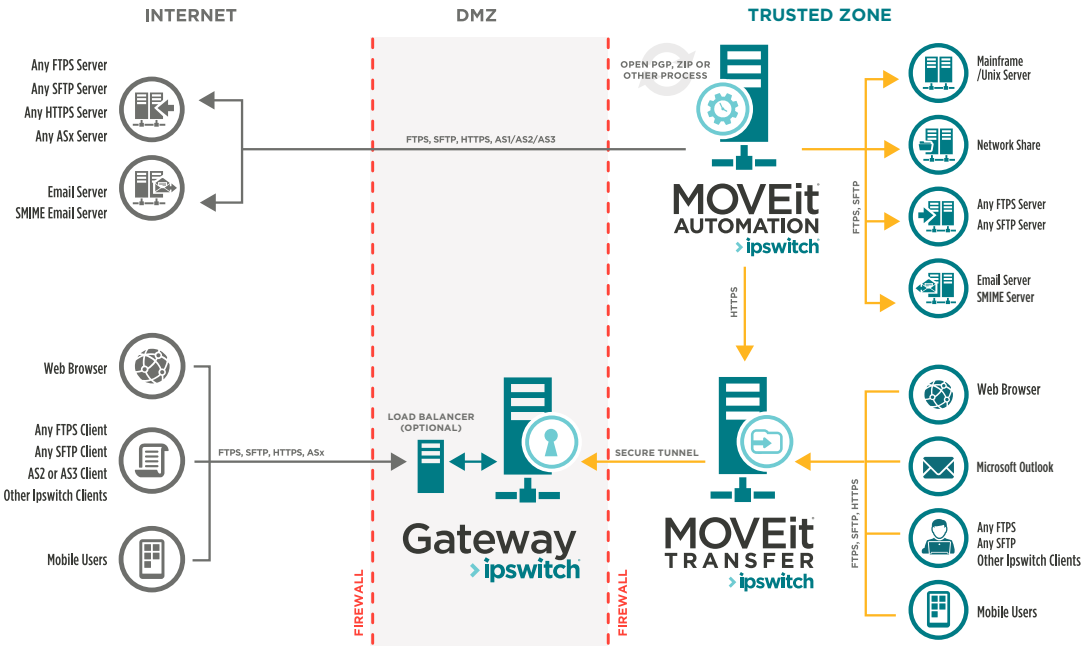
What is Ipswitch Gateway?

Ipswitch Gateway provides a multi-layered security approach that enables deployments of MOVEit Transfer within secured networks (behind the firewall). This ensures that data storage, authentication and file transfer activities do not occur in the DMZ network segment. When external regulations or internal security and compliance policies require the highest levels of security for data transmissions beyond your internal network, Ipswitch Gateway assures that:

- **Inbound connections from the public network are terminated in the DMZ network**
- **All data is secure within the trusted network – no data is stored in the DMZ network**
- **Authentication requests and authorization decisions are made within your trusted network as opposed to the DMZ network**

Deployment

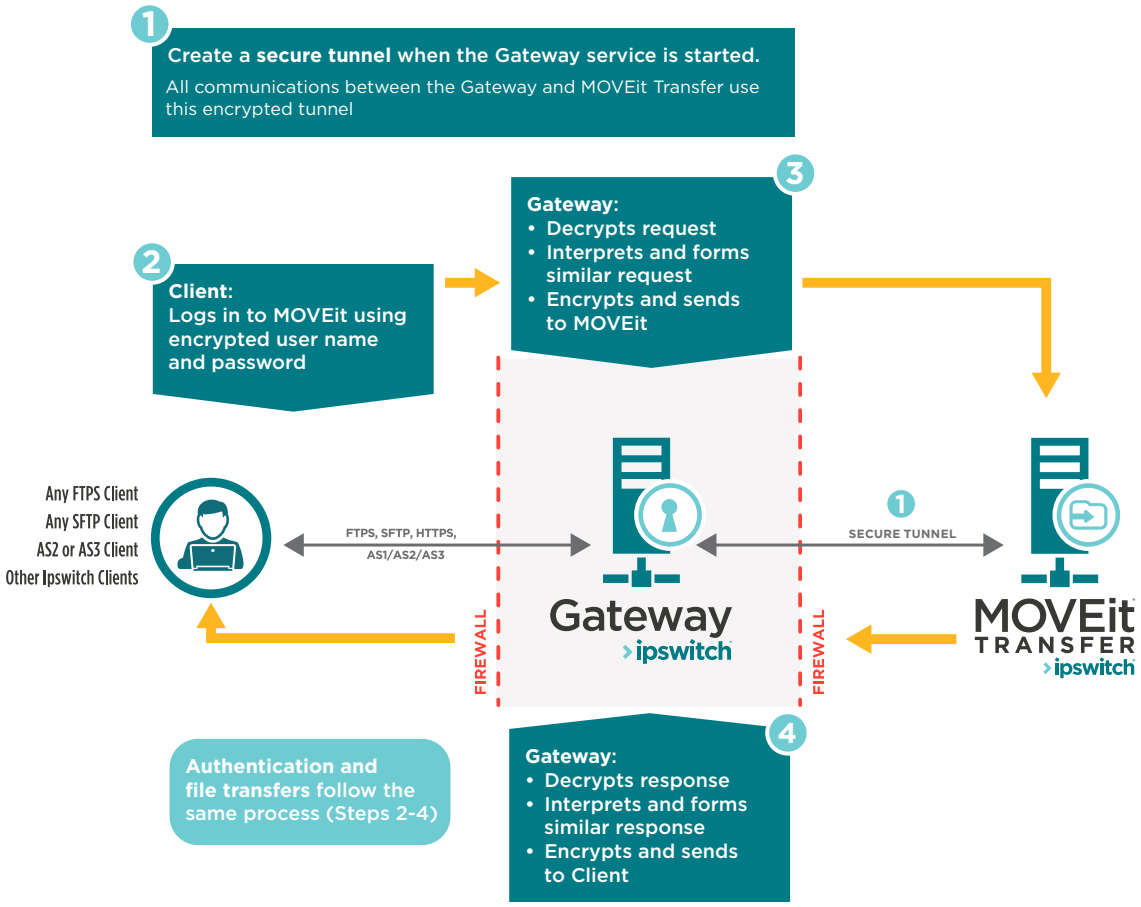
Ipswitch Gateway acts as a proxy between inbound connections from the public network and your internal trusted network. Deployed in the DMZ network, with MOVEit Transfer deployed behind the firewall in your secure network, it ensures that file transfer tasks are protected behind multiple layers of security.



Progress® MOVEit®

How it Works

When the Gateway service is started, it creates a secure tunnel to handle all communications between itself and the MOVEit Transfer server. Client SFTP and FTP/S authentication requests are terminated at the Gateway and formulated into a similar request between the Gateway and the MOVEit Transfer server. The response from the MOVEit server is again decrypted and reformed into a similar response which is then encrypted and sent back to the client. The same process is used for authentication and file transfer ensuring that all inbound connections are terminated, and all outbound connections originate at the Gateway and in the DMZ.



For a free trial please visit: www.ipswitch.com/forms/free-trials/moveit-transfer