ipswitch® › MOVEit

Ipswitch® 网关

MOVEit® 受控文件传输多层安全性

安全性优势

- 有助于遵循安全性要求，例如 PCI DSS 要求中 §1.3.7 受保护数据不得存储在隔离区（DMZ）网络中的规定。
- 免除了向具有公共访问风险的 DMZ 网络公开安全联网资源、AD 之类身份验证服务或审核数据的需要

MOVEit Transfer 和 MOVEit MFT Complete 的专业版和高级版提供了 Ipswitch 网关。Ipswitch 网关也可作为插件提供给 MOVEit Transfer（DMZ）的现有客户。

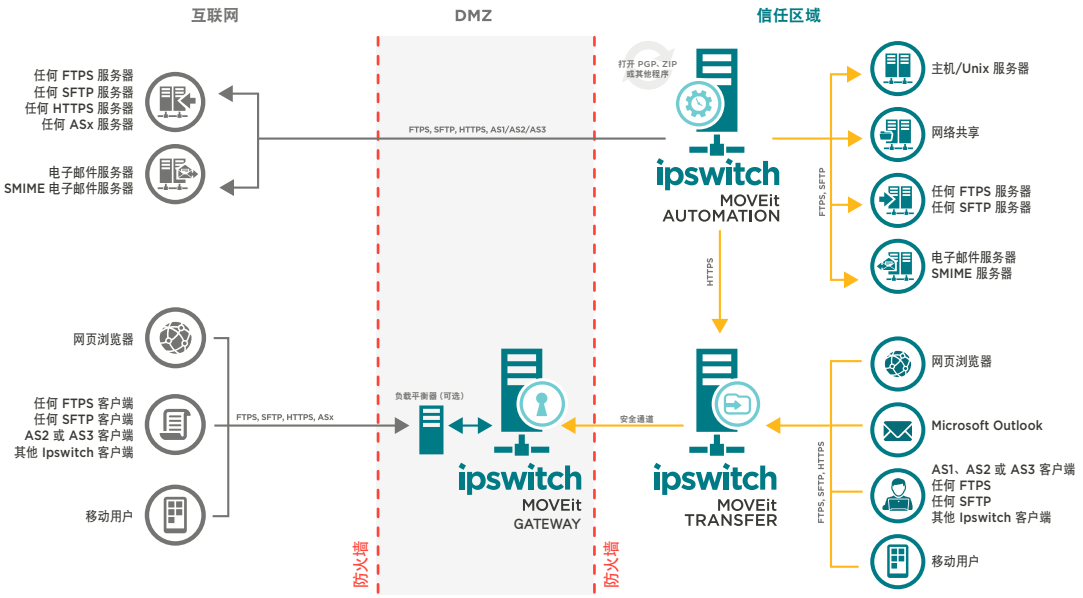
什么是 MOVEit 网关?

Ipswitch 网关采用达到并超过这些要求的一种多层安全方法提供 MOVEit Transfer 部署。它可以实现在安全网络内（防火墙后）对 MOVEit Transfer 的部署，确保数据存储、身份验证和文件传输活动不会在 DMZ 网络段进行。当外部法规或内部安全性和合规性政策要求内部网络以外的数据传输安全达到最高级别时，Ipswitch 网关可确保：

- 来自公共网络的入站连接在 DMZ 网络中终止
- 所有数据在可信网络中获得安全保障——数据没有存储在 DMZ 网络中
- 身份验证请求和授权决策在可信网络而非 DMZ 网络中作出

部署

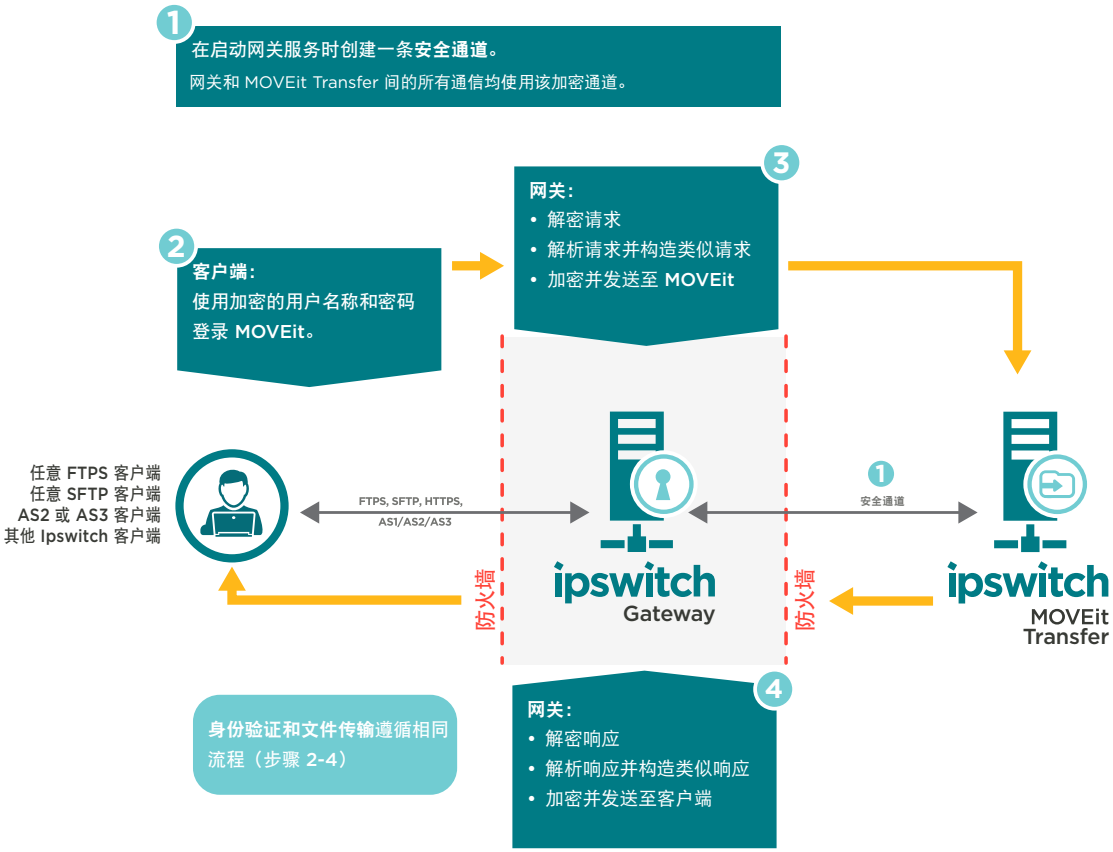
Ipswitch 网关充当来自公共网络和内部受信网络的入站连接间的代理。Ipswitch 网关部署在 DMZ 网络中，而 MOVEit Transfer 部署在安全网络的防火墙后，这确保了文件传输任务受到多层安全保护。



注：*MOVEit Automation* 是 *MOVEit Central* 的新名称，*MOVEit Transfer* 是 *MOVEit DMZ* 的新名称。

运作方式

网关服务启动时，会创建一条安全通道用来处理网关和 MOVEit Transfer 服务器间的所有通信。客户端 SFTP 和 FTP/S 身份验证请求终止于网关，构建出类似请求用于在网关和 MOVEit Transfer 间发送。来自 MOVEit 服务器的响应再次解密并重构成类似响应，在加密后发送回客户端。身份验证和文件传输采用相同流程，以确保所有入站连接在网关和 DMZ 中终止，所有出站连接在网关和 DMZ 中发起。



30 天免费试用，请登录： www.ipswitch.com/forms/free-trials/moveit-transfer

日本
Toru Sakakibara
sales_japan@ipswitch.com

中国、台湾、香港及澳门
Eric Yang
eyang@ipswitch.com

ASEAN
Raymond Lim
rlim@ipswitch.com

印度、韩国、澳洲及新西兰
Alessandro Porro
aporro@ipswitch.com