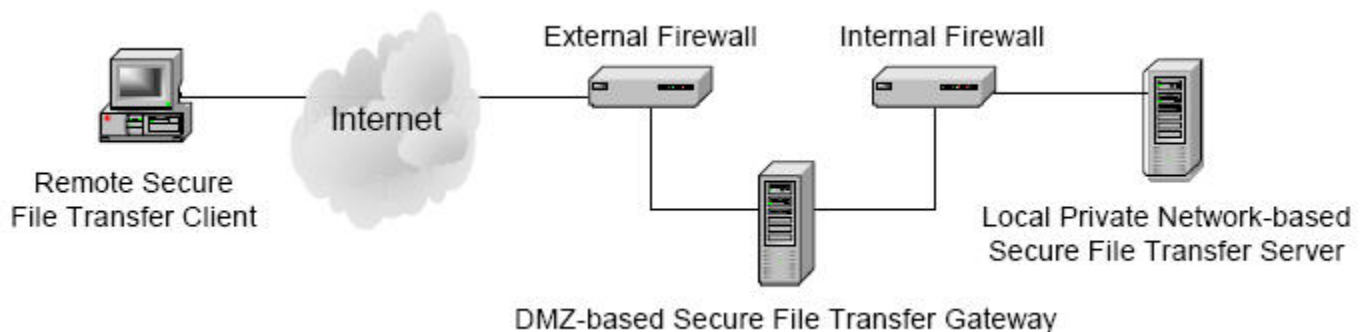


## SECURE FILE TRANSFER GATEWAYS: DANGER IN THE DMZ

BY JONATHAN LAMPE, GCIA, GSNA

To be accessible from the Internet, secure file transfer server solutions typically deploy some component in a demilitarized zone (a publicly accessible network segment known as a DMZ, which is attached to the firewall that protects the local private network). Some solutions place the server in the DMZ, which is how the MOVEit DMZ server by Ipswitch is deployed. Others put their server within the local private network and place a secure file transfer gateway (also referred to as a proxy or proxy server) in the DMZ, as shown in the diagram below.



This paper offers a general overview of gateways and security issues related to their use.

### What is a secure file transfer gateway?

A PC or appliance that plays a “man in the middle” role, exchanging authentication credentials, files, and other data between remote clients and a transfer server on the local private network.

### Why use one?

Gateways are intended to provide an extra layer of protection against attacks on the server by enabling it to be located on the access-restricted local private network instead of on the publicly accessible DMZ. The extra layer is intended to help keep unauthorized parties from gaining information about and access to the server, the files on it, and the local private network.

### How do they work?

Gateways are like actors — their job is to convince you that they are actually something else. When a remote client tries to connect to the server, the gateway intercepts the attempt and pretends to be the server. When talking to the server, the gateway pretends to be the client. The ability to fool clients and the server is an essential part of what gateways do — by design.

Some vendors offer gateways that initiate the connection to the server. This method requires open firewall ports from the publicly accessible DMZ into the restricted access private network. Under this approach, the gateway makes it appear to the client and server that they are talking directly to each other, even though a direct client-to-server connection does not actually exist.

Other vendors have their server initiate the connection to the gateway. This requires open firewall ports from the private network into the DMZ. This provides a virtual client-to-server connection because the gateway passes essentially everything sent to it by the client and server.

Server-initiated gateway connections are considered to be the more secure of the two methods because no ports have to be open from the publicly accessible DMZ into the private network.

### **What are the advantages of using a gateway?**

One advantage that is frequently cited by some secure file transfer vendors is that gateways do not store files in the publicly accessible DMZ — in contrast to DMZ-based file transfer servers. (It should be noted that this is not universally true; some gateways use virtual memory and/or disk caches to temporarily store files, authentication credentials, and other data that is being exchanged between the remote client and the server on the local private network.)

In theory, DMZ-based gateways also offer limited protection against a variety of common attacks. This claim must be judged in light of the following.

What are the disadvantages? While gateways are intended to create an extra layer of protection, serious security vulnerabilities are created when using a DMZ-based gateway with a server located on the local private network.

### **Using a gateway neutralizes an existing layer of defense.**

Whether initiated by the gateway or by the server, the connection between them is encrypted. This means the firewall that protects the local private network cannot monitor the traffic the gateway sends through it, and thus cannot block suspicious or dangerous protocols, data or files. In effect, the gateway-to-server connection is an open hole straight through the network firewall.

### **Gateways are a perfect tool for conducting Man-in-the-Middle (MITM) attacks.**

A MITM attack involves an unauthorized party gaining the ability to read, insert and/or modify the data being passed between remote clients and the server — without either being aware of it. Gateways are especially well-suited for use in a MITM attack. First, they are located between the remote clients and the server. Second, they are publicly accessible, with a fixed IP address that makes them easier to find. And third, because they do exactly what a MITM attack requires: make the client think it is talking to the server and the server think it is talking to the client. MITM attacks expose file contents (unless protected by PGP or similar third-party encryption). Even if such encryption is used, the authentication credentials sent by the client will be visible, enabling attackers to login to the server as authorized users, access files sent to or received by those users, and upload malware to attack the server and other systems on the private network.

### **A compromised gateway provides trusted access to the local private network.**

Unauthorized parties can take remote control of a gateway by running exploits against vulnerabilities in the gateway application and/or in the underlying operating system. Gateways that do protocol inspections of the traffic they receive are especially vulnerable to such attacks because they read – and

can be made to execute – commands that are sent to them. Gateways that ignore the traffic they pass are less vulnerable to such attacks, but are unable to detect them and thus offer no protection beyond what is already being provided by the firewall. Worse, if such a gateway is paired with a server that supports extended FTP commands for executing programs, then the gateway will actually forward the attack commands to the server.

**These security vulnerabilities make secure file transfer gateways a very tempting target.**

They are also an additional point of failure – and add hardware, software, and operational costs. For all these reasons, the MOVEit DMZ server by Ipswitch File Transfer *does not require a gateway*.

For additional information, please contact the Ipswitch File Transfer division or visit [www.lpswitchFT.com](http://www.lpswitchFT.com).



Contact Ipswitch's File Transfer Division