# TCP Firewall Port Guidelines

**THE INFORMATION IN THIS ARTICLE APPLIES TO:**

- EFT Server, all versions (Server Only)
- EFT Server Enterprise, all versions (Client and Server)
- CuteFTP, all versions (Client Only)

**DISCUSSION**

Following is an explanation of firewall rules needed for each protocol/mode to work:

For information about defining a range of ports, refer to "Specifying a PASV IP or Port Range" in the help documentation.

The ideal scenario is to support both Implicit SSL and Explicit SSL, when possible. From the server side, this support would look like this:

- INBOUND ports 21 from ANY
- INBOUND ports 990 from ANY
- INBOUND ports 28000-30000 from ANY
- OUTBOUND ports from source port 20 to ANY
- OUTBOUND from source port 989 to ANY

From the client view point:

- It is far simpler, easier, more secure, and more fool-proof to use Implicit SSL in PASV mode.
- Only OUTBOUND connections from their trusted network need to be allowed at that point. This reduces the security risk, avoids the need to set up complex firewall or NAT rules to maintain and conflicts to resolve, and it is encrypted from the moment the socket is opened.

Explicit SSL in PASV mode is the second-best choice. Sometimes Explicit SSL is the only FTPS type supported by some older legacy platforms, so there may not be any getting around that. But if Explicit SSL is used, then it is important to remember that Explicit SSL works by the client opening a socket and briefly communicating with in clear-text FTP mode, then issuing the AUTH_SSL or AUTH_TLS command to make the switch to SSL-encrypted FTP. This can cause problems with some firewall/NAT devices. These devices recognize, and

latch onto clear-text FTP connection, and then have no idea how to react during the SSL negotiations. It can often react by blocking any further communication that does not confirm to its idea of standard FTP. This is an exception, not the rule, but it is not rare, so be on the lookout for that.

PORT mode applies equally to both Explicit and Implicit SSL. The problem is that they have clients capable of being configured to issue public IP address and specific ports if client is behind NAT, as is always the case, as a part of the PORT command. It is a rare feature to have. But, they must also manage their firewall/NAT devices so as to appropriately allow direct incoming traffic from the untrusted public internet. This is rarely desirable, and it is never preferable when compared to PASV mode. It is not necessarily impossible, just potentially more painful and require intricate management and maintenance by administrators on the client side, deepening the furrows in the firewall and security personnel's collective brow. Usually this is only done when absolutely necessary due to legacy applications that have limitations which simply cannot be addressed in any other manner.

**Note:** The ports listed above are the default port configurations for EFT.  These ports can be configured for alternate ports within the application.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10022/TCP-Firewall-Port-Guidelines