Troubleshooting NAT firewalls

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT

DISCUSSION

Most NAT setups allow outbound connection initializations without any problems but if you need to configure outbound connections manually, refer to the chart below to see which ports should be allowed for *outbound* communications on the client side. The server side configuration is much more important in most cases.

For FTPS (SSL), the connection port and the PASV ports need to be forwarded. For SFTP (SSH2), there's no such thing as PASV mode, so only the connection port needs to be forwarded. The following list shows which ports should be forwarded to the server, assuming the default connection ports are being used. Please keep in mind that these ports need only be opened for *inbound* connections on the server side. You do not have to allow connections to be initialized outbound on the server side, as the connections will always be initiated from the client to the server.

Explicit SSL: 21, PASV range

Implicit SSL: 990, PASV range

SFTPS (SSH2): 22

The PASV range, which consists of ports 28000 to 30000 by default, can be defined in the Site Options tab, which is made accessible by clicking on the site in the tree view on the left. If you feel you need to restrict that range, the general rule of thumb is to take the maximum number of concurrent connections you think you're going to experience, and then add a third of that number to itself to get the total number of ports that should be open for smooth operation. NOTE: since the server will be behind NAT, you MUST specify the valid, external IP address (behind which the Server resides) in the PASV Mode Options.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10107/Troubleshooting-NAT-firewall...