



National Student Clearinghouse®
2300 Dulles Station Boulevard, Suite 300
Herndon, Virginia 20171

703-742-4200
www.studentclearinghouse.org

© 2009 National Student Clearinghouse. All rights reserved.

Secure FTP Firewall Guide

Client Firewall Settings

Web Browsers (HTTPS)

Web browsers use port 443 for establishing secure connections to the server.

- **REQUIRED: Allow TCP Port-443 to FTPS.NSLC.ORG**

FTP over SSL Clients (FTPS)

FTP connections are established from the client to the server via **Explicit** or **Implicit control channels**. Explicit FTPS control connections take place on TCP port 21. Implicit FTPS control connections take place on TCP port 990.

Once the control channel is established, the client and server negotiate a port for either **PASSIVE** or **ACTIVE MODE** data transfers. ACTIVE mode transfers take place on TCP port 20. PASSIVE mode transfers take place on a TCP port in the range 3000-3010. "Regular" FTP typically uses ACTIVE mode. However, for SSL connections, the Clearinghouse strongly recommends using PASSIVE MODE FTP transfers due to the following:

Simply specifying "FTP" on your firewall will rarely be enough to allow Secure FTP through. Firewalls that "understand FTP" look for the phrase "PORT" in data channels and open temporary holes in the firewall for communications over the designated ports between the two machines on either side of the data channel. However, secure data channels are encrypted, meaning the firewall will be unable to open any temporary ports.

Firewall Settings for Clearinghouse Recommended Implicit Control Channel, Passive Transfers:

- **REQUIRED: Allow TCP Port-990 to FTPS.NSLC.ORG (control channel)**
- **REQUIRED: Allow TCP Port range 3000-3010 to FTPS.NSLC.ORG (data channel)**

Alternate Firewall Settings for Explicit Control Channel, Active Transfers:

- **REQUIRED: Allow TCP Port-21 to FTPS.NSLC.ORG (control channel)**
- **REQUIRED: Allow TCP Port-20 to FTPS.NSLC.ORG (data channel)**

FTP over SSH Clients (SFTP)

A one-port SSH tunnel is established to support FTP over SSH clients. The use of a single SSH tunnel has an advantage over the multiple encrypted data streams used by FTP over SSL: fewer ports need to be opened on a firewall.

- **REQUIRED: Allow TCP Port-22 to FTPS.NSLC.ORG**

Questions?

If you have questions or need additional information, please contact Clearinghouse Customer Service at **703-742-4200** or secureftp@nslc.org.