

FTP OPERATION

NETASQ
Secure Internet Connectivity



Problem covered by the document

The **FTP** (File Transfer Protocol) used to transfer files between machines has specific features and the NETASQ firewall has been adapted to manage the protocol so as to safeguard and facilitate its use.

Development of the FTP

The first file transfer mechanism appeared in 1971, for use in an application on M.I.T. hosts. After many subsequent developments the FTP became the file transfer protocol between hosts on an ARPANET (the forerunner of the Internet) and its primary purpose was to transfer data efficiently and reliably between hosts to take advantage of a remote storage capacity. The choice of TCP as a transport protocol underlying the FTP made it possible to define the file transfer protocol as we know it today.

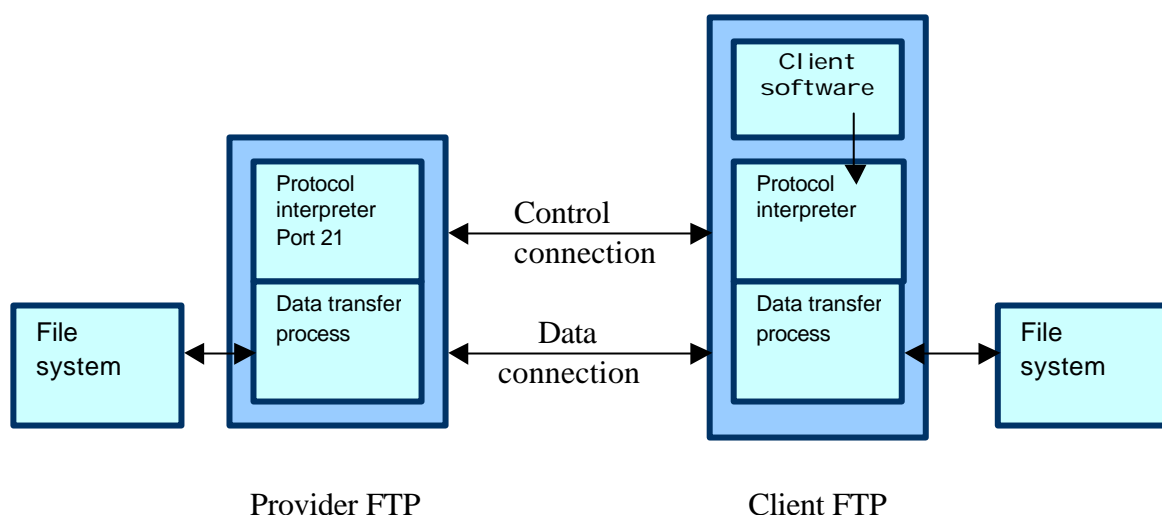
How the FTP operates

The FTP's main purpose is to promote file sharing and data transfers efficiently and reliably.

It uses two connections:

- a control connection on which FTP commands and control data are transmitted between the client and the provider
- a data connection for the transfer of data (files)

The FTP model can be schematised as follows:



The client FTP always controls the connection; using the interpreter the client asks for a connection with the provider through the provider's listening port (port 21) from a temporary port (with a port number higher than 1023). The provider makes the connection and the control channel is established.

There are two operational modes for the data connection - active and passive. The data connection may be established on the initiative either of the client or the provider, depending on the mode.

Explanation of the two FTP modes

The active mode:

In the active mode the provider initiates the data connection. In order to establish it the client sends his private IP address and the listening port which he will allocate to the future data connection through the control channel. This port is always a temporary port (with a port number greater than 1023). The provider receives this information and can then establish a connection with the client on the specified port from his own port 20 (FTP data).

The passive mode:

In the passive mode the client initiates the data connection. The provider sends his private IP address and the temporary port number for the data connection to the client via the control channel. The client who receives this information over the control channel can initiate the connection between one of his own temporary ports and the temporary port specified by the provider.

Most providers use both operating modes but some FTP clients use only one mode.

Differences between the active and passive modes:

The passive FTP involves a slight reduction in the transfer rate as compared with the active mode. However, it offers a better safeguard for your internal machines when you allow them access to FTP providers on the Internet – there is no connection from the Internet to your machines' temporary ports (the connection can only be initiated by your machines) but your users can connect to any temporary port of an Internet machine.

The active mode is safer when you host FTP providers as you do not authorize all the incoming connections on your FTP providers' temporary ports.

A few examples of FTP clients:

Passive clients: - Web browser using NETSCAPE Navigator and Communicator Web browser
- Web browser using Microsoft Internet Explorer (<5.0)

Active clients: - FTP DO client
- FTP UNIX client (other than Linux)
- Fetch (Macintosh) versions earlier than 3.03

Active/Passive clients: - Cute FTP
- WS FTP
- Smart FTP
- Fetch (Macintosh) versions later than 3.03
- FTP Linux Client
- Microsoft Internet Explorer 5 (active mode by default)






FTP management by the NETASQ firewall

Filtering

The NETASQ firewall has a proxy FTP that considerably simplifies FTP configuration. FTP operation usually requires two filtering rules - one for the control connection and one for the data connection --but with the FTP you only need to specify the control connection rule. The proxy FTP manages all the data connections, whether in active or passive mode and you don't need to worry about them any longer. This option safeguards your network even further, as the firewall will only open the ports required for FTP connections.

The rule is as follows:

Client (port: any) -> **Provider** (port: ftp - 21)

Source	Port source	Destination	Port destination	Action
 Client_FTP	 <Any>	 Serveur_FTP	 ftp	 pass

To activate the proxy FTP, select the option «Intelligent FTP» under the «General» heading in the network configuration.

Warning: the proxy FTP only operates in advance mode and not in transparent mode. You must therefore specify the following rules to authorize FTP in transparent mode.

In the active mode:

Client (port: any) -> **Provider** (port: ftp - 21)
Provider (port: ftp_data-20) -> **Client** (port > 1023)

Source	Port source	Destination	Port destination	Action
Client_FTP	= <Any>	Serveur_FTP	= ftp	pass
Serveur_FTP	= ftp-data	Client_FTP	> ephemeral_tcp	pass

In the passive mode:

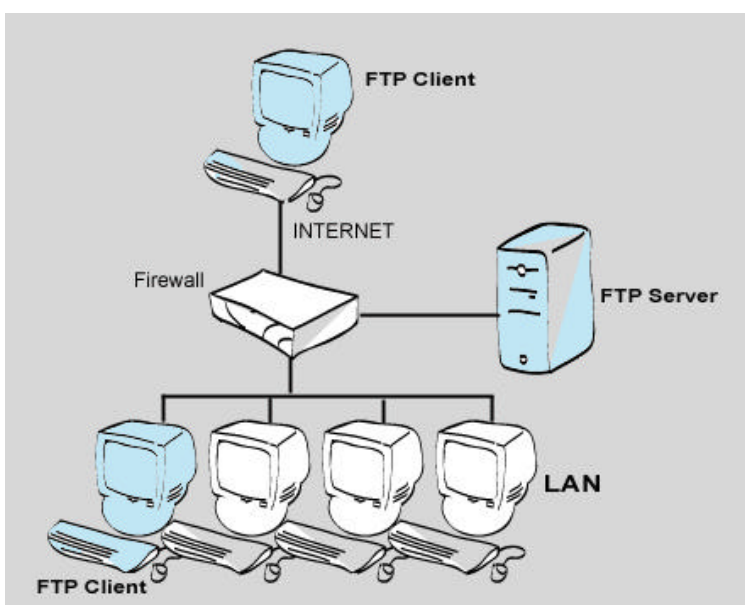
Client (port: any) -> **Provider** (port: ftp - 21)
Client (port > 1023) -> **Provider** (port > 1023)

Source	Port source	Destination	Port destination	Action
Client_FTP	= <Any>	Serveur_FTP	= ftp	pass
Client_FTP	> ephemeral_tcp	Serveur_FTP	> ephemeral_tcp	pass

If you define rules for a specific mode only clients and providers whose machines are compatible with this mode will be able to establish or receive a connection via the firewall (if the client machine accepts both active and passive modes it must be configured in the mode which complies with the published rules)

Note: the client may be on your network and the provider outside it (or vice versa). Client and Provider may represent a network.

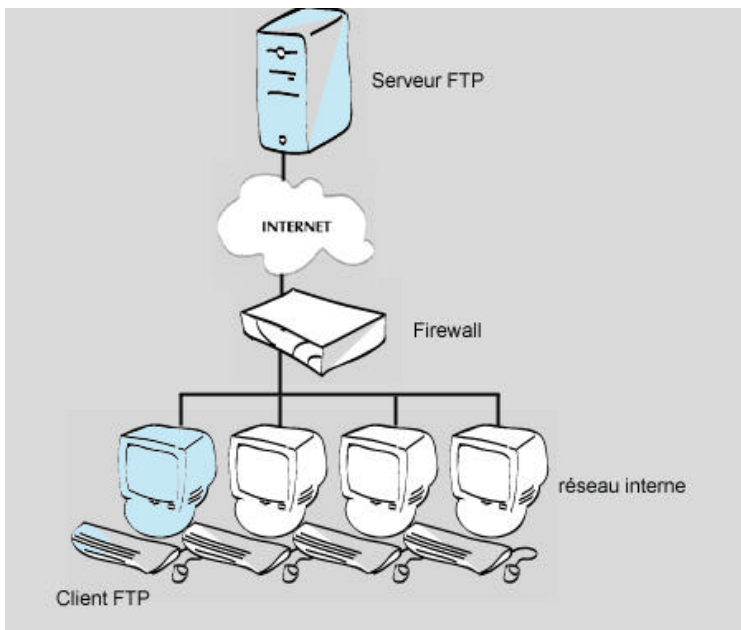
1st case: translating the FTP provider's address



The client FTP is located in the LAN or on the Internet and the FTP provider is in the DMZ. The FTP provider's private address is translated into a public address, either the external interface (internet) or the internal interface (LAN).

In this configuration the FTP operates in the active mode without difficulty but the passive mode cannot function. In this mode the provider sends the client his private IP address (in the control connection) and the port allocated to data connection. When the address is translated it does not match the address accessible to the client (the client can only contact the provider at his public address). The client can never access a provider whose address has been translated.

2nd case: translation of internal address



The client FTP is located in the LAN or on the Internet and the provider FTP is in the DMZ. The FTP provider's private address is translated into a public address, either to the external interface (Internet) or the internal interface (LAN).

In this configuration the FTP operates without difficulty with the NETASQ firewall in both active and passive modes.

In fact you can select the «Active FTP» in the address translation slots. If you choose this option the NETASQ firewall will change the address in the FTP command and will replace it with the translated address, enabling you to use the active FTP in all cases.

If the firewall has not carried out this additional operation it will not be possible to use the active FTP in the present configuration, as in this mode the client sends his private IP address in a command. The provider cannot access this address on the Internet as he only knows the client's translated (public) address.