Network Configuration

Setting up FTP is not easy. Since thousands of different firewalls and router models exist, it is impossible to give detailed step-by-step instructions suitable for every user. So in order to configure FileZilla as well as the routers and/or firewalls involved, it is important for the user to understand the basics of the FTP protocol. This documentation describes the history of the FTP protocol and how some aspects of the protocol work. Please read it carefully; it will save you a lot of trouble setting up FTP.

Contents

Background [edit]

This section will give a short overview about the historical and technical background of the FTP protocol. For detailed in-depth information, please have a look at the specifications.

Historical Background [edit]

In the fast living world of the Internet the FTP protocol is not just old, it's ancient. Early drafts of the FTP protocol range back as far as 1971, with the current specifications being from 1985. During the past two decades, the FTP protocol hasn't changed at all in its core. The protocol might even be older than you!

Back then, the Internet was mainly used by universities and research centers. The community was small, most users knew each other and all were collaborating together. The internet was a friendly place. Security was not a big issue. People either did not know about that topic or were unconcerned about it.

Since then, a lot has changed. Technology advanced way faster than anyone imagined and a new generation of users was born and grew up. The Internet is now ubiquitous, with millions of users communicating with each other in many different ways. One more thing has changed: The internet is now a hostile place. The availability and openness of the internet also attracted malicious users who are actively exploiting design flaws, bugs and the inexperience of other users. A well-known software company located in Redmond, WA certainly played a part in this.

Some of the by-products of this development are the following:

- NAT routers. Most of the internet uses the IPv4 protocol which has a very limited address range. Thanks to NAT routers, multiple systems can easily share the same external IP address.
- Personal firewalls which are designed to protect the user from flaws in the operating system and the applications running on top of it.

These products tend to conflict with the FTP protocol more often than not. To make things worse, some of them even have flaws themselves, causing additional problems regarding FTP.

With proper configuration however, FTP still works as a mature, reliable way to transfer files.

Technical background [edit]

What distinguishes FTP from most other protocols is the use of secondary connections for file transfers. If you connect to an FTP server, you establish the so-called *control connection* , over which the FTP commands and their replies are transferred. In order to transfer a file or a directory listing, the client sends some command over the control connection to establish the *data connection* .

This data connection can be established in two different ways, called active mode and passive mode.

In passive mode, which is the recommended mode, the client sends the PASV command to the server, and the server responds with an address. The client then issues a command to transfer a file or to get a directory listing and establishes a secondary connection to the address returned by the server.

In active mode, the client opens socket on the local machine, and tells its address to the server using the PORT command. Once the client issues a command to transfer a file or listing, the server will connect to the address provided by the client.

In both cases, the actual file or listing is then transferred over the data connection.

In general, establishing outgoing connections requires less configuration on the routers/firewalls involved than establishing incoming connections. In passive mode, the connection is outgoing on the client side and incoming on the server side. In active mode however, the roles are reversed: The data connection is incoming on the client side and outgoing on the server side. Please note that this only makes a difference for connection establishment: Once the data connection gets established it can be used for either up- or downloads.

A common network setup might look like this:

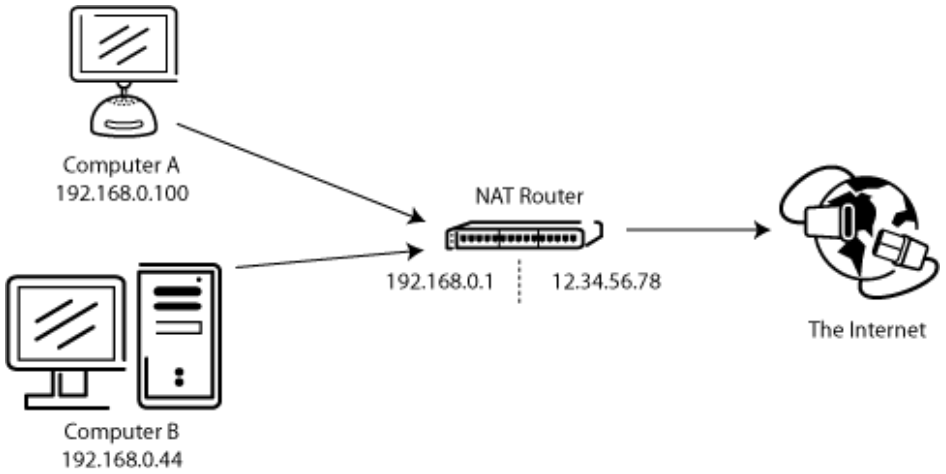
So in passive mode, the router and firewall on the server side need to be configured to accept and forward incoming connections. On the client side however, only outgoing connections have to be allowed, which will already be the case most of the time.

Analogous in active mode, the router and firewall on the client side need to be configured to accept and forward incoming connections. Apparently on the server side, only outgoing connections have to be allowed.

Since usually one server provides a service for many users, it is far easier to just configure the router and firewall on the server side once for passive mode, than to configure the client's router/firewall for each individual client in active mode. That is why passive mode is recommended.

NAT routers [edit]

For most broadband users, there will be a NAT (Network Address Translation) router between their computer and the internet. This NAT router may be a standalone router device (perhaps a wireless router), or it could be built into a DSL modem or Cable modem. In a NAT environment, all systems behind the NAT router form a *Local Area Network (LAN)* and each system in the LAN has a local IP address (recognizable as four small numbers separated by dots). The NAT router itself has a local IP address as well. In addition to that, the NAT router also has an external IP address under which it is known to the internet. The internal IP addresses are only valid inside the LAN, for a remote system they would make no sense. Example:



Assume a server is behind a NAT router. Imagine what happens if a client requests passive mode but the server does not know the external IP address of the NAT router. So the server sends its internal address to the client. In that case two things could happen:

- If the client is not behind a NAT, client would abort since address is invalid.
- If client is behind a NAT, the address given by the server might be the same as a system in the client's own LAN.

Obviously, in both cases passive mode would be impossible.

So if a server is behind a NAT router, it needs to know the external IP address of the router in passive mode. In that case, the server sends the router's external address to the client. The client then establishes a connection to the NAT router, which in turn routes the connection to the server.

Firewalls [edit]

The purpose of a *Personal Firewall* is to protect the user from security vulnerabilities in the operating system or the applications running on it. Over the internet, malware like for example worms try to exploit these flaws to infect your system. Firewalls can help to prevent such an infection.

Especially if using FTP, firewall users might sometimes see messages like this from their firewall:

```
Trojan Netbus blocked on port 12345 used by FileZilla.exe
```

In almost all cases, this is a **false alarm**. Any program can choose any port it wants for communication over the internet. So it can happen that FileZilla happens to choose a port that is incidentally the default port of a trojan or some other malware. As long as you download FileZilla from the official website, it is clean of any malware.

Malicious routers, firewalls and data sabotage [edit]

Some routers and firewalls pretend to be smart. They analyze the connections and if they think it is FTP, they silently change the data exchanged between client and server. If the user has not explicitly enabled this feature, this behavior is nothing else than data sabotage and can cause various problems.

To illustrate with an example, assume there is a client behind a NAT router trying to connect to the server. Let's further assume that this client does not know it is behind a NAT and wants to use active mode. So it sends the PORT command with his local, unroutable IP address to the server:

```
PORT 10,0,0,1,12,34
```

The above command tells the server to connect to the address 10.0.0.1 on port 12*256+34 = 3106

The NAT router sees this and silently changes the command to include the external IP address. At the same time, the NAT router will also create a temporary port forwarding for the FTP session, possibly on a different port even:

```
PORT 123,123,123,123,24,55
```

Now the above command tells the server to connect to the address 123.123.123.123 on port 24*256+55 = 6199

With this behavior, a NAT router allows an improperly configured client to use active mode.

But why is this bad? If this feature is enabled by default, without explicit user consent, it causes lots of problems. FTP connections in its most basic form appear to work, but as soon as there's some deviation from the basic case, everything will fail, leaving the user totally stumped:

- The NAT router blindly assumes some connection uses FTP based on criteria like target ports or the initial server response:
  - There is no guarantee that the used protocol really is FTP, yet it is detected as such (also called *false positive*). Though unlikely, it is conceivable that in a future revision of the FTP protocol, the syntax of the PORT command might change. A NAT router modifying the PORT command would silently change things it does not support and thus break the connection.
  - The router's protocol detection can fail to recognize an FTP connection (a *false negative*). Let's assume the router only looks at the target port, and if it is 21, it detects it as FTP. As such, active mode connections with an improperly configured client to servers running on port 21 will work, but connections to other servers on non-standard ports will fail.
- Obviously, a NAT router can no longer tamper with the connection as soon as an encrypted FTP session is used, again leaving the user clueless why it works for normal FTP but not for encrypted FTP.
- Assume a client behind a NAT router sends "PORT 10,0,0,1,12,34". How does the NAT router know the client is improperly configured? It is also possible that the client is properly configured, yet merely wants to initiate an FXP (server-to-server) transfer between the server it is connected to and another machine in the server's own local network.

As you can see, having protocol specific features enabled in a NAT router by default is a bad thing. A good NAT router should always be fully protocol-agnostic. The exception is if you as user have explicitly enabled this feature, knowing all its consequences.

While this section only discussed the combination of a NAT router on the client side with active mode, the same

applies to a server behind a NAT router and the reply to the PASV command.

Setting up FileZilla Client [edit]

In case you're running FileZilla 3, it's recommended you run the network configuration wizard. It will guide you through the necessary steps and can test your configuration in the end.

Obviously, if you want to connect to any server, you need to tell your firewall that FileZilla should be allowed to open connections to other servers. Most normal FTP servers use port 21, SFTP servers use port 22 and FTP over SSL/TLS (implicit mode) use port 990 by default. These ports are not mandatory though, so it's best to allow outgoing connections to arbitrary remote ports.

Since there are many servers on the internet that are misconfigured and don't support both transfer modes, it's recommended that you configure both transfer modes on your end.

Passive mode [edit]

The client has no control over what port the server chooses for the data connection in passive mode, so in order to use passive mode, you'll have to allow outgoing connections to all ports in your firewall.

Active mode [edit]

In active mode, the client opens a socket and waits for the server to establish the transfer connection.

By default, FileZilla Client asks the operating system for the machine's IP address and for a free port number. This configuration can only work if you are connected to the internet directly without any NAT router and if you have set your firewall to allow incoming connections on all ports greater than 1024.

If you have a NAT router, you need to tell FileZilla your external IP address or active mode connections will not work with servers outside your local network:

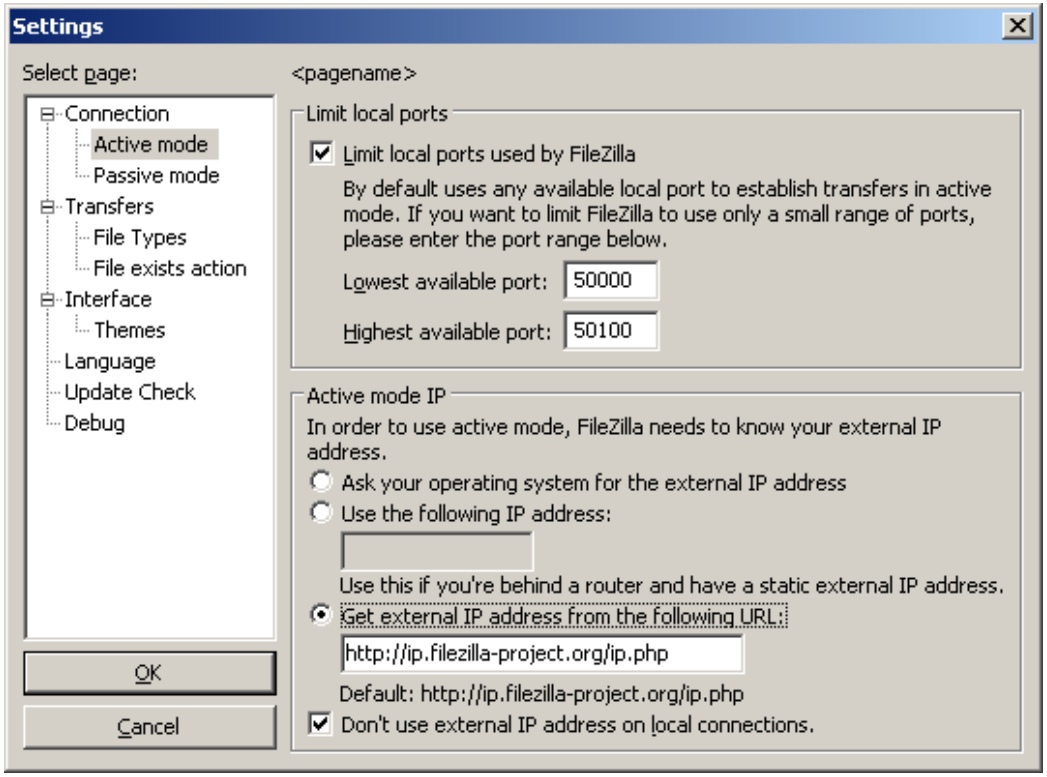
- If you have a fixed external IP address, you can enter it in the configuration dialog of FileZilla.

- If you have a dynamic IP address, you can let FileZilla obtain your external IP address from a special website automatically each time you start FileZilla. No matter what version of FileZilla you have, no information will be submitted to that website.

If in doubt, use the second option.

If you do not want to allow incoming connections on all ports, or if you have a NAT router, you need to tell FileZilla to use a specific range of ports for active mode connections. You will have to open these ports in your firewall. If you have a NAT router, you need to forward these ports to the local machine FileZilla is installed on. Depending on your router model, you can either forward a range of ports or you need to forward all ports individually.

Valid ports can be from 1 to 65535, however ports less than 1024 are reserved for other protocols. It is best to choose ports greater than or equal to 50000 for active mode FTP. Due to the nature of TCP (the underlaying transport protocol), a port cannot be reused immediately after each connection. Hence the range of ports should not be too small or transfers of multiple small files can fail. A range of 50 ports should be sufficient in most cases.



Setting up FileZilla Server [edit]

Setting up the server is very similar to setting up the client, the main difference is that the roles of active and passive mode are reversed.

One common mistake done especially from users with NAT routers is the way they test the server. If you are within your local network, you can only test using the local IP address of the server. Using the external address from the inside will probably fail. Basically one of the following could happen if you try to connect using the external address from the inside:

- It surprisingly works
- Router blocks access to its own external address from the inside as possible attack
- Router forwards connection to your ISP which then blocks it as possible attack

Even if that works, there is no guarantee an external user can really connect to your server and transfer files. The

only reliable way is to connect to your server from an external system outside of your LAN.

Active mode [edit]

Just make sure FileZilla Server is allowed to establish outgoing connections to arbitrary ports, since the client controls which port to use.

For the local end of the connection, FileZilla Server tries to use a port one less than that of the control connection (e.g. port 20 if server is listening on port 21). However this is not always possible, so don't rely on it.

Passive mode [edit]

Server configuration is very similar to client configuration for active mode.

In passive mode, the server opens a socket and waits for the client to connect to it.

By default, FileZilla Server asks the operating system for the machine's IP address and for a free port number. This configuration can only work if you are connected to the internet directly without any NAT router and if you have set your firewall to allow incoming connections on all ports greater than 1024.

If you have a NAT router, you need to tell FileZilla Server your external IP address or passive mode connections will not work with clients outside your local network:

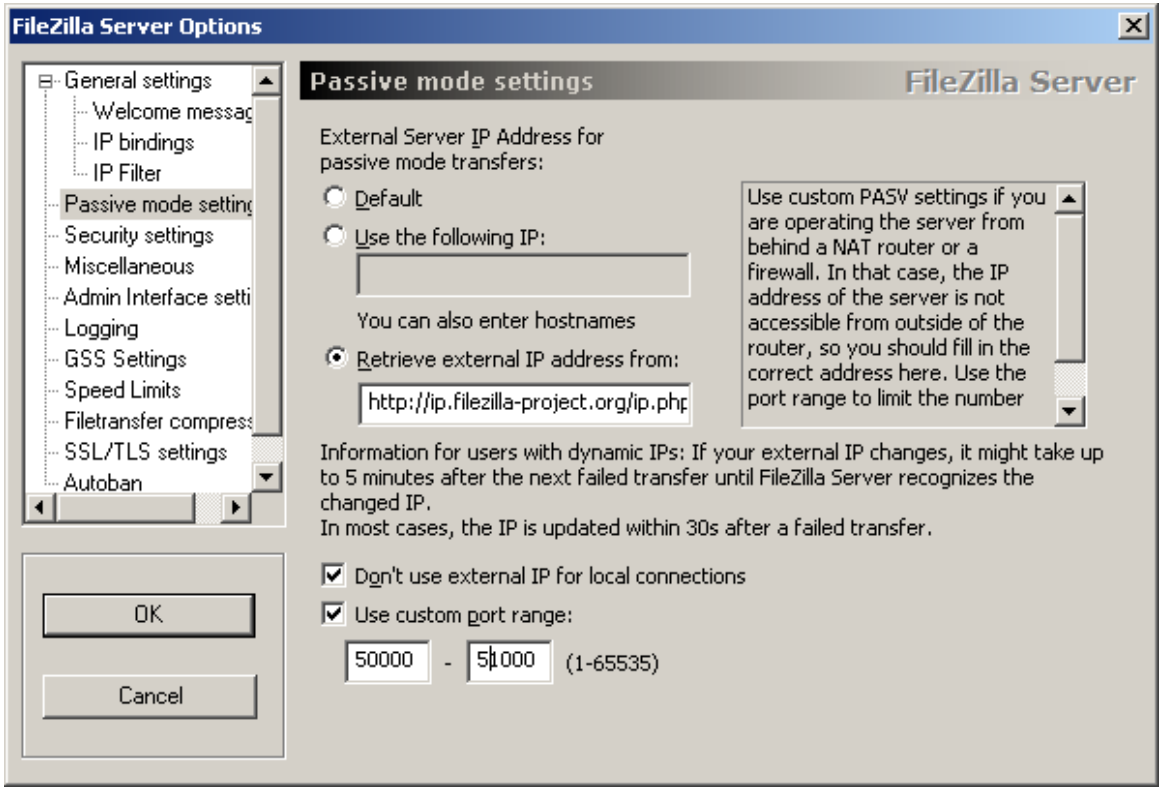
- If you have a fixed external IP address, you can enter it in the configuration dialog of FileZilla Server.
- If you have a dynamic IP address, you can let FileZilla Server obtain your external IP address from a special website automatically. Except your version of FileZilla Server, no information will be submitted to that website.

If in doubt, use the second option.

If you do not want to allow incoming connections on all ports, or if you have a NAT router, you need to tell FileZilla Server to use a specific range of ports for passive mode connections. You will have to open these ports in your firewall. If you have a NAT router, you need to forward these ports to the local machine FileZilla Server is

installed on. Depending on your router model, you can either forward a range of ports or you need to forward all ports individually.

Valid ports can be from 1 to 65535, however ports less than 1024 are reserved for other protocols. It is best to choose ports >= 50000 for passive mode FTP. Due to the nature of TCP (the underlaying transport protocol), a port cannot be reused immediately after each connection. Hence the range of ports should not be too small or transfers of multiple small files can fail. A range of 50 ports should be sufficient in most cases.



Troubleshooting [edit]

Unfortunately, many personal firewalls and consumer routers are flawed or in some cases, are even actively sabotaging FTP (e.g. SMC Barricade V1.2).

First of all, you should keep everything up-to-date. This includes the firewall software as well as the firmware version in your router.

If that does not help, you might want to try to **uninstall** your firewall to see what happens. Simply disabling your firewall might not work, as some firewalls cannot be fully disabled.

If possible, try to connect directly to the internet without a router.

If you are trying to setup a server and it works fine within your LAN but is not reachable from the outside, try changing the listening port. Some ISPs don't like its customers to host servers and block ports < 1024.

Another problem might be if you are hosting an FTP server on default port 21. There might be a firewall at the ISP side of your connection which can do odd things like changing the port for PASV commands. Try using another non-default port for your FTP server.

If you encounter "cannot open data connection" on a random basis, i.e. the ftp client can connect to the ftp server without problem for many connections until it encounters this problem, one possible reason may be your client PC anti-virus scanner being configured to block outgoing connections on certain ranges of ports. When your ftp connections are running on pasv mode, the client side outgoing ports are selected randomly and when it hits those prohibited ports, you will encounter your problem. To identify this problem, read your anti-virus log on that client. In general, any software e.g. PC firewall, etc that can block certain range of outgoing ports can cause similar ftp grief.

Timeouts on large files [edit]

If you can transfer small files just fine, but transfers of larger files end with a timeout, then there is a broken router and/or firewall between the client and the server that is causing this problem.

As mentioned above, FTP uses two TCP connections: One control connection to submit commands and to receive replies as well as one data connection for the actual file transfers. It is the nature of FTP that during a transfer the control connection stays completely idle.

The TCP specifications do not set a limit on the amount of time a connection can stay idle. Unless explicitly closed

a connection is assumed to remain alive indefinitely. Many routers and firewalls however automatically close idle connections after a while. Worse, they most of the time don't even notify the endpoints of this, instead they just silently drop the connection. So for FTP this means that during a long transfer the control connection can get dropped, but neither client nor server get to know about it. So when all data has been transferred, the server still thinks the control connection is alive and sends the transfer confirmation reply over the control connection. Likewise, the client as well thinks the control connection is alive and waits for the reply from the server. But since the control connection got silently dropped, this reply never arrives, eventually causing a timeout.

In an attempt to solve this problem, the TCP specifications include a way to send keep-alive packets on otherwise idle TCP connections, to tell all involved parties that the connection is still alive and needed. However, the TCP specifications also make it very clear that these keep-alive packets should not be sent more often than once every two hours. Thus, with added tolerance for network latency, connections can stay idle for up to 2 hours and 4 minutes.

The problem is that many routers and firewalls drop connections that have been idle for less than 2 hours and 4 minutes. Such behavior is violating the TCP specifications, RFC 5382 makes this very clear. In other words, all routers and firewalls that are dropping idle connections too early are broken, they just cannot be used for long FTP transfers. Unfortunately manufacturers of consumer-grade router and firewall vendors do not care about specifications, all they care about is getting your money and thus only deliver barely working lowest quality junk.

To solve this problem you need to uninstall affected firewalls and replace the faulty routers with a quality one.

Setting up FileZilla Server with Windows Firewall [edit]

If you are having problems with setting up FileZilla Server to run behind Windows Firewall (specifically, it fails on "List" and the client receives a "Failed to receive directory listing" error), you must add the FileZilla Server application to Windows Firewall's Exceptions list. To do this, follow these steps:

1. Open Windows Firewall under Control Panel.

2. If using Vista, click "Change Settings"
3. Select the "Exceptions" tab.
4. Click "Add program..."
5. Do NOT select "FileZilla Server Interface" from the list, instead click on "Browse..."
6. Locate the directory you installed FileZilla Server to (normally "C:\Program Files\FileZilla Server\")
7. Double click or select "FileZilla server.exe" and press open (Once again, NOT "FileZilla Server Interface.exe")
8. Select "FileZilla server.exe" from the list and click "Ok"
9. Verify that "FileZilla server.exe" is added to the exceptions list and that it has a check mark in the box next to it
10. Press "Ok" to close the window

Passive mode should now work. If you are still having problems connecting (from another computer or outside the network) check your router settings or try to add the port number in the Windows Firewall settings located in the Exceptions tab.

See the Microsoft kb article 931130 about running FileZilla with the "Routing and Remote Access" or the "Application Layer Gateway" service enabled. http://support.microsoft.com/kb/931130

Navigation

- Main Page
- Community portal
- Recent changes
- Random page
- Help
- Donate

Search

Go Search

Toolbox

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link