Firewall considerations when using active and passive FTP.

Creation date: 23/03/2011        Last Review: 29/03/2011        Revision number: 2

Document type: Documentation    Security status: EXTERNAL

Summary

FTP is an unusual service in that it utilizes two ports, a 'data' port (typically port 20) and a 'command' or 'control' port (typically port 21). The confusion begins however, when we find that depending on the mode, the data port is not always on port 20.

Details

Active FTP

Step 1. The FTP client makes a TCP connection (SYN, SYN ACK, ACK) from a random unprivileged port (N > 1023. e.g. 1026 in our example) to the FTP server's command port 21. (This is the Control channel)

Then, the FTP client sends the PORT FTP command to port 21 of the FTP server. In the PORT command, the FTP client indicates which port he wants to use for the data connection (Typically, this is N+1, 1027 in our example)

Step 2. The FTP Server acknowledges the PORT command.
The FTP client starts listening on port negotiated in the PORT command (port 1027 in our example)

Step 3. The FTP server initiates a TCP connection from its local dataport (port 20) to the port negotiated in the PORT command (port 1027)
(This is the Data channel)

Step 4. Finally, the client sends an ACK back.
The main problem with active mode FTP is on the client side. The FTP client doesn't make the actual connection to the data port of the server, it simply tells the server what port it is listening on and the server connects back to the specified port on the client. From the client side firewall this appears to be an outside system initiating a connection to an internal client, something that is usually blocked.

From the server-side firewall's standpoint, to support active mode FTP the following communication channels need to be opened:

- FTP server's port 21 from anywhere (Client initiates connection)
- FTP server's port 21 to ports > 1023 (Server responds to client's control port)
- FTP server's port 20 to ports > 1023 (Server initiates data connection to client's data port)
- FTP server's port 20 from ports > 1023 (Client sends ACKs to server's data port)

**Passive FTP**

In order to resolve the issue of the server initiating the connection to the client a different method for FTP connections was developed. This is known as passive mode FTP, or PASV, after the command used by the client to tell the server it is in passive mode.

In passive mode FTP the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening an FTP connection, the client opens two random unprivileged ports locally (N > 1023 and N+1). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the PASV command. The result of this is that the server then opens a random unprivileged port (P > 1023) and sends the PORT P command back to the client. The client then initiates the connection from port N+1 to port P on the server to transfer data.

When drawn, a passive mode FTP connection looks like this:
Step 1. The FTP client makes a TCP connection from a random unprivileged port (N > 1023, e.g. 1026 in our example) to the FTP server's command port 21. Then, the FTP client sends the PASV.

Step 2. The FTP Server replies with the FTP PORT 2024 command, telling the client which port it is listening to for the data connection.

Step 3. The FTP client makes a TCP connection from a random unprivileged port (1027 in our example) to the port 2024 of the FTP Server (this port was negotiated in the PORT command) the initiates the data connection from its data port to the specified server data port. Finally, the server sends back an ACK in

Step 4 The FTP server acknowledges the connection to the FTP client's data port.

From the server-side firewall's standpoint, to support passive mode FTP the following communication channels need to be opened:

- FTP server's port 21 from anywhere (Client initiates connection)
- FTP server's port 21 to ports > 1023 (Server responds to client's control port)
- FTP server's ports > 1023 from anywhere (Client initiates data connection to random port specified by server)
- FTP server's ports > 1023 to remote ports > 1023 (Server sends ACKs (and data) to client's data port)

Configuration for passive ftp

With the massive popularity of the World Wide Web, many people prefer to use their web browser as an FTP client. Most browsers only support passive mode when accessing ftp:// URLs.


Configure the FTP service to only use a limited number of ports for passive mode FTP
1. In the IIS 7.0 Manager, in the Connections pane, click the top node for your server.
2. In the details pane, double-click FTP Firewall Support.
3. Enter the range of port numbers that you want the FTP service to use. For example, 41000-41099 allows the server to support 100 passive mode data connections simultaneously.
4. Enter the external IPv4 address of the firewall through which the data connections arrive.
5. In the Actions pane, click Apply to save your settings.

Afterwards do a portforwarding for the range (41000-41099) to the ftp-server.