Firewalls and FTP external IP address for PASV

Most firewalls (we'd say all the ones we know) have NAT/PAT capabilities, and many are able to perform a protocol-level inspection when the connection is not encrypted. SSH (and SFTP) are always encrypted, but FTP can be either encrypted or not; yet, theoretically, **protocol inspection should only prevent protocol-related attacks, not modify client requests or server responses.**

Yet, one customer with a perfectly configured instance of Syncplify Server! reported experiencing a **weird behavior**: FTPS/FTPES (encrypted) sessions were working perfectly, while plain FTP sessions were dropped upon every attempt to open a data connection to transfer files.

Now, theoretically, this doesn't make any sense, as the core engine for the FTP protocol is the same, and the TLS channel is layered on top of (or, more precisely, encapsulates) it. The only possible explanation was that something between the client and the server **was actively modifying the protocol**, and could obviously do so only when the FTP connection was performed in clear, with no TLS encryption.

In this particular case, a SonicWall firewall was **rewriting Syncplify Server!'s response to the PASV command** in order to modify the IP address and Port for the next incoming (requested) passive data connection.

Now, Syncplify Server! – as most FTP/S servers – allows the server's administrator to configure an "*external IP for PASV connections*" to be used specifically when running our server behind NAT/PAT. This allows the server to tell the client to which public IP:Port it should connect to initiate the data transfer connection. If the firewall rewrites such information and re-routes the data connection towards a different IP or Port, then Syncplify Server! would **not accept the new incoming data connection request, because it is – de facto – tampered or spoofed**.

If you have a firewall that acts like this (more like a reverse proxy, rather than just a simple firewall) removing the "*external IP for PASV connections*" from Syncplify Server!'s configuration **may fix the issue**, as it did in our example case. But please keep in mind that such a configuration setting is there for a reason, and if your firewall is behaving transparently it is necessary to use it when behind NAT/PAT.

Revision #1
Created 22 July 2023 16:36:43 by DevTeam
Updated 28 January 2024 16:52:13 by DevTeam