

# Technical Note

No. 11

06 January 2003



Algorithmic Research

10 Nevatim St., Kiryat Matalon  
Petach Tikva, Israel 49561  
Tel: +927-3-9279500  
Fax: 927-3-9230864  
<http://www.arx.com>

Product: Private Wire

Subject: Securing FTP with PW and Checkpoint's FW1

## Symptom:

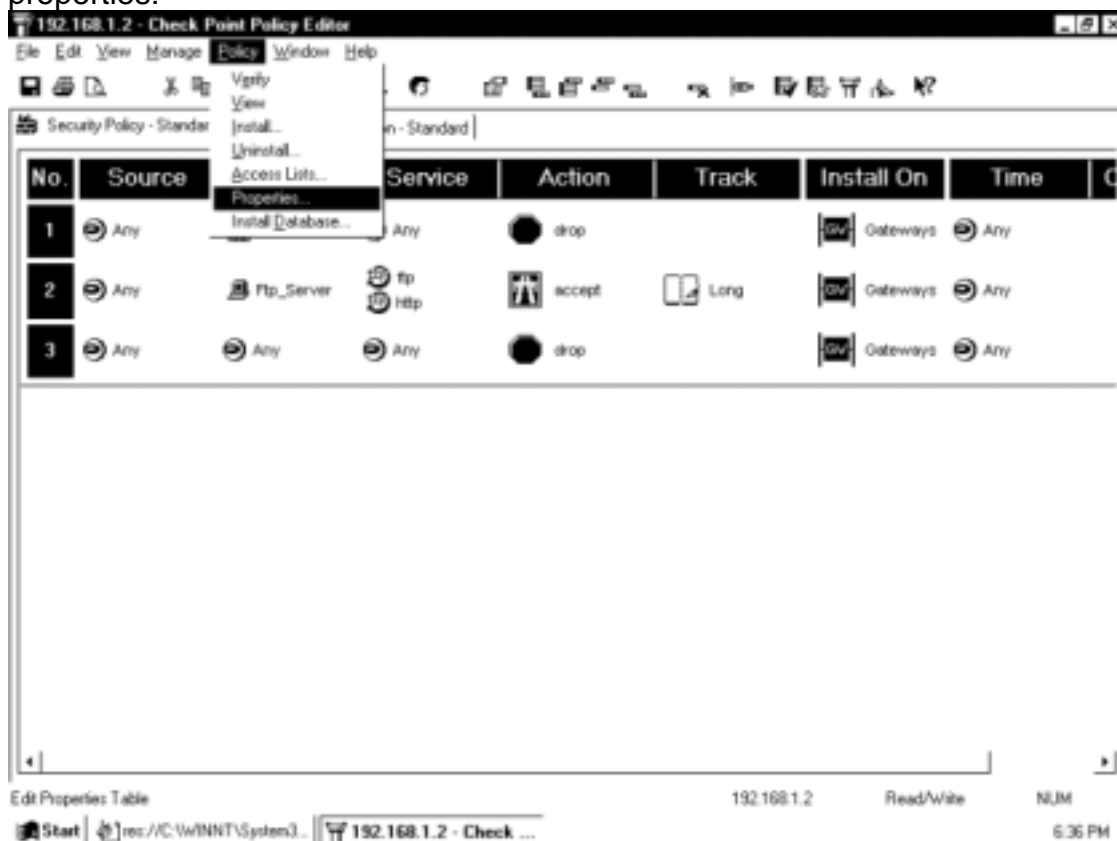
When securing FTP with PW through Checkpoint's FW1, errors occur when trying to perform FTP commands (list, get, put, etc.).

## Cause:

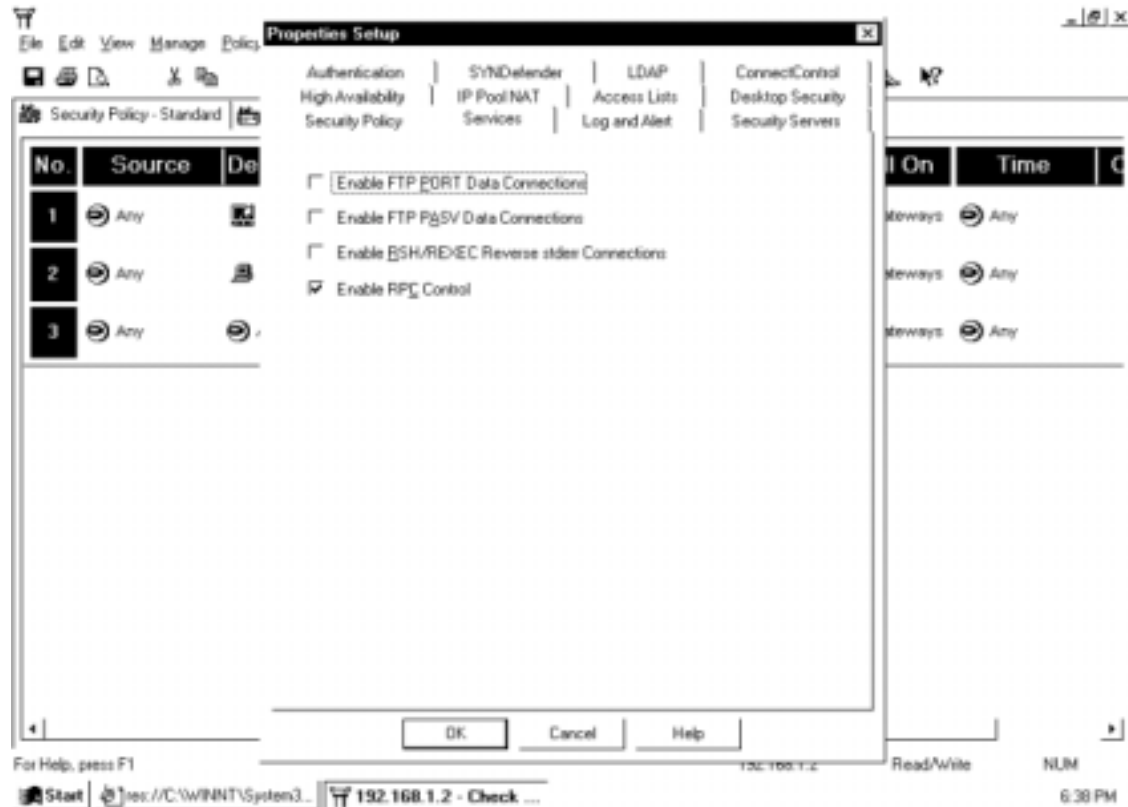
FW1 receives the secure data and blocks it when using the Checkpoint FTP module (the FTP module doesn't know how to handle the secure data).

## Solution:

In Checkpoint's policy editor go to "policy" menu and click properties:



Under “Security Policy” tab, uncheck “Enable FTP PORT Data Connections” and “Enable FTP PASV Data Connections”:



On Checkpoint’s Policy Editor set the same rules as in PW for securing FTP:

	Inter- face	Protocol	Source IP address	Source ports	Destination IP address	Service (Destination port)	Action	Log
1.	External	TCP	Any	1024 - 65535	ftp-server	21	Secure dest	None
2.	Internal	TCP	ftp-server	20	Any	1024 - 65535	Secure source	None
3.	External	TCP	Any	1024 - 65535	ftp-server	1024 - 65535	Secure dest	None

Rule 1 enables control connections.

Rule 2 enables data connections for an active FTP session. Note that the source port number 20, though widely used and accepted, is not standard. You therefore should refer to your FTP server's documentation to find the actual port number(s) used.

Rule 3 enables data connections for a passive FTP session.

If you want to allow only one type of data connection, either active or passive, but not both, use either rule 2 or 3, respectively.

AR Tech. Support