FTP Client Inspector

FTP Client Inspector Overview

Type	Inspector (passive)
Usage	Inspect
Instance Type	Multiton
Other Inspectors Required	`ftp_server`, `stream_tcp`
Enabled	`true`

File Transfer Protocol (FTP) is a network protocol used to transfer files between clients and servers over TCP/IP. Once a client and server establish a connection, the client issues commands to the server to upload files to or download files from the server, and interprets responses from the server.

The `ftp_client` inspector examines and normalizes responses on the FTP command channel.

Given an FTP command channel buffer, the `ftp_client` inspector interprets FTP response codes and messages. The `ftp_client` inspector enforces correctness of the parameters, determines when an FTP command connection is encrypted and when an FTP data channel is opened.

FTP Client Inspector Parameters

bounce

Specifies whether to check for FTP bounces by examining the host information in `ftp port` commands issued by the client. When `bounce` is `true`, if the host information in an `ftp port` command does not match the configured client IP address or host information , and rule 125:8 is enabled, the system generates an alert, and

in an inline deployment drops offending packets. This can be used to prevent FTP bounce attacks and permit FTP connections where the FTP data channel destination is different from the client.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

ignore_telnet_erase_cmds

Specifies whether to ignore the telnet escape sequences for the erase character (TNC EAC) and the erase line character (TNC EAL) when normalizing the FTP command channel. You should set this parameter to match how the FTP client handles telnet erase commands. Newer FTP clients typically ignore these telnet escape sequences, while legacy clients typically process them. When the `ignore_telnet_erase_cmds` parameter is `false`, the inspector uses rule 125:1 to generate alerts, and in an inline deployment, drop offending packets.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

max_resp_len

Specifies the maximum length for all response messages accepted by the client in bytes. If the message for an FTP response (everything after the 3 digit return code) exceeds that length, and rule 125:6 is enabled, the system generates an alert, and, in an inline deployments, drop offending packets. This is used to check for buffer overflow exploits within FTP clients.

Type: integer

Valid range: `0` to `4,294,967,295 (max32)`

Default value: `4,294,967,295`

telnet_cmds

Specifies whether to check for telnet commands on the FTP command channel. The presence of such commands could indicate an evasion attempt on the FTP command channel.

You can enable rule 125:1 to generate events for this parameter, and in an inline deployment, drop offending packets.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

FTP Client Inspector Rules

Enable the `ftp_client` inspector rules to generate events and, in an inline deployment, drop offending packets.

Table 1: FTP Client Inspector Rules

GID:SID	Rule Message
125:1	TELNET cmd on FTP command channel
125:6	FTP response message was too long
125:8	FTP bounce attempt

FTP Client Inspector Intrusion Rule Options

The `ftp_client` inspector does not have any intrusion rule options.