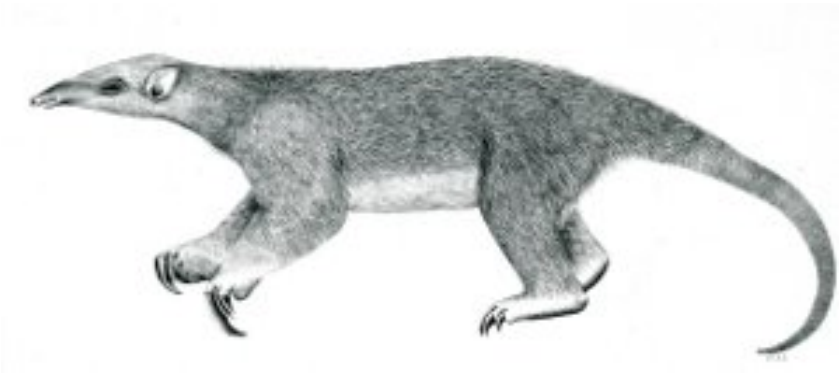
Tranalyzer2

tcpStates

TCP Connection Tracker



Tranalyzer Development Team

Contents

1 tcpStates

1.1 Description

The tcpStates plugin tracks the actual state of a TCP connection, by analyzing the flags set in the packet header. The plugin recognizes and reports non-compliant behavior.

1.2 Configuration Flags

None.

1.3 Flow File Output

The tcpStates plugin outputs the following columns:

Column	Type	Description
tcpStates	H8	TCP state machine anomalies

1.3.1 tcpStates

The tcpStates column is to be interpreted as follows:

tcpStates	Description
0x01	Malformed connection establishment
0x02	Malformed teardown
0x04	Malformed flags during established connection
0x08	Packets detected after teardown
0x10	Packets detected after reset
0x40	Reset from sender
0x80	Potential evil behavior (scan)

1.3.2 Flow Timeouts

The tcpStates plugin also changes the timeout values of a flow according to its recognized state:

State	Description	Timeout (seconds)
New	Three way handshake is encountered	120
Established	Connection established	610
Closing	Hosts are about to close the connection	120
Closed	Connection closed	10
Reset	Connection reset encountered by one of hosts	0.1

1.3.3 Differences to the Host TCP State Machines

The plugin state machine (Figure 1) and the state machines usually implemented in hosts differ in some cases. Major differences are caused by the benevolence of the plugin. For example, if a connection has not been established in a correct

way, the plugin treats the connection as established, but sets the *malformed connection establishment* flag. The reasons for this benevolence are the following:

- A flow might have been started before invocation of Tranalyzer2.
- A flow did not finish before Tranalyzer2 terminated.
- Tranalyzer2 did not detect every packet of a connection, for example due to a router misconfiguration.
- Flows from malicious programs may show suspicious behavior.
- Packets may be lost **after** being captured by Tranalyzer2 but **before** they reached the opposite host.

1.4 Plugin Report Output

The aggregated tcpStates anomalies is reported.

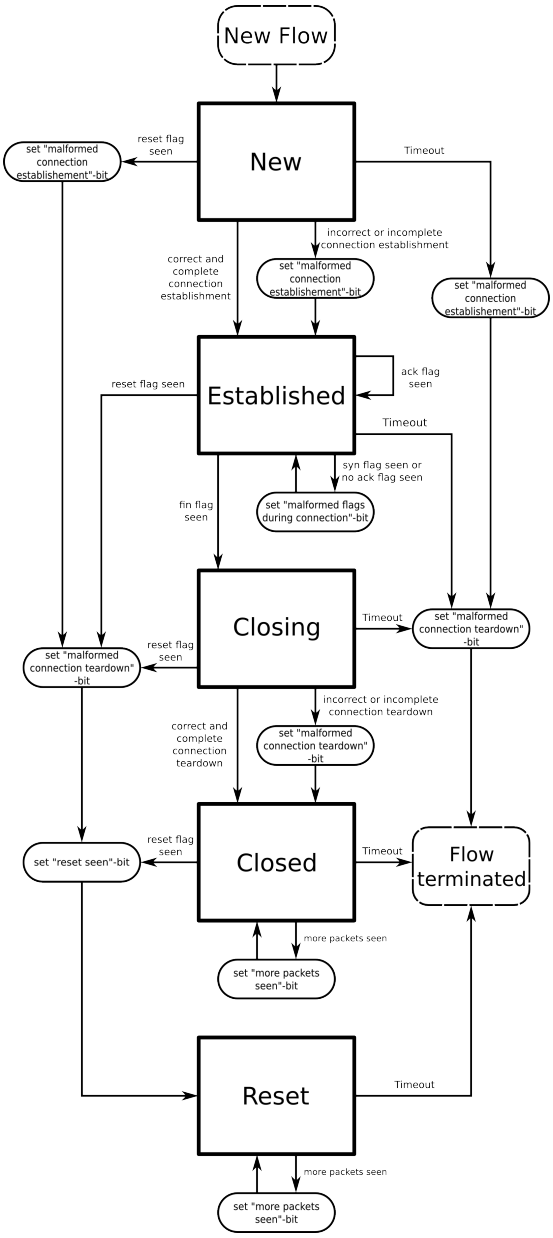


Figure 1: *State machine of the tcpState plugin*