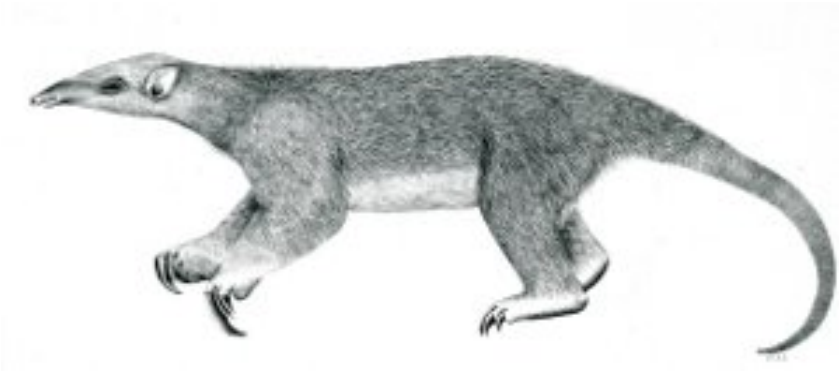
Tranalyzer2

connStat

Connection Statistics



Tranalyzer Development Team

Contents

Copyright © 2008–2019 by Tranalyzer Development Team

1 connStat

1.1 Description

The connStat plugin counts the connections between different IPs and ports per flow and during the pcap lifetime in order to produce an operational picture for anomaly detection.

1.2 Dependencies

1.2.1 Other Plugins

If the `basicFlow` plugin is loaded, then the country of the IPs with the most connections is displayed in the final report.

1.3 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description
`CS_HSDRM`	1	decrement IP counters when flows die
`CS_SDIPMAX`	1	0: number of src dst IP connnections 1: IP src dst connection with the highest count

1.4 Flow File Output

The connStat plugin outputs the following columns:

Column	Type	Description
`connSip`	U32	Number of unique source IPs
`connDip`	U32	Number of unique destination IPs
`connSipDip`	U32	Number of connections between source and destination IPs
`connSipDprt`	U32	Number of connections between source IP and destination port
`connF`	F	the f number, experimental: connSipDprt/connSip

1.5 Plugin Report Output

The following information is reported:

- Number of unique source IPs
- Number of unique destination IPs
- Number of unique source/destination IPs connections
- Max unique number of source IP / destination port connections
- IP prtcon/sdcon, prtcon/scon
- Source IP with the max connections
- Destination IP with max connections

Copyright © 2008–2019 by Tranalyzer Development Team