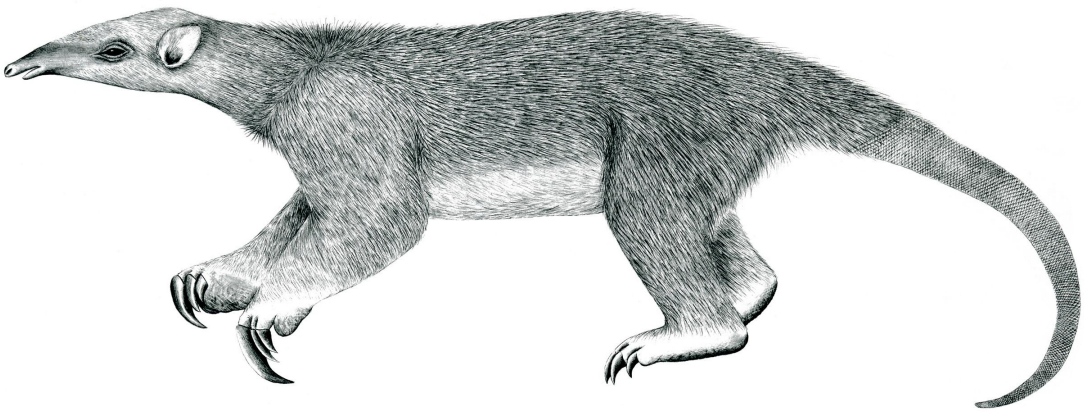
Tranalyzer2

connStat

Connection Statistics



Tranalyzer Development Team

Contents

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 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 connections, 1: IP src dst connection with the highest count
CS_MR_SPOOF	0	1: Activate MAC spoof detector
CS_PBNMAX	1	1: Report packet/byte biggest talker

1.3 Flow File Output

The connStat plugin outputs the following columns:

Column	Type	Description	Flags
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	
connMacSpf	U32	Number of MAC addresses per source IP	CS_MR_SPOOF=1
connF	F	The *f* number: connSipDprt/connSip [EXPERIMENTAL]	
connG	F	The *g* number: connSipDprt/connSipDip [EXPERIMENTAL]	
connNumPCnt	U64	Number of unique IP's source packet count	CS_PBNMAX=1
connNumBCnt	U64	Number of unique IP's source byte count	CS_PBNMAX=1

1.4 Monitoring Output

In monitoring mode, the connStat plugin outputs the following columns:

Column	Type	Description	Flags
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: connSipDprt/connSip [EXPERIMENTAL]	
connG	F	The *g* number: connSipDprt/connSipDip [EXPERIMENTAL]	

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 connF=connSipDprt/connSip
- IP connG=connSipDprt/connSipDip
- Source IP with max connections (`ANONYM_IP=0`)
- Destination IP with max connections (`ANONYM_IP=0`)
- Biggest L3 packets talker (`CS_PBNMAX=1`)
- Biggest L3 bytes talker (`CS_PBNMAX=1`)