Tranalyzer2
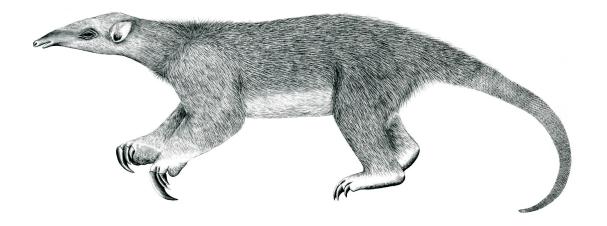
netflowSink

Output to any NetFlow collector

Tranalyzer Development Team

Contents

1 netflowSink

1.1 Description

This plugin is an interface of Tranalyzer to a NetFlow collector.

1.2 Dependencies

1.2.1 Other Plugins

This plugin requires the `basicFlow`, `basicStats` and `tcpFlags` plugins.
In addition, the `macRecorder` plugin is recommended, but optional.

1.3 Configuration Flags

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

Name	Default	Description
NF_SERVADD	"127.0.0.1"	Destination address
NF_DPORT	9995	Destination port
NF_SOCKTYPE	0	Socket type: 0: UDP; 1: TCP
NF_VER	9	NetFlow version 9 or 10 (IPFIX)
NF_NUM4FLWS	200	Max # of IPv4 flows in one message
NF_NUM6FLWS	100	Max # of IPv6 flows in one message

1.3.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (`ENVCNTRL>0`):

- `NF_NUM4FLWS`

- `NF_NUM6FLWS`

- `NF_SERVADD`

- `NF_DPORT`

1.4 Example

To collect T2 flow data with **nfcapd**, use the following command:

```
nfcapd -T all -B 1000000 -n wurst,127.0.0.1,.
```