MantisNet

CNFlow^{SM} - Advanced Flow Statistics for Cloud Native Observability
More granular flow records and statistics for network event correlation and attribution

WHY THIS MATTERS

More Detail: Legacy technologies, specifically IPFIX, NetFlow, JFlow and SFlow only provide basic network flow and traffic metrics. VPC mirroring and logs also provide standard metrics. CNFlow provides far more detailed, contextual, network communications insights.

Dynamic, Continuous, Real-Time: Predecessor technologies only provide a snapshot of network traffic performance and deliver status metrics over a predetermined time-frame. CNFlow includes more detailed and reliable forms of flow statistics of the functions, processes, and resulting events as they occur.

No Changes, No Additional Hardware and Unlimited Scale MantisNet CNFlow is vendor agnostic and doesn't require separate software and hardware to implement (no collector/exporter).

Observability & Control

Driven by eBPF, the MantisNet CVF provides infrastructure observability from the kernel level, providing unprecedented, real-time streaming visibility to the resources communicating on your network edge or core.

Advantages:
- k8s deployed - Daemonset or Replicaset
- No code changes required
- Event-driven, evoked on-demand
- Low overhead
- Decoupled from vendor/ hardware - generates agnostic telemetry without changing systems.

Containerized Visibility Fabric - CNFlow Function

MantisNet CNFlow (Cloud Native Flow) functionality, is a set of software probe and processing functions that allows you to instrument your infrastructure from the kernel, machine/node, process and container, up to the cluster, pod, and application. The MantisNet CNFlow engine leveraging eBPF operates at speed and scale; the lightweight, event-driven, sensor and processing functions are vendor, protocol and speed agnostic - they operate on-demand and deliver new forms of detailed, real-time, flow observability metrics and records (see table below) that can be correlated across the most complex public, private, or hybrid cloud infrastructure.
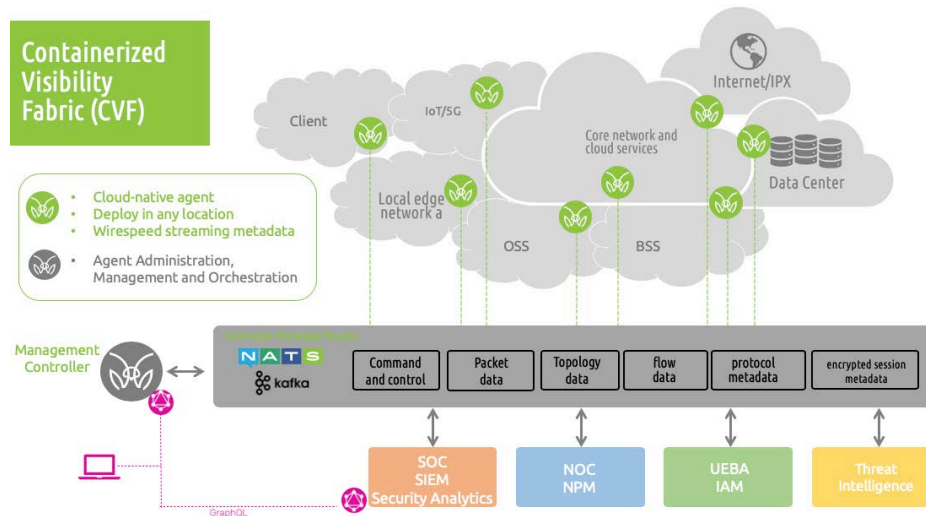
Get Standard Flow Metrics in Addition to CNFlow Advanced Metrics

Standard Flow Metrics

- Source Address
- Source Port
- Destination Port
- Destination Address
- Protocol
- Start Timestamp
- End Timestamp
- Packet Count
- Octet Count

CNFlow Advanced Flow Statistics

All Standard Flow Metrics	IP Version	Docker
State and Status	Segments Received	Pod Name
Lost Transmissions	Segments Transmitted	Pod Namespace
Bytes Retransmitted	Machine ID	Pod User ID
Out-of-order Packets Received	Container Name	Group ID
Receive Window	Namespace	Process ID
Delivery Rate	Container Image	Process User ID
Round Trip Time Variation	Container Unique ID	Flow Unique ID
Smoothed Round Trip Time	Packet Interval	Hostname

Enhanced Monitoring with Advanced Flow

Gain deeper insights into network communications and better correlate events with machines, applications and processes across nodes/clusters and containers/pods. MantisNet CNFlow is more open, detailed, reliable, flexible, scalable, and performant than other flow monitoring technologies. MantisNet CNFlow is built on a foundation of kernel level instrumentation combined with local in-node processing and an event driven architecture to support the next generation of development, operations and security applications regardless of protocol or speed. MantisNet CNFlow is cloud-native and supports streaming analytics using an open pub-sub message bus architecture and standards-based interfaces for deployment across public, private, or hybrid cloud environments and third-party integrations.

CNFlow

CNFlow is one of the many functions in the MantisNet CVF – a composable, containerized visibility fabric (CVF) – deployed as k8s for cloud-native and microservices environments with lightweight agents taking advantage of in-node processing. One can visualize the ephemeral topology of today's networks (hybrid/multi-cloud) and stream directly to analytic tools like Wireshark in a NetFlow format. We realize many organizations are structured for NetFlow and can provide that format for ingest.

Leveraging Cloud Native Flow (CNFlow)

SRE, Dev and Ops Teams

Use MantisNet CNFlow telemetry and correlate events to identify the cause of congestion, performance, and latency issues across complex environments down to the container, node and process. CNFlow metrics are more efficient and scalable because they are processed in-node and delivered continuously and in-real-time.

MantisNet CVF dynamic topology of container environments provides identification of inventory and drill down interface to stream network data (CNFlow, PCAP, protocol specific metadata, etc.) to desired analytic or management tool.

It operates as a daemon-set or replica set so it scales to provide a range of traffic visibility, processing and telemetry generation capabilities, regardless of the speed or volume of flows: under load, without new hardware - supporting better forms of application and network performance monitoring, complex traffic analysis, anomaly detection, troubleshooting, and remediation simple and economical for large, or complex, instances of cloud-native deployments.

Security and Compliance Teams

Get continuous, real-time visibility and the ability to uniquely correlate traffic flows with container-level events - enabling faster, more precise anomaly detection and remediation, providing immutable attribution to all network events. With CNFlow telemetry, teams can now more effectively allocate resources to focus on reducing the time-to-identify traffic of interest and ultimately resolve security and policy violations more quickly and efficiently.

Analysts and Data Scientists

MantisNet CNFlow operation and the resulting metadata is independent of the network protocol, vendor, or speed - meaning it can detect events regardless of scale, across the most complex enterprise, 5G / IoT / telecommunications applications – from the core to the edge. CNFlow telemetry includes advanced indexing data structures that allow for better event correlation and anomaly detection at speed and scale, regardless of the protocol. Furthermore, CNFlow metadata (as with all MantisNet CVF telemetry) can be natively streamed into event-driven streaming analytic platforms, or into (data-at-rest) storage repositories for follow-on analytics or forensic evaluation.
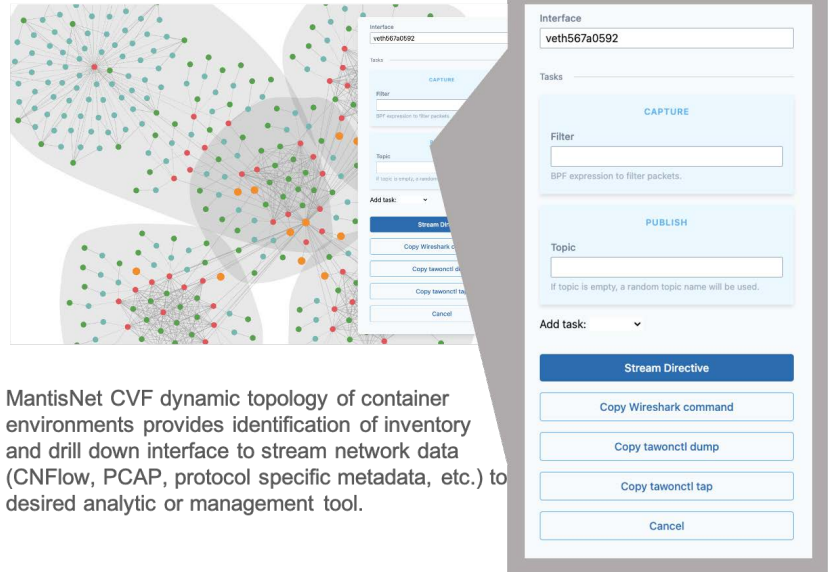
Cloud Network Planning, Architecture and Development Teams

MantisNet CNFlow telemetry, combined with other MantisNet CVF functions also serves Planning, and Development teams challenged with managing, planning for, and monitoring cloud-native infrastructure. MantisNet CNFlow telemetry provides continuous event-driven real-time monitoring to help better understand utilization and improve resource efficiencies by supporting both the latest generation of event-driven real-time streaming (AI and ML enabled) workflows as well as legacy data-at-rest based provisioning and monitoring solutions to monitor the performance and behavior of the infrastructure for changes, trends or anomalies over longer timeframes and/or as new demands arise.

ABOUT MANTISNET

MantisNet solutions provide organizations the real-time network monitoring and processing solutions they need. MantisNet's advanced technology enables organizations to better monitor and manage network traffic as compared to legacy hardware and software solutions. *For more information, visit www.MantisNet.com*

MantisNet

11160 C1 SOUTH LAKES DRIVE, SUITE 190 RESTON, VA 20191

571.306.1234
INFO@MANTISNET.COM

CVF-ACF-DS-02-JAN21