Progress® | Flowmon

Flowmon Probe

Flowmon Probe is the most powerful flow data exporter on the market. Where data exported from active network devices is not sufficient for user experience monitoring, network troubleshooting and threat detection, the Probe generates data down to application level and measures performance.

Key features and benefits

Provides deeper visibility that uncovers problems impacting user experience rather than just the red/green status information of server availability.

Reduction of Information Noise

Flowmon Probe collects network data and pre-filters it for relevant information, allowing for clearer analysis and visualization while also saving capacity and reducing investigation time.

Deployable Anywhere

No matter what type of network, a Flowmon Probe can be deployed anywhere without any impact on network traffic from 10 Mbps to 100 Gbps. As a virtual appliance, it can be deployed in virtual environments such as VMware, Hyper-V or OpenStack KVM or as a cloud application in AWS, Azure and Google Cloud.

Non-intrusive

The Probe connects passively through a SPAN port or network TAP and therefore represents no potential point of failure or hindrance. It is transparent from the L2/L3 perspective. In addition, the Probe supports remote monitoring sessions via GRE, ERSPAN or VxLAN.

Statistics from All Network Layers

Probes natively collect L2–L4 information on communication IPs, protocols, server response time, round trip time, jitter, and more. Flowmon's IPFIX extension provides additional L7 data, such as hostnames, URLs, browser information for HTTP/S protocols and other fields for protocols such as DNS, DHCP, SQL, SMTP, or Samba/CIFS.

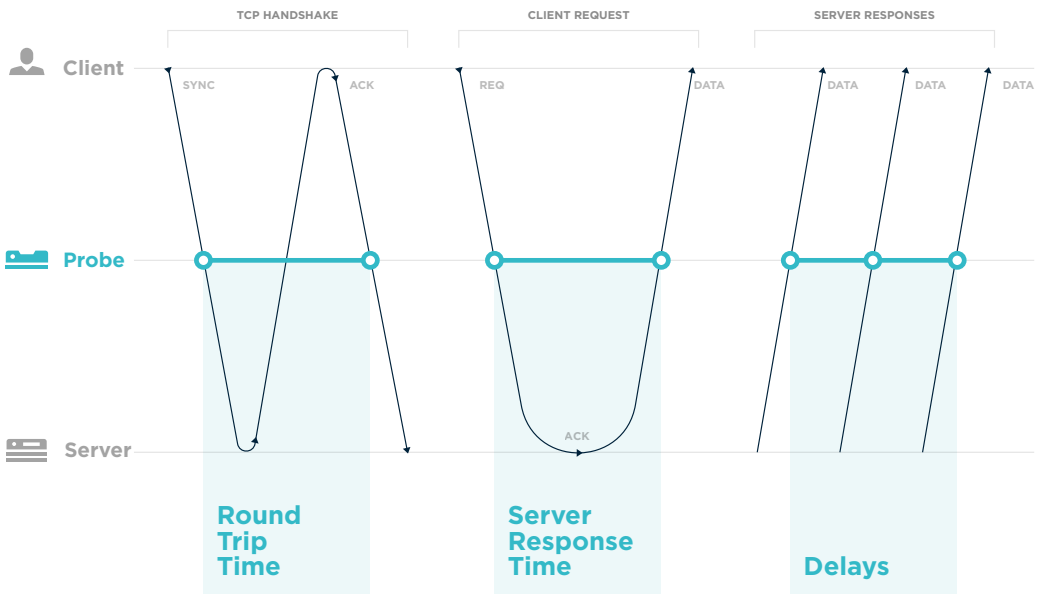
Scalability

A single Flowmon Probe can provide everything needed to monitor a smaller network, or combine with a Collector to cover the most complex, large distributed networks.

Use Cases

Network Performance Monitoring

As a standalone device with monitoring and packet capture capabilities, Flowmon Probe can help resolve up to 95% of all operational issues in the network and provide insight into its performance.



Troubleshooting and Forensics

Flowmon tracks individual user interactions with applications to provide an end-to-end understanding of the performance of the entire digital environment. Statistics, as well as raw packet data, are stored without aggregation or sampling for later use in forensic analysis.

Capacity planning

Flowmon provides IT teams with the necessary network transparency and predictability so that they can accommodate business-driven initiatives in modern digital environments and translate business decisions into straightforward operational requirements. They will transform from reactive operations to a proactive enabler of company success.

Cloud monitoring

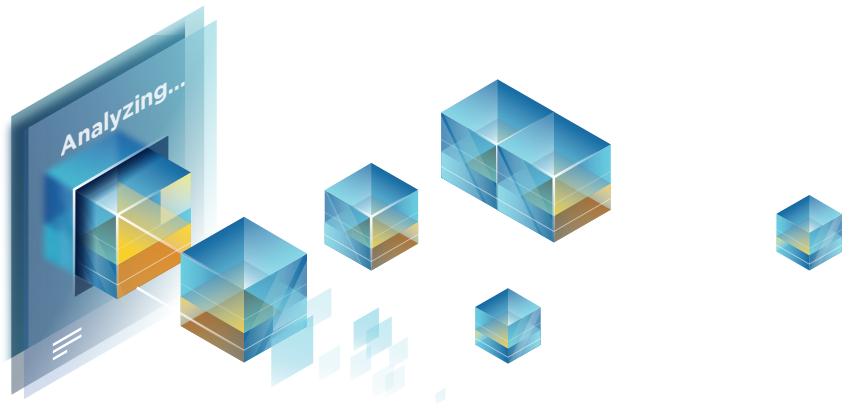
Flowmon tracks interactions between users and applications by analyzing network traffic, and reveals bottlenecks anywhere along the delivery chain - whether they fall within the scope of the user's responsibility or the service provider's.

Application recognition

Flowmon reports on the use of applications by analyzing L7 packets and exporting Network-Based Application Recognition (NBAR2) name or provides information on the source or destination of network traffic with the Autonomous System (AS) number.

Encrypted Traffic Analysis

Flowmon's encrypted traffic analysis collects network traffic metadata in the IPFIX format using Probes and enriches it with TLS protocol information (among others). This provides a wealth of information about the traffic and allows for the identification of out-of-date SSL certificates, policy non-compliant certificates, encryption strength and old TLS versions that may contain faults or vulnerabilities.



Features

The Key to Network Traffic Monitoring

Flowmon Probe exports network and application telemetry in the form of flow data based on raw packets and provides traffic statistics and metadata on all network layers.

L2

Probes decapsulate traffic to truly monitor the actual user-application conversation rather than the tunnel itself. This is available for all major protocols including GRE and OTV. This level of visibility is applicable even in MPLS networks to see per-tenant traffic as well as in VLAN segmented network.

L3/4

Standard NetFlow fields such as IP, port or protocol as well as advanced proprietary measurements such as Network Performance Monitoring Metrics, VxLAN visibility useful in remote monitoring e.g. in the cloud (in addition to L2 options such as GRE or ERSPAN), or ASN analysis.

L7

Provides a deeper understanding of application functionality for most common protocols ranging from HTTP, working even with HTTPS, SQL, DNS/DHCP, VoIP, Samba, email, etc.

Integrations

There are limitless possibilities to integrate the Probe with complementary tools and platforms. It can export flow data to different targets in multiple formats; e.g. send IPFIX to Flowmon Collector, NetFlow v9 to a SIEM system, or NetFlow v5 to an older legacy system. Network logging via syslog is an option for platforms that do not ingest flow data. It maximizes the investment into network infrastructure equipment from a variety of vendors by doubling their use as a source of telemetry data.