Feature Brief

FabricVUE Traffic Analyzer

Challenges

In a typical network deployment, customers use a variety of monitoring appliances to analyze Application Performance (APM), Network Performance (NPM) and Security (IDS, Forensics, DLP etc.) vulnerabilities. But how many monitoring appliance results does the NetOps or SecOps administrator have to examine to identify issues? Could they use a first-level dashboard to identify traffic patterns before taking any action?

The Gigamon Solution

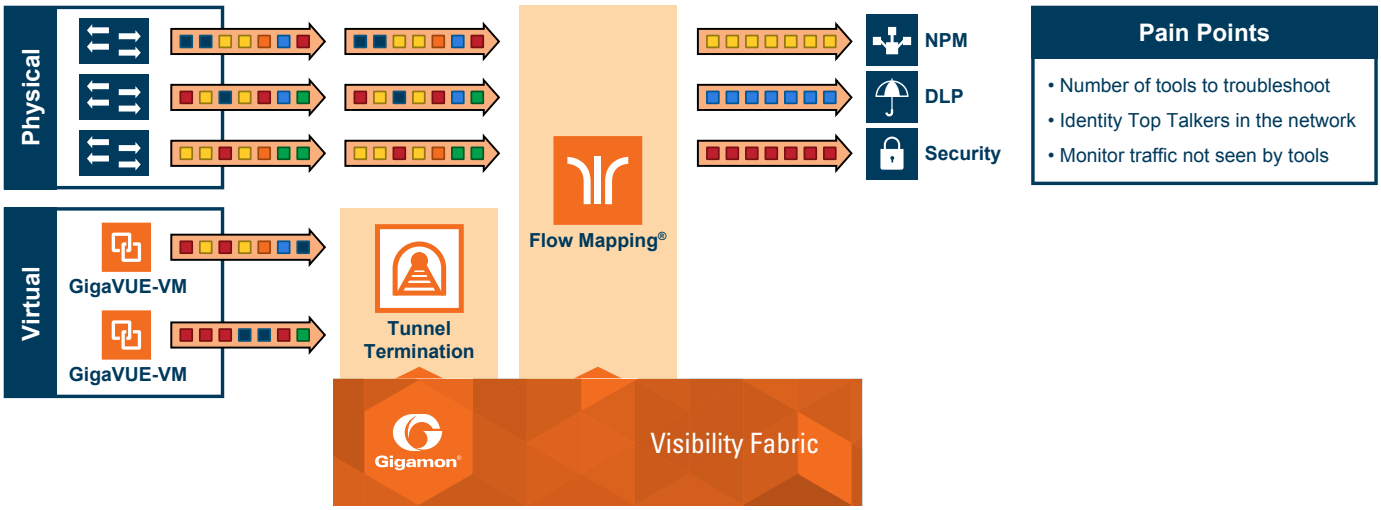
FabricVUE® Traffic Analyzer is an add-on licensable application for GigaVUE-FM that provides fabric-centric visualization of network traffic traversing the Visibility Fabric™ and the GigaSECURE® Security Delivery Platform. This allows SecOps and NetOps administrators to use GigaVUE-FM as a first-level dashboard to track the following Top-N metrics.

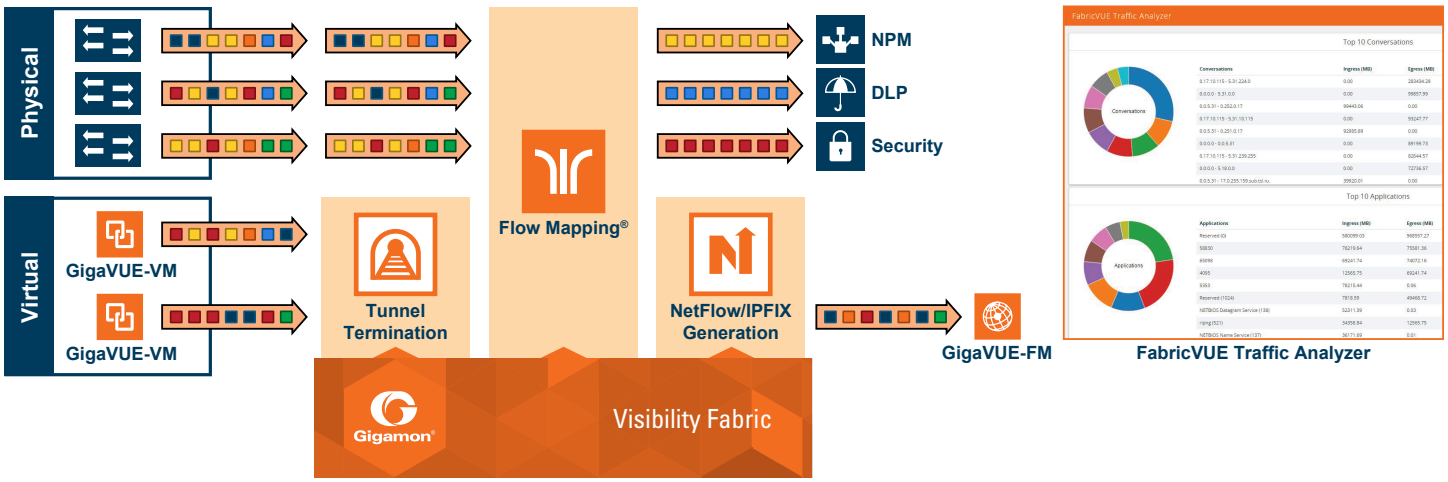
- Conversations—Between IP addresses or hosts
- Applications—Web, DB, Exchange etc.
- End Points—IP Addresses or Hosts that get the most traffic
- Protocols—TCP, UDP, SMTP etc.
- URLs—Web or Application URLs accessed by end-points
- HTTP Response Codes—Detect possible server compromise with redirects or DDoS attacks if server unavailable
- Production Neighbors—Network end points using CDP/LLDP discovery

These measures can be used by the operators to identify any suspicious or anomalous activity within the network. For example, if a certain end point is receiving more than the normal amount of traffic over a period of time, the SecOps team may analyze the traffic further for security violations.

FabricVUE Traffic Analyzer uses high-fidelity NetFlow/IPFIX records with context-aware extensions from GigaVUE® Visibility Fabric nodes to collect and measure this traffic to augment the monitoring infrastructure for the following use cases.

- Identify traffic that is being filtered out of the monitoring appliances
- Detect hot spots within new traffic sources that should be forwarded to the monitoring appliances





After identifying traffic hotspots within GigaVUE-FM, operators may

- Perform a deeper analysis in the monitoring/security appliance
- Add the suspicious traffic as a policy/rule in the Flow Mapping® engine that can then be forwarded to the monitoring appliance for packet capture and deeper analysis

Key Use Cases

- Provides indicators for SecOps/NetOps administrators who may want to conduct deeper analysis in the security/monitoring appliances
- Gives visualization of network traffic patterns measured using high-fidelity NetFlow/IPFIX flow records
- SecOps teams can detect possible server compromises or DDOS attacks with HTTP Response codes

Key Benefits

- Augment the organization's security and monitoring infrastructure with a top level view of traffic patterns
- Measure traffic that is not being filtered or forwarded to the monitoring appliances
- Identify and trend traffic patterns for new sources before forwarding to the right monitoring appliance

About Gigamon

Gigamon® solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies. For more information about the Gigamon Unified Visibility Fabric™ visit: **www.gigamon.com**

3174-02 12/15

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com