savvius™ | TECH BRIEF

How Packet-Based Analytics Complements NetFlow

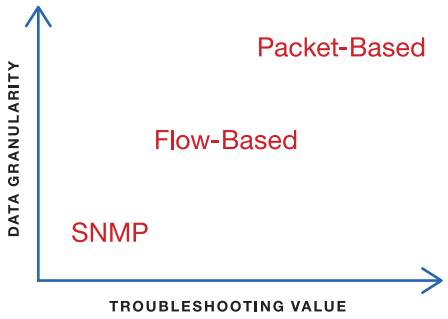
Although traditional NetFlow-based network monitoring tools have given NetOps teams valuable insight into network utilization and long-term trend analysis and capacity planning for many years, they do not have the precision of more advanced packet-based analytics tools. NetFlow simply wasn't designed with application performance, latency, TCP/IP or VoIP problems in mind. For that reason, packet-based tools are an ideal — and easily implemented — complement to NetFlow.

The Evolution of Network Monitoring Technologies

In the early days of large-scale network deployments, some of the first monitoring tools relied on Simple Network Management Protocol, or SNMP, which predates even NetFlow. SNMP was used to assess the status of network-connected devices and provide fundamental information about network infrastructure.

SNMP was followed by NetFlow, which is able to provide an additional layer of conversational information about the condition of the network and the devices or appliances that are operating on it. Compared with SNMP, NetFlow offers greater precision, with 'polling' intervals of approximately one second compared to a minute or longer for SNMP. This makes NetFlow more useful when trying to ascertain the general health of a network.

Evolution of Technologies



As shown in the chart below, packet-based network monitoring tools deliver a magnitude of data granularity and troubleshooting value that far exceed NetFlow. Much of this can be attributed to the tools' direct access to raw, unabbreviated and un-compiled data. Because these tools analyze the contents of the original packets, they are not only precise, they also enable much faster response times, which can be as short as several nanoseconds.

Using packet-based analytics to complement NetFlow

NetFlow

Provides wide network overview of where traffic is occurring. Ideal for:

- Capacity planning
- Trend analysis
- Utilization
- Conversational information

Packet Analysis

Precision down to the nanosecond for root-cause analysis. Ideal when monitoring:

- TCP/IP
- Application performance
- Network latency
- VoIP

NetFlow data is typically generated by Layer 3 network devices such as routers and firewalls. This data can be used to generate high-level information about traffic volumes between specific devices on the network. In practice, if volumes unexpectedly spike or drop, the NetOps team may first use NetFlow data to provide a general sense of where the problem lies. Once they have isolated the possible culprit, they can turn to packet-based solutions for more detailed network diagnostics. Rather than simply knowing where a problem is occurring, the packet-based approach allows the NetOps team to assign quantitative and qualitative metrics to network performance. Not only are packet-based analytics 100 percent accurate, these tools support monitoring and troubleshooting simultaneously, while not placing any additional burden on the network.

Finding root cause as quickly as possible is key when troubleshooting network performance. NetFlow-based tools provide valuable information about where traffic is being generated up to Layer 3. That conversational information is useful when scaling balancers and firewalls, and when confirming that those policies are working correctly. Packet analysis becomes useful in situations where the original packet data can be used to monitor and troubleshoot the network. It can be used to determine how well computers are communicating over the network, how long application response time is, how network latency compares to application latency, whether VoIP is operating well and prioritized correctly, and more.

When a NetOps team gets a trouble ticket regarding a slow network or a critical business application that isn't operating correctly, NetFlow would reveal the volume of traffic going between the client and the server or details about the ports. This limited information cannot provide a definitive solution.

Conversely, packet-based analysis fills the gap to reveal vital information about network performance and application response. These tools can easily compare network latency with application latency, and they can be used to evaluate the performance of VoIP over the network and help network engineers ensure that applications are prioritized correctly.

Using the combined strengths of both packet-based network analytics and NetFlow, a NetOps team is equipped to troubleshoot and solve a wide variety of common network issues, such as:

- Is the issue being caused by the network or the application?
- Is the issue isolated to a single user, a single server, or the entire network?
- Are critical applications using network resources efficiently?
- Is my network correctly configured for unified communications, and are unified communications co-existing with other network transactions?
- Are critical functions such as user authentication, failing due to protocol issues?

Summary

NetFlow continues to have an important role in the network monitoring hierarchy, but as network complexity rises, its limitations become more apparent. By deploying packet-based analytics tools to complement NetFlow, network professionals gain deeper insight into TCP/IP problems, application performance issues, network latency, VoIP problems and a host of other issues. This information helps ensure that network performance can be maintained while enabling rapid troubleshooting and Mean Time To Resolution (MTTR) for any unexpected issues, anywhere on the network.