

Network Traffic Analysis Equality with PacketTrap's ptFlow

Event

On February 5, PacketTrap announced the 3.0 release of their Perspective management platform, including a raft of new features and capabilities. Among those is a highly innovative feature that could make a big difference for network managers seeking to establish application-aware visibility across their managed domains. PacketTrap's ptFlow features enable operators to gather NetFlow records from devices that do not natively support NetFlow, and then to add those records into Perspective's Traffic Analysis solution for better business-aware network monitoring.

Background and Context

As the discipline of network management and the role of network operations evolve with the organizations they serve, it is incumbent upon network engineers and operators to understand not only what makes up the network, but also what the network is delivering. The vast majority of help desk calls come in due to lack of expected application performance, not specific network issues. And when those calls come in you need to know things like: How are those applications utilizing the network? What else is happening on those same links? Are there any unexpected applications being used, perhaps to the detriment of those upon which my organization is depending? To answer these questions, operations must become aware of the network view of application activity.

There are a few major choices for achieving such visibility. You can use packet capturing tools that give you snapshots, or packet-based real-time monitoring tools that can require a substantial investment in dedicated instrumentation. Most organizations are looking at a third option that offers both sustained monitoring as well as a more compelling cost point – flow records. Flow records are issued by network devices and chronicle who is using the network, which application they are using, and how much traffic they are generating. There are several alternatives and variants of flow record technologies, but the dominant version is NetFlow, which has achieved de facto standard status, and which is the basis for a true standard in IPFIX.

PacketTrap's ptFlow delivers NetFlow capabilities for any IP-connected device

As you design a NetFlow monitoring architecture and strategy, you will likely encounter one other major challenge. What to do when the devices in your network don't support NetFlow? There are only a few options that have traditionally been available. First, you could upgrade the device to a make or version that supports NetFlow, or perhaps you could add another hardware device in-line (such as a WAN

optimization appliance) that generates NetFlow records. Or you could deploy packet-based instrumentation, which usually requires dedicated hardware as well. But now there is a third option – ptFlow. PacketTrap's ptFlow delivers NetFlow capabilities for any IP-connected device, by means of an innovative application of packet monitoring software to generate flow records in NetFlow v5 format, and bringing application visibility to places where it had not been possible or practical before.

ptFlow is deployed by utilizing resident Perspective Agents or existing deployments of Perspective Server software to watch a copy of the packet flow stream coming into or from the device of interest. Deployment scenarios can fit local or remote devices, and network nodes or servers. An essential element in all of these scenarios is access to a copy of the packet stream traveling to or through the device of interest, whether by using port mirroring or use of a hub or tap. In many cases, an additional NIC will also be needed for the system where the Perspective software is running. The Perspective software parses those packet streams and creates ptFlow records, which are then available for monitoring and reporting via Perspective's Traffic Analysis module.

One of the more interesting capabilities that ptFlow provides when applied to servers is the ability to reveal traffic for one or more virtual machines that might be running on any given physical system. Installed within a VM instance, ptFlow will reveal the traffic generated by just that VM. Installed outside of an individual VM, ptFlow can reveal traffic by each and every VM active on that physical server. For operators struggling with how to integrate management and visibility of virtual servers, this represents a very effective means of getting both the big picture of operational activity as well as the details needed to help troubleshoot performance issues as they arise.

Key Ramifications

First and foremost, ptFlow will be bringing application traffic visibility to places where this important source of operational intelligence was not available before. Better visibility across the delivery infrastructure means better control, translating into better planning capabilities, faster recognition of problems, shorter troubleshooting times, and thus happier end users and, ultimately, happier networking professionals.

ptFlow will be bringing application traffic visibility to places where this important source of operational intelligence was not available before.

One of the side benefits of deploying ptFlow will be the opportunity to realize an extended lifespan out of existing infrastructure. By generating better operational metrics from devices that were incapable of providing this info, expensive node upgrades or replacements, as well as under-informed network capacity expansions could be delayed, in some cases indefinitely. While everything has a fixed total lifetime, network operators will appreciate this additional flexibility in deciding when the time is right.

Finally, this new feature offering substantially expands the value received by existing adopters of the PacketTrap Perspective product platform. By providing ptFlow as an integral feature of the Perspective Network Traffic Analysis module, operations teams can achieve this new level of visibility at no incremental cost in terms of software, and low cost in terms of hardware (usually just a new NIC).

EMA Perspective

In the view of Enterprise Management Associates (EMA), application awareness is the key to enlightenment, at least where network management is concerned. Yes, you need rock solid network element monitoring tools. Yes you need configuration tools that help you get things done fast. And yes, you need planning tools that help you figure out how you will be supporting the next set of business challenges your organization is facing. But unless you can see how IT end users are utilizing the infrastructure and connectivity that you are providing them, you're only dealing with a part of the picture. Applications and the ability to see them are key in transforming from device-centric to service-centric operations. PacketTrap has embraced application awareness through its support of NetFlow, and the addition of ptFlow adds an intriguing new dimension of possibility.

The ability for this approach to shine a light upon virtual machine activity adds another compelling and future-savvy dimension.

Also important is flexibility. With many different potential deployment scenarios supported, the ptFlow features offer significant flexibility to establish visibility where it makes sense and using whatever existing Perspective components have already been deployed. Adding to this, the ability to get NetFlow not only from network devices, but from key servers of interest, is very helpful for ops teams that must cover both systems and networks. The ability for this approach to shine a light upon virtual machine activity adds another compelling and future-savvy dimension.

EMA believes that PacketTrap's ptFlow initiative is unique in the industry, both from a technology perspective as well as in the way that it can be flexibly deployed to complement existing application-aware data sources. While the feature set is clearly designed as an integral component within their Perspective solution, it does create NetFlow v5 records, and thus we believe that it may also be of interest to organizations that are using other products for network and NetFlow monitoring, as a means to achieve pervasive visibility across diverse and distributed networks.