Leveraging a Big Data Model in the Network Monitoring Domain

White Paper

Introduction

Network monitoring is on the cusp of a radical shift away from the prevailing paradigm of appliance-only deployments. The scale of current networks and the associated growing data generation (upwards of 300x by 2020),[1] as well as the increasing need for visibility are driving a move to a big data model that leverages a decoupled hardware/software framework, large aggregate data stores, and a shared approach to servicing network monitoring, security, forensics, and compliance requirements for network visibility.

Architectures are evolving rapidly. Networks are moving towards software orchestration and virtualization of networking functions, catching up with the changes that virtualized compute and cost-effective, high performance storage systems. A similar evolution has been unfolding within network monitoring.

Beginning with the advent of network aggregation TAPs occurring about a decade ago, a redistribution of functions between the network monitoring appliances and the network TAPs has simplified the task of scaling out management networks with the network TAPs taking on a greater portion of the peripheral, hardware-centric functions that allowed the monitoring appliances to operate more efficiently to their core capabilities.

Network TAPs eventually matured into a new class of products called network packet brokers. Network TAPs, have persisted, but primarily as gateways to network packet brokers, which have assumed a wide range of packet pre-processing capabilities designed to tailor network traffic to the requirements of the monitoring and security appliances.

The emergence of this visibility plane, a distributed, dynamic layer that supplants older, silo-based systems or point-to-point centralization schemes and leverages the collective range and intelligence of a system of network packet brokers, laid the foundation within the last few years for the modern monitoring model, in which the monitoring and security tools—both out-of-band and inline—have in effect been "decoupled" from the network. This decoupling has increased the range of visibility to the tools and their adaptation to network changes, although the tools themselves have remained much as they were since their introduction—tightly integrated hardware/software packages.

While vertically integrated monitoring tools, combining capture, storage, processing, and analysis, are critical to managing networks today, they can pose challenges when scaling out without network packet brokers. Addressing these challenges requires the visibility plane to act as a proxy for the tools, capturing, mediating, and delivering traffic on their behalf.

This whitepaper will examine the historical context for the current state of network monitoring and the shifts in IT that are eroding the long-term viability of the existing model. It will further suggest the "network visibility plane" as a facilitator of a new monitoring paradigm — a big data model — in which network data is handled as a "big data" asset, using tools and techniques that allow it to be leveraged on a larger scale with greater efficiency and agility; not strictly under the purview of operations, but joined within the organization's data store for business intelligence extraction and holistic situational awareness.

In sum, the network visibility plane should facilitate the following changes in network monitoring for the purposes of promoting disaggregation of analytics tool functions for long term monitoring sustainability and flexibility:

Process network data where it occurs – there is certainly value in aggregating data for processing — big data deployments have borne this out; however, particularly for network data, preprocessing should be done early on and locally, prior to any offload to tools or big data systems. NPBs already perform hardware based processing of network data, and they should be increasingly relied on to sift through data for what's actionable. Capabilities such as deduplication, filtering, and others can provide this refinement.

Not only does this produce better data for analytics processing, it delivers it faster and prevents later processing overload.

Provide fungible ("open") data in a variety of formats, useable by a variety of platforms – move beyond the brokering of just "raw" packets, which require delivery to and processing by specialized tools. Supplement raw packet delivery with more widely digestible preprocessed data that can be acted on directly by users and applications. Examples of this data include PCAP files and premade metadata or index files, which contain flow information, and all of which can be consumed by a (sufficiently specified) generic server.

Providing and refining these capabilities will help organizations monitor the network data deluge using disruptive methods that are beginning to be leveraged elsewhere in the IT landscape, such as big data frameworks, COTs, and NFV.

What is big data?

Big data is a nebulous term that can take on different meanings or applications depending on context. Even in IT, where big data deployments are planned and implemented, big data is variously referred to as the "raw" source data, the extracted data, or the process that bridges these two.

Most often to those directly involved in the planning and execution of large scale data handling projects, big data is synonymous with the technologies that enable large aggregates of disparate data

[1] "The Digital Universe in 2020," IDC, 2012.

to be collected and parsed on an ostensibly shared platform. These technologies — or data handling frameworks — have done away with many of the limitations of using traditional SQL databases. These technologies include distributed computing frameworks, such as Hadoop, which is batch oriented, and Spark, which is stream based, as well as others, such as MongoDB and Cassandra.

These technologies are relevant to the monitoring architecture proposed in this paper; however, in terms of explication, they are subordinate to the overarching ideas and opportunities implicit in the notion of big data, namely data consolidation, resource sharing, processing efficiency, and the usage of platform independent hardware.

Gartner defines "big data" as "high-volume, high-velocity and high-variety information assets" — the ubiquitous 3Vs — "that demand cost-effective, innovative forms of information processing for enhanced insight and decision making." The latter portion of this definition is most interesting, because "big data" is not solely or even necessarily about a lot of data. Donald Feinberg of Gartner even goes so far as to note that "high volume, high velocity and high variety data has existed for many years. What are new are low-cost solutions and tools to process, manage and analyze this data in an efficient manner." It's the nature of the processing model that's the differentiator and separates "big data" from previous ways of extracting information and value from datasets.[2]

Simply stated, big data is comprised of information assets, often overwhelming in nature, that truly require a new data processing model in order to be fully leveraged and to scale.

Is big data relevant to network monitoring and security?

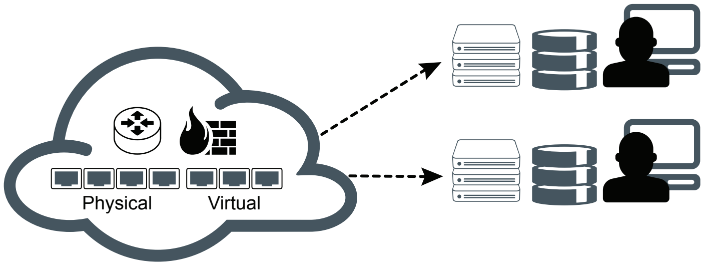
Network monitoring has long occupied a niche within networking, serving the needs of the network operations and network security groups, ensuring performance, service delivery, risk mitigation, data protection, and compliance. Given the large number of network processing and packet analysis solutions available and covering a variety of use cases, many of them highly specialized, it's reasonable to question the need to apply new processing frameworks to network data or to include network data in a general big data system.

Volume is one element of network data that is presenting a challenge to existing network monitoring norms, particularly for storage intensive applications. The volume of data flowing over today's networks is growing at a tremendous rate. According to IDC, networks are producing over 3.5 Exabytes of data each month, and that number is expected to grow 300x over the next 5 years.[3] These numbers, substantial as they are, are not surprising given the expanding global digital lifestyle, the so called "internet of things," and the resultant proliferation of data.

Although volume creates a substantial network monitoring pressure, it's not the only challenge. The nature of network data is changing as well:

- More network data is occurring in virtualized environments, and as virtualization infrastructure drives compute costs down and spinning up workloads that generate network traffic becomes increasingly automated, the cost of producing traffic approaches zero. Yet the cost of managing and securing the networks that carry this traffic is rising.
- Network data complexity is increasing as the number of services delivered over the network grows, changing traffic payloads. Analytics tools have become more specialized in response to this complexity — increasing the number of toolsets required to fully monitor network traffic.
- Organizations are migrating to higher velocity networks of 40Gbps and 100Gbps, requiring analytics tools to natively keep pace (an unlikely possibility) or use network packet brokers to preprocess the traffic into manageable streams.

Purely from a characteristics standpoint, network data is a "big data ready" problem. It possesses the 3Vs of big data (volume, velocity, variety) in extreme degrees. To understand why current monitoring solutions fall behind in efficiently and cost-effectively managing network data, the current monitoring landscape needs closer examination.



At a very basic level, Figure 1 illustrates network monitoring architectures (using vertically integrated tools) as they appear today. In this simplified diagram, the network visibility plane has been stripped out, but effectively network taps and packet brokers would do the job of capturing, preprocessing and delivering traffic (shown on the left) to network monitoring and security tools (shown on the right).

Under the existing model, the storage of network traffic is tightly coupled with the analytics application, with these tools typically processing and storing data in proprietary format. There are also, typically, multiple types of tools deployed across the same network segments, with each of these tools delivering specific functions. These tools and systems range from network or application performance monitoring (NPMs and APMs) tools to security or forensic analysis system or even continuous network recording for compliance purposes. Some of these applications may be acting

[2] "Predicts 2013: Big Data and Information Infrastructure," Gartner Research, 2012.

[3] "The Digital Universe in 2020," IDC, 2012.

only on network traffic that matches certain attributes, for example, HTTP traffic or RTP frames, but more often there is significant overlap of traffic that is directed to out-of-band tools. For this reason, identical network data is often replicated across multiple toolsets, and because each of these tools can store only a narrow slice of traffic at any given time, this has the unfortunate result of increasing the quantity of stored network data without also increasing scope.

Why is this a problem?

Apart from the high cost of storing data at a premium in an application-dedicated appliance, there are a number of issues the current architecture exposes:

- The data is tied to specific stakeholders (the operations group or security group), leading to incomplete data silos. Such silos hide elements of network data that departments need to access, fragmenting visibility.
- Data is not owned by network owners in any meaningful way, as the data is tied to the management tool and stored in proprietary format, so it cannot be accessed for use by other tools, or by anything that isn't in the tool silo. So the tool is the true owner of the data, not the organization.

Scalability is a considerable challenge, because the only way to keep up with the increase in network traffic and the growing number of applications and stakeholders who require access to it is to add more boxes. Over time this becomes untenable, not only in terms of capital expense but operating costs as well.

Tying data to tools, where each of these tools separately processes the data for its own use, is not only inefficient, it further does not reconcile with the current (and coming) IT architectures, which embrace hardware neutrality, fungible data, and efficient (often shared) resourcing.

Leveraging a big data model in the network IT domain

Organizations need to cost-effectively scale the processing and storage of network data to accommodate performance tools, security and forensics systems, and to make that data available to other applications, such as compliance tools, while maintaining flexible control of their data and the underlying delivery architecture.

One solution to scaling network data monitoring and management, particularly for storage-intensive compliance and forensics deployments, is to disaggregate the primary functions of the vertically integrated network tools, decoupling storage and processing from analytics. Providing storage independent of the high-level application enables hardware of choice to be used to maintain the physical store of data, where that data is available for use beyond a single application. Deploying analytics applications independent of the processing framework would allow greater uniformity in how network data is handled, and prevent data from being unavailable outside of a single toolset.

The advantage of decoupling or breaking apart these functions is that the data is returned to the network data owner, and can then be aggregated, and homogenized (pre-processed) for the organization's data platform or used for scalable forensics storage, using hardware not bound to a proprietary platform to reduce costs and increase agility and efficiency. The efficient, high volume processing power of distributed computing frameworks, such as Hadoop, can also be leveraged for large-scale network forensics and security, (and even business intelligence) applications.

The Evolution of Network Monitoring

There are a number of reasons why network monitoring and security applications have been slow to embrace a software centric model or leverage big data frameworks. One reason has to do with network data itself:

- Network data is in hex-encoded, and doesn't really have a repeatable structure, such as would be found in a tab delineated file or an SQL cube. It's structured for efficient delivery, not analysis.
- Applications riding over the network do not conform to an easily recognized format, making identification and analysis challenging.
- The format of network data as it occurs on the network (in packet form) requires it to be handled with specialized hardware (network capture interfaces).

Because of these constraints, network monitoring and security tools for the most part had to be vertically integrated, where a software-based analytics application was developed atop a specific appliance or appliances.

Moreover, network monitoring and security solutions, specifically those that rely and act on network packets, have historically been focused solutions and usually appliance based. There hasn't been significant benefit to changing this approach or a downside to maintaining the status quo until now. Changes within the space have largely been driven by a subset of the market (network packet brokers), which provision data to monitoring and security appliances in a decoupled fashion. This progress in capture, mediation, and delivery of packets hints at how monitoring can further leverage macro trends in the larger IT space and modernize network management.

Legacy Model

When network monitoring and security solutions began to emerge, they relied on one of two methods for getting network data off the network: mirror ports on switches (such as Cisco SPAN ports) or network TAPs, which were often "built in" to the recipient probe/tool. Network data was delivered to network probes with only the thinnest of mediation between the network and the tool.

This approach worked during the early Internet and Web eras in networking. It was fairly easy to get packets from the network using onboard mirror ports on a switch, and it was convenient to deploy probes “out of the box” if they had tapping function integrated. This phase was also a simpler time in the network, when it was unlikely that more than one type of tool would be used for monitoring and that monitoring tool was often used exclusively for ad-hoc troubleshooting.

Eventually basic TAPs and switch mirror ports became impractical. Both TAPs and mirror ports failed to scale with the size of networks; and as more tools and users needed network access, both approaches led to port contention. Typically only one or two mirror ports were available on the switch, and these ports were treated as low priority given that they were non-core functions. Mirror ports also had the added downside of dropping traffic with certain errors, which diminished their value in providing complete visibility.

TAPs, at the advent of the cloud age in networking, had another shortcoming. They passed along all traffic from a single link, but were only able to service a single tool. Introducing multiple TAPs on a single link to support additional tools or another user population wasn’t practical due to performance impact and management overhead.

Both basic (1:1) network TAPs and mirror ports had a limiting effect on the performance of the network tools. Network tools were required to have a dedicated port (or ports for full duplex) per network link, which depending on the link, may not have been appropriate; tool ports were often over or undersubscribed, leading in the former case to dropped packets and lost visibility, and in the latter case to wasted resources.

Current Model

The current model, going back only about 10 years, is when network monitoring started to transition away from purely TAP/SPAN capture. Network TAPs began to incorporate high-capacity aggregation, speed conversion and filtering, eventually leading to where we are today, where advanced, intelligent capture, preprocessing, and delivery has been offloaded from the network tools to what are now referred to as network packet brokers (NPBs). Preprocessing includes time stamping, deduplication, microburst detection, high data burst buffering, and other capabilities that optimize usage of the tools. In most large scale networks, NPBs are capturing and grooming vast amounts of network traffic for network tools and security systems.

This shift towards greater reliance on NPBs eliminated SPAN and TAP port contention because each link could be replicated as needed. It also allowed network owners to better maximize the efficiency and ROI of their monitoring tools because each could be given greater scope in terms of network visibility (through link aggregation) and, at the same time, unnecessary traffic could be filtered out. Network tool issues, such as packet loss, over or under utilization, and unnecessary processing could be eliminated by applying a visibility plane that properly orchestrated the traffic across the management and security infrastructure.

Again, this shift had significant positive effects on network monitoring, not only in terms of economics, but management efficiency. The tool vendors gained advantages as well. The physical probes had lagged behind the network in terms of operating at line rate, so being able to realistically deploy in production environments operating at higher speeds, and also demonstrate ROI beyond the current state of the network, became powerful incentives for tool vendors that embraced the new model.

Unfortunately, while the current model is critical to scaling network visibility across carrier and enterprise networks, the network tools themselves are still distributed and create data silos from a storage perspective. The NPBs proxy packets for the network tools. The current model is an improvement over the legacy approach, but there is still wastage and inefficiency, particularly around the replication of packet storage and the inflexibility of deploying applications with proprietary appliances.

As the analytics applications become increasingly specialized, just as data increases and the pressure to properly monitor and secure networks intensifies, network owners will likely demand greater flexibility from their monitoring and security architectures and infrastructure.

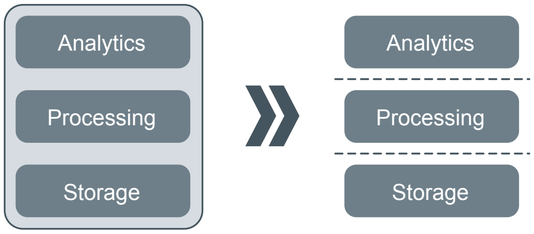
Next-Generation Model

The network landscape has changed considerably over just the last couple of years. Hardware has become faster, cheaper and commoditized, and new networking models are being embraced (e.g. SDN and NFV), which promise agility and flexibility, following in the steps of IT compute and storage. Big data technologies and architectures are also changing how data is handled and delivered. In particular a shared model is emerging, where data is federated and available to multiple applications and stakeholders. Data homogenization and the logical cohesion afforded by big data frameworks have also opened up the potential for new forms of analytics and new use cases.

In the current IT environment:

- Storage is cheaper–making tightly integrated hardware/software tools less attractive. The capture and grooming layer — NPBs — have become more sophisticated.
- Very large scale data processing has become viable for network data–even as probe based systems, where network data is stored in silos, remain tied to the integrated model for some use cases.
- Network visibility systems (NPBs) are more sophisticated, allowing them to take on greater functions, including producing metadata, flow metrics, and even utilization snapshots.

Each of these changes in IT further enables network monitoring to align itself with the strategic initiatives rolling out elsewhere in the networking space as part of “next-generation” deployments. A network analytics model that aligns with next-generation network architectures is one in which the capture, mediation and deliver and the storage, processing and analysis functions are separated.



Network packet brokers can facilitate a shift in monitoring to a next-generation model by providing not only access and preprocessing, but also the package of network data into openly accessible files — composed of either the full packet data or a derivative — eliminating the need for specialized network interfaces. This additional "preprocessing" function increases the range of hardware that would be capable of receiving and storing network data. Once the data is on an open/uniform storage or big data platform, it can be acted on by network, or by an intermediate processing framework that serves network data to visualization and analytics applications.

By offloading these additional processing functionalities (metadata extraction, write to file) from each network monitoring tool to the universal network visibility plane (which provides data to all the network tools), network owners can begin to:

- Eliminate redundancy (storage silos)
- Promote fungibility (data is not proprietary)
- Embrace a shared model for monitoring the network (infrastructure, resources, data assets)

How next-generation network visibility can pivot network data to big data

Adopting a next-generation, "big data" model for network data is an iterative process. It does not require that the existing model be abandoned and the existing toolsets ripped and replaced. Instead, it involves taking a measured approach to incrementally increasing the "openness" of network data (in multiple formats: full packet, metadata, flow metrics), while also emphasizing early, distributed data processing (where the data occurs), both of which translate into greater control and efficiency at every point in the data lifecycle.

The mechanism for gaining visibility into the network, in other words the Network Packet Brokers (operating as a system), are the obvious pivot point for adapting data to a new model. By providing network data in open file formats (whether PCAP, TSV, etc.) that can be directly digested by storage appliances—independent of the processing and analytics functions—the data is liberated. The data is open. The network owner owns the data. Organizations can federate it, centrally view it, run varied processes on it (including powerful, high-capacity processes using MapReduce and Stream), and leverage multiple analytics applications across it. Again, this is due to the NPB layer allowing the storage of data to be decoupled from the monitoring tools.

Instrumenting "network data openness" is the first step. Not in a disjointed, ad hoc way, stitching network adapters (which are essentially components) to disks, but using a proven visibility plane that already supplies network data in real time to network tools.

The near term use cases for open network data on non-specialized servers include targeted capture for forensics or troubleshooting (whether tool-directed, policy driven, or manual). More advanced network owners will be able to sustain continuous capture, and process and analyze this data using their own homegrown tools or by homogenizing it for inclusion in a big data platform.

Further areas for exploration include compliance, forensics, business intelligence (e.g. capacity planning), as well as other applications that would benefit from correlation with other types of data across the organization—in other words, functions that operate offline, taking place anywhere between near real time and long-term, "as needed" only.

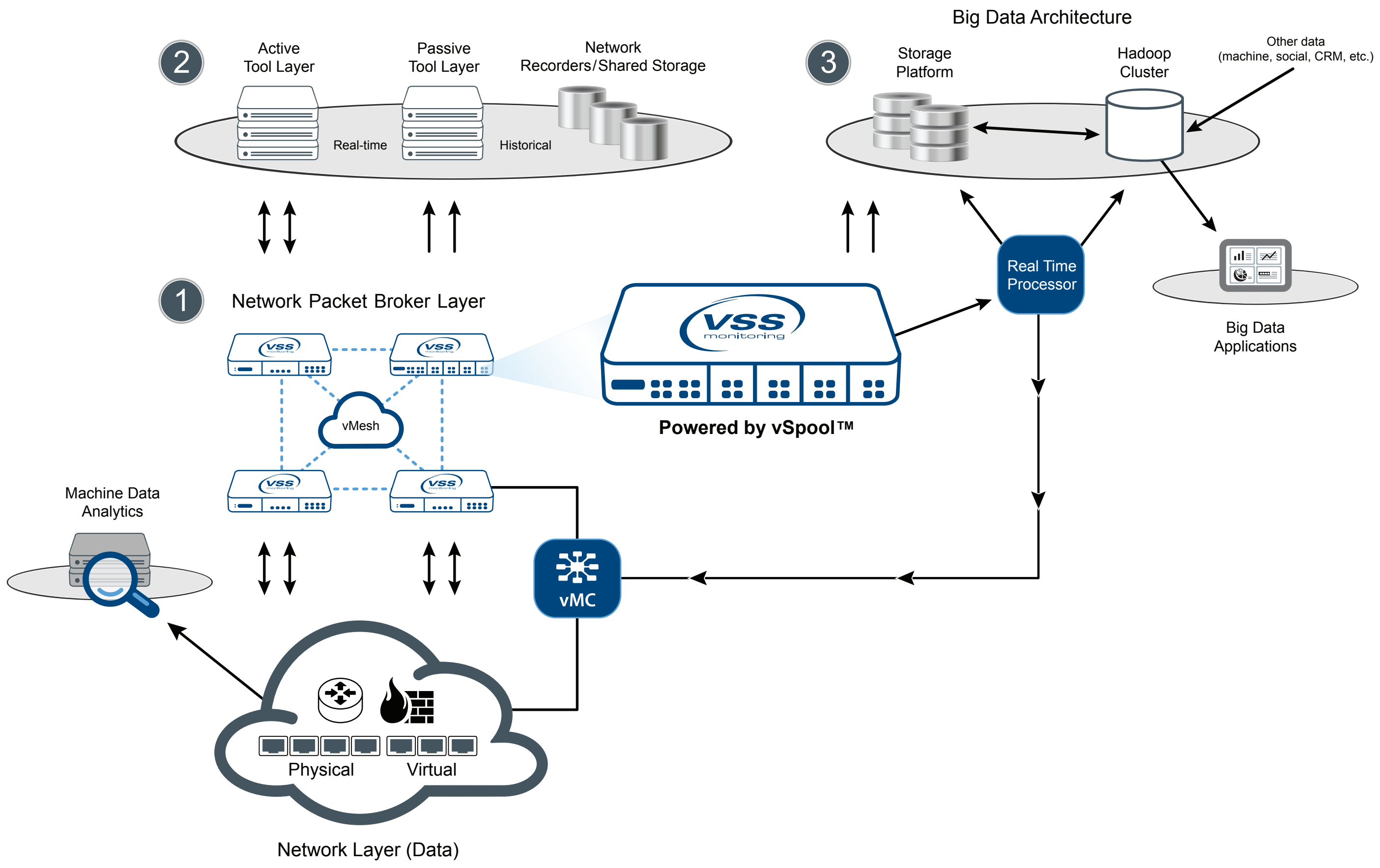
One caveat: There are certain network analytics functions, particularly in security, that require tight association with the underlying hardware in order to inspect and respond to network data in real time. In these cases, decoupling certain processing functions would be impractical. But, again, for most network analysis applications, tight association with the underlying hardware is unnecessary. Ultimately, hardware heavy solutions cost more to scale out and can only offer a silo view of the data.

The VSS Monitoring Big Data Visibility Architecture

VSS Monitoring has historically taken the technology lead in the network visibility (NPB) space on multiple fronts, including in its highly scalable systems approach, single pane management, and complete inline security solutions. In keeping with its forward looking approach, VSS has completed the visibility triad, delivering data to passive tools that receive raw copies of network data, to active tools, such as intrusion prevention systems, that act on live traffic, and now to storage platforms, big data systems (and other tools) in an open format. This comprehensive approach to network visibility is the coming paradigm and one that supports big data initiatives.

NPBs are a natural extension of big data processing, because they "handle" network data where it occurs, before it ever reaches an analytics tool. Indeed, they can serve as the front end preprocessor for the analytics, ensuring (in real time) only relevant, potentially actionable data (depending on the application) is sent for analysis. Preprocessing data where it occurs efficiently prevents information overload.

VSS has also implemented a file creation and offload capability in its platform that generates PCAPs and index files (containing key packet values), delivering them over a standard storage protocol. A PCAP has the advantage of being an "open," non-proprietary file format for complete network packets. In applications where the full packet is not required (or where a processing engine cannot read a packet), an index file, containing 5-tuple and other packet information, can be used in its stead. Index files can also be used to create flow statistics.



In the architecture shown below, the VSS Unified Visibility Plane is capturing and forwarding network data to out-of-band tools as well as active, inline tools. For those tools that retain the data at rest, it's typically stored in proprietary format. The left side of the diagram is known and well adopted. The right side of the diagram is where an open, big data model is applied. PCAPs can be offloaded directly to storage infrastructure, and indexed packet information in file format can be offloaded to big data systems for large scale processing, or else directly to monitoring tools or storage.

This new model allows for enhanced flexibility in terms of both the infrastructure and deployment architecture. It future proofs the data, and makes the future introduction of virtual probes/tools a more viable alternative to hardware based probes.

Use Cases

The opportunity to leverage open capture, whether they hold full packets or only metadata, may vary by organization based on internal expertise and willingness to explore new approaches to network data analysis; however, even with existing infrastructure and tools in place, there are use cases that can enhance security and performance monitoring deployments today. They include:

1. Enhanced visibility for security tools through intelligent triggered capture and sustained capture to sliding window storage for specified applications

2. Metadata for accelerated real time security or performance analysis

3. Medium to large scale sustained capture for forensics or back testing applications, potentially leveraging big data frameworks, such as Hadoop.

Enhanced visibility for security tools

Intelligent triggered capture is a relatively straightforward use case that provides backup full packet capture to storage based on real time direction from an inline security tool, such as an intrusion prevention system (IPS). The inline security tool is designed to be a "bump in the wire," inspecting packets and flows en route to delivery on the production network. When an anomalous packet or flow is detected, an action will be taken, such as blocking (preventing the packet or flow from proceeding through the network) or alerting. These tools are not designed to capture packets and store them, only to act on them as they occur on the network.

When inline tools are deployed using a VSS NPB, the deployment is simplified because live network traffic is mediated to the tools without requiring them to go inline. Once they are deployed with the NPB, the inline tools can leverage its API to trigger PCAPs to be generated and sent to a storage server based on an "event" (suspicious or anomalous traffic). This traffic could then be more deeply inspected, without taxing the inline tool or requiring significant storage capacity on a server. In this way, the actionable intelligence available to the network security team for forensic analysis is broadened. The benefit of adding this additional capture functionality to the NPB is to allow network data to be captured "on demand" regardless of whether a specialized tool is available.

Alternatively, to ensure complete capture of anomalous flows (including the first packet in the flow), the NPB connected to the inline tool could be configured to maintain sustained capture to a server, where that server maintains the traffic for a limited period, retaining only suspect/anomalous flows based on intelligence from the inline security tool. Simultaneously, gleaned intelligence can be used to shape inspection by the inline tool and readjust the NPBs traffic capture protocol. The advantage of this setup is that all suspect traffic can be collected in its entirety—which is not a capability the inline security tools have, as they may begin remediation mid-flow depending on the morphology of the threat. This use case is particularly relevant in sensitive environments, in which the full trace of anomalous or suspect traffic is critical to maintaining network security.

Both of these scenarios can significantly enhance network visibility for inline (and out of band) security tool deployments.

Metadata for security or performance analysis

Many security and performance analysis tools do not require full packets to perform their functions, and when they receive full packets, simply process them into a condensed output of metadata, such as flow metric or KPI. Network packets can require a significant amount of overhead to process, including special interface and accelerated performance and processing power. NPBs already perform optimization of network traffic for network monitoring and security tools, and the additional capability of pre-writing metadata files prior to offload to these tools can reduce the amount of processing overhead associated with traffic capture.

This use case, in which predefined metadata is delivered to the tools rather than the full packets does require that the tool understand the structure of the file and be able to process it to conform to its internal logic; however, the standardized nature of the metadata produced by the VSS NPBs can ease adoption.

Medium to large scale sustained capture

The most complex of the use cases outlined here involve large-scale capture (on non-specialized network tools) of either PCAPs or metadata files for aggregate analysis and/or sustainable, cost effective forensics storage. These scenarios are most suited for early adopters of distributing computing frameworks, such as Hadoop, or those organizations that use internally developed or enhanced applications, or else those that have a retrieval methodology suited for use with commodity servers.

Summary

The appliance model, where solutions become not necessarily better but bigger (accumulating metal along with Terabytes) is deeply entrenched in network monitoring. But as described above, there are significant changes occurring in networking that suggest this entrenchment cannot last. As users become more vocal about their desire for cost-effective scalability and greater flexibility in how solutions are deployed, vendors will respond.

In the short term, steps can be taken by network owners to achieve greater data openness and leverage both hardware and processing frameworks of choice, alongside existing monitoring and security toolsets. Each of these steps can be facilitated by the VSS Unified Visibility Plane.

The VSS Unified Visibility Plane, comprised of network packet brokers, has historically been quite agile, able to swiftly respond to both subtle and substantial shifts in networking. By adopting a VSS visibility plane that can provide both line rate network packet preprocessing from 100Mbps to 100Gbps, as well as deliver packets "raw," encapsulated, indexed, and in the form of metadata, network owners can gain enormous flexibility in how they choose to manage, monitor and secure their networks.

This is the future of network monitoring.

For more information please contact us at info@vssmonitoring.com

VSS Monitoring is a world leader in network packet brokers (NPB), providing a visionary, unique systems approach to integrating network switching and the broad ecosystem of network analytics, security, and monitoring tools.