White Paper

SMVData

Next-Generation Network Visibility

"No-Compromise" Network Monitoring and Security

Preface

As networks grow increasingly complex, gaining end-to-end network visibility becomes essential. While enterprises and service providers struggle to gain sufficient visibility using traditional network visibility approaches as businesses embrace new technologies, such as software-defined networking (SDN) and multi-cloud computing, to stay agile, flexible and effective. Specifically, a range of trends are conspiring to put huge pressure on business networks as a result of which organizations are facing significantly challenges in the way of broad-based network visibility.

SDN networking can offer impressive benefits on service provider and enterprise networks. The challenge, of course, is higher complexity. This complexity in turn impacts the ability to enable end-to-end network monitoring.

Hybrid and multi-cloud network architectures are also behind major gaps in enabling end-to-end visibility. Because cloud networks typically utilize dissimilar platforms, one major obstacle in itself is ensuring that there are appropriate set of monitoring tools needed to support different environments.

Ordinarily, network management teams can monitor traffic for threat analysis by monitoring data flows on physical, on-premises network devices. But traffic within cloud data centers frequently flows between virtual machines and application instances without ever traversing physical networking devices. Assailants can utilize security blind spots for attacks if such threats are not identified and addressed in a timely manner.

Limitations of Traditional Visibility Offerings

In the past, network visibility approaches for large enterprise and service provider datacenters utilized a combination of port mirroring, Test Access Points (TAPs) and network patches to forward traffic to monitoring and security tools pre-positioned in the network where they were likely to be required. As a consequence, uninterrupted visibility and monitoring were impossible.

As datacenter server scalability and agility requirements increased, a network visibility became necessary. As a result, conventional Network Packet Brokers (NPBs) employing proprietary monitoring fabrics came to the fore. NPBs permitted centralization of monitoring and security tools and undertook to permit Network Operations teams to respond to network and issues rapidly by reshaping visibility as-required.

Traditional NPB solutions utilize expensive, purpose-built hardware that is not architected to meet the scale, density and speeds required by next-generation cloud datacenters. Because they are based on costly one-off hardware platforms, NPBs supported comparatively limited port densities and inadequate throughput, at a very high per-port price. In typical cases, enabling 100% visibility required multiple times the cost of the actual production network. The consequence was very high CAPEX and OPEX, making it insurmountable to utilize NPBs to build monitoring networks which met datacenter scalability and performance requirements.

As a result, enterprise and cloud networks require the ability to efficiently capture and analyze all traffic and flows for enhanced visibility, security and troubleshooting without the excessive costs and scaling restrictions of conventional NPBs.

Next-Generation Network Visibility Requirements

The advanced capabilities of next-generation NPBs are critical to the success of modern enterprises. If an enterprise or service provider desires to rapidly expand the scale and functionality offered by their hybrid cloud network, the inadequate feature set and labor-intensive operation of conventional NPBs will hold the business back. Next-generation NPBs will revolutionize the packet broker product category and bring it into line with present requirements.

Software-based NPBs for scalable, on-demand deployment: Traditionally, network packet brokers have been offered as unified systems with integrated software and hardware. However, as network traffic and volumes increased exponentially, proprietary packet broker hardware could rarely meet the performance requirements and required massive and expensive deployments that most customers could not afford. In addition, deployment of new applications and new network infrastructure that need to be monitored and secured actually has driven an expansion of network visibility requirements.

Disaggregated, on-demand deployment of network packet brokers allows enterprises a way to scale their visibility fabrics economically. Typically, these solutions are software-based, enabling hardware flexibility by running on the same switch hardware that network operating systems vendors support.

Extensible, future-proof NPBs: Next-generation NPBs need to be compatible with the SDN/NFV networks, i.e. provide visibility into the inter-VM traffic that does not traverse a physical connection across the data center network. In addition, NPB offerings must be future-proof, i.e. expand with the SDN/NFV network; this is critical because the traditional solutions for physical networks are overprovisioned for peak traffic, making them highly inefficient from the CAPEX standpoint.

Disaggregated, software-based network packet brokers utilizing volume network switch hardware and operating systems will be more affordable than specialized appliances as well as enable cost reduction enabled by innovation in switches and CPU platforms in addition to the economy of scale of mass production. As a result, NPBs will be in rapid alignment as customer requirements and budget constraints evolve through a wide range of hardware options available in the market, scaling from the smallest to the most powerful network packet broker platforms

Centralized management: As the number of NPBs deployed within enterprise networks expand, the capability to manage them as distinct units becomes progressively demanding. Centralized management capabilities give IT management the capability to effect a solitary change and then immediately proliferate it across each NPB on the network. In addition, automation features would allow changes to be implemented on NPBs based on updating of business policies and without manual intervention by IT management. Progressively, implementation of AI technologies will enable business policy-based configuration changes on NPBs.

SDN's centralized traffic management capabilities will optimize NPB service delivery, reducing costs for enabling end-to-end network visibility while maintaining and improving the experience. Together, NFV and SDN will enable the fast and automatic alteration of NPB services, in response to a range of scenarios, from meeting service-level agreements (SLAs) to adoption of new features.

Introducing SMVData NPB: Massive Scalability and Extensibility, with Radical ROI

The industry-leading SMVData network visibility architecture allows optimal visibility and monitoring into service quality, network performance, and user experience as well as resource orchestration and threat remediation, which are critical to maintaining network health and performance and allowing optimal Return on Investment (ROI).

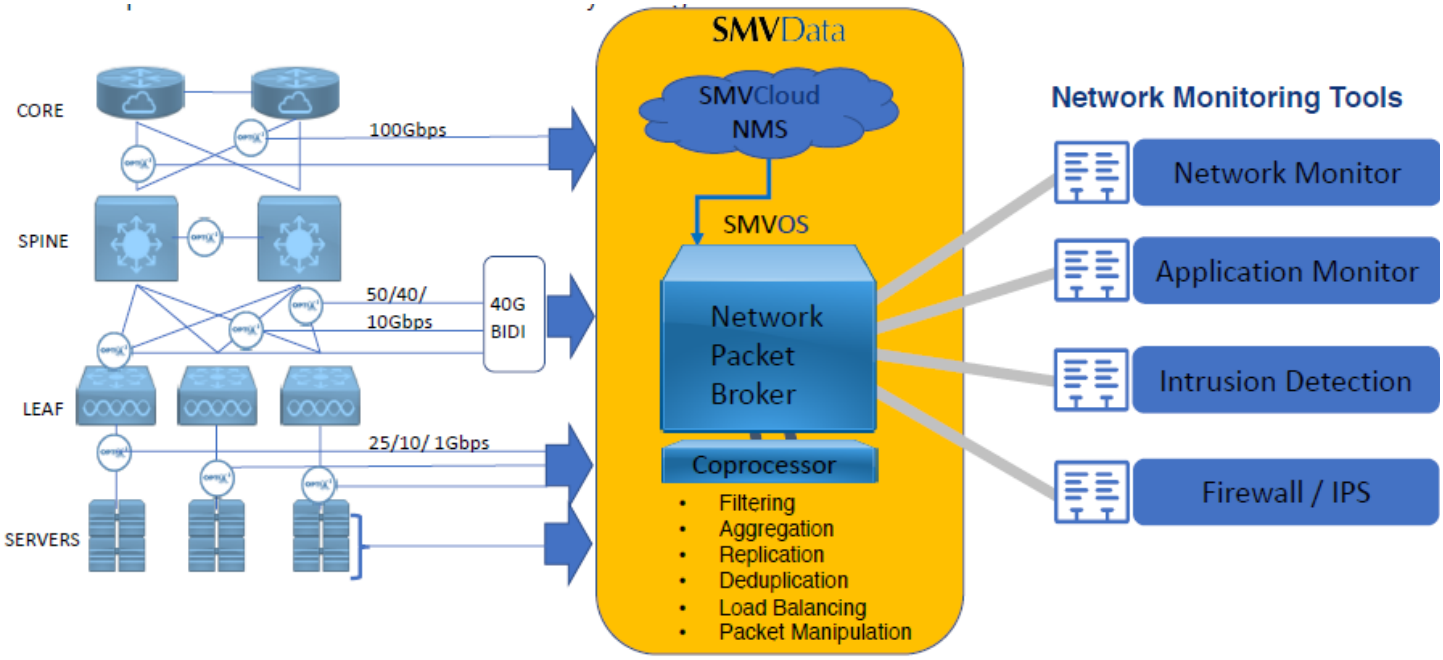

Figure 1. SMVData next-generation NPB allows highly efficient visibility and monitoring of network traffic for enterprise and cloud environments

Software-Based, Hardware-Agnostic: Data center and cloud networks are in the process of undergoing a dramatic shift from being built using large, monolithic chassis-based network infrastructure to flexible, scalable SDN-based networks. As network infrastructure have evolved, the case for NPB infrastructure undergoing a similar evolution is clear.

This is precisely the value proposition behind SMVDatas' next-generation NPB offering, which provides end-to-end network visibility capabilities including traffic capture, filtering, and optimization. SMVData NPB offerings enable a highly scalable, flexible network visibility fabric utilizing merchant silicon-based high-performance network fabric that that delivers optimum CapEx and allows easier management and scaling of NPB functionality. Additionally, SMVData-enabled hardware-agnostic visibility fabric spanning cloud and on-premise environments enables rapid delivery of new capabilities surpassing feature parity with traditional NPBs.

At the root of SMVData NPB offerings is Microsoft Software for Open Networking in the Cloud (SONiC), an extensible platform for network switch operations and management with a large and growing ecosystem of hardware and software partners which offer multiple switching platforms and various software components. Microsoft SONiC enables SMVData NPB offerings with a number of key advantages including use best-of-breed switching hardware, rapid release and deployment of new features without impacting end users, and update rollout securely and reliably.In addition, it provides an SDN software platform for simplified management of all NPB elements in the network, thus enabling unified network visibility fabric architecture.

Virtualized NPB: Virtualization of networking capabilities across on-premise and cloud networks has grown dramatically as enterprises and cloud service providers (CSPs) embrace next-generation architectures to improve service agility and operational efficiency. While providing valuable benefits, network virtualization also presents a new set of operational challenges. Networking functions residing on Virtual Machines (VMs) are vulnerable to malicious attacks that can spread to other functions and services. In addition, monitoring virtualized network functions for performance, service quality, and user impact can be extremely challenging.

SMVData delivers a feature-rich network virtualized NPB solution for cloud provider and enterprise networks. It offers an end-to-end set of visibility capabilities to maximize the productivity of network monitoring and analytics tools. Specifically, it permits real-time visibility into east-west traffic between Virtual Network Functions (VNF) with a full-featured, virtualized network visibility solution which can be deployed as a virtual tap for traffic interception and replication, or as a virtual broker for traffic aggregation, tool-specific filtering, and optimization.

Cloud-based Management: To effectively manage their network visibility fabric, cloud providers and enterprises require a centralized and intuitive management application that provides a “single pane of glass” for all physical and virtual NPBs deployed in their networks.

SMVCloud is a cloud-based, secure multi-tenant network management system that can manage deployment and on-going operations for the SMVData-enabled visibility fabric. SMVCloud maximizes efficiencies in the design, deployment, and operation of the visibility fabric using an intuitive and ease-to-use management system for significant OpEx savings. It permits customizable dashboards for deployment and management of network visibility infrastructure. As a result, NPB deployment is simplified and converged for end-to-end lifecycle management advantage.

About SMVData

SMVData Inc. is a Silicon Valley based company that designs and sells Network Packet Broker software and Cloud-Based Visibility solutions, which greatly enhance the effectiveness and reduce the cost of security applications for enterprise, government, and data center customers.

For more information about our products visit:

www.smvdata.com