SOLUTION BRIEF

Communications Service Providers
Network Security

Big Switch* Delivers Next-Gen Monitoring for Security

Big Switch Networks' Big Monitoring Fabric* is a next-generation network packet broker with advanced features powered by Intel® Xeon® processors and DPDK.

Overview

Data center network traffic is growing at an unprecedented pace driven by modern applications, as IT operations and security teams need increasing visibility into this traffic more than ever. The rise of server virtualization, new application architectures, and the ever-increasing sophistication of security attacks on data center resources have necessitated pervasive monitoring of data center traffic.

Intel® Network Builders ecosystem member Big Switch Networks* has developed a next-generation network packet broker (NPB), called Big Monitoring Fabric.* Big Monitoring Fabric leverages its SDN controller appliances that are powered by Intel® Xeon® processors, and its service node appliances based on the Data Plane Development Kit (DPDK), to provide advanced packet broker functions. The logical, scaled-out architecture of this solution enables comprehensive monitoring and security with the potential for a dramatically improved total cost of ownership (TCO) and operations for enterprises and service providers.

Challenge

The network monitoring requirements of organizations are increasing to support evolving needs of data centers, enterprises, and communications service providers (CommSPs). Today, typical monitoring application use cases include the following:

- security monitoring
- application performance monitoring
- network performance monitoring
- customer experience monitoring
- traffic analytics and recording

More complexity is introduced as the monitoring challenges within these categories evolve and expand. Network security monitoring, for example, becomes more complex with the increased volume of malware and the increased sophistication of attacks. Virtualization has created a different monitoring challenge, with growing amounts of intra-virtual machine (east-west) data traffic that is essential to understanding application and network performance. The answer to these challenges is pervasive monitoring of data center traffic along with advanced functions that enable the most relevant network packet data to be sent to the right monitoring tools, typically located in a centralized tool farm.

Solution

Big Monitoring Fabric (Big Mon) is a modern network visibility fabric that leverages high performance, open Ethernet switches to provide pervasive monitoring and visibility of an organization's network traffic to enable security, while offering the potential for reducing total cost of ownership (TCO). Using an SDN-centric architecture, Big Monitoring Fabric enables a scaled-out fabric for enterprise-wide monitoring, a single pane of glass for operational simplicity, and multitenancy, allowing multiple IT teams (network operations (NetOps), developer operations (DevOps), security operations (SecOps)) to simultaneously perform network monitoring using tenant-specific inline or out-of-band tools and policies.

The Big Monitoring Fabric architecture consists of the following components:

- Cluster of SDN-enabled Big Monitoring Fabric Controllers: A high availability (HA) pair of virtual machines or hardware appliances that control the entire monitoring network and act as a "single pane of glass" for network provisioning, troubleshooting, visibility, and analytics of the entire monitoring fabric. This appliance leverages the power of Intel® Xeon® processors to offer the fabric-wide control, visibility, and analytics functionalities.
- Open Ethernet Switches (White Box or Brite Box): The merchant silicon networking ASICs used in these switches are the same as those used by most incumbent switch vendors. These switches have been widely deployed in production in hyperscale data centers and increasingly in enterprise and SP data centers. These switches ship with Open Network Install Environment (ONIE), which enables vendor-agnostic, automatic installation of third-party network OS, and offers vendor choice to customers for both hardware and network OS.
- Big Switch's SDN-enabled Switch Light OS: A lightweight OS that runs on the switches in the Big Mon fabric. The ONIE-deployable Switch Light OS leverages complete HW ASIC capabilities to support production-grade data center features.
- Big Mon Service Node: An Intel Xeon processor-based appliance leveraging DPDK that connects to the Big Mon fabric (either by itself or as part of a service node chain) to provide advanced packet functions at high performance. Examples of these services are de-duplication, packet slicing, header-stripping, regex matching, packet masking, GTP correlation, UDP forwarding, and Netflow generation.

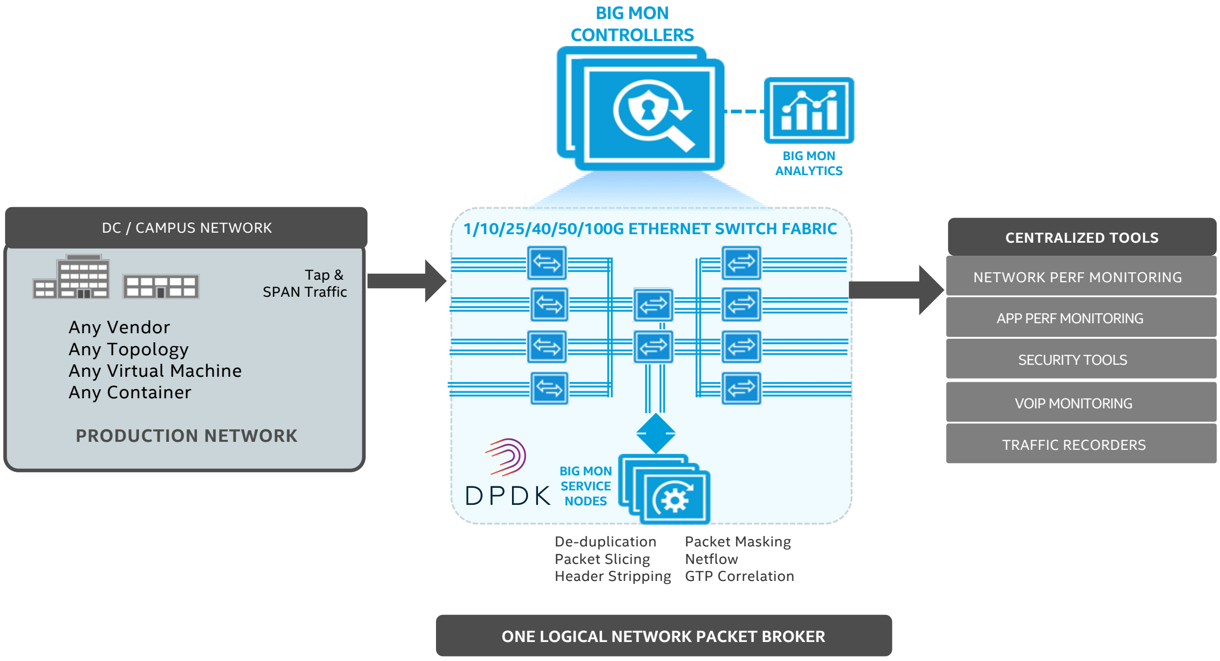

Figure 1. Big Switch Big Monitoring Fabric[1]

Big Mon Service Node Delivers Advanced Processing

One of the features that distinguishes the Big Monitoring Fabric is the ability to scale out advanced packet processing capabilities with the Service Node, an enterprise-class, NEBS Level 3, and ETSI-compliant server powered by Intel® Xeon® processors. It is available in two form factors: 1U with 4 x 10 G bi-directional Ethernet interfaces, and 2U with 16 x 10 G bi-directional Ethernet interfaces.

The Big Mon Service Node provides specialized packet functions like de-duplication, packet slicing, regex matching, header stripping, packet masking and Netflow generation. Once connected to the fabric, the Big Mon controller auto-discovers the service node and becomes the single, central point of management and configuration of the service node. This highly scalable architecture allows chaining of multiple service nodes that are connected to the fabric via the service node chaining function of the Big Monitoring Fabric.

Following are the major specialized packet functions that are supported:

- **Packet De-duplication:** Drops duplicate packets so that fewer packets must be analyzed by the tool.
- **Packet Slicing:** Strips off the payload from collected packets so that the network is processing smaller packets and so that that stripped data can't be intercepted if hacked.

- **Packet Masking:** Hides user/confidential information such as credit card number, SSN, passwords, and medical or financial data to comply with SOX, HIPAA, and PCI regulations.
    - **Regex Pattern Matching:** Filtering of traffic can be done based on regex patterns anywhere within the packet.
    - **Header Stripping:** For VXLAN, Cisco* Fabric Path, LISP, ERSPAN, and MPLS packets. Generic user-defined header stripping function is also supported.
    - **Netflow Generation:** Netflow spec generated by service node and collected in analytics node.
    - **GTP Correlation:** Associates user plane GTP-u data with control plane GTP-c sessions based on IMSI, IMEI, and TEID. Supports load balancing of GTP correlated data to multiple analytics tools while preserving subscriber data flow consistency without any filtering or drops. Supports filtering, whitelisting, and blacklisting of subscriber traffic.

These services all require extensive processing and data plane performance, which the Intel technology-powered Service Node appliance achieves by leveraging Data Plane Development Kit (DPDK) libraries and drivers for fast packet processing. Intel is a key supporting member of DPDK, which works to minimize the number of CPU cycles needed to send and receive data packets, develop fast packet capture algorithms, and run third-party fast path stacks on a general-purpose processor.

Additional deep packet matching intelligence allows the Big Monitoring Fabric to match up to 128 bytes of each packet at line rate to enable application protocol recognition, ensuring the routing of data to the proper analysis tool. This capability allows network engineers to create sophisticated monitoring policies, for example matching inner header fields for encapsulated packets such as MPLS, VXLAN, and GRE and/or mobile 4G/LTE protocols such as GTP and SCTP.

Solution Benefits

Scaled-out Network Visibility and Packet Functions: The scaled-out monitoring solution enables network access points from the entire network (through TAPs/SPANs) to be mapped to all tools, typically in a central tool farm. In addition, the solution offers the ability to scale out advanced packet processing with service nodes.

Excellent Operational Agility: Centralized control and zero-touch management reduces security burden and IT group contention with sharing of network access points, data, and tools among IT groups.

Optimized Network Tool Utilization: The solution enables tools to be fully utilized by policing data from many network access points and by ensuring that only the data that matters is sent to the tools by aggregating, filtering, policing, or modifying the appropriate traffic flows to the tools.

Rapid SDN-enabled Innovation Velocity: The solution leverages open networking hardware to support monitoring of any infrastructure with any vendor tool, offering simplicity, scalability, and reliability. The software-defined approach leveraging Intel Xeon architecture drives feature velocity and fast innovation.

Learn More

For additional information on the Big Monitoring Fabric, contact Big Switch via email at info@bigswitch.com, follow @bigswitch on Twitter, or visit www.bigswitch.com.

About Big Switch Networks

Big Switch Networks brings hyperscale data center networking technologies to a mainstream data center audience. The company's Big Monitoring Fabric is a feature-rich next-generation network packet broker to monitor and protect existing networks, and Big Cloud Fabric is the industry's most advanced open networking switching fabric intended for new data center pods such as OpenStack private cloud, VMware NSX, big data, and VDI.

About Intel® Network Builders

Intel Network Builders is an ecosystem of independent software vendors (ISVs), operating system vendors (OSVs), original equipment manufacturers (OEMs), telecom equipment manufacturers (TEMs), system integrators (SIs), enterprises, and service providers coming together to accelerate the adoption of network functions virtualization (NFV)-based and software-defined networking (SDN)-based solutions in telecom networks and in public, private, and hybrid clouds. The Intel Network Builders program connects service providers and enterprises with the infrastructure, software, and technology vendors that are driving new solutions to the market. Learn more at http://networkbuilders.intel.com.

[1] Figure courtesy of Big Switch Networks.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. **No computer system can be absolutely secure.** Check with your system manufacturer or retailer or learn more at intel.com.

Cost reduction scenarios described are intended as examples of how a given Intel- based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.