A10 Thunder Threat Protection System with Big Tap Monitoring Fabric

Leverage the power of A10 Threat Protection System (TPS) with Big Tap Monitoring Fabric based on bare metal switching and software defined networking (SDN) to enable rapid "mean time to mitigation" of data center-wide cyber threats with unmatched efficiency and at an unprecedented scale.

THE CHALLENGE

Data centers worldwide have seen an increasing demand for a higher portion of network traffic to be monitored in the past few years. In addition to Internet and WAN edge (north-south) traffic, new use cases, including public/private clouds, Big Data analytics and Virtual Desktops are driving IT organizations to monitor high-bandwidth east-west traffic in the data center. In many instances, east-west traffic in the data center constitutes up to 70% of total traffic, traversing hundreds of 10G and 40G links. With increased cyber-security concerns as well as Distributed Denial of Service (DDoS) attacks growing in frequency, size and complexity over the last few years, InfoSec organizations are determined to monitor their entire data center infrastructure for security attacks and breaches. It is clear that optimal tapping/mirroring of the networks is not only necessary but also increasingly paramount, as it vastly helps in quick and efficient troubleshooting key issues related to security, network and application performance.

THE SOLUTION

A10 Networks and Big Switch Networks have partnered to create an efficient, cost-optimized solution for DDoS attack detection across the entire data center. The solution is composed of A10's Thunder Threat Protection System (TPS) and Big Switch's SDN-based Big Tap Monitoring Fabric leveraging bare metal Ethernet switches. The solution enables security administrators to monitor data-center wide traffic (including east-west traffic) for sophisticated DDoS attacks and security breaches.

Customers can fully realize the unique benefits offered by Thunder TPS with its high-performance, multi-level DDoS protection capabilities combined with Big Tap's ultra-low cost, operationally simple and scale-out monitoring fabric.

THE TECHNOLOGY

The **A10 Thunder TPS** product mitigates the largest and most complex DDoS attacks with the following capabilities:

- Multi-level DDoS protection: A10 Thunder TPS detects and mitigates multiple classes of attack vectors, including volumetric, protocol, and enables continuous availability of services.

- Performance scalability with hardware acceleration: Multi-vector detection and mitigation functions are distributed across optimal system resources – high-performance Security and Policy Engine (SPE), which leverages specific hardware components for traffic acceleration such as FPGAs to immediately detect and mitigate over 50 common attack vectors in hardware (SYN cookies, for example) with more complex application-layer attacks (HTTP, SSL, DNS etc.) processed by Intel Xeon CPUs.

- Broad deployment flexibility: Flexible deployment models for in- and out-of-band operations, and routed or transparent operation modes are provided. With an open RESTful API, aXAPI, Thunder TPS enables integration into third-party network analytics solutions.

The **Big Tap Monitoring Fabric** leverages commodity bare-metal switches to provide the most scalable, flexible and cost-effective visibility fabric. Using SDN architecture, Big Tap allows users to centrally define and provision policies that deliver traffic from Any Tap to Any Tool at Any Time. The scale-out fabric supports multi-tier designs for various traffic loads (1/10/40G) and a range of tools. The Big Tap Controller has inbuilt multi-tenant support to provision On-Demand Monitoring-as-a-Service for internal teams (e.g., security team, network ops team).

By enabling efficient utilization of existing Network Packet Brokers (NPB) and leveraging bare metal economics, the Big Switch solution allows for a multi-fold reduction in total costs.

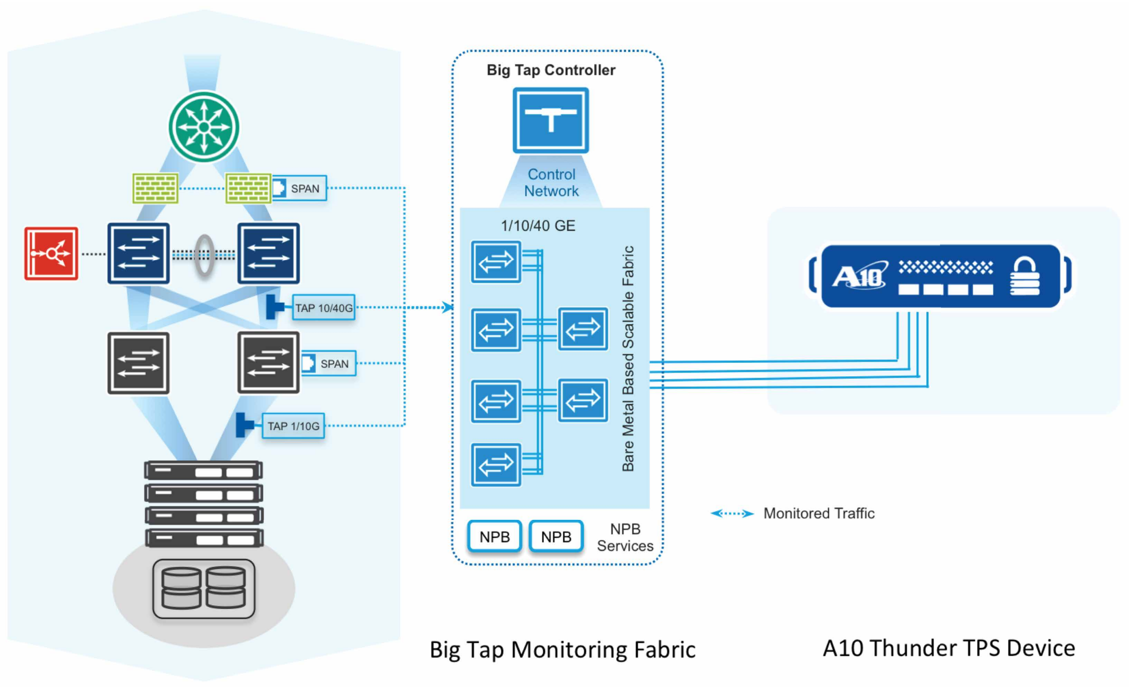

Figure 1: A10 Thunder TPS deployed along with the Big Tap Monitoring Fabric

KEY SOLUTION BENEFITS

When deploying Big Tap Monitoring Fabric, the security administrator can consolidate the A10 TPS devices and connect them to the monitoring fabric. Doing so, the user can deploy data center-wide Threat Protection designs to achieve the following benefits:

- **Advanced Data Center-Wide Threat Protection**—any tap traffic can be directed to any Thunder TPS device at any time, truly enabling the Thunder TPS platform to access any data center flow and detect DDoS attacks at a very high rate (10 to 155 Gbps, up to 1.2 Tbps in a cluster). This enables enormous threat intelligence list processing (16 million line lists to define known bad IPs and actors at very large scale), high-speed string search, and good packet capture capabilities. In addition, customized actions can be taken against advanced application-layer attacks as needed with aFlex Deep Packet Inspection (DPI) scripting.

- **Bring the traffic to the tool**—instead of the cost and operational challenges to deploy tools in disparate areas of the network, tools are consolidated in main data centers under the security administrator's control, and any traffic anywhere in the network can be presented to these tools. This prevents cross-organization approval requirements and enables monitoring of remote data centers/co-lo facilities as well as remote branch locations.

- **Flexible, Scale-Out Fabric Deployment**—hundreds of 1G/10G/40G TAP and SPAN ports can be connected to the Big Tap Monitoring Fabric, and network traffic can be automatically directed as per monitoring policies to the A10 TPS platform for analysis.

- **Policy based, Multi-Tenant Tap and Tool Sharing**—the same traffic can be accessed by multiple groups and sent to multiple devices—e.g., threat protection with A10 TPS for network security and availability, debugging for network operations, and recording for Legal Compliance can all be implemented simultaneously and without compromise. Furthermore, existing NPBs can still be leveraged for advanced features, such as time stamping or packet slicing.

- **Operational agility with Centralized Programmability**—monitored traffic is fully visible and can be steered from a single, centralized management pane. Policies can also be changed programmatically in real-time in response to a specific event trigger. For example, the security administrator can react to an ongoing attack in real time by altering the Big Tap policy to monitor more traffic and send it to more devices.

In summary, the combination of A10 Network's state-of-the-art Thunder Threat Protection System and Big Switch's Big Tap Monitoring Fabric uniquely leverages advanced and sophisticated threat protection and SDN-powered bare-metal switching fabric to combat Cyber Threat with unmatched efficiency and at an unprecedented scale.

ABOUT A10 NETWORKS

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: http://www.a10networks.com

big switch networks

Headquarters
3965 Freedom Circle, Suite
300, Santa Clara, CA 95054

+1.650.322.6510 **TEL**
+1.800.653.0565 **TOLL FREE**

www.bigswitch.com
info@bigswitch.com