Solution Brief

Enhanced Security Capabilities for Virtual Server Infrastructure

The Impact of Virtualization on the Evolving Security Threat Landscape
IT Security teams continue to mitigate security threats with traditional security devices. But virtualization has caused the enterprise to explore new ways to extend the reach of security tools into the virtual infrastructure. With today’s distributed application architecture that led to the growth in East-West traffic inside the hypervisor, security architects are looking for more efficient ways to gain visibility to that traffic on behalf of their existing and next-generation security appliances, such as IDS/IPS, Web server security, integrity monitoring and malware inspection, along with several other tools.

Server Virtualization Creates Silos of IT Hidden From Security Tools
Security tools such as perimeter firewalls and IDS/IPS sensors are commonly deployed at the perimeter of the network, where they inspect network traffic between untrusted zones like the Internet and trusted zones such as the core data center or end-user networks. However, today’s security threat mitigation can no longer be accomplished with just a firewall and IPS sensor. Comprehensive security must encompass all threat vectors including but not limited to, e-mail scanning, web application security, malware detection, and granular application control. These tools rely on live packet streams on the wire. They also rely on end-to-end packet flows between network segments, servers, and end-users. As the infrastructure is virtualized and the traffic migrates inside the virtual switch, tools examining that traffic can go dark—the virtual network becomes a hidden silo of IT.

Network Virtualization Introduces Another Barrier to Security Visibility
With the increasing adoption of overlay networking, traffic going to and from the virtual server environment is encapsulated to aid in workload mobility and resiliency. By wrapping an IP packet with an encapsulation header such as VXLAN, the packet may become invisible to network security inspection tools. Many tools are able to de-capsulate the packet, but that is an added burden on the tool, especially in light of growing network speeds up to 100Gb.

Many security tools are challenged to keep up with network speed growth in light of encapsulation protocols such as VXLAN, ERSSPAN, and even some well-proven protocols like MPLS.

Recording Virtual Machine Traffic
Many organizations face requirements to capture and store (or record) network traffic streams. There are numerous packet recorders and other security tools on the market today, including open source and commercial products. They receive packet streams from network TAPs or SPAN ports. In both cases, packets are captured on the wire and transit a physical network link to reach a network port on the security tool. When a server migrates to a virtual machine, all East-West traffic associated with that server may no longer be visible by the tools on the physical network.

Multiple Blind Spot Detection and Resolution
With most web application traffic hosted in the virtualized data center using SSL, the data center administrator now has multiple blind spots to deal with.

1. East-West VM traffic
2. SSL encrypted application traffic
3. Overlay networks (using VXLAN) that are created in a software-defined data center for tenant micro-segmentation

Gaining Visibility of VM Traffic with GigaVUE-VM
The Gigamon VM solution is represented in Figure 1. Gigamon’s GigaVUE-VM extends pervasive visibility for monitoring, analysis, and security tools into the virtual environment and private cloud. GigaVUE-VM is a small footprint VMware virtual machine. It supports the vNetwork Distributed Switch, Standard Switch, NSX vSwitch, as well as the Cisco Nexus 1000V for vSphere 5.x environments. Leveraging VMware’s native APIs, the GigaVUE-VM solution is able to instruct the vSwitch to send copies of VM traffic to another destination port. The GigaVUE-VM node is attached to the destination port and receives the copied packets. The packets are then filtered before being encapsulated on a tunnel and sent.
to a destination tool on the physical network via a physical fabric node enabled with Gigamon’s GigaSMART® technology. GigaVUE-VM can also perform packet slicing operations to target specific packet information prior to encapsulating traffic onto the tunnel. With Gigamon’s patented Flow Mapping® and packet slicing features, tool administrators are able to greatly reduce the amount of virtual machine traffic that is copied and sent to security tools in the physical network. The management, deployment, and configuration of the GigaVUE-VM nodes are accomplished with the GigaVUE-FM fabric manager, using a low-privilege vCenter user account, eliminating the need to hand over full administrative privileges to teams who do not control the virtual infrastructure.

**Maintaining Visibility During Virtual Machine Migration**

Another issue facing VM administrators is enabling continuous visibility during VM migration for the tools being used to monitor, analyze, and secure the entire data center infrastructure. Virtual servers have become the platform of choice for application deployment because of their dynamic nature. However, their dynamic nature makes them very difficult to monitor, especially when a vMotion event occurs. In the absence of the GigaVUE-VM solution, when a VM is moved from one hypervisor to another the only way to maintain visibility is for the VM administrator to go through a long list of configuration items to manually disable existing vSwitch port mirror sessions and create a new port mirror session on the destination hypervisor where the VM in motion has landed (see Figure 2).

**Figure 1: The GigaVUE-VM enables visibility for virtual machine traffic transiting the Virtual Switch**

**Figure 2: The GigaVUE-VM solution maintains visibility policies before and after a vMotion event occurs**
The GigaVUE-VM solution for monitoring of VM traffic, along with the GigaVUE-FM fabric manager, monitors the vCenter server alert function for vMotion events. When a VM is moved from one hypervisor to another, the GigaVUE-VM visibility policy moves with it to the new hypervisor, thus providing continuous visibility of the VM traffic before and after a vMotion event occurs.

SSL Traffic and Overlay Network Visibility
Gigamon’s GigaSMART intelligence, specifically SSL Decryption, header stripping, and Adaptive Packet Filtering could be service chained to perform the following functions before forwarding the traffic to the monitoring infrastructure, effectively removing any blind spots (see Figure 3).

1. Decrypt the SSL traffic (using pre-configured keys identified per application)
2. De-capussulate any overlay transport (for ex., VXLAN, MPLS)
3. Filter the packets per tenant (ex., VXLAN segment id or MPLS label, etc.)

Centrally Managed and Pervasive Visibility into the Virtualized Server Environment
Security monitoring is not just about preventing attacks. Security architecture covers a broad range of comprehensive security and forensic capabilities, using a combination of tools such as NPM, DLP, compliance monitoring, IDS/IPS, and APM, all of which require access to packet level detail off the wire. With the wire now being the virtual switch, security architects may have no scalable, seamless integrated method to see a virtual server’s ingress/egress traffic.

The GigaVUE-VM virtual fabric node by Gigamon delivers centrally managed and pervasive visibility into the virtual server environment. East-West and North-South traffic can now be captured and directed to security tools on a per-VM basis, giving security administrators full access to packet-level virtual traffic detail. GigaVUE-FM, which supports deploying and monitoring hundreds of GigaVUE-VM virtual fabric nodes, provides hotspot monitoring using Top-N and Bottom-N traffic widgets in the dashboards.

Figure 3: Service chaining with GigaSMART applications to remove security blind spots