IntellaTap-VM Use Cases

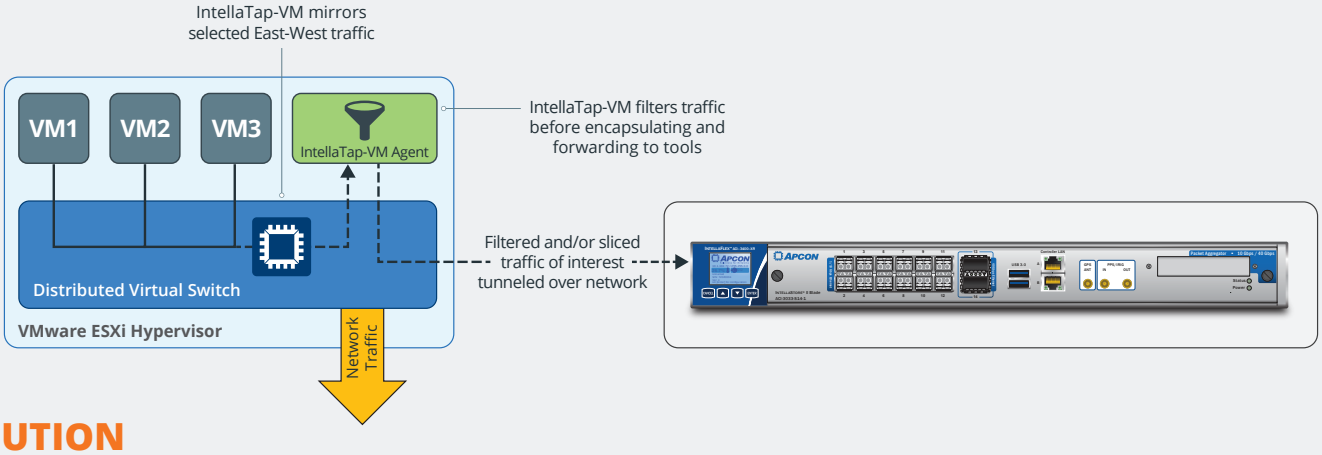
VMware network deployments come with a unique set of challenges including how to maintain security and visibility. APCON's IntellaTap-VM product helps to close visibility gaps and optimize existing security infrastructure.

Security Tools Dropping Packets

CHALLENGE

Many organizations are rapidly migrating towards Software Defined Data Centers (SDDC) and using VMware technologies to virtualize their IT environments. Fueling this migration is the need for a more flexible and dynamic infrastructure, which allows businesses to be more competitive and deliver innovations with faster time to market. While a rapidly growing VMware environment can enable a new level of productivity across an organization, it can also result in significant strain on existing network security appliances. As ever-increasing amounts of data flow across the network, traditional monitoring appliances can become overwhelmed with the growing volume of traffic.

To maintain a strong security posture, Network security and operations teams will often attempt spanning traffic from virtual switches into an IDS/IPS and perimeter firewall. These tools rely on live packet streams to properly secure the network. As the volume of east-west traffic grows, it's common to see these traditional tools experience a data throughput volume which is higher than the maximum rated capacity, resulting in dropped data packets. These dropped packets have now created a monitoring blind-spot. And for most organizations, it's entirely possible that some of these dropped packets can contain malware or ransomware C&C callback breadcrumbs. As organizations drive towards proactive threat detection and automated remediation, it is mission-critical to be able to detect a breach and mitigate damage. In an ideal scenario, the ingress ports on security appliances should be kept well below 80% of their capacity on average, so that intermittent data surges or microbursts do not overwhelm the ports.



SOLUTION

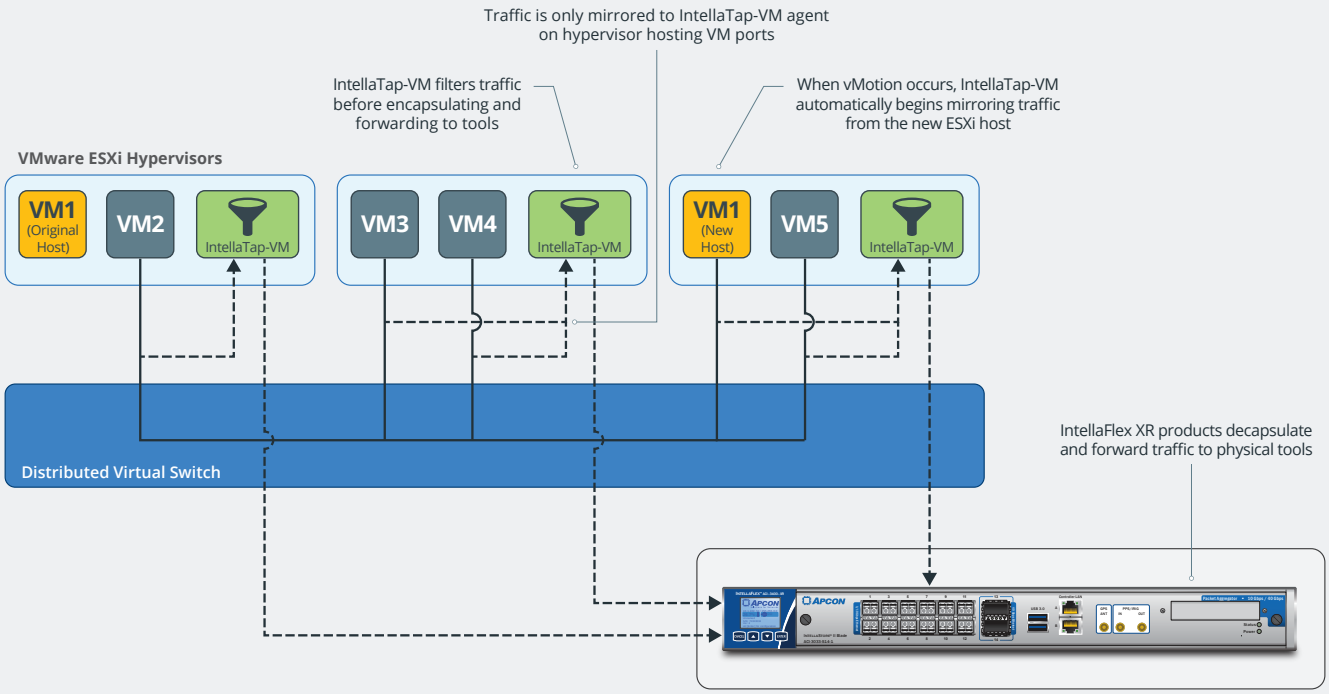
Deploying IntellaTap-VM agents to monitor your VMware network traffic allows you to not only capture previously unavailable east-west packet flows, but it also allows you to easily apply filters which will only forward traffic of interest. For example, if you only wanted to inspect web traffic you can apply filters to only capture those packets. Additionally, IntellaTap-VM agents can perform packet slicing, which removes the payload data from packets, leaving only header information. Filtering and packet slicing capabilities reduce bandwidth consumption and ensure security and performance monitoring appliances receive more condensed network data for analysis, thereby increasing efficiency and utilization.

Closing Private Cloud Visibility Gaps

CHALLENGE

Often times virtual machines in an ESXi cluster contain densely packed sensitive data, such as passwords, personal data, encryption keys, and license keys. They're usually also running critical applications that need to be carefully monitored for any potential issues. And in a dynamic Software Defined Networking (SDN) environment, maintaining visibility becomes increasingly difficult.

This scenario can create significant security vulnerabilities because traffic over your virtual network may not be visible to security protection devices on the physical network. Traditional monitoring technologies rely on having access to traffic on a physical link, but in a virtualized environment much of the VM traffic may never leave the host server. As more VMs are deployed, the chances of undetected malware or ransomware circulating within a virtual environment increases.



SOLUTION

By implementing a strategic deployment of IntellaTap-VM virtual agents throughout a VMware environment, organizations will be able to monitor virtual traffic of mission-critical applications and nodes. Administrators can pick and choose the type of traffic they wish to capture and send it to existing security appliances for deeper analysis. IntellaTap-VM also integrates with vCenter for full visibility of the entire port group inventory. Finally, in a dynamic virtual environment, VMs may be instantiated or relocated to different physical hosts to balance load capacity. IntellaTap-VM supports these vMotion events to maintain visibility over this ever-changing virtual infrastructure. With APCON's IntellaTap-VM organizations gain deeper visibility into VMware environments.