WHITEPAPER

VIRTUALIZATION & Cloud Review

MONITORING AND MANAGING NETWORK FLOWS IN VMWARE ENVIRONMENTS

By Trevor Pott

APCON
Solutions for Networks

www.apcon.com

Monitoring and managing network flows is a critical part of a secure and efficient approach to IT. Unfortunately, it's difficult to design networks to be monitored by the good guys without making it easy for the bad guys to do the same thing. One solution to this conundrum is packet brokers.

Network monitoring is useful because it allows us to see what data is traversing a network. In a practical sense, we want to make sure that individual users and servers are only communicating with devices and applications they absolutely need to. We also want to make sure critical information (for example, credit card data) doesn't leak out. This can all be done by observing network flows without interfering with them.

Network management is another story. Here we typically want to either prevent certain data flows from occurring (for example, blocking sites related to known malware) or redirect flows in order to manage network traffic.

Network monitoring and management isn't just about security; business units other than IT can derive real-world benefits from its use. Analysis of network data can lead to insights that benefit operations, development teams, and business units. Some of these insights come from direct efficiencies like workload locality or detecting oversubscription of resources. This information allows operations teams to make changes to infrastructure that increase efficiency.

Some of the benefits of network monitoring and management are preventative. These include helping detect compromise, recording resource access for regulatory purposes, and so forth.

Some benefits are predictive. These include predicting resource exhaustion or getting a better understanding of workload utilization and interaction so that operations teams can better plan for changes, migrations and upgrades.

Network monitoring for regulatory or security purposes is often concerned with the contents of a data flow. The data which is traversing the network is often the element of interest, with security solutions which act on data flows in real time serving as the receiver for those data flows.

Network monitoring for network management, usage insights and prediction is usually concerned with metadata about data flows. Here, data storage solutions coupled with post-process analytics packages serve as the receiver.

VIRTUALIZATION

Before virtualization, monitoring a network was reasonably straightforward. One could physically place a device between two network connections, effectively interposing it in the middle of a link. Alternately, one could configure a switch to mirror data to a specific port.

Virtualization presents some interesting challenges to those who wish to monitor data flows. Virtual machines connect to virtual switches and much of their communication may occur entirely within the bounds of their virtual host. In other words, network flows that administrators might wish to monitor may never traverse a wire or be seen by a switch.

Getting a handle on an organization's data flows requires the ability to bring information about data flows from multiple sources, traversing multiple types of networks into a single location. This is where packet brokers come in.

PACKET BROKERS

A packet broker is a solution that accepts traffic from multiple network links and then delivers relevant data to appropriate downstream solutions. Because packet brokers have a small footprint and low resource usage, this makes them ideal for use with virtualized environments. Data can be collected from multiple virtual switches and either processed in a VM on that host, or shipped off to a more central repository.

VIRTUALIZATION PRESENTS SOME INTERESTING CHALLENGES TO THOSE WHO WISH TO MONITOR DATA FLOWS.

Solutions to this problem have existed for some time: virtual switches have gained features similar to physical switches that allow data flows to be monitored. Unfortunately, these solutions have traditionally been difficult to use and manage, especially at scale.

Virtualization enables scale. Before virtualization, organizations had to expend significant resources to manage a few hundred machines. Virtualization enabled organizations to manage thousands of workloads with the same resources. Containers extended this to tens of thousands of workloads and the IT automation of cloud computing can bring it into the millions.

Packet brokers can send data to all sorts of other solutions. Using network taps and port mirroring (in which packet brokers do not interrupt the data flow) packet brokers can send data to network monitoring, application and intrusion detection systems. When serving as an interposer in which all data streams under management traverse the packet broker, the packet broker can service the above mentioned solutions, as well as firewalls, intrusion prevention systems and more.

THE THROUGHPUT PROBLEM

On a small enough network, it is possible to engage in network management by passing

all traffic through fixed points such as firewalls. The reality of most midsized and larger networks, however, is that network management can only be achieved by sampling multiple data flows and then applying management. These samples are obtained via filters applied to network taps.

Modern networks move around too much data for any individual firewall or router to handle, yet the principle of defense in depth demands that administrators monitor their networks in more places than at the edge.

The "eggshell" model of IT security is to build a tough shell around a network by defending the interface between that network and the internet. The hypothesis driving the eggshell security model is that malicious actors exist on the internet and will attack from there. This model ignores both insider threats and human error. It also assumes that the edge detection solutions will catch all compromise attempts.

Defense in depth—which is the generally accepted best practice approach to IT security—requires administrators to presume that any system, anywhere in the network, can be compromised. Defense in depth calls for monitoring of communications between systems at multiple points within a datacenter.

One example of communications inside the datacenter that need monitoring would be communications between a web server of a point-of-sale solution and a database back end. Both can exist as VMs on a single host, and neither is really supposed to ever be exposed to the internet.

It isn't a stretch to imagine that a user endpoint accessing the point-of-sales system's web server is one day compromised. Ideally, in addition to any defenses on the web server to protect against this, administrators would monitor requests between the web server and its database looking for suspicious activity.

Network connections deep within an organization's datacenter often operate at speeds of 10, 40 or even 100 gigabits per second. There can be thousands or even hundreds of thousands of network connections within a datacenter. No firewalls or routers exist which could handle all of that data at once, in real time.

Packet brokers are subject to the same forces. A packet broker can receive data from one or multiple sources and transmit that data to one or multiple sources. It is thus entirely possible for a packet broker to be asked to inspect more network data than the bandwidth available. For this reason, packet brokers employ filters.

INTELLATAP-VM

APCON's IntellaTap-VM is a virtual agent designed specifically for VMware ESXi virtualization environments. It is designed to operate as part of a larger solution that can include physical packet brokers for monitoring physical switches. IntellaTap-VM boasts a sophisticated set of layer 3 and 4 filters which allow it to sort through incoming packets and retain only those which are absolutely necessary.

IntellaTap-VM then encapsulates these packets in a GRE packet and sends it to a designated receiver. The receiver is a necessary part of the solution, because while IntellaTap-VM is designed to filter data streams, it relies on second-stage security or analytics software in order to do the actual

analysis. This allows IntellaTap-VM to keep the footprint on individual virtual hosts small.

IntellaTap-VM is lightweight. Each host agent consumes only a single virtual CPU, 512MB of RAM, and 512MB of disk per host. Host agents are managed by APCON's TitanXR, providing a single management solution for multiple packet brokers.

In and of itself, a lightweight packet broker with a set of capable filters is a useful solution for many organizations. Network monitoring isn't optional in today's datacenters, and packet brokers are just one of those "must have technologies." What sets IntellaTap-VM apart from similar offerings, however, is the focus on ease of use.

SOLVING THE EASE OF USE PROBLEM

Getting a packet broker installed and configured across every host in a cluster—and then across all the clusters under management in a datacenter—is annoying. Packet brokers for virtualization environments live inside VMs. Administrators must either stand up a VM, install an Operating System Environment (OSE) and then install the packet broker software, or deploy a virtual appliance to each host.

Once the packet broker software has been deployed, the Distributed Virtual Switch (dvswitch) must be configured to mirror data flows to the packet broker VM. Careful attention must be paid to the correct configuration of dvswitches, port groups and NICs so as not to impact production data flows.

IntellaTap-VM's installer interfaces directly with the vSphere server, and handles all of these complexities so that administrators don't have to. The IntellaTap-VM installer will deploy the packet broker VMs as needed, as well as configure the dvswitches and port groups.

From the administrator's perspective, they need only provide the IntellaTap-VM installer with their vSphere server credentials, the datastore they wish to deploy VMs to, and the address of the designated receiver.

Once engaged, the IntellaTap-VM installer creates a new port group on the target VMware cluster. This new port group will contain all of the monitor NICs for the packet broker VMs. This is done so that data flows, quotas, etc., on the production port group(s) aren't impacted. If administrators wish to monitor multiple port groups on the same distributed vswitch, the IntellaTap-VM install will simply add a new mirror to the existing port group already created for monitoring.

CONCLUSION

Network monitoring and management tools are largely invisible but increasingly critical components of every datacenter. They are critical to a defense in depth security approach, understanding network utilization, increasing efficiency and future planning.

Virtualization has created a very real problem in maintaining network monitoring capabilities. IntellaTap-VM not only solves this problem, it does so in an easy to use manner.

For more information, visit:

http://www.apcon.com

APCON
Solutions for Networks