CERIAS

The Center for Education and Research in Information Assurance and Security

An Analysis of Technologies for Monitoring Inter-VM Traffic

Grant Richards and Tyler Bautista PI: Dr. Baijian 'Justin' Yang

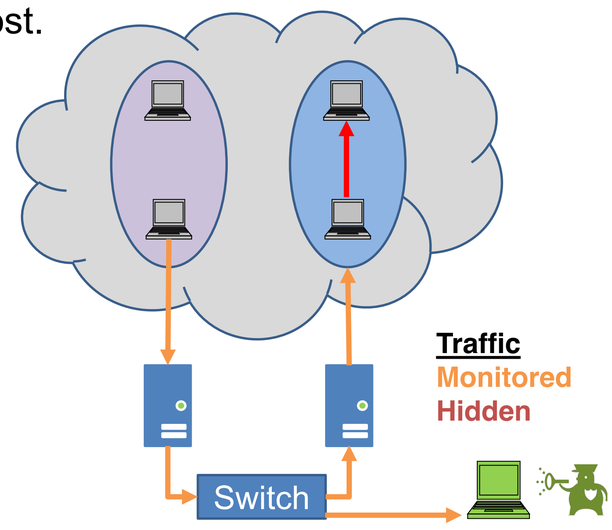
Problem Statement: Network traffic between virtual machines on the same physical host cannot be monitored by standard network management and security tools**.** This project investigates existing technologies that enable security monitoring and management for inter-VM traffic within the host.

Significance:

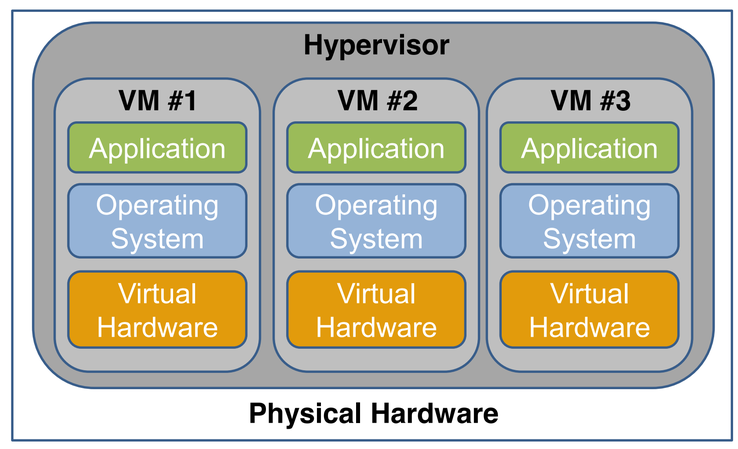
- Detecting and responding to attacks
- Policy enforcement
- Data theft
- Resource management

Research Methods:

- Literature review
- Contacting vendors and professionals
- Testing of Open vSwitch



Virtualization: This is a technology that enables a type of software called a hypervisor to create 'pretend' hardware called virtual machines (VM). VMs use the physical resources of the host machine to behave like it is a standalone computer.



Findings

Types

Virtualized Switch

- Software solution
- Most hypervisors have one already
- Can be configure to monitor the virtual network
- Must be configured for each host

Hardware Off-loading

- Hardware based solution
- Virtual network traffic sent to physical switch
- Standard tools can be used at the switch to monitor all traffic in the LAN (virtual and non-virtual)

Distributed Virtual Switch

- Hardware and software implementations
- Consolidates virtual switch management to one location
- Exposes virtual network traffic using NetFlow

Technology	VMware ESX/ESXi	Microsoft HyperV	XenServer	Documented/ Supported*	Additional Security
Open vSwitch	✗	✗	✓	**Well**	
HyperV Virtual Switch	✗	✓	✗	**Well**	**ARP/ND Poisoning Protection DHCP Guard**
VMware vSwitch	✓	✗	✗	**Well**	
Virtual Ethernet Port Aggregator(VEPA)**				**Very Poorly**	
Cisco VM-FEX	✓	✓	✓	**Well**	
Cisco VN-Link / Cisco Nexus 1000v ***	✓	✓	✗	**Very Well**	**Virtual Security Gateway**
VMware Distributed Virtual Switch (DvS)	✓	✗	✗	**Very Well**	**Port Mirroring Traffic Filtering**

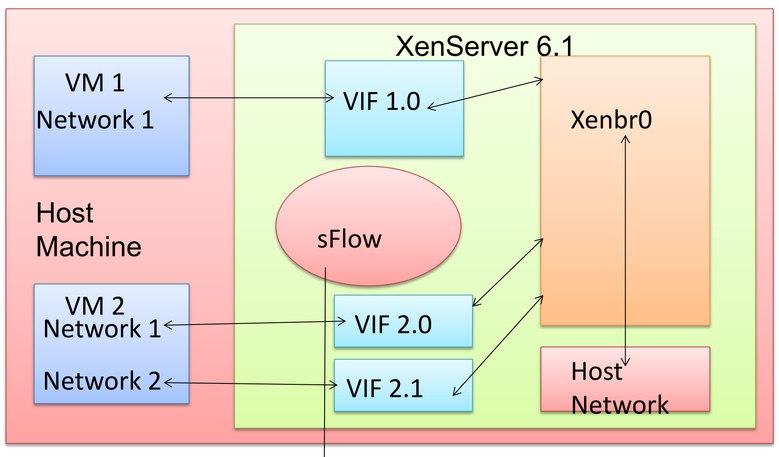
* Based on the opinion of the research team after literature review was performed.

** The VEPA standard has in essence been abandoned by industry. There is little documentation outside of the IEEE standard.

*** Cisco has both hardware and software implementation of the distributed virtual switch technology. The Nexus 1000v is the software implementation, and VN-Link is the software implemenation

Open vSwitch Testing:

Setup



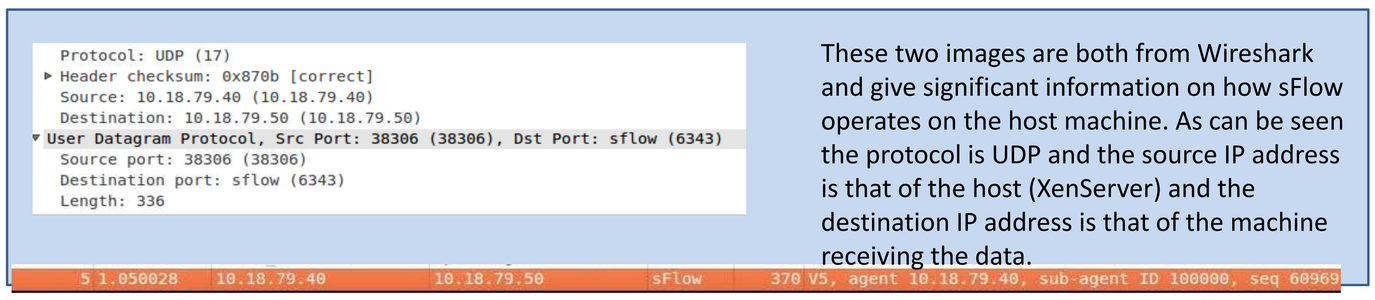
- Open vSwitch manages the physical hosts network through xenbr0
- Open vSwitch also controls the VM's individual networks through proxies called VIF's(Virtual Interface)
- There are two programs that allow traffic monitoring, a "transmitter" such as sFlow, and a "collector" such as Wireshark

Observations

- On XenServer Open vSwitch was easy to implement due to it being a default switch for the host
- Multiple options besides sFlow, sFlowTrend, and Wireshark to transmit and analyze the data
- sFlow is simple to install but it transmits the data through UDP packets
- This wrapping of the data obfuscates much of the information such as source IP address

Results/Conclusions

- Hardware off-loading solutions are potentially very difficult to implement, costly, and there is little documentation on them.
- Open vSwitch and software solutions are easier to implement, have minimal costs, and there is significant documentation on them.
- Recommendation is to use Open vSwitch along with whichever tools you are most comfortable with or that affords you the amount of detail you want to analyze on the network.



These two images are both from Wireshark and give significant information on how sFlow operates on the host machine. As can be seen the protocol is UDP and the source IP address is that of the host (XenServer) and the destination IP address is that of the machine receiving the data.

"This material is based upon work supported by the National Science Foundation under grant #1062970. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation."

PURDUE UNIVERSITY