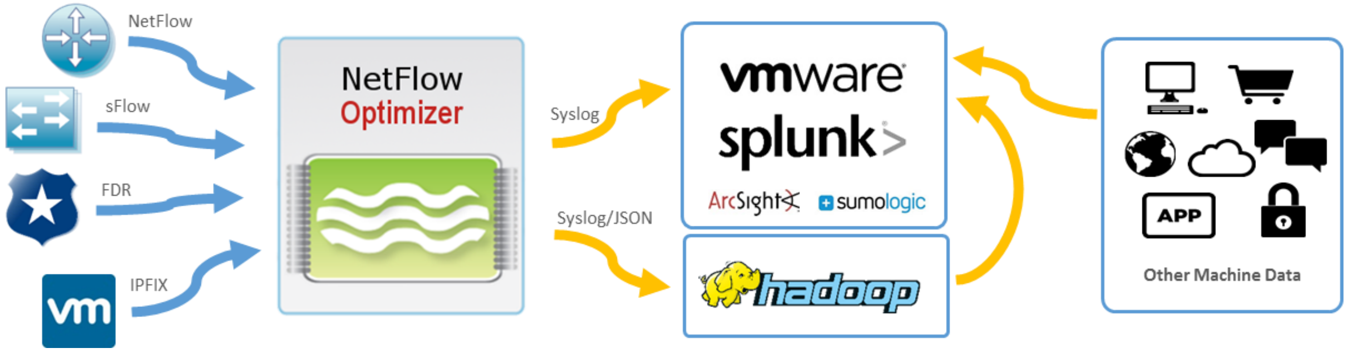
SOLUTION OVERVIEW

Real-time Operational Intelligence for Virtual & Physical Networks

Network devices are rich sources of information about the network's traffic, in the form of NetFlow, sFlow, J-Flow, or IPFIX formats.

This metadata is voluminous and most valuable for operational and security purposes. You get the best insights when the data are captured and analyzed in real time. This is where the data processing engine in NetFlow Optimizer comes in. It can process hundreds of thousands of these records per second. Users can apply a myriad of solutions to understand the health and robustness of their networks, as well as the imminence of security threats. The results of NetFlow Optimizer processing and analytics are then visually displayed via Splunk Enterprise, VMware vRealize Log Insight, Sumo Logic, or other systems.



Most network management tools use LLDP or CDP protocols (designed for topology discovery) to reveal network device connectivity, and do not identify the actual network traffic. On the other hand, NetFlow Optimizer's analytics are based on real network traffic. A useful analogy: if you are driving within a city, a city map will be helpful. However, it is much better to have both a map and a depiction of the traffic congestion, so you can navigate more efficiently.

SDDC vs. Physical DC

One of the biggest operational concerns for IT Operations and SDDC Administrators is the lack of visibility between the virtual and physical networking layers -- how to trace and troubleshoot connectivity issues. Typically, SDDC management tools monitor virtual network devices, such as vSphere Distributed Switch (VDS), Distributed Logical Routing, Distributed Firewall, Edge Services Gateway, and others. What if a performance degradation or outage is caused by physical device failures or overloading?

How do we know where virtual network traffic is encapsulated, and how it traverses the physical network?

Legacy tools break down at the virtual to physical boundary. Lacking correlation between logical and physical networks leads to longer time to resolution, and unacceptable outage time frames for many customers.

For complete visibility you need to collect and analyze flows from both virtual and physical devices. Luckily, most vendors support some sort of flow generation technology (Cisco - NetFlow, Juniper – j-Flow, Dell, HP, Arista, Brocade – sFlow, VDS - IPFIX).

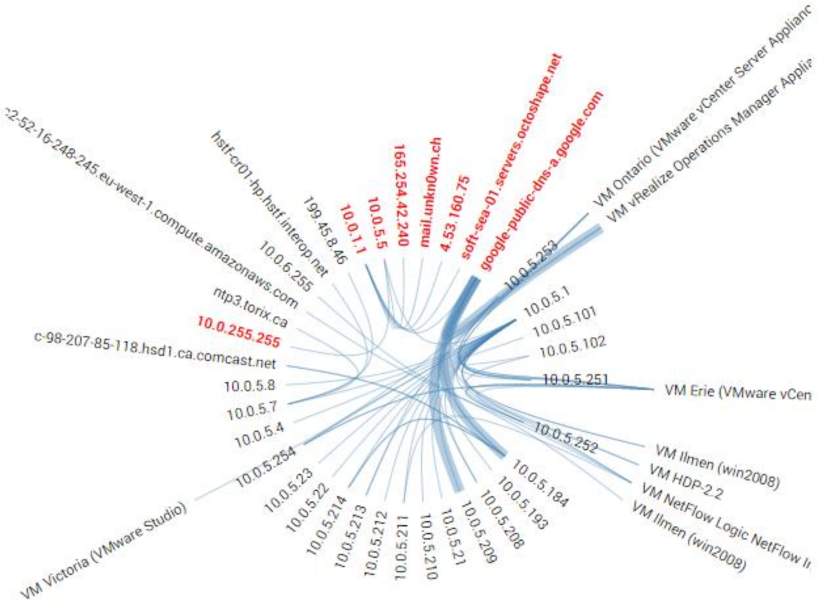
Configure all of your flow-capable exporters, such as Top of Rack switches, core and aggregation switches, routers, and virtual switches (e.g. as VDS or Open vSwitch) to send NetFlow/sFlow/J-Flow/IPFIX to NetFlow Optimizer for complete visibility of your virtual and physical networks.

Application Connectivity

It is common for an operational support team to spend 90% of its time trying to figure out what is going wrong with the applications. Is it an application-related problem, a server-related problem (CPU, memory), or network-related? If it is a network problem, is it caused by misconfiguration in the virtual overlay network, or outages / overloads of the underlying physical network? This dilemma often creates friction between teams responsible for supporting the company’s IT infrastructure.

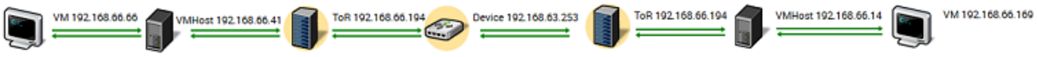
Which applications / VMs are impacted by physical network outages or overloads?

The following diagram is a depiction of the end-to-end communication between VMs, and VMs to gateways. When there is a problem in the path between them, they are highlighted in red to pinpoint issues related to the physical layer of the network e.g. network port down, over utilization of capacity, etc.



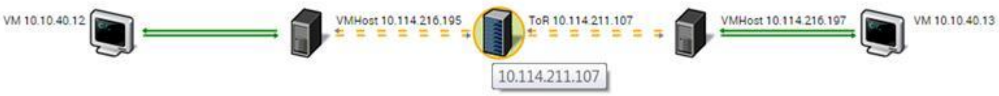
Network Path

Now that applications and hosts impacted by physical network outages are identified, an SDDC administrator can select end nodes to view where VM to VM traffic is encapsulated, and can see specifically which physical network devices the traffic went through.



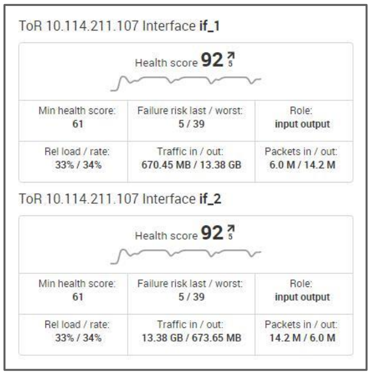
Now SDDC administrators can pinpoint which of the network devices in the path are a cause of application performance problems.

The following image shows network device interfaces involved in VM to VM communication.



For interfaces relaying a traced communication the following information is presented:

- Relative traffic load on this interface as a percent of its nominal capacity
- Relative packet rate on this interface as a percent of a maximal packet rate sustainable at a current average packet size
- A total number of bytes passed in each direction through this interface over a selected time interval
- A total number of packets passed in each direction through this interface over a selected time interval



ToR 10.114.211.107 Interface **if_1**

Health score **92** ↗ 5

Min health score: **61**	Failure risk last / worst: **5 / 39**	Role: **input output**
Rel load / rate: **33% / 34%**	Traffic in / out: **670.45 MB / 13.38 GB**	Packets in / out: **6.0 M / 14.2 M**

ToR 10.114.211.107 Interface **if_2**

Health score **92** ↗ 5

Min health score: **61**	Failure risk last / worst: **5 / 39**	Role: **input output**
Rel load / rate: **33% / 34%**	Traffic in / out: **13.38 GB / 673.65 MB**	Packets in / out: **14.2 M / 6.0 M**

The Path information is available not only for VM to VM (East-West traffic) within the data center, but also for VM to gateways (North-South traffic). This capability is useful in identifying network congestion and abnormal activity such as data exfiltration.

System Requirements

Hardware/Virtual Appliance

16GB RAM, 8 Cores CPU, 20 GB disk space.

Virtual Appliance

VMware ESXi 5.x and above

Operating System

Linux CentOS 5.5, 6.5, 7 – Debian 6 – RHEL 5.5, 6.5, 7 – SUSE ES 11 (kernel 2.6+ 64-bit)
Windows Server 2008 R2, 2012, and 2012 R2 (64-bit)

Contact NetFlow Logic
Website: www.netflowlogic.com
Email: info@NetFlowlogic.com
Phone: +1 (650) 308-8887