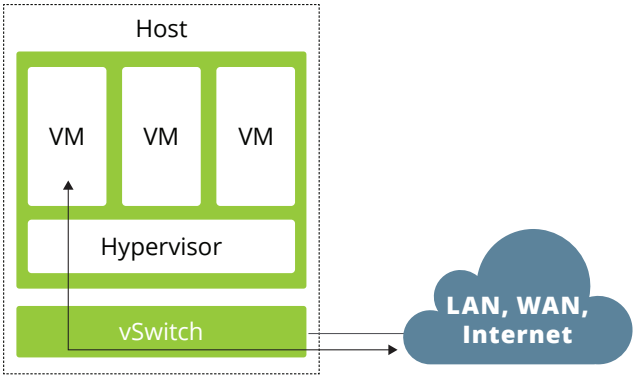
Visibility into Virtualized Networks and Applications

In traditional networks, monitoring can be achieved with high visibility by the use of physical switch mirror (SPAN) ports, network TAPs, and network packet broker (NPB) or packet flow switch (PFS) devices. If high reliability and full visibility of the traffic to the monitoring tools is required, then network tapping is greatly preferred over mirror ports. This layer of TAPs and NPB/PFS is then used to forward all or just some of the copied network traffic to select tools for analysis, recording, and presentation.

However, with the advent of virtualization in Enterprise datacenters, and Network Function Virtualization (NFV) occurring in Service Provider central offices and datacenters, where and how to access the traffic is NOT necessarily as clear or obvious.

Virtualization

In the case of virtualized services and applications, accessing the traffic is not necessarily always straightforward, since the traffic flowing between two applications (or endpoints) may never leave the virtualized machine environment (VME), and the applications themselves may move from one virtual machine (VM) to another (known as vMotion – although this may be a rare[1] event), within the same location or to a different physical location, resulting in changes to the traffic's origination and destination parameters. Only the hypervisors within these virtual environments have visibility into these movements. NPB/PFS solutions need to be able to support access to and continuous forwarding of targeted traffic, from environments that have virtualized applications and virtualized network links, to the monitoring tools.

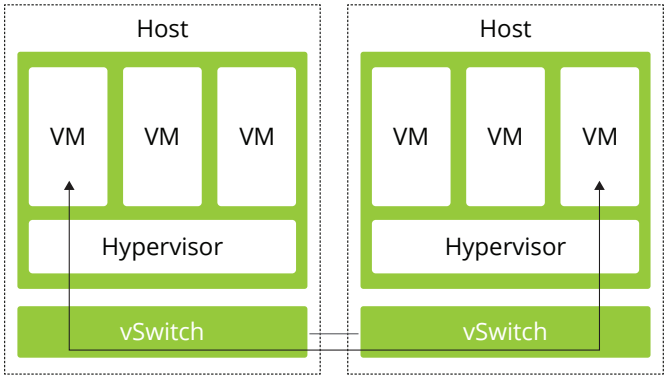


Use Case 1: To/From VMEs

Use Cases

There are essentially three types of situations or cases that may require three different approaches to traffic access for monitoring of traffic in virtual machine environments (VMEs). In practice, there can even be a situation made up of a mix of two or all three cases.

In networks where VMEs are serving the wider network, such as consumer end-users, all traffic is to/from the wider network, and hence always travels over a physical network.



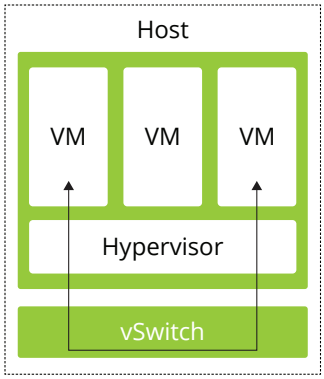
Use Case 2: Within Distributed VMEs

In networks where the VME is built around a distributed virtual switch, typically all traffic between the virtualized applications passes over a physical network between the distributed elements of the virtual switch (vSwitch). Depending on which vSwitch is being used, some kind of tunneling/tagging protocol is typically employed for the traffic between the distributed vSwitch elements, e.g. VN-tag for Cisco Nexus vSwitches.

Smaller VMEs, where the traffic passes between virtual applications only within the same self-contained VME server or server rack, the traffic remains within the host.

This situation may even exist when certain large volume traffic types traverse a physical network link, and other lower volume traffic (e.g. control elements in a network) passes between virtualized applications within the same self-contained VME.

1. Our research, to-date, indicates that vMotion is a quite rare event, and so does not need to be a focus at this time for traffic capture.



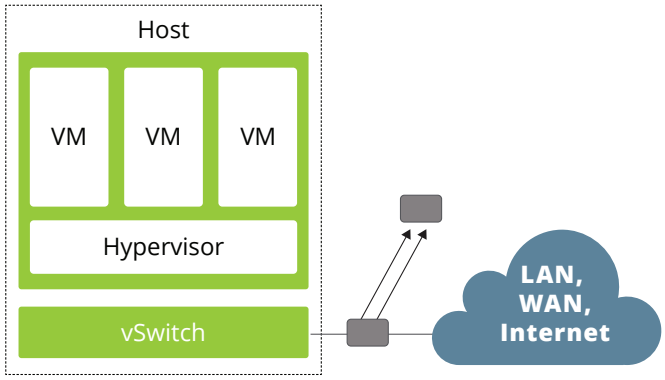
Use Case 3: Within VMEs

Addressing the Challenges

Since in a real network, all three situations may exist in some mix, it may be required to deploy a combination of all the following approaches to address the need for traffic access and visibility.

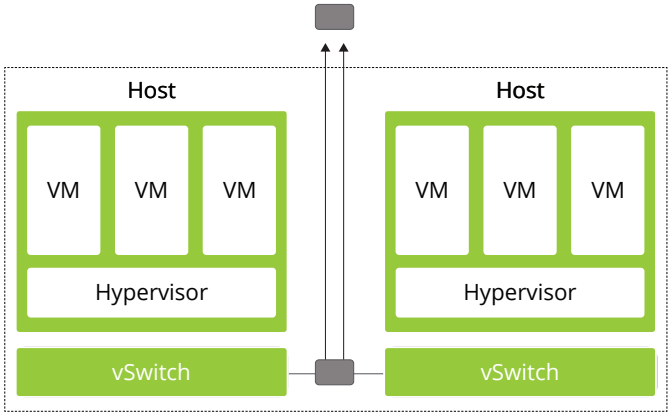
To/From VMEs

For this situation, it is best to use passive network TAPs (e.g. NETSCOUT's HD Fiber TAP) to get a copy of the traffic from the physical link. The traffic would look and be handled just like traffic between non-virtualized environments, and so feed from the network TAP into a PFS (e.g. from NETSCOUT) to be forwarded to the appropriate monitoring tools. This approach protects both servers and network since traffic processing occurs outside the servers and off the network. Within VMEs



Within Distributed VMEs

In this situation, it is also best to use passive network TAPs to feed into a PFS. The PFS can then remove/strip off the tagging or encapsulation that only exists within the virtualized network and therefore accommodate many tools not designed to understand or handle them. For example, the PFS could strip VN-tags and VXLAN headers.



Within VMEs

Monitoring traffic within VMEs requires a different approach since traffic is inaccessible to TAPs and SPANs. The best approach involves using the Hypervisor and vSwitch capabilities to forward a copy of the traffic of interest. Specifically, virtual NICs and virtual SPAN ports direct the traffic in one of the three ways described below. The selection of a method depends on several factors, such as physical configuration of the virtual servers, relative traffic volume outside vs. inside the VME, the VME owners' willingness to grant monitoring infrastructure personnel with access to the hypervisor and/or virtual switch that is not just read-only, or even their willingness to allow "foreign" 3rd party applications to be installed in the hypervisor or vSwitch for monitoring purposes.

One approach involves specialized software installed within the VME that forwards the traffic out of the VME to PFS devices and/or monitoring tools, and obtain information about movement of virtual applications. Addition of this specialized software is often prohibitive, due to the following challenges, including:

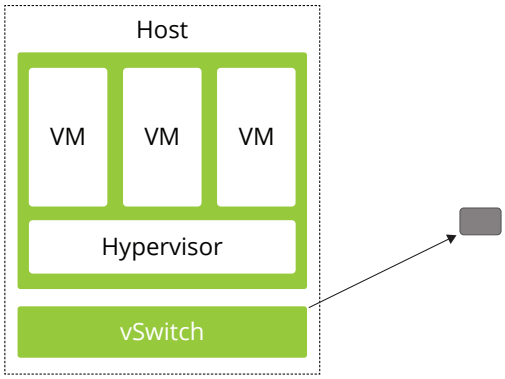
- IT organizations, who own and manage the VMEs, may not allow these invasive elements to be installed in their "clean" virtual environments
- The additional software places additional load on the available resources and the performance of the VME whose resources may be unable to accommodate the additional load

As it turns out, the current generation of VMEs includes several capabilities built into the hypervisor and vSwitch that can be leveraged to aid with traffic access and directing, without the need to develop or install additional pieces of hardware or software into each VME. These capabilities include:

- Creation and control of virtual mirror ports
- Applying filters to mirrored traffic
- Directing mirrored traffic to one or more destinations (physical NICs or IP endpoints)
- Monitoring movement of virtual applications (commonly referred to as vMotion)

Direct to Physical NIC

With this approach, traffic within the VME that passes between virtual applications through the virtual switch is directed from the vSwitch's virtual NIC/SPAN (vNIC/vSPAN) to an actual physical NIC on the vSwitch server, which is in turn physically cabled to a PFS device. This will depend on the environment and if one or more NICs are available on the physical server that houses the vSwitch.



The benefits include:

- Certain delivery of the packets to the PFS device
- No fragmentation of jumbo frames that can occur due to any encapsulation or tagging
- No additional traffic being sent out onto either the management or traffic networks
- Minimal load on the virtual environment since it is just making use of the distributed virtual switch capability of individually mirroring from selected vNICs and not having to encapsulate the traffic

The challenges are:

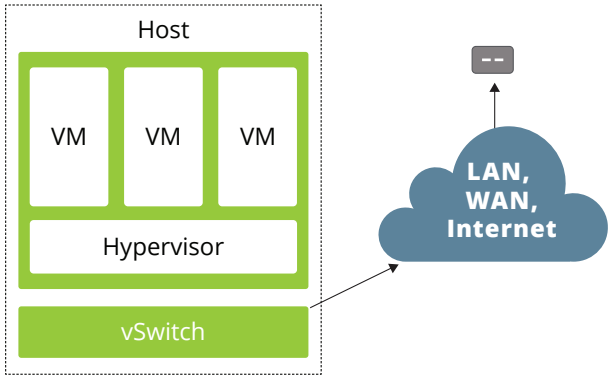
- Requires the availability of an unused physical NIC, and
- Requires privileged user access to be able to redirect packets from the vSwitch.

Tunnel to Physical Network

In this approach, packets are encapsulated and directed from the vNIC/vSPAN to a target IP endpoint with GRE or ERSPAN tunneling, or even RSPAN/VLAN. Traffic can be accessed by one of two methods:

- Using a passive network TAP to capture the traffic (targeted to a device in the network), which in turn feeds the packets to a PFS or tool
- Having the PFS or tool be the targeted GRE or ERSPAN endpoint

In both methods, the PFS or tool would need to be able to remove the tunneling encapsulation, since it bears no relation to the actual traffic that is being monitored. Although some monitoring applications may want the encapsulation retained due to the additional information contained in the tunneling headers.



The benefits include:

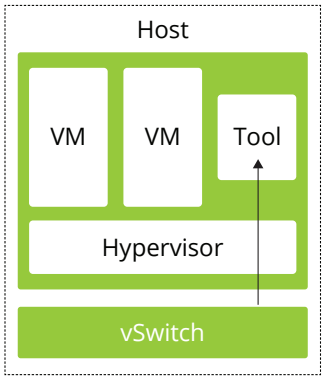
- Does not require availability of an unused physical NIC
- Traffic can be directed out over either a NIC that is being used for management or the network traffic

The challenges are:

- Uncertain delivery of the packets to the target (e.g. PFS) device due to GRE being best-effort delivery
- Jumbo frames being fragmented due to the act of encapsulating within GRE
- Additional traffic load being placed on the management or network traffic NICs and links (especially if the traffic to be forwarded is comparatively significant in volume)
- Increased load being placed on the vSwitch due to the act of encapsulation
- Requires privileged user access to be able to redirect packets from the vSwitch

Direct to Virtual Tool

With this approach, the monitoring tool is also virtualized, running on a VM, and similar to the Direct to Physical NIC approach, the traffic copied at the vNIC is directed to the VM that the monitoring tool is installed and running on.



The benefits include:

- Certain delivery of the packets to the virtual tool
- Jumbo frames not being fragmented due to no encapsulation or tagging
- No additional traffic being sent out onto either the management or traffic networks
- Minimal load on the virtual environment since it is just making use of the distributed virtual switch

- capability of individually mirroring from selected vNICs and not having to encapsulate the traffic
- The traffic is being forwarded directly to the tool

The challenges are:

- Amount of traffic being forwarded to the virtual tool may exceed that tool instance's throughput or capacity therefore requiring a balancing function
- Requires privileged user access to be able to redirect packets from the vSwitch
- Places additional load on the vSwitch which affects performance

NETSCOUT Solutions

Today

NETSCOUT offers a number of alternative solutions, for both physical and virtual approaches

Physical Tapping

This can be used to address the need to access traffic in both "To/From VMEs" and "Within Distributed VMEs":

Deploy 10/100/1000 Copper and HD Fiber TAPs for tapping the physical links that are carrying the traffic to/from the servers that house the VMEs. The TAPs generate a copy of all the network traffic on the link

- Traffic can be fed directly to a monitoring probe, such as an InfiniStream appliance, but more likely it will be fed to a PFS for optimizing delivery of the traffic to the tools
- If virtual tunneling protocols (e.g. VN-tagging within a Cisco Nexus vSwitch) are present from tapping links within a Distributed VME, then the PFS can be used to strip off those virtual network tunneling protocol headers that would not otherwise exist in a non-virtualized physical network and that the applications being monitored also never see. All NETSCOUT PFS products support this capability, while InfiniStream appliances with powerful Adaptive Service Intelligence (ASI) can analyze packets without need for de-encapsulation.
- Any of PFS 2204, PFS 4204, PFS 3901, PFS 3903, or PFS 6010 can be used to optimize the traffic and delivery to the InfiniStream appliances or other monitoring tools

Virtual Tapping

This can be used to address the need to access traffic "Within VMEs":

- Receive passive copies of traffic from between virtual machines, using virtual mirror/SPAN ports within the VME that can direct the traffic leveraging the virtual switch built-in capability to create virtual mirror/SPAN ports, and send:
  - Directly to a virtualized tool (e.g. InfiniStream virtual appliance) running on a VM in the VME
  - Directly to a physical NIC which would have a PFS connected for forwarding along with other traffic to an InfiniStream appliance or other monitoring tools
  - Tunneled (using GRE, NVGRE, or ERSPAN) to either a PFS or tool (e.g. InfiniStream) acting as an tunnel endpoint
- Set up the mapping from the virtual NICs to either virtual tools or physical NICs, using the hypervisor UI or API (e.g. VMware's vCenter)

Any of PFS 2204, PFS 4204, PFS 3901, PFS 3903, or PFS 6010 can be used to optimize the traffic and delivery to the InfiniStream appliances or other monitoring tools.

The PFS 6010 can be used as a GRE, NVGRE, or ERSPAN tunneling endpoint, and any of PFS 2204, PFS 4204, or PFS 6010 can be used to selectively de-encapsulate the tunneled traffic.

Future

Moving forward, NETSCOUT has a well thought out plan for expanding its current capabilities and adding new capabilities to keep up and evolve with the industry.

Summary

It is clear that virtualization in the network will continue to grow, but it certainly won't be overnight, and in no way will it curtail the need for NPB/PFS systems to be deployed for monitoring networks.

NETSCOUT solutions already today provide a number of virtual network access methods for network intelligence appliances. Telecom providers, enterprises, and government agencies make use of these virtualized network access methods to improve the visibility and optimization of their network performance and security tools.

Each customer's needs are different, i.e. one size won't fit all, and the largest need will be the ability to support hybrid (i.e. both physical and virtualized) environments in a single PFS system-based solution that can scale. Needs differ somewhat:

- Between telecom service providers and enterprises and government agencies
- As driven by application performance, network performance, and network security focused tools

Key things to look for in a PFS system, as it relates to virtualization, are:

- Future-proof upgradability
- An overall system architecture that can scale

NETSCOUT is committed to delivering innovative solutions to support virtualization of the network as these technologies mature and take hold in our customers' networks.

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000