# *Virtual Switch Security - An Overview*

**Andrea Covello**
Defense Department, scip AG
anco@scip.ch
https://www.scip.ch

**Marc Ruef (Editor)**
Research Department, scip AG
maru@scip.ch
https://www.scip.ch

Keywords: API, Backup, Cisco, Cloud, Detect, Firewall, Framework, Hardening, iOS, IPsec

## 1. Preface

This paper was written in 2013 as part of a research project at scip AG, Switzerland. It was initially published online at *https://www.scip.ch/en/?labs.20130919* and is available in English and German. Providing our clients with innovative research for the information technology of the future is an essential part of our company culture.

## 2. Introduction

Virtualization and cloud environment are a *clear and present danger* for all ICT people involved in security and operation. Boundaries are dissolving and not only for the physical boxes that used to host several machines. In fact also the things that used to connect them together are vanishing into the virtualization layer. I'm talking here not only of the network interfaces, but also of the cables that were used to patch it to a switch port and the switch itself.

*Virtual switches* manage and route traffic in a *virtual environment*, but often network engineers don't have direct access to these *vSwitches*. Often vSwitches that are inside the hypervisors don't offer the type of visibility and management like the physical box do.

Meanwhile there are alternatives to the standard vSwitches inside the hypervisors and we like to here to have a short discussion about the vSwitch functionalities and its inherent contribute to network security (for the god and for the bad).

## 3. vSwitch Impact on Networks

In a virtualized environment, the network's access layer is embedded into the hypervisor and internal vSwitches manage the packet traffic. Traditional physical switches determine where to send message frames based on *MAC addresses* on physical devices. vSwitches act similarly in that each virtual host must connect to a vSwitch the same way a physical host must be connected to a physical switch.

A closer look reveals quite differences between physical and virtual switches. On physical switches when a dedicated network cable or port goes bad, only one server is affected. With virtualization, one cable could offer connectivity to 10 or more virtual machines, causing a loss in connectivity to multiple VMs.

On the other end, connecting multiple VMs requires more bandwidth, which needs to be handled by the vSwitch. These differences are especially evident in larger networks with complex designs, like the ones needed for infrastructure across data centers or for disaster recovery sites.

Standard vSwitches are manually configured and managed per hypervisor, major misconfigurations or errors can be implemented by an administrator or network engineer without a solid understanding of virtualization and hypervisor management.

## 4. vSwitch Types and Features

The hypervisors internal basic vSwitch has a straightforward management interface, and supports all the basic features needed to operate a virtual network. Meanwhile, to help facilitate the move to virtualization in the datacenters, vendors developed technologies to increase the functionality of the vSwitch inside a hypervisor. They introduced additional cost and a more intricate management interface, but also provides access to advanced switch features and ensures a deeper level of security.

Advanced switch features requires an extended layer of network virtualization to provide support over several hypervisors and network devices. The solution is named *Distributed Virtual Switch* and is comprised of:

- a control module and
- a virtual Ethernet or switch module,

which work together with other components of the virtual environment to ensure smooth data transfer as showed in the image below:

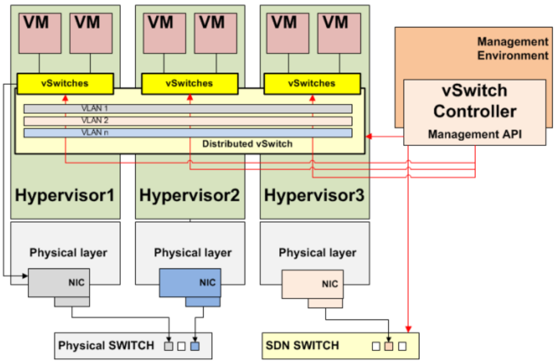

Figure: vSwitch Architecture

Following is a table with some of the most common vSwitch solution available today:

| Vendor | Components | Description |
|---|---|---|
| Cisco | Nexus 1000V | It's a replacement vSwitch for ESX that gives the network back to the network operations team. |
| Nicira Networks | Open vSwitch Project | The project provides downloadable open source code for the open source virtual switch. It currently supports Xen, XenServer, KVM and VirtualBox but can be ported to other virtualization environments. |
| VMware | DVS (Distributed Virtual Switch) | It's a vSwitch that spans its ports and management across all ESX servers in the cluster. |
| VMware | NSX | Just recently VMware – with the acquisition of Nicira Networks – implemented the Open vSwitch capabilities inside the new ESXi 5.5 hypervisor. Together with a control framework inside the vSphere solution it has been named NSX. This should replace the VDS feature in the near future. NSX has also capabilities to configure physical network switches that support its API calls, making possible to manage the complete network environment as known under the acronym SDN (Software Defined Networking) |

All of these switches support *802.1Q tagging*, which allows multiple VLANs to be used on a single physical switch port to reduce the number of pNICs needed in a host. This works by applying tags to all network frames to identify them as belonging to a certain VLAN.

### 5. vSwitch General Issues

Networking teams often loose control over management in a virtualized environment. In fact, virtualization can introduce new networking challenges like:

- Limited network traffic visibility in virtual network switches
- Inconsistent network policy enforcement (the need for new kinds of network policy enforcement)
- Poor management scalability and often manual vSwitch and network reconfiguration
- Limited I/O bandwidth (for example: capacity problems due to VM migration)

Beyond technical challenges, virtualization can also cause organizational issues between virtualization and network administrators. Many of these issues are caused from the fact that traffic between VMs on the same host never leaves the server to run over the physical network, making it difficult for networking teams to monitor or manage this traffic. Lack of visibility also means that network firewalls, QoS, ACLs and IDS/IPS systems cannot see this data transfer activity over the physical network.

What's more, both the standard and distributed vSwitches do not have features that lend themselves to easy management. Administrators only have control of the uplink ports from the physical NICs in the host and not the numerous virtual ports that exist on a vSwitch. To address these issues, networking teams are turning to new network management and security product specifically designed to secure, monitor and control virtual network traffic on a host. Below is a list of such solution available today:

- VMware vShield (now called vCNS and stands for vCloud Networking and Security)
- Cisco Virtual Secure Gateway (VSG)
- Juniper Virtual Gateway (vGW)
- Reflex System's Virtual Management Centre
- Altor Networks' Virtual Firewall
- Catbird's vSecurity

Now let's take a closer look to some of the features available in two of the most used distributed vSwitch flavors: The Cisco 1000v an the Open vSwitch (which speaks also moslty for NSX).

### 6. Nexus 1000v

Here is an overview of the features on the Cisco 1000v virtual switch solution:

| Components | Description |
|---|---|
| Cisco NX-OS Interface | It offers the well-known Cisco IOS command line interface to manage virtual networking. |
| Traveling Port Profiles | Security and network properties are tied to a VM's port profile. As that VM moves from server to server with VMotion, that port profile follows it. This way, security policies can be enforced on VMs just as they can be enforced on physical servers. |
| Advanced Cisco NX-OS Features | Quality of Service (QoS), rate limits, continuous data protection, switched port analyzer, NetFlow, VLANs, and port channels |
| NX-OS Security Features | port security, authentication authorization and accounting (AAA), access control lists |
| Optional VSG Module | You can add the VSG module for statefull inspection firewall functionality as a separate licensed feature. |

### 7. Open vSwitch (NSX)

Here is an overview of the features on the Open vSwitch (OVS) solution:

| Components | Description |
|---|---|
| Visibility into inter-VM communication | via NetFlow, sFlow, IPFIX, SPAN, RSPAN, and GRE-tunneled mirrors |
| Advanced switch capabilities | LACP (IEEE 802.1AX-2008), standard 802.1Q VLAN model with trunking, a subset of 802.1ag CCM link monitoring, STP, fine-grained QoS control, IPv6 support |
| Per VM Interface Traffic Policing | Security and network properties are tied to virtual switch port profile. |
| NIC Bonding | With source-MAC load balancing, active backup, and L4 hashing. |
| Advanced Management Control | Supports OpenFlow protocol with many extensions for virtualization. |
| Multiple Tunneling Protocols | Supports GRE, VXLAN, IPsec, GRE and VXLAN over IPsec. |
| Security Features | Port filtering |

Please note that while the OVS and the Nexus 1000v are basically a system in a VM solution, the NSX has it's code embedded inside the hypervisor (ESXi) code. And this makes a big difference

### 8. vSwitch Security Recommendations

Security is also an important issue using vSwitches and to conclude this overview hare are some hints in help securing your virtual environment:

| Recommendation | Description |
|---|---|
| vSwitches are still made of code | Be prepared to failures that may lead to DoS or isolation failures. |
| Segregate your (virtual) network | Isolate the management traffic from the network stream used for the virtualized machines, this is one of the key issue you should address. The vSwitch control instance uses API calls to configure the vSwitch Ethernet modules, this traffic need to be secured like any other management access. |
| Implement Hardening | Apply vendor recommended hardening procedure. |
| Activate vSwitch security features | Most vSwitch default configuration are not secure. Activate port security, implement policy on the VM switch ports, deactivate promiscuous mode, detect and reject MAC forgery, enforce VLAN separation with control modules. |
| Use strong authentication | Distributed virtual switches like the Nexus 1000v supports AAA allowing a Radius or Tacacs+ authentication, using this in conjunction with a OTP token will greatly minimize the risk of unauthorized access. |
| Use advanced security modules | Especially if you have to deal with different security zones, use advanced security modules like the one listed above. |

I hope this overview gave you some hint on how to approach security in your virtual networking environment.