Leveraging SDN Capabilities for Securing Virtual Networks

Dr. R. Chandramouli (Mouli)
mouli@nist.gov

(Information Technology Lab, NIST, USA)

(Slides for Discussion in IEEE SRPSDVE Study Group)

Dec 8, 2015

Leveraging SDN Capabilities for Securing Virtual Networks

- Virtual Network - Context
- Components of Virtual Network inside a Hypervisor (H-VN)
- Current Security Solutions for H-VN
- How can SDN Capabilities be leveraged for securing H-VN
- **VLAN Configuration Automation using SDN-enabled Virtual Switches**
- **Implementing Sophisticated Firewall Rules using SDN-enabled Virtual Switches**

Virtual Network - Context

- Current Trend in Server Virtualization is well established
- A Virtualized host hosts the hypervisor software and multiple Virtual Machines (VMs)
- The software-defined communication fabric inside the virtualized host defined using the hypervisor management interface is the Virtual Network (H-VN) in our context
- H-VN links the multiple VMs in the virtualized host to each other and to the enterprise network through the physical NICs of the virtualized host

Components of Hypervisor-based Virtual Network (H-VN)

- Software-defined Virtual Network interface cards (vNICs) for each VM
- Software-defined virtual switches (vSwitches) that provide the switching fabric for H-VN
- Physical Network Interface cards (pNICs) of the Virtualized host

Common Security Solutions for H-VN

- Segmentation of H-VN using VLANS – *H-VN-SS1* (**VLAN Configuration**)
- Traffic control into individual VMs using hypervisor-level firewall run as Virtual Security Appliance on a privileged VM and uses the Introspection API of the hypervisor –*H-VN-SS2* (**Running Firewalls as a VSA**)

VLAN Configuration Automation using SDN-enabled Virtual Switches (H-VN-SS1 Enhanced)

- Hypervisor must support the definition of Open vSwitch
- Open vSwitch is a software-based virtual switch that supports the OpenFlow Protocol (this is the Southbound Interface)
- One also needs a SDN controller that exposes an API that can be integrated with the Hypervisor Management tool (or any Virtual Infrastructure Management Server) – this API is the Northbound Interface

VLAN Configuration Automation using SDN-enabled Virtual Switches .. Contd 1

Case Study : Define a NEW VLAN (VLAN-x) for a new client or LOB (CLIENT-X): -1

- Hypervisor Management tool identifies the VM instances belonging to CLIENT-X, their locations (Virtualized Host or NODE CLUSTER) and instructs OpenFlow (SDN) controller to define the VLAN
- Controller generates the Open Flow protocol calls to Southbound Interface to create the VLAN ID on the Open vSwitches of the identified virtualized hosts.

- **VLAN Configuration Automation using SDN-enabled Virtual Switches .. Contd 2**

Case Study : Define a NEW VLAN (VLAN-x) for a new client or LOB (CLIENT-X): -2

- Controller also links the identified VMs to the VLANID ports on the vSwitches
- Thus automated configuration of VLANs using API calls eliminates the chances of errors in manual configuration & re-configuration

REFERENCE: Cloud Computing: What Changes with SDN – Secure Cloud Computing: 2014

VLAN Configuration Automation using SDN-enabled Virtual Switches .. Contd 3

Case Study : Define a NEW VLAN (VLAN-x) for a new client or LOB (CLIENT-X): -3

- The addition of this new VLANID on the external physical switch connected to the virtualized hosts can also be automated if that physical switch provides SDN support.
- Also reconnecting a migrated VM to the port on the vSwitch in the destination host can also be automated if the target vSwitch is an Open vSwitch.

Implementing Sophisticated Firewall Rules using SDN-enabled Virtual Switches

Case Study : Define firewall rules using a SDN enabled vSwitch -1

- An Openflow enabled vSwitch implements flow table
- A Flow table provides rules to match a packet based on (Source & Destination MAC, IP & TCP addresses + VLAN ID + Switch Port) to make data forwarding decision
- Thus firewall rules governing traffic into a VM can be directly implemented on the vSwitch instead of running a separate firewall as a VSA

Implementing Sophisticated Firewall Rules using SDN-enabled Virtual Switches Contd 1

Case Study : Define firewall rules using a SDN enabled vSwitch - 2

- The simple firewall rules that Flow table simulates can be enhanced using the programming logic in SDN controllers.
- A set of VMs can be assigned to a Security Groups and traffic rules can be added to the Security Groups. SDN controller can resolve these rules into Flow Table rules and implement them on vSwitches

REFERENCE : (2012) Elastic IP & Security Group Implementation using Open Flow – S.G.Rosen et al

Summary

- *Existing Security Solutions can either be enhanced or implemented in an alternate way with better security assurance using SDN enabled Virtual Switches and Integrating SDN controller with Hypervisor Management software*
- *In the case of VLAN configuration, it can be completely automated reducing manual configuration errors*
- *In the case of a firewall solution, the alternate solution using the Virtual switch reduces network traffic and makes available additional compute cycles for existing VMs*

Contact Details & Questions

- Contact Details:

  Dr. Ramaswamy Chandramouli

  Computer Security Division – Information Technology Lab

  National Institute of Standards and Technology

  (301) -975-5013 – mouli@nist.gov

- Questions (?):