Abstract

SDN and NFV have been creating paradigm shifts across major service providers, governments, and industries. In most recent months, these two novel frameworks created jitters and excitements across major academic institutions and communities of practice. While these are considered disruptive to major network infrastructures operating on status quo, SDN and NFV nonetheless bring network resiliency, scalability, manageability, and, most importantly, lower long-term operational expenditures.

They create opportunities for innovation that engage key players from networks, security, and software to develop new software controllers, APIs, networks, and technologies.

This document aims to propose a formal security architecture that overarches important aspects of SDN and NFV’s frameworks.

The architecture can be elaborated and modified as these two frameworks mature over time.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 21, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved. This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Bernardo, DV Expires March 20, 2015

Internet-Draft SDN/NFV Security Architectures September 2014

Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

1.1 Even though its concept had been around for decades, SDN did not really gain momentum until it was implemented within an academic environment in 2011. This has gained prominence since then.

In 2012, it was widely speculated that Google implemented SDN and OpenFlow into their networks, and created their own OpenFlow-enabled switches due to the limited vendors supporting this protocol.

This speculation has since gained significant interests across many industries.

To understand SDN is to look at the OSI layer, where one will find similar concepts of abstraction and separation, and tiering and layering.

In SDN, control and data planes are separated, centralizing the control and programmability of the network. APIs are Application Program Interfaces, created to connect applications on the plane.

The Northbound APIs achieve abstractions to the top of the framework while the Southbound APIs do the same at the bottom of the framework. East and westbound APIs, which are formally introduced in this draft, can be used for horizontal communications across devices, systems, or software on a given plane. To put it simply, the northbound and southbound APIs are used for vertical connections, while the east and westbound APIs are for horizontal connections.

The application tier hosts business applications and application-based security systems. The control plane composes controllers, where routing and security policies are implemented. The data plane is basically the infrastructures composing network devices, routers, switches, and security devices.

Each plane can be virtualized as and when needed. Initially, it targeted campus, data centre and cloud, but eventually adapted by service and network providers.

1.2 What is NFV

On the other hand, NFV, which was formalized in 2012, relocates network functions from dedicated hardware appliances to generic servers. It was initially intended for routers, firewalls, and gateways, but can be expanded to include load balancers and other intermediary devices.

Unlike SDN, NFV does not have a specific protocol. Both SDN and NFV create open innovation by third parties, reducing capital and operational expenditures.

2. Security Risks

The creation of SDN/NFV is undoubtedly based on the existing traditional networks. The defined goals are focused on either the enhancement of existing network designs or innovation, building new infrastructures from scratch as part of the green field strategy or moving traditional infrastructures to SDN (i.e., Brownfield) with a mixture of frameworks (hybrid).

This novel creation brings new perspectives on how to effectively manage infrastructures that are beneficial to the businesses' bottom lines, while supporting a significant increase of traffic engineering requirements.

Subsequently, since the design is based on the traditional networks in terms of design, the risks associated with the traditional networks are inherited by the new frameworks. It is therefore important to evaluate risks according to best practices, whenever available. However, SDN/NFV best practices are limited to date, due to the lack of extensive industry-based use cases surrounding security and risks.

SDN and NFV, like any new frameworks, have new security risks that need to be addressed. For example, the issues surrounding the absence of standards in the development of northbound APIs, including limited information about the east and westbound APIs, raise potential risks - especially when they are open to third-party development, where almost everyone can participate in an open-source software development for SDN controllers, orchestrators, and applications, and can design the systems whenever he/she likes without functional and security considerations put in place.

Certainly, the need to identify the risks when implementing SDN is equally paramount to achieving resilient and secure infrastructures.

- The following are the risks identified on SDN/NFV based on the traditional network designs.
  - Adversarial traffic flows - traffic passing through network devices, interfaces, and hosts.
b. Attacks on vulnerabilities in network devices - not updated patch and version

c. Attacks on vulnerabilities in orchestrators and administrative servers - unsecure servers, lacks security on admin profile
d. Attacks on control plane communications - single point of failures, unreliable controllers and unsecure connections

e. New risks associated with SDN/NFV implementations are identified, and are as follows:

f. Attacks on SDN controllers - unreliable software APP/SDN controller

f. Attacks on Southbound interfaces - exposed interfaces
g. Unsecure openflow traffic - unencrypted/unsecure traffic

h. Unreliable North/East-West APIs - unreliable software installed across the same broadcast domain

i. Vulnerable Programming models - inadequate security involvement in the Software Development Lifecycle

3. Security Mitigations

A few have been identified that must be considered when implementing SDN/NFV.

j. Hypervisors must be secure

k. Controllers must be secure

l. Hardening OS security

m. Extensive API validations

n. Extensive APPs penetration tests

o. Monitor traffic

p. Protocol must be secure

q. Session establishment protocol for communication and traffic flow must be secure

r. Multiple authentication

s. Limited time options for messaging

t. Network devices must be secure

u. Separation/segmentation of networks and subnets

4. Security Architectures

4.1 Practical Security Architecture

---

Application Security

Application Plane

[Security]

VMs

APPS

VMs

+-----+<----- Extensive

| Monitoring |

(v,n,m) Validations

[SSL/TLS, SSH/HTTPS]

Governance

+-----+<----- Extensive

(q) BEST Practices

Control Plane Security

Control Plane

[Security](k)

SDN Controllers

(u)

West API

---

(SSH/HTTPS, PCE, GMNP)

SouthBound API

| Monitoring | Secure

(v,q) Connections

Data Plane

| [Security] (l)
4.2 Enterprise Security Architecture

This document does not require any action from IANA.

7. Security Considerations

All components discussed in this draft paper have their own specific security requirements that MUST be considered.

The enterprise security architecture and its underlying considerations for SDN and NFV are presented here.

8. Acknowledgements

9. Normative References


Author’s Addresses

Danilo Valeros Bernardo
Sydney, Australia.
Email: bernardan@gmail.com