Network Working Group H.Rafiee
INTERNET-DRAFT D. Zhang
Intended Status: Informational Huawei Technologies
Expires: April 27, 2015 October 27, 2014

Analysis of Existing Work for I2NSF
<draft-zhang-gap-analysis-00.txt>

Abstract

This document analysis the status of the arts in industries and the existing IETF work/protocols that are relevant to I2NSF.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document has two purposes ? analyzes Network Virtualized Function (NFV)/ Software Defined Network (SDN) status of the art in industries (security architectures) to compare available features, and analyzes the existing IETF work/protocols that are relevant to I2NSF. The result of this work can assist to understand the status of the arts and understand the requirements for the features that need to be standard (or addressed during standardization) because of possible interoperability and orchestration of the services among different players.

One of the I2NSF goals is to develop application or user oriented policies (or the descriptors) of the network security functions that clients can request and query from 3rd party providers. Another goal is to have proper mechanism to carry the policies between clients and providers.

There are many network security functions being deployed and new ones are popping up with business and application demands. In order to have a concrete context for the protocols discussion, we start with the following network security related functions:

- Firewall

- DDOS/Anti-DOS

- Access control/Authorization/Authentication

- Remote identity management

- Secure Key management

- Intrusion Detection System/ Intrusion Prevention System (IDS/IPS)

It is envisioned that clients of the I2NSF interfaces include management applications, service orchestration systems, network controllers, or user applications that may solicit network security resources.

Various aspects to I2NSF include:

* The mechanism for clients (applications) to request/negotiate/validate security functions those are not physically located on the local premises,

* The mechanism for creating virtual security functions on physical appliances, and

- Application/user oriented rules/policies to instantiate virtual security functions as VMs on common compute servers (NFV initiative).

The objective of the proposed work is to standardize the protocols (or the interface) and architecture for Requester and Provider to negotiate the functions needed as well as the associated attributes.

The proposed protocols between requester and provider can be used for the following scenarios:

* A Client requests a certain network security function from a provider

* The provider fulfills the request for example, by instantiating an instance of the service in question, or configures an additional rule in an already provisioned service.

2. Conventions Used In This Document

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 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC 2119 significance.

- Cloud DC: The data centers that are not on premises of enterprises yet have the compute/storage resources that can be requested or purchased by the enterprises. What the enterprises actually get is Virtual Data Centers.

- DC: Data Center

- Domain: The term ?Domain? in this draft has different connotations in different scenarios:

- Client <-> Provider relationship, i.e. client requesting some network functions from its provider;

- Domain A <-> Domain B relationship, i.e. one operator domain requesting some network functions from another operator domain; or

- Applications <-> Network relationship, i.e. an application (e.g. cluster of servers) requesting some functions from network, etc.

- Virtual Security Function: a security function that can be requested by one domain but may be owned or managed by another domain.

- Cloud-based security functions: used interchangeably with the ?Virtual Security Functions? in this draft.

- NBI: Northbound Interface. ?Northbound? can be ambiguous because ?northbound? to entity A can be southbound to entity B. So we try to avoid using ?northbound? in I2NSF.

3. Analysis of NFV Status of the Arts in Industry

Network Function Virtualization (NFV) provides the service providers with flexibility, cost effective and agility to offer their services to customers. However, there might be different trends or policies to offer the services to end users. This might prevent end users to receive services from different service providers because of no possible interoperability between the service providers. It might also confuse end users to ask services from service providers. There are several players that offer provide their services to different service providers that here we only list some of them. For example, one of players focused on the mechanisms to provide orchestration between programmable networking technologies and other powerful services. Simplifying the management tasks, traffic virtualization, advanced flow control, Improved Converged Network agility, Security as a Service (deep packet inspection and Network Admission Control) and Network more programmable is some of the features. The others focus on the combination of Software Defined Network (SDN) approaches with NFV. Some of the features are flexibility in distributing over the virtual infrastructure in WAN and the use of visualized network functions (VNF), easily adaptability with different networks, the possibility to run an application on different hardware platform and data centers are close to the point of data consumption. One more example is a player who offers a platform on which network functions can become more secure than ever, provide the security as a service, improve automation, easily upgradable,

Therefore, in industries, the current architectures don?t mostly maintain interoperability and there might be no clear policies on how two/many service providers suppose to interact with eachother to provide a service to end users. This is because the assumptions often are that end users use services from the same service providers, data centers are close to service providers so that end users can easily be verified and simply access different services on data centers and data centers belong to the same service providers. This is why there is a missing common language for exchanging policies and automatically allowing several authorized services from different service providers to work with eachother. This is especially critical and complex where some of these virtualized services should provide end users with security functions (such as a firewall).

4. Comparison of Current IETF Works

4.1. NSIS

NSIS is for standardizing an IP signaling protocol (RSVP) along data path for end points to request its unique QoS characteristics, unique FW policies or NAT needs (RFC5973) that are different from the FW/NAT original setting. The requests are communicated directly to the FW/NAT devices. NSIS is like east-west protocols that require all involved devices to fully comply to make it work.

NSIS is path-coupled, it's possible to message every participating device along a path without having to know its location, or its location relative to other devices (this is particularly a pressing issue when you've got one or more NATs present in the network, or when trying to locate appropriate tunnel endpoints).

Here are some aspects that I2NSF is different from NSIS:

- The I2NSF requests from clients don?t usually go directly to network security devices, but instead to controller or orchestrator that can translate the application/user oriented policies to the involved devices in the interface that they support.

- The I2NSF doesn?t require all network functions to comply.

- I2NSF is to define clients (applications) oriented descriptors (profiles, or attributes) to request/negotiate/validate network security functions that are not physically located on the local premises.

Why we believe I2NSF has higher chance to be deployed than NSIS:

1- OpenStack already has preliminary implementation, but the specification is not complete. IETF can play an active role to make the specification complete. Extend what OpenStack has to more comprehensive specifications that can meet operators requirement, and then have operators encourage their suppliers to contribute open source per IETF specifications to the OpenStack community. As the software development cycle: Architecture, Design specification, and coding: IETF can take the ownership of the first two steps.

2- The requests are to controllers, instead of to devices. It doesn?t require all middle boxes to be changed to make it work. The security can be better controlled by the controllers.

3- There is very strong momentum to make virtualized network functions to be deployed by operators (NFV initiative).

4.2. SACM

IETF SACM (Security Assessment and Continuous Monitoring) specifies the mechanisms to assess end point security. The end points can be routers, switches, clustered DB, installed piece of software. SACM is about ?How to encode that policy in a manner where assessment can be automated?.

Here are the major differences between SACM and I2NSF:

SACM:

* End points can be routers, switches, clustered DB, installed piece of software

* How to encode policies in a manner where assessment can be automated

Example:

- a Solaris 10 SPARC or Window 7 system used in a environment that requires adherence to a policy of Mission Critical Classified.

- rules like "The maximum password age must be 30 days" and "The minimum password age must be 1 day"

I2NSF:

- Protocols for clients to request/query/verify Security related functions from Network Providers

- Firewall

- DDOS/Anti-DOS

- Access control/Authorization/Authentication

- Remote identity management

- Secure Key management

- Intrusion Detection System/ Intrusion Prevention System (IDS/IPS)

Example:

* vCPE needs vFW that are hosted in the network.

* vCPE provides the ?Group Policies? for the vFW, like A can talk to B & C, but B can?t talk to C.

4.3. MIDCOM

To be added.

4.4. PCP

As indicated by the name, the Port Control Protocol (PCP) enables an IPv4 or IPv6 host to flexibly manage the IP address and port mapping information on Network Address Translators (NATs) or firewalls, to facilitate communication with remote hosts.

Here are some aspects that I2NSF is different from PCP:

? PCP only support the management of port and address information rather than any other security functions

4.5. SFC & VNFpool

IETF SFC is about mechanism of chaining together service functions; IETF SFC treats all those ?Service Functions? as black box, i.e. SFC doesn?t care what actions those functions are performing. SFC defines the SFC header to carry Metadata with payload to those functions. But SFC itself doesn?t specify what content is encoded in the metadata.

I2NSF is targeted to define the descriptor (the actual rules & policies) of the network security functions needed and the negotiation scheme.

Those policies or descriptors don?t usually go with user payload.

VNFpool is about the reliability and availability of the virtualized network functions. But none of them address how service functions are requested, or how service functions are fulfilled.

VNFpool does not cover in-depth specification (e.g. rules for the requested FW) for clients to request its needed functions. In SFC & VNFpool, FW function is a black box, that is treated in same way as Video Optimization function. SFC/VNFpool don?t cover the negotiation part, e.g. Client needs Rule x/y/z for FW, but the Provider can only offer x/z.

4.6. ANIMA

ANIMA (Autonomic Networking Integrated Model and Approach) introduces a control paradigm where network processes, driven by objectives (or intent), coordinate their local decisions, autonomically translate them into local actions, and adapt them automatically according to various sources of information including external information and protocol information bases.

ANIMA will develop protocols to achieve auto discovery among management system and devices. The listed drafts proposed ?The

Configuration Discovery and Negotiation protocol designed to be a generic platform, which is independent from the negotiation contents.? There are also the Security aspects being discussed in the ANIMA drafts (like secure messages, or keys, among the parties (to be discovered).

I2NSF is to develop application /user oriented policies (the attributes, the profiles, or the descriptors) of the network security functions that clients can request/query from 3rd party providers.

There might be some elements/protocols developed by ANIMA that can be used by I2NSF.

5. Conclusion and Recommendation

In industries there is a missing common language that can help service providers to inter-operate with eachother. For having this common language (standard), the mechanism to carry the policies between clients and providers can be built upon the past IETF work and protocols.

6. Security Considerations

There is no security consideration

7. IANA Considerations

There is no IANA consideration

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

Hosnieh Rafiee
HUAWEI TECHNOLOGIES Duesseldorf GmbH
Riesstrasse 25, 80992,
Munich, Germany
Phone: +49 (0)162 204 74 58
Email: ietf@rozanak.com

Dacheng Zhang
HUAWEI TECHNOLOGIES
Q14 huawei campus, Beiqing Rd., Haidian Dist.,
Beijing, China
E-mail: zhangdacheng@huawei.com