Network Working Group
Internet-Draft
Intended status: Experimental
Expires: April 28, 2015

A. Pastor
D. Lopez
Telefonica I+D

October 25, 2014

Access Use Cases for an Open OAM Interface to Virtualized Security Services
draft-pastor-i2nsf-access-usecases-00

Abstract

This document describes the use cases for providing network security as a service in the access network environment. It considers both mobile and residential access.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document describes the use cases for an open OAM interfce to virtualized network security services in residential and mobile network access.

Not only enterprise customers, but also residential and mobile ones are becoming more and more aware of the need for security, just to find that security services are hard to operate and become expensive in the case of reasonably sophisticated ones. This general trend has caused that numerous operators and security vendors start to leverage cloud-based models to deliver security solutions. In particular, the methods around Network Function Virtualization (NFV) are meant to facilitate the management of various resources for the benefit of customers, who may not own or physically host those network functions.

This document analyzes the use cases for the provision, operation and management of virtualized Network Security Function (vNSF) in the access network environment, as shown in the following figure.

```
    Customer   +     Access     +     Core
               |                |     +--------+
               |          ,-----+--.  |Network |
               |        ,'      |   `-|Operator|
 +-----------+ |       /+-----+ |     |Mgmt Sys|
 |Residential|-+------/-+vCPE+----+   +--------+
 +-----------+ |     /  +-----+ |  \          :
               |    /           |   \         |
               |   ;            |    +----+   |
               |   |            |    |vNSF|   |
               |   :            |    +----+   |
               |    :           |   /         |
    +--------+ |    :   +-----+ |  /          ;
    |Mobile  |-+-----\--+vEPC+----+          /
    +--------+ |      \ +-----+ |      ISP ,-'
               |       `--.     |      _.-'
               |           `----+----''
               +                +
```

Figure 1: Customer Access Network

2. 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 [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.

3. Actors in the Access Environment

Different types of actors can use an open OAM interface to the vNSFs to allocate and operate network security functions. The envisioned actors are:

- Network operators that provide and manage vNSF in their administrative domain or through external providers.

- Customers, accessing through the Network Operator, and requiring a security service implemented by one or more vNSF.

The access network technology environment also defines the characteristics of the type of access in each use case:

- Closed environments where there is only one administrative network domain. More permissive access controls and lighter validation shall be allowed inside the domain because of the protected environment. Integration with existing identity management systems is also possible.

- Open environments where some vNSFs can be hosted in external administrative domains, and more restrictive security controls are required. The interfaces to the vNSFs must use trusted channels. Identity frameworks and federations are common models for authentication and Authorization.

4. Operator-Managed Security Functions

The Virtual CPE described in [NFVUC] use cases #5 and #7 cover the model of virtualization for mobile and residential access, where the operator may offload security services from the customer local environment (or even the terminal) to the operator infrastructure supporting the access network.

This use case defines the operator interaction with vNSF through

automated interfaces, typically by B2B communications performed by the operator management systems (OSS/BSS).

4.1. vNSF Deployment

The deployment process consists of instantiating a vNSF on a Virtualization Infrastructure (NFVI), within the operator administrative domain(s) or an external domain. This is a required step before a customer can subscribe to a security service supported in the vNSF.

4.2. vNSF Customer Provisioning

Once a vNSF is deployed, any customer can subscribe to it. The provisioning lifecycle includes:

- Customer enrollment and cancellation of the subscription to a vNSF.

- Configuration of the vNSF, based on specific configurations or derived from common security policies defined by the operator.

- Retrieve and list of the vNSF functionalities, extracted from a manifest or a descriptor. The network operator management systems can demand this information to offer detailed information through the commercial channels to the customer.

5. Customer-Managed Security Functions

This is an alternative use case where the management is delegated directly to the customer. The open OAM interface permits direct interactions between the vNSF and the customer. This allows customers to have dynamic and flexible interactions with security services, more adequate for dynamic allocation of these virtualized security services.

5.1. Self-Provisioning

This process allows a residential or mobile customer to enroll on its own to a security service provided by a vNSF or a set of vNSF. The open OAM interface must support the enrollment process.

5.2. Validation

Customers MAY require to validate vNSF availability, provenance, and its correct execution. The validation process includes at least:

- Integrity of the vNSF. The vNSF is not manipulated.

- Isolation. The execution of the vNSF is self-contained for privacy requirements in multi-tenancy scenarios.

6. Policies and Configuration

vNSF configurations can vary from simple rules (i.e. block a DDoS attack) to very complex configuration (i.e. define a user firewall rules per application, protocol, source and destination port and address). The possibility of using configuration templates per vNSF type is a common option as well.

The operator can push security policies using complex configurations in their managed vNSF through its management system. The open OAM interface has to accommodate this application-driven behavior.

Computer-savvy customers may pursue a similar application-driven configuration through the open OAM interface, but standard residential and mobile customers may prefer to use the definition of security policies in the form of close-to-natural-language sentences with high-level directives or a guide configuration process. The representation for these policies will be of the form:

```
+-------+   +------+   +------+   +------------------+
|Subject| + |Action| + |Object| + |Field_type = Value|
+-------+   +------+   +------+   +------------------+
```

Figure 2: High-Level Security Policy Format

Subject indicates the customer or device in the access.

Action can include a variety of actions: check, redirect, allow, block, record, inspect...

Object can be optional and specifies the nature of the action. The default is all the customer traffic, but others possible values are connections and connections attempts.

Field_type allows to create fine-grained policies, including destinations list (i.e. IPs, domains), content types (i.e. files, emails), windows of time (i.e. weekend), protocol or network service (i.e. HTTP).

An example of a customer policy is:

"My son is allowed to access Facebook from 18:30 to 20:00"

7. Security Functions at the Access Network

This section collects a representative list of use cases of possible vNSFs that requires an open OAM interface for control and management.

7.1. Traffic Inspection

A common use case for customers accessing the Internet or additional services through it is security supervision. Some examples are:

- Intrusion detection systems

- Deep packet inspection

- Data leakage protection

An open OAM interface will allow the configuration of the vNSF inspection features: signatures updates, behavioral parameters or type of traffic to supervise.

7.2. Traffic Manipulation

A more intrusive use case of vNSF includes the capacity of manipulate the traffic at the access network segment. Some examples are:

- Redirect traffic, as in the case of captive portals

- Block traffic: Firewalls, intrusion prevention system, anti-DoS mechanisms...

- Encrypt traffic: VPN services that encapsulate and encrypt the user traffic. A SSL VPN is a representative example.

An open OAM interface will allow the configuration of the vNSF manipulation features, such as redirect and block rules.

7.3. Impersonation

Some vNSFs can impersonate a customer service or Internet service to provide security functions. Some examples are:

- Honeypots, impersonating customer services, such as HTTP, NetBios or SSH

- Anonymization services, hiding the source identity, as in the case of TOR

An open OAM interface will allow the configuration of the vNSF impersonation features, like the service to impersonate.

8. Security Considerations

TBD

9. IANA Considerations

This document requires no IANA actions.

10. References

10.1. Normative References

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

10.2. Informative References

[NFVUC] "ETSI NFV Group Specification, Network Functions Virtualization (NFV) Use Cases", <http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf>.

Authors' Addresses

Antonio Pastor
Telefonica I+D
Don Ramon de la Cruz, 82
Madrid, 28006
Spain

Phone: +34 913 128 778
Email: antonio.pastorperales@telefonica.com

Diego R. Lopez
Telefonica I+D
Don Ramon de la Cruz, 82
Madrid,   28006
Spain

Phone: +34 913 129 041
Email: diego.r.lopez@telefonica.com