Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 7, 2015

K. Wang
X. Zhuang
China Mobile

March 6, 2015

Integrated Security with Access Network Use Case
draft-qi-i2nsf-access-network-usecase-02

Abstract

In traditional telecommunication system, operators usually provide general and limited security protection service for users during access (e.g. AKA in 3G/4G network). Now, with the development of network virtualization technology and data center, physical network devices can be replaced by network function softwares which are running on virtual machines and the network function can be flexible and elastic. Operators can provide users with more security services. So this interfaces between operator's network and users are highly desired. These interfaces will be used to request/achieve (Virtual) Network Security Functions from operator's network. This draft describes use cases for using the interface in operator's network environment.

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). 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/.

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 August 31, 2015.

Table of Contents

1. Introduction

This draft is a revised version of draft-qi-i2nsf-access-network-usecase and refines the original use cases. In draft-qi-i2nsf-access-network-usecase, an interface between UE and network was described while this draft describes two interfaces.Users can use client to achieve security service of operator via these interfaces. The user can be an enterprise, an enterprise user, administrator of operator and so on. The revisions details as below: 1.For original use case-Interface about sending security configuration information from network to UE: All examples have been deleted and network did not send configuration information to UE via interface. Instead Users will send security service requests to security controller to

configure NSF(s). 2.For original use case-Interface about optional security function negotiation between Network and UE: All examples have been deleted and there is no security function negotiation between network and UE. Instead Users will send security service request to security controller to configure NSF(s). 3.For original

use case-UE proposed security request to the network: The original interactions between user and network will be more concrete. For example, the original interaction between user and specific network element will be revised into interaction between user's client and security controller. The interaction between specific network element and security function settings will be described in detail. 4.For original section of Abstraction and The Benefits: Corresponding modifications have been made to match revised use cases better.

2. Conventions used in this document

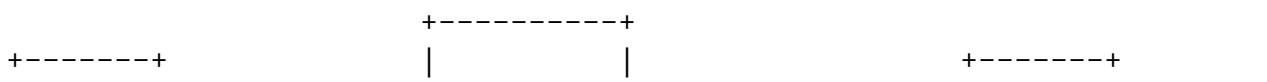
The section clarifies the intended meaning of specific terms used within this document.

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 [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 [RFC2119] significance.

3. Use case summary

This draft describes use cases of users (e.g. enterprise user, operator's administrator and so on) using operators' flexible security services. For example, a user can request a security service through a client (e.g. APP, BSS/OSS, OAM etc.).An operator's network entity(e.g. gateway) can invoke (v)NSF(s) according to user's service request. In order to make the description more clear, we call operator's network entity as security controller. The interaction between entities above(i.e. client, security controller, NSF) can be showed as below:



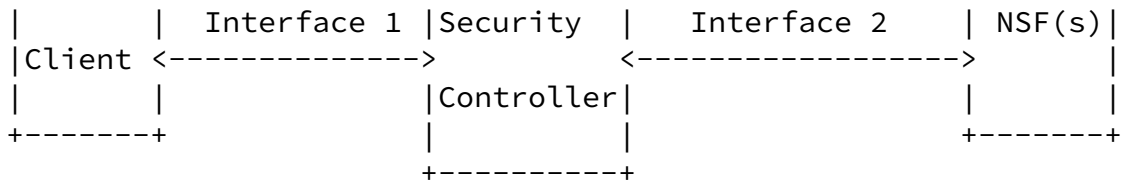


Figure 1. Interaction between Entities

Interface 1 is used for receiving security requirements from client and translating them into commands that NSF(s) can understand and execute. Moreover, it is also responsible for giving feedback of NSFs' security statistics to client.Interface 2 is used for interacting with NSFs according to commands. Moreover, it is also

responsible for receiving the results of commands from NSFs.NSF mentioned in this draft includes virtualized NSF and physical NSF.

4. Use case for Instantiation and Configuration of Security Service Function

Client sends collected security requirements through interface 1 to the security controller in operator's network which then translates them into a security function or a set of security functions then the corresponding NSFs are instantiated and configured through interface 2.For example, an enterprise user A is a tenant of operator data center and wants to filter all TCP data packets flowing to A's network. Such a requirement is sent from client to security controller through interface 1. The security controller translates the requirement into a firewall function and then instantiates a firewall NSF through interface 2. The corresponding filter rule is also configured onto this firewall NSF.

5. Use case for Updating Security Service Function

User can use client to update security service function, including adding/deleting a security service function and updating configurations at former security service function. For example,a user who has instantiated a security service before wants to enable an IDS service additionally, this requirement will be sent to security controller through interface 1 and be translated and then security controller instantiates and configures an IDS NSF through interface 2. Another example is that if the user A mentioned in use case 1 wants to filter all UDP packets besides TCP packets, client

sends this requirement to security controller through interface 1 and then security controller configures translated requirement onto the former firewall NSF.

6. Use case for Collecting and Feedback of Status of Security Service Function

When users want to get the executing status of security service, they can request the status statistics information of NSF(s) from client. Security controller can collect NSFs' status statistics information through interface 2 and give feedback to client through interface 1, which is helpful for user analyzing or updating security requirements. Users can collect status statistics information of NSF(s) related to their security service and can also be authorized to collect all NSFs' status statistics information for the analysis of big data for network security like the overall security status of the network in operator's data center.

7. The Benefits

There are numerous benefits by defining such interfaces. Operators could provide more flexible and customized security services for specific users and this would provide more efficient and secure protection to each user.

8. IANA Considerations

TBD

9. Informative References

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

Authors' Addresses

Ke Wang
China Mobile
32 Xuanwumenxi Ave,Xicheng District
Beijing 100053
China

Email: wangkeyj@chinamobile.com

Xiaojun Zhuang
China Mobile
32 Xuanwumenxi Ave, Xicheng District
Beijing 100053
China

Email: zhuangxiaojun@chinamobile.com

Minpeng Qi
China Mobile
32 Xuanwumenxi Ave,Xicheng District
Beijing 100053
China

Email: qiminpeng@chinamobile.com