Annex I: A.1 justification for proposed draft new Recommendation X.ssc

Question:	2/17	**Proposed new ITU-T Recommendation**	Geneva, Switzerland, 29 August – 06 September 2017
Reference and title:	ITU-T X.ssc " Security Service Chain Architecture "		

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This Recommendation is to study security service chain in order to provide customized security services dynamically and adaptively for the network and applications. This Recommendation:

- Introduces security service chain;
- designs an architecture for security service chain;
- gives scenarios to explain how to create security service chain.

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

Network Function Virtualization (NFV) is to reduce capital expenditure and operational expenditure [b-FIS 2010] by replacing proprietary hardware-based network equipment with software-based Virtualized Network Functions (VNFs) that can be instantiated dynamically on commodity servers (e.g., x86 based systems) and located more flexibly in the network. Software Defined Networking (SDN) [b-ONF SDN] enables automated and dynamic application deployment and reconfiguration due to its network-wide and fine-grained control of the network flows. These two complementary technologies (i.e. NFV and SDN) open up new ways to deploy applications rapidly and automatically using service function chain (SFC) [b-IETF RFC 7665] in a more efficient and scalable fashion. Correspondingly, security as one of key features for application also has to be provided dynamically and adaptively to meet different security requirements for today's rapid-increasing and evolving networks and applications.

However, traditional security appliances (e.g. Firewall, IDS) are implemented as hardware-based middleboxes and placed at fixed locations in the network. It is of the administrators' duties to overload path selection mechanisms to force traffic through the desired sequences of security middleboxes as defined within security policies [b-SIGCOMM 2008]. Since these security middleboxes are hardware-based and rather static, it is difficult to meet different security requirements for today's networks and applications. Moreover, it will be a heavy and complicated workload for the administrator to overload path selection mechanisms when traditional security appliances are deployed in a large-scale network. It will be even worse that those path selection mechanisms overloaded by the administrator are inconsistent.

This Recommendation is to design security service chain architecture and give scenarios to explain how to create security service chain dynamically and adaptively in order to meet different security requirements for the network and applications. It also supports real-time threat detection and policy-based automated response so that the administrator could not be involved into path selection mechanisms overloading.

Relations to ITU-T Recommendations or to other standards (approved or under development):

- ITU-T SG17 X.sdnsec-3: focuses on security issues of SDN-based realization of SFC. This new proposal X.ssc will study how to provide security service by SFC.
- IETF related RFCs & drafts: mainly focuses on architecture, protocol, deployment models and security environments of SFC. How to create security service chains by SFC is not discussed in IETF.
- ETSI GS NFV 001 (NFV Use Cases): defines a use case on VNF Forwarding Graph, which is similar to SFC. However, VNFFG only involves VNF. Moreover, no security related issues are mentioned in this use case. This new proposal X.ssc applies for both VNF and PNF (Physical Network Function). It will also provide security services by SFC.
- ETSI GS NFV-SEC 013 (NFV Security, Security Management and Monitoring specification): focuses on NFV Security Lifecycle Management and Security Monitoring. This new proposal X.ssc is to study how to establish security chain by orchestrating security functions (including virtual security functions and physical security equipment) to provide security services.
- ONF TS-027 "L4-L7 Service Function Chaining Solution Architecture", which gives how to implement SFC in SDN network to improve the inefficiencies faced by the traditional network. Some security logical functions like Firewall

were mentioned as general service functions to explain how to create SFC. However, there is no discussion on how to create security service chains according to different security requirements from the network and applications.

Liaisons with other study groups or with other standards bodies:

IETF SFC, ETSI

Annex II: Draft Recommandation ITU-T X.ssc

Security Service Chain Architecture

Summary

<Mandatory>

Keywords

<Mandatory>

Introduction

Network Function Virtualization (NFV) is to reduce capital expenditure and operational expenditure [b-FIS 2010] by replacing proprietary hardware-based network equipment with software-based Virtualized Network Functions (VNFs) that can be instantiated dynamically on commodity servers (e.g., x86 based systems) and located more flexibly in the network. Software Defined Networking (SDN) [b-ONF SDN] enables automated and dynamic application deployment and reconfiguration due to its network-wide and fine-grained control of the network flows. These two complementary technologies (i.e. NFV and SDN) open up new ways to deploy applications rapidly and automatically using service function chain (SFC) [b-IETF RFC 7665] in a more efficient and scalable fashion. Correspondingly, security as one of key features for application also has to be provided dynamically and adaptively to meet different security requirements for today's rapid-increasing and evolving networks and applications.

However, traditional security appliances (e.g. Firewall, IDS) are implemented as hardware-based middleboxes and placed at fixed locations in the network. It is of the administrators' duties to overload path selection mechanisms to force traffic through the desired sequences of security middleboxes as defined within security policies [b-SIGCOMM 2008]. Since these security middleboxes are hardware-based and rather static, it is difficult to meet different security requirements for today's networks and applications. Moreover, it will be a heavy and complicated workload for the administrator to overload path selection mechanisms when traditional security appliances are deployed in a large-scale network. It will be even worse that those path selection mechanisms overloaded by the administrator are inconsistent.

This Recommendation is to design security service chain architecture and give scenarios to explain how to create security service chain dynamically and adaptively in order to meet different security requirements for the network and applications. It also supports real-time threat detection and policy-based automated response so that the administrator could not be involved into path selection mechanisms overloading.

1 Scope

This Recommendation is to study security service chain in order to provide customized security services dynamically and adaptively for the network and applications. This Recommendation:

- Introduces security service chain;
- designs an architecture for security service chain;
- gives scenarios to explain how to create security service chain;

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.yyy] Recommendation ITU-T X.yyy (date), *Title*.

3 Definitions

<Check in the ITU-T terms and definitions database at www.itu.int/go/terminology-database whether the term has already been defined in another Recommendation. It would be more consistent to refer to such a definition rather than to redefine the term>

3.1 Terms defined elsewhere

<Normally, terms defined elsewhere will simply refer to the defining document. In certain cases, it may be desirable to quote the definition to allow for a stand-alone document>

This Recommendation uses the following terms defined elsewhere:

3.1.1 <Term 1> [Reference]: <optional quoted definition>.

3.1.2 <Term 2> [Reference]: <optional quoted definition>.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Security Service Chain: one type of SFC (Service Function Chain), defines an ordered set of security functions and ordering security policies that must be applied to packets and/or flows selected as a result of classification.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

SFC	Service Function Chain
SSC	Security Service Chain

5 Conventions

In this Recommendation:

The keywords **"is required to"** indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords **"is recommended"** indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords **"is prohibited from"** indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords **"can optionally"** indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of Security Service Chain

6.1 Non-User-Oriented Security Chains

6.2 User-Oriented Security Chains

7 Architecture for Security Service Chain

8 Creation of Security Service Chain

Annex A

<Annex Title>

(This annex forms an integral part of this Recommendation.)

<Body of annex A>

Appendix I

<Appendix Title>

(This appendix does not form an integral part of this Recommendation.)

<Body of appendix I>

Bibliography

[b-FIS 2010] J. Carapinha, P. Feil, P. Weissmann, S. E. Thorsteinsson, C¸ . Etemo˘glu, O´ . Ingo´rsson, S. C¸ iftc¸i, and M. Melo, "Network Virtualization – Opportunities and Challenges for Operators," in Future Internet - FIS 2010. Springer Berlin Heidelberg, 2010, pp. 138–147.

[b-ONF SDN] "Software-Defined Networking (SDN) Definition", Open Networking Foundation.

[b-IETF RFC 7665] J. Halpern and C. Pignataro. Service function chaining (sfc) architecture. IETF RFC 7665, October 2015

[b-SIGCOMM 2008] D. A. Joseph, A. Tavakoli, and I. Stoica, "A policy-aware switching layer for data centers," in Proceedings of the ACM SIGCOMM 2008 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Seattle, WA, USA. ACM, 2008, pp.51–62.

_____