Draft Recommendation X.sdnsec-3

Security guideline of Service Function Chain based on software defined network

Summary

This recommendation is to analyze the security threats of the SDN-based Service Function Chain and gives security guideline on how to mitigate these threats. This security guideline can help the reader to understand the security risks encountered when using SDN-based Service Function Chain and further help to develop and implement secure Service Function Chain architecture.

Keywords

SDN; Service Function Chain

Table of Contents

Introduction

Service Function Chain enables the administrators to distribute network policies more efficiently and conveniently, while Software-Defined Networking (SDN) helps to adjust traffic dynamically according to the changing requirements. These two technologies can be combined to give the network higher flexibility and stronger capability of serving on demand. However, it is realized that such SDN-based Service Function Chain also introduces new security challenges into the network, not only the legacy SDN threats, but also some new threats along with Security Function Chain, and there is an urgent need for a security guideline.

Because of using the SDN architecture, the common SDN threats will show up in the Service Function Chain based on SDN according to [ITU-T X.1038] and [ITU-T Y.3300], such as more severe DoS/DDoS attack caused by centralized SDN controller, and attacks on Application-Control interface, etc.

More security issues will also arise because of the deployment of the Service Function Chain. New network elements are introduced, like Service Function Chain Forwarder, and new information will be transferred among the network elements, like Service Function Chain. Threats against these entities should be mitigated.

Draft Recommendation ITU-T X.sdnsec-3

Security guideline of Service Function Chain based on software defined network

1. Scope

This recommendation analyzes the security threats encountered in the Service Function Chain based on software defined network, and provides the security guideline for SDN-based Service Function chain architecture. This recommendation covers as follows:

- Describe a general security architecture for SDN-based Service Function Chain;

- Analyze the security threats and requirements of network elements and corresponding interfaces in the above-mentioned general architecture;

- Describe and analyze the problem of policy management in SDN-based service Function chain;

- Provide countermeasures of above mentioned problems;.

2. References

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking.*

[ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking.*

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined in section 1.4 of IETF RFC 7665 [b-IETF RFC 7665].

3.1.1 Classification[b-IETF RFC 7665]**:** Locally instantiated matching of traffic flows against policy for subsequent application of the required set of network service functions. The policy may be customer/network/ service specific.

3.1.2 Classifier[b-IETF RFC 7665]**:** An element that performs Classification.

3.1.3 Service Function Chain (SFC) [b-IETF RFC 7665]**:** A service function chain defines an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification.

3.1.4 Service Function (SF) [b-IETF RFC 7665]**:** A function that is responsible for specific treatment of received packets and can be realized as a virtual element or be embedded in a physical network element. A non-exhaustive list of abstract service functions includes: firewalls, WAN and server load balancing etc.. An SF may be SFC encapsulation aware (that is, it receives and acts on information in the SFC encapsulation) or unaware (in which case, data forwarded to the SF does not

contain the SFC encapsulation). This is often referred to as "SFC aware" and "SFC unaware", respectively.

3.1.5 Service Function Forwarder (SFF) [b-IETF RFC 7665]**:** A service function forwarder is responsible for forwarding traffic to one or more connected service functions according to information carried in the SFC encapsulation, as well as handling traffic coming back from the SF. Additionally, an SFF is responsible for delivering traffic to a classifier when needed and supported, transporting traffic to another SFF (in the same or different type of overlay), and terminating the Service Function Path (SFP).

3.1.6 Service Function Path (SFP) [b-IETF RFC 7665]**:** The service function path is a constrained specification of where packets assigned to a certain service function path must go. While it may be so constrained as to identify the exact locations, it can also be less specific. The SFP provides a level of indirection between the fully abstract notion of service chain as a sequence of abstract service functions to be delivered, and the fully specified notion of exactly which SFF/SFs the packet will visit when it actually traverses the network. By allowing the control components to specify this level of indirection, the operator may control the degree of SFF/SF selection authority that is delegated to the network.

3.1.7 SFC Encapsulation [b-IETF RFC 7665]**:** The SFC encapsulation provides, at a minimum, SFP identification, and is used by the SFC-aware functions, such as the SFF and SFC-aware SFs. The SFC encapsulation is not used for network packet forwarding. In addition to SFP identification, the SFC encapsulation carries metadata including data-plane context information.

3.1.8 SFC Proxy [b-IETF RFC 7665]**:** Removes and inserts SFC encapsulation on behalf of an SFC-unaware service function. SFC proxies are logical elements.

3.1.9 SFC-Enabled Domain [b-IETF RFC 7665]**:** A network or region of a network that implements SFC. An SFC-enabled domain is limited to a single network administrative domain.

3.1.10 Metadata [b-IETF RFC 7665]**:** Provides the ability to exchange context information between classifiers and SFs, and among SFs.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 SFC controller: A function in SDN controller that instructs the functional elements on the SFC resource layer to process packets within an SFC-enabled domain. After receiving the SFC requirements from the APPs, the SFC controller translates the requirements to the SFC classification rules and SFP forwarding rules and sends them to the classifiers and the SFFs respectively via the SDN controller.

3.2.2 SFC Classification rule: Refers to a rule generated and maintained by a SFC controller and a classifier respectively. It reflects the policies for binding an incoming flow to a given SFC and Service Function Path (SFP). A SFC classification rule can be translated a SFC flow rule by the SDN controller and formed an entry in a SFC classification table like a SDN flow entry in a SDN flow table.

3.2.3 SFP forwarding rule: Refers to a rule generated and maintained by a SFC controller and a SFF respectively. It reflects the policies for forwarding an incoming flow to a given SF. A rule can be translated a SFC flow rule by the SDN controller and formed an entry in a SFP forwarding rule table like a SDN flow entry in a SDN flow table.

3.2.4 SFC flow rule: Refers to a flow rule translated by the SDN controller from the SFC classification rule and the SFP forwarding rule.

4. Abbreviations

This Recommendation uses the following abbreviations and acronyms:

SF Service Function

SFC Service Function Chain

SFP Service Function Chain Path

SFC Proxy Service Function Chain Proxy

SFF Service Function Chain Forwarder

DDoS Distributed Denial of Service

5. Conventions

6. Overview

The High-level architecture of SDN is defined in ITU-T Y.3300. It includes three layers, i.e. application layer, control layer and resource layer. The SDN control layer provides a means to dynamically and deterministically control the behavior of network resources (such as data transport and processing), as instructed by the application layer. The features of SDN (i.e. decoupled control function and transportation function, centralized control layer) are suitable to implement SFC(Service Function Chain) , i.e. controller layer can program the SFC policy from the application layer and control the resource layer to forward packages/flows according to the SFC policy.

Based on the High-level architecture of SDN in ITU-T Y.3300, the following Figure1 defines a general reference architecture of SFC based on SDN as a base for the security analysis.

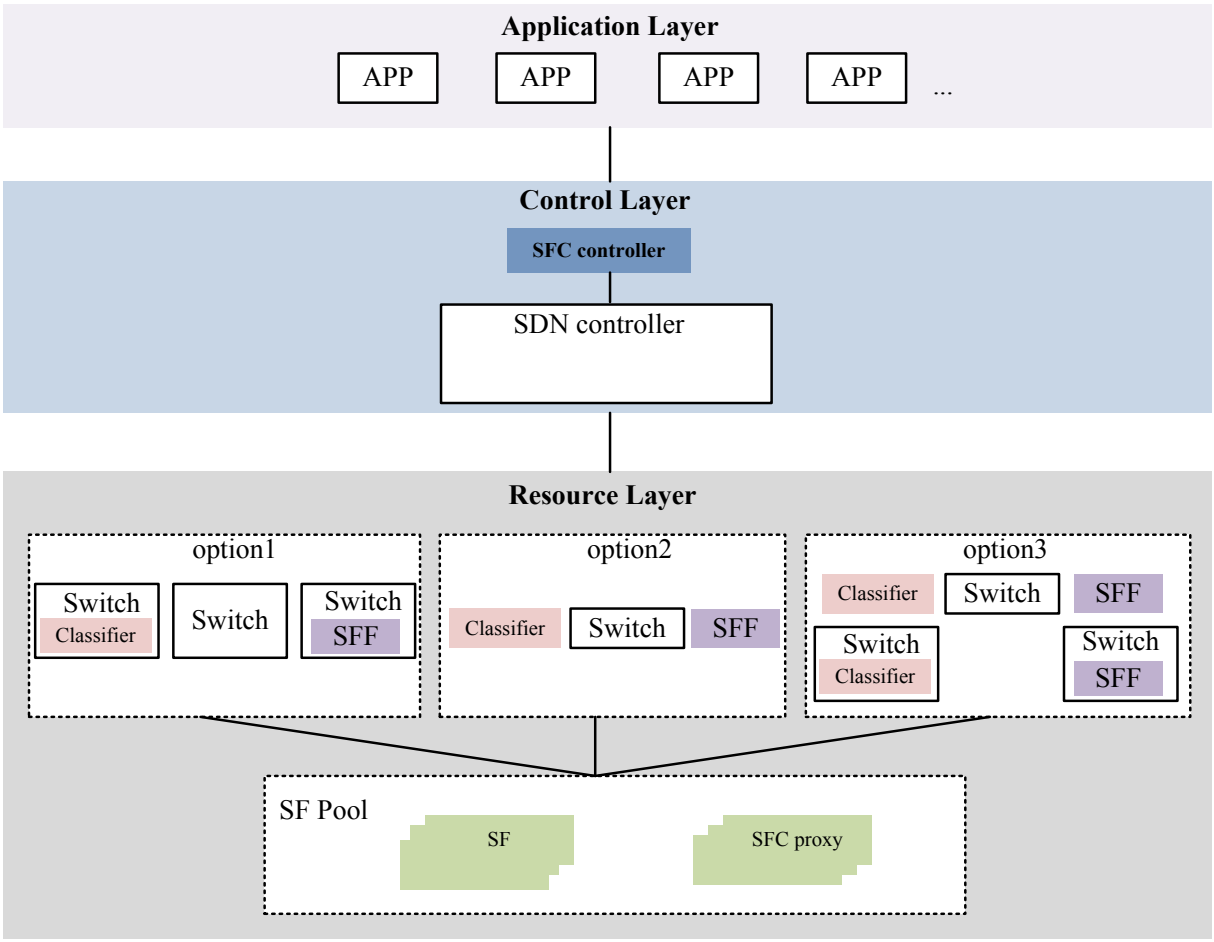

Figure1 General Reference Architecture of SDN-based SFC

The defined network elements of data plane in RFC 7665 such as classifier, SFF, SF and SFC proxy are included in the resource layer. There may be more than one classifier and SFF in the resource layer and both of them can be implemented in the switches or in an independent device. So, the resource layer in Figure1 gives three options. The SFC control function (referred as SFC controller in this Recommendation) can be an APP on the SDN controller or as a function in the SDN controller. This means the interface between the SFC controller and the SDN controller can either be an application-control interface or be a private interface. It's up to the implementation.

The components and functions of each layer are as follows:

- Application layer: This layer refers to the application layer in SDN architecture of ITU-T Y.3300 and especially the APPs can send the user's SFC requirements to the SFC controller to customize the behavior of the user's flows. The APPs can also request SFC information from the SFC controller.

- Control layer: This layer is like the control layer in SDN architecture (ref. Y.3300) except that the SFC controller is included.

  - The SFC controller is responsible for programming the SFC classification rules and the SFP (Service Function Path) forwarding rules according to received the SFC policies from the APPs. Before transporting the SFC classification rules and the SFP forwarding rules to the SDN controller, the SFC controller checks whether these new SFC classification rules and the SFP forwarding rules conflict with the stored active

SFC classification rules and the SFP forwarding rules in SFC repertory of the SFC controller.

- The SDN controller translates the SFC classification rules and the SFP forwarding rules into flow rules and sends these flow rules to the related switches. The SDN controller also needs to process and coordinates the policy conflict between the translated flow rules from the SFC classification rules and the SFP forwarding rules and the traditional SDN flow rules.

- Resource Layer: This layer includes the switches, classifiers, SFFs, SFC Proxies and SFs.

- The Classifiers and the SFFs process the flows according to the flow rules. The Classifier classifies the flows and adds the SFC encapsulation into the package to be used by the SFFs and the SFs etc. The SFFs transport the flows to a SF/SFC proxy or next SFF. The classifier and SFF can be implemented on the switches.

- The SFs are responsible for processing the received flows and also need to inform its status to the SFC controller. The SF can be a VNF or a physical device. The SFC proxies are responsible for removing and inserting SFC encapsulation on behalf of an SFC-unaware service function.

7. General Security Framework of SDN-based Service Function Chain

The security reference architecture for SDN is defined in ITU-T X.1038 and can be applied to the SDN-based SFC, with the addition of some specific security features. A general security architecture of SDN-based SFC is given as below and only emphasizes the specific security for SDN-based SFC.

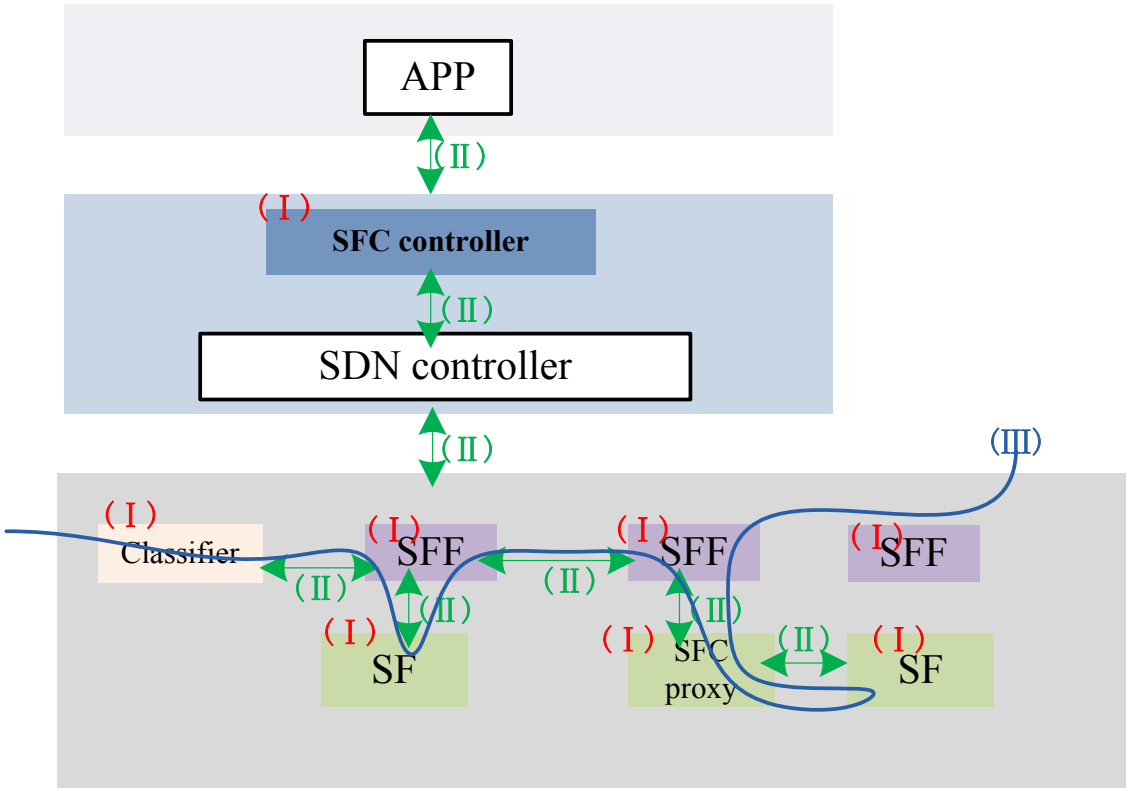

Figure2 General Security Framework of SDN-based Service Function Chain

Three security feature groups are defined in the above figure2:

(Ⅰ) Critical Network elements security: The set of security features that provide the security functions on the network entities to support that the SFC can be securely created, run, maintained and deleted.

(Ⅱ) Interface security: The set of security features that provide the security functions to ensure the secure transportation of the communication data.

(Ⅲ) Policy management: The set of security feature that provide the policy management to resolving the SFC policy conflict e.g. the conflict between the new SFC classification rules/SFP forwarding rules and the stored active SFC classification rules/SFP forwarding rules in SFC repertory of the SFC controller, the conflict between the translated flow rules from the SFC classification rules/ SFP forwarding rules and the traditional SDN flow rules on the SDN controller. .

<TBD>

8. Threat analysis and requirements of Critical network elements

8.1 Critical network elements

SF：

SFF：

SFC：

SFP：

SFC Proxy：

Metadata：

-

<TBD>

8.2 Security threats and requirements

<TBD>

8.2.1 Security threats and requirements of SF

<TBD>

8.2.2 Security threats and requirements of SFF

<TBD>

8.2.3 Security threats and requirements of <xxx>

<TBD>

9. Threat analysis and requirements of interfaces

<TBD>

10. Security considerations of Policy management

<TBD>

11. Countermeasures

<TBD>

Appendix I

SFC Architecture defined in other SDOs

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

The following Figure I.1 is quoted from the section 4 of RFC 7665 (Service Function Chaining (SFC) Architecture).

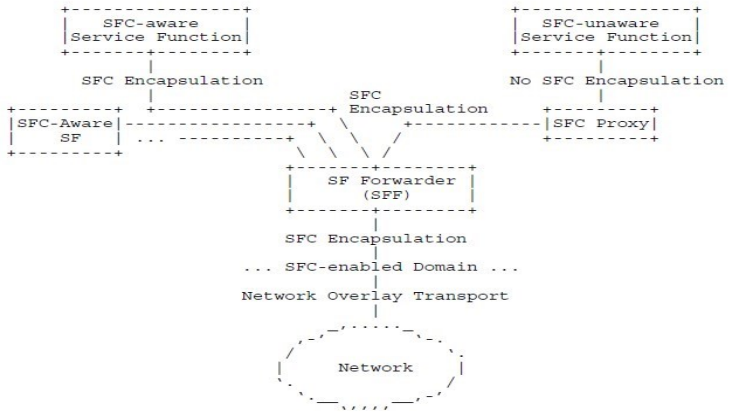

Figure I.1 SFC Architecture Components After Initial Classification

The above architecture only describes the network elements in data plane, i.e SFF, SF and SFC proxy. The classifier is not included in the figure1 because the figure1 describes shows architecture after initial classification.

The following Figure I.2 is quoted from the section 4 of L4-L7 Service Function Chaining Solution Architecture specified by ONF.

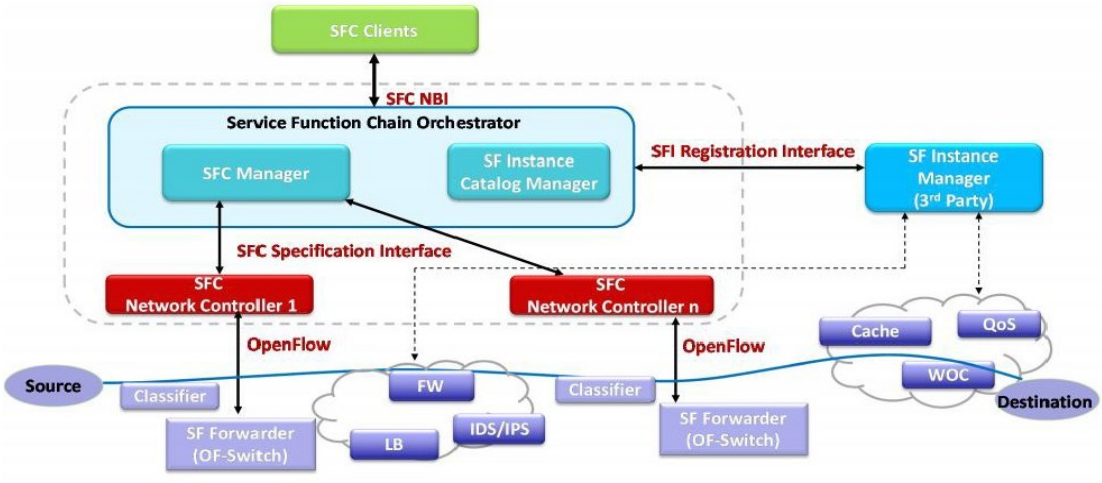

Figure I.2 L4-L7 SDN SFC Architecture

The above architecture is ONF SDN-based and the intent is to build a common base for concrete NBI specifications and OpenFlow (OF) extensions needed for SFC.

Bibliography

[b-IETF RFC 7665] IETF RFC 7665 (2015), *Service Function Chaining (SFC) Architecture*.

[b-IETF draft] IETF draft-ietf-sfc-control-plane-08, *Service Function Chaining (SFC) Control Plane Components & Requirements* (Expires: April 26, 2017)

[b-ONF TS-027] ONF TS-027 (2015), *L4-L7 Service Function Chain Solution Architecture*