Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 18, 2018

J. Jeong
S. Hyun
Sungkyunkwan University
T. Ahn
Korea Telecom
S. Hares
Huawei
D. Lopez
Telefonica I+D

July 17, 2017

Applicability of Interfaces to Network Security Functions to Networked Security Services
draft-jeong-i2nsf-applicability-01

Abstract

This document describes the applicability of Interface to Network Security Functions (I2NSF) to networked security services in Network Functions Virtualization (NFV) environments, such as firewall, deep packet inspection, and attack mitigation.

Table of Contents

1. Introduction

Interface to Network Security Functions (I2NSF) proposes a standard framework and standard interfaces for networked security services in Network Functions Virtualization (NFV) environments. The I2NSF enables multiple security-vendor products to be used cost-effectively in the NFV environment by utilizing the capabilties of such products and the virtualization of security functions in the NFV platform.

This document describes the applicability of I2NSF to networked security services with use cases, such as firewall, Deep Packet Inspection (DPI), and Distributed Denial of Service (DDoS) attack mitigation.

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 RFC 2119 [RFC2119].

3. Terminology

This document uses the terminology described in [RFC7149], [ITU-T.Y.3300], [ONF-OpenFlow], [ONF-SDN-Architecture], [ITU-T.X.1252], [ITU-T.X.800], [i2nsf-framework], [consumer-facing-inf-im], [consumer-facing-inf-dm], [i2nsf-nsf-cap-im], [nsf-facing-inf-dm], [registration-inf-im], [registration-inf-dm], and [nsf-triggered-steering]. In addition, the following terms are defined below:

- Software-Defined Networking: A set of techniques that enables to directly program, orchestrate, control, and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner [ITU-T.Y.3300].

- Firewall: A firewall that is a device or service at the junction of two network segments that inspects every packet that attempts to cross the boundary. It also rejects any packet that does not satisfy certain criteria for disallowed port numbers or IP addresses.

- Centralized Firewall System: A centralized firewall that can establish and distribute access control policy rules into network resources for efficient firewall management. These rules can be managed dynamically by a centralized server for firewall. SDN can work as a network-based firewall system through a standard interface between an SDN switch and a firewall function as a vitual network function (VNF).

- Centralized VoIP/VoLTE Security System: A centralized security system that handles the security issues related to VoIP and VoLTE services. SDN can work as a network-based security system through a standard interface between an SDN switch and a VoIP/VoLTE security function as a VNF.

- Centralized DDoS-attack Mitigation System: A centralized mitigator that can establish and distribute access control policy rules into network resources for efficient DDoS-attack mitigation. These rules can be managed dynamically by a centralized server for DDoS-attack mitigation. SDN can work as a network-based mitigation system through a standard interface between an SDN switch and a DDoS-attack mitigation function as a VNF.

4. I2NSF Framework

This section describes an extended I2NSF framework with SDN for I2NSF applicability and use cases, such as firewall system, deep packet inspection system, and DDoS-attack mitigation system.

Figure 1 shows an I2NSF framework with SDN networks to support networked security services [i2nsf-framework]. As shown in Figure 1, I2NSF User can use security services by delivering their high-level security policies to Security Controller via Consumer-Facing Interface [consumer-facing-inf-im][consumer-facing-inf-dm].

Security Controller can translate the high-level security policies (received from I2NSF User via Consumer-Facing Interface) into low-level security policies for the corresponding NSFs. These low-level security policies are sent to NSFs via NSF-Facing Interface [i2nsf-nsf-cap-im][nsf-facing-inf-dm].

Security Controller asks NSFs to perform low-level security services via NSF-Facing Interface. The NSFs run as Virtual Network Functions (VNFs) on top of virtual machines through Network Functions Virtualization (NFV) [ETSI-NFV]. Security Controller also asks Switch Controller to perform their required security services on switches under the supervision of Switch Controller (i.e., SDN Controller). In addition, Security Controller uses Registration Interface [registration-inf-im][registration-inf-dm] to communicate with Developer's Management Aystem for registering (or deregistering) the developer's NSFs into (or from) the NFV system using the I2NSF framework.

Consumer-Facing Interface between I2NSF User and Security Controller can be implemented by RESTCONF [RFC8040], which is a protocol based on HTTP for configuring data defined in YANG [RFC6020], using the datastore concepts defined in Network Configuration Protocol

(NETCONF) [RFC6241]. YANG data models can describe high-level security services for the sake of I2NSF User. A data model in [consumer-facing-inf-dm] can be used for the I2NSF Consumer-Facing Interface.

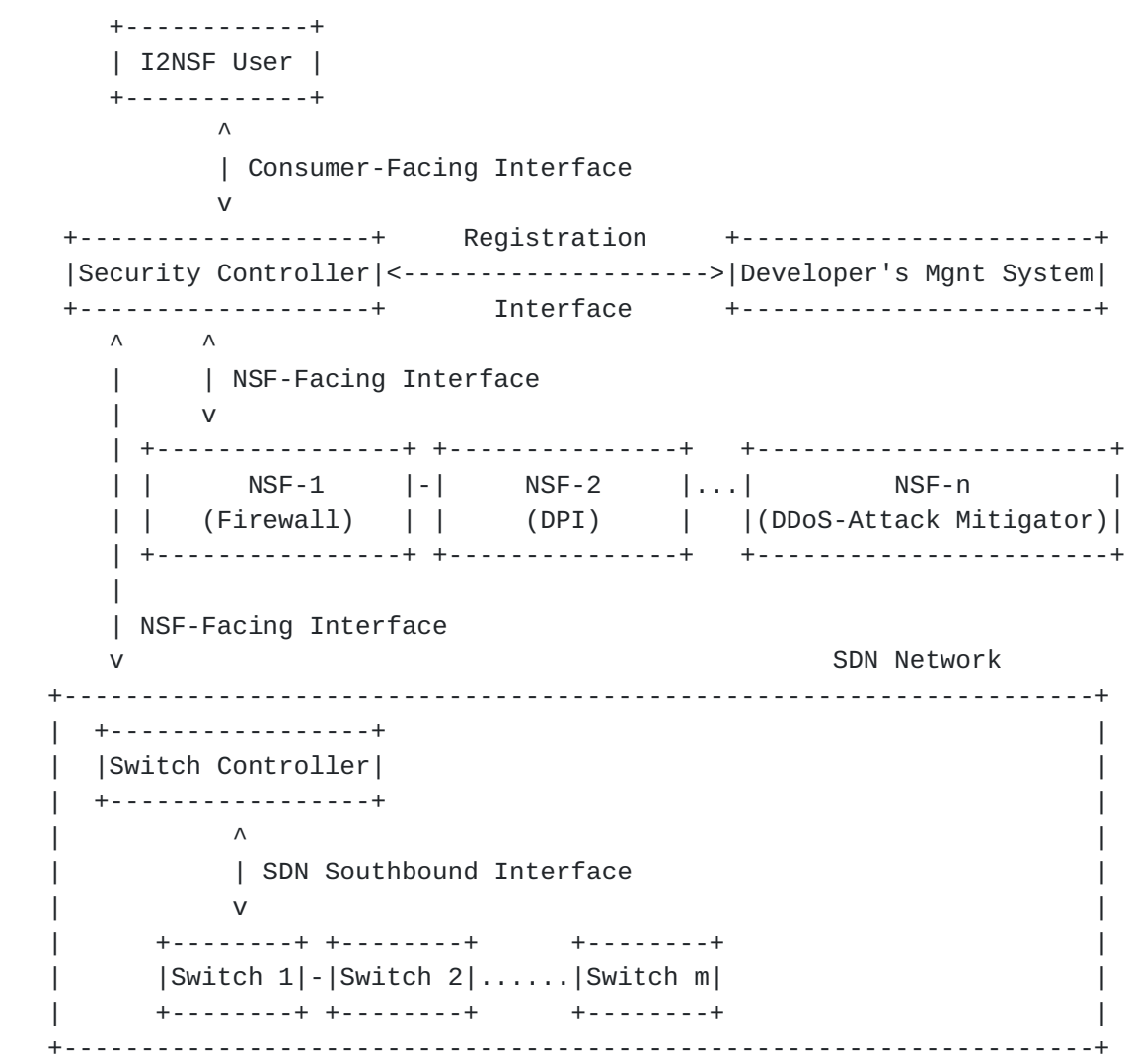

Figure 1: An I2NSF Framework with SDN Networks

NSF-Facing Interface between Security Controller and NSFs can be implemented by NETCONF [RFC6241] for configuring data defined in YANG [RFC6020]. YANG data models can describe low-level security services for the sake of NSFs. A data model in [nsf-facing-inf-dm] can be used for the I2NSF NSF-Facing Interface.

Registration Interface between Security Controller and Developer's Management System can be implemented by RESTCONF [RFC8040] for configuring data defined in YANG [RFC6020]. YANG data models can describe the NSF capabilities of networked security services. A data

model in [registration-inf-dm] can be used for the I2NSF Registration Interface.

Also, the I2NSF framework can enforce mutliple chained NSFs for the low-level security policies with a service function chaining (SFC) for the I2NSF architecture in [nsf-triggered-steering].

5. Use Cases

This section introduces three use cases for cloud-based security services: (i) firewall system, (ii) deep packet inspection system, and (iii) attack mitigation system.

5.1. Firewall: Centralized Firewall System

For the centralized firewall system, a centralized network firewall can manage each network resource and firewall rules can be managed flexibly by a centralized server for firewall (called Firewall). The centralized network firewall controls each switch for the network resource management and the firewall rules can be added or deleted dynamically.

The procedure of firewall operations in the centralized firewall system is as follows:

1. Switch forwards an unknown flow's packet to Switch Controller.

2. Switch Controller forwards the unknown flow's packet to an appropriate security service application, such as Firewall.

3. Firewall analyzes the headers and contents of the packet.

4. If Firewall regards the packet as a malware's packet with a suspicious pattern, it reports the malware's packet to Switch Controller.

5. Switch Controller installs new rules (e.g., drop packets with the suspicious pattern) into switches.

6. The malware's packets are dropped by switches.

For the above centralized firewall system, the existing SDN protocols can be used through standard interfaces between the firewall application and switches [RFC7149][ITU-T.Y.3300][ONF-OpenFlow] [ONF-SDN-Architecture].

Legacy firewalls have some challenges such as the expensive cost, performance, management of access control, establishment of policy,

and packet-based access mechanism. The proposed framework can resolve the challenges through the above centralized firewall system based on SDN as follows:

- Cost: The cost of adding firewalls to network resources such as routers, gateways, and switches is substantial due to the reason that we need to add firewall on each network resource. To solve this, each network resource can be managed centrally such that a single firewall is manipulated by a centralized server.

- Performance: The performance of firewalls is often slower than the link speed of network interfaces. Every network resource for firewall needs to check firewall rules according to network conditions. Firewalls can be adaptively deployed among network switches, depending on network conditions in the framework.

- The management of access control: Since there may be hundreds of network resources in an administered network, the dynamic management of access control for security services like firewall is a challenge. In the framework, firewall rules can be dynamically added for new malware.

- The establishment of policy: Policy should be established for each network resource. However, it is difficult to describe what flows are permitted or denied for firewall within a specific organization network under management. Thus, a centralized view is helpful to determine security policies for such a network.

- Packet-based access mechanism: Packet-based access mechanism is not enough for firewall in practice since the basic unit of access control is usually users or applications. Therefore, application level rules can be defined and added to the firewall system through the centralized server.

5.2. Deep Packet Inspection: Centralized VoIP/VoLTE Security System

For the centralized VoIP/VoLTE security system, a centralized VoIP/VoLTE security system can monitor each VoIP/VoLTE flow and manage VoIP/VoLTE security rules controlled by a centralized server for VoIP/VoLTE security service (called VoIP IPS). The VoIP/VoLTE security system controls each switch for the VoIP/VoLTE call flow management by manipulating the rules that can be added, deleted or modified dynamically.

The procedure of VoIP/VoLTE security operations in the centralized VoIP/VoLTE security system is as follows:

1. A switch forwards an unknown call flow's signal packet (e.g., SIP packet) to Switch Controller. Also, if the packet belongs to a matched flow's packet related to SIP (called matched SIP packet), Switch forwards the packet to Switch Controller so that the packet can be checked by an NSF for VoIP (i.e., VoIP IPS) via Switch Controller, which monitors the behavior of its SIP call.

2. Switch Controller forwards the unknown flow's packet or the matched SIP packet to an appropriate security service function, such as VoIP IPS.

3. VoIP IPS analyzes the headers and contents of the signal packet, such as IP address, calling number, and session description [RFC4566].

4. If VoIP IPS regards the packet as a spoofed packet by hackers or a scanning packet searching for VoIP/VoLTE devices, it requests the Switch Controller to block that packet and the subsequent packets that have the same call-id.

5. Switch Controller installs new rules (e.g., drop packets) into switches.

6. The illegal packets are dropped by switches.

For the above centralized VoIP/VoLTE security system, the existing SDN protocols can be used through standard interfaces between the VoIP IPS application and switches [RFC7149][ITU-T.Y.3300] [ONF-OpenFlow][ONF-SDN-Architecture].

Legacy hardware based VoIP IPSes have some challenges, such as provisioning time, the granularity of security, expensive cost, and the establishment of policy. The proposed framework can resolve the challenges through the above centralized VoIP/VoLTE security system based on SDN as follows:

- Provisioning: The provisioning time of setting up a legacy VoIP IPS to network is substantial because it takes from some hours to some days. By managing the network resources centrally, VoIP IPS can provide more agility in provisioning both virtual and physical network resources from a central location.

- The granularity of security: The security rules of a legacy VoIP IPS are compounded considering the granularity of security. The proposed framework can provide more granular security by centralizing security control into a switch controller. The VoIP IPS can effectively manage security rules throughout the network.

- Cost: The cost of adding VoIP IPS to network resources, such as routers, gateways, and switches is substantial due to the reason that we need to add VoIP IPS on each network resource. To solve this, each network resource can be managed centrally such that a single VoIP IPS is manipulated by a centralized server.

- The establishment of policy: Policy should be established for each network resource. However, it is difficult to describe what flows are permitted or denied for VoIP IPS within a specific organization network under management. Thus, a centralized view is helpful to determine security policies for such a network.

5.3. Attack Mitigation: Centralized DDoS-attack Mitigation System

For the centralized DDoS-attack mitigation system, a centralized DDoS-attack mitigation can manage each network resource and manipulate rules to each switch through a centralized server for DDoS-attack mitigation (called DDoS-attack Mitigator). The centralized DDoS-attack mitigation system defends servers against DDoS attacks outside private network, that is, from public network.

Servers are categorized into stateless servers (e.g., DNS servers) and stateful servers (e.g., web servers). For DDoS-attack mitigation, traffic flows in switches are dynamically configured by traffic flow forwarding path management according to the category of servers [AVANT-GUARD]. Such a managenent should consider the load balance among the switches for the defense against DDoS attacks.

The procedure of DDoS-attack mitigation operations in the centralized DDoS-attack mitigation system is as follows:

1. Switch periodically reports an inter-arrival pattern of a flow's packets to Switch Controller.

2. Switch Controller forwards the flow's inter-arrival pattern to an appropriate security service application, such as DDoS-attack Mitigator.

3. DDoS-attack Mitigator analyzes the reported pattern for the flow.

4. If DDoS-attack Mitigator regards the pattern as a DDoS attack, it computes a packet dropping probability corresponding to suspiciousness level and reports this DDoS-attack flow to Switch Controller.

5. Switch Controller installs new rules into switches (e.g., forward packets with the suspicious inter-arrival pattern with a dropping probability).

6. The suspicious flow's packets are randomly dropped by switches with the dropping probability.

For the above centralized DDoS-attack mitigation system, the existing SDN protocols can be used through standard interfaces between the DDoS-attack mitigator application and switches [RFC7149] [ITU-T.Y.3300][ONF-OpenFlow][ONF-SDN-Architecture].

The centralized DDoS-attack mitigation system has challenges similar to the centralized firewall system. The proposed framework can resolve the challenges through the above centralized DDoS-attack mitigation system based on SDN as follows:

- Cost: The cost of adding DDoS-attack mitigators to network resources such as routers, gateways, and switches is substantial due to the reason that we need to add DDoS-attack mitigator on each network resource. To solve this, each network resource can be managed centrally such that a single DDoS-attack mitigator is manipulated by a centralized server.

- Performance: The performance of DDoS-attack mitigators is often slower than the link speed of network interfaces. The checking of DDoS attacks may reduce the performance of the network interfaces. DDoS-attack mitigators can be adaptively deployed among network switches, depending on network conditions in the framework.

- The management of network resources: Since there may be hundreds of network resources in an administered network, the dynamic management of network resources for performance (e.g., load balancing) is a challenge for DDoS-attack mitigation. In the framework, as dynamic network resource management, traffic flow forwarding path management can handle the load balancing of network switches [AVANT-GUARD]. With this management, the current and near-future workload can be spread among the network switches for DDoS-attack mitigation. In addition, DDoS-attack mitigation rules can be dynamically added for new DDoS attacks.

- The establishment of policy: Policy should be established for each network resource. However, it is difficult to describe what flows are permitted or denied for new DDoS-attacks (e.g., DNS reflection attack) within a specific organization network under management. Thus, a centralized view is helpful to determine security policies for such a network.

So far this document has described the procedure and impact of the three use cases for networked security services using the I2NSF framework with SDN networks. To support these use cases in the proposed data-driven security service framework, YANG data models

described in [consumer-facing-inf-dm], [nsf-facing-inf-dm], and [registration-inf-dm] can be used as Consumer-Facing Interface, NSF-Facing Interface, and Registration Interface, respectively, along with RESTCONF [RFC8040] and NETCONF [RFC6241].

6. Security Considerations

The I2NSF framework with SDN networks in this document is derived from the I2NSF framework [i2nsf-framework], so the security considerations of the I2NSF framework should be included in this document. Therefore, proper secure communication channels should be used the delivery of control or management messages among the components in the proposed framework.

This document shares all the security issues of SDN that are specified in the "Security Considerations" section of [ITU-T.Y.3300].

7. Acknowledgements

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning).

This document has greatly benefited from inputs by Hyoungshick Kim, Jung-Soo Park, Se-Hui Lee, Jinyong Kim, Daeyoung Hyun, and Dongjin Hong.

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.

[i2nsf-framework] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", draft-ietf-i2nsf-framework-05 (work in progress), May 2017.

[RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, January 2017.

8.2. Informative References

[consumer-facing-inf-im] Kumar, R., Lohiya, A., Qi, D., Bitar, N., Palislamovic, S., and L. Xia, "Information model for Client-Facing Interface to Security Controller", draft-kumar-i2nsf-client-facing-interface-im-02 (work in progress), April 2017.

[consumer-facing-inf-dm] Jeong, J., Kim, E., Ahn, T., Kumar, R., and S. Hares, "I2NSF Consumer-Facing Interface YANG Data Model", draft-jeong-i2nsf-consumer-facing-interface-dm-02 (work in progress), July 2017.

[i2nsf-nsf-cap-im] Xia, L., Strassner, J., Basile, C., and D. Lopez, "Information Model of NSFs Capabilities", draft-xibassnez-i2nsf-capability-01 (work in progress), March 2017.

[nsf-facing-inf-dm] Kim, J., Jeong, J., Park, J., Hares, S., and L. Xia, "I2NSF Network Security Functions-Facing Interface YANG Data Model", draft-kim-i2nsf-nsf-facing-interface-data-model-02 , July 2017.

[registration-inf-im] Hyun, S., Jeong, J., Woo, S., Yeo, Y., and J. Park, "I2NSF Registration Interface Information Model", draft-hyun-i2nsf-registration-interface-im-02 (work in progress), July 2017.

[registration-inf-dm] Hyun, S., Jeong, J., Yeo, Y., Woo, S., and J. Park, "I2NSF Registration Interface YANG Data Model", draft-hyun-i2nsf-registration-dm-01 (work in progress), July 2017.

[nsf-triggered-steering] Hyun, S., Jeong, J., Park, J., and S.

Hares, "NSF-triggered Traffic Steering Framework", draft-hyun-i2nsf-nsf-triggered-steering-03 (work in progress), July 2017.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, March 2014.

[ITU-T.Y.3300] Recommendation ITU-T Y.3300, "Framework of Software-Defined Networking", June 2014.

[ONF-OpenFlow] ONF, "OpenFlow Switch Specification (Version 1.4.0)", October 2013.

[ONF-SDN-Architecture] ONF, "SDN Architecture", June 2014.

[ITU-T.X.1252] Recommendation ITU-T X.1252, "Baseline Identity Management Terms and Definitions", April 2010.

[ITU-T.X.800] Recommendation ITU-T X.800, "Security Architecture for Open Systems Interconnection for CCITT Applications", March 1991.

[AVANT-GUARD] Shin, S., Yegneswaran, V., Porras, P., and G. Gu, "AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks", ACM CCS, November 2013.

[ETSI-NFV] ETSI GS NFV 002 V1.1.1, "Network Functions Virtualisation (NFV); Architectural Framework", October 2013.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

Appendix A. Changes from draft-jeong-i2nsf-applicability-00

The following changes have been made from draft-jeong-i2nsf-applicability-00:

- Figure 1 is modified such that Security Controller and Switch Controller are directly connected with each other via NSF-Facing Interface for the security policy configuration.

Authors' Addresses

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4957
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Sangwon Hyun
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 290 7222
Fax: +82 31 299 6673
EMail: swhyun77@skku.edu
URI: http://imtl.skku.ac.kr/

Tae-Jin Ahn
Korea Telecom
70 Yuseong-Ro, Yuseong-Gu
Daejeon 305-811
Republic of Korea

Phone: +82 42 870 8409
EMail: taejin.ahn@kt.com

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA

Phone: +1-734-604-0332
EMail: shares@ndzh.com

Diego R. Lopez
Telefonica I+D
Jose Manuel Lara, 9
Seville, 41013
Spain

Phone: +34 682 051 091
EMail: diego.r.lopez@telefonica.com