

Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 5, 2018

J. Jeong
S. Hyun
Sungkyunkwan University
T. Ahn
Korea Telecom
S. Hares
Huawei
D. Lopez
Telefonica I+D
October 2, 2017

**Applicability of Interfaces to Network Security Functions to Network-
Based Security Services
draft-ietf-i2nsf-applicability-00**

Abstract

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

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 5, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Requirements Language	3
3.	Terminology	3
4.	I2NSF Framework	4
5.	Use Cases	6
5.1.	Firewall: Centralized Firewall System	6
5.2.	Deep Packet Inspection: Centralized VoIP/VoLTE Security System	7
5.3.	Attack Mitigation: Centralized DDoS-attack Mitigation System	9
6.	Security Considerations	11
7.	Acknowledgments	11
8.	Contributors	11
9.	References	12
9.1.	Normative References	12
9.2.	Informative References	12

1. Introduction

Interface to Network Security Functions (I2NSF) defined a framework and interfaces for interacting with Network Security Functions (NSFs). The I2NSF framework allows heterogeneous NSFs developed by different security solution vendors to be used in the NFV environment by utilizing the capabilities of such products and the virtualization of security functions in the NFV platform. In the I2NSF framework, each NSF initially registers the profile of its own capabilities into the system in order for themselves to be available in the system. In addition, the Security Controller registers itself to the I2NSF user so that the user can request security services to the Security Controller.

This document describes the applicability of I2NSF to network-based security services with use cases, such as firewall [[opsawg-firewalls](#)], Deep Packet Inspection (DPI), and Distributed Denial of Service (DDoS) attack mitigation. We implemented the I2NSF framework based on SDN for these use cases, and the implementation successfully verified the effectiveness of the I2NSF framework.

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](#)], [[i2nsf-terminology](#)], [[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:

- o Software-Defined Networking (SDN): 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](#)].
- o Firewall: A service function 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, for example, disallowed port numbers or IP

addresses.

- o Centralized Firewall System: A centralized firewall that can establish and distribute 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 virtual network function (VNF).
- o Centralized VoIP Security System: A centralized security system that handles the security functions required for 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.
- o 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. The SDN controller and switches can cooperatively work as a network-based firewall system through a standard interface between an SDN switch and a firewall function as a VNF running in the SDN controller.

4. I2NSF Framework

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

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

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

The Security Controller requests NSFs to perform low-level security services via the NSF-Facing Interface. The NSFs are enabled as Virtual Network Functions (VNFs) on top of virtual machines through Network Functions Virtualization (NFV) [[ETSI-NFV](#)]. The Security Controller also instructs the Switch Controller to perform their

required security services on switches under the supervision of Switch Controller (i.e., SDN Controller). In addition, the Security Controller uses the I2NSF Registration Interface [[registration-inf-im](#)][[registration-inf-dm](#)] to communicate with Developer's Management System (called Developer's Mgmt System) for registering (or deregistering) the developer's NSFs into (or from) the NFV system using the I2NSF framework.

The Consumer-Facing Interface between an I2NSF User and the Security Controller can be implemented using, for example, RESTCONF [[RFC8040](#)]. Data models specified by YANG [[RFC6020](#)] describe high-level security policies to be specified by an I2NSF User. The data model defined in [[consumer-facing-inf-dm](#)] can be used for the I2NSF Consumer-Facing Interface.



Figure 1: An I2NSF Framework with SDN Networks

The NSF-Facing Interface between Security Controller and NSFs can be implemented using NETCONF [[RFC6241](#)]. YANG data models describe low-level security policies for the sake of NSFs, which are translated from the high-level security policies by the Security Controller. The data model defined in [[nsf-facing-inf-dm](#)] can be used for the I2NSF NSF-Facing Interface.

The Registration Interface between the Security Controller and the Developer's Mgmt System can be implemented by RESTCONF [[RFC8040](#)]. The data model defined in [[registration-inf-dm](#)] can be used for the I2NSF Registration Interface.

Also, the I2NSF framework can enforce multiple chained NSFs for the low-level security policies by means of service function chaining (SFC) techniques for the I2NSF architecture described 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. [[RFC8192](#)]

5.1. Firewall: 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 this system is as follows:

1. A switch forwards an unknown flow's packet to one of the Switch Controllers.
2. The Switch Controller forwards the unknown flow's packet to an appropriate security service application, such as the Firewall.
3. The Firewall analyzes, typically, the headers and contents of the packet.
4. If the Firewall regards the packet as a malicious one with a suspicious pattern, it reports the malicious packet to the Switch Controller.
5. The Switch Controller installs new rules (e.g., drop packets with the suspicious pattern) into underlying switches.

6. The suspected packets are dropped by these switches.

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:

- o 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.
- o 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.
- o The management of access control: Since there may be hundreds of network resources in a 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.
- o 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.
- o 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

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 Intrusion Prevention System (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 this system is as follows:

1. A switch forwards an unknown call flow's signal packet (e.g., SIP packet) to the Switch Controller. Also, if the packet belongs to a matched flow's packet related to SIP (called matched SIP packet), the Switch forwards the packet to the Switch Controller so that the packet can be checked by an NSF for VoIP (i.e., VoIP IPS) via the Switch Controller, which monitors the behavior of its SIP call.
2. The 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 addresses, calling number, and session description headers [[RFC4566](#)].
4. If, for example, 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. The Switch Controller installs new rules (e.g., drop packets) into underlying switches.
6. The illegal packets are dropped by these switches.

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 IPS has some challenges, such as provisioning time, the granularity of security, expensive cost, and the establishment of policy. The I2NSF framework can resolve the challenges through the above centralized VoIP/VoLTE security system based on SDN as follows:

- o 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.

- o 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.
- o 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.
- o 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

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 management should consider the load balance among the switches for the defense against DDoS attacks.

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

1. A Switch periodically reports an inter-arrival pattern of a flow's packets to one of the Switch Controllers.
2. The Switch Controller forwards the flow's inter-arrival pattern to an appropriate security service application, such as DDoS-attack Mitigator.
3. The DDoS-attack Mitigator analyzes the reported pattern for the flow.
4. If the 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. The 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:

- o 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.
- o 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.
- o 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.
- o 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 network-based 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. Acknowledgments

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).

8. Contributors

I2NSF is a group effort. I2NSF has had a number of contributing authors. The following are considered co-authors:

- o Hyounghshick Kim (Sungkyunkwan University)
- o Jung-Soo Park (ETRI)
- o Tae-Jin Ahn (Korea Telecom)
- o Se-Hui Lee (Korea Telecom)
- o Mohamed Boucadair (Orange)

9. References

9.1. 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-07](#) (work in progress), August 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.

9.2. Informative References

- [consumer-facing-inf-im] Kumar, R., Lohiya, A., Qi, D., Bitar, N., Palislaamovic, S., and L. Xia, "Information model for Client-Facing Interface to Security Controller", [draft-kumar-i2nsf-client-facing-interface-im-03](#) (work in progress), July 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-04](#) (work in progress), October 2017.
- [i2nsf-nsf-cap-im] Xia, L., Strassner, J., Basile, C., and D. Lopez, "Information Model of NSFs Capabilities", [draft-ietf-i2nsf-capability-00](#) (work in progress), September 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-03](#) (work in progress), October 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, "Service Function Chaining-Enabled I2NSF Architecture", [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.
- [i2nsf-terminology] Hares, S., Strassner, J., Lopez, D., Xia, L., and H. Birkholz, "Interface to Network Security Functions (I2NSF) Terminology", [draft-ietf-i2nsf-terminology-04](#) (work in progress), July 2017.
- [opsawg-firewalls] Baker, F. and P. Hoffman, "On Firewalls in Internet Security", [draft-ietf-opsawg-firewalls-01](#) (work in progress), October 2012.
- [RFC8192] Hares, S., Lopez, D., Zarny, M., Jacquenet, C., Kumar, R., and J. Jeong, "Interface to Network Security Functions (I2NSF): Problem Statement and Use Cases", [RFC 8192](#), July 2017.

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://imt1.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

