Workgroup: I2NSF Working Group
Internet-Draft:
draft-kim-i2nsf-security-controller-interface-
dm-00
Published: 24 October 2022
Intended Status: Standards Track
Expires: 27 April 2023
Authors: J. Kim
Sungkyunkwan University
P. Lingga
Sungkyunkwan University
R. Marin-Lopez
University of Murcia
J. Jeong, Ed.
Sungkyunkwan University
S. Hares
Huawei

I2NSF Security Controller-Facing Interface YANG Data Model for Cross-Domain IPsec Flow Protection

Abstract

This document defines an information model and a YANG data model for the Security Controller-Facing Interface between two security controllers in an Interface to Network Security Functions (I2NSF) framework. This interface is used for the exchange of IPsec flow protection information between two Network Security Functions (NSFs) in cross-domain environments. The YANG data model in this document is built on the basis of the YANG data model for IPsec flow protection based on Software-Defined Networking (SDN).

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 https://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 27 April 2023.

Table of Contents

1. Introduction

Interface to Network Security Functions (I2NSF) defines a framework and its interfaces for the security management and monitoring of Network Security Functions (NSFs) for security services. The NSFs are manufactured by different vendors [RFC8329]. I2NSF allows users to easily configure security policies on a target network. In an I2NSF framework, NSFs are network functions that are used to defend a target network against various security attacks such as Distributed Denial of Service (DDoS) attacks, viruses, and data breaches.

To support multiple security services for a traffic flow with multiple NSFs, a Service Function Chaining (SFC) [RFC7665] can be used. In SFC, the integrity and confidentiality of security services between the NSFs must be guaranteed. [RFC9061] protects the flow between NSFs with a centralized security controller by generating, managing, and distributing the keys of NSFs. Flow protection covered in this document describes the flow protection and key management process (i.e., IKE case and IKE-less case) between NSFs within the

coverage of I2NSF managed by one security controller, i.e., within one I2NSF domain (e.g., an autonomous system (AS)).

However, recently, the concept of Software-Defined Wide Area Network (SD-WAN) was introduced to manage multiple SDN infrastructures. The goal of SD-WANs is to provide flexible and automated deployment from a centralized point to enable on-demand network security services, such as IPsec Security Association (SA) management [RFC9061]. To meet this goal of SD-WAN, a centralized point that can manage multiple I2NSF domains is needed. In addition, it was necessary to introduce a new interface for centralized management of NSFs existing on different I2NSF domains, i.e., a cross-domain environment (multiple ASs). Also, flow protection for collaboration and exchanging information between NSFs located in different I2NSF domains are needed in such cross-domain environments.

In order to manage controllers in different I2NSF domains together, an interface that can exchange information (security policies, IPsec parameters) between security controllers in cross-domain environments for flow protection between NSFs located in different I2NSF domains and policy delivery is essential.

Therefore, this document proposes an information model and a YANG data model for a Security Controller-Facing Iterface for exchanging information between security controllers to manage the security policy and flow protection among NSFs in cross-domain environments.

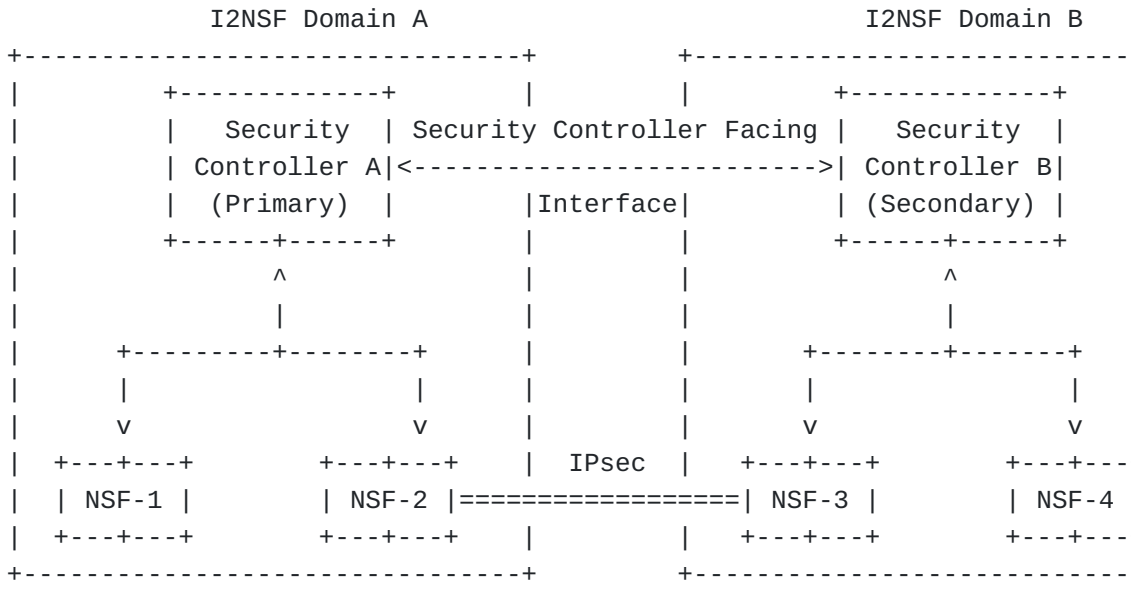

Figure 1: I2NSF Framework for Cross-Domain IPsec Flow Protection

Figure 1 illustrates two I2NSF systems located in different I2NSF domains. To let NSFs of different I2NSF systems, which have their own security controller, communicate with each other, a security controller can be used as the intermediary. Two security controllers in different domains MUST have a secure and trust connection, this connection is out of the scope of this document. Through this secure connection, the security controller, which is a primary as a coordinator for other security controllers, can receive the IPsec parameters of secondary security controllers and can establish IPsec SA with secondary security controllers. The primary security controller can act as a centralized controller and can exchange information about managed NSFs safely through the Security Controller-Facing Interface (SFI) with all connected security controllers as secondaries.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

I2NSF Domain: An area that one I2NSF security controller can manage the security services of all the flows in its domain.

Cross-Domain: An environment where multiple I2NSF domains (e.g., ASs) exist and are able to exchange information among the security controllers.

3. Information Model for Security Controller-Facing Interface

In [RFC9061], the I2NSF security controller enables the key management procedure to be performed for flow protection between NSFs in an I2NSF domain it manages. Therefore, this section introduces the information model for exchanging information in different domains using Security Controller-Facing Interface (SFI) between I2NSF Security Controllers to provide flow protection between NSFs existing in different I2NSF domains.

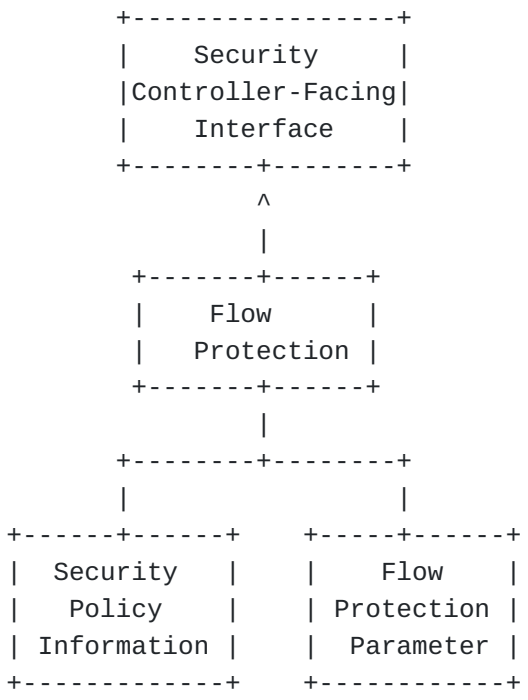

Figure 2: Diagram for Security Controller-Facing Interface

Figure 1 shows the high-level concept of SFI to deliver cross-domain flow protection for IPsec. Information that can be delivered through SFI is as follows:

*Flow Protection Parameters: Parameters required to establish IPsec Security Associations (SAs) [RFC9061]. To establish IPsec SAs with NSFs located in a different domain, the security controller MUST be able to securely exchange the necessary parameters for those SAs.

*Security Policy Information: Security policy information to configure the security policy rules [I-D.ietf-i2nsf-nsf-facing-interface-dm] of NSFs located in a cross-domain environment. The security controller can deliver the security policy rules to the other I2NSF domains security controller through SFI. After receiving the security policy, the security controller can deliver the security policy to the target NSFs via the NSF-Facing Interface [I-D.ietf-i2nsf-nsf-facing-interface-dm].

3.1. Use Cases for the Security Controller-Facing Interface in Cross-Domain Environments

3.1.1. Use Case of Peer-to-Peer Security Controllers

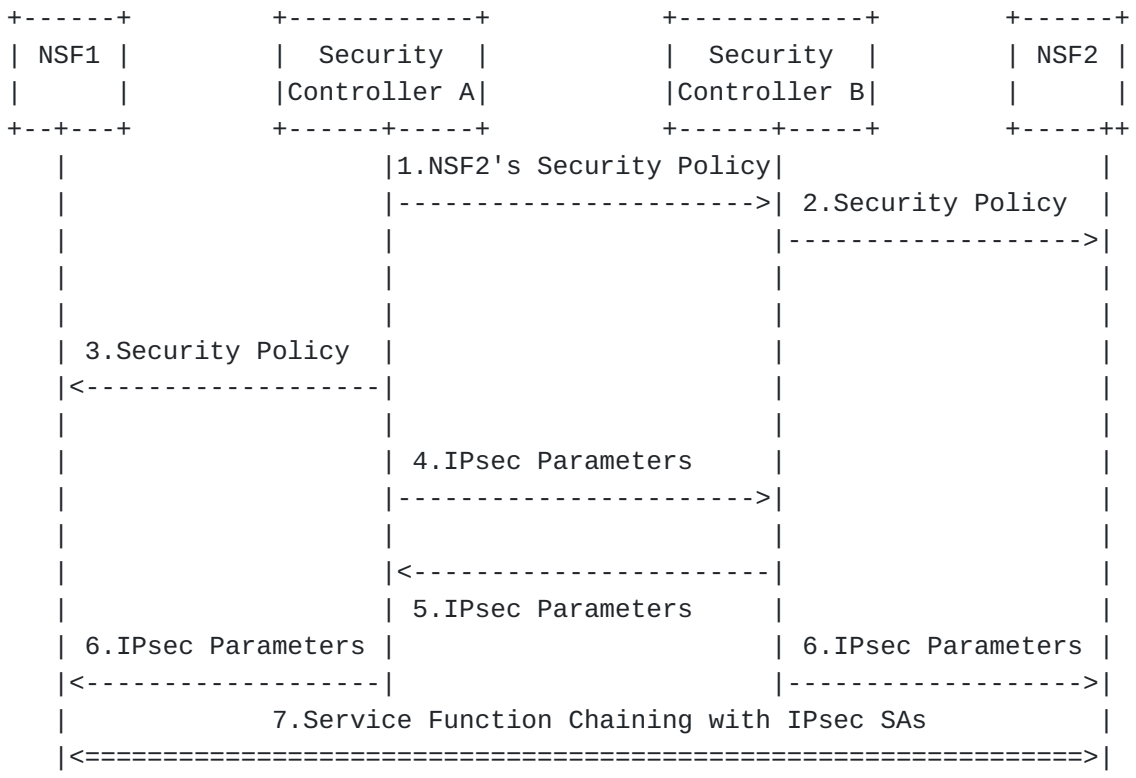

Figure 3: Use Case of the Peer-to-Peer Security Controllers

Figure 3 shows a message sequence between entities in multiple domains. In the case where an I2NSF user requests a security service that cannot be provided by the NSFs (e.g., BGP peers) in its own I2NSF domain, the security controller may request a trusted security controller in a different I2NSF domain for the required security service. In this scenario, it is assumed that the secure connection between the two security controllers is already set. The detailed sequence is as follows:

1. Security controller A delivers the security policy for NSF2 through SCFI via security controller B in a cross-domain environment.

2. If security controller B can handle the received security policy, it delivers the security policy to the target NSF, i.e., NSF2, through the NFI.

3. Security controller A also delivers the security policy for the NSF in its own I2NSF domain that can handle the security policy, i.e., NSF1, through the NFI.

4. Security controller A delivers IPsec parameters for NSF2 to establish IPsec SAs with NSF1 located in a cross-domain environment to security controller B.

5. Security controller B delivers IPsec parameters for NSF1 to establish IPsec SAs with NSF2 located in a cross-domain environment to security controller A.

6. Security controller A and security controller B deliver the IPsec parameters to the NSF1 and NSF2, respectively.

7. NSF1 and NSF2 establish an IPsec SAs using the received IPsec parameters and provide the requested security service to the user through SFC.

3.1.2. Use Case of Hierarchical Distribution Security Controllers

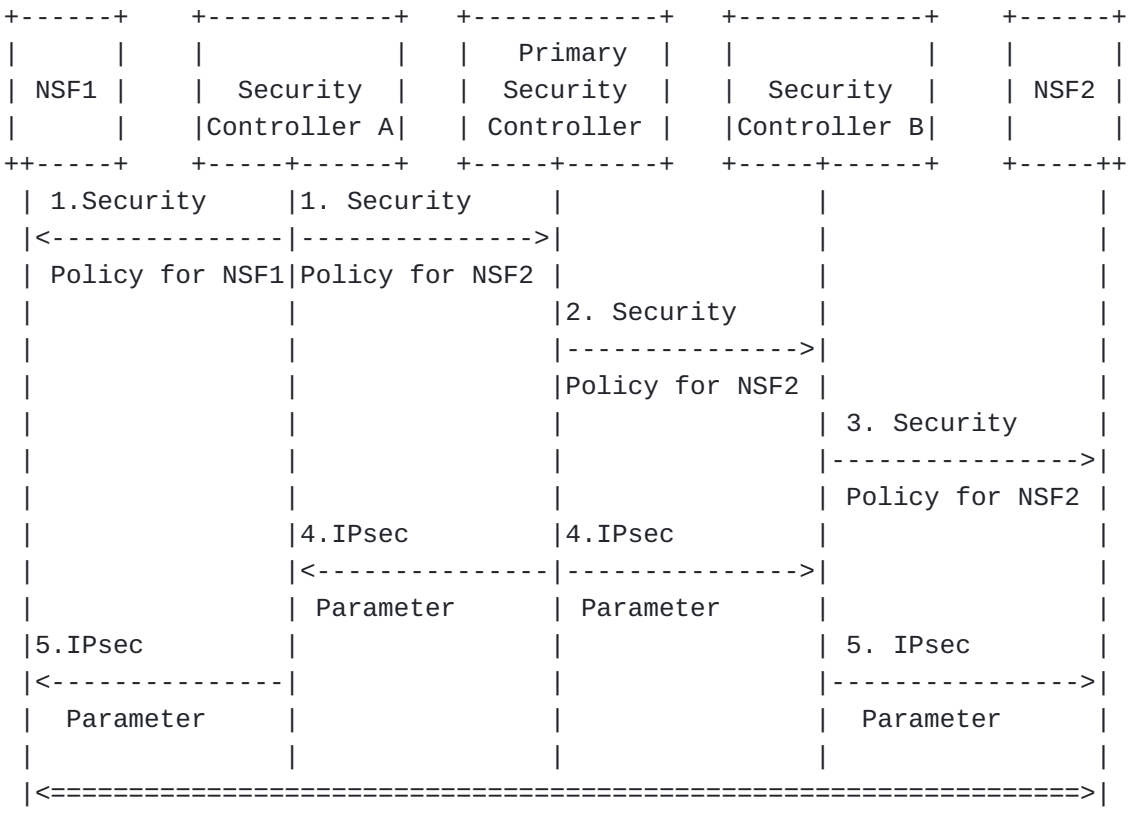

Figure 4: Use Case of the Hierarchical Distribution Security Controllers

Figure 4 shows a message sequence between entities in multiple domains with a primary security controller. In the case where an I2NSF user requests a security service that the NSFs cannot be provided in its I2NSF domain, the security controller may request the primary security controller for the required security service. In this scenario, it is assumed that the secure connections between the security controllers and the primary security controller are

already set. Also, it is assumed that the primary security controller has all the necessary IPsec parameters in advance. The detailed sequence is as follows:

1. Security controller A delivers the security policy through SFI to the primary security controller and delivers the security policy to NSF1 via NFI.

2. The primary security controller delivers the received security policy to the security controller that can provide the requested security services, i.e., security controller B.

3. Security controller B delivers the security policy it can handle to the target NSF, i.e, NSF2, through the NFI.

4. The primary security controller delivers the IPsec parameters to establish IPsec SAs between NSF1 and NSF2 located in different I2NSF domains to the responsible security controllers.

5. Security controller A and security controller B deliver the IPsec parameters to the NSF1 and NSF2, respectively.

6. NSF1 and NSF2 establish an IPsec SAs using the received IPsec parameters and provide the requested security service to the user through SFC.

4. IANA Considerations

This document does not require any IANA actions.

5. Security Considerations

The same security considerations for the I2NSF framework [RFC8329] are applicable to this document.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8329] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, DOI 10.17487/RFC8329, February 2018, <https://www.rfc-editor.org/info/rfc8329>.

[RFC9061] Marin-Lopez, R., Lopez-Millan, G., and F. Pereniguez-Garcia, "A YANG Data Model for IPsec Flow Protection Based on Software-Defined Networking (SDN)", RFC 9061, DOI 10.17487/RFC9061, July 2021, <https://www.rfc-editor.org/info/rfc9061>.

6.2. Informative References

[I-D.ietf-i2nsf-nsf-facing-interface-dm] Kim, J. T., Jeong, J. P., Park, J., Hares, S., and Q. Lin, "I2NSF Network Security Function-Facing Interface YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-i2nsf-nsf-facing-interface-dm-29, 1 June 2022, <https://www.ietf.org/archive/id/draft-ietf-i2nsf-nsf-facing-interface-dm-29.txt>.

Appendix A. Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT)(No. 2022-0-01015, Development of Candidate Element Technology for Intelligent 6G Mobile Core Network).

This work was supported in part by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT)(No. 2022-0-01199, Regional strategic industry convergence security core talent training business).

Appendix B. Contributors

This document is made by the group effort of I2NSF WG. Many people actively contributed to this document, such as Linda Dunbar, Yoav Nir, and Diego R. Lopez. The authors sincerely appreciate their contributions.

The following are co-authors of this document:

Jiyong Uhm - Department of Computer Science and Engineering, Sungkyunkwan University, 2066 Seobu-Ro Jangan-Gu, Suwon, Gyeonggi-do 16419, Republic of Korea. EMail: jiyong423@skku.edu

Jung-Soo Park - Electronics and Telecommunications Research Institute, 218 Gajeong-Ro, Yuseong-Gu, Daejeon, 34129, Republic of Korea. EMail: pjs@etri.re.kr

Yunchul Choi - Electronics and Telecommunications Research Institute, 218 Gajeong-Ro, Yuseong-Gu, Daejeon, 34129, Republic of Korea. EMail: cyc79@etri.re.kr

Gabriel Lopez-Millan - University of Murcia, Faculty of Computer Science, Campus de Espinardo S/N, 30100 Murcia, Spain. Phone: +34 868 88 85 04, EMail: gabilm@um.es

Fernando Pereniguez-Garcia - University Defense Center, Spanish Air Force Academy, MDE-UPCT, 30720 San Javier Murcia, Spain. Phone: +34 968 18 99 46, EMail: fernando.pereniguez@cud.upct.es

Authors' Addresses

Jeonghyeon Joshua Kim
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4957
Email: jeonghyeon12@skku.edu

Jaehoon Paul Jeong (editor)
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

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

Patrick Lingga
Department of Electrical and Computer Engineering

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

Phone: +82 31 299 4957
Email: patricklink@skku.edu

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
United States of America

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

Rafa Marin-Lopez
University of Murcia
Faculty of Computer Science
Campus de Espinardo S/N
30100 Murcia
Spain

Phone: +34 868 88 85 01
Email: rafa@um.es