Network Service Header (NSH) Context Header Allocation (Network Security)
draft-wang-sfc-nsh-ns-allocation-01

Abstract

This document provides a recommended default allocation of the mandatory fixed context headers for a Network Service Header (NSH) relevant to Service Function Chaining (SFC) for network security Service Functions. NSH is defined in [I-D.ietf-sfc-nsh]. This allocation is intended to support the use cases described in [I-D.wang-sfc-ns-use-cases].

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 http://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 April 23, 2017.

Copyright Notice

Copyright (c) 2016 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
1. Introduction

Service Function Chaining (SFC) provides a mechanism for network traffic to go through a set of Service Functions in sequence. Network Service Header (NSH) allows metadata to be shared between Service Functions along with the packets. Such metadata is carried by either a fixed number of 32-bit context headers (MD-Type 1) or a variable number of TLVs (MD-Type 2), as defined in NSH [I-D.ietf-sfc-nsh]. This document provides a recommended default allocation of the fixed size context headers for network security Service Functions forming a Service Function Chain. The allocation may also form a MD-Type 2 metadata TLV. Supporting use cases for a metadata definition in this context are described in SFC-NS-Use-Cases [I-D.wang-sfc-ns-use-cases]. This document does not define any other variable TLVs. It does not address the control plane mechanisms.

1.1. 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].

2. Definition Of Terms

This document uses the terms as defined in RFC 7498 [RFC7498], [RFC7665] and [I-D.ietf-sfc-nsh].
3. Network Service Header (NSH) Context Headers

NSH MD-Type 1 is composed of three parts as described in
[I-D.ietf-sfc-nsh]: a 4-byte base header, a 4-byte service path
header, and four 4-byte mandatory context headers.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Ver|O|C|R|R|R|R|R|   Length  |  MD-Type = 1  | Next Protocol |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Service Path ID                      | Service Index |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Mandatory Context Header                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Mandatory Context Header                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Mandatory Context Header                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Mandatory Context Header                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 1: Network Service Header - MD-Type 1

4. Recommended Security Mandatory Context Allocation

The following context header allocation provides information used to
support SFC operation within a generic network security environment.
The 16-byte context headers are used to deliver metadata and
classification results between security Service Functions. Service
Functions may use the metadata for local policy enforcement, security
actions, classification refinement, and other functionality.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              D|   Reserved  |               Tenant ID                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Destination Class / Reserved |        Source Class           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Reserved            | Dest Score    |  Src Score    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 2: NSH Security Context Allocation
4.1. Network Security Allocation Specifics

The specific 16-byte allocation of the mandatory context headers is as follows:

Session ID: Session ID is used to identify a particular connection, transaction, or any unit that the security Service Functions use to maintain states. Session ID may be used to associate a packet with existing states even if the packet does not contain all the network headers for deriving the Session ID, or if the network headers are modified by a Service Function. It may appear in events and logs for correlation between Service Functions in the SFC-domain.

The Session SHOULD be bi-directional so that both directions of Service Paths are associated with the same Service Function instance. Service Path reclassification for the same session MUST not change the Session ID.

Flag bits: Bits 0-7 of the 2nd word are flag bits. Only bit 0 is defined in this document and the remaining bits are reserved.

D bit: The D-bit is used to indicate whether the Destination Class field in the 3rd word is used. If D-bit is not set then the 3rd word is reserved.

Tenant ID: The tenant identifier is used to represent the tenant or security policy domain that the Service Function Chain is being applied to. The Tenant ID is a unique value assigned by a control plane. The distribution of Tenant ID’s is outside the scope of this document. As an example application of this field, the first node on the Service Function Chain may insert a VRF number, VLAN number, VXLAN VNI or a policy domain ID.

Destination Class: The destination class represents the logical classification of the destination of the traffic. This field is optional and/or the Destination Class may not be known. The D-bit is used to indicate that this field contains a valid Destination Class.

Source Class: represents the logical classification of the source of the traffic. For example, this might represent a source application, a group of like endpoints, or a set of users originating the traffic. This grouping is done for the purposes of applying policy. Policy is applied to groups rather than individual endpoints.
The 4th word contains security classification results for communicating immediate actions and accumulated verdicts to downstream Service Functions.

Score: Security Score is a numeric value for participating Service Functions to deliver security classification results based on their processing of the packet data. The Score value may be set by one Service Function and refined by a subsequent Service Function to produce an accumulated result. Alternatively, each Service Function may set a different score value which is collected by a control point. The Score value is interpreted consistently in the SFC-domain. For example, a Score value of -5 may trigger additional scanning functions to be conducted by the subsequent Service Function for the Session. As another example, a Score value -20 may result in block of the source or destination host by a Service Function. The interpretation of the Score is distributed by a control plane and is outside the scope of the document.

5. Context Allocation and Control Plane Considerations

This document describes an allocation scheme for the NSH context headers in the context of network security SFC use cases.

The suggested allocation in this document would be considered as a guideline only. Some of the allocated fields are specific to certain use cases. A control plane mechanism is required to ensure consistency among the SFC components participating in the allocation scheme. The actual control plane mechanism is out of the scope of this document.

6. Security Considerations

The SFC control plane responsible for identifying and distributing the allocation scheme should ensure the communication mechanism is secure.

The metadata defined in this document carries important information for participating Service Functions to make security policy decisions. Some of the metadata such as the security score may be accumulated before a Service Function takes an action. There is a risk that the metadata may be intercepted or even spoofed by an unauthorized party. Proper precaution must be taken to ensure the confidentiality and integrity of the metadata fields.
7. Acknowledgments

Authors would like to thank Jeremy Felix and Jay Iyer for their contributions.

8. IANA Considerations

This document includes no request to IANA.

9. References

9.1. Normative References

[I-D.ietf-sfc-nsh]


9.2. Informative References

[I-D.wang-sfc-ns-use-cases]

Authors’ Addresses

Eric Wang
Cisco Systems Inc.
170 W Tasman Dr
San Jose, CA 95134
U.S.A.

Email: ejwang@cisco.com