Abstract

This document introduces the security extension of the VXLAN encapsulation.

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/1id-abstracts.html

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

Copyright and License Notice

Copyright (c) 2015 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
Network Virtualization Overlays (NVO3) enable network virtualization for data center networks environment that assumes an IP-based underlay.

[GUE] specifies a security extension of the UDP tunnel, which can be used to secure the network virtualization overlay over IP networks. However, [GUE] does not apply to VXLAN encapsulation which has already been deployed some where.

VXLAN encapsulation is specified in [RFC7348]. In this document, security is specified as an optional field of the VXLAN header. This extension exposes the VNI to the NVEs. In other words, it allows per VNI security configuration. For example, VNI 1 enables the security transportation while VNI 2 disables the security transportation.

2. Acronyms and Terminology

2.1. Acronyms and Terms

VXLAN: Virtual eXtensible Local Area Network

NVO3: Network Virtualization Overlays

2.2. Terminology

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].
Familiarity with [RFC7348] is assumed in this document.

3. Protocol Extension

In the VXLAN header, two bits (bit 9 and bit 10) are used to indicate the security extension.

VXLAN Header and Body:

```
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
| R | R | R | R | I | R | R | R | SEC | Reserved         |
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
|                | VXLAN Network Identifier (VNI) | Reserved       |
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
|                | Security Parameters Index (SPI) |
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
|                | Sequence Number |
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
|                | Payload Data* (variable) |
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
```

Figure 3.1: The security extension of VXLAN header and body.

4. Backward Compatibility
Legacy devices that do not support the security extension in this document will simply ignore the optional Security field. The Security field being received will be incorrectly processed as the Ethernet header. In other words, the extension specified in this document is not backward compatible. When there is a connection between a legacy VXLAN device and a new VXLAN device, the Security feature of the new VXLAN device defined in this document MUST be disabled. By doing this, the new VXLAN device simple downgrades to a legacy VLAN device.

5. Security Considerations

This document introduces the per VNI security for VXLAN.

6. IANA Considerations

The document does not require any IANA action. RFC editor, please remove this section before publication.

7. References

7.1. Normative References


7.2. Informative References

Author’s Addresses

Yuanjiao Liu
Huawei Technologies
No.156 Beiqing Rd. Haidian District,
Beijing 100095 P.R. China
EMail: liuyuanjiao@huawei.com

Wenhui Li
Huawei Technologies
No.156 Beiqing Rd. Haidian District,
Beijing 100095 P.R. China
EMail: jason.liwenhui@huawei.com