Geneve encapsulation for Group Based Policy
draft-lemon-geneve-gbp-02

Abstract

This document describes how a Group Policy Identifier is encapsulated in Geneve for the purposes of policy enforcement.

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 September 12, 2019.

Copyright Notice

Copyright (c) 2019 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 (https://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.
1. Introduction

This document defines the group-based policy (GBP) encapsulation for Geneve [I-D.ietf-nvo3-geneve]. The GBP sub-header carries a 16-bit group policy ID that is semantically equivalent to the 16-bit group policy ID defined in [I-D.smith-vxlan-group-policy].

Group-based policy provides a more scalable alternative to access control lists (ACLs) by allowing separation of source marking and destination enforcement. This allows a decrease in the amount of information needed at each entry node, rather than a cross product of every possible source and every possible destination. It also allows assigning source marking based many different possibilities, not just the source address. It also allows not having to know where the packet will end up since whatever the destination is can enforce the policy specific to the destination service.

1.1. Conventions

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 [RFC2119].

1.2. Abbreviations used in this document

GBP: Group-Based Policy

Geneve: Generic Network Virtualization Encapsulation

2. Treatment By Intermediate Nodes

Any receiving device may use the group policy information contained in the Group-Based Policy (GBP) sub-header. If an intermediate device applies policy based upon the GBP sub-header, then it must set the Policy Applied Bit, described below.
If an intermediate device terminates the Geneve tunnel and reencapsulates the data in a new tunnel with the ability to convey the group policy information, it SHOULD propagate the group policy information and the Policy Applied bit into the new tunnel, unless there is an explicit policy not to do so.

3. Group Based Policy Encapsulation in Geneve

For encapsulating group policy IDs into Geneve [I-D.ietf-nvo3-geneve] the group policy ID field is included in the Geneve header using tunnel options. The group policy ID field uses a tunnel option class specific for GBP. In an administrative domain where GBP is used, insertion of the GBP tunnel option in Geneve is enabled at the Geneve tunnel endpoints. The Geneve header is defined in [I-D.ietf-nvo3-geneve]. GBP semantics are described in [I-D.smith-vxlan-group-policy].

The packet format of the GBP ID when encapsulated in Geneve is defined below.

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|Ver|  Opt Len  |O|C|    Rsvd.  |          Protocol Type        |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|        Virtual Network Identifier (VNI)       |    Reserved   |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|  Option Class = GBP           |  Type         |R|R|R| Length  |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|            GBP ID             |A|D|  Rsvd |Ver|   Reserved    | ID
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Figure 1: Group Based Policy as a Geneve Tunnel Option

The GBP header consists of 8 octets, as illustrated in Figure 1. The first 4 octets are the Geneve Tunnel Option header [I-D.ietf-nvo3-geneve], whose format is as follows:

Option Class: 16-bit unsigned integer that determines the GBP option class. The value is from the IANA registry setup for Geneve option classes as defined in [I-D.ietf-nvo3-geneve].

Type: 8-bit unsigned integer defining the GBP ID type. Two values are defined:

GBP_Source_ID: The Group Policy ID associated with the source of the packet. The allocation of Group Policy ID values is outside the scope of this document.
GBP_Destination_ID: The Group Policy ID associated with the end
destination of the packet. The allocation of Group Policy ID
values is outside the scope of this document.

Note that if the packet carries a GBP_Destination_ID, it MUST also
carry a GBP_Source_ID.

R (3 bits): Option control flags reserved for future use. MUST be
zero on transmission and ignored on receipt.

Length: 5-bit unsigned integer. Length of the GBP HDR in 4-octet
units.

The next 4 octets are the GBP header, whose format is as follows:

Group Policy ID: 16-bit group policy identifier as as defined in
[I-D.smith-vxlan-group-policy].

Policy Applied bit (A bit): The A bit is set to 0 to indicate that
the group policy has not (yet) been applied to this packet. Group
policies MUST be applied by devices when the A bit is set to 0 and
the destination group has been determined. Devices that apply the
group policy MUST set the A bit to 1 after the policy has been
applied. The A bit is set to 1 to indicate that the group policy
has already been applied to this packet. Policies that redirect
the packet MUST NOT be applied by devices when the A bit is set.
Policies that cause the packet to be dropped MAY be applied.

Don’t Learn bit (D bit): The D bit is set to 1 to indicate that the
tunnel endpoint MUST NOT learn the source address of the
encapsulated frame.

Rsvd (4 bits): reserved for future use. MUST be zero on
transmission and ignored on receipt.

Ver (2 bits): indicates the Version of the Group Policy sub-header.
The initial version is 0.

Reserved (8 bits): reserved for future use. MUST be zero on
transmission and ignored on receipt.

4. IANA Considerations

IANA is requested to allocate a Geneve "option class" number for GBP:
5. Security Considerations

The security considerations of Geneve are discussed in [I-D.ietf-nvo3-geneve]. The security considerations of GBP are discussed in [I-D.smith-vxlan-group-policy]. Additionally, the security policy value carried in the GBP header impacts security directly. There is a risk that this identifier could be altered. Accordingly, the network should be designed such that this header can be inserted only by trusted entities, and can not be altered before reaching the destination. This can be mitigated through physical security of the network and/or by encryption or validation of the entire packet, including the GBP.

6. Normative References


Authors’ Addresses

John Lemon (editor)
Broadcom Inc.
270 Innovation Drive
San Jose, CA  95134
USA

Email: john.lemon@broadcom.com