Geneve encapsulation for Group Based Policy
draft-lemon-geneve-gbp-03

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 November 1, 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 shim header carries a group policy ID that is semantically equivalent to the 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) shim header. If an intermediate device applies policy based upon the GBP shim header, then it must set the Policy Applied Bit, described below.

Because the group policy information is associated with the payload (rather than the tunnel or other means by which it is conveyed), 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. If an intermediate device can propagate only some of the group policy IDs, it SHOULD propagate as many as it can, and it MUST select which ones to propagate by the sequence that the GBP IDs are placed in the Geneve header.

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 with a narrow Group Policy ID is shown in Figure 1.

```
0                   1                   2                   3
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        |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Hdr
|        Virtual Network Identifier (VNI)       |    Reserved   |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--+
|  Option Class = GBP           |  Type         |R|R|R| Length  |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ GBP
|A|   Rsvd  |Ver|    Reserved   |       Group Policy ID         | ID
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-<+-
```

Figure 1: Group Based Policy as a Geneve Option Shim
The GBP shim header consists of 8 octets, as illustrated in Figure 1. The first 4 octets are the Geneve Tunnel Option shim 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. The following values are defined:

0x00: GBP_Source_ID. A value of 0 indicates that this shim header carries the Group Policy ID associated with the source of the packet.

0x01: GBP_Destination_ID. A value of 1 indicates that this shim header carries the Group Policy ID associated with the end destination of the packet.

0x02 to 0x7F: Unassigned. For assignment by IANA, as described in Section 5.

0x80 to 0xFF: Locally Assigned. For local assignment.

If a packet carries a GBP_Destination_ID, it SHOULD 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 excluding the option header. The value of this field is 1 for this version.

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

Policy Applied bit (A bit): The A bit MUST be set on a specific GBP shim header if a frame is returned to a forwarding instance that it has already visited after having been redirected at a forwarding instance along the native forwarding path to its destination by a redirection policy that matched on the value in that specific GBP shim header. If a GBP option type has the A bit set, a redirection policy that matches on this GBP option type MUST not be applied. Redirection policies MAY continue to be applied so long as they only match on GBP option types that do not have the A bit set. This procedure is necessary to prevent forwarding loops. The method that ensures that on returned frames...
the A bit is applied only to GBP option types involved in the match at the original redirection policy is outside the scope of this draft. Once an A bit is set on a GBP shim header, it MUST remain set. Additionally, once a GBP ID is set for a GBP option type it SHOULD not be changed to avoid redirection related loops.

Rsvd (5 bits): reserved for future use. MUST be zero on transmission and ignored on receipt.

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

Reserved (8 bits): When using a 16-bit Group Policy ID, these 8 bits are reserved for future use and MUST be set to zero on transmission and ignored on receipt.

Group Policy ID: 16-bit identifier that indicates the Group Policy ID being encapsulated by this GBP shim header. The Default GBP ID value is special and indicates that the GBP option was not set. Packet filters SHOULD be able to match on the Default GBP ID value as a way to match packets that do not have the GBP option set. The default Default GBP ID is 0, but MAY be configured to be a value other than 0. The allocation of Group Policy ID values is outside the scope of this document.

4. Use Of Multiple GBP shim headers

A tunnel header MAY carry multiple GBP shim headers where each GBP shim header carries a unique GBP type. There MUST be only one shim header of a specific GBP type per tunneled packet.

5. IANA Considerations

5.1. Geneve Option Class Value

IANA is requested to allocate a Geneve "option class" number for GBP:

+---------------+-------------+---------------+
| Option Class  | Description | Reference     |
+---------------+-------------+---------------+
| TBD           | GBP_ID      | This document |
+---------------+-------------+---------------+

5.2. GBP Type Values

IANA is requested to set up a registry of "GBP Type". These are 8-bit values. GBP Type values in the table below are defined in this
draft. New values in the range of 0x02 through 0x7F are assigned via Standards Action [RFC5226].

+----------------+--------------------+---------------+
<table>
<thead>
<tr>
<th>GBP Type Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>GBP_Source_ID</td>
<td>This document</td>
</tr>
<tr>
<td>0x01</td>
<td>GBP_Destination_ID</td>
<td>This document</td>
</tr>
<tr>
<td>0x02 - 0x7F</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>0x80 - 0xFF</td>
<td>Local assignment</td>
<td></td>
</tr>
</tbody>
</table>

6. 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 shim 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.

7. Normative References

[I-D.ietf-nvo3-geneve]

[I-D.smith-vxlan-group-policy]


Authors’ Addresses

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

Email: john.lemon@broadcom.com

Michael Smith
Cisco Systems

Email: michsmit@cisco.com

Aldrin Isaac
Juniper Networks
1133 Innovation Way
Sunnyvale, CA  94089
USA

Email: aldrin.isaac@gmail.com