

IDR Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 9, 2017

S. Hares
Q. Liang
J. You
Huawei
July 8, 2016

BGP Flow Specification Filter Component for Time Constraints
draft-liang-idr-flowspec-v1-time-00.txt

Abstract

BGP flow specification version 1 (RFC5575) describes the distribution of traffic filter policy (traffic filters and actions) which are distributed via BGP to BGP peers to support the following 3 applications: (1) mitigation of Denial of Service (DoS), (2) traffic filtering in BGP/MPLS VPNs, and (3) centralized traffic control for networks with SDN or NFV controllers. A BGP Flow Filter that combines packet filter with time may provide an ability to for these three applications to have a flow filter operate for only a specific time.

This document proposes a new BGP Flow specification filter based on time.

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 January 9, 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 the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

| | |
|---------------------------------------|---|
| 1. Introduction | 2 |
| 2. RFC 2119 language | 3 |
| 3. Encoding of BGP-FS time | 3 |
| 4. IANA Considerations | 4 |
| 5. Security Considerations | 4 |
| 6. References | 5 |
| 6.1. Normative References | 5 |
| 6.2. Informative References | 5 |
| Authors' Addresses | 6 |

1. Introduction

BGP flow specification [RFC5575] describes the distribution of filters and actions that apply when packets are received on a router with the flow specification function turned on. If one considers the reception of the packet as an event, then BGP [RFC4271] flow specification describes a set of minimalistic Event-MatchCondition-Action (ECA) policies where the match-condition is defined in the BGP NLRI, and the action is defined either by the default condition (accept traffic) or actions defined in Extended BGP Communities values [RFC4360].

The initial set of policy [RFC5575] for this policy includes 12 types of match filters encoded in two application specific AFI/SAFIs for the IPv4 AFI and the following SAFIs:

```
IP traffic: AFI:1, SAFI, 133;
```

```
BGP/MPLS VPN AFI:1 VPN SAFI, 134) for IPv4.
```

The 12 filters specified in [RFC5575] are "ANDED" and measured in a specific order. The packet does not match unless all filters match.

The popularity of these flow specification filters in deployment for the following applications has led to the requirement for more BGP

flow specification match filters in the NLRI and more BGP flow specification actions to support these applications

- o mitigation of Denial of Service (DoS),
- o support of traffic filtering in BGP/MPLS VPNs,
- o centralized traffic control for networks with SDN or NFV controllers.

See [I-D.hares-idr-rfc5575bis] for additional details on these additional filters for BGP Flow Specification 1.

Since DDoS attacks are dynamic, redirection or filtering of a flow may be necessary only for some specified, and may be undesirable at other times. Thus network administrators may want to add a time filter to group of filters to be matched. For example, a network administrator may need to insert DoS filters for only a specific period while a DoS attack or a Distributed DoS (DDoS) attack is occurring. Another example, is the filter of traffic in the BGP/MPLS VPN to support prioritization of high priority services such as video traffic and limiting of bandwidth of low priority services (such as web browsing).

2. RFC 2119 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 [RFC2119].

3. Encoding of BGP-FS time

The encoding for BGP Flow Specification time

Type: Time Filter (TBD) Flow Specification Component type

Function: Match filter based on time.

Encoding: <type(1 octet), length(1 octet), <value>

value field: has the form shown in figure 3.

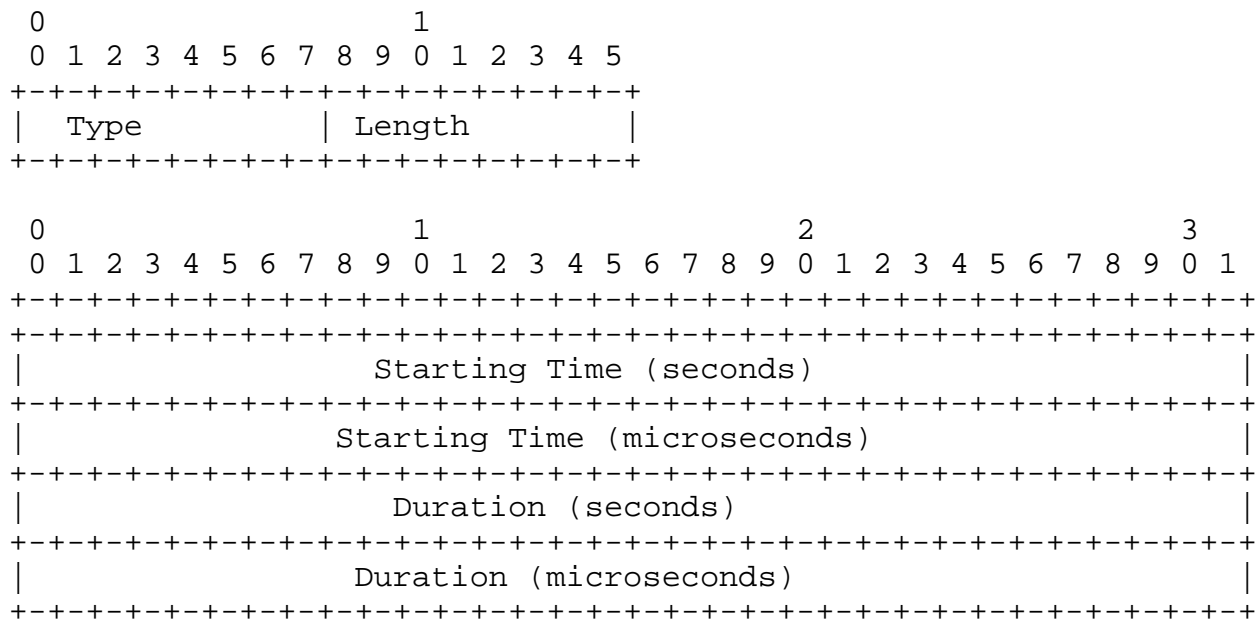


Figure 1:Time filersub-TLV Format

Starting Time: Expressed in seconds and microseconds since midnight (zero hour), January 1, 1970 (UTC). Precision of the "Starting Time" is implementation-dependent. If the "Starting Time Type" is set to 0, this field is invalid. An Invalid FlowSpecification filter is logged, and the NLRI ignored.

Duration: Expressed in seconds and microseconds. If this field is zero this filter is invalid. An Invalid FlowSpecification filter is logged, and the NLRI ignored.

4. IANA Considerations

This document requests IANA BGP allocations in line with [RFC7153].

This document requests IANA allocates an entry in the Flow Specification Component Types Registry with the following values:

| Name | Value | Document |
|-------------|-------|----------------|
| Time Filter | TBD | This document. |

5. Security Considerations

The time filter augments the other BGP Flow Filters with an indication of the time these filters are active. It is anticipated that these filters are deployed within secure BGP infrastructures and

not in home environments. In home environments, the time of filters may provide insight to the activities of individuals. Anyone installing BGP Flow Filters in home environments should secure any flow filters by encrypting the data that flows over IP links.

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, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <<http://www.rfc-editor.org/info/rfc4271>>.
- [RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <<http://www.rfc-editor.org/info/rfc4360>>.
- [RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <<http://www.rfc-editor.org/info/rfc4760>>.
- [RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <<http://www.rfc-editor.org/info/rfc5575>>.
- [RFC7153] Rosen, E. and Y. Rekhter, "IANA Registries for BGP Extended Communities", RFC 7153, DOI 10.17487/RFC7153, March 2014, <<http://www.rfc-editor.org/info/rfc7153>>.
- [RFC7674] Haas, J., Ed., "Clarification of the Flowspec Redirect Extended Community", RFC 7674, DOI 10.17487/RFC7674, October 2015, <<http://www.rfc-editor.org/info/rfc7674>>.

6.2. Informative References

- [I-D.hares-idr-rfc5575bis] Hares, S., McPherson, D., and J. Mauch, "Dissemination of Flow Specification Rules", draft-hares-idr-rfc5575bis-00 (work in progress), July 2016.

Authors' Addresses

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com

Qiandeng Liang
Huawei
101 Software Avenue, Yuhuatai District
Nanjing 210012
China

Email: liangqiandeng@huawei.com

Jianjie You
Huawei
101 Software Avenue, Yuhuatai District
Nanjing 210012
China

Email: youjianjie@huawei.com