Dissemination of Flow Specification Rules for NVO3
draft-hao-idr-flowspec-nvo3-02.txt

Abstract

This draft proposes a new subset of component types to support the NVO3 flow-spec application.

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), 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 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
BGP Flow-spec is an extension to BGP that allows for the dissemination of traffic flow specification rules. It leverages the BGP Control Plane to simplify the distribution of ACLs, new filter rules can be injected to all BGP peers simultaneously without changing router configuration. The typical application of BGP Flow-spec is to automate the distribution of traffic filter lists to routers for DDOS mitigation.

RFC5575 defines a new BGP Network Layer Reachability Information (NLRI) format used to distribute traffic flow specification rules. NLRI (AFI=1, SAFI=133) is for IPv4 unicast filtering. NLRI (AFI=1, SAFI=134) is for BGP/MPLS VPN filtering. [IPv6-FlowSpec] defines flow-spec extension for IPv6 data packets. [Layer2-FlowSpec] extends the flow-spec rules for layer 2 Ethernet packets.

In cloud computing era, multi-tenancy has become a core requirement for data centers. Since NVO3 can satisfy multi-tenancy key requirements, this technology is being deployed in an increasing number of cloud data center network. NVO3 focuses on the construction of overlay networks that operate over an IP (L3) underlay transport network. It can provide layer 2 bridging and layer 3 IP service for each tenant. VXLAN and NVGRE are two typical NVO3 encapsulations.

[EVPN-Overlays] provides a scalable and efficient multi-tenant solution within the Data Center where VXLAN, NVGRE or MPLS over GRE
can be used as possible data plane encapsulation options. It uses EVPN as the control plane. [Inter-Overlays] provides a interconnect solution for EVPN overlay networks.

Both in data center inside or DCI networks, we also have requirements to deploy BGP Flow-spec for DDoS attack traffic mitigation. The Flow specification rules in NVO3 network can be based on inner layer 2 Ethernet header, inner layer 3 IP header, outer layer 2 Ethernet header, outer layer 3 IP header, and/or NVO3 header information. Currently the Flow specification rule [RFC5575] only includes single layer IP information like source/destination prefix, protocol, ports, and etc, the match part lacks layer indicator and NVO3 header information, so it can’t be used for the traffic filtering based on NVO3 header or a specified layer header directly.

This draft proposes a new subset of component types to support the NVO3 flow-spec application.

2. The Flow Specification encoding for NVO3

In default, the current flow-spec rules can only impose on the outer layer header of NVO3 encapsulation data packets. To make traffic filtering based on NVO3 header and inner header of NVO3 packets, a new component type acts as a delimiter is introduced. The delimiter type is used to specify the boundary of the inner or outer layer component types for NVO3 data packets. All the component types defined in [RFC5575], [IPv6-FlowSpec], [Layer2-FlowSpec], and etc can be used between two delimiters.

The NVO3 outer layer address normally belongs to public network, the "Flow Specification" NLRI only for the outer layer header doesn’t need to include Route Distinguisher field (8 bytes).

VNID is the identification for each tenant network, the "Flow Specification" NLRI for NVO3 header part should always include VNID field, Route Distinguisher field doesn’t need to be included.

The inner layer address normally belongs to a VPN, the NLRI format for the inner header should consist of a fixed-length Route Distinguisher field (8 bytes) corresponding to the VPN, the RD is followed by the flow specification for the inner layer. The NLRI length field shall include both the 8 bytes of the Route Distinguisher as well as the subsequent flow specification.

Flow specification rules received via this NLRI apply only to traffic that belongs to the VPN instance(s) in which it is imported.
This document proposes the following extended specifications for NVO3 flow:

Type TBD1 - Delimiter type

Encoding: \(<type (1\ octet),\ length (1\ octet),\ Value>\).

When the delimiter type is present, it indicates the component types for the inner or outer layer of NVO3 packets will be followed immediately. At the same time, it indicates the end of the component types belonging to the former delimiter.

The value field defines encapsulation type and is encoded as:

```
  0 1 2 3 4 5 6 7
+---+---+---+---+---+---+---+---+
|          Encap Type           |
+---+---+---+---+---+---+---+---+
| I | O |        Resv           |
+---+---+---+---+---+---+---+---+
```

This document defines the following Encap types:

- VXLAN: Tunnel Type = 0
- NVGRE: Tunnel Type = 1

I: If I is set to one, it indicates the component types for the inner layer of NVO3 packets will be followed immediately.

O: If O is set to one, it indicates the component types for the outer layer of NVO3 packets will be followed immediately.

For NVO3 header part, the following additional component types are introduced.

Type TBD2 - VNID

Encoding: \(<type (1\ octet),\ [op,\ value]>\).

Defines a list of \(\{\text{operation, value}\}\) pairs used to match 24-bit VN ID which is used as tenant identification in NVO3 network. For NVGRE encapsulation, the VNID is equivalent to VSID. Values are encoded as 1- to 3-byte quantities.
Type TBD3 - Flow ID

Encoding: <type (1 octet), [op, value]+>

Defines a list of (operation, value) pairs used to match 8-bit Flow id fields which are only useful for NVGRE encapsulation. Values are encoded as 1-byte quantity.

Other types:

The additional types for GENEVE [GENEVE], GUE [GUE] and GPE [GPE] header specific part will be added later.

3. The Flow Specification Traffic Actions for NVO3

The current traffic filtering actions can still be used for NVO3 encapsulation traffic. For Traffic Marking, only the DSCP in outer header can be modified.

4. Security Considerations

No new security issues are introduced to the BGP protocol by this specification.

5. IANA Considerations

IANA is requested to create and maintain a new registry entitled:

"Flow spec NVO3 Component Types":

Type TBD1 - Delimiter type

Type TBD2 - VNID

Type TBD3 - Flow ID

5.1. Normative References

5.2. Informative References


6. Acknowledgments

The authors wish to acknowledge the important contributions of Susan Hares, Qiandeng Liang, Nan Wu, Yizhou Li, Lucy Yong.
Authors’ Addresses

Weiguo Hao
Huawei Technologies
101 Software Avenue,
Nanjing 210012
China
Email: haoweiguo@huawei.com

Shunwan Zhuang
Huawei Technologies
Huawei Bld., No.156 Beiying Rd.
Beijing 100095
China
Email: zhuangshunwan@huawei.com

Zhenbin Li
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China
Email: lizhenbin@huawei.com