BGP Flowspec Redirect to VPN RD Extended Community
draft-yong-idr-flowspec-redirect-vpn-rd-00

Abstract

This document defines a new type of the redirect extended community, called as Redirect to VPN RD Extended Community. When activated, the Redirect to VPN RD Extended Community is used to identify the unique VPN instance within a router.

Requirements 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 RFC 2119 [RFC2119].

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 September 18, 2016.

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
1. Introduction

"Dissemination of Flow Specification Rules" [RFC5575], commonly known as BGP Flowspec, provided for a BGP Extended Community [RFC4360] that served to redirect traffic that matched the flow specification’s Network Layer Reachability Information (NLRI) to a Virtual Routing and Forwarding (VRF) instance that lists the specified route-target in its import policy. In that RFC, the Redirect Extended Community was documented as follows:
The redirect extended community allows the traffic to be redirected to a VRF routing instance that lists the specified route-target in its import policy. If several local instances match this criteria, the choice between them is a local matter (for example, the instance with the lowest Route Distinguisher value can be elected). This extended community uses the same encoding as the Route Target extended community [RFC4360].

11. IANA Considerations

The following traffic filtering flow specification rules have been allocated by IANA from the "BGP Extended Communities Type - Experimental Use" registry as follows:

0x8008 - Flow spec redirect

[RFC7674] updates RFC 5575 ("Dissemination of Flow Specification Rules") to clarify the formatting of the BGP Flowspec Redirect Extended Community. This document defines the following redirect extended communities:

<table>
<thead>
<tr>
<th>type</th>
<th>extended community</th>
<th>encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x8008</td>
<td>redirect AS-2byte</td>
<td>2-octet AS, 4-octet Value</td>
</tr>
<tr>
<td>0x8108</td>
<td>redirect IPv4</td>
<td>4-octet IPv4 Address, 2-octet Value</td>
</tr>
<tr>
<td>0x8208</td>
<td>redirect AS-4byte</td>
<td>4-octet AS, 2-octet Value</td>
</tr>
</tbody>
</table>

2. Operation Concerns in Redirect VRF Action

Following example is a case used in a backbone network.

Traffic Analyzer is installed at the edge of the backbone to detect the attack.
Scrubbing Center is installed at the edge of the backbone to tackle the attack.

VRF scrubbing-vpn is configured on R1 and R2. A default route in R1’s scrubbing-vpn VRF is configured to reach the Scrubbing Center, and MP-BGP is configured to advertise the default route from VRF scrubbing-vpn to the remote router R2.

Upon detecting the attack target to the user of the backbone network, Traffic Analyzer will push a Flowspec rule to R1 with Redirect RT: 100:1.

R1 will advertise the receiving Flowspec rule to R2.

If the VRF scrubbing-vpn on R2 is the only VRF routing instance, then the receiving Flowspec rule from R1 can be imported by the VRF routing instance scrubbing-vpn. The attack traffic that matches the Flowspec rule on R2 will be redirected to the VRF scrubbing-vpn and sent to the Scrubbing Center.
However in this case, there are several local instances on R2 can match the Redirect RT: 100:1(as shown in following table). To make it work, according to RFC 5575, an operator has to configure R2 so that ‘Redirect to VPN’ will point to the scrubbing-vpn, which introduces operation complex and/or prone to an error. To avoid this configuration, a unique RT value for BGP FS ‘Redirect to VPN’ action has to be selected, which can be an operation complex in a large network.

+---------------+--------------------+----------------+
| VRF           | IRT                | RD             |
+---------------+--------------------+----------------+
| vpn1          | 10:1 100:1         | 10:1           |
| scrubbing-vpn | 100:1              | 100:1          |
| vpn2          | 10:1 100:1         | 200:1          |
+---------------+--------------------+----------------+

The reason for the above issue is that the IRT isn’t unique on one router, for example, IRT 100:1 can be assigned to multiple VRF instances: vpn1, scrubbing-vpn and vpn2.

The Route Distinguisher is unique on one router, In order to address this operational concern, this document introduces a new type of the redirect extended community, called as Redirect to VPN RD Extended Community, When activated, the Redirect to VPN RD Extended Community is used to identify the unique VPN instance within a router.

3. Redirect to VPN RD Extended Community Format

This document defines a new type of the redirect extended community, called as Redirect to VPN RD Extended Community. This extended community is a new transitive extended community with the Sub-Type field is TBD. The IANA registry of BGP Extended Communities clearly identifies communities of specific formats: "Two-octet AS Specific Extended Community" [RFC4360], "Four-octet AS Specific Extended Community" [RFC5668], and "IPv4 Address Specific Extended Community" [RFC4360]. Route Targets [RFC4360] identify this format in the high-order (Type) octet of the Extended Community, Redirect to VPN RD Extended Community uses the same mechanism.

This document defines the following VPN RD Extended Communities:
It should be noted that the low-order nibble of the Redirect’s Type field corresponds to the Route Target Extended Community format field (Type). (See Sections 3.1, 3.2, and 4 of [RFC4360] plus Section 2 of [RFC5668].) The low-order octet (Sub-Type) of the Redirect to VPN RD Extended Community is TBD, in contrast to 0x02 for Route Targets and 0x08 for Redirect to VPN RT Extended Community.

4. Using Redirect VPN RD Extended Community

Upon detecting the attack target to the user of the backbone network, Traffic Analyzer will push a Flowspec rule to R1 with Redirect VPN RD: 100:1.

R1 will advertise the receiving Flowspec rule to R2.

In R2, the receiving Flowspec rule from R1 can be imported by the VRF routing instance scrubbing-vpn. The attack traffic that matches the Flowspec rule on R2 will be correctly redirected to the VRF scrubbing-vpn and sent to the Scrubbing Center.
5. IANA Considerations

TBD.

6. Security Considerations

TBD.

7. References

7.1. Normative References


7.2. Informative References


Authors’ Addresses

lucy.yong
Huawei Technologies

Email: lucy.yong@huawei.com