Inter-Domain Routing
Internet-Draft
Intended status: Standards Track
Expires: May 21, 2020

S. Litkowski
Individual
A. Simpson
Nokia
K. Patel
Arrcus, Inc
J. Haas
Juniper Networks
L. Yong
Huawei

November 18, 2019

Applying BGP flowspec rules on a specific interface set
draft-ietf-idr-flowspec-interfaceset-05

Abstract

The BGP Flow Specification (flowspec) Network Layer Reachability Information (BGP NLRI) extension (draft-ietf-idr-rfc5575bis) is used to distribute traffic flow specifications into BGP. The primary application of this extension is the distribution of traffic filtering policies for the mitigation of distributed denial of service (DDoS) attacks.

By default, flow specification filters are applied on all forwarding interfaces that are enabled for use by the BGP flowspec extension. A network operator may wish to apply a given filter selectively to a subset of interfaces based on an internal classification scheme. Examples of this include "all customer interfaces", "all peer interfaces", "all transit interfaces", etc.

This document defines BGP Extended Communities (RFC4360) that allow such filters to be selectively applied to sets of forwarding interfaces sharing a common group identifier. The BGP Extended Communities carrying this group identifier are referred to as the BGP Flowspec "interface-set" Extended Communities.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Status of This Memo

Copyright Notice

Table of Contents

1. Use case

While a network may provide connectivity to a homogenous class of users, it often provides connectivity to different groups of users. The nature of these different groups, and how they're classified, varies based on the purpose of the network. In an enterprise network, connectivity may exist between data centers, offices, and external connectivity. In a virtual private networking (VPN) network, it may consist of customers in different sites connected through a VPN, the provider core network, and external networks such as the Internet. In a traditional Internet service provider (ISP) network, the network may consist of points of presence (POPs), internal infrastructure networks, customer networks, peer networks, and transit networks.

The BGP flowspec extension permits traffic filters to be distributed to routers throughout a network. However, these filters often should not be uniformly applied to all network interfaces. As an example, a rate-limiting filter applied to the SMTP protocol may be applied to customer networks, but not other networks. Similarly, a DDoS attack on the SSH protocol may be deemed appropriate to drop at upstream peering routers but not customer routers.

By default, BGP flowspec filters are applied at all interfaces that permit flowspec filters to be installed. What is needed is a way to selectively apply those filters to subsets of interfaces in a network.

2. Interface specific filtering using BGP flowspec

The uses case detailed above require application of different BGP flowspec rules on different sets of interfaces.

We propose to introduce, within BGP flowspec, a traffic filtering scope that identifies a group of interfaces where a particular filter should be applied. Identification of interfaces within BGP flowspec will be done through group identifiers. A group identifier marks a set of interfaces sharing a common administrative property. Like a BGP community, the group identifier itself does not have any significance. It is up to the network administrator to associate a particular meaning to a group identifier value (e.g. group ID#1 associated to Internet customer interfaces). The group identifier is a local interface property. Any interface may be associated with one or more group identifiers using manual configuration.

When a filtering rule advertised through BGP flowspec must be applied only to particular sets of interfaces, the BGP flowspec BGP UPDATE will contain the identifiers associated with the relevant sets of interfaces. In addition to the group identifiers, it will also contain the direction the filtering rule must be applied in (see Section 3).

Configuration of group identifiers associated to interfaces may change over time. An implementation MUST ensure that the filtering rules (learned from BGP flowspec) applied to a particular interface are always updated when the group identifier mapping is changing.

As an example, we can imagine the following design :

- Internet customer interfaces are associated with group-identifier 1.
- VPN customer interfaces are associated with group-identifier 2.
- All customer interfaces are associated with group-identifier 3.
- Peer interfaces are associated with group-identifier 4.
- Transit interfaces are associated with group-identifier 5.
- All external provider interfaces are associated with group-identifier 6.
- All interfaces are associated with group-identifier 7.

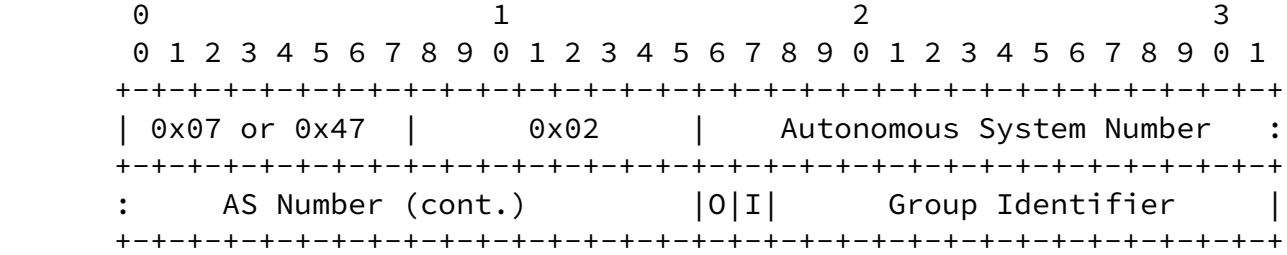
If the service provider wants to deploy a specific inbound filtering on external provider interfaces only, the provider can send the BGP flow specification using group-identifier 6 for the inbound direction.

There are some cases where nodes are dedicated to specific functions (Internet peering, Internet Edge, VPN Edge, Service Edge ...), in this kind of scenario, there is an interest for a constrained distribution of filtering rules that are using the interface specific filtering. Without the constrained route distribution, all nodes will received all the filters even if they are not interested in those filters. Constrained route distribution of flowspec filters would allow for a more optimized distribution.

3. Interface-set extended community

This document proposes a new BGP Route Target extended community called the "flowspec interface-set". This document expands the definition of the Route Target extended community to allow a new value of high order octet (Type field) to be 0x07 for the transitive flowspec interface-set extended community, or 0x47 for the non-transitive flowspec interface-set extended community. These are in addition to the values specified in [RFC4360].

This new BGP Route Target extended community is encoded as follows :



The flags are :

- O : if set, the flow specification rule MUST be applied in outbound direction to the interface set referenced by the following group-identifier.

- I : if set, the flow specification rule MUST be applied in inbound direction to the interface set referenced by the following group-identifier.

Both flags can be set at the same time in the interface-set extended community leading to flow rule to be applied in both directions. An interface-set extended community with both flags set to zero MUST be treated as an error and as consequence, the flowspec update MUST be discarded. As having no direction indicated as no sense, there is no need to propagate the filter informations in the network.

The Group Identifier is encoded as a 14-bit number, values 0..16383.

Multiple instances of the interface-set extended community may be present in a BGP update. This may occur if the flowspec rule needs to be applied to multiple sets of interfaces.

Multiple instances of the extended community in a BGP update MUST be interpreted as a "OR" operation. For example, if a BGP UPDATE

contains two interface-set extended communities with group ID 1 and group ID 2, the filter would need to be installed on interfaces belonging to Group ID 1 or Group ID 2.

Similar to using a Route Target extended community, route distribution of flowspec NLRI with interface-set extended communities may be subject to constrained distribution as defined in [RFC4684].

4. Scaling of per-interface rules

In the absence of an interface-set extended community, a flowspec filter is applied to all flowspec enabled interfaces. When interface-set extended communities are present, different interfaces may have different filtering rules, with different terms and actions. These differing rules may make it harder to share forwarding

instructions within the forwarding plane.

Flowspec implementations supporting the interface-set extended community SHOULD take care to minimize the scaling impact in such circumstances. How this is accomplished is out of the scope of this document.

5. Deployment Considerations

5.1. Add-Paths

There are some cases where a particular BGP flowspec NLRI may be advertised to different interface groups with a different action. For example, a service provider may want to discard all ICMP traffic from customer interfaces to infrastructure addresses and want to rate-limit the same traffic when it comes from some internal platforms. These particular cases require ADD-PATH ([RFC7911]) to be deployed in order to ensure that all paths (NLRI+interface-set group-id+actions) are propagated within the BGP control plane. Without ADD-PATH, only a single "NLRI+interface-set group-id+actions" will be propagated, so some filtering rules will never be applied.

5.2. Inter-domain Considerations

The Group Identifier used by the interface-set extended community has local significance to its provisioning Autonomous System. While [I-D.ietf-idr-rfc5575bis] permits inter-as advertisement of flowspec NLRI, care must be taken to not accept these communities when they would result in unacceptable filtering policies.

Filtering of interface-set extended communities at Autonomous System border routers (ASBRs) may thus be desirable.

Note that the default behavior without the interface-set feature would to have been to install the flowspec filter on all flowspec enabled interfaces.

6. Security Considerations

This document extends the Security Considerations of [I-D.ietf-idr-rfc5575bis] by permitting flowspec filters to be

selectively applied to subsets of network interfaces in a particular direction. Care must be taken to not permit the inadvertant manipulation of the interface-set extended community to bypass expected traffic manipulation.

7. Acknowledgements

Authors would like to thanks Wim Hendrickx and Robert Raszuk for their valuable comments.

8. IANA Considerations

8.1. FlowSpec Transitive Extended Communities

This document requests a new type from the "BGP Transitive Extended Community Types" extended community registry from the First Come First Served range. This type name shall be 'FlowSpec Transitive Extended Communities'. IANA has assigned the value 0x07 to this type.

This document requests creation of a new registry called "FlowSpec Transitive Extended Community Sub-Types". This registry contains values of the second octet (the "Sub-Type" field) of an extended community when the value of the first octet (the "Type" field) is the value allocated in this document. The registration procedure for values in this registry shall be First Come First Served.

8.2. FlowSpec Non-Transitive Extended Communities

This document requests a new type from the "BGP Non-Transitive Extended Community Types" extended community registry from the First Come First Served range. This type name shall be 'FlowSpec Non-Transitive Extended Communities'. IANA has assigned the value 0x47 to this type.

This document requests creation of a new registry called "FlowSpec Non-Transitive Extended Community Sub-Types". This registry contains values of the second octet (the "Sub-Type" field) of an extended community when the value of the first octet (the "Type" field) is the

value allocated in this document. The registration procedure for

values in this registry shall be First Come First Served.

8.3. FlowSpec interface-set Extended Community

Within the two new registries above, this document requests a new subtype (suggested value 0x02). This sub-type shall be named "interface-set", with a reference to this document.

8.4. Allocation Advice to IANA

IANA is requested to allocate the values of the FlowSpec Transitive and Non-Transitive Extended Communities such that their values are identical when ignoring the second high-order bit (Transitive). See section 2, [RFC4360].

It is suggested to IANA that, when possible, allocations from the FlowSpec Transitive/Non-Transitive Extended Community Sub-Types registries are made for transitive or non-transitive versions of features (section 2, [RFC4360]) that their code point in both registries is identical.

9. Normative References

[I-D.ietf-idr-rfc5575bis]
Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", draft-ietf-idr-rfc5575bis-17 (work in progress), June 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <https://www.rfc-editor.org/info/rfc4360>.

[RFC4684] Marques, P., Bonica, R., Fang, L., Martini, L., Raszuk, R., Patel, K., and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)", RFC 4684, DOI 10.17487/RFC4684, November 2006, <https://www.rfc-editor.org/info/rfc4684>.

[RFC7911] Walton, D., Retana, A., Chen, E., and J. Scudder, "Advertisement of Multiple Paths in BGP", RFC 7911, DOI 10.17487/RFC7911, July 2016, <https://www.rfc-editor.org/info/rfc7911>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

Stephane Litkowski
Individual

Email: slitkows.ietf@gmail.com

Adam Simpson
Nokia

Email: adam.1.simpson@nokia.com

Keyur Patel
Arrcus, Inc

Email: keyur@arrcus.com

Jeffrey Haas
Juniper Networks

Email: jhaas@juniper.net

Lucy Yong
Huawei

Email: lucy.yong@huawei.com