

Routing Area Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: June 25, 2015

S. Litkowski  
Orange  
A. Simpson  
Alcatel Lucent  
K. Patel  
Cisco  
J. Haas  
Juniper Networks  
December 22, 2014

**Applying BGP flowspec rules on a specific interface set**  
**draft-litkowski-idr-flowspec-interfaceset-01**

Abstract

BGP Flow-spec is an extension to BGP that allows for the dissemination of traffic flow specification rules. The primary application of this extension is DDoS mitigation where the flowspec rules are applied in most cases to all peering routers of the network.

This document will present another use case of BGP Flow-spec where flow specifications are used to maintain some access control lists at network boundary. BGP Flowspec is a very efficient distributing machinery that can help in saving OPEX while deploying/updating ACLs. This new application requires flow specification rules to be applied only on a specific subset of interfaces and in a specific direction.

The current specification of BGP Flow-spec does not detail where the flow specification rules need to be applied.

This document presents a new interface-set flowspec action that will be used in complement of other actions (marking, rate-limiting ...). The purpose of this extension is to inform remote routers on where to apply the flow specification.

This extension can also be used in a DDoS mitigation context where a provider wants to apply the filtering only on specific peers.

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 [[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 June 25, 2015.

## Copyright Notice

Copyright (c) 2014 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

<a href="#">1.</a>	Use case . . . . .	<a href="#">3</a>
<a href="#">1.1.</a>	Specific filtering for DDoS . . . . .	<a href="#">3</a>
<a href="#">1.2.</a>	ACL maintenance . . . . .	<a href="#">4</a>
<a href="#">2.</a>	Collaborative filtering and managing filter direction . . . . .	<a href="#">5</a>
<a href="#">3.</a>	Interface specific filtering using BGP flowspec . . . . .	<a href="#">6</a>
<a href="#">4.</a>	Interface-set extended community . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Interaction with interface ACLs . . . . .	<a href="#">7</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">9</a>
<a href="#">7.</a>	Acknowledgements . . . . .	<a href="#">9</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">9</a>
<a href="#">9.</a>	Normative References . . . . .	<a href="#">10</a>
	Authors' Addresses . . . . .	<a href="#">10</a>



## 1. Use case

### 1.1. Specific filtering for DDoS

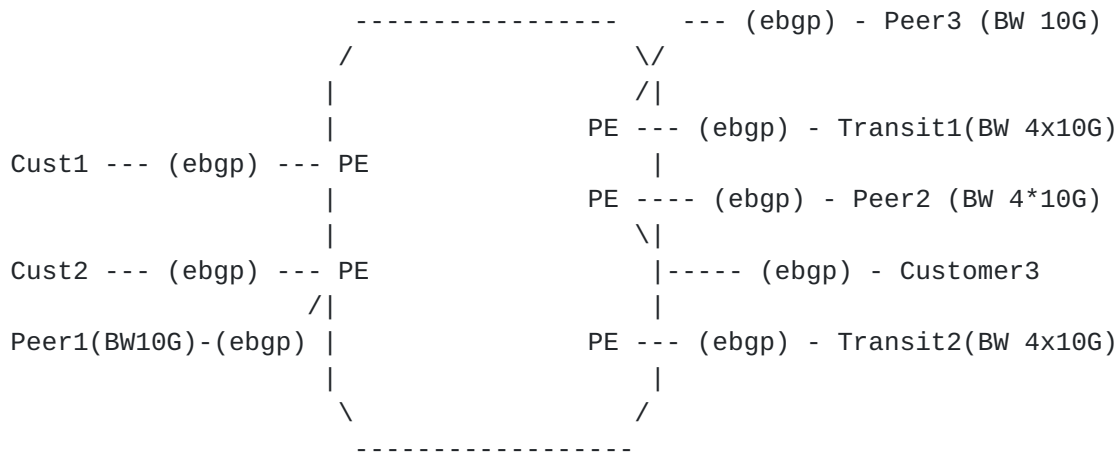


Figure 1

The figure 1 above displays a typical service provider Internet network owing Customers, Peers and Transit. To protect proactively against some attacks (e.g. DNS, NTP ...), the service provider may want to deploy some rate-limiting of some flows on peers and transit links. But depending on link bandwidth, the provider may want to apply different rate-limiting values.

For 4\*10G links peer/transit, it may want to apply a rate-limiting of DNS flows of 1G, while on 10G links, the rate-limiting would be set to 250Mbps. Customer interfaces must not be rate-limited.

BGP Flow-spec infrastructure may already be present on the network, and all PEs may have a BGP session running flowspec address family. The Flowspec infrastructure may be reused by the service provider to implement such rate-limiting in a very quick manner and being able to adjust values in future quickly without having to configure each node one by one. Using the current BGP flowspec specification, it would not be possible to implement different rate limiter on different interfaces of a same router. The flowspec rule is applied to all interfaces in all directions or on some interfaces where flowspec is activated but flowspec rule set would be the same among all interfaces.

Section [Section 3](#) will detail a solution to address this use case using BGP Flowspec.



## 1.2. ACL maintenance

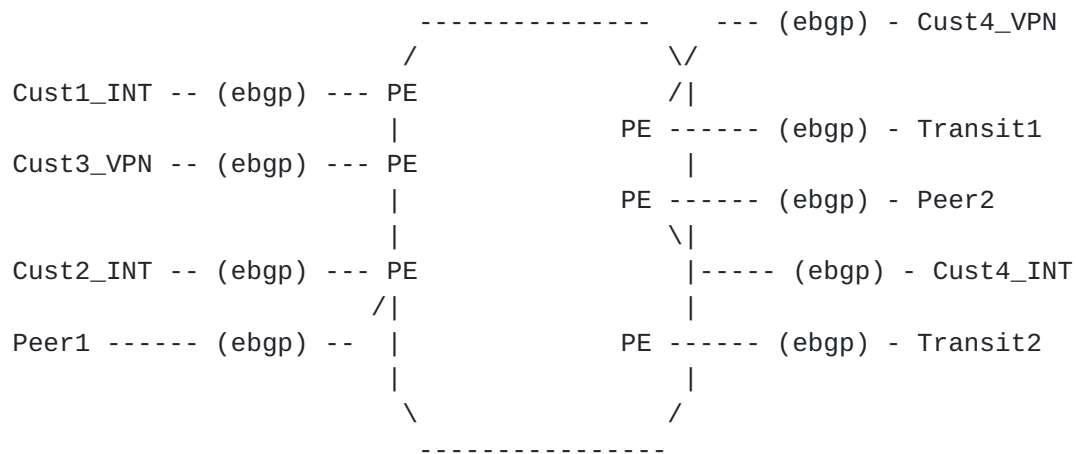


Figure 2

The figure 1 above displays a typical service provider multiservice network owing Customers, Peers and Transit for Internet, as well as VPN services. The service provider requires to ensure security of its infrastructure by applying ACLs at network boundary. Maintaining and deploying ACLs on hundreds/thousands of routers is really painful and time consuming and a service provider would be interested to deploy/updates ACLs using BGP Flowspec. In this scenario, depending on the interface type (Internet customer, VPN customer, Peer, Transit ...) the content of the ACL may be different.

We can imagine two cases :

- o Maintaining complete ACLs using flowspec : in this case all the ingress ACL are maintained and deployed using BGPFlowspec. See section [Section 6](#) for more details on security aspects.
- o Requirement of a quick deployment of a new filtering term due to a security alert : new security alerts often requires a fast deployment of new ACL terms. Using traditional CLI and hop by hop provisioning, such deployment takes time and network is unprotected during this time window. Using BGP flowspec to deploy such rule, a service provider can protect its network in few seconds. Then the SP can decide to keep the rule permanently in BGP Flowspec or update its ACL or remove the entry (in case equipments are not vulnerable anymore).

Section [Section 3](#) will detail a solution to address this use case using BGP Flowspec.



## 2. Collaborative filtering and managing filter direction

[RFC5575] states in [Section 5](#). : "This mechanism is primarily designed to allow an upstream autonomous system to perform inbound filtering in their ingress routers of traffic that a given downstream AS wishes to drop."

In case of networks collaborating in filtering, there is a use case for performing outbound filtering. Outbound filtering permits to apply traffic action one step before and so may permit to prevent impact like congestions.

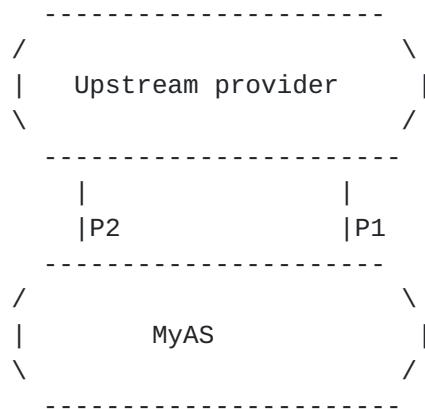


Figure 3

In the figure above, MyAS is connected to an upstream provider. If a malicious traffic comes in from the upstream provider, it may congestion P1 or P2 links. If MyAS apply inbound filtering on P1/P2 using BGP Flowspec, the congestion issue will not be solved.

Using collaborative filtering, the upstream provider may propose to MyAS to filter malicious traffic destined to MyAS. We propose to enhance [\[RFC5575\]](#) to make myAS able to send BGP FlowSpec updates (on eBGP sessions) to the upstream provider to request outbound filtering on peering interfaces towards MyAS. When the upstream provider will receive the BGP Flowspec update from MyAS, the BGP flowspec update will contain request for outbound filtering on a specific set of interfaces. The upstream provider will apply automatically the requested filter and congestion will be prevented.





### **3. Interface specific filtering using BGP flowspec**

The use case detailed above requires application of different BGP Flowspec rules on different set of interfaces. The basic specification detailed in [\[RFC5575\]](#) does not address this and does not give any detail on where the FlowSpec filter need to be applied.

We propose to introduce an identification of interfaces within BGP Flowspec. All interfaces may be associated to one or more group-identifiers and a BGP Flowspec rule may also be associated with one or more group-identifiers including a filtering direction (input/output/both) , so the FlowSpec rule will be applied only on interfaces belonging the the group identifier included in the BGP FlowSpec update.

Considering figure 2, we can imagine the following design :

- o Internet customer interfaces are associated with group-identifier 1.
- o VPN customer interfaces are associated with group-identifier 2.
- o All customer interfaces are associated with group-identifier 3.
- o Peer interfaces are associated with group-identifier 4.
- o Transit interfaces are associated with group-identifier 5.
- o All external provider interfaces are associated with group-identifier 6.
- o 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 and including inbound direction.

### **4. Interface-set extended community**

This document proposes a new BGP extended community called "flow spec interface-set". This new BGP extended community is part of TRANSITIVE FOUR-OCTET AS-SPECIFIC EXTENDED COMMUNITY and has subtype TBD.

The Global Administrator field of this community MUST be set to the ASN of the originating router. The Local Administrator field is encoded as follows :



```

    0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| 0 | I |   Group Identifier   :
+---+---+---+---+---+---+---+---+
: Group Identifier (cont.)    |
+---+---+---+---+---+---+---+---+

```

The flags are :

- o 0 : if set, the flow specification rule MUST be applied in outbound direction to the interface set referenced by the following group-identifier.
- o I : if set, the flow specification rule MUST be applied in input 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.

The Group Identifier is coded as a 14-bit number (values goes from 0 to 16383).

Multiple instances of the interface-set community may be present in a BGP update. This may appear if the flow rule need to be applied to multiple set of interfaces.

Multiple instances of the community in a BGP update MUST be interpreted as a "OR" operation : if a BGP update contains two interface-set 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.

## 5. Interaction with interface ACLs

Deploying interface specific filters using BGP FlowSpec (dynamic entries) may interfere with existing permanent interface ACL (static entries). The content of the existing permanent ACL MUST NOT be altered by dynamic entries coming from BGP FlowSpec. Permanent ACLs are using a specific ordering which is not compatible with the ordering of FS rules and misordering of ACL may lead to undesirable behavior. In order, to keep a deterministic and well known behaviour, an implementation SHOULD process the BGP FlowSpec ACL as follows :



- o In inbound direction, the permanent ACL action is applied first followed by FlowSpec action. This gives the primary action to the permanent ACL as it is done today.
- o In outbound direction, FlowSpec action action is applied first followed by permanent ACL. This gives the final action to the permanent ACL as it is done today.

Inbound filters	Outbound filters
-----	-----
Permanent  ->  Dynamic  ->  Forwarding	Dynamic  ->  Permanent

In order for a flow to be accepted, the flow must be accepted by the two ACLs and a flow is rejected when one of the ACL rejects it as described in the table below :

Permanent ACL entry action	FlowSpec ACL entry action	Result action
Drop	Drop	Drop
Drop	Accept	Drop
Accept	Drop	Drop
Accept	Accept	Accept

Example :

- o ACL permanent IN :

- \* Entry 1 : permit udp from 10/8 to 11/8 port 53
- \* Entry 2 : permit tcp from 10/8 to 11/8 port 22
- \* Entry 3 : deny ip from 10/8 to 11/8

- o ACL dynamic FlowSpec IN :

- \* Entry 1 : deny udp from 10.0.0.1/32 to 11/8 port 53
- \* Entry 2 : permit tcp from 10/8 to 11/8 port 80

In the example above :

- o a UDP flow from 10.0.0.1 to 11.0.0.2 on port 53 will be rejected because the dynamic ACL rejects it.



- o a UDP flow from 10.0.0.2 to 11.0.0.2 on port 53 will be accepted because both ACLs accept it.
- o a TCP flow from 10.0.0.2 to 11.0.0.2 on port 80 will be rejected because permanent ACL rejects it.

## **6. Security Considerations**

Managing permanent Access Control List by using BGP Flowspec as described in [Section 1.2](#) helps in saving roll out time of such ACL. However some ACL especially at network boundary are critical for the network security and loosing the ACL configuration may lead to network open for attackers.

By design, BGP flowspec rules are ephemeral : the flow rule exists in the router while the BGP session is UP and the BGP path for the rule is valid. We can imagine a scenario where a Service Provider is managing the network boundary ACLs by using only FlowSpec. In this scenario, if , for example, an attacker succeed to make the internal BGP session of a router to be down , it can open all boundary ACLs on the node, as flowspec rules will disappear due to the BGP session down.

In reality, the chance for such attack to occur is low, as boundary ACLs should protect the BGP session from being attacked.

In order to complement the BGP flowspec solution is such deployment scenario and provides security against such attack, a service provider may activate Long lived Graceful Restart [[I-D.uttaro-idr-bgp-persistence](#)] on the BGP session owning Flowspec address family. So in case of BGP session to be down, the BGP paths of Flowspec rules would be retained and the flowspec action will be retained.

## **7. Acknowledgements**

Authors would like to thanks Wim Hendrickx for his valuable comments.

## **8. IANA Considerations**

This document requests a new sub-type from the "TRANSITIVE FOUR-OCTET AS-SPECIFIC EXTENDED COMMUNITY SUB-TYPES" extended community registry. The sub-type name shall be 'Flow spec interface-set'.





## **9. Normative References**

- [I-D.uttaro-idr-bgp-persistence]  
Uttaro, J., Chen, E., Decraene, B., and J. Scudder,  
"Support for Long-lived BGP Graceful Restart", [draft-uttaro-idr-bgp-persistence-03](#) (work in progress), November 2013.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", [RFC 5575](#), August 2009.

### Authors' Addresses

Stephane Litkowski  
Orange

Email: [stephane.litkowski@orange.com](mailto:stephane.litkowski@orange.com)

Adam Simpson  
Alcatel Lucent

Email: [adam.simpson@alcatel-lucent.com](mailto:adam.simpson@alcatel-lucent.com)

Keyur Patel  
Cisco

Email: [keyupate@cisco.com](mailto:keyupate@cisco.com)

Jeff Haas  
Juniper Networks

Email: [jhaas@juniper.net](mailto:jhaas@juniper.net)

