

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: February 13, 2017

T. King  
C. Dietzel  
DE-CIX Management GmbH  
J. Snijders  
NTT  
G. Doering  
SpaceNet AG  
G. Hankins  
Nokia  
August 12, 2016

BLACKHOLE BGP Community for Blackholing  
draft-ietf-grow-blackholing-03

Abstract

This document describes the use of a well-known Border Gateway Protocol (BGP) community for destination-based blackholing in IP networks. This well-known advisory transitive BGP community named BLACKHOLE allows an origin AS to specify that a neighboring network should discard any traffic destined towards the tagged IP prefix.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [[RFC2119](#)] only when they appear in all upper case. They may also appear in lower or mixed case as English words, without normative meaning.

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 February 13, 2017.

---

Internet-Draft    BLACKHOLE BGP Community for Blackholing    August 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 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>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	BLACKHOLE Community . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Operational Recommendations . . . . .	<a href="#">3</a>
3.1.	IP Prefix Announcements with BLACKHOLE Community Attached	3
<a href="#">3.2.</a>	Local Scope of Blackholes . . . . .	<a href="#">4</a>
<a href="#">3.3.</a>	Accepting Blackholed IP Prefixes . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Vendor Implementation Recommendations . . . . .	<a href="#">5</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">5</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">5</a>
<a href="#">7.</a>	References . . . . .	<a href="#">6</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">6</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">6</a>
<a href="#">Appendix A.</a>	Acknowledgements . . . . .	<a href="#">7</a>
	Authors' Addresses . . . . .	<a href="#">7</a>

## [1.](#) Introduction

Network infrastructures have been increasingly hampered by DDoS attacks. In order to dampen the effects of these DDoS attacks, IP networks have offered blackholing with BGP [[RFC4271](#)] using various mechanisms such as those described in [[RFC3882](#)] and [[RFC5635](#)].

DDoS attacks targeting a certain IP address may cause congestion of links used to connect to adjacent networks. In order to limit the impact of such a scenario on legitimate traffic, networks adopted a mechanism called BGP blackholing. A network that wants to trigger

blackholing needs to understand the triggering mechanism adopted by its neighboring networks. Different networks provide different mechanisms to trigger blackholing, including but not limited to pre-defined blackhole next-hop IP addresses, specific BGP communities or via an out-of-band BGP session with a special BGP speaker.

Internet-Draft    BLACKHOLE BGP Community for Blackholing    August 2016

Having several different mechanisms to trigger blackholing in different networks makes it an unnecessarily complex, error-prone and cumbersome task for network operators. Therefore, a well-known BGP community [[RFC1997](#)] is defined for operational ease.

Having such a well-known BGP community for blackholing also further simplifies network operations because:

- o Implementing and monitoring blackholing becomes easier when implementation, and operational guides do not cover many variations to trigger blackholing.
- o The number of support requests from customers about how to trigger blackholing in a particular neighboring network will be reduced as the codepoint for common blackholing mechanisms is unified and well-known.

## [2.](#) BLACKHOLE Community

This document defines the use of a new well-known BGP transitive community, BLACKHOLE.

The semantics of this community allow a network to interpret the presence of this community as an advisory qualification to drop any traffic being sent towards this prefix.

## [3.](#) Operational Recommendations

### [3.1.](#) IP Prefix Announcements with BLACKHOLE Community Attached

Accepting and honoring the BLACKHOLE community, or ignoring it, is a choice that is made by each operator. This community MAY be used in all bilateral and multilateral BGP deployment scenarios. In a bilateral peering relationship, use of the BLACKHOLE community MUST be agreed upon by the two networks before advertising it. In a multilateral peering relationship, the decision to honor or ignore the BLACKHOLE community is to be made according to the operator's

routing policy. The community SHOULD be ignored, if it is received by a network that it not using it.

When a network is under DDoS duress, it MAY announce an IP prefix covering the victim's IP address(es) for the purpose of signaling to neighboring networks that any traffic destined for these IP address(es) should be discarded. In such a scenario, the network operator SHOULD attach the BLACKHOLE BGP community.

The BLACKHOLE community MAY also be used as one of the trigger communities in a [[RFC5635](#)] destination-based RTBH configuration.

### [3.2.](#) Local Scope of Blackholes

A BGP speaker receiving an announcement tagged with the BLACKHOLE community SHOULD add the NO\_ADVERTISE or NO\_EXPORT community as defined in [[RFC1997](#)], or a similar community to prevent propagation of the prefix outside the local AS. The community to prevent propagation SHOULD be chosen according to the operator's routing policy.

Unintentional leaking of more specific IP prefixes to neighboring networks can have adverse effects. Extreme caution should be used when purposefully propagating IP prefixes tagged with the BLACKHOLE BGP community outside the local routing domain, unless policy explicitly aims at doing just that.

### [3.3.](#) Accepting Blackholed IP Prefixes

It has been observed in provider networks running BGP that announcements of IP prefixes longer than /24 for IPv4 and /48 for IPv6 are usually not accepted on the Internet (see [section 6.1.3 \[RFC7454\]](#)). However, blackhole prefix length should be as long as possible in order to limit the impact of discarding traffic for adjacent IP space that is not under DDoS duress. The blackhole prefix length is typically as specific as possible, a /32 for IPv4 or a /128 for IPv6.

BGP speakers in a bilateral peering relationship using the BLACKHOLE community MUST only accept and honor BGP announcements carrying the BLACKHOLE community under the two following conditions:

- o the announced prefix is covered by an equal or shorter prefix that the neighboring network is authorized to advertise.
- o the receiving party agreed to honor the BLACKHOLE community on the particular BGP session

In topologies with a route server or other multilateral peering relationships, BGP speakers SHOULD accept and honor BGP announcements under the same conditions.

An operator MUST ensure that origin validation techniques (such as [\[RFC6811\]](#)) do not inadvertently block legitimate announcements carrying the BLACKHOLE community.

The BLACKHOLE community is not intended to be used with [\[RFC5575\]](#) NLRI to distribute traffic flow specifications.

The error handling for this community follows the process in [\[RFC7606\]](#) that causes a malformed community to be treated as a withdrawn.

Operators are encouraged to store all BGP updates in their network carrying the BLACKHOLE community for long term analysis or internal audit purposes.

#### 4. Vendor Implementation Recommendations

Without an explicit configuration directive set by the operator, network elements SHOULD NOT discard traffic destined towards IP prefixes which are tagged with the BLACKHOLE BGP community. The operator is expected to explicitly configure the network element to honor the BLACKHOLE BGP community in a way that is compliant with the operator's routing policy.

Vendors MAY provide a shorthand keyword in their configuration language to reference the well-known BLACKHOLE BGP community attribute value. The suggested string to be used is "blackhole".

#### 5. IANA Considerations

The IANA is requested to register BLACKHOLE as a well-known BGP community with global significance:

BLACKHOLE (= 0xFFFF029A)

The low-order two octets in decimal are 666, a value commonly associated with BGP blackholing among network operators.

## 6. Security Considerations

BGP contains no specific mechanism to prevent the unauthorized modification of information by the forwarding agent. This allows routing information to be modified, removed, or false information to be added by forwarding agents. Recipients of routing information are not able to detect this modification. BGPsec [[I-D.ietf-sidr-bgpsec-protocol](#)] does not resolve this situation. Even when BGPsec is in place, a forwarding agent can alter, add or remove BGP communities.

The unauthorized addition of the BLACKHOLE BGP community to an IP prefix by an adversary may cause a denial of service attack based on denial of reachability.

In order to further limit the impact of unauthorized BGP announcements carrying the BLACKHOLE BGP community, the receiving BGP

speaker SHOULD verify by applying strict filtering (see [section 6.2.1.1.2 \[RFC7454\]](#)) that the peer announcing the prefix is authorized to do so. If not, the BGP announcement should be filtered.

BGP announcements carrying the BLACKHOLE community should only be accepted and honored, if the neighboring network is authorized to advertise the prefix. The method of validating announcements is to be chosen according to the operator's routing policy.

It is RECOMMENDED that operators use best common practices to protect their BGP sessions, such as the ones in [[RFC7454](#)].

## 7. References

## 7.1. Normative References

- [RFC1997] Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", [RFC 1997](#), DOI 10.17487/RFC1997, August 1996, <<http://www.rfc-editor.org/info/rfc1997>>.
- [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>>.
- [RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "Revised Error Handling for BGP UPDATE Messages", [RFC 7606](#), DOI 10.17487/RFC7606, August 2015, <<http://www.rfc-editor.org/info/rfc7606>>.

## 7.2. Informative References

- [I-D.ietf-sidr-bgpsec-protocol] Lepinski, M. and K. Sriram, "BGPsec Protocol Specification", [draft-ietf-sidr-bgpsec-protocol-17](#) (work in progress), June 2016.
- [RFC3882] Turk, D., "Configuring BGP to Block Denial-of-Service Attacks", [RFC 3882](#), DOI 10.17487/RFC3882, September 2004, <<http://www.rfc-editor.org/info/rfc3882>>.

- [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>>.
- [RFC5635] Kumari, W. and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", [RFC 5635](#), DOI 10.17487/RFC5635, August 2009,

<<http://www.rfc-editor.org/info/rfc5635>>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", [RFC 6811](#), DOI 10.17487/RFC6811, January 2013, <<http://www.rfc-editor.org/info/rfc6811>>.

[RFC7454] Durand, J., Pepelnjak, I., and G. Doering, "BGP Operations and Security", [BCP 194](#), [RFC 7454](#), DOI 10.17487/RFC7454, February 2015, <<http://www.rfc-editor.org/info/rfc7454>>.

## [Appendix A](#). Acknowledgements

The authors would like to gratefully acknowledge many people who have contributed discussions and ideas to the making of this proposal. They include Petr Jiran, Yordan Kritski, Christian Seitz, Nick Hilliard, Joel Jaeggli, Christopher Morrow, Thomas Mangin, Will Hargrave, Niels Bakker, David Farmer, Jared Mauch, John Heasley and Terry Manderson.

### Authors' Addresses

Thomas King  
DE-CIX Management GmbH  
Lichtstrasse 43i  
Cologne 50825  
Germany

Email: [thomas.king@de-cix.net](mailto:thomas.king@de-cix.net)

Christoph Dietzel  
DE-CIX Management GmbH  
Lichtstrasse 43i  
Cologne 50825  
Germany

Email: [christoph.dietzel@de-cix.net](mailto:christoph.dietzel@de-cix.net)



NTT Communications  
Theodorus Majofskistraat 100  
Amsterdam 1065 SZ  
NL

Email: [job@ntt.net](mailto:job@ntt.net)

Gert Doering  
SpaceNet AG  
Joseph-Dollinger-Bogen 14  
Munich 80807  
Germany

Email: [gert@space.net](mailto:gert@space.net)

Greg Hankins  
Nokia  
777 E. Middlefield Road  
Mountain View, CA 94043  
USA

Email: [greg.hankins@nokia.com](mailto:greg.hankins@nokia.com)