Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: January 13, 2022

P. Bergeon, Ed.
Nokia

July 12, 2021

Flowspec TTL (Time to Live) Match
draft-bergeon-flowspec-ttl-match-00

Abstract

This document defines a new component type to match TTL (Time to Live) values using BGP Flow Specification rules.

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 https://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 January 13, 2022.

Copyright Notice

Table of Contents

1. Introduction

One general purpose of BGP Flowspec [RFC8955] is to distribute firewall rules, also known as filtering or Access Control Lists (ACLs) rules, in receiving routers for mitigation of denial-of-service (DoS) attacks using flows specifications encoded as BGP NLRI [RFC4271].

BGP Flowspec [RFC8955] defines 12 component types that can be used as match criteria in filtering rules with destination prefix, source prefix, IP protocol, port, destination port, source port, ICMP type, ICMP code, TCP flags, packet length, DSCP and fragment.

The IP header field Time to Live (TTL) is a notable absent of the component types defined in BGP Flowspec [RFC8955].

This document proposes to address this by adding support for a new Flowspec component type to add support for TTL match.

2. Definitions of Terms Used in This Memo

NLRI - Network Layer Reachability Information.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Motivation

As defined in [RFC0791], the TTL is an indication of an upper bound on the lifetime of an internet datagram. It is set by the sender of

the datagram and reduced by each router along the route where it is processed.

This unique property of the IP header TTL field can make it particularly useful for security and distributed-denial-of-service (DDoS) mitigation.

Studies such as the one presented at NANOG 82 Tracing DDoS End-to-End [1] highlight how filtering traffic based on TTL values can be used as an effective mitigation for DDoS attacks at the IP edge of the network. In particular, the TTL value can be used to differentiate legitimate traffic from DDoS attack traffic generated by DDoS for hire services.

Different IP edge routers of a given network under attack may see the same attack traffic using slightly different TTL values, however these routers can use a common set of filtering rules propagated via BGP flowspec to mitigatie the attack using range(s) of TTL values.

4. Specification

This document defines a new Flowspec component type, value TBD, named "TTL (Time to Live)".

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

Defines a list of {numeric_op, value} pairs used to match the 8-bit TTL field value.

This component type uses the Numeric Operator (numeric_op) as defined already in [RFC8955] section 4.2.1.1.

Type TBD component values SHOULD be encoded as single octet (numeric_op len=00).

5. Ordering of Flow Specifications Considerations

The ordering of Flow Specifications rules defined in [RFC8955] remains unchanged and applies to the component type introduced in this document.

6. Security Considerations

The new component type introduced in this document does not introduce new security considerations other than the ones already defined in [RFC8955].

7. IANA Considerations

IANA is requested to assign a type from the First Come First Served range of the "Flow Spec Component Types" registry:

Type Value	Name	Reference
TBD	TTL (Time to Live)	this document

Reference: this document

Registry Owner/Change Controller: IESG

Registration procedures:

Range	Registration Procedures
0-127	IETF Review
128-249	First Come First Served
250-254	Experimental
255	Reserved

Note: a separate "owner" column is not provided because the owner of all registrations, once made, is "IESG".

8. References

8.1. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[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>.

[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, <https://www.rfc-editor.org/info/rfc4271>.

[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>.

[RFC8955] Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", RFC 8955, DOI 10.17487/RFC8955, December 2020, <https://www.rfc-editor.org/info/rfc8955>.

8.2. URIs

[1] https://www.nanog.org/news-stories/nanog-tv/nanog-82-webcast/tracing-ddos-end-to-end-in-2021/

Author's Address

Philippe Bergeon (editor)
Nokia

Email: philippe.bergeon@nokia.com