Independent Submission
Request for Comments: 8367
Category: Informational
ISSN: 2070-1721

T. Mizrahi
Marvell
J. Yallouz
Intel

1 April 2018

Wrongful Termination of Internet Protocol (IP) Packets

Abstract

Routers and middleboxes terminate packets for various reasons. In some cases, these packets are wrongfully terminated. This memo describes some of the most common scenarios of wrongful termination of Internet Protocol (IP) packets and presents recommendations for mitigating them.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8367.

Table of Contents

1. Introduction 2
2. Abbreviations 2
3. Wrongful Termination Scenarios 3
3.1. Color-Based Termination 3
3.2. Age-Based Termination 3
3.3. Origin-Based Termination 4
3.4. Length-Based Termination 4
3.5. IP-Version-Based Termination 5
3.6. Flag-Based Termination 5
4. Security Considerations 5
5. IANA Considerations 5
6. Conclusion 6
7. References 6
7.1. Normative References 6
7.2. Informative References 6
Authors' Addresses 6

1. Introduction

IP packets are often terminated by network devices. In some cases, control-plane packets are terminated and processed by the local device, while in other cases packets are terminated (discarded) due to a packet filtering mechanism. Packet filtering is widely employed in network devices for sanity checking, policy enforcement, and security. IP routers and middleboxes, such as firewalls, often terminate packets that do not comply with a predefined policy. Unfortunately, some filtering policies cause false positive or unnecessary packet termination. Moreover, these wrongful terminations are sometimes biased and discriminate against packets based on their color, age, origin, length, or IP version.

This memo discusses some of the most common scenarios of wrongful termination of IP packets and presents recommendations for preventing such discrimination.

2. Abbreviations

IP Internet Protocol

TTL Time To Live

OAM Operations, Administration, and Maintenance

3. Wrongful Termination Scenarios

3.1. Color-Based Termination

Synopsis

IP packets are terminated due to their color.

Description

Routers often employ metering mechanisms [RFC4115]. These mechanisms often support a color-aware mode, in which the packet's color (green, yellow, or red) is used as a criterion in the metering algorithm. This mode has been known to prefer green packets over red and yellow packets.

Recommendation

Use of color-blind metering is recommended, as it allows equal opportunity for packets of different colors.

3.2. Age-Based Termination

Synopsis

IP packets are terminated based on their TTL.

Description

The IPv4 TTL field [RFC791] and the IPv6 Hop Limit field [RFC8200] are used for loop prevention. These fields essentially represent the packet's age. A router that receives an IP packet with a TTL value of 0 or 1 typically terminates the packet. In this document, packets with a TTL or Hop Limit of 0 or 1 are referred to as 'senior packets'.

Recommendation

When possible, the practice of reverse discrimination is recommended. Notably, senior packets have been known to be highly effective for OAM tasks, such as Hello [RFC2328] and Traceroute [RFC2151]. Therefore, senior packets should not be easily dismissed; to the extent possible, senior packets should be used in control-plane protocols.

3.3. Origin-Based Termination

Synopsis

IP packets are terminated based on their origin (source IP address prefix).

Description

Routers and middleboxes often perform IP address filtering. Packets are often discarded based on the prefix of their source IP address. In this memo, prefix-based source address filtering is referred to as origin-based filtering. While source IP address filtering is an acceptable technique for preventing security attacks performed by known attackers, filtering an entire prefix may lead to unnecessary termination of legitimate traffic.

Recommendation

Origin-based filtering should be limited, to the extent possible, so as not to punish an entire autonomous system for the crime of a single host. Individual address-based filtering should be preferred in cases where the address of the potential threat is well known.

3.4. Length-Based Termination

Synopsis

Short IP packets are wrongfully terminated due to their length.

Description

The minimum permissible size of an IPv4 [RFC791] packet is 20 octets, and the minimum size of an IPv6 [RFC8200] packet is 40 octets. However, due to the size limits of Ethernet, it is often the case that IP packets that are shorter than 46 octets are discarded. This is because the minimal Ethernet frame size is 64 octets, the minimal Ethernet header size is 14 octets, and the Ethernet Frame Check Sequence is 4 octets long (i.e., 64 - 14 - 4 = 46). In the context of this memo, legitimate IP packets that are less than 46 octets long are referred to as 'short IP packets'.

Recommendation

Short IP packets should not be discarded. The Ethernet frame length should be enforced at the Ethernet layer, while the IP layer should avoid discrimination of short IP packets.

3.5. IP-Version-Based Termination

Synopsis

IPv6 packets are terminated due to their version.

Description

Many routers and middleboxes are configured to process only IPv4 [RFC791] packets and to reject IPv6 [RFC8200] packets.

Recommendation

It is quite unsettling that there are still networks in which IPv6 packets are deemed unwanted in the second decade of the 21st century. Indeed, IPv6 packets have a slightly shorter payload than IPv4 packets. However, they are essential to the future growth of the Internet. It is time for operators to finally give IPv6 its well-deserved opportunity.

3.6. Flag-Based Termination

Synopsis

IPv4 packets are terminated because their More Fragments (MF) flag is set.

Description

Many routers and middleboxes are configured to discard fragmented packets.

Recommendation

A packet should not be discarded on the grounds of a flag it supports. All flags should be respected, as well as the features they represent.

4. Security Considerations

This memo proposes to practice liberality with respect to IP packet filtering in routers and middleboxes. Arguably, such a liberal approach may compromise security in some cases. Not only must security be done; it must also be seen to be done.

5. IANA Considerations

This document has no IANA actions.

6. Conclusion

This memo recommends that every router and middlebox be an Equal Opportunity Device, which does not discriminate on the basis of actual or perceived rate, color, age, origin, length, IP version, fragmentation characteristics, higher-layer protocols, or any other IP characteristic.

7. References

7.1. Normative References

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

7.2. Informative References

[RFC2151] Kessler, G. and S. Shepard, "A Primer On Internet and TCP/IP Tools and Utilities", FYI 30, RFC 2151, DOI 10.17487/RFC2151, June 1997, <https://www.rfc-editor.org/info/rfc2151>.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <https://www.rfc-editor.org/info/rfc2328>.

[RFC4115] Aboul-Magd, O. and S. Rabie, "A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic", RFC 4115, DOI 10.17487/RFC4115, July 2005, <https://www.rfc-editor.org/info/rfc4115>.

Authors' Addresses

Tal Mizrahi
Marvell
Email: talmi@marvell.com

Jose Yallouz
Intel
Email: jose@alumni.technion.ac.il