Workgroup: Network Working Group

Internet-Draft:

draft-lin-opsec-trustroute-problem-

statement-01

Published: 14 December 2021 Intended Status: Informational

Expires: 17 June 2022

Authors: T. Lin H. Li X. Shi

H3C H3C Tsinghua University

X. Yin W. Chen

Tsinghua University Capital Normal University

Problem Statement and Use Cases of Trustworthiness-based Routing

### Abstract

Currently, network operators are trying to provide fine-granularity Service Level Agreement (SLA) guarantee to achieve better Quality of Experience (QoE) for end users and engage customers, such as ultralow latency and high reliability service. However, with increasing security threats, differentiated QoE services are insufficient, the demands for more differentiated security service are emerging.

This document explores the requirements for differentiated security services and identifies the scenarios for network operators. To provide differentiated security services, possible trustworthiness-based routing solution is discussed.

### 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 17 June 2022.

## Copyright Notice

Copyright (c) 2021 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

(<a href="https://trustee.ietf.org/license-info">https://trustee.ietf.org/license-info</a>) 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

### Table of Contents

- 1. Introduction
- Terminology
- 3. Problem Statement
  - 3.1. Use Case 1: Customers Require Security Service
  - 3.2. Use Case 2: Providers Require Secure defense
- 4. Solution Discussions
- 5. Security Considerations
- 6. IANA Considerations
- 7. Contributors
- 8. References
  - 8.1. Normative References
  - 8.2. Informative References

Authors' Addresses

## 1. Introduction

For the traditional best effort service provided by IP networks, routing is optimized for a single arbitrary metric, e.g. IGP cost in OSPF and IS-IS. To support differentiated services, additional routing metrics are used, such as bandwidth, jitter and delay. However, security metrics and methods of corresponding treatment are seldom taken into considerations.

Customers may request the network to transfer their traffic flows with different security guarantees. Or the provider may classify traffic flows into different classes by security-related features. These traffic flows of different security service classes are expected to be transmitted by different sets of nodes, because the trustworthiness of different nodes is possibly not the same. The traffic flows which have higher security requests are expected to be transmitted by the nodes with higher trustworthiness. Trustworthiness is used as a security metric to evaluate the qualification of network elements for differentiated security services.

This document describes the requirements and use cases of trustworthiness-based routing.

# 2. Terminology

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.

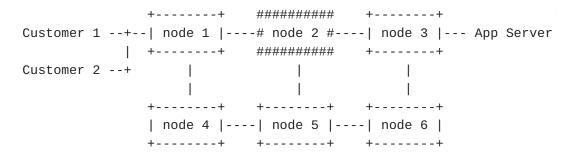
Trustworthiness: The attribute of a network element used to evaluate its qualification for security services.

### 3. Problem Statement

With more and more security incidents occur repeatedly, security continues to be an increasingly important common concern for network users and network operators. Good connectivity is insufficient, higher and higher requirements for network security are emerging. From different perspectives of operators and end users, there will be different needs. On the one hand, end users require network operators to ensure network security, on the other hand, network operators need to prevent the intrusion and attack from malicious users. Two following use cases are described:

## 3.1. Use Case 1: Customers Require Security Service

From the perspective of end users, different users may have different security level requirements. Some users are sensitive to security and would like the network path given by the operator to have higher security. The network path is composed by many network forwarding devices, and the trustworthiness of each device affects the trustworthiness of the whole path. These network forwarding devices come from different vendors, have different security capabilities, and may have different security status at a certain time. Therefore, operators need to evaluate the trustworthiness of network forwarding devices, and choose different security level paths for users with different security requirements.



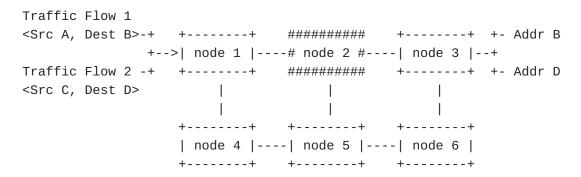
In the above network, node 1, node 3, node 4, node 5 and node 6 have advanced anti-hacker modules, but node 2 does not have such module. Two customers at node 1 both need to visit the application server at node 3. Customer 1 requests normal service. Customer 2 needs to

transmit confidential information and requests the network to provide secure service.

For the packets from Customer 1, the shortest path <node 1, node 2, node 3> is used. For the packets from Customer 2, the path only contains the nodes with advanced anti-hacker modules, which can reduce the risk of manipulation or disclosure. Therefore, node 2 is excluded and the best path is <node 1, node 4, node 5, node 6, node 3>.

# 3.2. Use Case 2: Providers Require Secure defense

For network operators, different users have different levels of trustworthiness. Most users are normal and harmless, but there are also a small number of users suspected of threatening network security. Therefore, for users with threats, operators may consider choosing paths with different security levels.



In the above network, node 1, node 3, node 4, node 5 and node 6 have tracing modules which can record attacking packets, but node 2 does not have such module. Two traffic flows enter the network at node 1 and need to be transmitted to node 3. A and B are authenticated addresses, but C or D is not. The traffic flow which comes from an authenticated address and goes to another authenticated address is classified by the provider as a credible flow. Therefore, Traffic Flow 1 is classified as credible, and Traffic Flow 2 is classified as incredible. For Traffic Flow 1, the shortest path <node 1, node 2, node 3> is used. For Traffic Flow 2, the packets are transmitted by the nodes with tracing modules. If there are attacking packets in Traffic Flow 2, these packets will be recorded and may be analyzed to trace the attacker. Therefore, node 2 is excluded and the best path is <node 1, node 4, node 5, node 6, node 3>.

### 4. Solution Discussions

To provide differentiated security services, specific traffic flows should be identified by the network. For example, the IPv4 TOS field, the IPv6 Traffic Class field, or the 5-tuple in the IP and

transport protocol header of a packet can be used to determine its security service class.

For the traditional best effort service, routing is optimized for a single arbitrary metric, e.g. IGP cost in OSPF and IS-IS. To support differentiated services, additional routing metrics are used, such as bandwidth, jitter and delay.

Trustworthiness is an attribute of a network element which is used as a security metric to evaluate its qualification for differentiated security services. Trustworthiness attributes may be taken into consideration of device capability, administration authority, security protocol, etc.

When computing paths for differentiated security services, trustworthiness attributes are added into the constraints. Then particular traffic flows are steered into these paths. There are several existing technologies that can steer traffic over a path that is computed using different constraints instead of the shortest IGP path. They may be extended to implement trustworthiness-based routing. For example, Segment Routing Policy, as defined in [1-<u>D.ietf-idr-segment-routing-te-policy</u>], enables the instantiation of an ordered list of segments on a node for implementing a source routing policy with a specific intent for traffic steering from that node. For another example, Flexible Algorithm, as defined in [1-D.ietf-lsr-flex-algo], provides a mechanism for IGP to compute constraint-based paths under a combination of calculation-type, metric-type, and constraints. Other technologies, such as multitopology routing, may also be candidates. Because of the flexibility of these technologies, they can adapt to different perspectives and needs from end users and network operators.

## 5. Security Considerations

TBD.

### 6. IANA Considerations

No IANA action is required so far.

## 7. Contributors

In addition to the authors listed on the front page, the following co-authors have also contributed to this document:

Mengxiao Chen H3C

Email: chen.mengxiao@h3c.com

Xiangqing Chang H3C

Email: chang.xiangqing@h3c.com

### 8. References

### 8.1. Normative References

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

### 8.2. Informative References

### [I-D.ietf-idr-segment-routing-te-policy]

Previdi, S., Filsfils, C., Talaulikar, K., Mattes, P., Jain, D., and S. Lin, "Advertising Segment Routing Policies in BGP", Work in Progress, Internet-Draft, draft-ietf-idr-segment-routing-te-policy-14, 10 November 2021, <a href="https://www.ietf.org/internet-drafts/draft-ietf-idr-segment-routing-te-policy-14.txt">https://www.ietf.org/internet-drafts/draft-ietf-idr-segment-routing-te-policy-14.txt</a>.

# **Authors' Addresses**

Tao Lin H3C

Email: lintao@h3c.com

Hao Li H3C Email: <a href="mailto:lihao@h3c.com">lihao@h3c.com</a>

Xingang Shi

Tsinghua University

Email: <a href="mailto:shixg@cernet.edu.cn">shixg@cernet.edu.cn</a>

Xia Yin

Tsinghua University

Email: <a href="mailto:yxia@tsinghua.edu.cn">yxia@tsinghua.edu.cn</a>

Wenlong Chen

Capital Normal University

Email: <a href="mailto:chenwenlong@cnu.edu.cn">chenwenlong@cnu.edu.cn</a>