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 ultra-low 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

Copyright Notice

Table of Contents

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.

```
                +---------+    ##########    +---------+
Customer 1 --+--| node 1 |----# node 2 #----| node 3 |--- App Server
             |  +---------+    ##########    +---------+
Customer 2 --+       |              |              |
                     |              |              |
                +---------+    +---------+    +---------+
                | node 4 |----| node 5 |----| node 6 |
                +---------+    +---------+    +---------+
```

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.

```
Traffic Flow 1
<Src A, Dest B>-+   +--------+    ##########    +--------+  +- Addr B
                +-->| node 1 |----# node 2 #----| node 3 |--+
Traffic Flow 2 -+   +--------+    ##########    +--------+  +- Addr D
<Src C, Dest D>          |             |             |
                         |             |             |
                    +--------+    +--------+    +--------+
                    | node 4 |----| node 5 |----| node 6 |
                    +--------+    +--------+    +--------+
```

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 [I-D.ietf-idr-segment-routing-te-policy], 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 [I-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 multi-topology 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

[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>.

[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>.

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, <https://www.ietf.org/internet-drafts/draft-ietf-idr-segment-routing-te-policy-14.txt>.

[I-D.ietf-lsr-flex-algo] Psenak, P., Hegde, S., Filsfils, C., Talaulikar, K., and A. Gulko, "IGP Flexible Algorithm", Work in Progress, Internet-Draft, draft-ietf-lsr-flex-algo-18, 25 October 2021, <http://www.ietf.org/internet-drafts/draft-ietf-lsr-flex-algo-18.txt>.

Authors' Addresses

Tao Lin
H3C

Email: lintao@h3c.com

Hao Li
H3C

Email: lihao@h3c.com

Xingang Shi
Tsinghua University

Email: shixg@cernet.edu.cn

Xia Yin
Tsinghua University

Email: yxia@tsinghua.edu.cn

Wenlong Chen
Capital Normal University

Email: chenwenlong@cnu.edu.cn