Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-chen-secure-routing-use-cases-02
Published: 13 March 2023
Intended Status: Informational
Expires: 14 September 2023

Authors:	Chen	L. Su	B. Yang
	China Mobile	China Mobile	China Mobile

The Use Cases for Secure Routing

Abstract

Current routing mechanism is based on the shortest path, which only take the link status and the path accessibility into consideration, without the security of links and forwarding nodes. As security has become an important factor to the user. This paper proposes to add security factor in the routing process.

With the frequent occurrence of security incidents, services security is an essential demand for the users. As there are many security devices in the ISP's network, this draft proposes secure routing mechanism. The purpose of secure routing is to converge security and routing to ensure the secure data transmission.

The scope is transmission process security, while end-to-end security and application layer security are out of scope.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

With the frequent occurrence of network security accidents, users' demand for network security is greatly increased; there is no doubt that security of services is required. The current security risk mainly comes from attacks, users need security services to ensure the continuity of business.

Some users build security centers by themselves, some buy third-party cloud security services, and some hope that ISPs can provide security services by secure routing. Secure routing provided by ISPs can be implemented which can forward traffic to security functions. With the development of programmable network (such as SDN) and SRv6 technology, the forwarding requirements of the application layer can be completed through routing programming; accessibility and security in the routing process can be processed synchronously to provide users with secure routing.

Network functions are also updating and integrated security functions to cope with complex security environments, such as routers with anti-DDoS attack functions.

2. Analysis of security requirements

From ISPs' perspective, the nodes' trustworthiness is different, it is necessary to provide routing policy from the security protection for the important users.

For users, different users have different security requirements which depend on their services. For example, e-commerce and Internet companies focus on phishing prevention, anti-DDoS attacks and data security; Medical companies focus on data security and security isolation, and so on.

3. Security and routing convergence

If security functions and network functions are highly integrated, security can be as available as network connection. Optimize existing routing protocols to obtain information about security functions in the network, secure routing can be implemented by combine security policy and routing policy. Figure1 describes the relationship between the Network Programming controller and network functions and security functions.

In this draft, Nodes are used to represent network elements. What is Node with security function? There are two deployment methods. 1. The security function and routing function are independent, but they are deployed in one site, as show in Figure1-1; 2. The security functions and routing functions are integrated, as show in Figure1-2.

```
                       +------------+
                       | Network    |
                       | Programming|
                       | Controller |
                       +------+-----+
                              |
        +---------------------+--------------------+
        |                                          |
        |                                          |
+-------+-------+     +----------------------------+--------+
|       |       |     |                            |        |
|   +---+---+   |     | +----------+           +---+---+    |
|   | Router|-----------| Security |-----------| Router|    |
|   +---+---+   |     | | Function |           +-------+    |
|       |       |     | +----------+                        |
|  +----+----+  |     |                                     |
|  |Security |  |     +-------------------------------------+
|  |Function |  |                      Node
|  +---------+  |
|               |
+---------------+
      Node
```

Figure 1-1: Functions independent mode of Node

```
                     +------------+
                     | Network    |
                     | Programming|
                     | Controller |
                     +------+-----+
                            |
      +---------------------+--------------------+
      |                                          |
+-------------------+                       +---------+
| Network function  |                       |  Router |
| Security function |                       +---------+
+-------------------+                         Node
     Node
```

Figure 1-2: Functions integration mode of Node

4. Secure Routing Use Cases

Two use cases are described below.

1. Routing policy ensure transmission security based on network node security appraisal;

2. Differentiated security path to meet diverse service requirements.

4.1. Basic path for secure routing

This scenario occurs in the network. High security users require the link and forwarding node physical isolation, and through a specific link path. To satisfied this requirement, it is necessary for the network programming controller to collect the network node information.

Network programming controller obtain the information of nodes and appraise the trustworthiness can improve nodes security awareness. Figure2 describes nodes security appraisement.

```
            +-------------+
            | Network     |
            | Programming |
            | Controller  |
            +-------------+
                   | appraise
                   | trustworthiness
    +--------------+---------------+
    ^              ^               ^
    |              |               |
    |              |               |
+---+----+     +---+---+      +----+---+
| Node1  |     | Node2 |      | Node3  |
+--------+     +-------+      +--------+
```

Figure2 : Node security appraisement

Also, the trustworthiness of node is different, for Node3 with poor trustworthiness, important users will avoid Node3 for routing policy. Figure3 describes userA's link forwarding process avoids Node3,select path<1,2,3,4>.

```
          Ingress

+--------+  1    +------+   5    +---------+  6  +-------+
| UserA  |------>| Node1|--------|  Node3  |-----| Node5 |
+--------+       +------+        +---------+     +-------+
                     |                |              |
                     |                |              |
                     | 2              |7             |8
                     |                |              |
                     |                |              |
                     v                |              |
                 +-------+    3   +-------+    4  +-------+
                 | Node2 |------->| Node4 |------>| Node6 |---->
                 +-------+        +-------+       +-------+  Egress
```

Figure3 : Link forwarding protection

4.2. Differentiated service for secure routing.

ISPs have built many security functions and security resource pools in the network, once the network node is attacked, it needs fast and efficient scheduling security function to mitigate. Users have clear requirements for their own security services.

The types of users are different, and the corresponding security requirements are different. The security requirement is no longer simply divided into high, medium and low levels, but more specific. For example, in addition to considering low-latency connections, customers in the game industry should first consider anti-DDoS services for security requirements,therefore, ISPs are required to provide anti-DDoS security services. For financial customers, data security is the most important requirement, it is required that data cannot be tampered with, eavesdropped or copied, and so on.

For customers with specific security requirements, ISPs need to transmit data at the security level expected by customers. For example, if the user needs anti-ddos and IPS services, the secure routing must pass through Node4 and Node5.

When userA needs Anti-ddos services, the secure routing must pass through Node5, Figure4-1 shows the path<1,5,6,10> selected for UserA which require anti-ddos service.

```
                                                 +----------+
+--------+  1    +------+   5    +---------+  6  | Node5    |
| UserA  |------>| Node1|------->|   Node3 |---->| Anti-ddos|----+
+--------+       +---+--+       +----+----+     +----------+    |
         ingress     |                |              |           |
                     |                |              |           |
                     | 2              |7             |8          |10
                     |                |              |           |
                     |                |              |           |
                     |                |              |           V
                 +------+     3   +------+    4  +--------+   9 +------+
                 | Node2|---------| Node4|-------| Node6 |-----|Egress|-
                 | WAF  |         | IPS  |       +--------+     +------+
                 +------+         +------+                         |
                     |                      11                     |
                     +-------------------------------------------+
```

Figure4-1 : User require anti-ddos service

When userA needs IPS services, the secure routing must pass through Node4, Figure4-2 shows the path<1,5,7,4,9> selected for UserA which require IPS service.

```
                                                 +----------+
+--------+  1    +------+   5    +---------+  6  | Node5    |
| UserA  |------>| Node1|------->|   Node3 |-----| Anti-ddos|----+
+--------+       +---+--+       +----+----+     +----------+    |
         ingress     |                |              |           |
                     |                |              |           |
                     | 2              |7             |8          |10
                     |                |              |           |
                     |                |              |           |
                     |                |              |           |
                 +------+     3   +---v--+    4  +-------+ 9   +------+
                 | Node2|---------| Node4|------>| Node6 |---->|Egress|-
                 | WAF  |         | IPS  |       +-------+     +------+
                 +------+         +------+                       |
                     |                      11                   |
                     +-------------------------------------------+
```

Figure4-2 : User require IPS service

When userA needs WAF services, the secure routing must pass through Node2, Figure4-3 shows the path<1,2,11> selected for UserA which require IPS service.

```
                                                 +----------+
+--------+  1    +------+   5    +---------+  6  | Node5    |
| UserA  |------>| Node1|--------|   Node3 |-----| Anti-ddos|----+
+--------+       +---+--+       +----+----+     +----------+    |
         ingress     |                |              |           |
                     |                |              |           |
                     | 2              |7             |8          |10
                     |                |              |           |
                     |                |              |           |
                     V                |              |           |
                 +------+     3   +------+    4  +-------+ 9   +------+
                 | Node2|---------| Node4|-------| Node6 |-----|Egress|-
                 | WAF  |         | IPS  |       +-------+     +------+
                 +------+         +------+                       ^
                     |                      11                   |
                     +-------------------------------------------+
```

Figure4-3 : User require WAF service

When userA needs IPS, WAF and Anti-ddos services, the secure routing must pass through Node4, Node2 and Node5, Figure4-4 shows the path<1,2,3,7,6,10> selected for UserA which require IPS, WAF and Anti-ddos services.

```
                                                 +----------+
+--------+  1    +------+   5    +---------+  6  | Node5     |
| UserA  |------>| Node1|--------|   Node3 |---->| Anti-ddos|----+
+--------+       +---+--+        +----+----+     +----------+    |
         ingress     |                ^              |           |
                     |                |              |           |
                     | 2              |7             |8          |10
                     |                |              |           |
                     |                |              |           |
                     V                |              |           V
                 +------+     3   +------+    4  +-------+ 9   +------+
                 | Node2|-------->| Node4|-------| Node6 |-----|Egress|-
                 | WAF  |         | IPS  |       +-------+     +------+
                 +------+         +------+                       |
                     |                      11                   |
                     +-------------------------------------------+
```

Figure4-4 : User require WAF IPS and Anti-ddos services

5. IANA Considerations

This memo includes no request to IANA.

6. Security Considerations

TBD

Authors' Addresses

Meiling Chen
China Mobile
BeiJing
China

Email: chenmeiling@chinamobile.com

Li Su
China Mobile
BeiJing
China

Email: suli@chinamobile.com

Bo Yang
China Mobile
BeiJing
China

Email: yangbo@chinamobile.com