SFC Use Cases for Network Security

draft-wang-sfc-ns-use-cases-00

Eric Wang (ejwang@cisco.com)
Kent Leung (kleung@cisco.com)
Jeremy Felix (jefelix@cisco.com)
Jay Iyer (jiyer@cisco.com)
Purpose

• Identify use cases for network security functions to participate in SFC
• Identify potential work items in the SFC framework
Service Classification

- Identifying flow **initiator** and **responder**
- Classification based on both **network** and **application criteria**
- Switching to a **new Service Function Path** based on application criteria (e.g. TLS traffic to a new path)
Service Function

- Embedding SC for Service Policy re-evaluation based on L5-7 data
- Mid-stream flow pick-up
- Bypass/offloading with intelligent control (e.g. TCP control packets, # of packets)
  draft-kumar-sfc-offloads-01
- Tap mode (e.g. IDS, Packet Capture)
Service Function Packet Handling

- **Dropping** packets and closing flows
- **Injecting** new packets
  - [draft-penno-sfc-packet-01](http://example.com/draft-penno-sfc-packet-01)
- **Initiating** new connections
- Producing security classification results for subsequent Service Functions
Thank you!
Flow Initiator and Responder

(a) Flows from Host A

(b) Flows from Host B
Mid-stream Service Function Path Update

---

<table>
<thead>
<tr>
<th>Packets</th>
<th>Service Function Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Handshake</td>
<td>SFP-1. AVC:Firewall</td>
</tr>
<tr>
<td>TLS Client Hello</td>
<td>SFP-1; Switched to SFP-2 after AVC</td>
</tr>
<tr>
<td>Rest of TLS HS</td>
<td>SFP-2. AVC:TLS Proxy:Firewall</td>
</tr>
<tr>
<td>HTTPS Data</td>
<td>SFP-2. AVC:TLS Proxy:Firewall</td>
</tr>
</tbody>
</table>
Service Function Bypass with Control
Tap Mode Service Function

[ ] denotes a packet sink
Packet Drop and Flow Close
Accumulated Security Classification Results

Diagram:

- C (Client) -> Reputation (Client Reputation score 6)
- Reputation (Client Reputation score 6) -> Web Proxy
- Web Proxy -> Accessing website rep score 2 (Accessing website rep score 2) -> Malware found in download
- Malware found in download -> V (Client Reputation score 6)
- V (Client Reputation score 6) -> V
- V -> Block
- Block

Legend:

- C: Client
- S: Server
- Reputation: Client Reputation score
- Web Proxy
- Accessing website rep score
- Malware found in download
- Block

IETF Logo
Aggregated Security Classification Results