SFC Network Security Use Cases
draft-wang-sfc-ns-use-cases-02

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

Network Service Header (NSH) Context Header Allocation (Network Security)
draft-wang-sfc-nsh-ns-allocation-01

Eric Wang (ejwang@cisco.com)
Kent Leung (kleung@cisco.com)
Andrew Ossipov (aossipov@cisco.com)
SFC Network Security Use Cases – Updates
draft-wang-sfc-ns-use-cases-02

• Published -01, -02 versions
  • Incorporated review comments
  • New use cases
  • Listed items that may require WG work
SFC Network Security Use Cases Recap

**Stateful**
- Bi-directional traffic
- Traffic initiator vs. responder

**Application Level Processing**
- SC with application criteria
- SFP change by SF with SC capability at application level
- Mid-stream pick-up; frame w/o L2-L4 headers
- Session grouping by application

**Other Behaviors**
- Bypass/Offloads
- Receive-only
- Initiating connections
- Sharing of security classification
## Use Cases Addressed by WG Drafts

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
<th>Addressed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful SFs</td>
<td>SFC MUST support the use of stateful Service Classifiers and Service Functions if present.</td>
<td>draft-wang-sfc-nsh-ns-allocation-01</td>
</tr>
<tr>
<td>Frames w/o L2-L4 headers</td>
<td>SFC SHOULD allow packet frames carrying only L5 and upper layer traffic data without L2-L4 headers.</td>
<td></td>
</tr>
<tr>
<td>SF bypass/offload</td>
<td>SFC SHOULD support bypass of a Service Function in the middle of a connection while allowing necessary control packets to reach the Service Function.</td>
<td>draft-kumar-sfc-offloads-03, draft-wang-sfc-nsh-ns-allocation (to be revised)</td>
</tr>
<tr>
<td>Receive-only SF</td>
<td>SFC control plane and packet plane MUST support receive-only Service Functions.</td>
<td>draft-wang-sfc-receive-only-01</td>
</tr>
<tr>
<td>Packet injection by SF</td>
<td>SFC MUST support packet injection to the opposite direction of a Service Path</td>
<td>draft-penno-sfc-packet-03</td>
</tr>
<tr>
<td>Sharing of security classification</td>
<td>SFC SHOULD allow metadata passing classification results</td>
<td>draft-wang-sfc-nsh-ns-allocation-01</td>
</tr>
<tr>
<td>[New] Grouping related application sessions</td>
<td>SFC SHOULD support SFs to group related sessions using unique identifiers</td>
<td>draft-wang-sfc-nsh-ns-allocation (to be revised)</td>
</tr>
</tbody>
</table>
NSH Network Security Allocation
draft-wang-sfc-nsh-ns-allocation-01

• Support major requirements by a network security SFC domain
  • Statefulness
  • Security policy
  • Application session grouping
  • Security classification sharing
  • Offloads
  • Multi-tenancy
• MD-Type 1 and a TLV of MD-Type 2
NSH Security Allocation

Session ID

Application Session ID

Destination Class / Reserved

Source Class

Tenant ID

Dst Score

Src Score

Offloads

Multi-tenancy

Statefulness

Related Sessions

Security Policy

Security Classification
Q&A
Thank you!