DPDK SUMMIT CHINA 2017
Tencent Data Center Security Use case

DPDK based security service layer on data center

haohao zhang
Agenda

- what and why of the security service layer
- how to design
- performance optimize
- evolution for large volume
where is the layer

security on host:
- different OS
- CPU used must be controled
- complex policy

challenges of deploy on network perimeter:
- traffic control
- forward information--act like a router
- performance --latency, Throughput
- debug

support security function
- Anti-DDoS
- WAF
- IDS
- Forensics
- ........
comparison between DPDK and another option

<table>
<thead>
<tr>
<th></th>
<th>multi core platform</th>
<th>DPDK on x86</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td>high</td>
<td>middle</td>
</tr>
<tr>
<td>Reliability on massive deployment</td>
<td>high malfunction ratio</td>
<td>good</td>
</tr>
<tr>
<td>Development cost</td>
<td>high</td>
<td>middle</td>
</tr>
<tr>
<td>Debug</td>
<td>hard</td>
<td>middle</td>
</tr>
</tbody>
</table>

1. Reliability is very important when you need to manage thousands of devices.
2. Some weird problem leads to hardware like fiber.
Deployment Status

- Cover all the perimeter globally
- Thousands of DPDK based security devices
- Support all types of business, including web, game, video...
- Continue increasing
the software architecture
multi process model

- **primary process is stable**
  - packet forwarding information
  - router information
  - memory management
  - basic statistic
  - TAP management

- **secondary process changes quickly**
  - doing the security logical
  - update frequently
fake dequeue

1. avoid packet losing after secondary process crash
2. not in high performance mode

① secondary read head and tail of ring
② secondary copy mbuf without dequeue
③ secondary process packet
④ use volatile variable notify the primary process to dequeue
performance optimization

- Local variable VS global variable
- Hyper Thread for different scenarios:
  - whether threads number need larger than physical thread
  - pipeline mode
- sometimes tx queue number can affect
- assemble language can be used for critical function
- memcpy cost
evolution for large volume

- 100G NIC
- FPGA
- CPU on other NUMA Node
Thanks!!