Practice of Network Monitoring and Security Technologies in Cloud Data Center

Kai, Wang
YunShan Networks
Data center is evolving to be cloud based and software defined.
The monitoring and security problems in SD-C DC

- The logical topologies become more and more complex
  - Difficult to quickly find and locate the network problems in the tenant business
- The collection of network data is inefficient
  - Netflow/sFlow/IPFIX: Sampling, per-packet interrupt & netlink upcall
  - Limited variety of supported fields for collected flows
- The analysis of overlay traffic is insufficient
  - Unable to do flexible & find-grain traffic collection on demand
  - Unable to distinguish duplicated traffic from multiple tenants
  - Unable to effectively aggregate the overlay packets in tunnel capsulation and IP fragments
- The physical boundaries of network security disappear
  - Zero trust for the nodes in internal network
The monitoring solution
The security solution
Our solution: hypervisor based DFI (Deep Flow Inspection)
- Probe utilizing OvS in Hypervisor
- Overlay traffic collection
- Kernel module + Userspace agent + OvS action
- Cons: invasive deployment
  - Stability Problems: crash, soft lockup
  - Influence to tenant business

Our solution: VM based DFI
- Deployed in VM
- Mirror overlay traffic to VM
- Performance bottleneck

Technology evolution for virtualized networks monitoring
Our current solution: DPDK based
- Utilizing OvS-DPDK
  - Fully exploit the compute resource of VM
- Extend functions based on OvS-DPDK conntrack
  - ACL
  - Flow generation
  - Packet header extraction and compression
  - DPI
  - NPB
- SDN
- More efficient, flexible, benefit for debug
- Used for physical networks monitoring as well
Further optimization for exporter

- NIC Multi-queue & Symmetric RSS
  - VM template
- Parallelize conntrack processing
  - Make it scalable
- Optimize the datapath classifier (dpcls) algorithm Tuple Space Search (TSS)
  - HyperSplit algorithm
- Intel vTune Amplifier
  - Lock, Polling & Interrupt
Analysis & Visualization

- Cluster-based analyzer
  - Use Storm to do real-time analysis
    - DDoS/Port Scan
    - Abnormal connections/transactions, Abnormal login
    - ARP/MAC/IP Spoof
    - Loop detection
  - Use Spark to do off-line analysis
    - Security analysis model
  - Use Elasticsearch/Kibana to do search and visualization
    - Customized statistics in different dimensions
    - Trace back of historical events
- Third-party analysis tool
  - E.g. SQUIL, SQL injection detection
From monitoring to security control

- Use the monitoring results to generate security policies
  - Exporter
    - Overview the security problems & risks in cloud networks
  - Analyzer
    - Locate the problematic nodes or areas
  - Controller
    - Prevent/Protect these nodes or areas via SDN
Security service chain and problems

- Use VNF to do security detection/prevention
  - Based on VXLAN
- Pros
  - Elastic and flexible
- Cons
  - Inefficient and low-performance, hard to cover the large-scale east-west traffic
    - VXLAN encap/decap load
    - Poor scalability of security service chain
    - vSwitch and VNF performance bottlenecks
Use VLAN instead of VXLAN to introduce traffic to assigned security nodes

- Offload VXLAN encap/decap to ToR switch, save more CPU for SSE processing

  ```
  table=0,priority=20,d1_vlan=2000,ip,actions=output:20
  table=0,priority=102,in_port=10,d1_vlan=0xffff,ip,actions=mod_vlan_vid:2000,resubmit(),0
  ```
Performance optimization

- Single VNF/SSC has limited performance
- Use SDN policies based trade-off to dispatch traffic to multiple chains
  - Based on pseudo node
  - Linearly increase the performance
- E.g.
  - priority=401,table=0,dl_vlan=1000,ip,tcp,p,
    tp_src=0/0x0001,tp_dst=0/0x0001,actions
    =mod_vlan_vid:2000,resubmit(,0)
  - priority=401,table=0,dl_vlan=1000,ip,tcp,p,
    tp_src=1/0x0001,tp_dst=1/0x0001,actions
    =mod_vlan_vid:2000,resubmit(,0)
  - priority=401,table=0,dl_vlan=1000,ip,tcp,p,
    tp_src=0/0x0001,tp_dst=1/0x0001,actions
    =mod_vlan_vid:3000,resubmit(,0)
  - priority=401,table=0,dl_vlan=1000,ip,tcp,p,
    tp_src=1/0x0001,tp_dst=0/0x0001,actions
    =mod_vlan_vid:3000,resubmit(,0)
Performance optimization

- Use OvS-DPDK to accelerate the networking in security resource pool
- Use DPDK to accelerate SSE
  - TOPSEC
Security cloud

- ISP
- Core Router
- Security Cloud
- SLB Cluster
- OpenStack
- x86 KVM Cluster, OvS-DPDK
- SDN Switch
- vFW
- vIPS
- VNF
- Controller
- SQL injection attack detection
- DDoS situational awareness
- Kibana visualization
- Custom development LB + vFW + vIPS

Traffic traction via route

Controller

Security analysis and protection
Thanks!!