DPDK

IT大咖说 知识分享平台

DPDK DATA PLANE DEVELOPMENT KIT

THE LINUX FOUNDATION

DPDK SUMMIT CHINA 2017

主办方： intel

参与方： 腾讯云 ZTE 美团云 Panabit 太一星晨 Balance Your Networks UnitedStack 云杉网络 Yunshan Networks

协办方： SDNLAB 专注网络创新技术

视频支持方： IT大咖说 知识分享平台

Practice of Network Monitoring and Security Technologies in Cloud Data Center

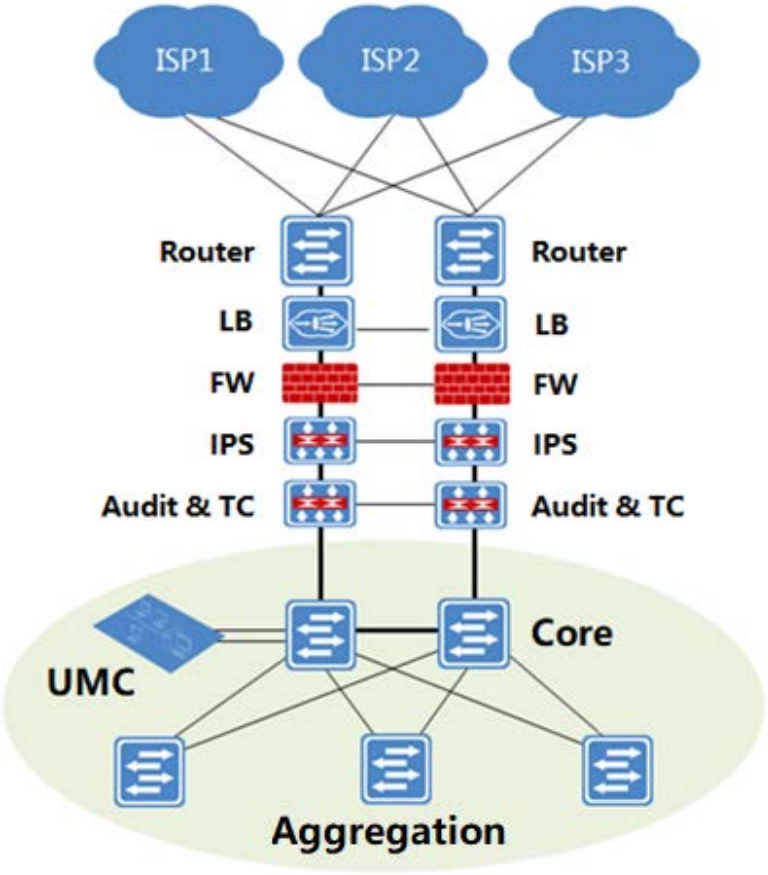
Kai, Wang
YunShan Networks

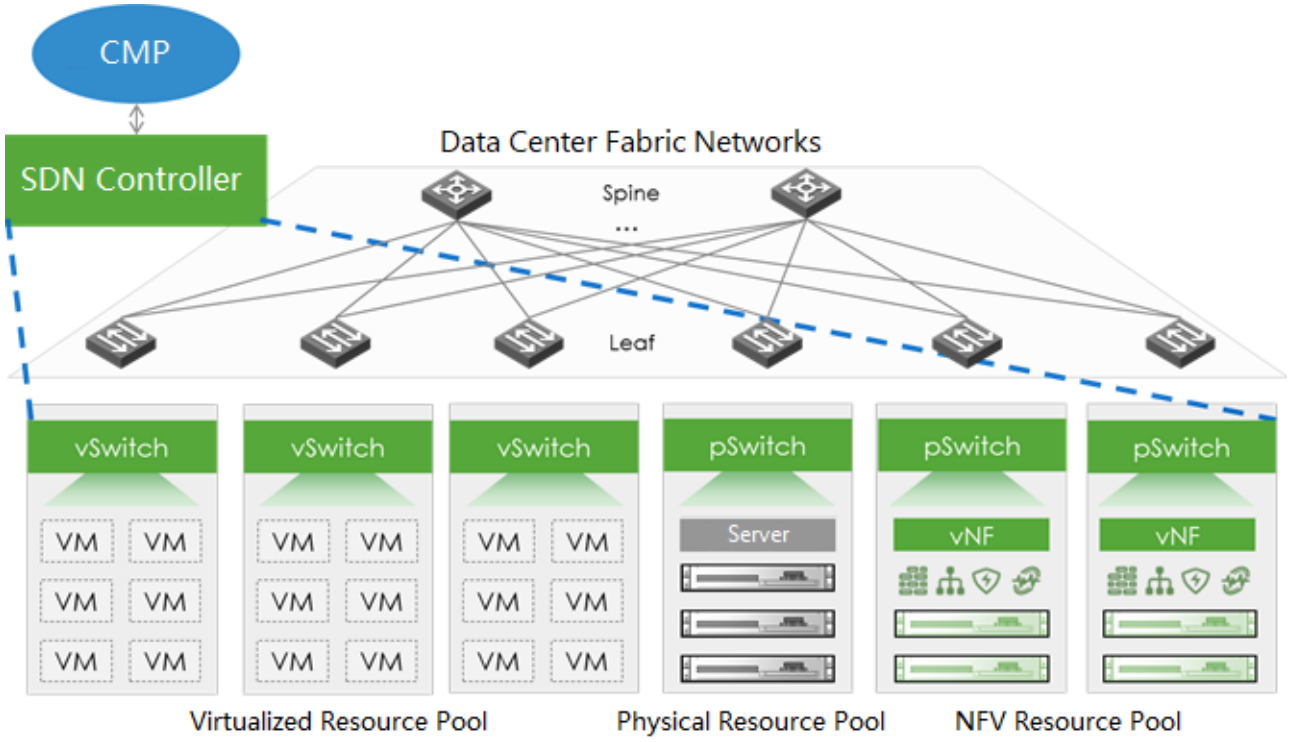
主办方：intel

参与方：腾讯云 ZTE 美团云 Panabit 太一星晨 云杉网络

协办方：SDNLAB 视频支持方：IT大咖说

Data center is evolving to be cloud based and software defined

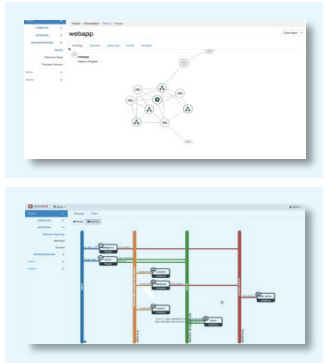




The monitoring and security problems in SD-CDC

- **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

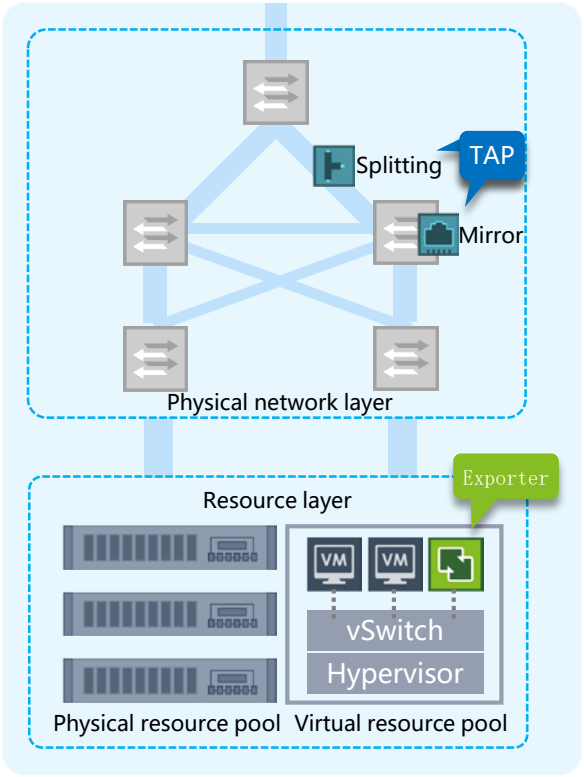
The monitoring solution



openstack KVM vmware docker 阿里云 腾讯云 amazon web services Microsoft Azure

Management

openstack

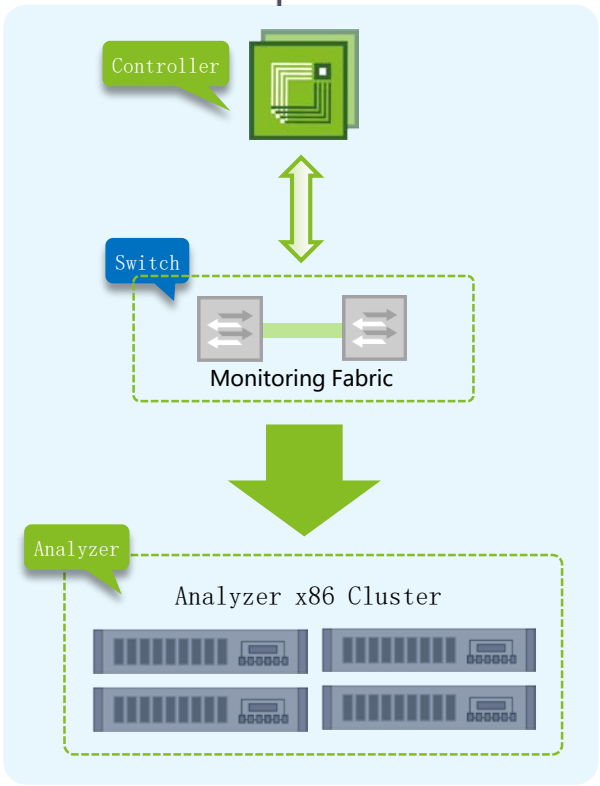


Traffic

Traffic

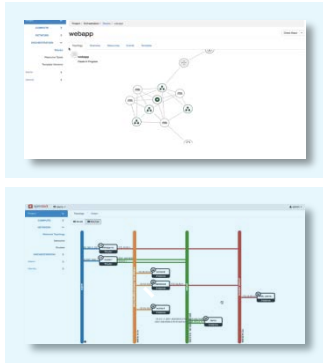
Traffic

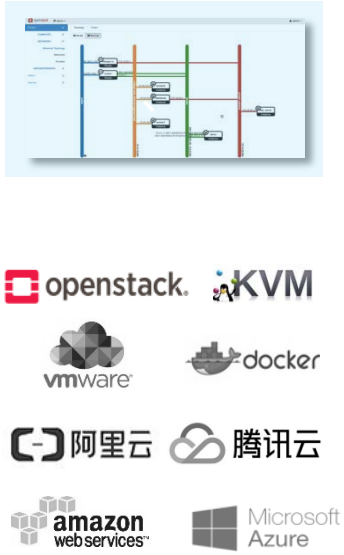
DeepFlow™



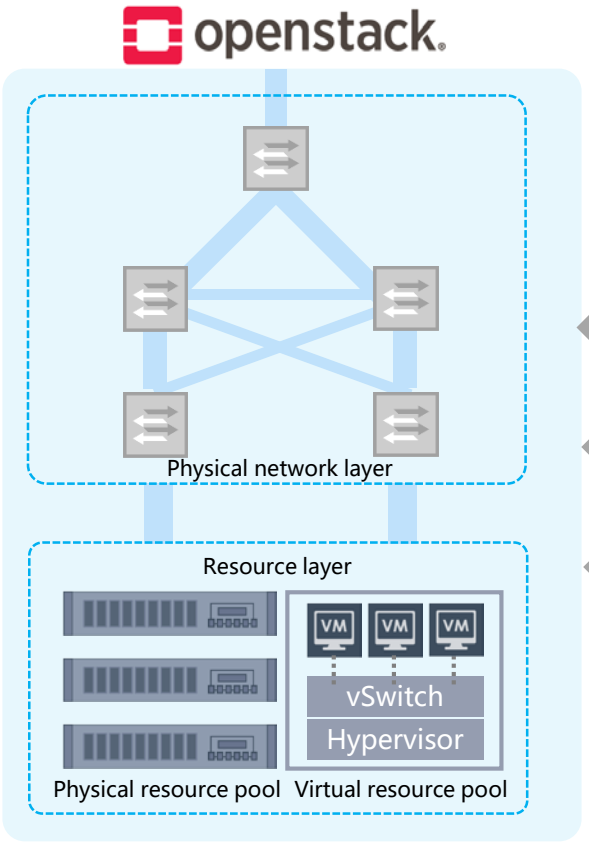
Cloud Analyzer

The security solution





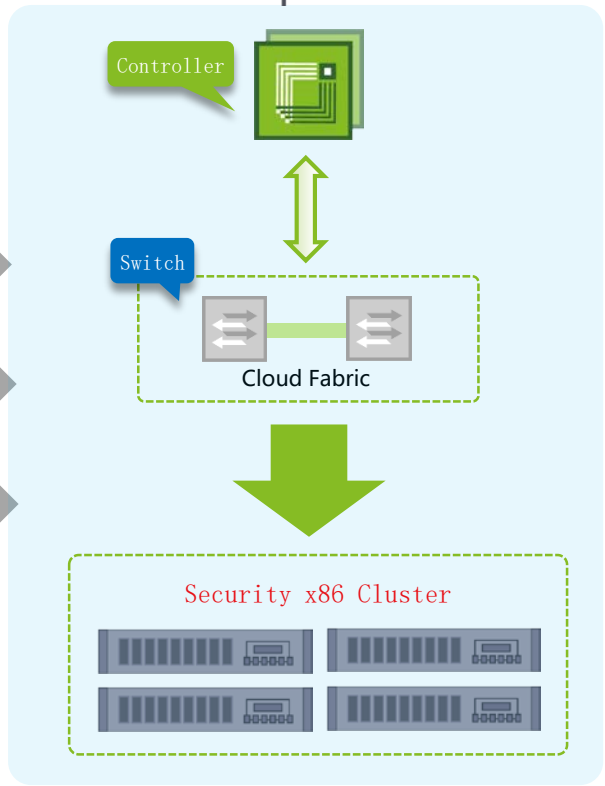
Management



Traffic

Traffic

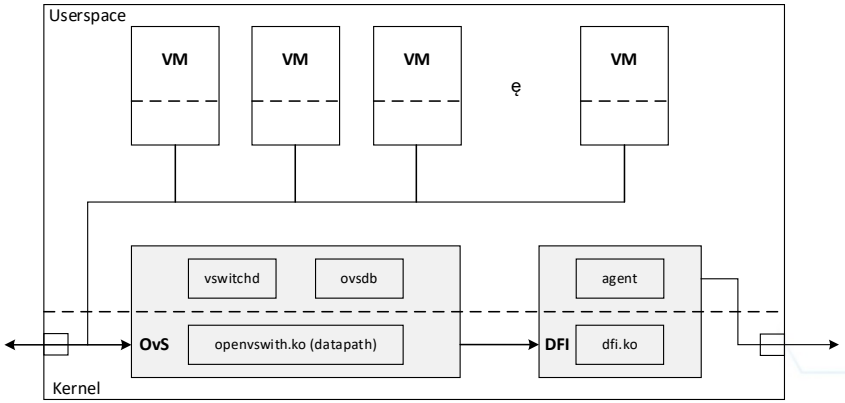
Traffic

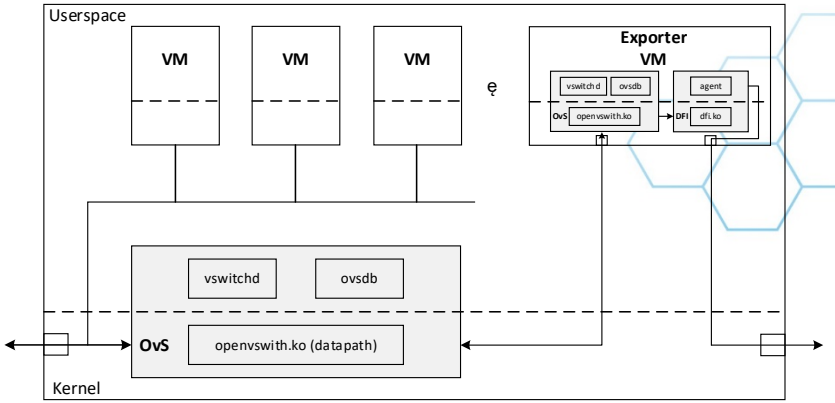


Security Protection

Technology evolution for virtualized networks monitoring

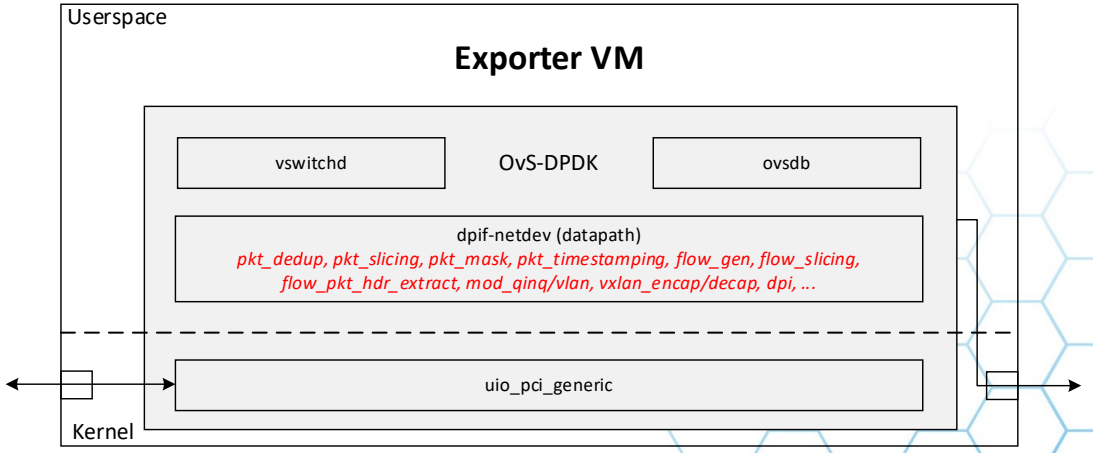
- Our solution: hypervisor based DFI (Deep Flow Inspection)
  - Probe utilizing OvS in Hypervisor
  - Overlay traffic collection
  - Kernel module + Userspace agent + OvS action
  - Cons: invasive deployment
    - Stability Problems: crash, soft lockup
    - Influence to tenant business
- Our solution: VM based DFI
  - Deployed in VM
  - Mirror overlay traffic to VM
  - Performance bottleneck





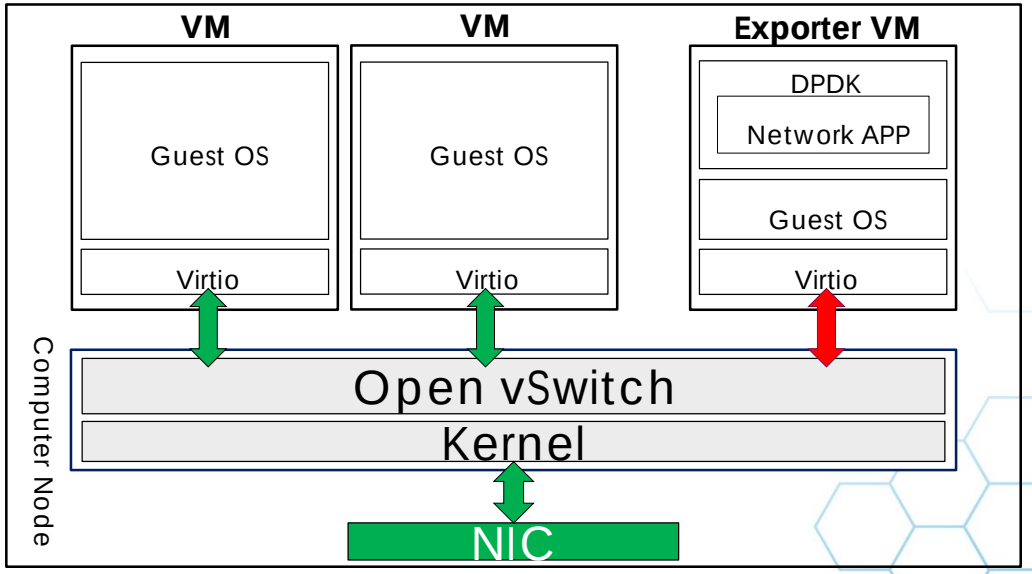
Technology evolution for virtualized networks monitoring

- 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



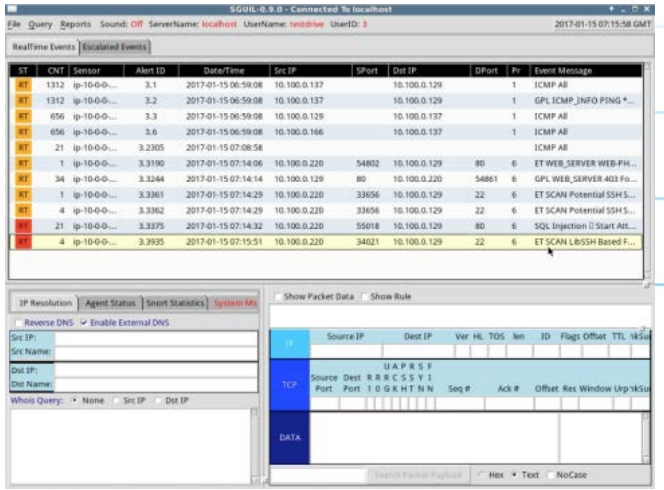
Further optimization for exporter

- 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



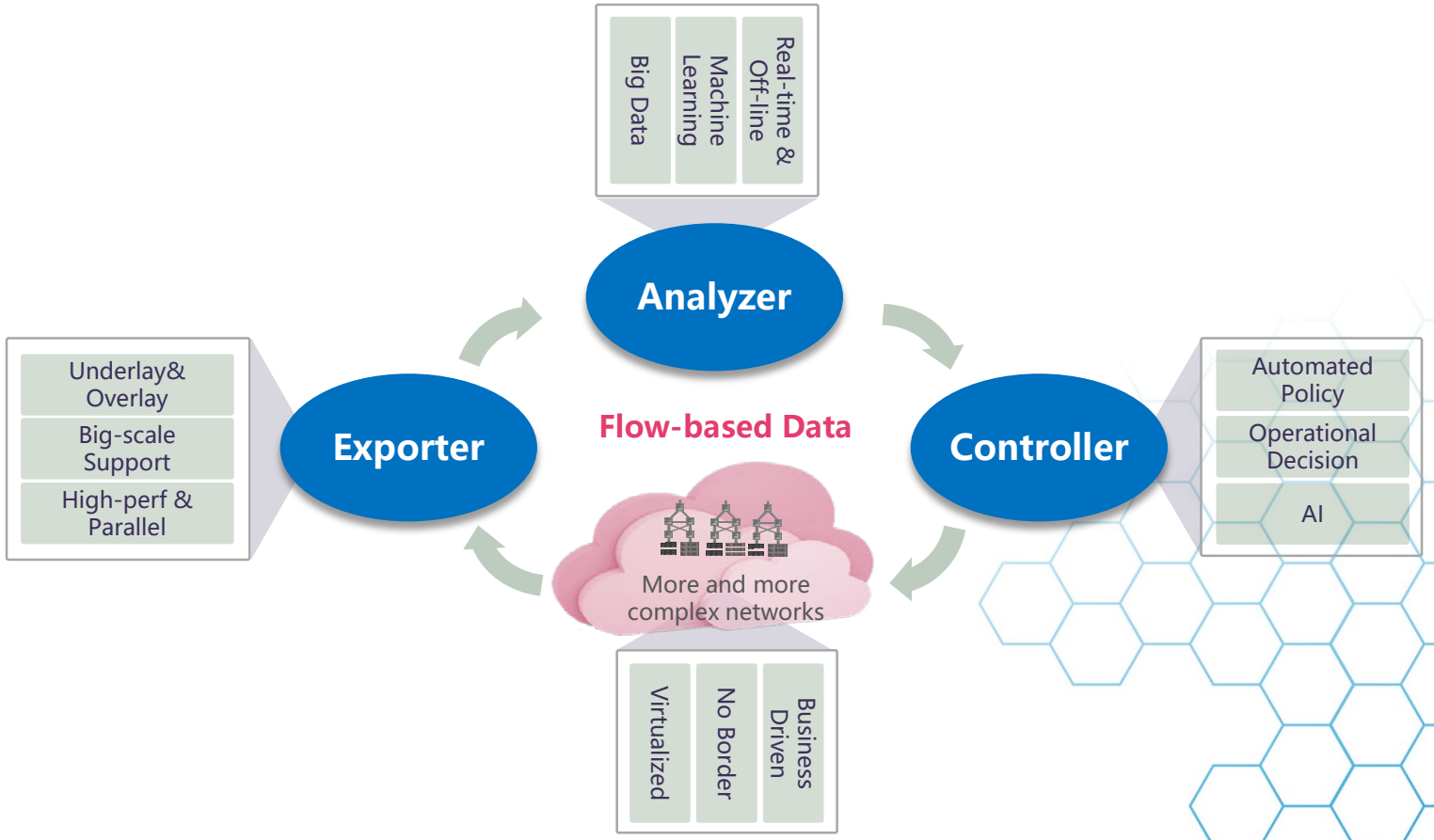
Analysis & Visualization

- 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



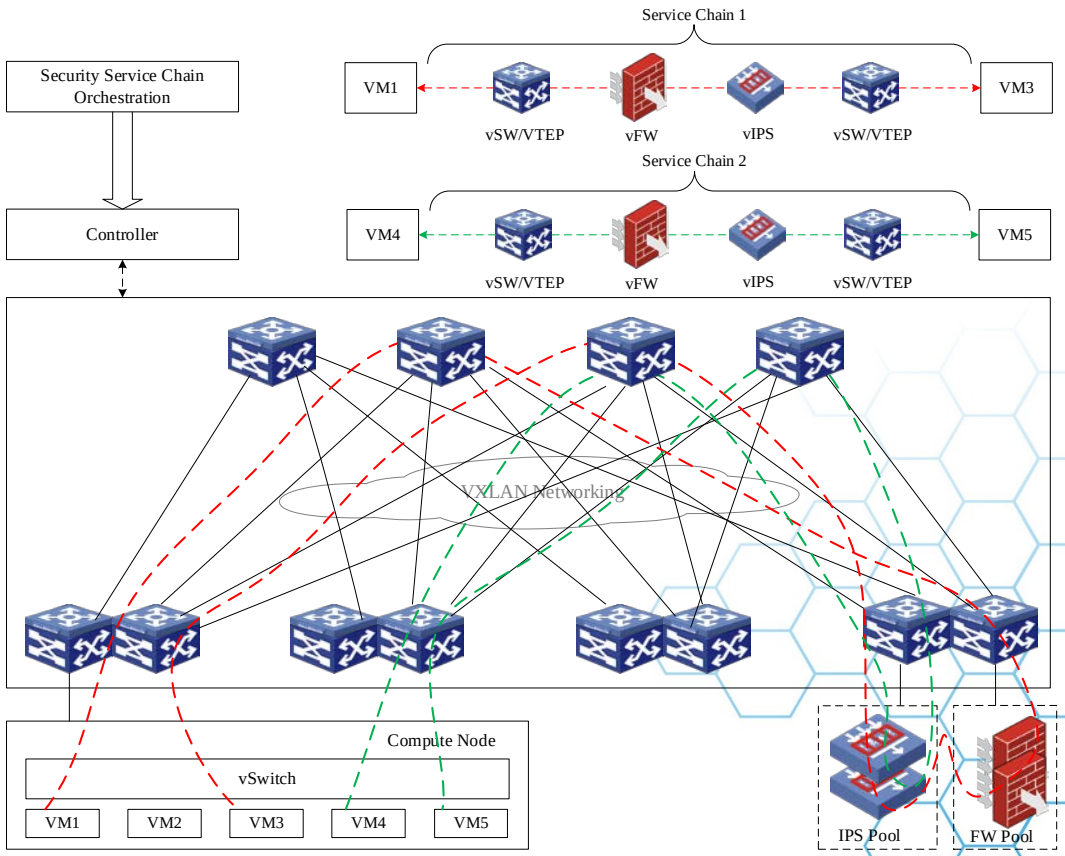
From monitoring to security control

- 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



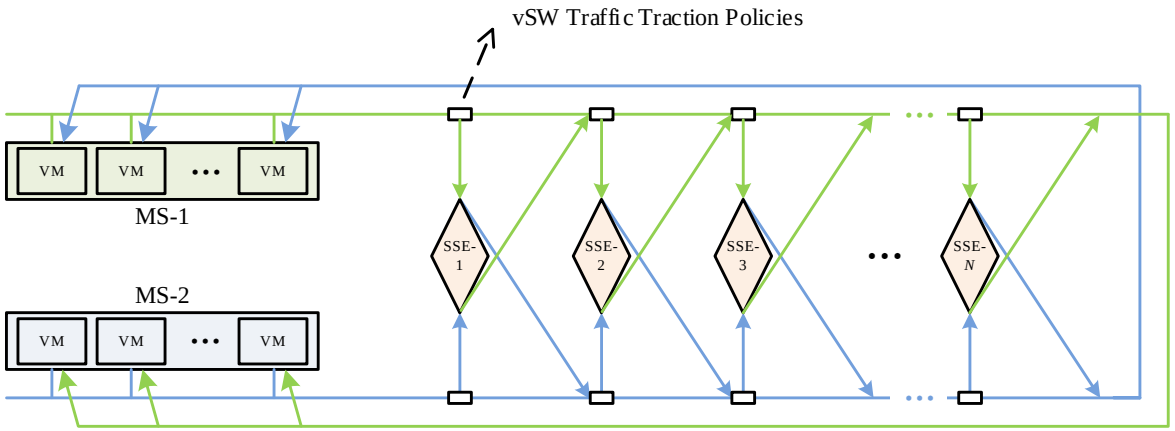
Security service chain and problems

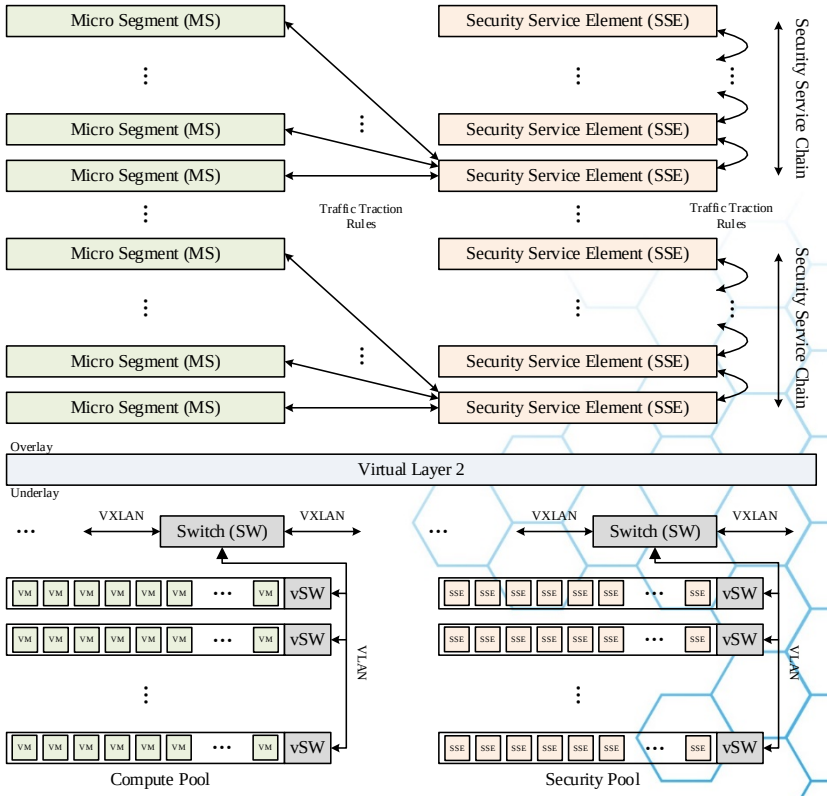
- Use VNF to do security detection/prevention
  - Based on VXLAN
- Pros
  - Elastic and flexible
- Cons
  - Inefficient and low-performance, hard to cover the large-scale east-west traffic
    - VXLAN encap/decap load
    - Poor scalability of security service chain
    - vSwitch and VNF performance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



Performance optimization

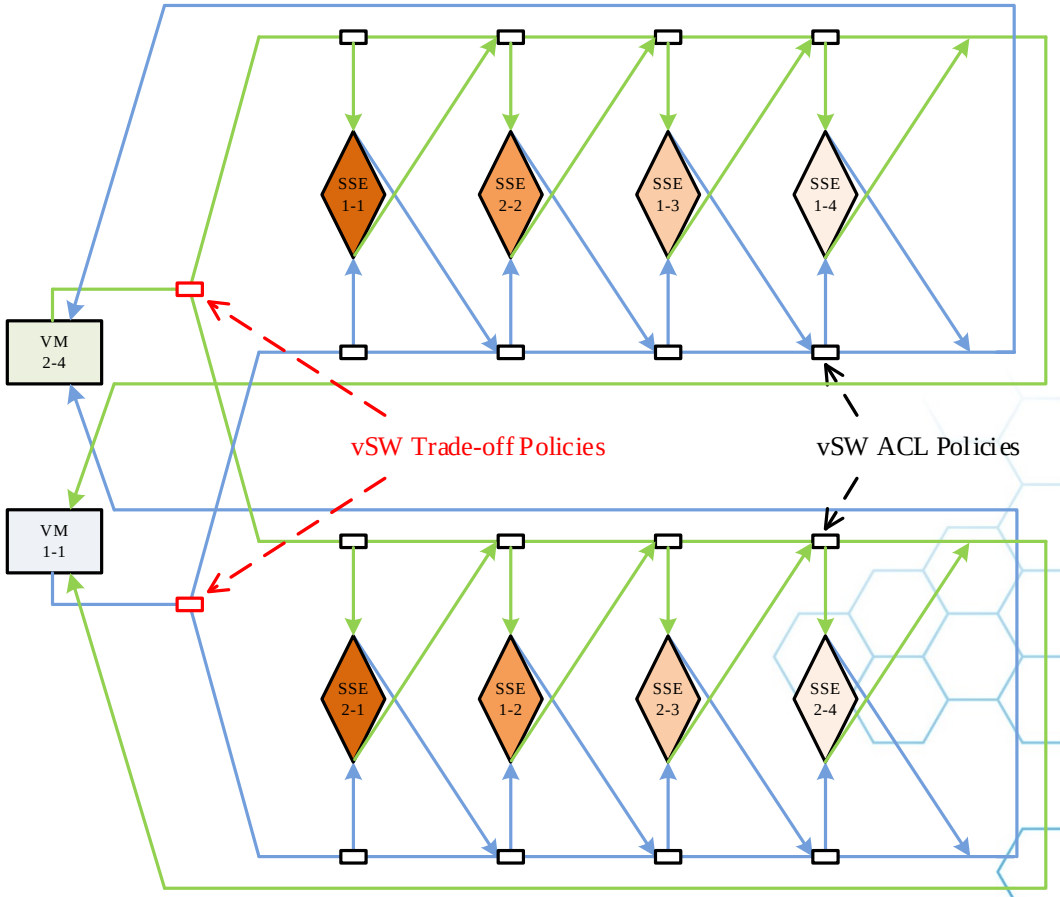
- Use VLAN instead of VXLAN to introduce traffic to assigned security nodes
  - Offload VXLAN encap/decap to ToR switch, save more CPU for SSE processing
    - table=0,priority=202,dl_vlan=2000,ip,actions=output:20
    - table=0,priority=102,in_port=10,dl_vlan=0xffff,ip,actions=mod_vlan_vid:2000,resubmit(,0)





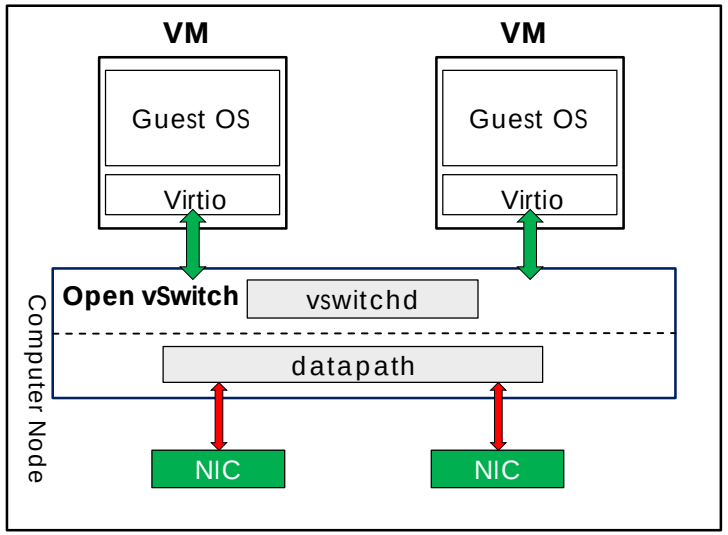
Performance optimization

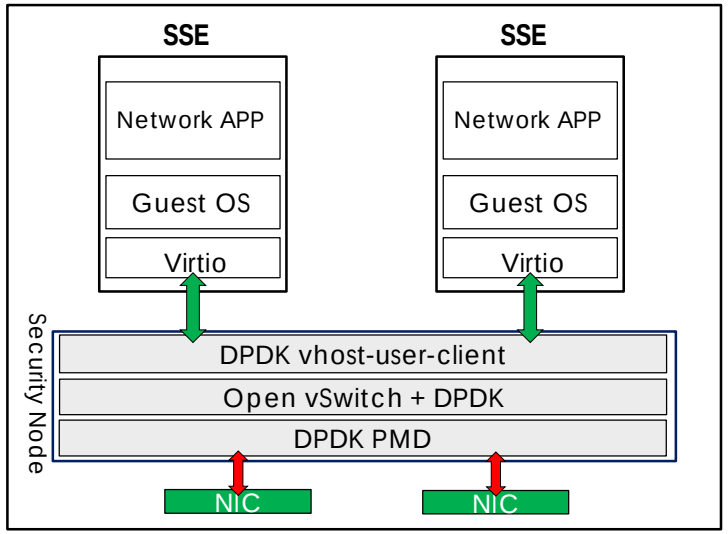
- Single VNF/SSC has limited performance
- Use SDN policies based trade-off to dispatch traffic to multiple chains
  - Based on pseudo node
  - Linearly increase the performance
- E.g.
  - priority=401,table=0,dl_vlan=1000,ip,tcp,tp_src=0/0x0001,tp_dst=0/0x0001,actions=mod_vlan_vid:2000,resubmit(,0)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

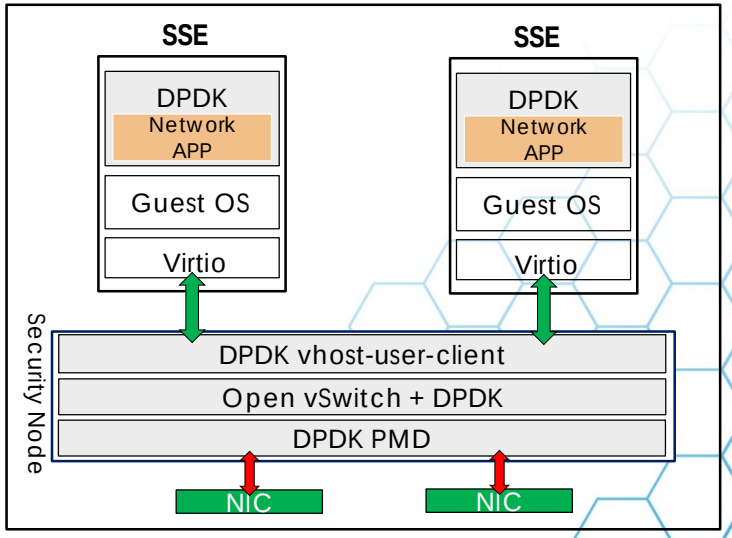


Performance optimization

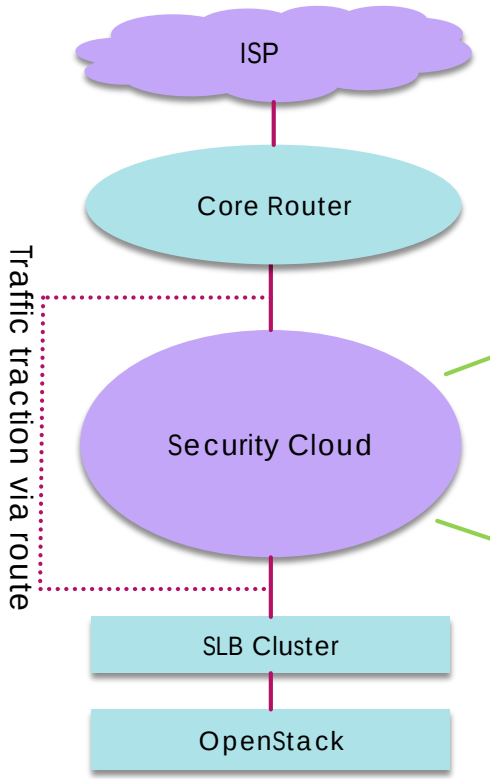
- Use OvS-DPDK to accelerate the networking in security resource pool
- Use DPDK to accelerate SSE
  - TOPSEC

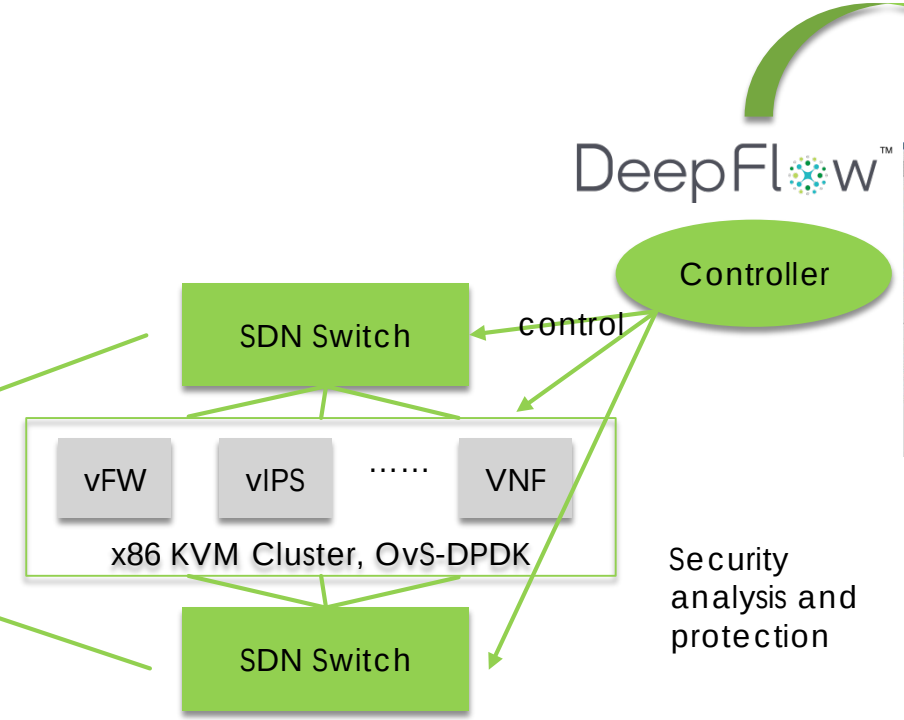




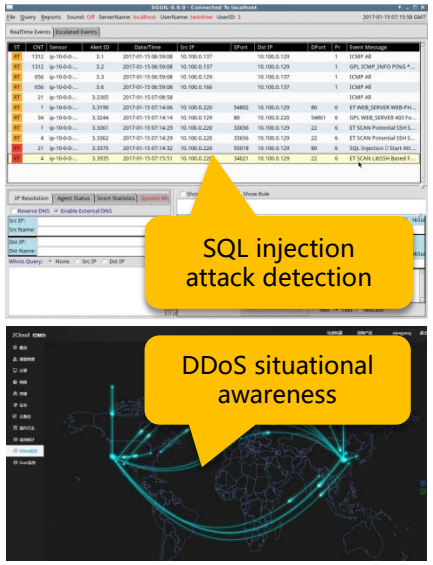


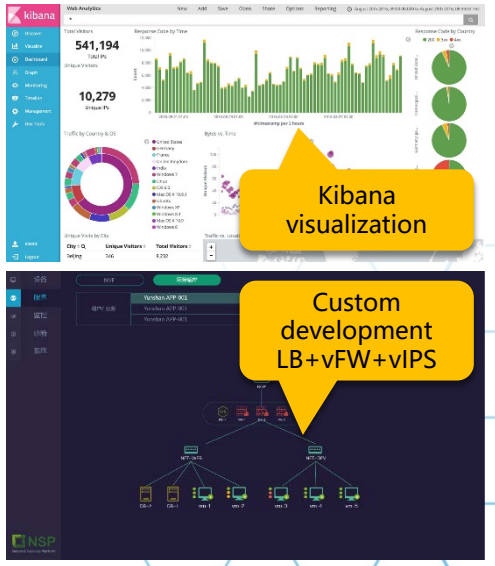
Security cloud





Security analysis and protection





+

Thanks!!