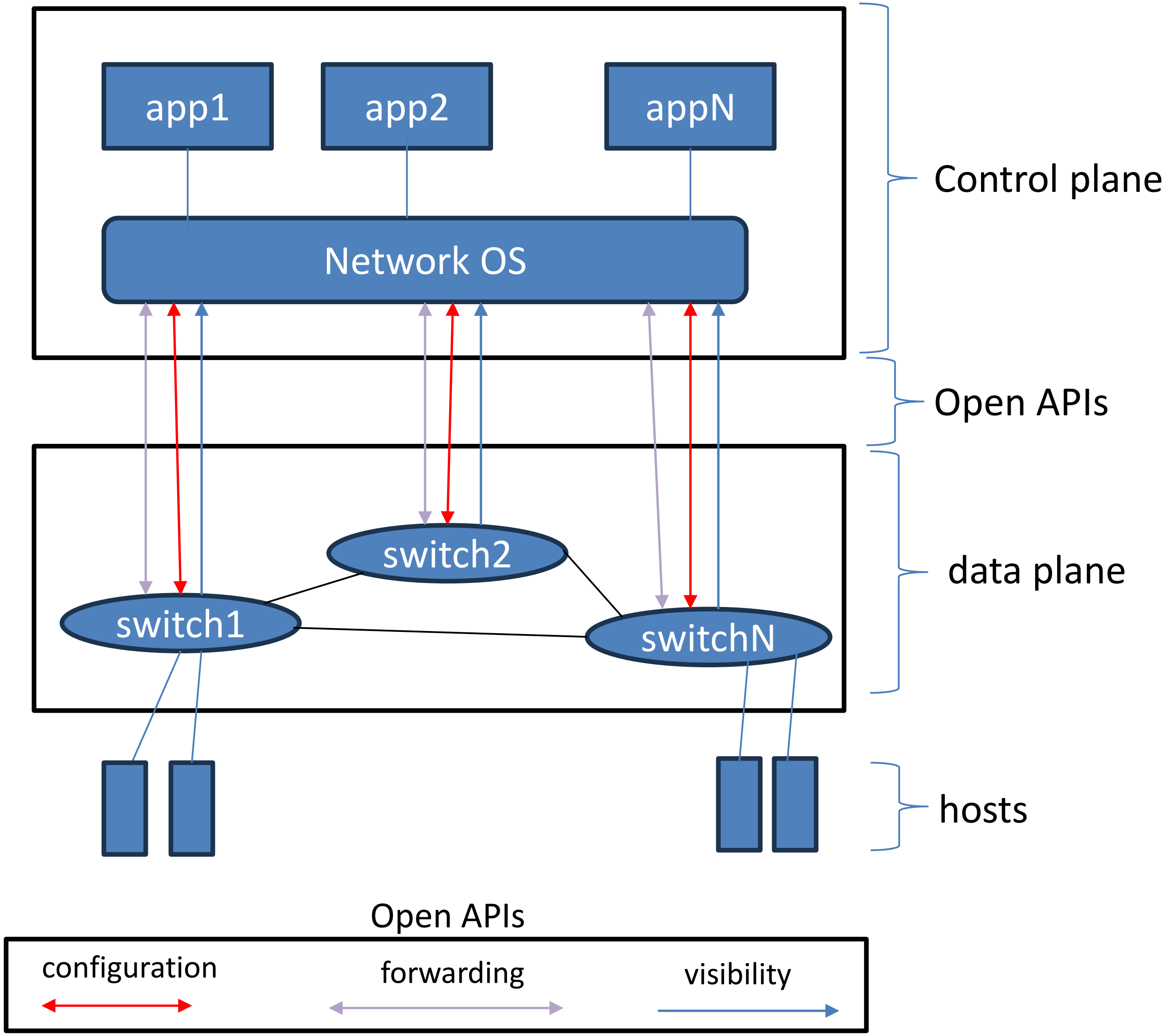
Secure Operating Systems

Nikos Tziritas

Software Defined Networking

Software Defined Networking



app1

app2

appN

Network OS

Control plane

Open APIs

data plane

switch2

switch1

switchN

hosts

Open APIs

configuration

forwarding

visibility

SDN Components

- Switches do not rely on proprietary software to control their forwarding behavior
- Data plane comprises switches connected together to form a network
- Control plane: switches in an SDN architecture are controlled by a Network OS (NOS) that interacts with the switches to provide an abstract model of the network topology to Applications running on the NOS
- Applications can adapt the network behavior to suite specialized requirements, for example, providing network virtualization services that allow multiple logical networks to share a single physical network - similar to the way in which a hypervisor allows multiple virtual machines to share a single physical machine

Open APIs

- **Forwarding**: The OpenFlow protocol was originally developed so that academic researchers could experiment with external control of switch packet forwarding. OpenFlow quickly gained support, leading to the formation of the Open Networking Foundation (ONF) to develop and promote the OpenFlow standard.
- **Configuration**: It was quickly realized that OpenFlow alone isn't sufficient - a configuration protocol is needed to assign switches to controllers, configure port settings and provision queues.
- **Visibility**: Current efforts in the SDN community are focused on provisioning of network services. Going beyond merely providing connectivity to creating a NOS that is aware of network performance requires an API providing visibility into switch traffic. A performance aware NOS allows applications to manage resource allocation, balance loads and ensure quality of service.

Security Advantages of SDN

- Effective monitoring of abnormal traffic
- Timely dealing with vulnerabilities

SDN Security Issues

- Vulnerable controller
- Risks caused by open programmable interfaces
- More attack points

Possible Attack Points

- The SDN Switch
- The links between SDN Switches
- The SDN Controller
- The links between controller and switches
- The links between controllers
- The Application software

Data Plane Threats

- Man in the middle attack between switch and controller
  - Attack to tamper with the rules
- DoS attack to saturate the flow table and flow buffer

Control Plane Threats

- DoS/DDoS attacks on the controller
- Threats on distributed multi-controllers
- Threats from applications

Application Plane Threats

- Illegal access
- Security rules and configuration conflicts

Countermeasures

- Deploying security applications to handle security issues per threat
- Solving security issues directly by changing SDN rules

Network Function Virtualization (NFV)

- Network Functions Virtualization (NFV) is used as a virtualized method to design, deploy, and manage networking services
- NFV takes network functions that operate from a hardware base and allows them to run within software as virtual machines
- Network functions that can be virtualized with NFV include Domain Name Service (DNS), Network Address Translation (NAT), firewalls, encryption

Limitations of using hardware

- Hardware is expensive
- Hardware cannot be updated easily as software
- Replacing hardware is also expensive
- The network is limited in its capabilities by the hardware it is currently using

Why NFVs (1/2)

- No need to configure and manage physical devices
- Manual devices are complicated to manage because they need to be maintained and cabled together
- a NFV allows the user to interact with network functions at the server level

Why NFVs (2/2)

- NFVs allow enterprises to move away from the constraint of managing physical devices
- Services can be customized and deployed when they are needed and not when a vendor device is appropriate
- With NFVs we can abstract physical resources

Why not traditional firewall and routing devices

- They are prune to failure against virtualized versions
- With physical devices you cannot change easily the network structure
- With NFVs you can perform a change in the network structure dynamically
- If a natural disaster or system failure affects your network then physical devices cannot escape being affected
  - On the other hand a virtual device can be moved to any location.

Advantages of NFVs

- Reduced hardware needs
- Saving space and power
- Lowers time to releasing services
- Scalability

Reduced Hardware Needs

- By virtualizing your infrastructure you minimize the amount of hardware you need to purchase and maintain
- You can also avoid the problem of over provisioning that is common with hardware

Saving Space and Power

- One of the issues with hardware is that it takes up space and needs to be powered and cooled in order to stay operational
- This isn’t the same for virtual services which can be managed entirely with software

Lower time to releasing services

- You can deploy networking services at a faster rate than is possible with hardware
- Every time the requirements of your enterprise change you can make a change and keep up quickly.

Scalability

- Being able to upscale and downscale services on demand provide you with the long-term capacity potential that you need to be successful in the future

Threats to NFV

- Even though NFV provide many advantages against using physical devices, they also come with a number of substantial risks
- With NFV services are less transparent (e.g., network traffic is much more difficult to monitor)

Lack of monitoring (1/2)

- On a legacy network, traffic can be monitored through a range of means and measured by network monitoring tools
- This is different in virtual environments because many traffic doesn’t interact with physical devices but virtual machines

Lack of monitoring (2/2)

- Data exchanged between virtual machines flies under the radar of most network monitoring tools and techniques
- This is a substantial problem because it makes it difficult for administrators to diagnose performance issues and to detect cyber attacks
- Therefore when you deploy NFVs your network become less transparent

New Security Concerns (1/2)

- We have a new architecture that needs to be managed
- This architecture is an area where several security risks can be posed
  - The network administrator needs to be aware of new security risks

New security concerns (2/2)

- An administrator needs to manage new software components
  - Hypervisor
  - VMs
- An administrator needs to think of the way the NFVs work.
  - An attack to an NFV may cause failure to another NFV

Performance Bottlenecks

- Since now the network functions are deployed in virtual resources we need to monitor for performance bottlenecks

NFV and its connection to IoT and 5G (1/2)

- 5G promises to build on the widespread connectivity delivered by 4G and enable more wireless devices to connect to the internet.
- The growth of 5G is increasing the need for a network architecture that departs from the legacy model.
- Network functions virtualization is one of the key technologies that can ally with 5G to form the next generation of networking

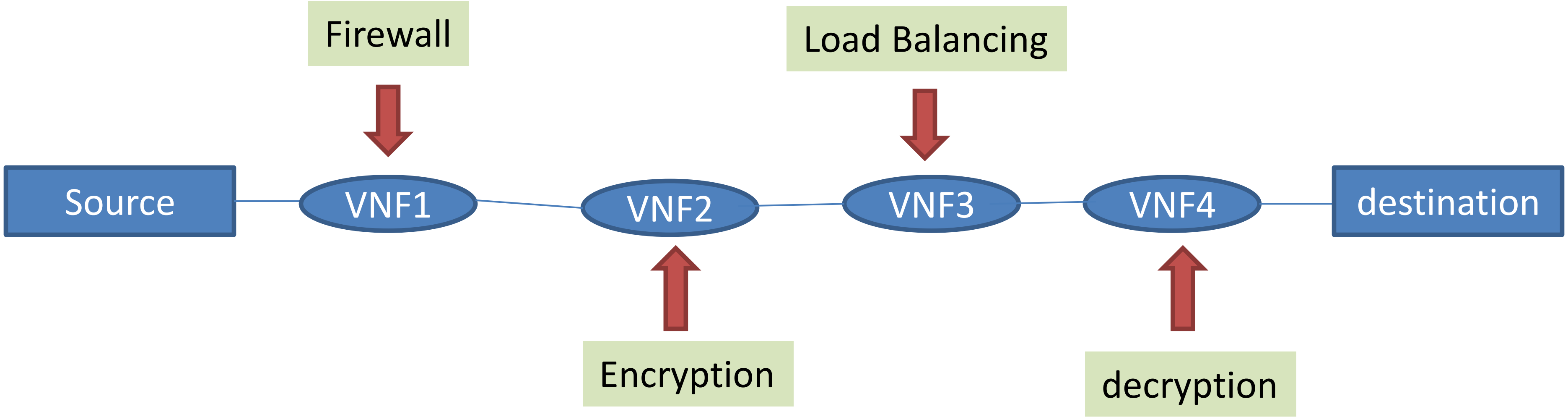
NFV and its connection to IoT and 5G (2/2)

- Within the context of 5G, NFV can be used to separate one physical network into multiple virtual networks
- This is referred to as network slicing. Network slicing will enable organizations to segment networks and cater towards different types of services and customers
- Administrators will be able to manage multiple networks in a format with less latency and more security than ever before

Virtual Network Functions (VNFs)

- A VNF may be for example a DNS service, load balancing, encryption etc.
- SDN and NFV enable the flexible composition of network functions which is known as Network Service Chaining (NSC)

Network Service Chain - Example



Source

VNF1

VNF2

VNF3

VNF4

destination

Firewall

Encryption

Load Balancing

decryption

VNFs Remediation Mechanisms

- VNF Migration
- Load Balancing
- Auto-Scaling

VNF Migration

- the resource migration strategy has to determine which VM should be selected for migration and where it should be deployed

VNF load balancing

- The load balancing aims to eliminate hot-spots in order to improve resource utilization and energy efficiency
- When a VNF gets overloaded, new VNFs are instantiated and the traffic will be shared between the old and the new instances
- The network has to forward the traffic to the old as well as to the new VNF instances

VNF Auto-scaling

- The auto-scaling is the ability to dynamically scale the resources according to the current demand
- Two types of auto-scaling are defined in the literature which are the vertical and horizontal auto-scaling
  - In vertical auto-scaling, the focus is on a single machine to become more (scale-up) or less (scale-down) powerful
  - In horizontal auto-scaling, the focus is on addition (scale-out) or removals (scale-in) of VMs

Putting them all together

- NFV
  - communications abstraction
- SDN
  - Network abstraction
- Cloud
  - compute abstraction

NFV vs SDN

- NFV is used to optimize network services by taking network functions away from hardware.
  - Network functions run at the software level so that provisioning can take place more efficiently.
  - Decouples network services from physical hardware appliances
- SDN separates the control plane from the forwarding plane and provides a top-down perspective of the network infrastructure.
  - With a centralized view of the network, an administrator can make decisions about how switches and routers will handle traffic

NFV and SDN Comparisons in a table

Parameter	NFV	SDN
Type of abstraction	Communications	Network
Architecture for	Network Elements	Network
VNF Relevance	Defines VNFs	Provides connectivity between VNFs
Key focus	Services	Network resources
Optimizes	Network Functions	Network

If you want to relate SDN and NFV to the OSI stack, you can think of it as bottom three layers (layer 1 to layer3) mapped to SDN and the top four layers (layer 4 to layer 7) mapped to NFV