OWASP
Open Web Application Security Project

$ whoami

Almog Ohayon

Co-founder and Chief Product @ Javelin-Networks

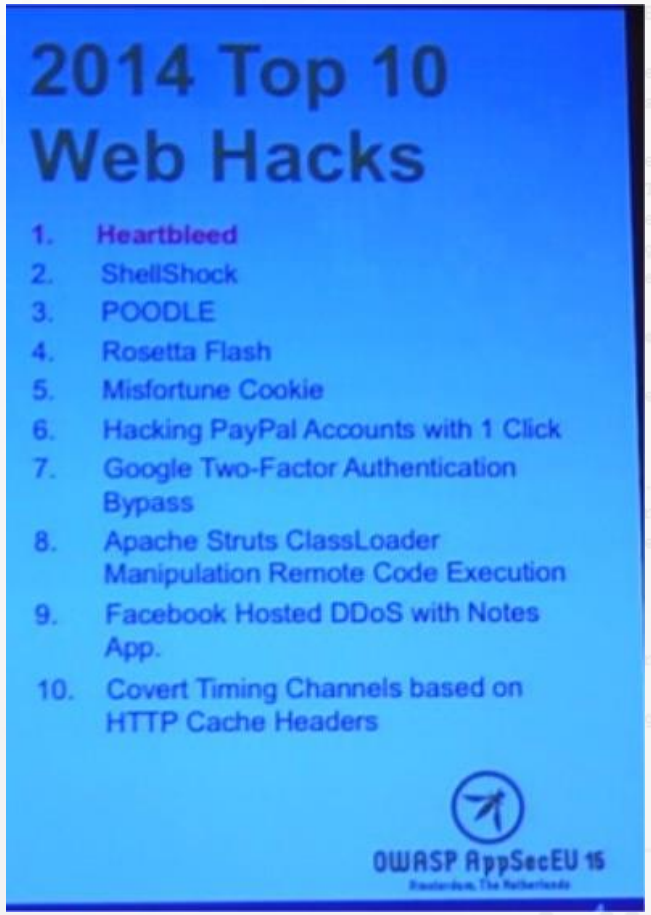
Lots of Certifications
Lots of Hands-on
Lots of Customers
Lots of Lectures
Lots of Hacking

https://twitter.com/md5session
almog@javelin-networks.com

Is it really that bad out there ???

CERT-UK

In 2014 we saw the highest number of reported vulnerabilities (CVEs) ever, reaching 7945. Over 2000 vulnerabilities have been reported in 2015.



Tens of Alexa Top 1,000 Websites Vulnerable to Heartbleed Attacks

Yahoo, Flickr, Imgur and KAT are still vulnerable, experts found

POODLE Attack and SSLv3 Deployment

Good News! Your browser does not support SSLv3.

Emails blamed for Bundestag cyberattack

The cyberattack on Germany's parliament has been traced to a link contained in at least two emails, according to a newspaper report. Parliamentarians left unaware of the breach for three weeks have slammed the delay.

AA FONT SIZE + PRINT AP

OPM Breach Just Put America's Spies 'At High Risk'

JUNE 12, 2015 BY PATRICK TUCKER

Hackers may now have detailed biographical information and a virtual phonebook of virtually every United States intelligence asset. Intelligence

THE DUQU 2.0

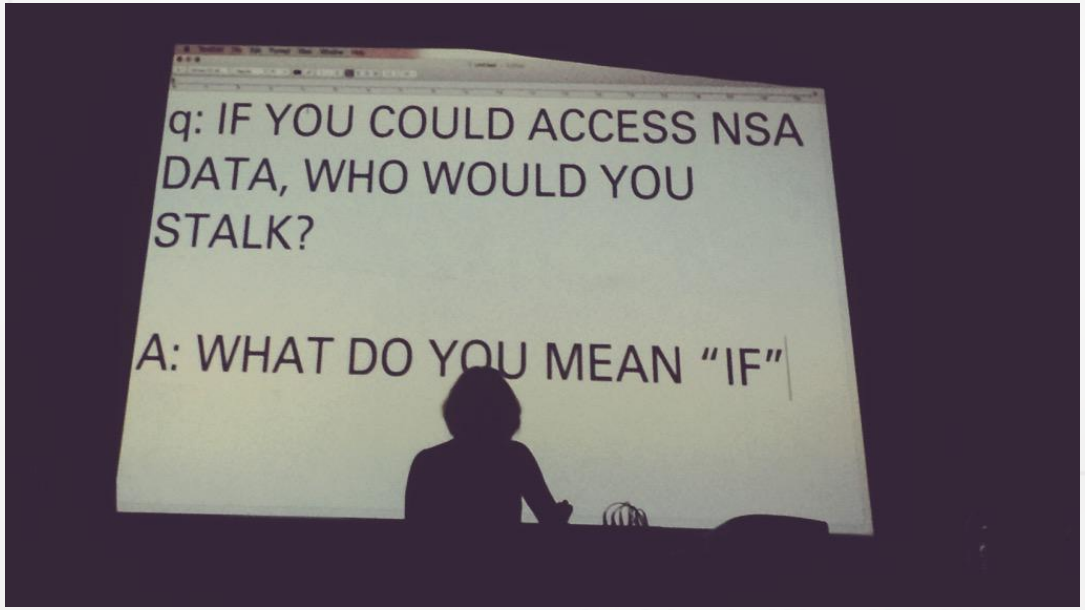
KASPERSKY lab

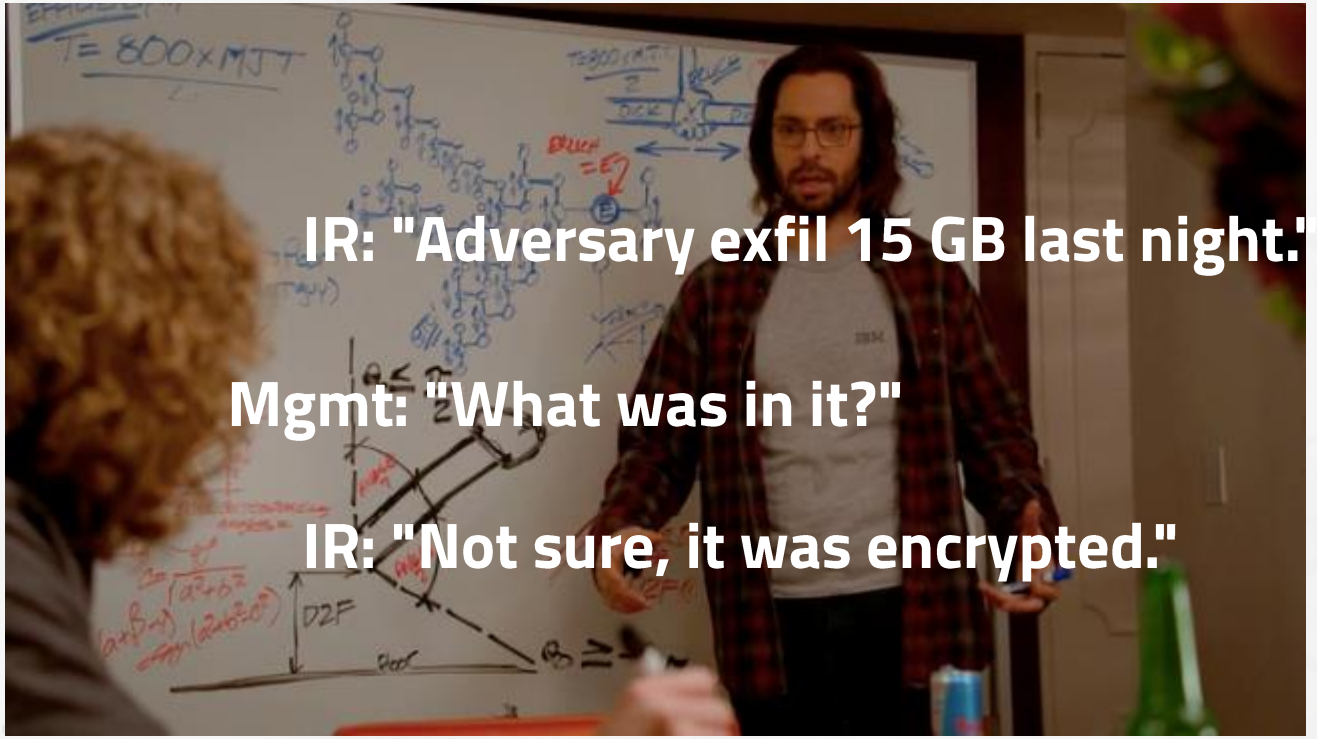
APT28:

A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?

Security Mindset Have Changed
But rarely implemented

- **Zero-Trust**
- **Assume breached**





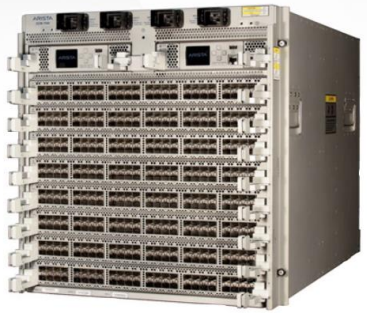
YAHOO!

AppSec is Eating Security

PRESENTED BY **Alex Stamos** | AppSec Cali | January 27, 2015

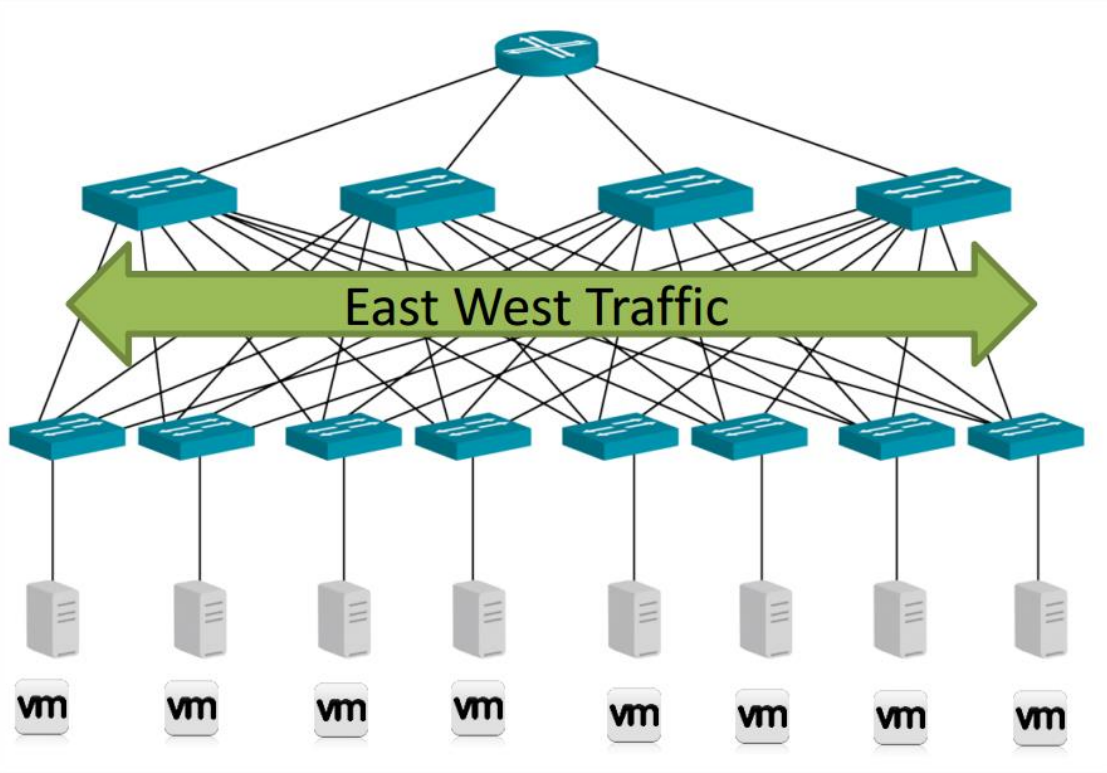
Alex Stamos - Yahoo's CISO and VP of InfoSEC

Security hardware is becoming un-buyable



Arista 7508E
1152 x 10GbE
30Tbps backplane
5kW

Palo Alto 7050
120Gbps throughput
2.4kW



SDN

Compare Search terms

Software-defined networking
Topic

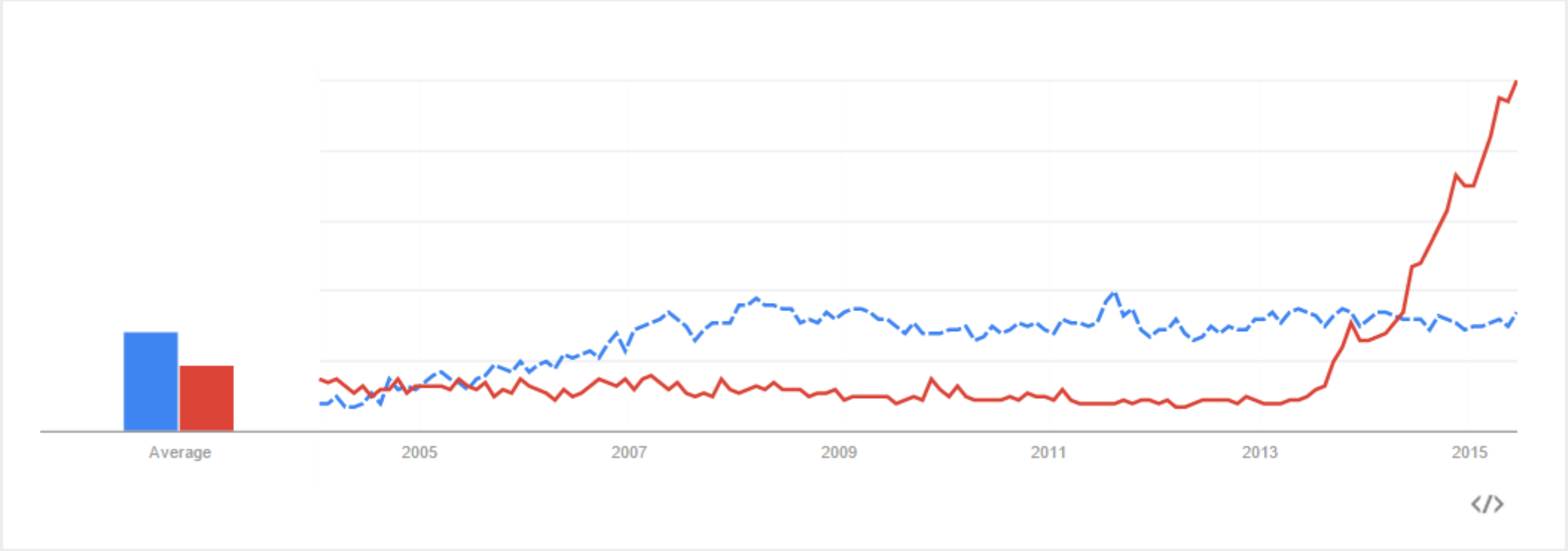
docker
Search term

+ Add term

Beta: Measuring search interest in *topics* is a beta feature which quickly provides accurate measurements of overall search interest. To measure search interest for a specific *query*, select the "search term" option.

Interest over time

News headlines Forecast



Misconceptions

big switch networks

1996

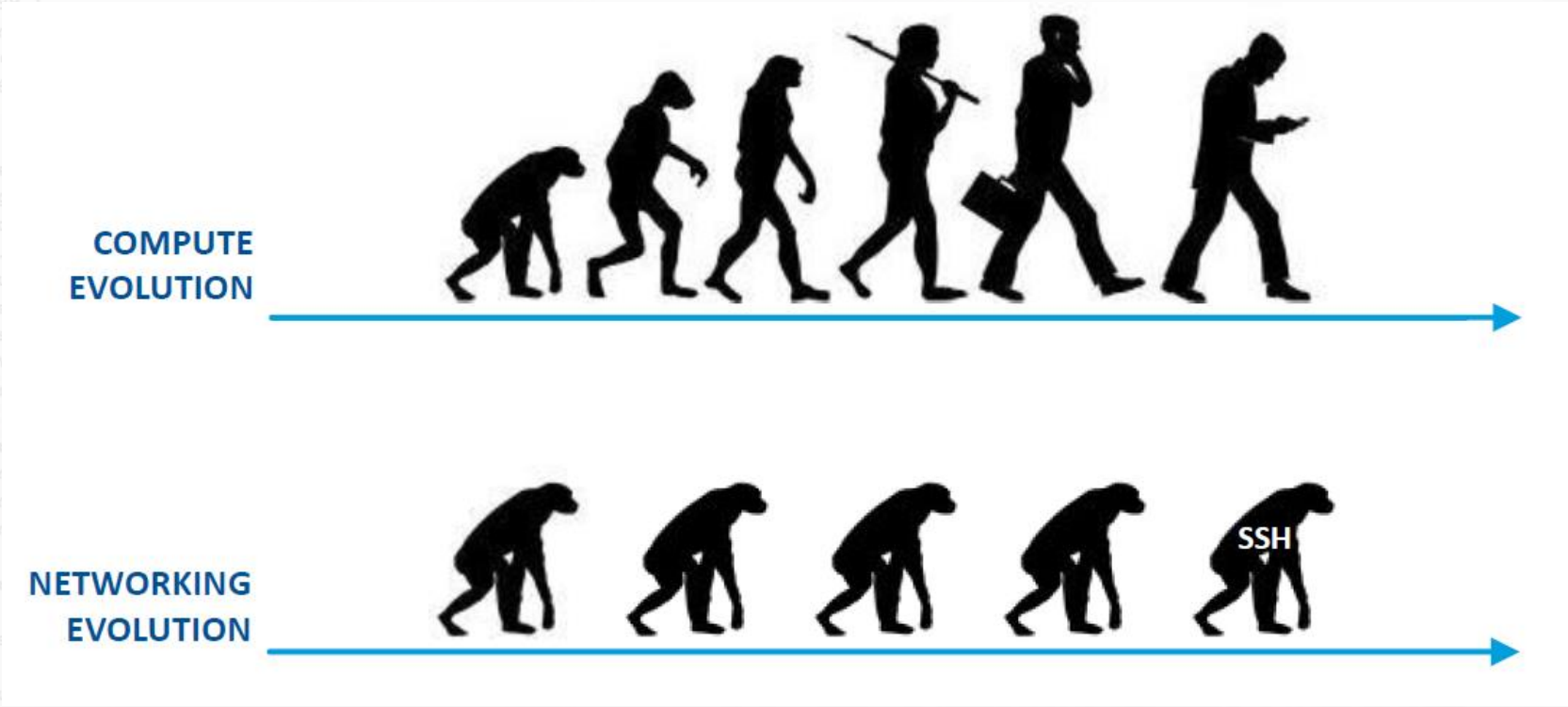
```
Router> enable
Router# configure terminal
Router(config)# enable secret cisco
Router(config)# ip route 0.0.0.0 0.0.0.0 20.2.2.3
Router(config)# interface ethernet0
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface serial0
Router(config-if)# ip address 20.2.2.2 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 20.0.0.0
Router(config-router)# exit
Router(config)# exit
Router# copy running-config startup-config
Router# disable
Router>
```

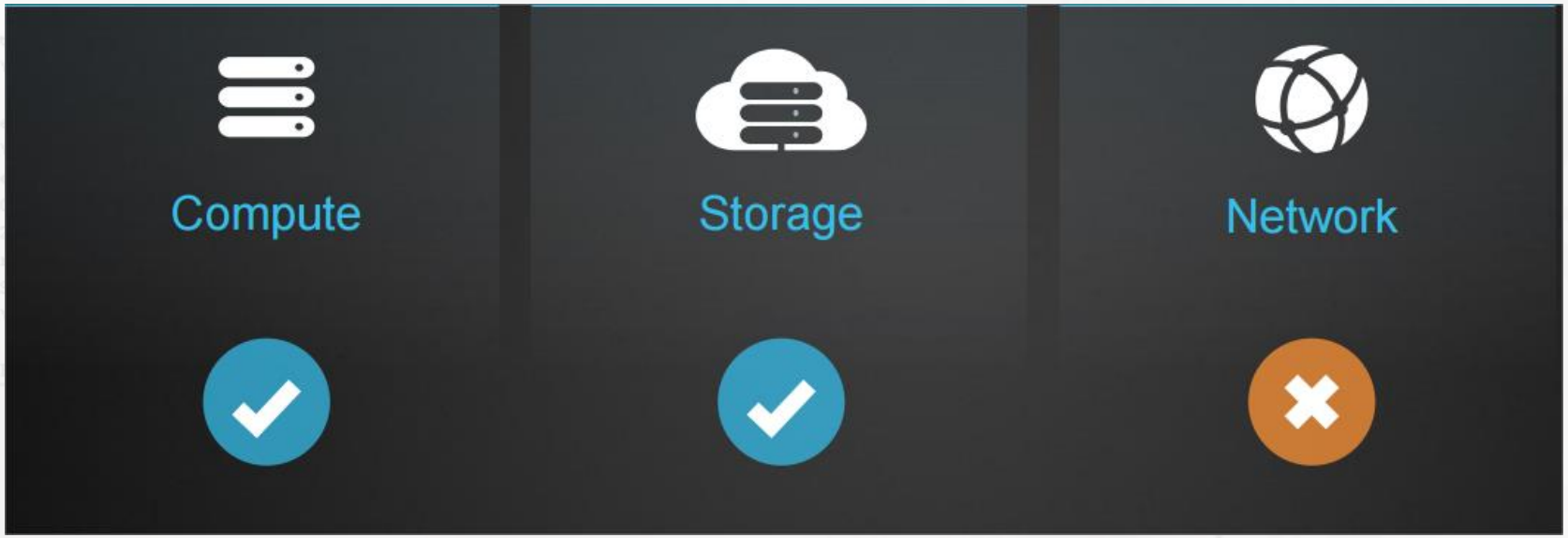
Terminal Protocol: **Telnet**

2013

```
Router> enable
Router# configure terminal
Router(config)# enable secret cisco
Router(config)# ip route 0.0.0.0 0.0.0.0 20.2.2.3
Router(config)# interface ethernet0
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface serial0
Router(config-if)# ip address 20.2.2.2 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 20.0.0.0
Router(config-router)# exit
Router(config)# exit
Router# copy running-config startup-config
Router# disable
Router>
```

Terminal Protocol: **SSH**


COMPUTE
EVOLUTION
NETWORKING
EVOLUTION
SSH


Compute
Storage
Network

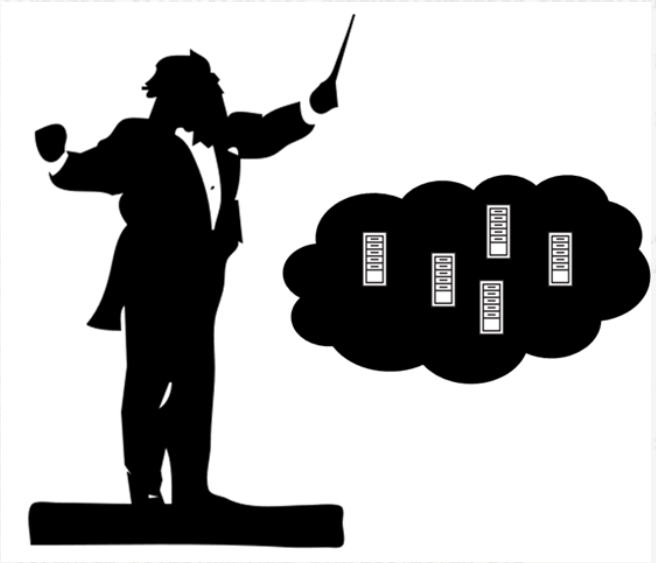
In terms of Deployment SDN is Slightly different for:

- Service Provider
- Data Center
- Enterprise
- Campus networks
- Cloud
- WAN and Metro Links

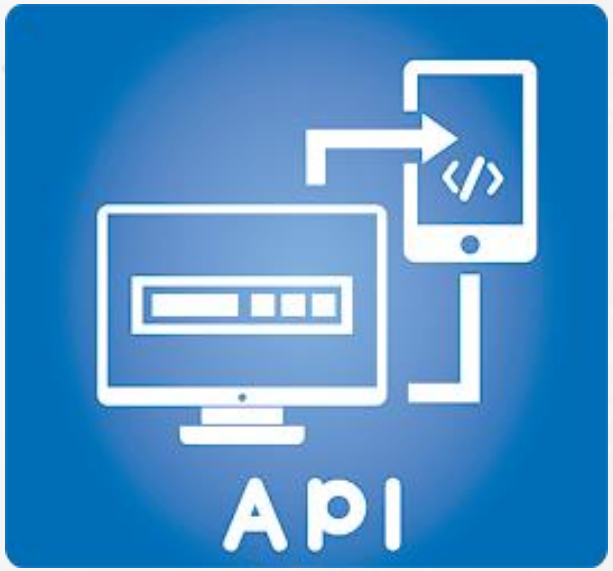
Ok, please tell me what is SDN, Please…

Long story short, SDN is mainly about

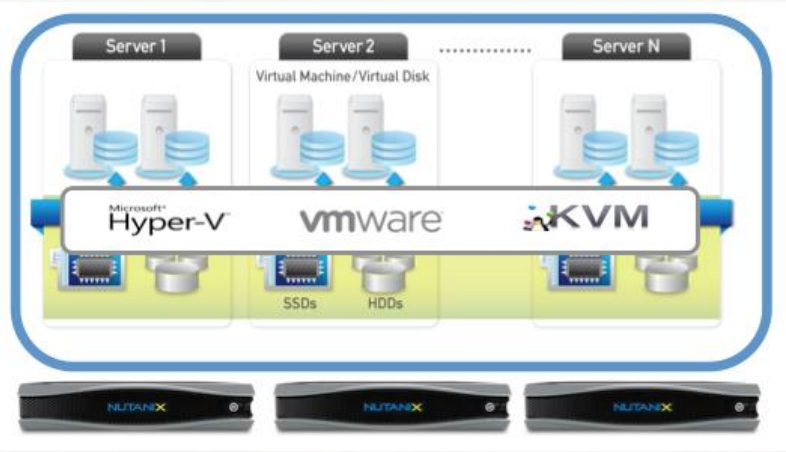
Orchestration



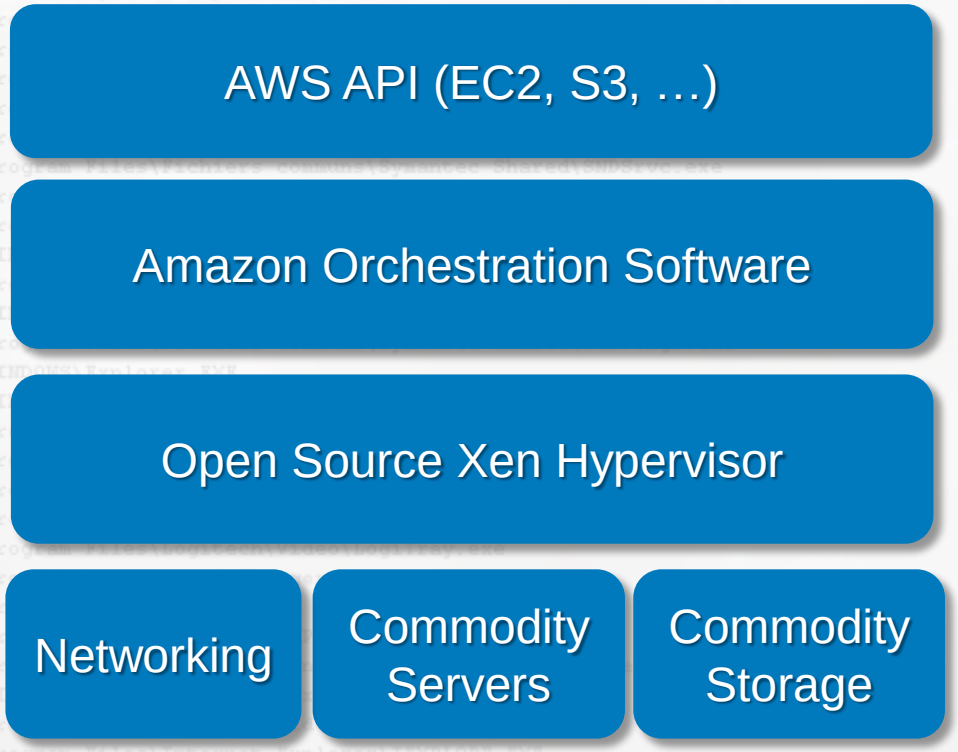
Programmability



Hypervisors



How did Amazon AWS build its cloud?



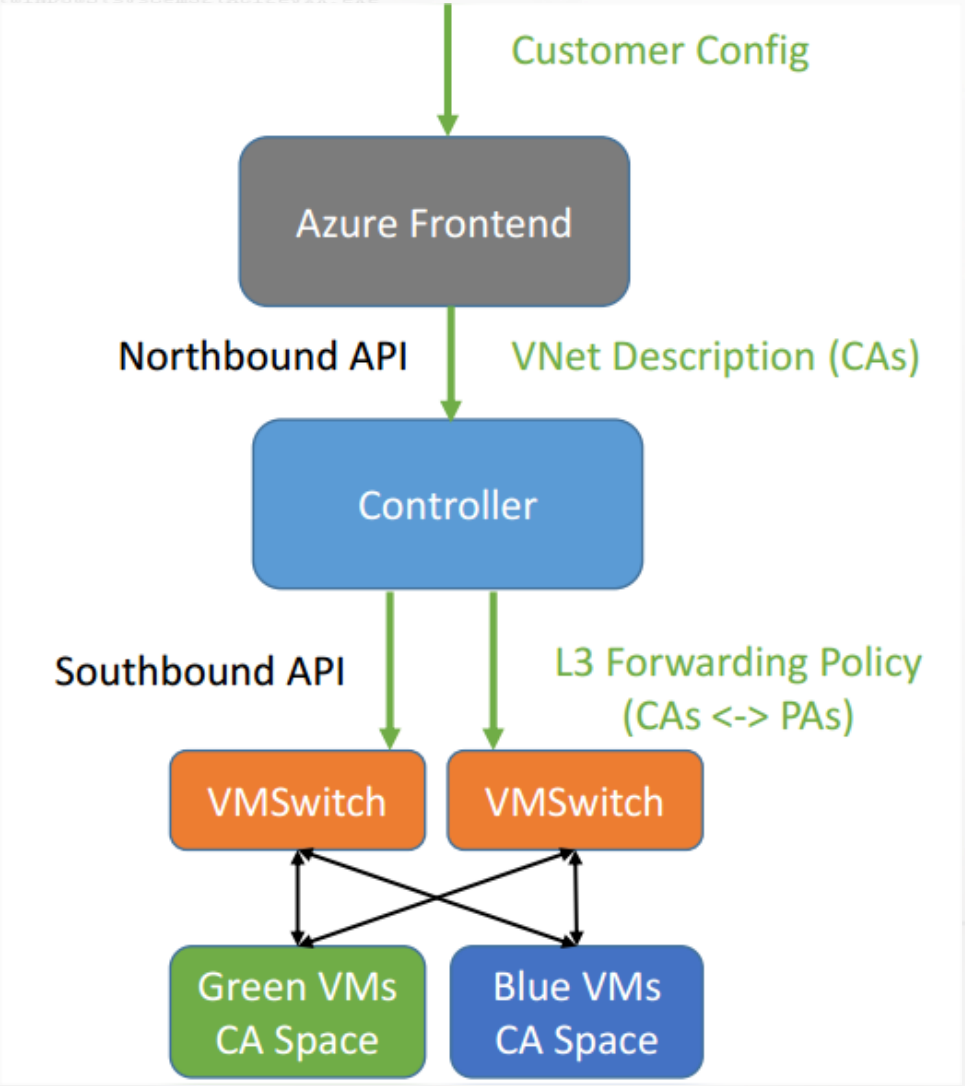
Programmability

Orchestration

Hypervisors

amazon web services™

How Microsoft build its cloud?



Microsoft

How companies can build their SDN network?

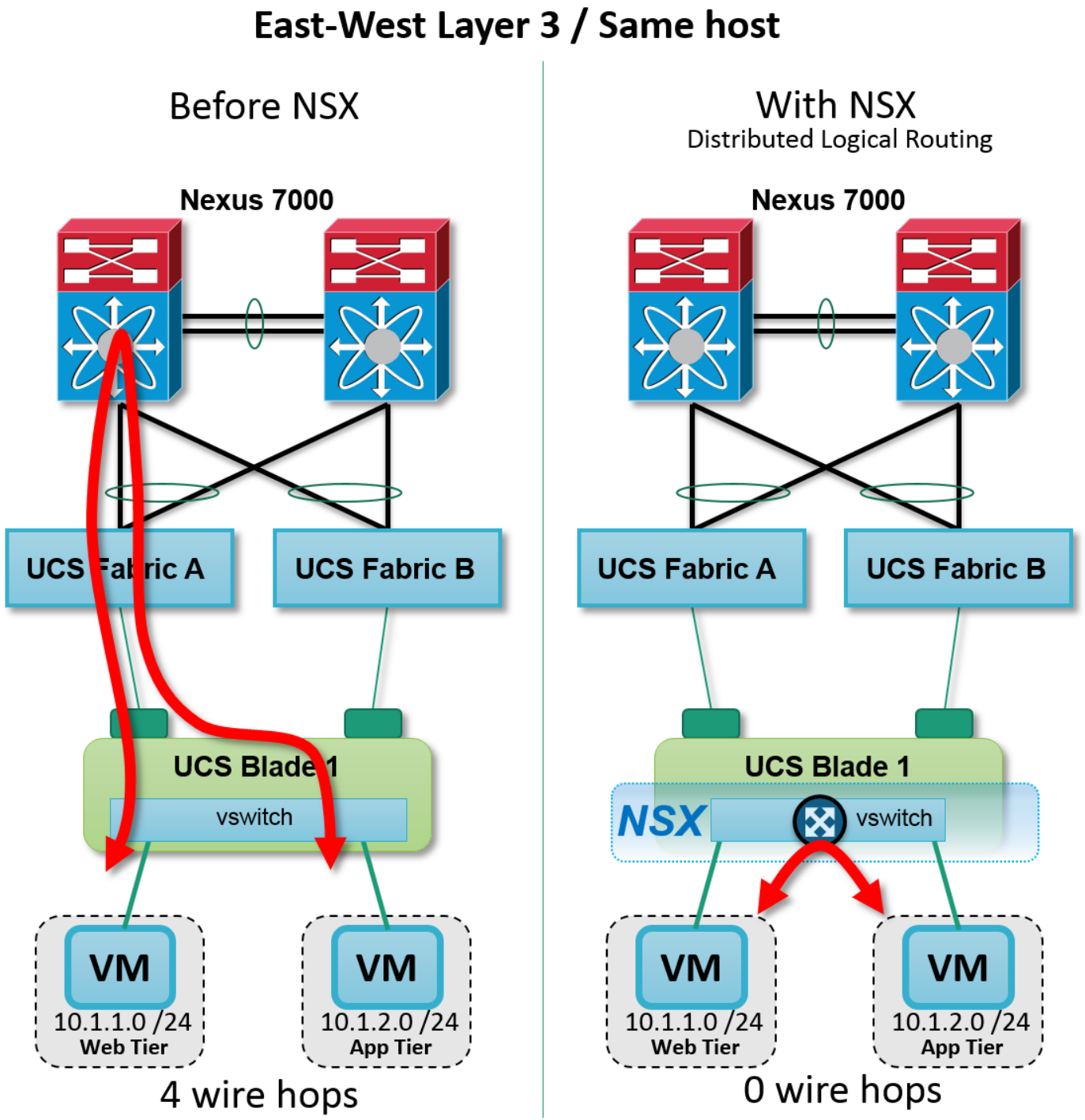
- Vmware NSX
- Openstack
- Cisco ACI
- CloudStack
- Juniper Contrail
- Microsoft azure pack

- There are some more...

Now let's see the magic

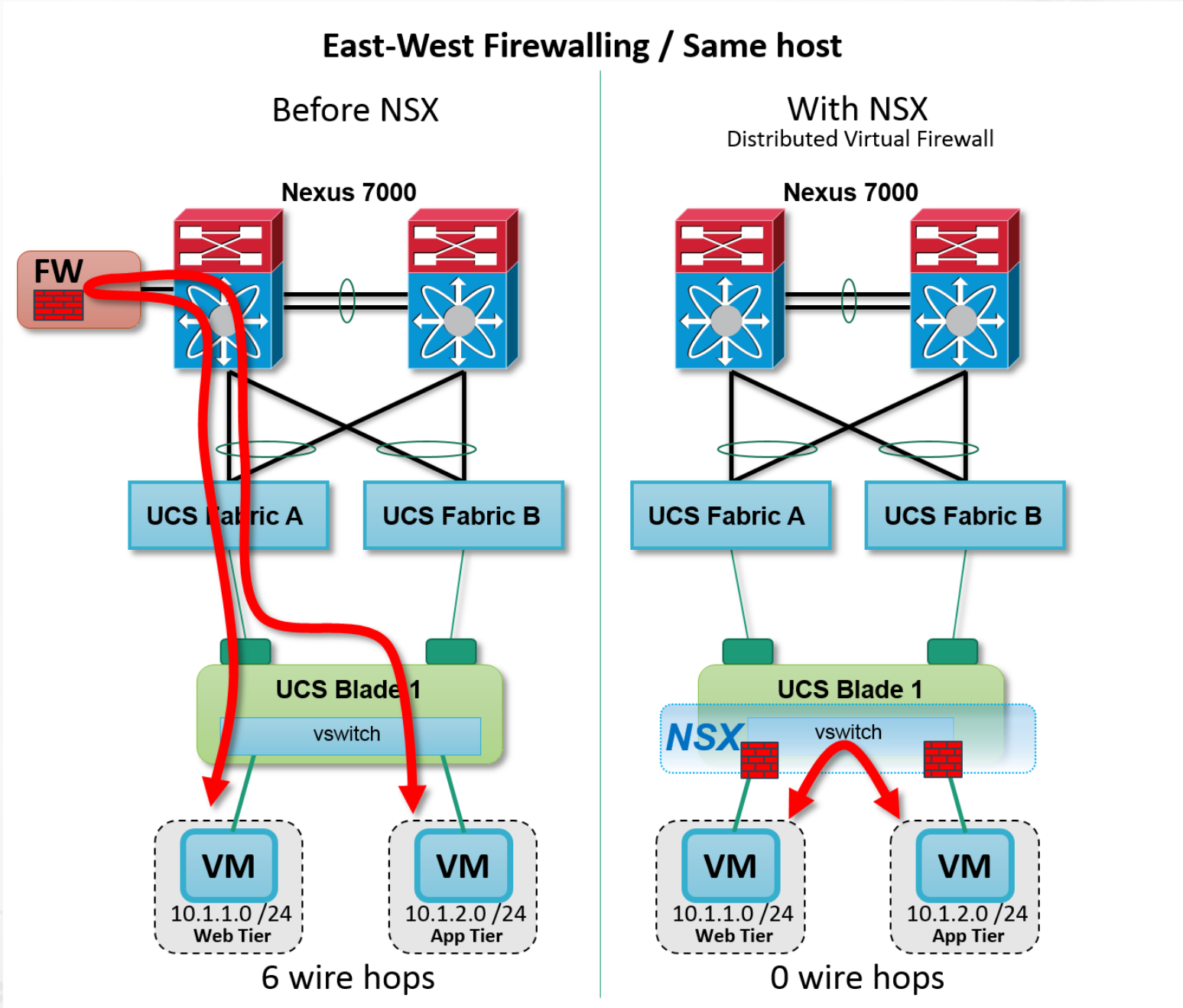
Before/After

SDN



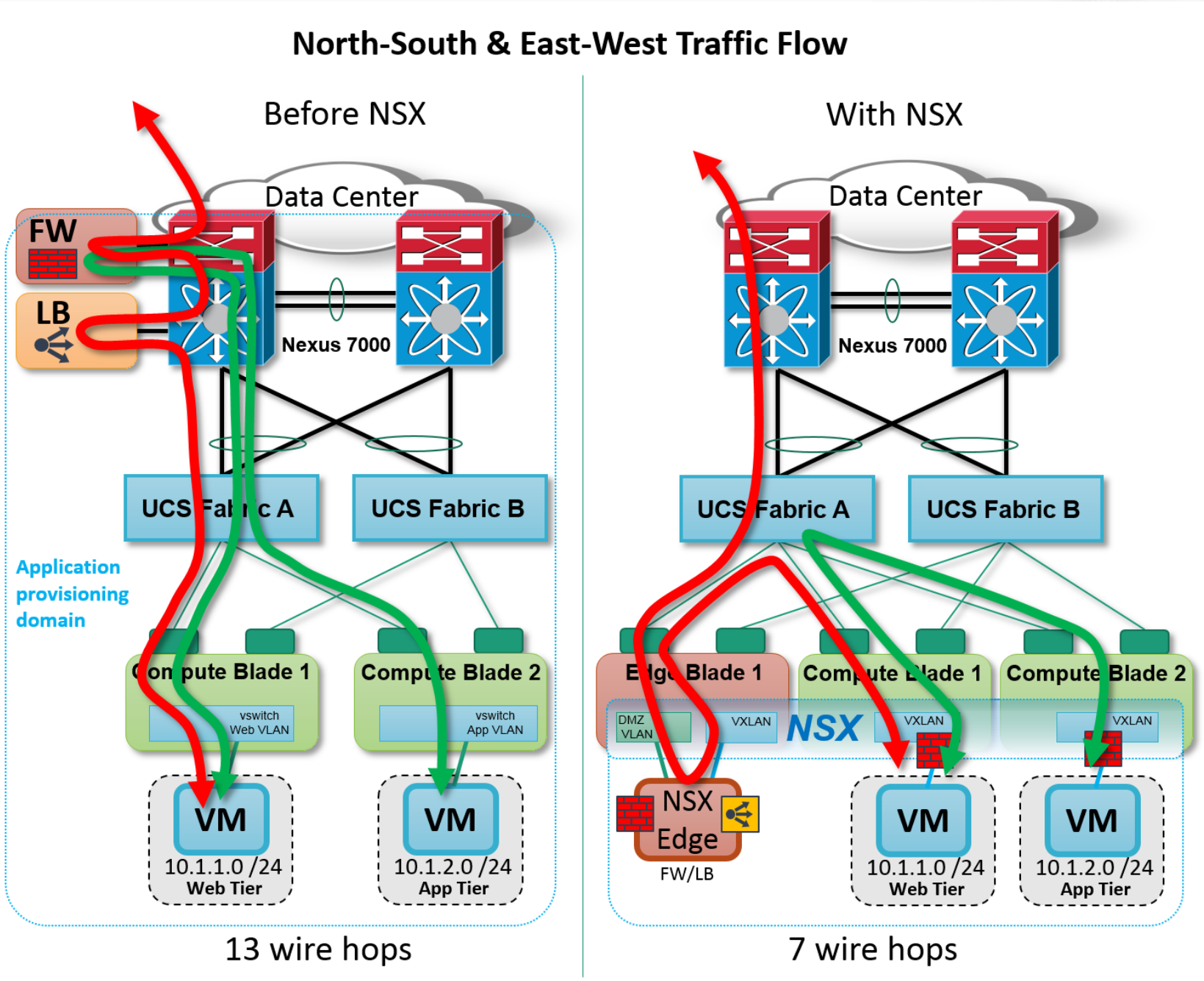
Before/After

SDN

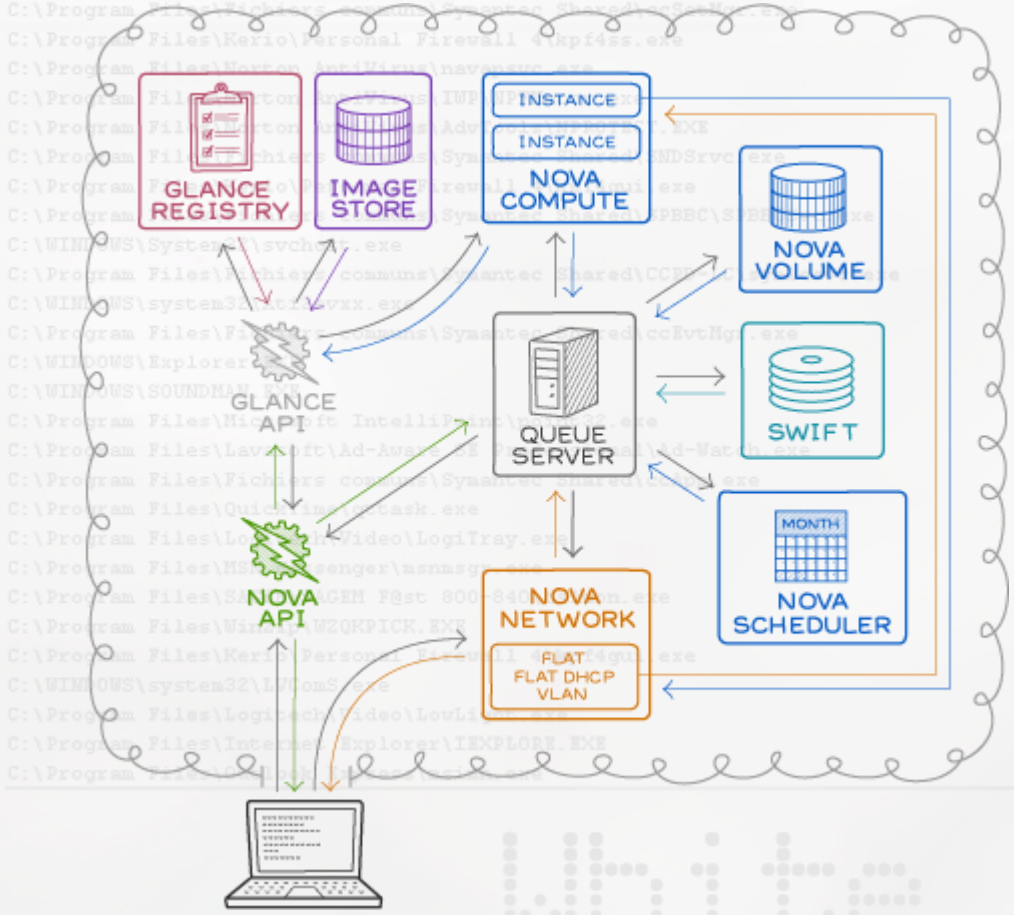


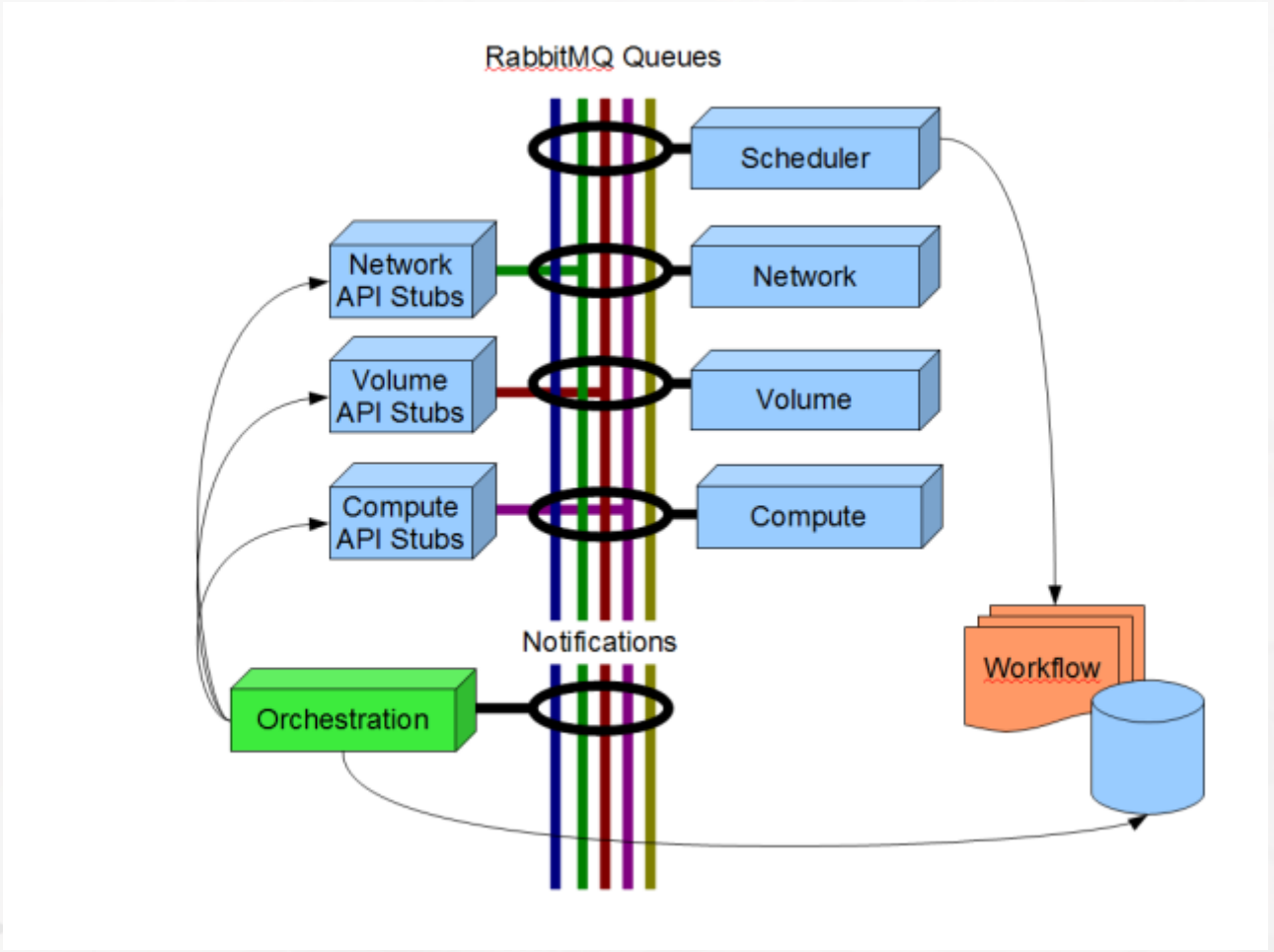
Before/After

SDN



openstack™

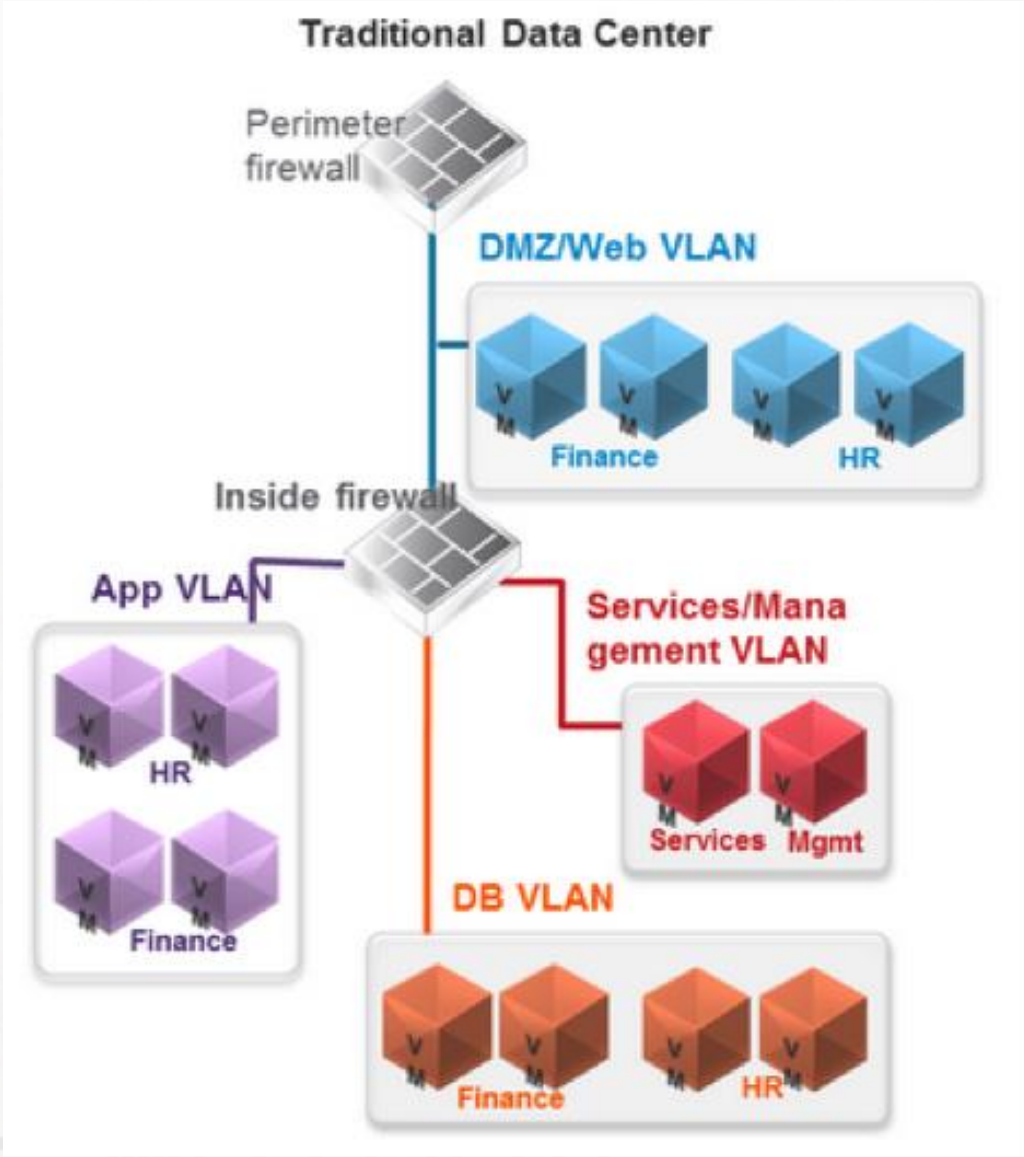

GLANCE REGISTRY
IMAGE STORE
INSTANCE
INSTANCE
NOVA COMPUTE
NOVA VOLUME
GLANCE API
QUEUE SERVER
SWIFT
NOVA API
NOVA NETWORK
FLAT
FLAT DHCP
VLAN
MONTH
NOVA SCHEDULER


RabbitMQ Queues
Scheduler
Network API Stubs
Network
Volume API Stubs
Volume
Compute API Stubs
Compute
Notifications
Orchestration
Workflow

Micro-Segmentation using SDN

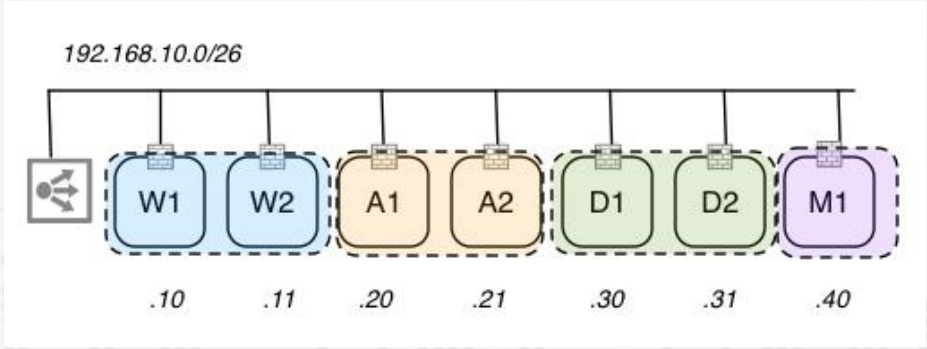
Before SDN

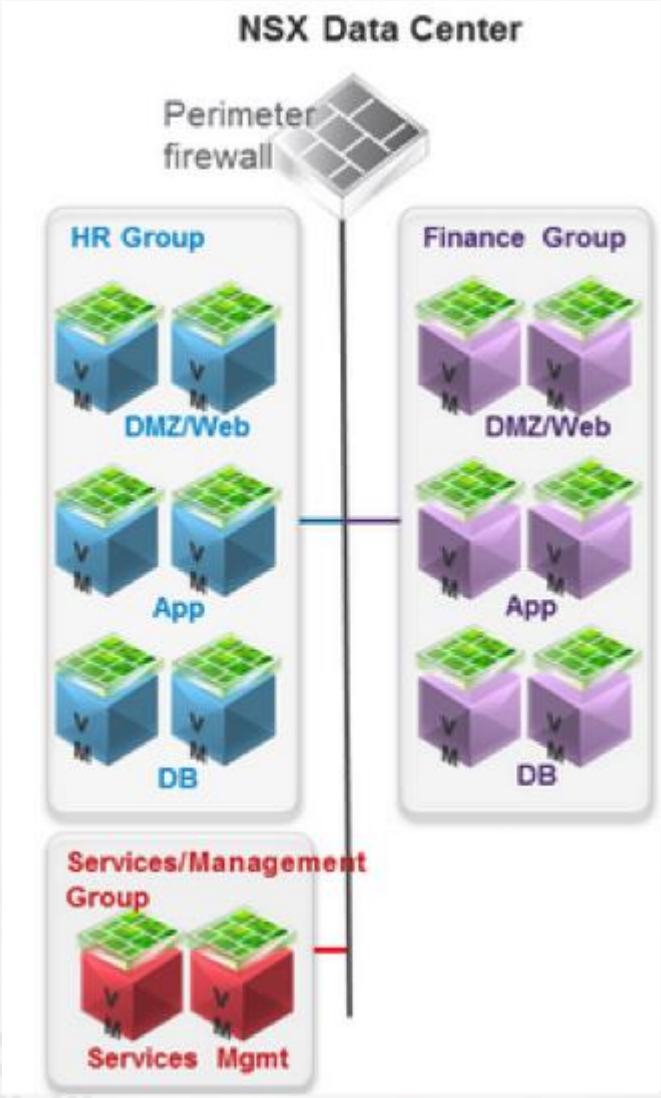
- Vlan oriented
- Choke points
- Unmanageable
- Big attack surface



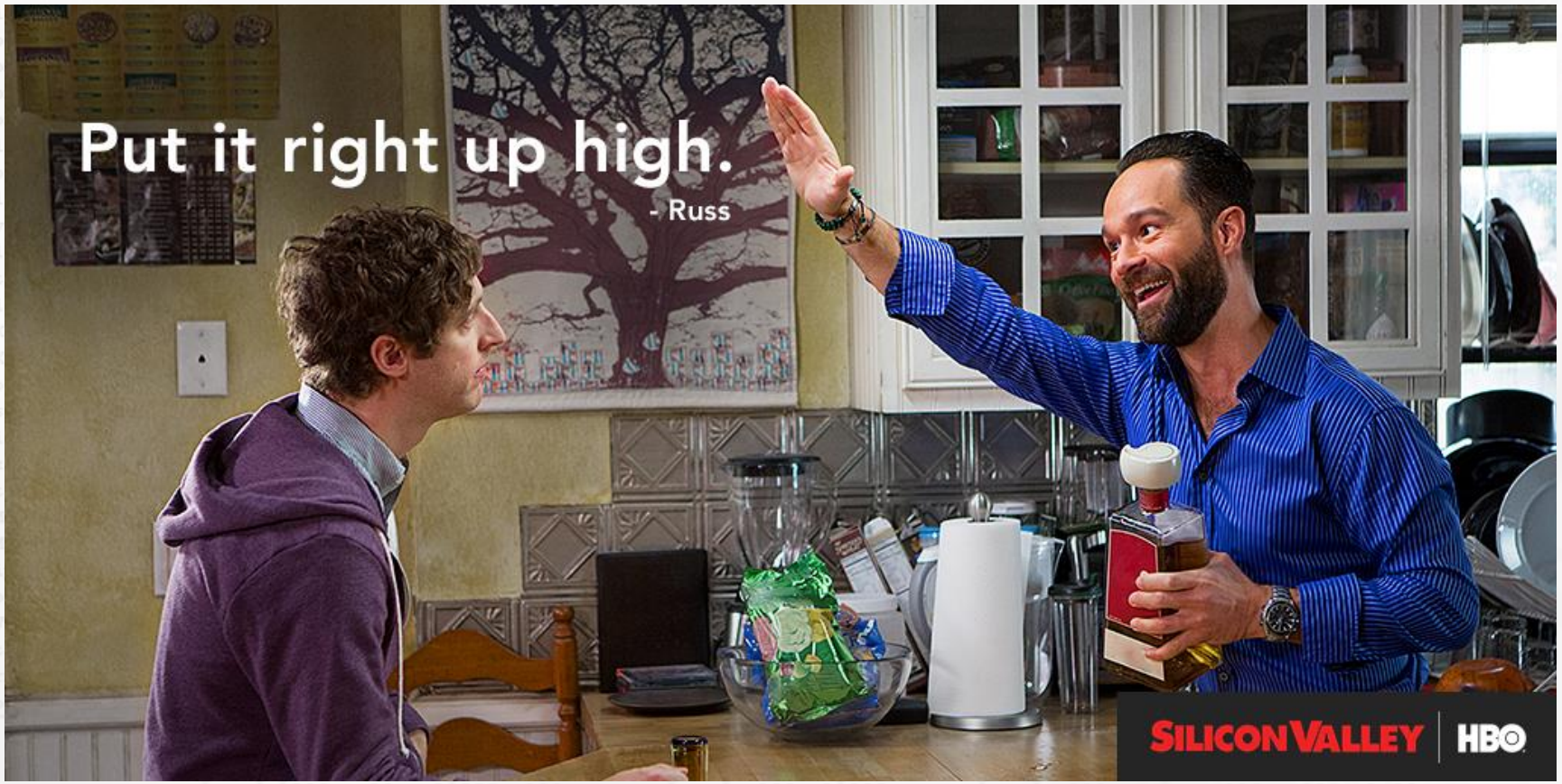
After SDN

- Smaller attack surface, small domains
- Distributed Firewall
- Hypervisor's in-kernel L2/L3/FW
- Simplified deployment



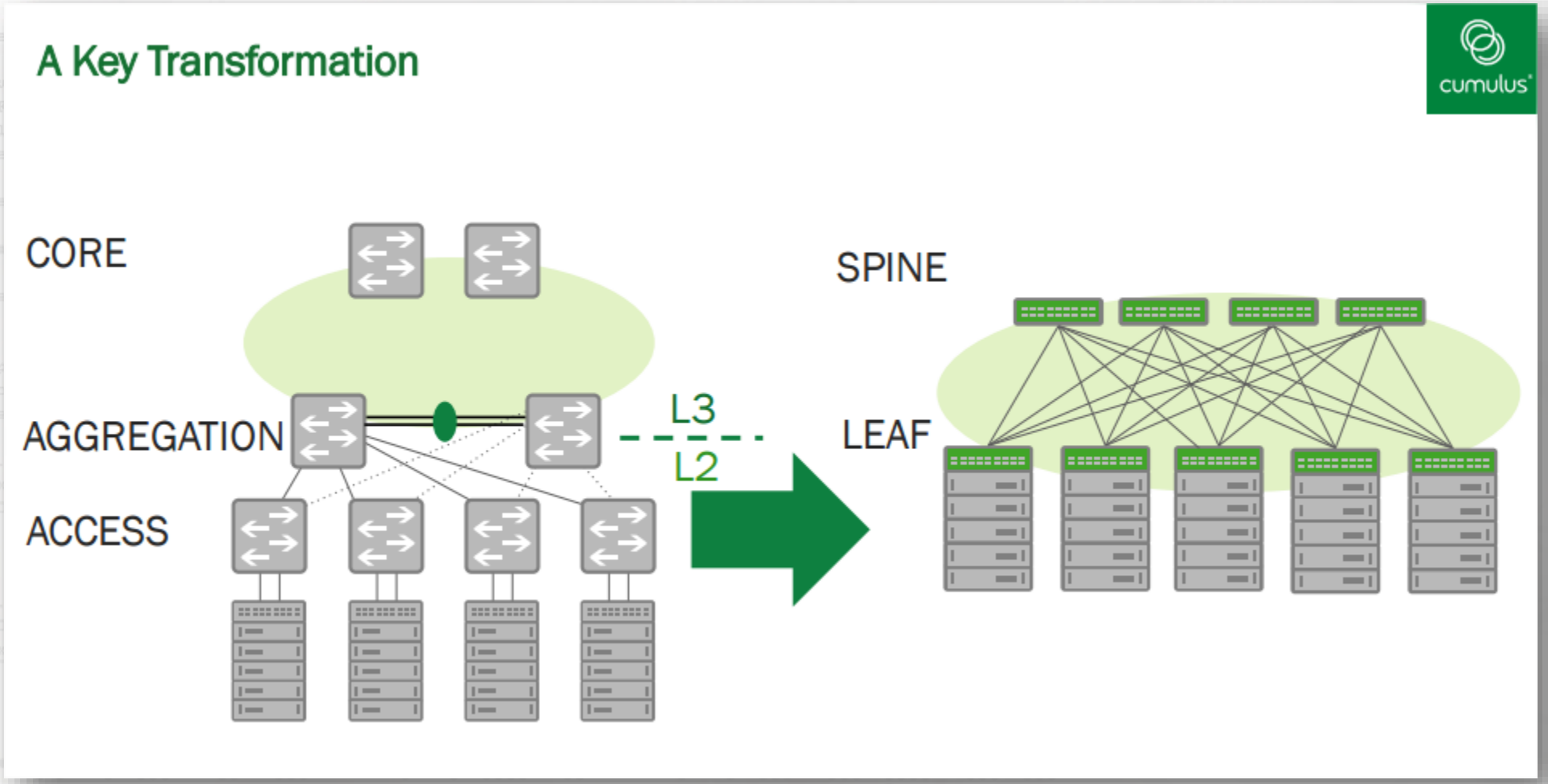


Is it awesome or what ? ;-)

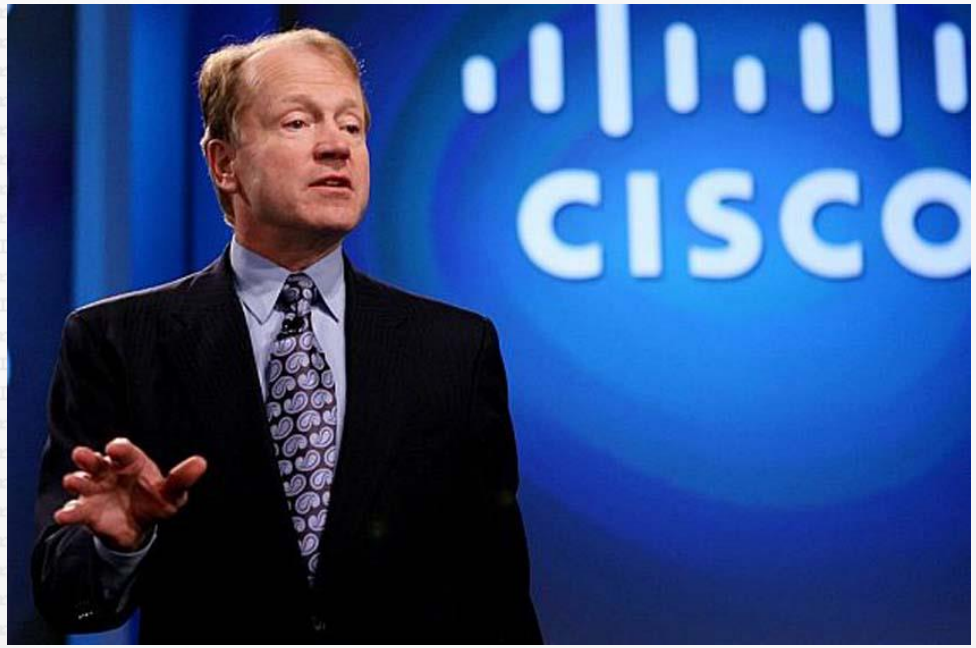


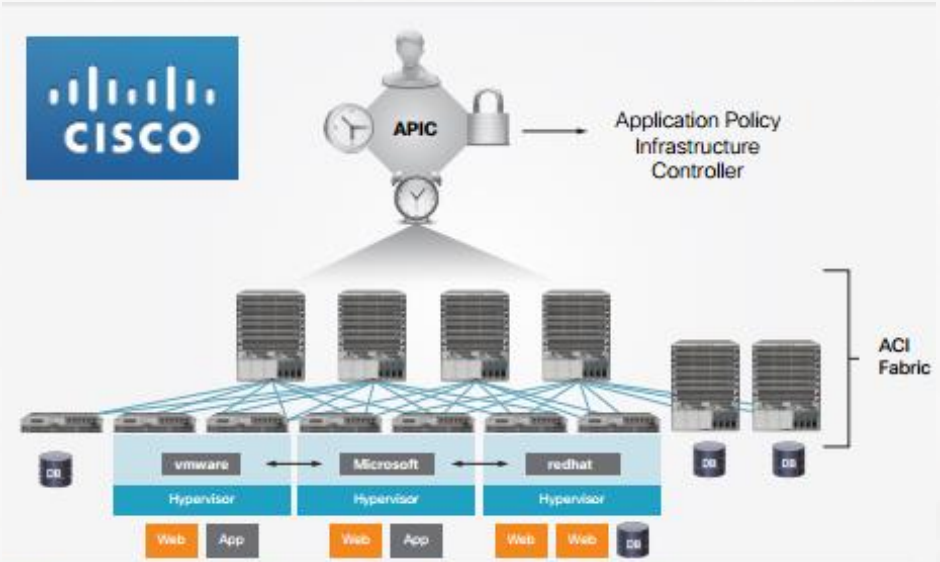
If we have some more time

- **Nobody care anymore about the underlying networking**
- **Hypervisor is the new** **king!!!**



IMHO, biggest loser would be:





Cisco Application Centric Infrastructure

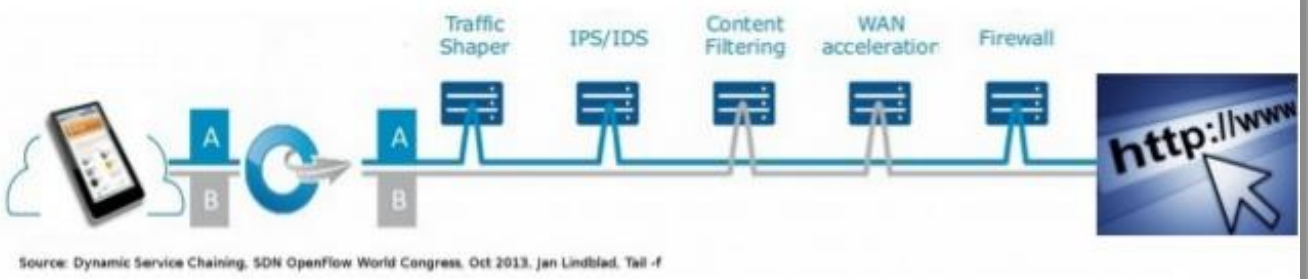
IMHO, biggest winner would be:

- Currently VP, GM & CTO in Vmware
- King of the valley
- Nicira was acquired by VMware for $1.26 billion
- Invented the network virtualization

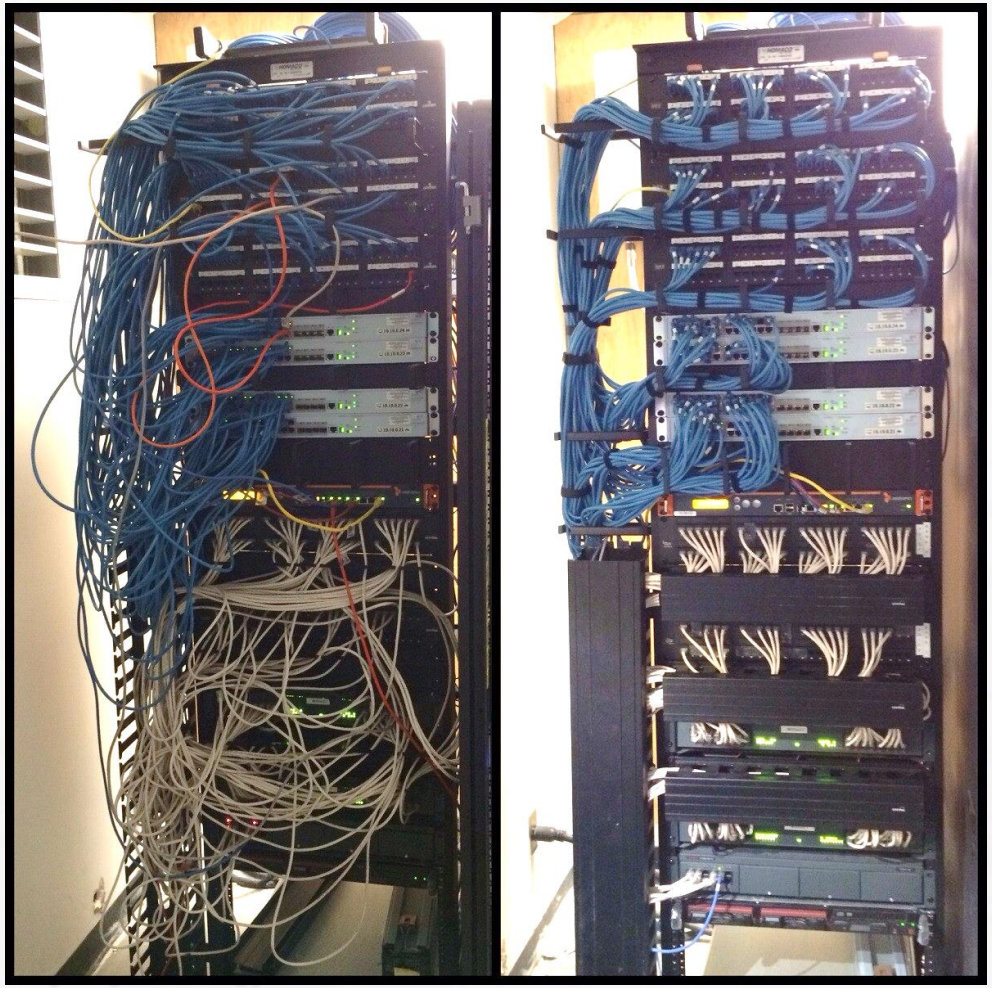
NFV - Network functions virtualization

Service Chaining

Moving network functions into software means that building a service chain no longer requires acquiring hardware.



Source: Dynamic Service Chaining, SDN OpenFlow World Congress, Oct 2013, Jan Lindblad, Tail -f



Business Impact

- Chip hardware - switches, storage, etc..
- Smaller physical space, less hardware
- Less operational guys
- Fast services for end-users
- Pay as you grow

Any Questions ?