# Network Security challenges in a cloud environment – A perspective

Prepared by : Manahil Ahmed Khan

CYBERNET
Total Quality Network

RapidCompute™
A division of CYBERNET

# Introduction

- IaaS Cloud is a collection of multiple enterprise IT
- Significantly complex architectures
- Internet, Storage, LAN traffic

RapidCompute™
A division of CYBERNET

# Introduction

- East West traffic problems

- Scalability & automation issues

RapidCompute™
A division of CYBERNET

# Enterprise IT

- Small workload
  - 5-10 VMs, 2-3 VLANs, single IP space
- Medium workload
  - 10-50 VMs, 5+ VLANs, multiple IP subnets, VPNs
- Large workloads
  - 50+VMs, 10 VLANs, dedicated firewalls, load balancers
  - Distributed DC deployment & L2 interconnects

RapidCompute™
A division of CYBERNET

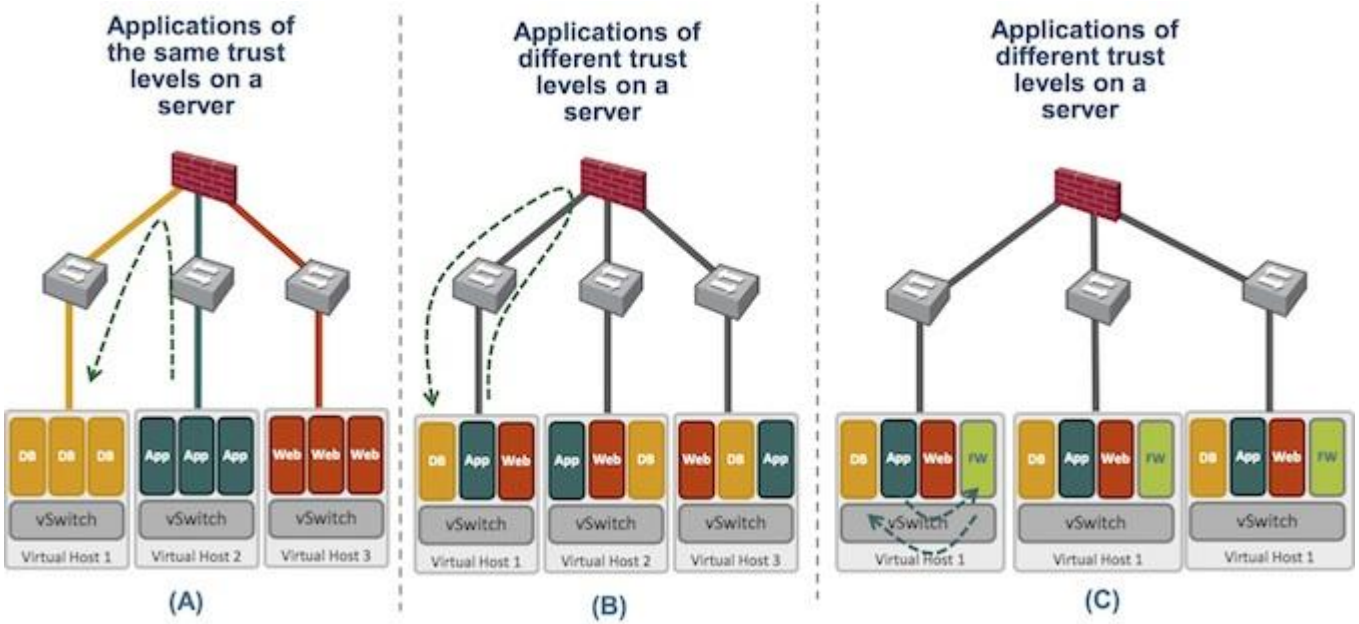
# Traffic inspection in virtualization Layer

- 75% of data center network traffic is East-West

- Nearly all security controls look exclusively at North-South traffic, which is the traffic moving into and out of the data center; 90% of East-West traffic never sees a security control.

RapidCompute™
A division of CYBERNET

# Network Traffic Monitoring




RapidCompute™
A division of CYBERNET

# Virtual firewalls

- Intra host communication
- Physical Firewall vs Virtual Firewall

RapidCompute™
A division of CYBERNET

# Next Generation Firewalls

- Management of firewall clusters.
  - Traffic Flows Increased
  - Expensive design

- Virtual firewall :
  - Design challenge
  - Programming challenge

RapidCompute™
A division of CYBERNET

# 10Gbps Interfaces

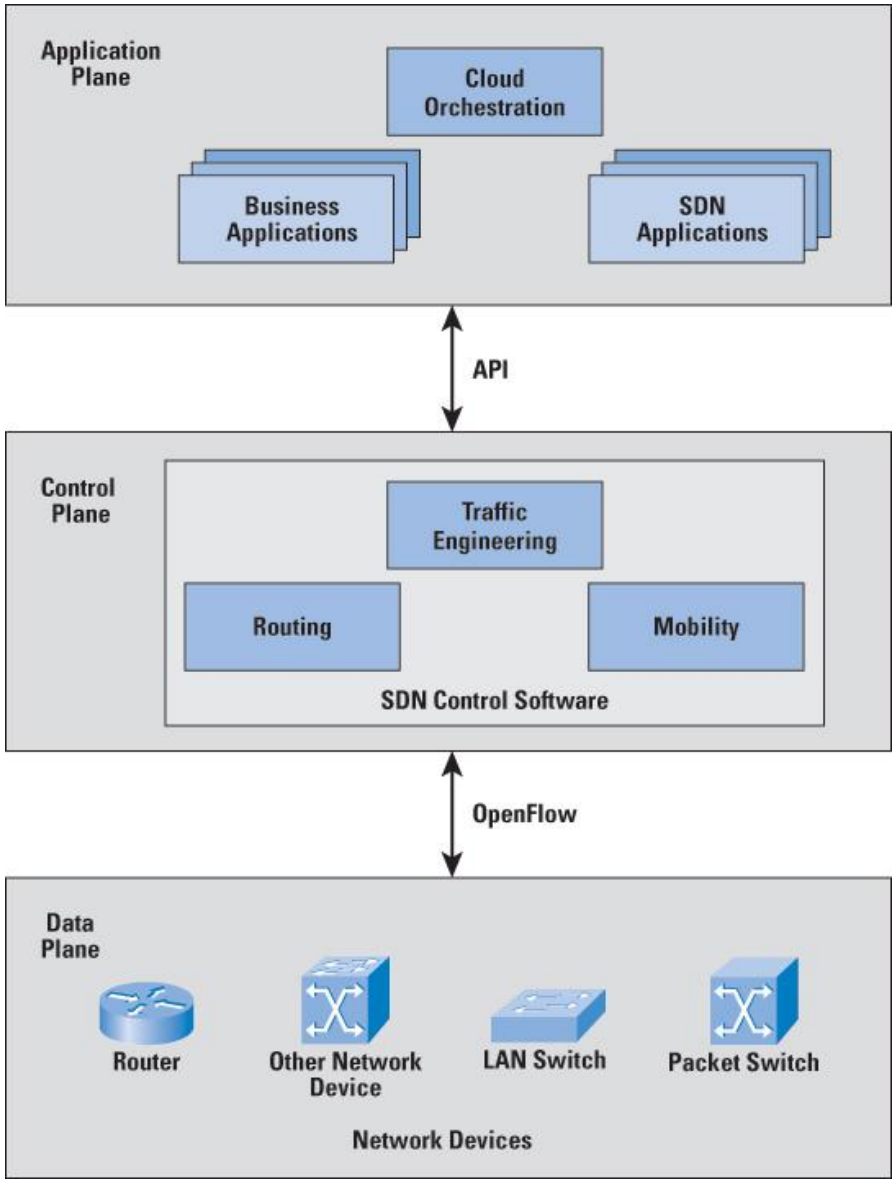
- BUM – Broadcast, unknown and Multicast traffic
- For 20 server  48 x 10Gbps
- Sflow – Network trends monitoring

RapidCompute™
A division of CYBERNET

# Software Defined Networks

- Network control function separated from forwarding function
- New approach to network management.
- Agility and control for network designers.

RapidCompute™
A division of CYBERNET




SDN OVERVIEW

RapidCompute™
A division of CYBERNET

# Bare-metal & white-box switches

- Reduce cost
- Increased flexibility
- Switches has a programmable control panel and data fwd plane
- Bare metal switches can help in monitoring of inter VM traffic, Storage migration/replication and hypervisor communication

RapidCompute™
A division of CYBERNET

# TAPS

- Legal Intercept of traffic
- Monitoring
  - SIEM
  - DLP
  - Flow analysis

RapidCompute™
A division of CYBERNET

# Security Information and Event Management (SIEM)

- Active log management
- Log correlation
- Ticket management
- Vulnerability assessment

RapidCompute™
A division of CYBERNET

# SIEM VENDORS

- HP
- IBM Security
- McAfee
- SPLUNK
- ALIENVAULT
- LOGRHYTHM
- EMC

RapidCompute™
A division of CYBERNET

# Conclusion

- Networking in an IaaS cloud is a new paradigm
- Network engineers should learn programming
- Openflow based switches are the future
- Flow analysis and programming is the key to an agile and self-healing network
- SDN is the key

RapidCompute™
A division of CYBERNET