Network Security challenges in a cloud environment – A perspective

Prepared by: Manahil Ahmed Khan
Introduction

• IaaS Cloud is a collection of multiple enterprise IT

• Significantly complex architectures

• Internet, Storage, LAN traffic
Introduction

• East West traffic problems

• Scalability & automation issues
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
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.
Network Traffic Monitoring
Virtual firewalls

• Intra host communication

• Physical Firewall vs Virtual Firewall
Next Generation Firewalls

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

• Virtual firewall:
  • Design challenge
  • Programming challenge
10Gbps Interfaces

• BUM – Broadcast, unknown and Multicast traffic

• For 20 server  48 x 10Gbps

• Sflow – Network trends monitoring
Software Defined Networks

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

• Legal Intercept of traffic

• Monitoring
  – SIEM
  – DLP
  – Flow analysis
Security Information and Event Management (SIEM)

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

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