

Hybrid is here. Is Security ?

Edy Almer, VP Product, AlgoSec



Trends in the market

- Private Software Defined Cloud



- Open Stack



- Public Cloud



Why Yes ?

- Cost
- Agility
- Pay only for what you use
- Cloud availability (Global, Pan-European)

Why Not ?

- Access Control
- Data Protection
- **Infrastructure Protection and Segmentation**

Security Controls for IaaS

- Host based Firewalls
- Commercial cloud-ready Firewalls
(Firewalls running on cloud provided instances)
- Cloud/Platform provided controls

Host-based Firewalls

- Servers come with open-source, basic firewall (E.g. Linux IP Tables, Windows Host Firewall)
- Set a policy on each image
- Difficult to manage
- Limited functionality
- This method works across cloud providers

Commercial Products

- E.g. Cisco ASA 5500V, Check Point VE, PAN, Fortinet, Juniper, IBM, HP etc.
- Pay by the hour or Bring-Your-Own-Licenses

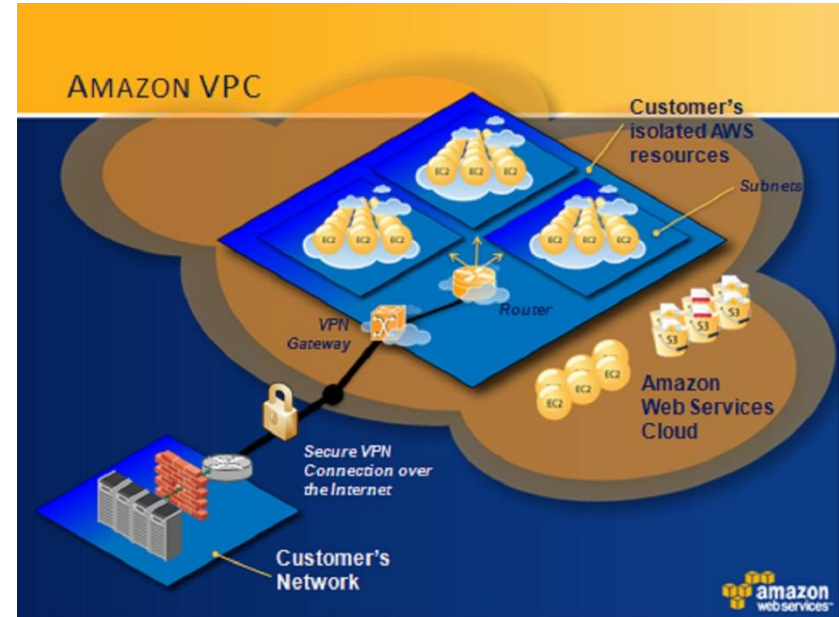
Platform Provided Security Controls

- E.g. AWS Security Groups
- Define what is allowed to/from an instance (similar to firewall rules)
- Assign instances to security groups
- “Magical” (abstracted) enforcement (I.e. no box with blinking lights, no software you can point to)



Amazon VPC

- Virtual Private Circuit – VPN access and private fixed IP addresses
- Most common enterprise configuration
- Similar pricing to EC2



Amazon Security Groups

- Simplifying – no groups, no hierarchy
- Complicating – not IP address based – need to collect all instances to make sense of each IP address, complex dynamic hierarchy

Azure Firewalling

- Rely on 3rd party tools – Sophos & Barracuda
- More partners soon



How to deal with different environment ?

- Support internal users early, and support business
- Only use tools that manage entire deployment E2E
- Ask for support of both Cloud and Legacy devices and topologies
- New applications are easy. Migration is HARD
- Ask for migration tools !

Questions ?

edy.almer@algosec.com

