Protection Is Becoming a Challenge

Multiple reasons why security is a key concern

- **Attackers:** from script kiddies to organized crime and intelligence services
- **Increased sophistication:** advanced persistent threats (APT), bootkit-based threats
- **Disruptive technologies:** control/data plane separation; virtualization; open versus proprietary
NFV: Opportunity or Threat to Network Security?

**Opportunities**
- Immediate activation of security safeguards
- Security analytics
- PaaS and security offload, pooling of security expertise
- Application isolation, micro-segmentation, central control
- Image, patch management

**Challenges**
- Larger attack surface, high-value targets
- Higher system complexity
- Shared resources, common hypervisor
- From proprietary to open protocols
- Out-of-country processing (compliance)

Managed security services is a $20 to $30bn market – KEEP THE BALANCE
Vodafone VPN+ Multi-Vendor Demonstration at Mobile World Congress, February 2016

Use Case 1:
Automated site activation including firewalling

Use Case 2:
Automated scale-in and scale-out

Use Case 3:
DDoS prevention with analytics
Some Attack Vectors

Virtualised Network Functions (VNFs)

- Rogue VNF, noisy neighbor, malicious code
- Backdoor to hypervisor, control software
- Rootkit
- Spoofing, sniffing, MITM

NFV Infrastructure (NFVI)

- Virtual Compute
- Virtual Storage
- Virtual Network
- Virtualisation Layer
- Compute
- Storage
- Network
- Hardware Resources

Management and orchestration

- Compromise remote debugging/test interfaces
- Disgruntled employee
- Increased complexity, human error
- Social engineering
- Customer portal, public APIs e.g. DDoS
- Hypervisor and controller attacks
- Increased complexity, human error
OpenStack Security Controls

- Keystone authentication and token-based authorization
- TLS for accessing APIs
- SSH for VM management / system-level communication; SSH key injection with VM creation
- Multi-tenant capability
- Traffic isolation by VLANs, Linux name spaces, security groups (Neutron, Nova); port/tenant based: address filter, firewall, NAT
- Availability zones
- Sanitization of released storage space
vCPE Use Case – Edge NFV

- OpenStack optimized for DC applications within security perimeter
- vCPE Use case: internal OpenStack interfaces connect over public networks
- End point in untrusted environment (CSP view)
- Present implementations do not provide comprehensive security controls*

Challenges with OpenStack in a distributed compute environment

*Source: NFV Interoperability Evaluation, NIA/EANTC report on LightReading.com; Dec. 2015
A BT Perspective:
Securing Openstack Over the Internet

Challenge 5: Securing Openstack over the Internet

- We connected a compute node over the Internet to a controller in our NFV Lab
- Over 500 pin holes had to be opened in the firewall to allow this to work
  - Includes ports for VNC and SSH for CLIs.
- Firewall had to be reconfigured every time the compute node’s dynamic IP address changed.
  - Which it did several times during testing.
- It is a realistic scenario for the vBranch.
- Openstack’s design presents too many attack vectors.

Source: “How NFV is different from Cloud: Using Openstack for Distributed NFV”, Peter Willis, BT; SDN and OF World Congress, Düsseldorf, Oct 2015.
Risk Mitigation in Edge NFV

Risk mitigation with OpenStack security controls

Security appliances such as IDS/IPS, firewalls but also service assurance functions

Security additions to DPDK e.g. experimental Crypto API (Release 2.2), keep alive signaling, new performance management functions

Encryption per virtual connections and/or bulk encryption

Trusted platform module, hardware security modules for secure boot, key integrity

Lower layer encryption becomes essential security control
Security Assurance in Edge NFV

- COTS Server
  - Open OS/Hyperv.
  - X86 Server

- OpenStack in box
  - perf. assurance
  - hardened SW/HW

- Open OS/Hyperv.
  - X86 Server

- Hybrid Server
  - FSP 150 ProVM
  - tamper resistant
  - HW acceleration
  - HW encryption
  - perf. assurance
  - hardened SW/HW
  - Open OS/Hyperv.
  - X86 Server

assurance level

functionality
Security Work of Selected Standard Bodies and Industry Alliances

- ETSI NFV ISG: “NFV Security; Problem Statement”, ETSI GS NFV-SEC 001, October 2014 + SEC 00x releases in 2015
- OpenStack Foundation: “OpenStack Security Guide”; best practices and implementation guide for securing an OpenStack implementation
- ONOS: Security response process, security emergency team
- OPNFV security-related projects such as Moon, Barbican

Standard bodies and industry alliances focus on security
Securing Edge NFV Devices

- OpenStack in distributed compute environments calls for additional security controls
- Defense in depth for mitigating attack surface in NFV-centric networks
- Pure-player software and hybrid edge NFV devices for different levels of security assurance

ADVA Optical Networking - your expert in edge NFV
Thank You