Open Security Controller - Security Orchestration for OpenStack

Tarun Viswanathan
Platform Solution Architect
Intel

Manish Dave
Platform Architect
Intel
Notices and Disclaimers

- Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

- No computer system can be absolutely secure.

- Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

- Intel, the Intel logo and others are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others.

- © 2016 Intel Corporation.
SDI—The Application Defines the System

- **The evolution to software-defined infrastructure**

  - **One application per system**
    - Static perimeter-focused security hardware appliances
  - **One application per virtual system**
    - Partially automated security physical/virtual appliances
  - **Applications define the system**
    - Fully automated software-defined security

  - **TRADITIONAL HARDWARE**
    - Compute
    - Network
    - Storage
  - **ABSTRACTING THE HARDWARE**
    - Applications
      - VM Manager
  - **ABSTRACTING THE DATA CENTER**
    - Storage
    - Compute
    - Network
    - Resource pool
Enterprise Multi Cloud Security Challenges

How can I provide consistent security across a multi cloud data center environment.

Open Security Controller addresses this challenge.
Open Security Controller Key Design Goals

- **Centralized security policy management** for a multi-cloud environment.
- **Automated provisioning, distribution, and delivery** of security inside data center perimeter.
- **Dynamic scale-out Security VNFs**
- **No Lock-in** Vendor agnostic open solution
- **Policies aligned** with specific application workloads
- **Separation of duties** to enable use of familiar tools
Orchestrating security policies with network provisioning across multiple virtual environments

- **Security Function Manager**: Centralized management and separation of duties
  - Virtualized Security Function Manager
  - Security Management
  - Physical Security Appliances

- **Security Controller**: Security service automation and orchestration
  - Security Functions Catalog
  - Security Controller
  - vIPS, vNGFW, vWAF, vADC
  - Distributed Virtual Appliances

- **Virtualization Infrastructure Management**: Abstracts compute, storage, and network
  - SDN
    - OpenStack*
  - SDN
    - Kubernetes*
  - MANO
    - OpenStack*
  - Network virt.
  - Compute virt.
OpenStack* Micro-Segmentation Use Case

- Advanced threat protection for East-West traffic flows
OSC API Interaction Model

- Applications, User Intent, and Policies
- Cloud Apps
- User Intent
- Policies

Open Security Controller

- Security Functions Catalog
- Manager Plug-ins
- VNF Agent Plug-ins
- H2 Database

User Interface

- Business Logic
- Service Dispatcher
- Jobs Engine

Security Function/Element Managers

- IPS Managers
- NGFW Managers
- ADC Managers

Open Security Controller Manager

- Policy interface
- User intent
- Application intent

SDN Controllers

- NSX*
- Nuage*
- Midokura*
- Brocade*
- VSP*

Virtual Infra

- OpenStack*
- Virtual Compute
- Virtual Storage
- Virtual Network

Virtualization Layer

- Physical Infrastructure
- Computing Hardware
- Storage Layer
- Network Hardware

Rest API

- Web Sockets
- REST API IPC
- REST API Images, deployment, notifications, authentication

- Dynamic policy updates and mapping
- Domain/sub domain updates and mapping
- Control path agent: provisioning, de-provisioning, heartbeats, etc.
- Data path agent: instrumentation and real time statistics

- Policy interface
- User intent
- Application intent
- Traffic redirection API
- SFC policy API
- Advanced visibility functionality (example 6 tuple visibility)
- Lifecycle management
- Deployment specs, auto-scaling and HA
- Authentication
- Image services
- Notification for events
- Role based access control
Customer PoC: Health industry IT services provider

- Customer has to adhere to HIPAA regulatory requirements
- Existing solution was based on DC edge devices.
- Customer wanted to get to a dynamic policy based security solution for East-West traffic inspection.
Customer Deployment Architecture

Current: Topology Based Security
- Physical Appliances
  - Firewall
  - Intrusion Prevention Systems/Intrusion Detection Systems
  - Application Delivery Controller
  - Top of Rack Switch
  - X86 Server
- East-west Traffic
- High Latency

Future: Dynamic Policy Based East-West Security
- Security Function Manager
- SDN Controller
- Security Controller
- Top of Rack Switch
- East-west Traffic
- Security between Tenants and Tiers
- Latency Goes Down
- Granular Control and Scalability

- X86 server
- vIPS
- vADC
- App
- App
- App
- App
Customer PoC: Large financial services provider

- Customer has to adhere to PCI regulatory requirements
- Customer wanted to get to a Risk Based automated security policy management capability for their OpenStack environment
## Customer deployment Workflow

### One Time Setup
1. Openstack Connector
2. Create Security Services
   a) Policy manager Plugins for NGFW 1, NGFW 2
3. Configure Security Services
   a) Distributed Appliance
   b) Deployment Specifications

### Protection Policy
1. Define Global Risk based Sec-Groups
2. All Policy managers dynamically updated
3. Automated traffic redirection via SDN Plugin

### Automated Zero-Trust Security
Spins workload up or down
Network flows automatically updated to redirect traffic to security service chain

Security Admin

Dev-Ops
DEMO

Automated Security Services Orchestration for Openstack
Demo Topology

- Open Security Controller
- Security Manager Plugins
- NGFW Manager
- Security Management
- OpenStack® Controller
- SDN Plugin
- Virtualization Connector
- Attacker VM
- Protected Web VM
- SDN Controller
- OpenStack Compute Node
Apply: Risk Based Approach

1. Identify workload which needs micro segmentation
2. Identify security controls to mitigate risks (vIPS, vNGFW, vADC)
3. Automate Security Controls orchestration
Call to Action

- **Current Status**
  - POC with early adopter customers / Security VNF’s
  - Open Security Controller available as Opensource ~ Mid 2017 compatible with few Security VNF and SDN vendors

- **Call to Action**
  - Contact us to get engaged in the community: Email: manish.dave@intel.com or Tarun@intel.com
  - Additional Information: www.intel.com/osc