VNFs for Security

Ali Bidabadi
Principal Cloud Solutions Architect
Global Products & Solutions
Fortinet Security VNFs Tested

- Fortinet integrated with OSM since Release 2

- New with Release 5
  - Ansible based primitives
  - 5G POC

- OSM is our first go to for testing: NSH, 5G, MEC

- Generic vnfd, demos (by Fortinet):
  - https://github.com/fortinet-solutions-cse/fortistacks/tree/master/osm

- Joint PoCs:
  - OSM PoC #2
  - Multi Vendor Showcase
What Makes a Security VNF Viable?

**Broad Integration**
Available to launch in all major NFVIs

**Automation**
Support day0/day1/day2 configuration automation

**Cloud Grade Performance**
Fast instantiation and high throughput
Fortinet Security VNF – FortiGate NGFW

• Feature parity with FortiGate appliance
  • *On any Cloud, any hypervisor*

• **Leanest security VNF image in the market!!**

• Performance:
  • *Boot in seconds*
  • *Leverage accelerations (EPA)*
  • *Proven throughput and scalability*

• Active-Active Session Synchronization

• Utility license model – PAYG

• High resiliency and scale out/up
FortiGate Automation

- Day zero – bootstrapping
  - Cloud Init
    - License
    - Full configuration

- Day 2 Configuration
  - REST APIs
  - Ansible
  - FortiOS Terraform modules
FortiGate Security Automation – Fortinet Fabric Connectors

• Fortinet “Plug-ins” that allow visibility of third party objects in FortiGate firewall

• The Objects created by the Connector correspond to FortiGate Firewall address (Fabric Connector Address)

• When the Object content changes in the third party platform the Connector Address get automatically updated

• Continuous communication between Fortinet and third party platform
Fabric Connector in Action | Automated Synchronization

No manual updates necessary

FortiGate #1

FortiManager*

FortiGate #2

Fabric Connector

Update Objects

Convert

Dynamic Objects

Hybrid Networks

Hybrid Cloud

Public Cloud

VM

*FortiManager Optional

© Fortinet Inc. All Rights Reserved.
Security for the Telco Cloud/Mobile Core

**CHALLENGE**
- Increasing need by Mobile Carriers to deliver security services as VNFs for LTE & 5G mobile infrastructures

**SOLUTION**
- Fortinet VNFs provide a rich set of security functions for the virtual mobile infrastructure
- Solution focus areas—4G to 5G security, Edge Cloud & Cloud RAN, Telco Cloud

**BENEFITS**
- VNFs support modern acceleration technologies such as DPDK, SR-IOV and Advanced Encryption
- Securing and enhancing the Telco Cloud with flexible, open Multi-Cloud capabilities & Integration
- VNFs for MEC—Edge Security & Control, User-plane inspection, Service chaining and SecGW
Service Function Chaining w/ NSH

- **FortiGate understands packets with NSH header !!**
- Service insertion/chaining with FortiGate – map NSH id to security policy
**Key Solution Features**

- Automated provisioning and orchestration via VMware NSX
- Persistent security utilizing VMware NSX micro-segmentation
- Secure VXLAN segments with advanced protection across tiers

**Key Benefits**

- Automated deployment and orchestration of FortiGate-VMX for Software Defined Data Centers/Private Cloud
- Operationally feasible NSX-based micro-segmentation with advanced threat protection of east-west traffic

**Integration: NetX SDK**

- Purpose-built product “FortiGate-VMX”
- SDN Connector

---

**Fortinet-VMware Joint Solution**

1. Register Fortinet as a security service with NSX Manager
2. Auto-deploy FortiGate-VMX to all hosts in security cluster
3. FortiGate-VMX connects with FortiGate-VMX Service Manager
4. License verification and configuration synchronization with FortiGate-VMX
5. Redirection policy rules updated for enablement of FortiGate-VMX security service
6. Real-time updates of object database
7. Push policy synchronization to all FortiGate-VMX deployed in cluster
Integration—VMware-NSX-T (North-South)

1. Register Fortinet as security service with NSX Manager (installation time) or deregister at uninstallation time

Support A-P HA (Unicast)

FortiManager (optional) can work just like any other use cases. It is just not purpose-built on NSX-T yet.

API Client (CentOS)

Web server (ovf is located)

VMware NSX Manager

Redirect policy rules updated for enablement of FortiGate-VM security service

VMware NSX-T logical router A

VMware NSX-T logical router B

© Fortinet Inc. All Rights Reserved.
FortiGate – A Multi-Cloud Security VNF

**Zero Trust Deployment**
- Block lateral threat propagation in East-West direction
- Comprehensive protection in North-South direction
- Advanced security (L7 Firewall, IPS, and ATP) for all traffic paths
- Security workflows that adapt to deployment changes
- Auto-provisioning of security services across all platforms

**End-to-End Automation**
- Single Policy Set across all deployments
- Leverage metadata instead of traditional IP in security policies
- Automated workload and metadata discovery
- Centralized management & analytics across deployments
- Intuitive visibility
- Automated VPN provisioning for multi-cloud connectivity
- Quarantine infected workloads automatically

**Operational Simplicity**

**Cloud Security Components**
- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Auto Scaling Security
- Denial of Service Protection

---

**FortiGate – A Multi-Cloud Security VNF**

- **AWS**
- **Azure**
- **Cloud Sandboxing**
- **Internet**
- **VPN / SD-WAN**
- **MPLS**
- **Remote Workforce**
- **Cloud Access & VPN**
- **Policy Enforcement Connector / Management and Analytics**
- **Enterprise Data Center / Branch Office**

---

**AWS**

- CFT
- ARM
- Terraform
- Python
FortiGate-VM Performance Enhancements

Enhancing performance by supporting:

- SR-IOV
- DPDK+vNP Offloading (aka vSPU)
- Intel QuickAssist Technology  

Diagram showing the relationship between Hypervisor switch, PF driver, vNIC, DPDK RX/TX, I/F #0, I/F #1, and vNP.
Performance Enhancements with DPDK+vSPU Offloading

FortiGate-VM on KVM
8vCPU Throughput (Gbps)
Non-vSPU vs vSPU-enabled

- Firewall UDP: 35.3 non-vSPU vs 80 vSPU
- IPS Enterprise Mix: 6.8 non-vSPU vs 8.1 vSPU (19% improvement)
- NGFW Enterprise Mix: 5.2 non-vSPU vs 6.1 vSPU (17% improvement)
- Threat Prevention Enterprise Mix: 4.2 non-vSPU vs 5.1 vSPU (21% improvement)
- App Control HTTP 64k: 4.0 non-vSPU vs 11.0 vSPU (x2.75 improvement)
Intel QAT Support

- Intel cryptographic accelerator
- FortiGate-VM IPSec-VPN
- Supported on v6.2.0 FortiOS
- Support 8970 & 8950 adapters
  - More adapters/chipsets to be supported in future versions
- Other QAT benefits such as packet compression (WAN optimization) to be considered
Performance Enhancements with Intel QAT

FGT-VM on KVM
Frame Size/Throughput (Mbps)
Non-QAT vs QAT-enabled

- DELL R740 x 1 Host
- Use 2 VDOMs on 2 FGT-VMs to configure VPN within the same host
- Encrypted traffic using AES-256-SHA1
- CPU Utilization 100%, no packet loss

**Frame Size (bytes)**

<table>
<thead>
<tr>
<th>Frame Size (bytes)</th>
<th>Non-QAT</th>
<th>QAT-enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>256</td>
<td>355</td>
<td>664</td>
</tr>
<tr>
<td>512</td>
<td>509</td>
<td>973</td>
</tr>
<tr>
<td>1024</td>
<td>819</td>
<td>2056</td>
</tr>
<tr>
<td>1360</td>
<td>973</td>
<td>2830</td>
</tr>
<tr>
<td>9000</td>
<td>664</td>
<td>8089</td>
</tr>
</tbody>
</table>

**Performance Enhancements**

- **X2.5**
- **X2.9**

Mbps
Fortinet Security VNF – Summary

- Integrated and tested with Open Source MANO (OSM)
- Leanest security VNF image in the market
- Proven throughput and scalability
- Scale up/out support
- Day0/Day1/Day2 configuration automation
- SFC/NSH support
- Utility license model – PAYG