Security Automation with VMware NSX and Network Function Virtualization (NFV)

[NET1047BES]
SESSION OBJECTIVES

- Fortinet in a Nutshell
- Fortinet’s SDDC Security Approach
- Fortinet and VMware’s SDDC Component Integration
- Fortinet’s FortiGate-VMX Licensing Model
FORTINET: GLOBAL NETWORK SECURITY LEADER

- Founded in 2000
- 100+ Offices across the globe
- In excess of $1bn revenue
- 4,700+ Employees worldwide
- $1.46bn in cash
- 30% year on year growth
- 3.3m shipped security devices
- 320k customers
- 395 patents issued
- 316 in process
- Headquartered in Sunnyvale, California
CONTINUED GROWTH – TAKING MARKET SHARE

Network Security Appliance Shipments

- **Fortinet**
- **Palo Alto Networks**
- **Cisco**
- **Check Point**

IDC WW, 2016
Advanced Security for VMware’s Software Defined Data Center
ADDED VALUE OF SECURITY INTEGRATION IN SDDC

- Not just firewall, but advanced features
- Micro-Segmentation and Zero Trust
- Control of ‘east-west’ traffic, Inter and Intra VM security, Logical Security Zone (multi-tier)
- Integration, Orchestration and Automation
COMPONENTS FOR NSX FOR VSPHERE INTEGRATION

- VMware vCenter Server v5.5 or v6.x
- VMware vSphere (Advanced license v5.5 or v6.x)
- ESXi Hosts
- REST API
- Fortinet Solution
  - FortiGate-VMX Service Manager
  - FortiGate-VMX Security Appliance

VMware vSphere (Advanced license v5.5 or v6.x)
WHAT IS FORTIGATE-VMX?

- Purpose-built security solution with VMware NSX for SDDC which runs in between the VMs
- Full Next Generation security functionality solution in one platform
- Backed by FortiOS™ policy configuration and FortiGuard™ for real time intelligence updates
- Proven multi-tenant capable using virtual domains (VDOM)

Traffic will be redirected through the FortiGate-VMX based on applied policy

Group A

Group B

Group C

FortiGate-VMX Security Node

Hypervisor
1. Register Fortinet as 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. Policy synchronization to all FortiGate-VMX deployed in cluster
FORTIGATE-VMX AND VMWARE NSX FILTER DRIVER INTERACTION

Packet Flow
1. From VM to NSX Filter Driver
2. NSX Filter Driver Forward to Third party Solution (FGT-VMX)
3. FGT-VMX applies Security and sends packet back to NSX Filter Driver
4. NSX Filter Driver can do service chaining or send packet to destination
COMPETITIVE ADVANTAGES

Real Multi-tenancy (VDOM) support

Virtual Domain (VDOM) dedicated per tenant or individual security feature

Redirection Policy based on FortiGate VDOM ensure proper segmentation
COMPETITIVE ADVANTAGES

Real Multi-tenancy (VDOM) support
- Virtual Domain (VDOM) dedicated per tenant or individual security feature
- Redirection Policy based on FortiGate VDOM to ensure proper segmentation
- VDOMs can be used for different use cases
COMPETITIVE ADVANTAGES

Real Multi-tenancy (VDOM) support
OVF footprint < 40 MB
Automatic import and update of objects from NSX
FORTIMANAGER NSX OBJECTS AND SERVICE MANAGER INTEGRATION

- NSX Security Groups Objects imported in FortiManager using **Dynamic Objects**
- FortiManager sends to FortiGate reference to Dynamic Object
- Dynamic Objects **automatically** updated from NSX Manager
- NSX Security Groups available in hybrid environment for **East-West** and **North-South** security
CONFIGURE FIREWALL POLICY FROM FORTIMANAGER

<table>
<thead>
<tr>
<th>Seq. #</th>
<th>Name</th>
<th>From</th>
<th>To</th>
<th>Source</th>
<th>Destination</th>
<th>Schedule</th>
<th>Service</th>
<th>Users</th>
<th>Action</th>
<th>Security Profiles</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Incoming to Web</td>
<td>external</td>
<td>internal</td>
<td>all</td>
<td>Web-SG</td>
<td>always</td>
<td>HTTP</td>
<td></td>
<td>Accept</td>
<td>default</td>
<td>Log Security Events</td>
</tr>
<tr>
<td>2</td>
<td>Web to VIP</td>
<td>external</td>
<td>internal</td>
<td>Web-SG</td>
<td>VIP-SG</td>
<td>always</td>
<td>HTTP</td>
<td></td>
<td>Accept</td>
<td>default</td>
<td>Log Security Events</td>
</tr>
<tr>
<td>3</td>
<td>VIP to App</td>
<td>external</td>
<td>internal</td>
<td>VIP-SG</td>
<td>App-SG</td>
<td>always</td>
<td>HTTP</td>
<td></td>
<td>Accept</td>
<td>default</td>
<td>Log Security Events</td>
</tr>
<tr>
<td>4</td>
<td>App to DB</td>
<td>external</td>
<td>internal</td>
<td>App-SG</td>
<td>DB-SG</td>
<td>always</td>
<td>MYSQL</td>
<td></td>
<td>Accept</td>
<td>default</td>
<td>Log Security Events</td>
</tr>
</tbody>
</table>
NSX SECURITY GROUP DEFINITION AND USAGE

Service Groups created in NSX Manager automatically get sent to the FortiGate-VMX and are available for Policy Creation.

Policy created in FortiGate-VMX using Exchanged Security Group.
FORTIGATE-VMX LOGS TO FORTIANALYZER

- Configuration is done on the FortiGate-VMX Service Manager
- Logs are relayed from the FortiGate-VMX to the FortiGate-VMX Service Manager
### FORTIGATE-VMX LOGS TO FORTIANALYZER

- Configuration is done on the FortiGate-VMX Service Manager
- Logs are relayed from the FortiGate-VMX to the FortiGate-VMX Service Manager
- Only the FortiGate-VMX Service Manager serial number is reported on FortiAnalyzer

---

**Log View**

<table>
<thead>
<tr>
<th>#</th>
<th>Date/Time</th>
<th>Device ID</th>
<th>Action</th>
<th>Source</th>
<th>Destination IP</th>
<th>Service</th>
<th>Sent/Received</th>
<th>Application</th>
<th>Security Event List</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14:53:01</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>172.16.1.6</td>
<td>10.0.1.12</td>
<td>HTTP</td>
<td>642.0 B/600.0 B</td>
<td>HTTP_BROWSER_Chrome</td>
<td>APP 1</td>
</tr>
<tr>
<td>2</td>
<td>14:53:01</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>172.16.1.6</td>
<td>10.0.1.11</td>
<td>HTTP</td>
<td>1.2 KB/24.4 KB</td>
<td>HTTP_BROWSER_Chrome</td>
<td>APP 1</td>
</tr>
<tr>
<td>3</td>
<td>14:53:01</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>172.16.1.6</td>
<td>10.0.1.12</td>
<td>HTTP</td>
<td>698.0 B/795.0 B</td>
<td>HTTP_BROWSER_Chrome</td>
<td>APP 1</td>
</tr>
<tr>
<td>4</td>
<td>14:52:56</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>10.0.1.12</td>
<td>172.16.1.6</td>
<td>HTTP</td>
<td>954.0 B/892.0 B</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>14:52:56</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>10.0.2.11</td>
<td>10.0.3.11</td>
<td>MYSQL</td>
<td>655.0 B/662.0 B</td>
<td>MYSQL</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>14:52:56</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>10.0.1.12</td>
<td>172.16.1.6</td>
<td>HTTP</td>
<td>916.0 B/883.0 B</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>14:52:56</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>10.0.1.12</td>
<td>172.16.1.6</td>
<td>HTTP</td>
<td>916.0 B/883.0 B</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>14:52:56</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>10.0.1.12</td>
<td>172.16.1.6</td>
<td>HTTP</td>
<td>879.0 B/1.2 KB</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>14:52:56</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>10.0.2.12</td>
<td>10.0.3.11</td>
<td>MYSQL</td>
<td>657.0 B/769.0 B</td>
<td>MYSQL</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>14:52:56</td>
<td>FGTVMX00000000093</td>
<td>✓</td>
<td>10.0.1.12</td>
<td>172.16.1.6</td>
<td>HTTP</td>
<td>373.0 B/1.1 KB</td>
<td>HTTP</td>
<td></td>
</tr>
</tbody>
</table>
FORTIGATE-VMX LICENSE MODEL

- One license for the FortiGate-VMX Service Manager
- Simple license based on number of FGT-VMX Security Appliance deployed
  - One FortiGate-VMX license per ESXi host
  - No limits placed on resources (virtual or hardware), nor number of protected VM workloads
NextGen Firewall use case at KPN

Use case, proof of concept and the next steps

September 12th 2017, VMworld Barcelona
Let me introduce myself …

Albert W. Alberts:

- Working at KPN since 1999:
- Started as Software Engineer
- KPN patents
- Currently Architect

https://www.linkedin.com/in/albertalberts/
@a_w_alberts
albert.albert@kpn.com
KPN, the company

- KPN (Koninklijke PTT Nederland)
- Dutch landline and mobile telecommunications company
- 4G, 5G, LoRa
- Internet Services Provider
- TV
- ICT-services
KPN, the company

- 15,000 employees
- 6.3 million fixed-line telephone customers
- 33 million subscribers in Netherlands, Germany, Belgium, France and Spain
- 2.1 million Internet access customers
- 1 of 15 worldwide VMware showcase partners
MANAGED HYBRID CLOUD

CLOUD MANAGED SERVICES

- Operating Systems
- Business Continuity
- Database
- Networking
- Security
- Enterprise WebHosting

JOURNEY TO THE CLOUD

CLOUD CONNECT

CLOUD CONTROL
Customer Interface

APP FACTORY
Continuous Delivery

PRIVATE CLOUD

VIRTUAL PRIVATE CLOUD

ON-PREMISES

CLOUD NL

PUBLIC CLOUD

AWS Cloud

AZURE Cloud
CloudNL features:

• Services are delivered from KPN datacenters within the Netherlands;
• Operational maintenance from within the Netherlands under Dutch law and regulations;
• Assurance through the Cloud Compliance Framework (CCF).
MANAGED HYBRID CLOUD

Cloud features:
- Self-service management
- Create own infrastructure
- Manage own infrastructure
- Scalable
- Per-per-use
CloudNL VMware, based on VMware technology

- vRealize Automation;
- vRealize Orchestration;
- NSX;
- vCenter & vSphere.
How does a customer get it?

Interfaces

Porta

CloudNL VMware

ReST API

vRealize Automation

vRealize Orchestration

Python

Go

Ruby

C#

Compute resources

Networking resources

Storage resources

VMware
What does a customer get?

Default network setup: front-end & back-end

Tenant A
private IP

Internet

Perimeter ESG

Tenant A
ESG

Distributed
Logical
Router

VM
VM
default GW

transport network

public IP
private IP

Datacenter 1

Datacenter 2

Tenant A
ESG

Distributed
Logical
Router

VM
VM
default GW

transport network

public IP
private IP

PNat(ting)

Internet

Perimeter ESG

NSX Edge pair

Default network setup:
- Front-end & back-end
- Public network, without NAT(ting)
- Private network, with sNAT(ting)

VMworld 2017 Content: Not for publication or distribution
What does a customer get?

Default network setup: front-end & back-end

[Diagram showing network setup with Fortinet devices and VMs]
Next Gen Firewall

Proof-of-concept at KPN CloudNL VMware
Next Gen Firewall PoC

Client requirement:
- Next Gen Firewall

Platform requirements:
- Integration with NSX
- Multi-tenancy within NSX
- Multi-tenant self-service portal
- Multi-tenant API
- Integration with vRealize
KPN CloudNL VMware, default tenant network

Management network
- NSX Manager
- Fortigate SVM
- Fortigate-VMX Security Node

Core Router
- Perimeter ESG
- Tenant ESG
- Distributed Logical Router

Core Router
- Perimeter ESG
- Tenant ESG
- Distributed Logical Router

internet

Datacenter 1
- public IP
- default GW
- restriction of 10 connections
- transport network
- default GW
- private IP

Datacenter 2
- public IP
- default GW
- transport network
- default GW
- private IP

Management network
- NSX Manager
- Fortigate SVM
- Fortigate-VMX Security Node

internet

private network, without NAT(ting)

private network, with sNAT(ting)
vRealize expected user interface

vRA portal as single “pane of glass”

No easy integration with vRealize Automation
vRealize actual user interface

A Fortigate Service Manager GUI for each datacenter

Possible but not preferred
vRealize preferred user interface

vRA portal for simple tasks, FortiManager GUI for more advanced tasks

FortiManager solves the dual interface problem but was not available during the Poc. Current status is beta
Next Gen Firewall PoC results

Platform requirements:

- Integration with NSX ✓
- Multi-tenancy within NSX ✓
- Multi-tenant self-service portal ✓ but two self-service portals
- Multi-tenant API ✓ but two interfaces
- Integration with vRealize X no, this requires developer effort
Platform requirements:

- Integration with NSX ✓
- Multi-tenancy within NSX ✓
- Multi-tenant self-service portal ✓
- Multi-tenant API ✓
- Integration with vRealize ✗ plans to build it for most used configs
Questions?