FortiGate-VMX Deployment Use Cases

Deployment of Fortinet's Next-Generation Firewall into VMware NSX Environment
# FortiGate-VMX Deployment Use Cases

## Table of Contents

- Introduction .................................................. 3
- VMware NSX Overview ........................................ 4
  - Control Plane ................................................ 5
  - Data Plane .................................................... 5
  - Management Plane and Consumption Platforms ............... 5
- FortiGate-VMX Overview ....................................... 5
- VMware NSX and FortiGate-VMX ................................ 5
  - Service Insertion .............................................. 6
  - Security Groups, Security Tags ............................... 6
  - Virtual Domains .............................................. 8
- Use Cases ....................................................... 9
  - Internal Segmentation Firewall for SDDC ....................... 9
  - Multi-tiered Application Threat Defense ...................... 10
  - VDOMs with NSX Service Profiles ............................ 11
- Conclusion ..................................................... 12
FortiGate-VMX Deployment Use Cases

Introduction
This document is intended for IT administrators and security architects who specialize in cloud and virtualization in VMware’s Software Defined Data Center (SDDC). It focuses on deployment of Fortinet’s Next-Generation Firewall into VMware NSX environment. It also covers advanced security solutions, differentiators and use cases. It does not attempt to cover architectural design decisions, technical API details or installation.

As VMware NSX matures into production environments, network and security architects are looking to operationalize NSX with more advanced integration and manageability. Fortinet’s FortiGate-VMX solution programmatically integrates with VMware’s latest NSX APIs to provide industry leading Firewall functionality as a service into SDDC deployments.

Fortinet’s security framework embraces and delivers advanced security for VMware SDDC with key pillar features on orchestration agility, OPEX cost reduction and provisioning and deployment at scale.

Fortinet’s FortiGate-VMX provides protection against potential vulnerabilities. The joint solution provides:

- Introspection for east-west traffic between VMs.
- Automatic security node deployment for expanding workloads reduces manual intervention and human error.
- Service insertion and service chaining enable effective Microsegmentation.
- Managed service and departmental segmentation through use of Virtual Domains (VDOMs).

Like with previous versions of FortiGate-VMX, the solution can automatically and transparently be deployed on every ESXi hypervisor added to NSX defined security cluster. The latest security policies are dynamically applied to all ESXi platforms in the cluster. These policies are also inherited during VM migration and resource balancing.
The integrated solution provides the best-in-class FortiOS™ threat intelligence and next-generation firewall and UTM capabilities deployed automatically. It offers distributed services scale out and avoids hair-pinning with efficient routes.

With network virtualization, the functional equivalent of a “network hypervisor” reproduces the complete set of layer 2 to layer 7 networking services (e.g., switching, routing, firewalling and load balancing) in software. As a result, these services can be programmatically assembled in any arbitrary combination, to produce unique, isolated virtual networks in a matter of seconds.

VMware NSX Overview

IT organizations have gained significant benefits as a direct result of server virtualization. Server consolidation reduces physical complexity, increases operational efficiency, and provides the ability to dynamically re-purpose underlying resources to quickly and optimally meet the needs of increasingly dynamic business applications. These are just a handful of the gains that have already been realized. Now, VMware’s Software Defined Data Center (SDDC) architecture is extending virtualization technologies across the entire physical data center infrastructure. VMware NSX, the network virtualization platform, is a key product in the SDDC architecture. With VMware NSX, virtualization now delivers for networking what it has already delivered for compute and storage. In much the same way that server virtualization programmatically creates, snapshots, deletes and restores software-based virtual machines (VMs), VMware NSX network virtualization programmatically creates, snapshots, deletes, and restores software-based virtual networks. The result is a completely transformative approach to networking that not only enables data center managers to achieve orders of magnitude better agility and economics, but also allows for a vastly simplified operational model for the underlying physical network. With the ability to be deployed on any IP network, including both existing traditional networking models and next generation fabric architectures from any vendor, NSX is a completely non-disruptive solution. In fact, with NSX, the physical network infrastructure you already have is all you need to deploy a software-defined data center.
Control Plane
The NSX control plane runs in the NSX controller. In a vSphere-optimized environment with vDS (vSphere Distributed Switch), the controller enables multicast free VXLAN and control plane programming of elements such as Distributed Logical Routing (DLR). In all cases the controller is purely a part of the control plane and does not have any data plane traffic passing through it. The controller nodes are also deployed in a cluster of odd members in order to enable high-availability and scale.

Data Plane
The NSX Data plane consists of the NSX vSwitch. The vSwitch in NSX for vSphere is based on the vSphere Virtual Distributed Switch (vDS) with additional components to enable rich services. The add-on NSX components include kernel modules (VIBs) which run within the hypervisor kernel providing services such as distributed routing, distributed firewall and enable VXLAN bridging capabilities. The NSX vDS abstracts the physical network and provides access-level switching in the hypervisor. It is central to network virtualization because it enables logical networks that are independent of physical constructs such as VLANs. Some of the benefits of the NSX vSwitch are:

- Support for overlay networking with the use of the VXLAN protocol and centralized network configuration. Overlay networking enables the following capabilities:
  - Creation of a flexible logical layer 2 (L2) overlay over existing IP networks on existing physical infrastructure without the need to re-architect any of the data center networks.
  - Agile provision of communication (east-west and north-south) while maintaining isolation between tenants.
  - Application workloads and virtual machines that are agnostic of the overlay network and operate as if they were connected to a physical L2 network.
- NSX vSwitch facilitates massive scale of hypervisors.
- Multiple features—such as Port Mirroring, NetFlow/IPFIX, Configuration Backup and Restore, Network Health Check, QoS, and LACP—provide a comprehensive toolkit for traffic management, monitoring and troubleshooting within a virtual network.

Additionally, the data plane also consists of gateway devices that can provide communication from the logical networking space (VXLAN) to the physical network (VLAN). This functionality can happen at Layer 2 (NSX bridging) or at L3 (NSX routing).

Management Plane and Consumption Platforms
The NSX management plane is built by the NSX manager. The NSX manager provides the single point of configuration and the REST API entry-points in a vSphere environment for NSX. The consumption of NSX can be driven directly via the NSX manager UI. In a vSphere environment this is available via the vSphere Web UI itself. Typically end-users tie in network virtualization to their cloud management platform for deploying applications. NSX provides a rich set of integration via the REST API.

FortiGate-VMX Overview
VMware NSX has a powerful traffic steering capability which it uses to intercept traffic at the hypervisor level and hands it off to FortiGate-VMX for advanced security policy enforcement.

There are two main components in the solution:

- FortiGate-VMX Service Manager not only registers the security service definitions with NSX, but centralizes license management and configuration synchronization with all FortiGate-VMX Security Node instances.
- Fortinet FortiGate-VMX Security Nodes receive the redirected traffic and apply the protection policies on this traffic.
- Fortinet FortiAnalyzer (optional) for network security logging, analysis, and reporting securely aggregates log data from the Fortinet FortiGate-VMX security solution.

FortiGate-VMX Service Manager communicates directly with the NSX environment. It registers the FortiGate-VMX security service enabling auto-deployment of required FortiGate-VMX Security Nodes. The management plane flow is two-way in that the FG-VMX Service Manager supplies service definitions to the NSX Manager, while NSX Manager sends updates to the FortiGate-VMX Service Manager about new or updated dynamic security groups and objects, upon which policy is based in real time.

FortiGate-VMX Service Manager obtains proactive security threat updates from FortiGuard and synchronizes those updates to all FortiGate-VMX Security Nodes.

VMware NSX and FortiGate-VMX
FortiGate-VMX together with VMware NSX provides a truly flexible and Efficient Data Center Architecture. By means of Network Virtualization, NSX is capable of distributing Layer 2 to Layer 7 networking and security services including routing, switching, firewalling etc.
FortiGate-VMX integrates with VMware NSX Service Composer to implement a new model for consuming network and security services. It allows IT administrators to provision and assign firewall policies and security services to application workloads in real time.

Thus, Network virtualization and orchestration with VMware NSX architecture makes the enforcement of security possible despite workload changes. Networks and network security can be remapped, adjusted or expanded when workloads are migrated or changed.

Fortinet is the only network security provider who offers integrated Segmentation Network Security solution for the entire network with one operating system with FortiOS. FortiOS delivers highly effective & flexible security with real time updates from FortiGuard Labs to help combat the latest threats, and has received top effectiveness ratings in industry tests: NSS Labs, VB100, AV Comparatives.

**Service Insertion**

One of the key enablers brought in through VMware NSX is the concept of Service Insertion. It provides APIs and an interface to let the FortiGate-VMX Register as a service. Once enabled, based on the system configuration, The FortiGate-VMX advanced security services are now enabled to secure traffic flowing to and from the VM at the hypervisor level. Registering the Security Service

1. FortiGate-VMX Service Manager registers the Fortinet security service with NSX Manager (FortiGate-VMX): The registration process uses the NetX management plane API to enable bi-directional communication between FortiGate-VMX Service Manager and the NSX Manager.
2. Auto-deploy FortiGate-VMX to all hosts in security cluster: The NSX Manager collects the FortiGate-VMX image from the URL specified during registration and installs an instance of FortiGate-VMX on each ESXi host in the designated cluster(s). The image update is instantaneous and beneficial for on-demand, software-defined data center requirements.
3. FortiGate-VMX connects with FortiGate-VMX Service Manager: The FortiGate-VMX initiates a connection to the FortiGate-VMX Service Manager to register with the Service Manager and obtain its license.
4. License verification and configuration synchronization with FortiGate-VMX: FortiGate-VMX Service Manager verifies the serial number and synchronizes configuration and policy.
5. Redirection policy rules updated for enablement of FortiGate-VMX security service: For all objects secured in the cluster, a policy of redirection of all traffic to FortiGate-VMX is ready.
6. Real-time updates of object database: The NSX Manager sends real-time updates on the changes in the virtual environment to the FortiGate-VMX Service Manager.
7. FortiGate-VMX Service Manager dynamically synchronizes object database and policy to all FortiGate-VMX virtual appliance instances deployed in cluster.

**Security Groups, Security Tags**

**SECURITY GROUPS**

VMware Service Composer supports the configuration of Security groups, these could be either static or dynamic and can be defined based on various parameters, including security tags, VM names, dvPortGroups, VXLAN segments, etc…
When a Security group is created, any VMs matching the parameters defined in the Security group are automatically added to the Security group. When any one of these parameters is changed, the grouping for that VM will be automatically re-evaluated and it will be added to any Security groups it should fall in. Without VMware NSX integration, this would be a painstaking process which would need to be done manually.

Security groups are always automatically synced real time between the FortiGate-VMX Service Manager and the NSX Manager.

**SECURITY TAGS**

VMware NSX which allows the creation of Security tags. These tags can then be assigned to VMs. This can either be done programmatically or manually. Once done, this can be used as a classifier to automatically assign all VMs with a tag to a specific Security group.

This Security group membership information will also be synchronized real-time with the FortiGate-VMX Service Manager.

In the screenshots above we see the following flow:

1. A new tag is created for infected systems. This will be dynamically assigned to any systems detected as infected.
2. Second screenshot shows the creation of a Security group which dynamically includes all infected systems. Any VM marked as
an infected system with the above tag will become a part of this
group.

3. On FortiGate-VMX Service Manager, a policy is created to allow infected systems access only to a restricted domain and to apply all protection to these flows.

By doing this, we are able to exercise precise control over east-west traffic and prevent spreading of threats and infections laterally.

SERVICE PROFILE

When the FortiGate-VMX Service Manager has registered with the VMware NSX Manager, NSX can be configured to use FortiGate-VMX as a Network Introspection Service.

Once such a policy is configured, any traffic to a Security Group will automatically be redirected to a FortiGate-VMX Security node.

CONFIGURING REDIRECTION TO A FORTIGATE-VMX SERVICE

SECURITY POLICY

Once a Security group is configured and has been synced to the FortiGate-VMX Service Manager, this Security group is automatically made available to be used in configuring security policies.

AUTOMATIC PROVISIONING OF FORTIGATE-VMX WHEN AN ESXI JOINS THE CLUSTER

When an ESXi instance is added to the cluster, NSX Manager will communicate with FortiGate-VMX Service Manager and together they will auto-deploy a FortiGate-VMX Security Node on the newly added ESXi. As a result any workloads added or moved to this hypervisor will still be protected with the proper security policy relevant to that workload.

Virtual Domains

Virtual Domains are a method of dividing a single FortiGate-VMX unit into multiple virtual units that function as individual units.

MULTITENANCY USING FORTINET VIRTUAL DOMAINS

Beyond the flexibility provided by NSX Manager, FortiGate-VMX also supports multiple VDOMS (Virtual Domains). A FortiGate-VMX with multiple VDOMs can provide different levels of protection for different server groups or traffic streams.

This is particularly useful to Service providers who can host each tenant on a different VDOM. This way the VDOMs are completely segregated and can be managed independently of each other. A more detailed example is seen in the use case section.

NFV FOR SECURITY USING VDOMS

By using VDOMs, security functions can be hosted on a single FortiGate-VMX Security node, but can be segregated into multiple VDOMs with each VDOM responsible for a specific security service.

This feature is particularly useful for enterprise customers. Using VDOMs an enterprise can split the different security functions like Antivirus, IPS, App Control etc., into different VDOMs. A more detailed example is seen in the use case section.
Use Cases

Below are three use cases for VMware NSX and Fortinet Fortigate-VMX Integrated solution.

Internal Segmentation Firewall for SDDC

Advanced Threats are taking advantage of the flat Internal Network. Once through the border defense, there is little to stop their spread and eventual extraction of valuable targeted assets. Because traditional Firewalls have been architected to slower speeds of the Internet Edge, it’s hard to deploy these security devices internally.

Using the Internal Segmentation Firewall (ISFW) that sits at strategic points of the internal network provides Network Segmentation inside the perimeter. The ISFW may sit in front of specific servers that contain valuable intellectual property or a set of user devices or web applications sitting in the cloud.

Fortinet has an array of existing Hardware FortiGates which provide high speed NGFW functionalities and thus facilitate deployment of Firewalls between the network segments. By extending the ISFW principle into the Software Defined Data Center with the VMware NSX and FortiGate-VMX integration, we can provide Firewall functionality between the virtual microsegments.

By creating Security Groups for related devices within the network, we are able to Define smaller trust groups which can then be protected using a firewall. This protects against threats spreading across these smaller groups within the network. As a result we are able to bring in the advantages of Internal Segmentation firewalls deeper into the Datacenter by protecting traffic between Virtual Segments.
Group A, B and C can be used to define the smaller Security Groups. For instance, Group A could be all the Organization's Internal Service servers like HR Databases, other highly secure devices. Group B could be hosted services for Employee use example company email, central storage for intellectual property. Group C could include hosted web-services provided by the company including the company webpage, other externally exposed services.

We would define 3 Security groups for this:

**Group A** – Limited access group for Sensitive data, limited visibility

**Group B** – Internal group for internally accessible Data

**Group C** – Publicly visible Group for services/machines visible to the outside world

By using the principles of having an Internal Segmentation Firewall, threats which might have penetrated one network can be prevented from reaching other parts of the trusted network.

**Multi-tiered Application Threat Defense**

Traditionally, to provide Threat defense to different applications, the network would need to be segmented such that the different applications would be in distinct virtual networks.

Using VMware NSX and FortiGate-VMX, we can define Microsegments such that Services requiring different levels of protection can be protected with the appropriate Security Policy.

This can be effectively set up by configuring (either statically or dynamically) Security groups for each application type. Once this is done, the FortiGate-VMX can be configured with the relevant Security policies for each group.

By doing this, NSX will automatically redirect the traffic to the FortiGate-VMX. For instance, FortiGate-VMX will see all traffic bound to Email Server Group Devices unless the traffic originates from an Email Server Group device.

This can be seen from the green flow, since E3 is an email server while S2 is a secure storage server, the FortiGate-VMX will see this traffic, and apply any relevant policies on it.

Similarly, traffic from File server F1 to Database D3 will flow through the FortiGate VMX.

As in the above case, using VMware NSX in conjunction with FortiGate-VMX helps secure east-west traffic as well as north south traffic.
VDOMs with NSX Service Profiles
Fortinet Virtual Domains (VDOMs) allow network administrators to segment a single FortiGate-VMX Security Node to service different flows completely separate from each other.

This is a very valuable feature providing greater flexibility for both Enterprise and Managed Service Providers as seen in the sample Security Policy configurations below. We will look at one use case for each segment.

MSSP: MULTITENANCY USING VDOMS AND NSX SERVICE PROFILES
In this example, a managed service provider provides an infrastructure hosting web services to it’s tenants.

The provider would have a security group for web services (and potentially other security groups for each different service offered). Security policies assigned for traffic to/from this group will be re-directed to the FortiGate-VMX Security Node. The FortiGate-VMX Service Manager will in turn have three separate VDOMs configured; one for each tenant – over which the corresponding tenant would have full autonomy.

Here, the three tenants: Orange, Blue and Red would all be protected using the same FortiGate-VMX Security node, yet would be completely separate from one another and have autonomy over their segment. This is even more valuable when there are multiple services offered.

This deployment model reduces cost by removing the need to provide each tenant with their own FortiGate-VMX security service. It also enables them to extend their VDOM configurations from parallel Hardware deployments.
By using different VDOMs for different Security features, we can ensure that the right features are used for the right flows and Security Groups.

Conclusion

The VMware NSX with FortiGate-VMX security solution brings together the flexibility afforded by VMware NSX and the industry leading security of Fortinet FortiOS with real time intelligence updates by FortiGuard Labs. Together, these components provide unmatched Threat visibility and protection both for east/west and north/south traffic.

This solution is an ideal fit for scale up and scale out scenarios. VMware NSX and FortiGate-VMX together ensure that any new workloads introduced and changes to existing workloads will automatically be evaluated to provide FortiGate-VMX’s security service.

With the automation capabilities provided by the VMware NSX APIs and the FortiGate Single pane of Glass visibility and control, this solution is able to provide extremely effective security while making data center security management both simple and more efficient.

1. VMware® NSX for vSphere (NSX-V) Network Virtualization Design Guide