Secure Virtualization for Healthcare

A Reference Architecture for Deploying Fortinet's Next-Generation Firewall into a VMware NSX Environment

In recent years, Healthcare companies have increased their investment in virtualization and as a result, data centers are becoming home to increasing volumes of patient related data and medical applications. Because of this shift in data storage and application deployment, security has become a foundational design aspect when building today's Data Centers. Most common security architectures revolve around building a strong perimeter defense to prevent any threats from penetrating the Data Center. This however fails to account for any threats that do manage to get through the perimeter, via innumerable available means, and into the data center. Once in, threats potentially have unrestricted access to all patient data and applications sitting within the virtual solution.

VMware's NSX platform begins to address the complexities of administering and securing a large virtual infrastructure. Through Security Group tags and the distributed firewall, NSX provides a mechanism for an easily managed virtual infrastructure with a basic stateful firewall built-in along with core features offering micro-segmentation and multi-tenancy capabilities. These features demand an increased level of security to manage the traffic between tenants and applications. Fortinet provides a comprehensive, next-generation security solution that enables Healthcare organizations to securely complete their Software Defined Data Center (SDDC) ecosystem.

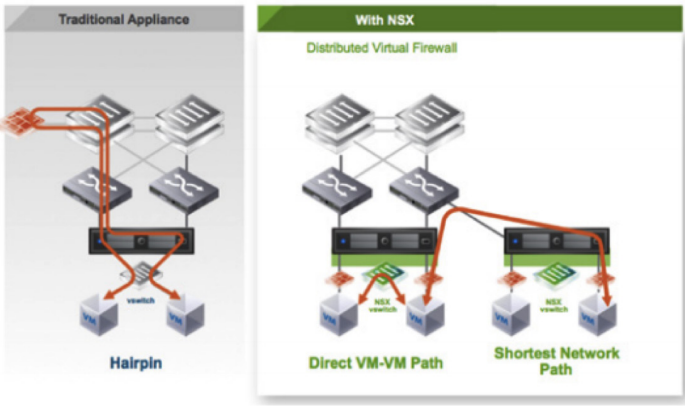
Fortinet's FortiGate-VMX provides protection against potential vulnerabilities and security threats. The joint VMware NSX/ Fortinet VMX solution provides:

- East-West inter-VM traffic visibility
- Less error-prone manual configuration for firewall rules
- Automatic security provisioning based on application workloads
- Managed micro segmentation through service insertion and service chaining
- Secured VXLAN segments to enable tiered workload mobility
- Centralized visibility and proactive protection with FortiGuard across virtual and physical environments
- Security services provisioned in minutes

Fortinet's FortiGate-VMX solution integrates seamlessly withVMware's latest NSX APIs, utilizing key pillar features of NSX such as orchestration agility, OPEX cost reduction, as well as provisioning and deployment at scale.

Healthcare is increasingly relying on virtualization to solve expanding data needs with limited space and staff. VMware's NSX solution creates an easily managed environment to grow server and database resources with automated networking tools, reducing reliance on highly specialized staff. Adding FortiGate-VMX to the solution likewise simplifies securing systems and traffic within and without the SDDC. FortiGate-VMX can automatically and transparently be deployed on every ESXi hypervisor, dynamically applying security policies to all ESXi platforms in the cluster as they are deployed.

The integrated solution provides the best-in-class FortiOS™ threat intelligence and next-generation firewall and UTM capabilities deployed automatically. It offers distributed services that scale out and provide full security and visibility without the necessity of hair-pinning traffic to hardware security appliances.



NSX EFFICIENT ROUTING

FortiGate-VMX Overview

VMware NSX API integration provides agents inserted between the distributed vSwitch and vNIC of every workload (virtual machine) deployed in the cluster. This agent intercepts the 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 registers the security service definitions with NSX and centralizes license management and configuration synchronization with all FortiGate-VMX Security Nodes
- Fortinet FortiGate-VMX Security Node processes runtime traffic and enforces policy
- Fortinet FortiAnalyzer (optional) for network security logging, analysis, and reporting securely aggregates log data from the Fortinet FortiGate-VMX security solution along with any other physical or virtual Fortinet solutions, creating a single location for all security reporting.

FortiGate-VMX Service Manager communicates directly with the NSX environment. It registers the FortiGate-VMX security service with NSX which enables auto-deployment of FortiGate-VMX Security Nodes. The management plane flow is two-way; the FG-VMX Service Manager supplies service definitions to the NSX Manager, while NSX Manager sends updates to the FortiGate-VMX Service Manager on new or updated dynamic Security Groups and objects. FortiGate-VMX policies are based on those Security Groups and updated 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

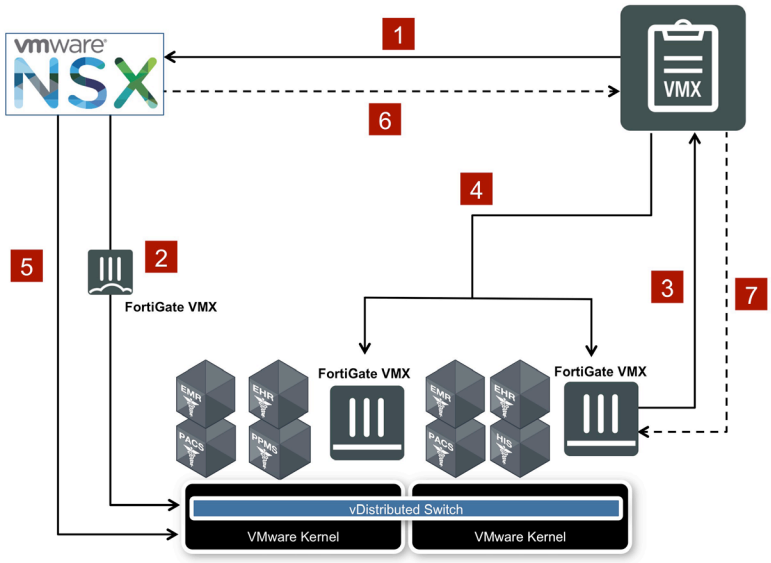
FortiGate-VMX together with VMware NSX provides a truly flexible and Efficient Data Center Architecture for Healthcare environments. By means of Network Virtualization, NSX is capable of distributing Layer 2 to Layer 7 networking and security services including routing, switching, firewalling, etc.

FortiGate-VMX integrates with VMware NSX Service Composer to implement a new model for consuming network and security services. It allows health IT administrators to provision and assign firewall policies and security services to application workloads in real time. Thus, Network virtualization and orchestration with the 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 a single operating system. FortiOS delivers highly effective and flexible security with real time updates from FortiGuard Labs to help combat the latest threats, and has received top effectiveness ratings in independent 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 registered

the FortiGate-VMX advanced security services are now enabled to secure traffic flowing to and from the VM at the hypervisor level. The following illustration shows how VMX registers with the NSX the Security Service:



FORTIGATE-VMX SERVICE MANAGER REGISTRATION FLOW

1. FortiGate-VMX Service Manager registers the Fortinet security service with NSX Manager via the NetX management plane API.

2. The NSX Manager collects the FortiGate-VMX image and auto-deploys an instance of FortiGate-VMX on each ESXi host in the designated cluster(s).

3. The FortiGate-VMX initiates a connection to the FortiGate-VMX Service Manager to register with the Service Manager and obtain its license.

4. FortiGate-VMX Service Manager verifies the serial number and synchronizes configuration and policy.

5. For all objects secured in the cluster, a redirection policy for all traffic to FortiGateVMX is installed.

6. 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.

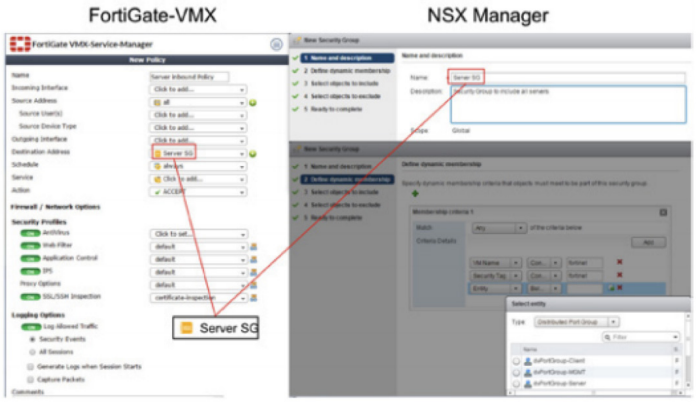
Security Groups, Security Tags

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 or modified, any VMs matching the parameters defined in the Security Group are automatically added to the Security Group. Without VMware NSX, this would be a painstaking process requiring manual intervention on every VM.

These Security Groups are automatically synced real time between the FortiGate-VMX Service Manager and the NSX Manager, ensuring that the FortiGate-VMX always has the most up to date group information.

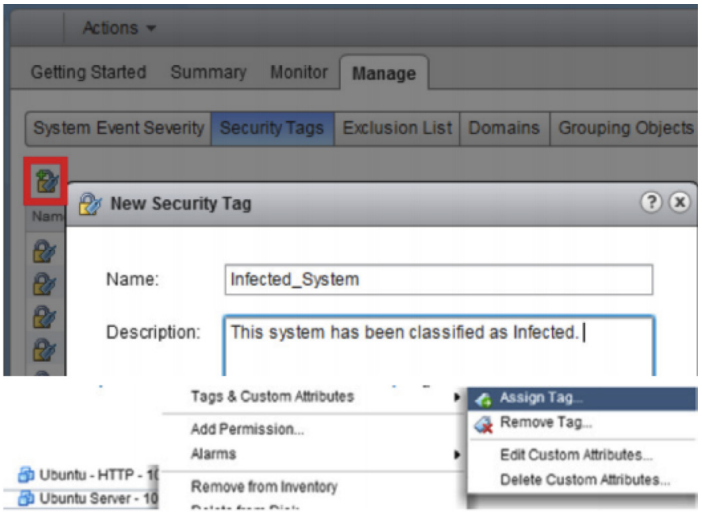


ADDING SECURITY GROUPS ON NSX AND CREATING POLICY ON FORTIGATE-VMX

SECURITY TAGS

VMware NSX also allows the creation of Security tags that can be assigned to individual 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.

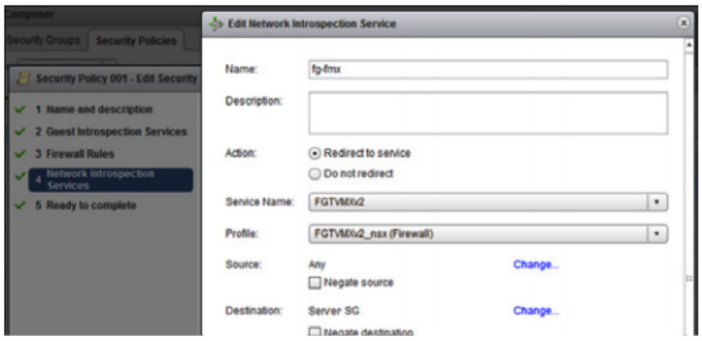
This Security Group membership information will also be synchronized real-time with the FortiGate-VMX Service Manager.



VMWARE NSX ADDING TAGS | ASSIGNING TAG SCREENSHOT

SERVICE PROFILE

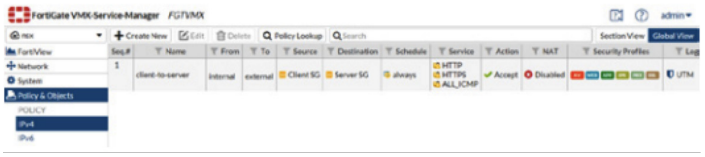
When the FortiGate-VMX Service Manager has registered with the VMware NSX Manager, NSX can be configured to use FortiGate-VMX as a Network Introspection Service. Once such a policy is configured, any traffic to a Security Group will automatically be redirected to a FortiGate-VMX Security Node.



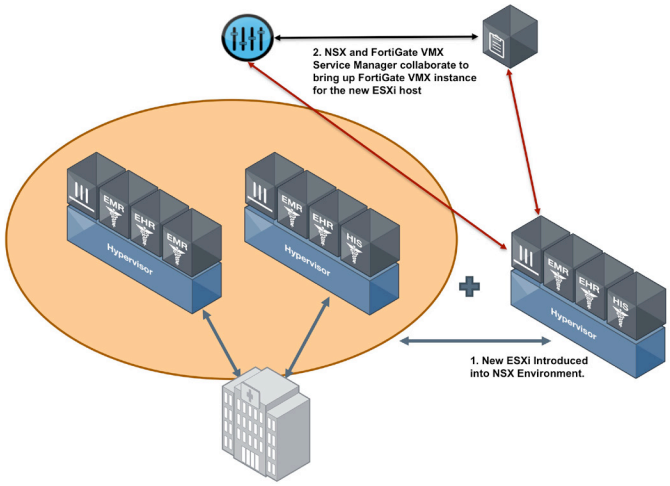
CONFIGURING REDIRECTION TO A FORTIGATE-VMX SERVICE

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.



FORTIGATE-VMX SERVICE MANAGER CREATE SECURITY POLICY SCREENSHOT



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.

Healthcare Reference Architecture

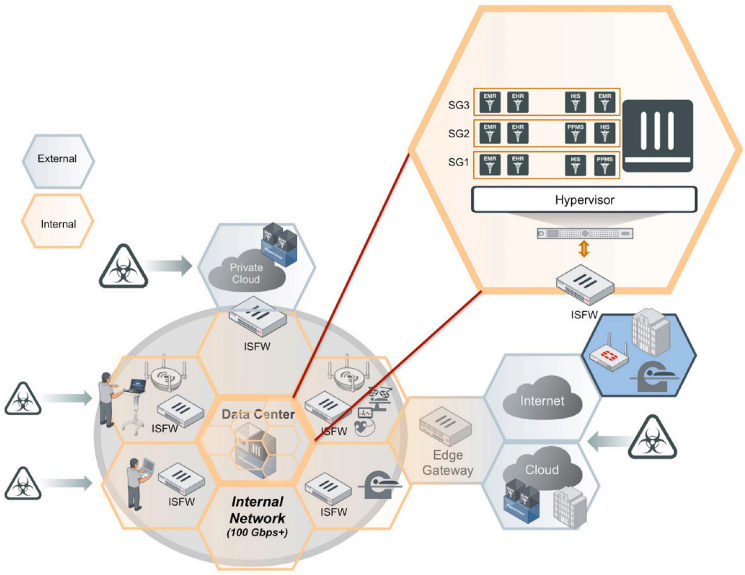
Below is a healthcare specific reference architecture for a VMware NSX and Fortinet FortiGate-VMX Integrated solution. This reference architecture involves integrating three concepts into a hospital based data center solution. These include internal segmentation, multi-tiered application threat defense, and finally, multi-tenancy utilizing NSX profiles and FortiGate VDOMS. Each will be explained below to further strengthen the security offering available through an NSX integrated solution.

INTERNAL SEGMENTATION FIREWALL FOR SDDC

Advanced Threats are taking advantage of the flat Internal Network commonly found throughout healthcare environments. Once through the border defense, there is little to stop their spread and eventual extraction of valuable targeted assets like Protected Health Information and Personally Identifiable Information.

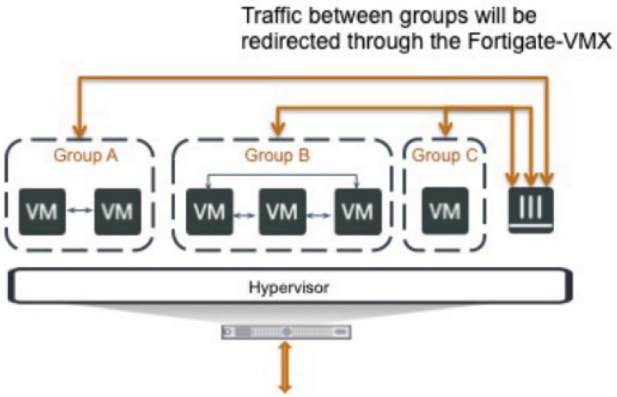
Because traditional Firewalls have been architected to slower speeds of the Internet Edge, it's hard to deploy these security devices internally as Internal Segmentation Firewalls (ISFW). On the physical network, ISFWs sit at strategic points of the internal network providing effective Secure Network Segmentation and preventing the spread of malicious applications.

The ISFW may sit in front of specific servers that contain valuable patient information or clinical data or a set of patient interfacing devices or web applications sitting in the cloud. Fortinet's ISFW utilize custom ASIC-accelerated hardware to provide these high speed NGFW capabilities, even on modern multi-gigabit network backbones. The ISFW principle can also be extended into the Software Defined Data Center. With VMware NSX and FortiGate-VMX integration, we can provide that same NGFW/ISFW functionality between VMs within the NSX infrastructure.



EXTENDING INTERNAL SEGMENTATION FIREWALL USING FORTIGATE-VMX

By creating Security Groups for related devices within the network, Healthcare Systems are able to define smaller trust groups, which can then be protected using the FortiGate-VMX Security Node. This brings Internal Segmentation Firewalls deeper into the Data Center creating a micro-segmentation environment, and protects against threats spreading through these smaller groups within the network.



MICRO-SEGMENTATION TO IMPLEMENT VIRTUAL INTERNAL SEGMENTATION FIREWALL

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 HL7 Brokers, EHR Databases, Radiology Systems, or HIS Systems. Group B could be a healthcare specific web application used by a particular physician practice. Group C could include hosted services from a healthcare vendor to support medical devices within the hospital infrastructure. We would define 3 Security Groups for this:

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

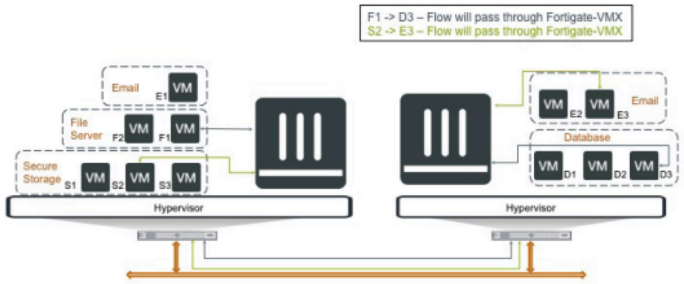
Group B – Internal group for internally accessible Data

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

By utilizing micro-segmentation, 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 healthcare applications would be in distinct virtual networks. Using VMware NSX and FortiGate-VMX, we can define micro-segments such that Services requiring different levels of protection can be protected with the appropriate Security Policies.



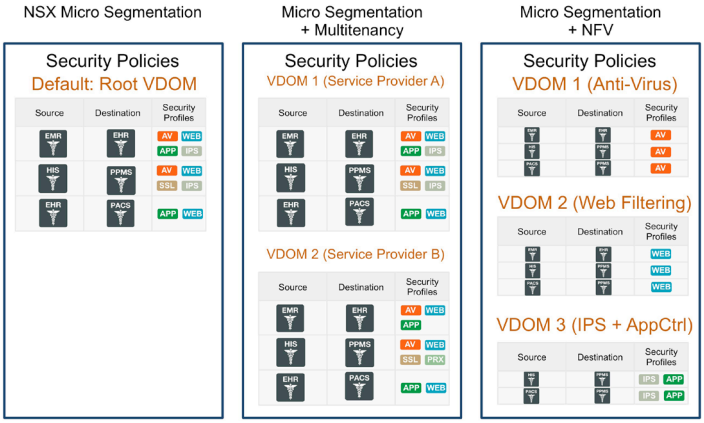
MICRO-SEGMENTATION AND MULTI-TIERED APPLICATION THREAT DEFENSE

This can be effectively set up by configuring Security Groups for each application type. Once this is done, the FortiGate-VMX can be configured with the relevant Security policies for each group. NSX will then automatically redirect the traffic to the FortiGate-VMX based on the Security Group. 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 in the diagram above, 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. Traffic between Email servers E1, E2 and E3 will not be redirected to the FortiGate-VMX allowing for rapid, unimpeded synchronization of email.

VDOMS WITH NSX SERVICE PROFILES

Fortinet is the only security vendor that can support Virtual Domains (VDOMs) in NSX. This capability allows IT 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 the Healthcare Enterprise as seen in the sample Security Policy configurations below. We will look at one use case for each segment.

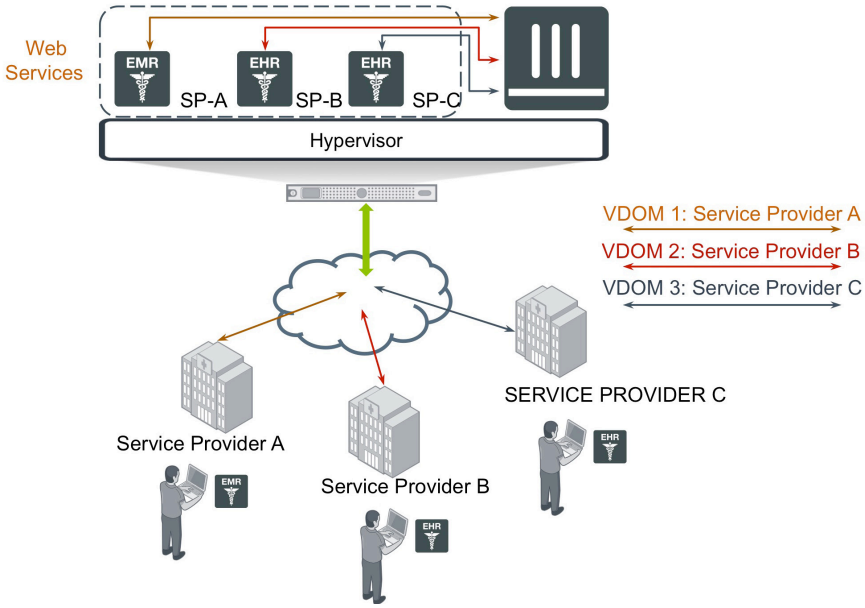


FLEXIBILITY PROVIDED BY VDOM CONFIGURATIONS WHEN USED WITH NSX MICRO SEGMENTATION

MULTITENANCY USING VDOMS AND NSX SERVICE PROFILES

In this example, an enterprise healthcare system provides an infrastructure hosting web services to physician practices and ancillary companies. The healthcare system would have a Security Group defined for web services. 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 to manage and control their own practice management system. 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

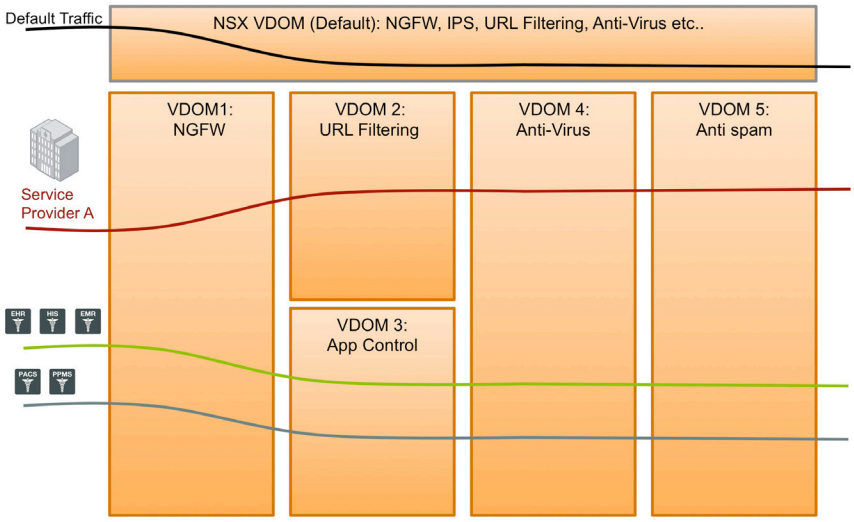
across the enterprise system. This deployment model reduces cost by removing the need to provide each tenant with their own FortiGate-VMX security service.



MULTI-TENANCY CONFIGURATION USING VDOMS AND NSX SERVICE PROFILES

HOSPITAL ENTERPRISE: NFV USING VDOMS AND NSX SERVICE PROFILES

In this example, an enterprise healthcare customer has different VDOMs configured to handle different Security features. Consider the case where an organization has multiple applications hosted in the data center. As in most cases, these applications have very different security requirements; for instance, all applications may require NGFW Services, but only Application Server A requires URL Filtering and Application Servers B and C need application control and so on. Here VMware NSX Service Policies will be used to ensure that the workloads are each in the correct Security Groups.



NETWORK FUNCTION VIRTUALIZATION USING VDOMS AND NSX SERVICE PROFILES

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 within a healthcare enterprise environment. This solution is an ideal fit for scale up and scale out scenarios including healthcare applications and hospital platforms that need a more layered security implementation. This helps segregate virtual network traffic and isolate access to authorized entities within the enterprise. VMware NSX and FortiGate-VMX together ensure that any new workloads introduced are dynamically adjusted to support any changes which 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 meet the extreme security needs of increasingly targeted healthcare environments, while making data center security management both simple and more efficient.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

May 31, 2016