WHITE PAPER – **OCTOBER 2017**

FORTINET VMX WITH VMWARE NSX

Deployment Use Cases

vmware®

Table of Contents

Introduction

This document is intended for IT administrators and security architects who specialize in cloud and virtualization in the Software-Defined Data Center (SDDC). It focuses on deployment of Fortinet's next-generation firewall and UTM (unified threat management) into the VMware NSX® platform and environment. It also covers advanced security solutions, differentiators, and use cases. It does not attempt to cover architectural design decisions, installation and deployment, or automation and orchestration details using the VMware NSX API™.

As VMware NSX matures into production environments, network and security architects are looking to operationalize NSX with more advanced security and manageability. Fortinet's FortiGate-VMX solution programmatically integrates directly with the latest NSX API to provide industry-leading firewall and UTM functionality as a service into SDDC deployments.

Fortinet's security framework embraces and delivers advanced security for the VMware SDDC with key features of automation and orchestration, agility, OpEx cost reduction, provisioning, and deployment at scale.

Fortinet's FortiGate-VMX security solution provides visibility and real-time protection against potential vulnerabilities. The joint solution provides the following:

- Introspection for east-west traffic between virtual machines (VMs)
- Automatic security node deployment for expanding workloads, reducing manual intervention and human error
- Service insertion and service chaining, which enable advanced layer 4-7 services
- Managed service and departmental segmentation through use of virtual domains (VDOMs)
- Full next-generation security solution in one integrated platform

As with previous versions of FortiGate-VMX, the solution can be automatically and transparently deployed on every ESXi hypervisor added to an NSX deployed cluster. The latest security policies are dynamically applied to all ESXi hosts in the cluster. These policies are also inherited during VM migration and resource balancing.

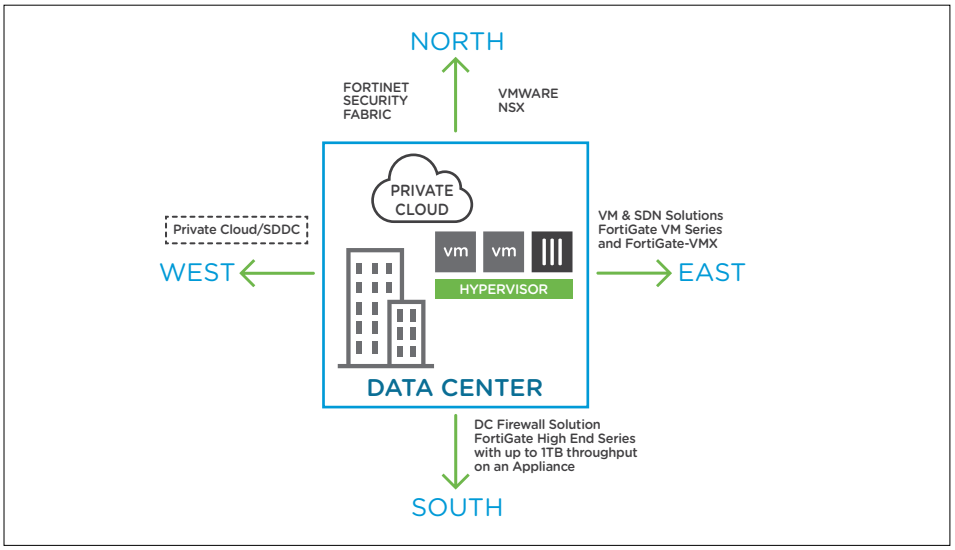

Figure 1: VMware NSX with FortiGate-VMX

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 traffic hairpinning, where flows would otherwise have to leave the virtual environment to be processed by a hardware appliance.

VMware NSX Overview

IT organizations have gained significant benefits through server virtualization. Server consolidation reduces physical complexity, increases operational efficiency, and provides the ability to dynamically repurpose underlying resources to quickly and optimally meet the needs of increasingly dynamic business applications. The SDDC architecture is extending virtualization technologies across the entire physical data center infrastructure. VMware NSX, the network virtualization platform, now delivers for networking what vSphere® has delivered for compute and storage. In much the same way that server virtualization enables the programmatic creation, deletion, and changes of software-based VMs, NSX programmatically creates, deletes, and changes software-based virtual networks. The result is a transformative approach to networking that not only enables data center managers to achieve better agility and economics by orders of magnitude, but also allows for a simplified operational model for the underlying physical network. Because it can be deployed on any IP network, including both existing traditional networking models and next-generation fabric architectures, NSX is a nondisruptive solution; the existing physical network infrastructure is all you need to deploy a Software-Defined Data Center.

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.

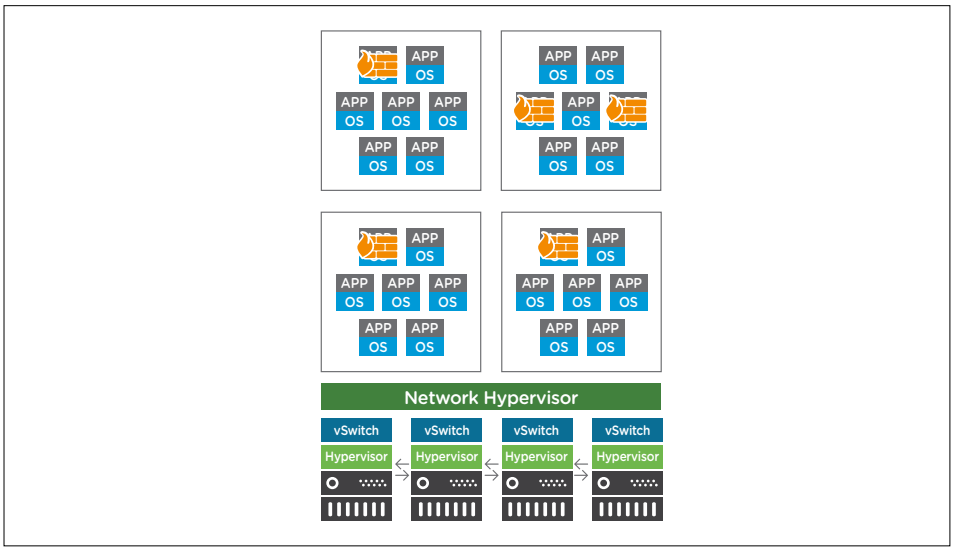

Figure 2: NSX, the Network Hypervisor

Just as VMs are independent of the underlying x86 platform and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware and allow IT to treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand. Unlike legacy architectures, virtual networks can be provisioned, changed, stored, deleted, and restored programmatically without reconfiguration of the underlying physical hardware or topology. By matching the capabilities and benefits derived from familiar server and storage virtualization solutions, this transformative approach to networking unleashes the full potential of the SDDC.

An NSX deployment consists of a data plane, control plane, and management plane.

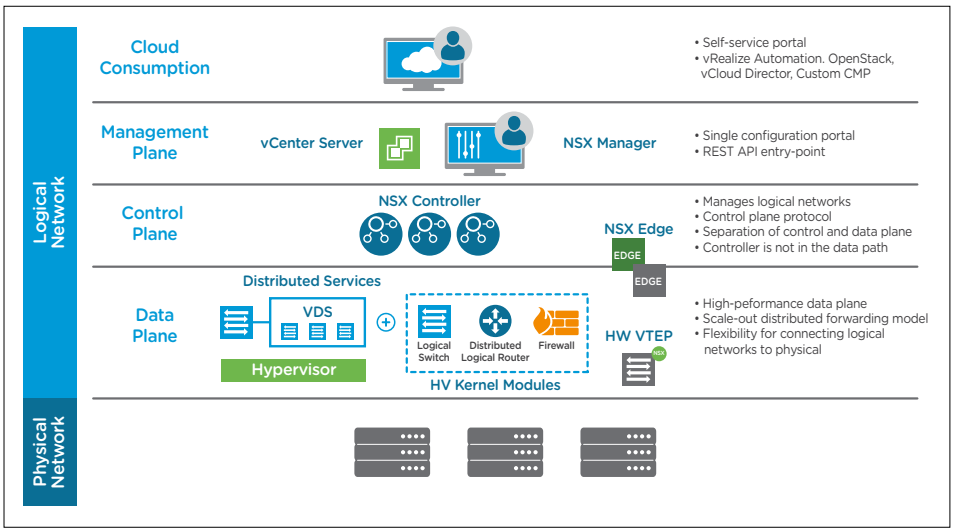

Figure 3: NSX Components

Data Plane

The NSX data plane consists of the NSX vSwitch. The vSwitch in NSX for vSphere is based on the vSphere 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 and 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. Here are some of the benefits of the NSX vSwitch:

- 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 rearchitect any of the data center network.
  - 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.
- The NSX vSwitch provides distributed routing and a distributed firewall that scale out with 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 layer 3 (NSX routing).

The NSX distributed firewall provides layer 4 firewall functionality at the vNIC of every VM. Because dynamic policies based on tags and security groups are used, this allows zero trust micro-segmentation within the SDDC while remaining administratively manageable.

Control Plane

The NSX control plane runs in VMware NSX Controller™. In a VMware vSphere® optimized environment with VDS, 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 to enable high availability and scale.

Management Plane and Consumption Platforms

The NSX management plane is built by VMware NSX Manager™. NSX Manager provides the single point of configuration and the REST API. The consumption of NSX can be driven directly via the NSX Manager UI, which, in a vSphere environment, is available via the vSphere web UI. Typically, end users tie network virtualization into their cloud management platform for deploying applications. NSX provides a rich set of REST APIs for extensibility.

FortiGate-VMX Overview

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

There are two required components and an optional one 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 communication is two-way in that FortiGate-VMX Service Manager supplies service definitions to NSX Manager, while NSX Manager sends updates to 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 and VMware NSX provide a truly flexible and efficient data center architecture. By means of network and security virtualization, NSX can distribute layer 2 to layer 7 networking and security services, including routing, switching, firewalling, and load balancing.

FortiGate-VMX utilizes the 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.

Because network and security virtualization are combined through automation and orchestration with the NSX architecture, security can be enforced despite workload changes. Networks and network security can be remapped, adjusted, or expanded when workloads are migrated or changed.

Fortinet offers an integrated Segmentation Network Security solution for the entire network with one operating system: FortiOS. 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 industry tests: NSS Labs, VB100, and AV Comparatives.

Service Insertion

One of the key enablers of 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 can secure traffic flowing to and from the VM at the hypervisor level. Redirection is based on a traffic-steering policy, which should be designed to allow bulk protocols that have a low threat risk to bypass the FortiGate service.

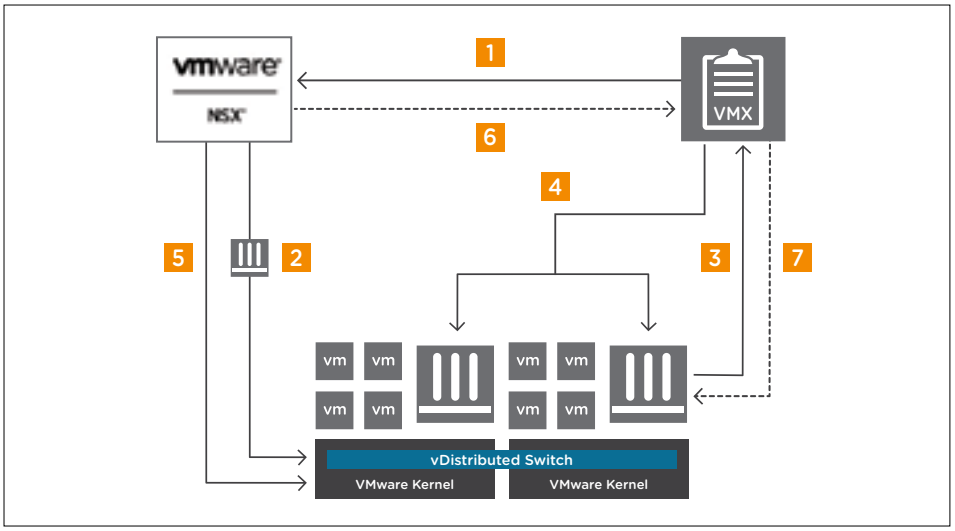

Figure 4: FortiGate-VMX Service Manager Registration Flow

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 bidirectional communication between FortiGate-VMX Service Manager and NSX Manager.
2. FortiGate-VMX is auto-deployed to all hosts in security cluster: NSX Manager collects the FortiGate-VMX image from the URL specified during registration and installs an instance of FortiGate-VMX on each VMware ESXi™ host in the designated clusters. The FortiGate-VMX image is very small (in the order of tens of megabytes), providing fast and efficient deployment to each host in the cluster.
3. FortiGate-VMX connects with FortiGate-VMX Service Manager: FortiGate-VMX initiates a connection to 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 are updated for enablement of FortiGate-VMX security service: For all objects secured in the cluster, a policy of redirection of specified traffic to FortiGate-VMX is ready.
6. Real-time updates of the object database: NSX Manager sends real-time updates on the changes in the virtual environment to FortiGate-VMX Service Manager.
7. FortiGate-VMX Service Manager dynamically synchronizes the object database and policy to all FortiGate-VMX virtual appliance instances deployed in the cluster.

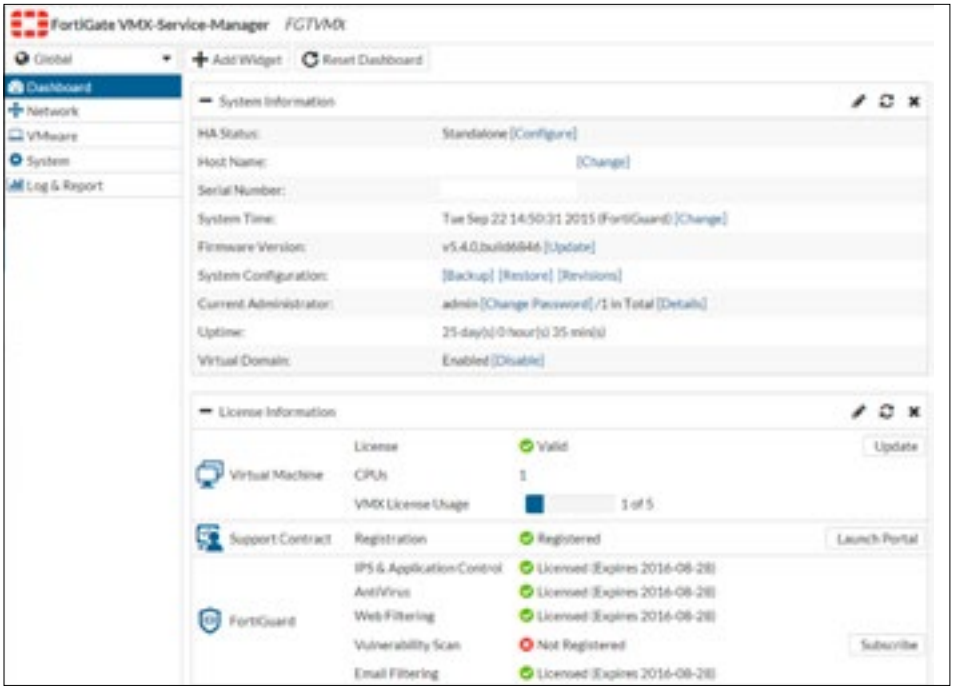

Figure 5: FortiGate-VMX Service Manager Console—Post-Registration

Security Groups, Security Tags

Security Groups

VMware Service Composer supports the configuration of security groups. These groups can be either static or dynamic and can be defined based on various parameters, such as security tags, VM names, dvPortGroups, VXLAN segments, and so on.

When a security group is created, VMs matching the parameters defined in the security group are automatically added to the security group. When any of these parameters is changed, the grouping for that VM is automatically re-evaluated. Without NSX integration, this would be a painstaking process that would need to be done manually.

Security groups are automatically synced between FortiGate-VMX Service Manager and NSX Manager.

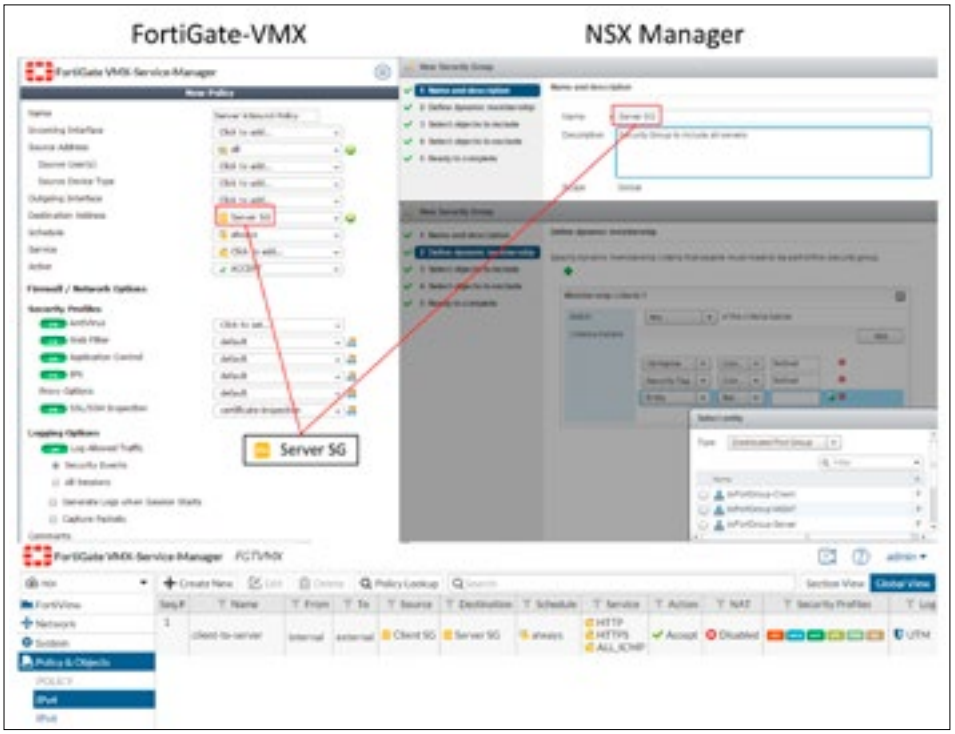

Figure 6: Adding Security Groups on NSX and Creating Policy on FortiGate-VMX

Security Tags

NSX allows the creation of security tags that can be assigned to VMs. This can be done programmatically or manually. Security tags can be used as classifiers to automatically assign all VMs with a tag to a specific security group.

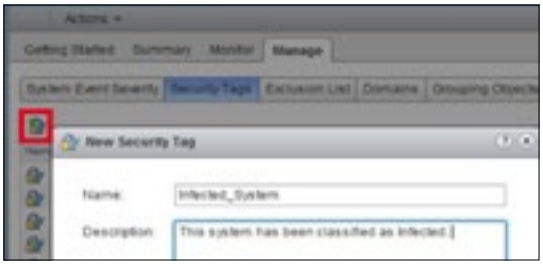

Figure 7: Adding a Security Tag in NSX

Figure 8: Adding a Security Tag in NSX

Figure 9: Adding a Security Tag in NSX

Figures 8 and 9 show the following flow:

1. A new tag is created for infected systems. This will be dynamically assigned to any systems detected as infected.
2. A security group is created; it dynamically includes all infected systems. If a VM is marked as an infected system with the tag just created, the VM becomes 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.
4. By doing this, we can exercise precise control over east-west traffic and prevent spreading of threats and infections laterally.

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

When FortiGate-VMX Service Manager has registered with 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 is automatically redirected to a FortiGate-VMX Security Node.

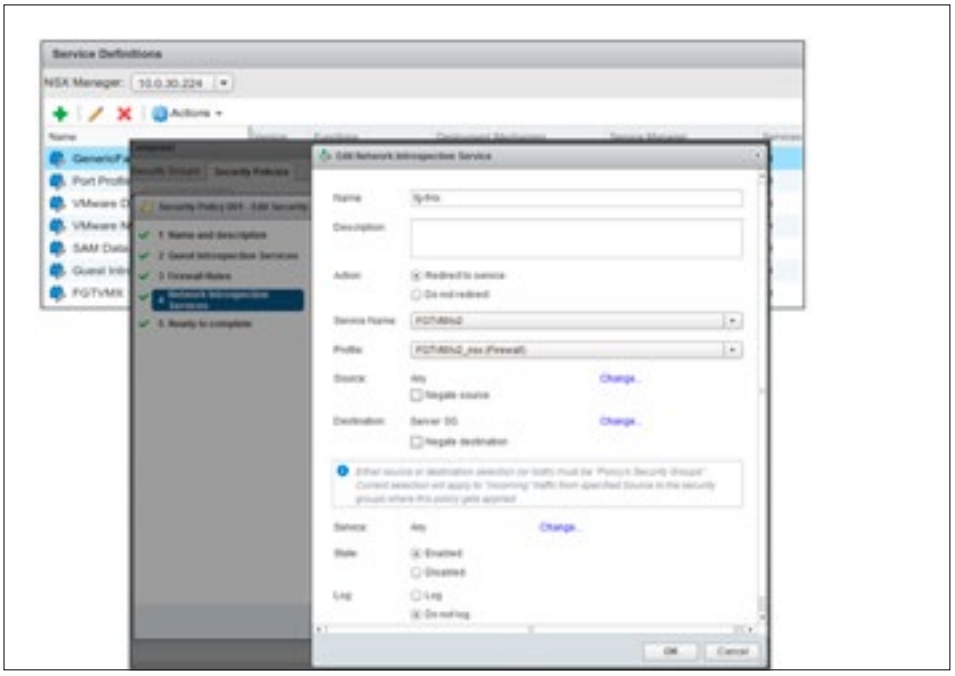

Figure 10: Configuring Redirection to a FortiGate-VMX Service

Security Policy

Once a security group is configured and has been synced to FortiGate-VMX Service Manager, this security group is automatically made available for consumption in security policies.

Figure 11: Creating a Security Policy in FortiGate-VMX Service Manager

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

Virtual Domains

Virtual domains (VDOMs) are a method of dividing a single FortiGate-VMX instance into multiple virtual units that function as individual security nodes.

Multitenancy Using Fortinet VDOMs

Beyond the flexibility provided by NSX Manager, FortiGate-VMX also supports multiple VDOMs. A FortiGate-VMX instance 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. The VDOMs are completely segregated and can be managed independently of each other. See the use case section for a more detailed example.

Network Functions Virtualization (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.

For enterprise customers, VDOMs can be used to split the different security functions, such as anti-virus, IPS, and application control. A more detailed example is seen in the use case section.

Use Cases

The following sections describe three use cases for the NSX and FortiGate-VMX integrated solution.

Internal Segmentation Firewall for the SDDC

Advanced threats are taking advantage of the flat internal network. Once they get through the border defense, there is little to stop their spread and eventual extraction of valuable targeted assets. Because traditional firewalls have been limited to the slower speeds of the Internet edge, it has been expensive 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 in the cloud.

Fortinet has an array of existing hardware FortiGates that provide high-speed next-generation firewall functionalities and thus facilitate deployment of firewalls between the network segments. By extending the ISFW principle into the SDDC with the NSX and FortiGate-VMX integration, we can provide firewall functionality between the VMs.

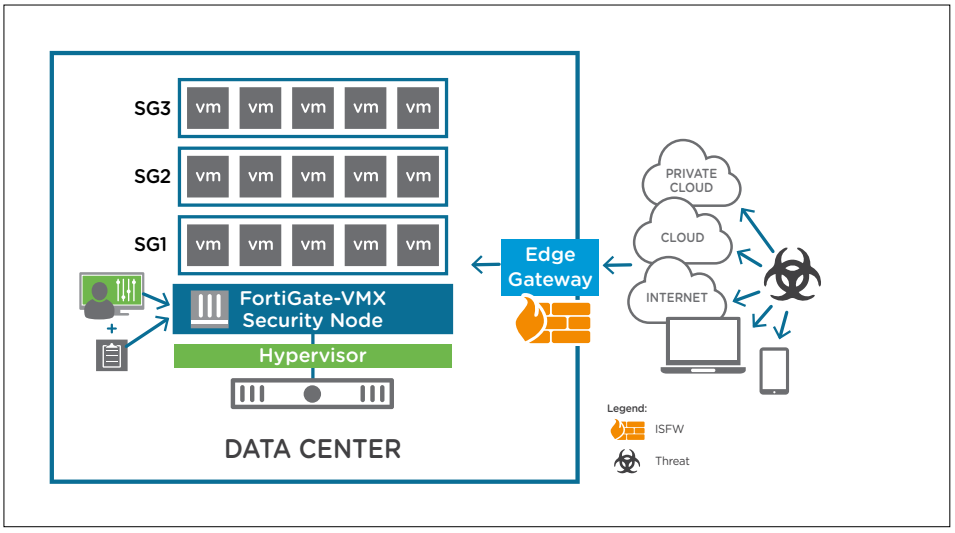

Figure 12: Extending the Internal Segmentation Firewall Using FortiGate-VMX

By creating security groups for related devices within the network, we can define smaller trust groups that can then be protected using a firewall. This protects against threats spreading across these smaller groups within the network. As a result, we can bring the advantages of Internal Segmentation Firewalls deeper into the data center by protecting traffic between individual VMs.

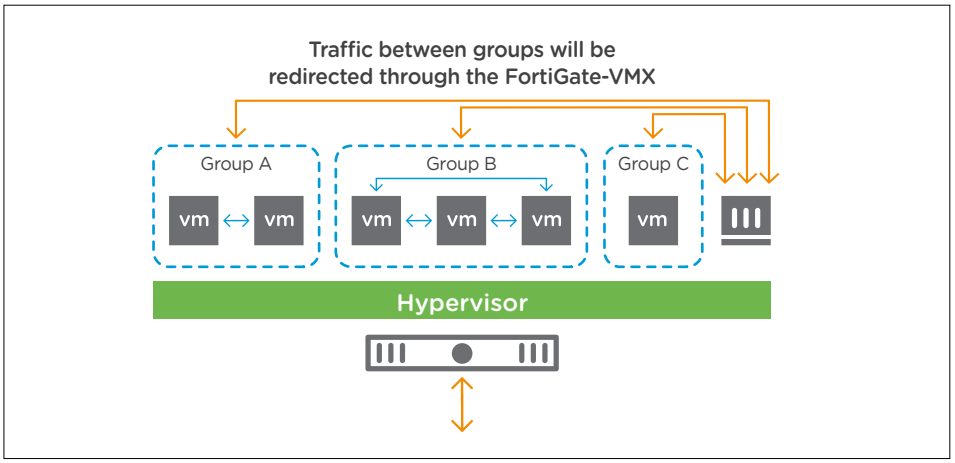

Figure 13: Micro-Segmentation to Implement a Virtual Internal Segmentation Firewall

Groups A, B, and C can be used to define the smaller security groups. For instance, group A might be all the organization's internal service servers, such as HR databases and other highly secure devices. Group B might be hosted services for employee use—company email, central storage for intellectual property. Group C might include hosted web services provided by the company, such as the company web page and other externally exposed services.

We would define three 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 and machines visible to the outside world

By using ISFW principles, threats that might have penetrated one network can be prevented from reaching other parts of the trusted network.

Multitiered Application Threat Defense

Traditionally, to provide threat defense to different applications, the network needs to be segmented such that the different applications are in distinct virtual networks. Using NSX and FortiGate-VMX, we can define micro-segments so that services requiring different levels of protection can be covered by the appropriate security policy.

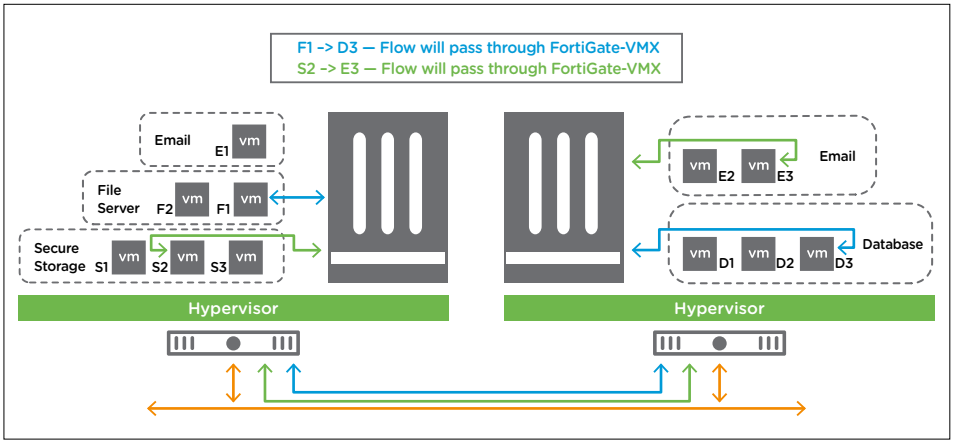

Figure 14: Micro-Segmentation and Multitiered Application Threat Defense

This can be effectively set up by statically or dynamically configuring security groups for each application type. Then FortiGate-VMX can be configured with the relevant security policies for each group.

NSX then automatically redirects the traffic to FortiGate-VMX. For instance, FortiGate-VMX sees all traffic bound to email server group devices unless the traffic originates from an email server group device.

Figure 14 shows this in the green flow. Because E3 is an email server and S2 is a secure storage server, FortiGate-VMX sees this traffic and applies relevant policies on it. Similarly, traffic from file server F1 to database D3 flows through FortiGate-VMX.

As in the previous case, using NSX with FortiGate-VMX helps secure east-west traffic as well as north-south traffic.

VDOMs with NSX Service Profiles

Fortinet VDOMs allow network administrators to segment a single FortiGate-VMX Security Node to service different flows separately from each other.

This valuable feature provides greater flexibility for both enterprise and managed service providers, as shown in the sample security policy configurations in Figure 15.

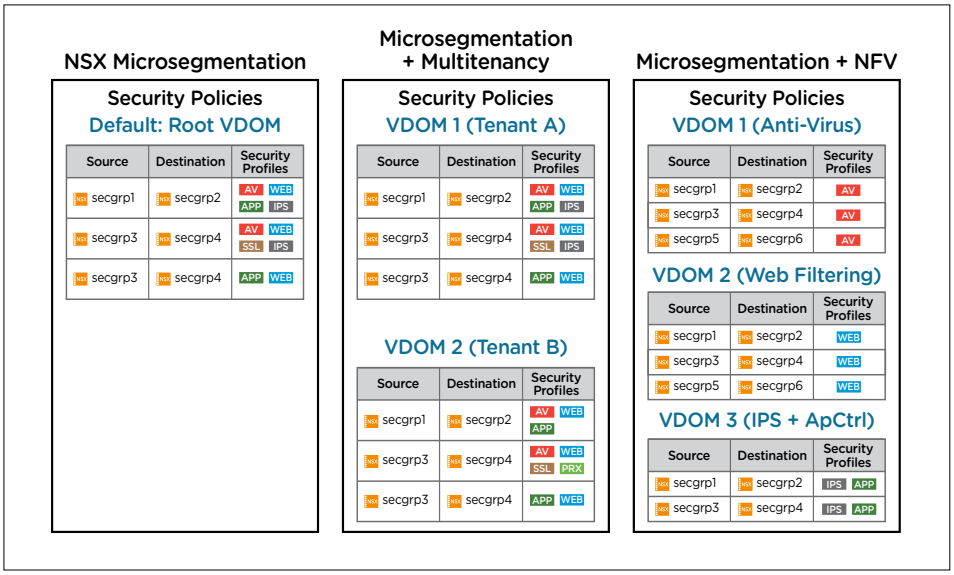

Figure 15: Flexibility Provided by VDOM Configurations When Used with NSX Micro-Segmentation

MSSP: Multitenancy Using VDOMs and NSX Service Profiles

In this example (Figure 16), a managed service security provider (MSSP) provides an infrastructure hosting web services to its tenants.

The provider has a security group for web services (and potentially other security groups for each different service offered). Security policies assigned for traffic to and from this group are redirected to the FortiGate-VMX Security Node. FortiGate-VMX Service Manager in turn has three separate VDOMs configured—one for each tenant—over which the corresponding tenant has full autonomy.

Here, the three tenants—orange, blue, and red—are all protected using the same FortiGate-VMX Security Node, yet are completely separate from one another, and each has autonomy over its 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 its own FortiGate-VMX security service. It also enables tenants to extend their VDOM configurations from parallel hardware deployments.

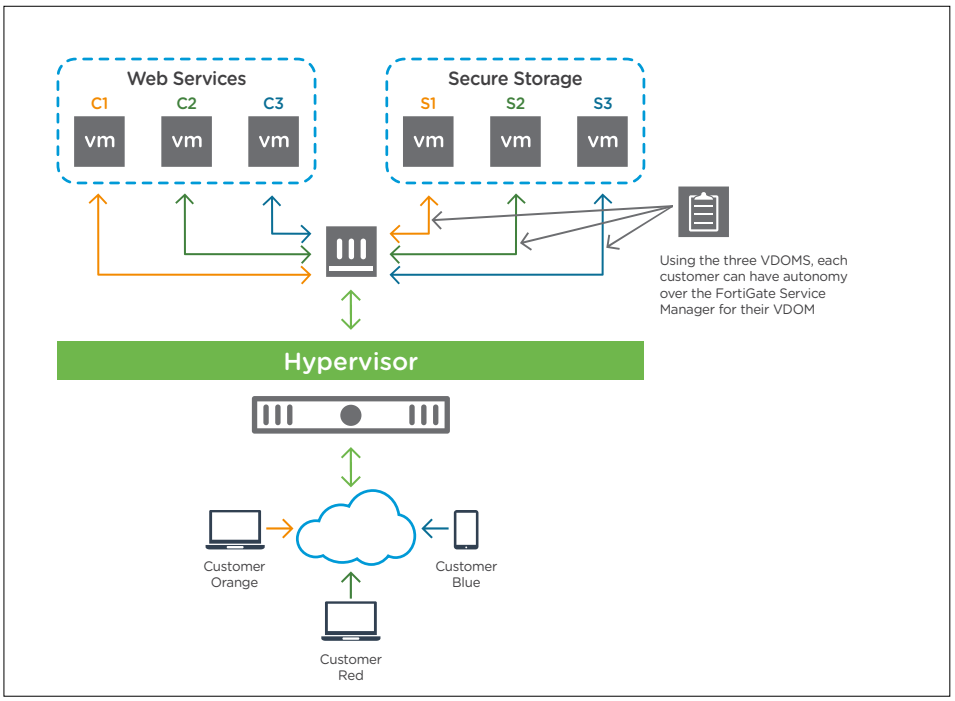

Figure 16: Multitenancy Configuration Using VDOMs and NSX Service Profiles

Enterprise: NFV Using VDOMs and NSX Service Profiles

In this example (Figure 17), an enterprise customer has different VDOMs configured to handle different security features. The company has multiple applications hosted in the data center, and these applications have different security requirements. For instance, all applications might require next-generation firewall services, but only application server A requires URL filtering, only application servers B and C need application control, and so on.

Here, NSX service policies are used to ensure that the workloads are each in the correct security groups.

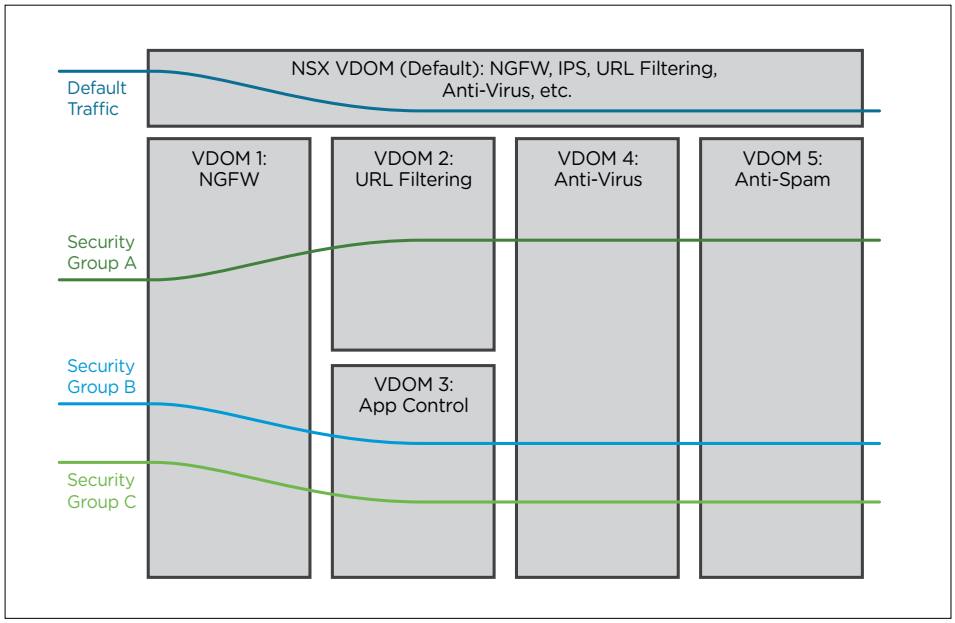

Figure 17: NFV Using VDOMs and NSX Service Profiles

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 NSX with FortiGate-VMX security solution joins 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 threat visibility and protection for both east-west and north-south traffic.

This solution is especially ideal for scale-up and scale-out scenarios. NSX and FortiGate-VMX ensure that new workloads and changes to existing workloads are automatically provided with FortiGate-VMX's security service.

With the automation and orchestration capabilities provided by the NSX API and the FortiGate single pane of glass visibility and control, this solution provides extremely effective security while making data center security management simpler and more efficient.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com