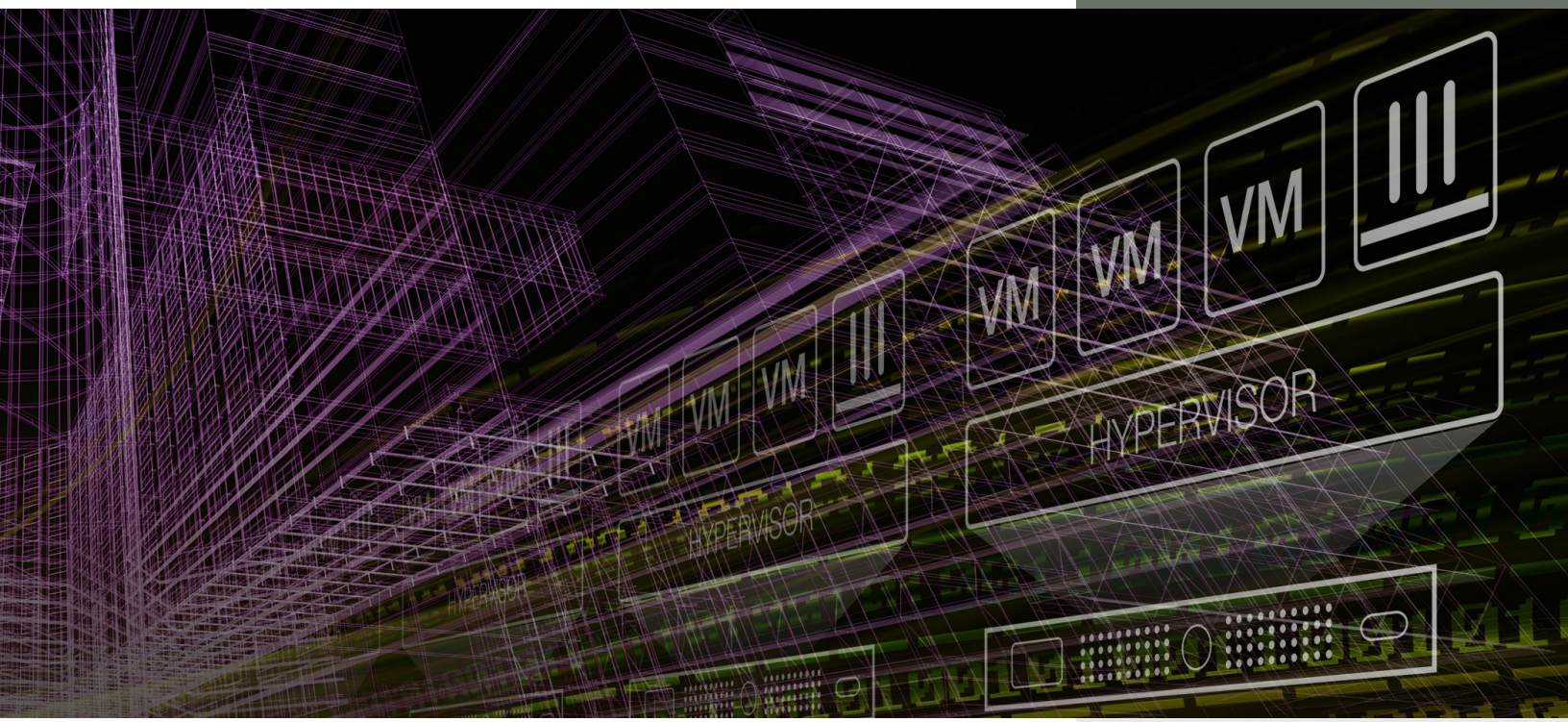


Automating Advanced Security for the Software Defined Data Center

With the growing investment in virtualization; data centers are becoming home to increasing volumes of data and applications. Data center security is proving to be a foundational design aspect when it comes to building the Data Center of today. Most common data center security architectures today 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 as once in, threats then have unrestricted access to the whole datacenter. The solution is to protect by controlling traffic as it flows east to west within the datacenter. Another key pain point seen in the deployment phase is the need for manual intervention when it comes to deploying and managing an ever-expanding datacenter with resulting in costly mistakes and in the slowing of growth and expansion.

A Software Defined Data Center (SDDC) approach enables fundamentally better data center security. Fortinet leverages VMware NSX, the network virtualization pillar of the SDDC, to fully automate FortiGate-VMX 2.0 for advanced protection of server-server traffic inside the data center.

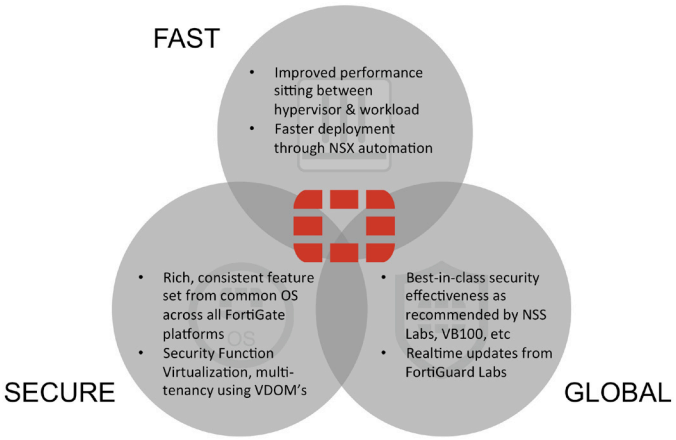
NSX enables FortiGate-VMX security nodes to be automatically provisioned and deployed to each ESXi and allows effective automated configuration of security policies per workload for maximum consistency and visibility into threats while reducing error-prone manual intervention.

Benefits

- Automated deployment and orchestration of FortiGate-VMX for Software Defined Data Centers
- Operationally feasible NSX-based micro-segmentation with advanced threat protection of East-West traffic
- 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

FortiGate-VMX v2.0 further 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.

The solution is part of the VMware NSX partner ecosystem and extends the NSX distributed firewalling capability with Fortinet's advanced firewall. FortiGate-VMX features can be updated in real time with FortiGuard advanced threat intelligence.



Automated Provisioning and Orchestration via VMware NSX

In VMware NSX-enabled datacenters, FortiGate-VMX deployments are fully automated to address elastic workloads and constantly changing (e.g. resizing) ESXi clusters. Policy is dynamically synchronized with all FortiGate-VMX instances in the complete security cluster. The solution supports re-balancing of workloads in the ever-changing environment (e.g., support for vMotion and full DRS clusters).

The NSX distributed firewall is a stateful firewall that runs in the kernel and does L2-L4 traffic filtering. NSX enables policy to be applied at the vNIC or virtual layer and intercepts traffic at the hypervisor level not allowing any workload to by-pass inspection. The NSX firewall steers traffic selectively to FortiGate-VMX based on policy for advanced traffic inspection.

Persistent Security Utilizing VMware NSX Micro-Segmentation

VMware NSX provides inherent network isolation and a "honeycomb" of trust zones to make micro-segmentation easier than ever before. IT administrators can describe the service functions and workload characteristics to designate proper security policies for app, web or data tiers by asking questions like "What will this workload be used for?" "Who can access the workload?" "What is the data sensitivity zoning for each workload?" Micro- segmentation merges these characteristics to define inherited policy attributes as they are added to the security cluster, without the need to configure firewall rules and complex access control policies.

This granular and layered approach to security policy filtering and mapping workload characteristics allows administrators to segment a single policy into sub-policies, and create a network segment to apply security rules. It also provides the East-West inter-VM traffic visibility in the SDDC.

Secure VXLAN Segments with Advanced Protection Across Tiers

To enable communication between Web, App, and Data tiers,VMware utilizes the logical routing function in NSX to create a single logical router instance across distributed switches. In the NSX enabled security cluster, the distributed firewall (DFW) module redirects traffic to a FortiGate-VMX firewall for threat inspection. Security policies defined in the FortiGate-VMX Service Manager are enforced based on workload segments.

Multi Tenancy using Virtual Domains

With Fortinet's patented Virtual Domain(VDOM) Technology, FortiGate-Service Manager supports the use of multiple VDOMS to allow for effective segmentation between tenants while allowing each Tenant complete administrative autonomy over their segment. Fortinet's virtual portfolio is the only virtual security solution today to support this.

Tenant Function Segmentation with Virtual Domains

Using VDOMs, enterprises are able to apply more effective security policies by segmenting them across both separate departments and application types. This allows the administrator to apply targeted policies tailored to each domain while improving the overall performance of the system. This also provides for unmatched visibility across the network.

Security Orchestration and Automated Provisioning with VMware NSX

The VMware NSX network virtualization platform provides a distributed service framework to enable partner services like FortiGate-VMX to be dynamically inserted, deployed and orchestrated. NSX enables fully automation of FortiGate-VMX inside the data center perimeter.

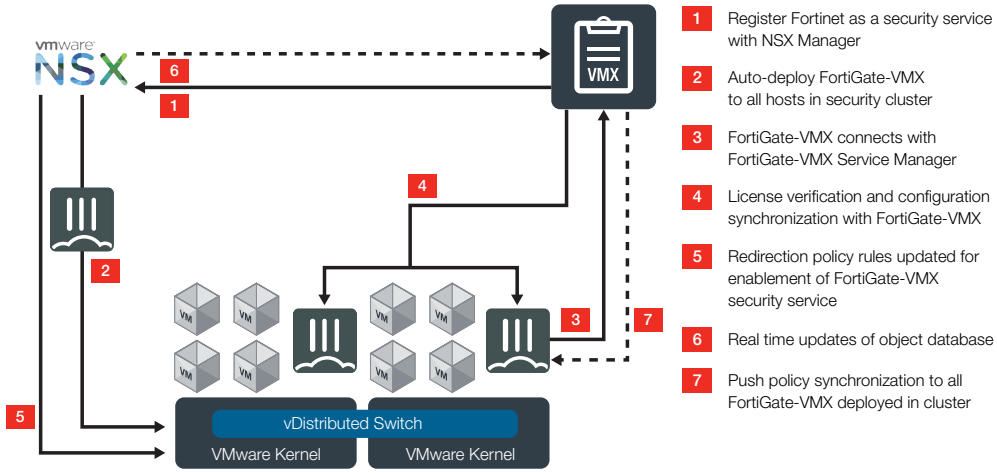
There are two main components in the solution:

- 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 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

FortiGate-VMX Service Manager communicates directly with the NSX environment. It registers the FortiGate-VMX security service to allow for enablement and 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.



Summary

FortiGate-VMX v2.0 integrated with VMware NSX solution extends the NSX firewall functionality with advanced security services and allows IT to unlock all the benefits of the software defined data center with agility and efficiency. IT organizations can automatically provision the delivery of best-in- class security services from Fortinet where management plane, control plane and data plane work seamlessly in lockstep.

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

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

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

Oct 8, 2015