DATA SHEET

FortiGate®-VMX

Extensible Security Controls for VMware Environments

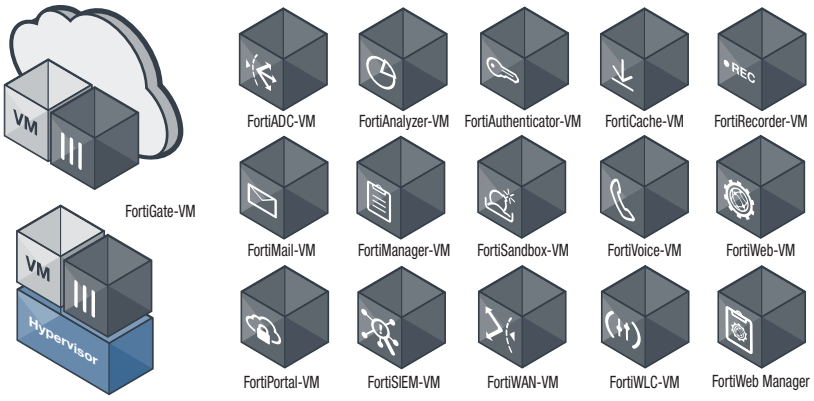
Next Generation Firewall

FortiGate-VMX is a specific security solution for VMware environments that provides purpose-built integration for VMware's Software-Defined Data Center (SDDC) — encompassing interoperability with VMware NSX and vSphere. Through direct API integration, FortiGate-VMX has visibility into and can secure virtualized network traffic at the hypervisor level.

Automated deployment and management orchestration are used to secure workloads in dynamic software-defined networks and infrastructure to enable protection and close compliance gaps.

Proven Success in Virtual Environments

Fortinet introduced virtual domain (VDOM) technology in 2004. Since that time, we have offered virtualized security solutions to service providers and enterprises alike. With the initial release of the FortiGate-VM virtual appliance form factor in 2010, Fortinet paved a path of greater choice and flexibility to customers by providing the ability to deploy our security solutions within existing virtualized and Cloud infrastructure.

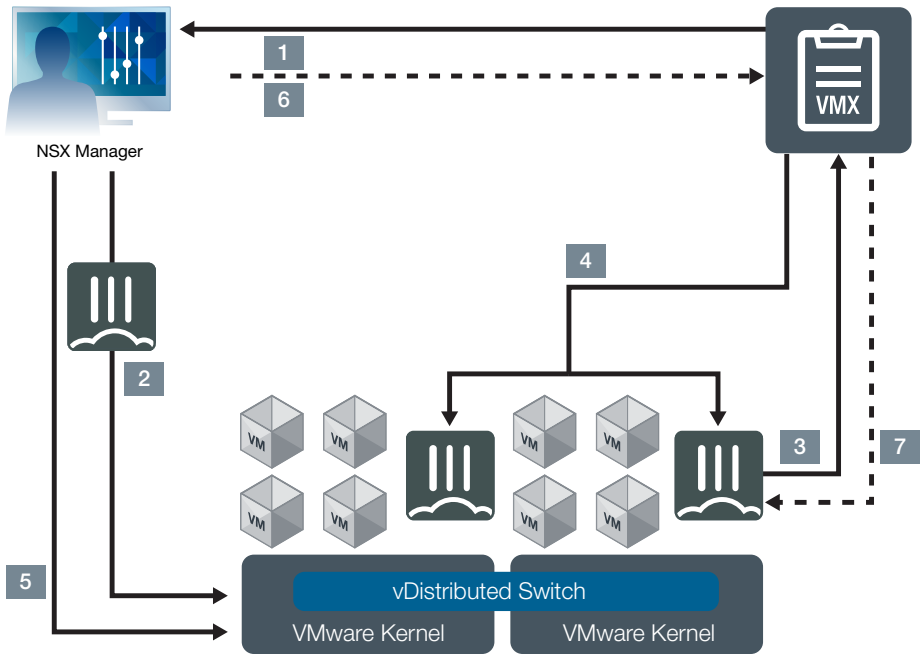


Growing from that first successful launch, Fortinet now offers 16+ virtualized security solutions for VMware environments — FortiGate-VMX spearheading that portfolio.

Highlights

- Visibility into all vSphere virtual network traffic
- Automated deployment and provisioning of FortiGate-VMX security nodes to new ESXi hosts
- Instant-on real-time protection of new VM workloads
- Session-state retained across live migration events (vMotion)
- Support for multi-tenant environments
- Full Next Generation security functionality solution in one platform Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement

DEPLOYMENT



1. Register FortiGate-VMX 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 in NSX
6. Real-time updates of object database
7. Push policy synchronization to all FortiGate-VMX deployed in cluster

1. Register FortiGate-VMX as a security service

The registration process uses the NetX (Network Extensible) management plane API to enable bidirectional communication between the FortiGate-VMX Service Manager and NSX Manager.

2. Auto-deploy of FortiGate-VMX to all ESXi hosts in the 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 cluster.

3. Connection is established between FortiGate-VMX and the FortiGate-VMX Service Manager

FortiGate-VMX initiates a connection to the FortiGate-VMX Service Manager to obtain license information.

4. Configuration synchronization of FortiGate-VMX

The FortiGate-VMX Service Manager verifies FortiGate-VMX status and synchronizes the configuration.

5. Redirection rules enabled

NSX Network Introspection Service Security Policy rules are enabled to redirect all designated communication flows to FortiGate-VMX for securing of traffic.

6. Real-time updates of objects

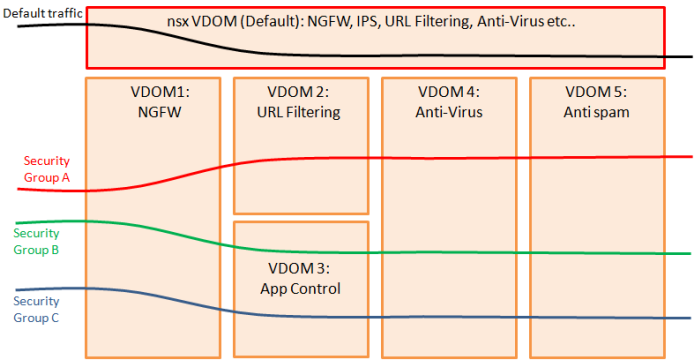
NSX Manager sends real-time updates on changes in the virtual environment to the FortiGate-VMX Service Manager

7. Policy synchronization to all FortiGate-VMX instances deployed in the ESXi cluster

Newly created security policies are pushed to all FortiGate-VMX security nodes. Every FortiGate-VMX deployed in the cluster will have the same set of policies.

Virtual Segmentation Function

Extending Fortinet's VDOM technology into FortiGate-VMX allows for segmentation of security functions and enablement of multi-tenancy. Mapping NSX Service Profiles to Fortinet VDOMs segregates policies to be enforced for specific traffic flows. This model reduces the added complexity of registering a specific security solution for each tenant hosted in the environment.



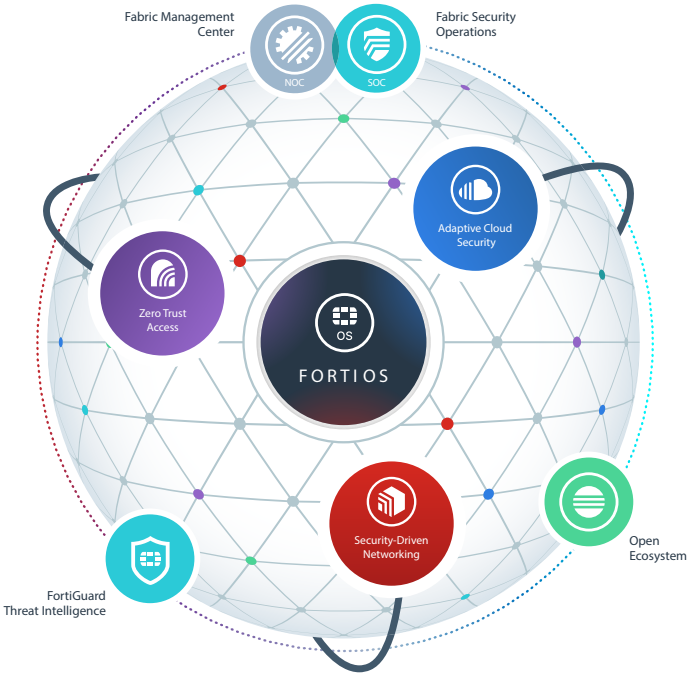
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad**: Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated**: Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated**: Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

SOLUTION

Visibility

Unlike traditional deployments where the security virtual appliance is required to be in the flow of traffic to enforce policy, FortiGate-VMX can see traffic as it traverses between the virtual switch port and the virtual NIC (vNIC) of the workload VM itself.

Automated Deployment and Provisioning

FortiGate-VMX Service Manage talks directly with VMware's NSX Manager to communicate information about and register the Fortinet security service. The VMware environment then automates the deployment of FortiGate-VMX Security Nodes to each VMware ESXi host in the designated cluster. Licensing and security policy is also automated between the FortiGate-VMX Service Manager and the FortiGate-VMX Security Nodes.

Object-based Protection

FortiGate-VMX security policy is based on dynamic NSX Security Groups and their associated objects. Any additions or other changes to these Security Groups in the NSX Manager will be automatically associated with the proper FortiGate-VMX security policy without requiring any manual changes in the FortiGate-VMX Service Manager. Policies are enforced independent of broadcast domain or port connection. Policy will also follow the workload VM from host to host during live migration (vMotion) events.

Policy Redirection

Through integration with VMware NSX APIs and NSX Service Composer, custom redirection security policies enable application traffic flow to/from specific VM workload within the designated ESXi cluster(s) to be secured by the FortiGate-VMX security service. No manual configuration of network flows are required.

Real-time Protection

With policies based on NSX dynamic Security Groups, new VM workloads are automatically associated to their proper security policy in real-time upon creation. No more lag-time between creation and enforcement or mistakes commonly associated with communication between data center administrators and security administrators.

Cluster-based Scaling

Because FortiGate-VMX is a security service within the VMware environment, any new hosts added to the secure ESXi cluster will immediately fall under the same security policy. FortiGate-VMX security nodes will automatically deploy to those new ESXi hosts without any manual intervention.

Summary

Using the advanced FortiOS™ operating system, FortiGate appliances effectively neutralize a wide range of security threats facing your software defined datacenter (SDDC). Whether deployed at the edge as a front-line defense (FortiGate hardware appliances), within the virtual infrastructure for inter-zone security and VPN termination at the application (FortiGate-VM) or utilized for inter-VM and advanced hypervisor-based security (FortiGate-VMX), FortiGate appliances protect your infrastructure with some of the most effective security available today.

SPECIFICATIONS

SOLUTION		VERSION SUPPORT	
Fortinet			
	FortiGate-VMX Service Manager	v5.6.3	v6.0.1+
	FortiGate-VMX Security Node	v5.6.3	v6.0.1+
	FortiAnalyzer (Optional)	v5.6.0+	v6.0.1+
VMware			
	NSX	6.2.4+ / 6.3.0+ / 6.4.0	6.3.0+ / 6.4.0+ (up to 6.4.6)
	ESXi	5.5 / 6.0 / 6.5	6.0 / 6.5 / 6.7 (7.0 is not supported)

For up-to-date compatibility matrix of all components listed above, visit the Fortinet section of the VMware Compatibility Guide.
FortiGate-VMX maintains a carrying-forward compatibility with the subsequent versions after certification. For example, if FortiGate-VMX 6.0.1 was certified with VMware NSX, 6.0.1+ (such as 6.0.2 and 6.0.3) on the same 6.0 line is supported and works with VMware NSX, unless mentioned otherwise.
Check supported version compatibility of FortiAnalyzer that works with certain FortiGate versions. "FortiOS" is the operating system used on FortiGate-VMX.
https://docs.fortinet.com/document/fortianalyzer/6.0.0/compatibility-with-fortios

PERFORMANCE REFERENCE

FORTIGATE-VMX			
Technical Specifications			
vCPU Support (Minimum / Maximum)	1 / Unlimited	v5.6.3	v6.0.1+
Memory Support (Minimum)	2 GB	v5.6.3	v6.0.1+
Virtual Domains (Default / Maximum)	10 / 250	v5.6.0+	v6.0.1+
Firewall Policies (VDOM / System)	50,000 / 100,000		
System Performance	**2 vCPU**	**4 vCPU**	**8vCPU**
Concurrent Sessions (TCP)		RAM Dependent (No Limit)	
New Sessions/Second (TCP)	48,600	49,000	49,000
Firewall Throughput (HTTP 1MB)	14.4 Gbps	14.8 Gbps	15.2 Gbps
IPS Throughput (HTTP 1MB)	6.6 Gbps	9.6 Gbps	13.0 Gbps
IPS Throughput (Enterprise Mix)	2.4 Gbps	4.1 Gbps	6.6 Gbps
Application Control Throughput (HTTP 64KB)	2.8 Gbps	4.7 Gbps	8.0 Gbps
NGFW Throughput (Enterprise Mix)	2.1 Gbps	3.4 Gbps	6.0 Gbps
Threat Protection Throughput (Enterprise Mix)	1.9 Gbps	3.0 Gbps	5.4 Gbps

Specification is measured on a Dell PowerEdge R740 server (CPU Intel® Xeon® Gold 6136 CPU @ 3.00 GHz), Testing tool: Two pairs of BPS VE 8.4 using FortiGate VMX 6.0.2, VMware NSX 6.4.0, ESXi v6.5.0.

ORDERING INFORMATION

Product	SKU	Description
FortiGate-VMX Service Manager	FG-VMX-MGMT	FortiGate-VMX Service Manager for VMware NSX environments.
FortiGate-VMX Security Node	FG-VMX-1	One (1) FortiGate-VMX instance for VMware NSX environments.

ORDERING INFORMATION

Product	SKU	Description
FortiGate-VMX Service Manager	FG-VMX-MGMT	FortiGate-VMX Service Manager for VMware NSX environments.
FortiGate-VMX Security Node	FG-VMX-1	One (1) FortiGate-VMX instance for VMware NSX environments.

BUNDLES

FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•
FortiGuard IPS Service	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•
FortiGuard Web and Video[1] Filtering Service	•	•	
FortiGuard Antispam Service	•	•	
FortiGuard Security Rating Service	•		
FortiGuard IoT Detection Service	•		
FortiGuard Industrial Service	•		
FortiConverter Service	•		

1. Available when running FortiOS 7.0

FORTINET®

www.fortinet.com