FortiGate®-VMX

Extensible Security Controls for VMware Environments

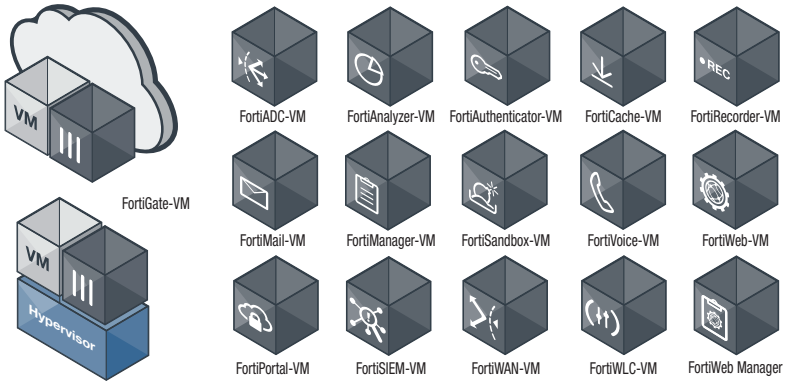
FortiGate-VMX is a specific security solution for VMware environments that provides purpose-built integration for VMware's Software-Defined Data Center (SDDC) — encompassing interoperability with VMware NSX and vSphere. Through direct API-integration, FortiGate-VMX has visibility into and can secure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

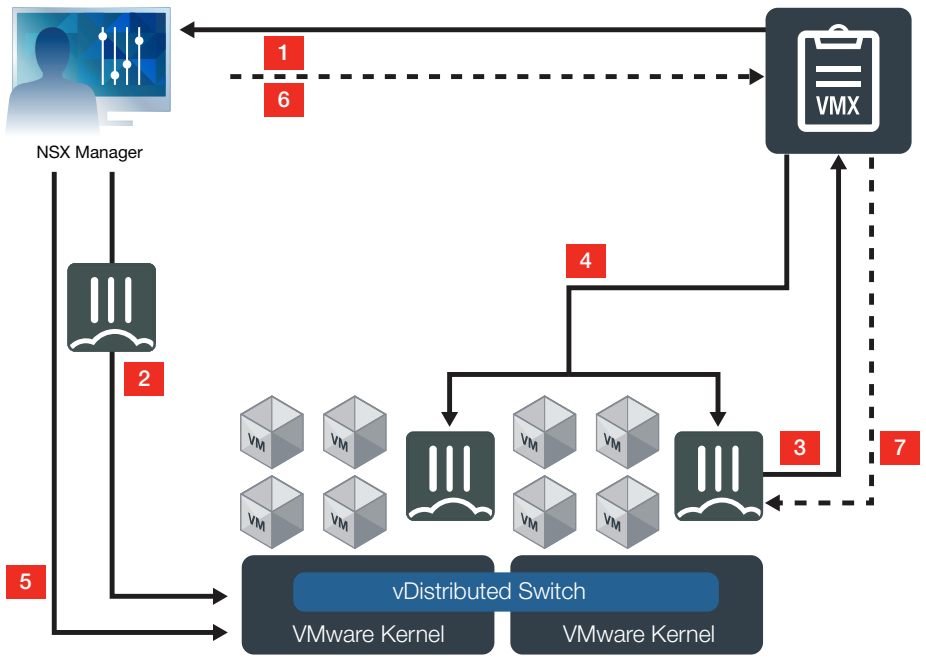


Fortinet comprehensive virtual appliance offerings

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

DEPLOYMENT

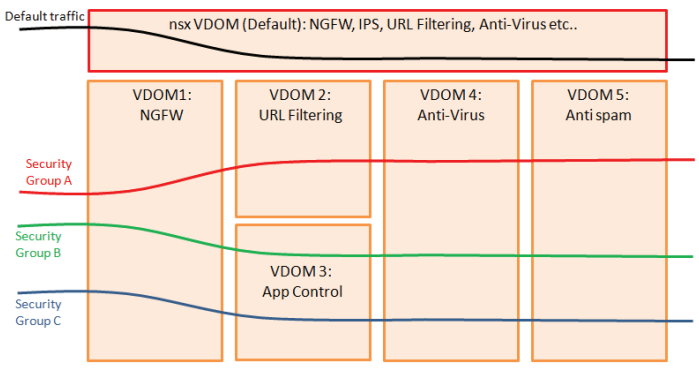


1. Register FortiGate-VMX security service with NSX Manager
2. Auto-deploy FortiGate-VMX to all hosts in security cluster
3. FortiGate-VMX connects with FortiGate-VMX Service Manager
4. License verification and configuration synchronization with FortiGate-VMX
5. Redirection policy rules updated in NSX
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. **Re-direction 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

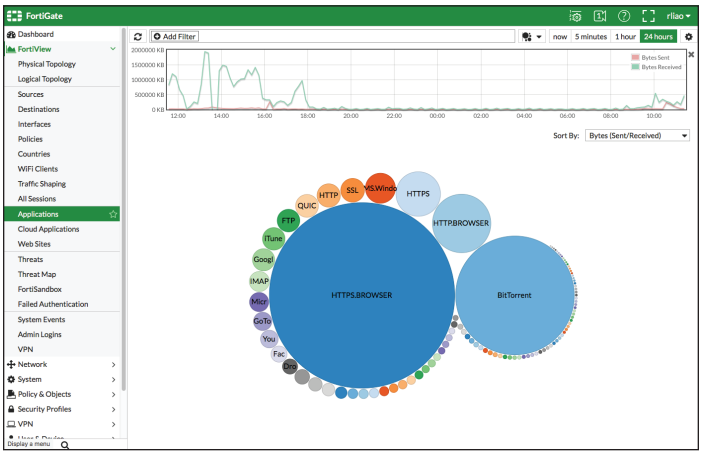
Extending Fortinet's Virtual Domain technology into FortiGate-VMX allows for segmentation of security functions and enablement of multi-tenancy. Mapping NSX Service Profiles to Fortinet VDOMs segregates policies to be enforced for specific traffic flows. This model reduces the added complexity of registering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



SOFTWARE

FortiOS

Control all the security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce operating expenses and save time with a truly consolidated next generation security platform.



- A truly consolidated platform with one OS for all security and networking services for all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives and ICSA validated security and performance.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings.
- Detect, contain and block advanced attacks automatically in minutes with integrated advanced threat protection framework.
- Solve your networking needs with extensive routing, switching, WiFi, LAN and WAN capabilities.
- Activate all the SPU-boosted capabilities you need on the fastest firewall platform available.

For more information, please refer to the FortiOS data sheet available at www.fortinet.com

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, other network and security vendors, as well as law enforcement agencies:

- **Real-time Updates** — 24x7x365 Global Operations research security intelligence, distributed via Fortinet Distributed Network to all Fortinet platforms.
- **Security Research** — FortiGuard Labs have discovered over 170 unique zero-day vulnerabilities to date, totaling millions of automated signature updates monthly.
- **Validated Security Intelligence** — Based on FortiGuard intelligence, Fortinet's network security platform is tested and validated by the world's leading third-party testing labs and customers globally.

FortiCare™ Support Services

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East and Asia, FortiCare offers services to meet the needs of enterprises of all sizes:

- **Enhanced Support** — For customers who need support during local business hours only.
- **Comprehensive Support** — For customers who need around-the-clock mission critical support, including advanced exchange hardware replacement.
- **Advanced Services** — For global or regional customers who need an assigned Technical Account Manager, enhanced service level agreements, extended software support, priority escalation, on-site visits and more.
- **Professional Services** — For customers with more complex security implementations that require architecture and design services, implementation and deployment services, operational services and more.

Enterprise 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 the FortiGuard Enterprise Bundle. This bundle contains the full set of FortiGuard security services plus FortiCare service and support offering the most flexibility and broadest range of protection all in one package.

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
	FortiGate-VMX Security Node	v5.6.3
	FortiAnalyzer (Optional)	v5.6.0+
VMware		
	NSX	6.2.4+ /6.3.0+ /6.4.0
	ESXi	6.0/6.5

Note: For up-to-date compatibility matrix of all components listed above, please visit the Fortinet section of the VMware Compatibility Guide: https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=security&productid=44827&vcl=true

PERFORMANCE REFERENCE

	FORTIGATE-VMX		
Technical Specifications			
vCPU Support (Minimum / Maximum)	1 / Unlimited		
Virtual Domains (Default / Maximum)	10 / 250		
Firewall Policies (VDOM / System)	50,000 / 100,000		
Unlimited User License	Yes		
System Performance	**2 vCPU**	**4 vCPU**	**8 vCPU**
Concurrent Sessions (TCP)	RAM Dependent (No Limit)	RAM Dependent (No Limit)	RAM Dependent (No Limit)
New Sessions/Second (TCP)	50,000	50,000	
Firewall Throughput (HTTP 1M)	18 Gbps	18 Gbps	17.5 Gbps
IPS Throughput (HTTP / Enterprise Mix) [1]	7.3 / 2.3 Gbps	11 / 4 Gbps	13 / 5 Gbps
Application Control Throughput [2]	2.8 Gbps	5.4 Gbps	6 Gbps
NGFW Throughput [3]	2 Gbps	3.4 Gbps	4.7 Gbps
Threat Protection Throughput [4]	1.8 Gbps	3.1 Gbps	4 Gbps

Note: All performance values are "up to" and vary depending on system configuration. Specification is measured on a Dell PowerEdge R730 server with CPU Intel Xeon ES-2687W @ 3.10 GHz. VMware ESXi 6.5.0, NSX 6.4.0, FortiGate-VMX based on FortiOS 5.6. 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix. 2. Application Control performance is measured with 64 Kbytes HTTP traffic. 3. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 4. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.

ORDER 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.

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
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard
#12-01 Suntec Tower Three
Singapore 038988
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990