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
Deployment

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.
Fortinet Security Fabric

Security Fabric
The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric covers the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats

FortiOS
FortiGates are the foundation of the Fortinet Security Fabric—the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Leverage the latest technologies such as deception-based security.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection.
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation.
- Utilize virtual SPU hardware acceleration to boost network security performance.

Services

**FortiGuard™ Security Services**
FortiGuard Labs offer 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™ 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.

For more information, please refer to forti.net/fortiguard and forti.net/forticare
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 Manager 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

<table>
<thead>
<tr>
<th>SOLUTION</th>
<th>VERSION SUPPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td></td>
</tr>
<tr>
<td>FortiGate-VMX Service Manager</td>
<td>v6.0.3</td>
</tr>
<tr>
<td>FortiGate-VMX Security Node</td>
<td>v6.0.3</td>
</tr>
<tr>
<td>FortiAnalyzer (Optional)</td>
<td>v5.6.0+</td>
</tr>
<tr>
<td>VMware</td>
<td></td>
</tr>
<tr>
<td>NSX</td>
<td>6.2.4+ / 6.3.0+ / 6.4.0</td>
</tr>
<tr>
<td></td>
<td>6.3.0+ / 6.4.0+</td>
</tr>
<tr>
<td>ESXi</td>
<td>5.5 / 6.0 / 6.5</td>
</tr>
<tr>
<td></td>
<td>6.0 / 6.5 / 6.7</td>
</tr>
</tbody>
</table>

For up-to-date compatibility matrix of all components listed above, please visit the Fortinet section of the VMWare Compatibility Guide.

FortiGate-VMX maintains a carry-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

<table>
<thead>
<tr>
<th>SOLUTION</th>
<th>2 vCPU</th>
<th>4 vCPU</th>
<th>8vCPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Policies (VDOM / System)</td>
<td>10 / 100</td>
<td>10 / 100</td>
<td>10 / 100</td>
</tr>
<tr>
<td>System Performance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td>48,000</td>
<td>49,000</td>
<td>49,000</td>
</tr>
<tr>
<td>Firewall Throughput (HTTP 1MB)</td>
<td>14.4 Gbps</td>
<td>14.8 Gbps</td>
<td>15.2 Gbps</td>
</tr>
<tr>
<td>IPS Throughput (HTTP 1MB)</td>
<td>6.8 Gbps</td>
<td>9.6 Gbps</td>
<td>13.0 Gbps</td>
</tr>
<tr>
<td>IPS Throughput (Enterprise Mix)</td>
<td>2.4 Gbps</td>
<td>3.1 Gbps</td>
<td>5.6 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput (HTTP 64KB)</td>
<td>2.8 Gbps</td>
<td>4.7 Gbps</td>
<td>6.0 Gbps</td>
</tr>
<tr>
<td>NSFW Throughput (Enterprise Mix)</td>
<td>2.1 Gbps</td>
<td>3.4 Gbps</td>
<td>5.0 Gbps</td>
</tr>
<tr>
<td>Threat Protection Throughput (Enterprise Mix)</td>
<td>1.9 Gbps</td>
<td>3.0 Gbps</td>
<td>5.4 Gbps</td>
</tr>
</tbody>
</table>

Order Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate-VMX Service Manager</td>
<td>FG-VMX-MGMT</td>
<td>FortiGate-VMX Service Manager for VMware NSX environments.</td>
</tr>
<tr>
<td>FortiGate-VMX Security Node</td>
<td>FG-VMX-1</td>
<td>One (1) FortiGate-VMX instance for VMware NSX environments.</td>
</tr>
</tbody>
</table>