The FortiGate-VM on VMware ESXi delivers next generation firewall capabilities for organizations of all sizes. It protects against cyber threats with high performance, security efficacy, and deep visibility.

**Security**
- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

**Performance**
- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology with DPDK+vNP offloading and SR-IOV technologies
- Provides industry-leading performance and protection for SSL encrypted traffic

**Certification**
- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

**Networking**
- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources (only BYOL supports VDOM)
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

**Management**
- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

**Security Fabric**
- Enables Fortinet and Fabric-ready partners’ products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation
- Out-of-the-box integration and orchestration with leading SDN platforms

Fortinet’s comprehensive security virtual appliance lineup supports VMware ESXi
DEPLOYMENT

Next Generation Firewall (NGFW)

- Reduce complexity by combining threat protection security capabilities into single high-performance network security appliances
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Delivers the industry's highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- Proactively blocks newly discovered sophisticated attacks in real-time with advanced threat protection

TECHNOLOGIES

SR-IOV (Single Root I/O Virtualization)

In enabling SR-IOV on the KVM host, a single physical network controller can be partitioned into multiple virtual interfaces (called virtual functions (VFs)), consisting of an ESXi virtual network pool of adapters, which can be used by local host processors or directly by VMs like the FortiGate-VM. The VM then talks directly to the network adapters through Direct Memory Access (DMA) by bypassing virtualization transports, which improves north-south network performance.

Data Plane Development Kit (DPDK) and vNP Offloading

DPDK and vNP enhance FortiGate-VM performance by offloading part of packet processing to userspace while bypassing kernel within the operating system. You must enable and configure the capability with FortiGate CLI commands.
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.
# SPECIFICATIONS

<table>
<thead>
<tr>
<th>SPECIFICATIONS</th>
<th>FORTIGATE-VM01/01V/01S</th>
<th>FORTIGATE-VM02/02V/02S</th>
<th>FORTIGATE-VM04/04V/04S</th>
<th>FORTIGATE-VM08/08V/08S</th>
<th>FORTIGATE-VM16/16V/16S</th>
<th>FORTIGATE-VM32/32V/32S</th>
<th>FORTIGATE-VMUL/ULV/ULS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Specifications</td>
<td>vCPU Support</td>
<td>Minimum</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Memory Support (Minimum)</td>
<td>2 GB</td>
<td>2 GB</td>
<td>2 GB</td>
<td>2 GB</td>
<td>2 GB</td>
<td>2 GB</td>
</tr>
<tr>
<td></td>
<td>Network Interface Support (Minimum / Maximum)</td>
<td>1 / 24</td>
<td>1 / 24</td>
<td>1 / 24</td>
<td>1 / 24</td>
<td>1 / 24</td>
<td>1 / 24</td>
</tr>
<tr>
<td></td>
<td>Wireless Access Points Controlled</td>
<td>32 / 64</td>
<td>512 / 1,024</td>
<td>512 / 1,024</td>
<td>1,024 / 4,096</td>
<td>1,024 / 4,096</td>
<td>1,024 / 4,096</td>
</tr>
<tr>
<td></td>
<td>Storage Support (Minimum / Maximum)</td>
<td>32 GB / 2 TB</td>
<td>32 GB / 2 TB</td>
<td>32 GB / 2 TB</td>
<td>32 GB / 2 TB</td>
<td>32 GB / 2 TB</td>
<td>32 GB / 2 TB</td>
</tr>
<tr>
<td></td>
<td>Maximum Number of Registered Endpoints</td>
<td>2,000</td>
<td>2,000</td>
<td>8,000</td>
<td>20,000</td>
<td>20,000</td>
<td>20,000</td>
</tr>
<tr>
<td>System Performance</td>
<td>Firewall Throughput (UDP Packets)</td>
<td>12.0 Gbps</td>
<td>13.7 Gbps</td>
<td>19.1 Gbps</td>
<td>30.8 Gbps</td>
<td>36.0 Gbps</td>
<td>50.0 Gbps</td>
</tr>
<tr>
<td></td>
<td>New Sessions / Second (TCP)</td>
<td>45,000</td>
<td>100,000</td>
<td>125,000</td>
<td>150,000</td>
<td>150,000</td>
<td>150,000</td>
</tr>
<tr>
<td></td>
<td>IPsec VPN Throughput (AES256+SHA1, 512 Byte)</td>
<td>1.0 Gbps</td>
<td>1.5 Gbps</td>
<td>3.0 Gbps</td>
<td>5.5 Gbps</td>
<td>6.5 Gbps</td>
<td>7.0 Gbps</td>
</tr>
<tr>
<td></td>
<td>Client-to-Gateway IPsec VPN Tunnels</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
<td>2,000</td>
</tr>
<tr>
<td></td>
<td>SSL VPN Throughput</td>
<td>0.8 Gbps</td>
<td>0.83 Gbps</td>
<td>2.0 Gbps</td>
<td>4.5 Gbps</td>
<td>8.5 Gbps</td>
<td>8.6 Gbps</td>
</tr>
<tr>
<td></td>
<td>Concurrent SSL VPN Users (Recommended Maximum)</td>
<td>1,000</td>
<td>2,000</td>
<td>4,500</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>IPS Throughput (^a)</td>
<td>1.0 Gbps</td>
<td>2.0 Gbps</td>
<td>3.6 Gbps</td>
<td>7.2 Gbps</td>
<td>12.0 Gbps</td>
<td>19.0 Gbps</td>
</tr>
<tr>
<td></td>
<td>IPS HTTP 1M (^a)</td>
<td>3.5 Gbps</td>
<td>5.4 Gbps</td>
<td>8.8 Gbps</td>
<td>15.5 Gbps</td>
<td>25.0 Gbps</td>
<td>29.0 Gbps</td>
</tr>
<tr>
<td></td>
<td>Application Control Throughput (^a)</td>
<td>2.0 Gbps</td>
<td>2.7 Gbps</td>
<td>5.2 Gbps</td>
<td>10.2 Gbps</td>
<td>17.0 Gbps</td>
<td>17.5 Gbps</td>
</tr>
<tr>
<td></td>
<td>NGFW Throughput (^a)</td>
<td>0.85 Gbps</td>
<td>1.5 Gbps</td>
<td>2.9 Gbps</td>
<td>5.9 Gbps</td>
<td>9.0 Gbps</td>
<td>16.5 Gbps</td>
</tr>
<tr>
<td></td>
<td>Threat Protection Throughput (^a)</td>
<td>0.70 Gbps</td>
<td>1.2 Gbps</td>
<td>2.2 Gbps</td>
<td>4.5 Gbps</td>
<td>7.0 Gbps</td>
<td>13.0 Gbps</td>
</tr>
</tbody>
</table>

Note: All performance values are "up to" and vary depending on system configuration. Actual performance may vary depending on the network and system configuration. Note that these metrics are updated periodically as the product performance keeps improving through internal testing. The discrepancy in the performance numbers may be noted in different versions of the document so ensure that you refer to the latest datasheets. Performance metrics were observed using DELL R740 (CPU Intel Xeon Platinum 8168 @ 2.7 GHz, 96 cores, Intel X710 network adapters). DPDK numbers were measured on the special build of FOS v5.6, SR-IOV is enabled. Tested with VMware vSphere ESXi 6.5.0 Update 1. 1. Applicable to 6.4.0+. The actual working number of consumable network interfaces varies depending on VMware ESXi instance types/sizes and may be less. 2. FG-VMxxV and FG-VMxxS series do not come with a multi-VDOM feature by default. 3. FG-VMxxV and FG-VMxxS series do not come with a multi-VDOM feature by default. 4. Application Control performance is measured with 64 Kbyte HTTP traffic. 5. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 6. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
## SPECIFICATIONS

<table>
<thead>
<tr>
<th>Technical Specifications</th>
<th>FORTIGATE-VM02/02V/02S</th>
<th>FORTIGATE-VM04/04V/04S</th>
<th>FORTIGATE-VM08/08V/08S</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU Support (Minimum / Maximum)</td>
<td>1 / 2</td>
<td>1 / 4</td>
<td>1 / 8</td>
</tr>
<tr>
<td>Memory Support (Minimum)</td>
<td>2 GB</td>
<td>2 GB</td>
<td>2 GB</td>
</tr>
<tr>
<td>Network Interface Support (Minimum / Maximum)</td>
<td>1 / 24</td>
<td>1 / 24</td>
<td>1 / 24</td>
</tr>
<tr>
<td>Storage Support (Minimum / Maximum)</td>
<td>32 GB / 2 TB</td>
<td>32 GB / 2 TB</td>
<td>32 GB / 2 TB</td>
</tr>
<tr>
<td>Wireless Access Points Controlled</td>
<td>512 / 1,024</td>
<td>512 / 1,024</td>
<td>1,024 / 4,096</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>10,000</td>
<td>10,000</td>
<td>200,000</td>
</tr>
<tr>
<td>Maximum Number of Registered Endpoints</td>
<td>2,000</td>
<td>8,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Unlimited User License</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Performance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall Throughput (UDP Packets)</td>
<td>56.3 Gbps</td>
<td>80.0 Gbps</td>
<td>80.0 Gbps</td>
</tr>
<tr>
<td>IPSec VPN Throughput (AES256+SHA1, 512 Byte)</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>IPS HTTP 1M Throughput 7</td>
<td>10.5 Gbps</td>
<td>18.0 Gbps</td>
<td>32.0 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>4.0 Gbps</td>
<td>7.4 Gbps</td>
<td>12.5 Gbps</td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>1.9 Gbps</td>
<td>3.6 Gbps</td>
<td>6.5 Gbps</td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>1.5 Gbps</td>
<td>3.0 Gbps</td>
<td>5.6 Gbps</td>
</tr>
</tbody>
</table>

Note: All performance values are "up to" and vary depending on system configuration. Actual performance may vary depending on the network and system configuration. Please note that these metrics are updated periodically as the product performance keeps improving through internal testing. The discrepancy in the performance numbers may be noted in different versions of the document so please make sure to refer to the latest datasheets.

Performance metrics were observed using a DELL R740 (CPU Intel Xeon Platinum 8168 @ 2.7 GHz, 96 cores, Intel X710 network adapters). DPDK numbers were measured on the special build of FOS v5.6. SR-IOV is enabled. Tested with VMware vSphere ESXi 6.5.0 Update 1.

1. Applicable to 6.4.0+. The actual working number of consumable network interfaces varies depending on VMware ESXi instance types/sizes and may be less.
2. FG-VMxxV and FG-VMxxS series do not come with a multi-VDOM feature by default. You can add it by applying separate VDOM addition perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. It is highly recommended to allocate as much RAM size as the licensed limit for maximum performance. V6.2.3 GA supports DPDK and no longer restricts RAM sizes by licenses.
4. DPDK+vNP offloading does not support encrypted traffic. It is recommended to disable the DPDK option or adopt non-DPDK+vNP builds in using IPSec-VPN and SSL-VPN features. See Non-DPDK section for the performance data.
5. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
6. Application Control performance is measured with 64 Kbyte HTTP traffic.
7. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
8. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.

For the sizing guide, please refer to the sizing document available on [www.fortinet.com](http://www.fortinet.com)
## ORDERING INFORMATION

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate-VM01</td>
<td>FG-VM01, FG-VM01V</td>
<td>FortiGate-VM 'virtual appliance': 1x vCPU core. No VDOM by default for FG-VM01V model.</td>
</tr>
<tr>
<td>FortiGate-VM02</td>
<td>FG-VM02, FG-VM02V</td>
<td>FortiGate-VM 'virtual appliance': 2x vCPU cores. No VDOM by default for FG-VM02V model.</td>
</tr>
<tr>
<td>FortiGate-VM04</td>
<td>FG-VM04, FG-VM04V</td>
<td>FortiGate-VM 'virtual appliance': 4x vCPU cores. No VDOM by default for FG-VM04V model.</td>
</tr>
<tr>
<td>FortiGate-VM08</td>
<td>FG-VM08, FG-VM08V</td>
<td>FortiGate-VM 'virtual appliance': 8x vCPU cores. No VDOM by default for FG-VM08V model.</td>
</tr>
<tr>
<td>FortiGate-VM16</td>
<td>FG-VM16, FG-VM16V</td>
<td>FortiGate-VM 'virtual appliance': 16x vCPU cores. No VDOM by default for FG-VM16V model.</td>
</tr>
<tr>
<td>FortiGate-VM32</td>
<td>FG-VM32, FG-VM32V</td>
<td>FortiGate-VM 'virtual appliance': 32x vCPU cores. No VDOM by default for FG-VM32V model.</td>
</tr>
<tr>
<td>FortiGate-VMUL</td>
<td>FG-VMUL, FG-VMULV</td>
<td>FortiGate-VM 'virtual appliance': Unlimited vCPU cores. No VDOM by default for FG-VMULV model.</td>
</tr>
</tbody>
</table>

### Optional Accessories/Spares

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FG-VDOM-5-UG</td>
<td>Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.</td>
</tr>
<tr>
<td>FG-VDOM-15-UG</td>
<td>Upgrade license for adding 15 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.</td>
</tr>
<tr>
<td>FG-VDOM-25-UG</td>
<td>Upgrade license for adding 25 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.</td>
</tr>
<tr>
<td>FG-VDOM-50-UG</td>
<td>Upgrade license for adding 50 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.</td>
</tr>
<tr>
<td>FG-VDOM-240-UG</td>
<td>Upgrade license for adding 240 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.</td>
</tr>
</tbody>
</table>

The number of configurable VDOMs can be stacked up to the maximum number of supported VDOMs per vCPU model. Please refer to Virtual Domains (Maximum) under SPECIFICATIONS.

The following SKUs adopt the annual subscription licensing scheme:

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate-VM01-S</td>
<td>FC1-10-FGVVS-&lt;Support Bundle&gt;-02-DD</td>
<td>Subscriptions license for FortiGate-VM (1 vCPU core)</td>
</tr>
<tr>
<td>FortiGate-VM02-S</td>
<td>FC2-10-FGVVS-&lt;Support Bundle&gt;-02-DD</td>
<td>Subscriptions license for FortiGate-VM (2 vCPU cores)</td>
</tr>
<tr>
<td>FortiGate-VM04-S</td>
<td>FC3-10-FGVVS-&lt;Support Bundle&gt;-02-DD</td>
<td>Subscriptions license for FortiGate-VM (4 vCPU cores)</td>
</tr>
<tr>
<td>FortiGate-VM08-S</td>
<td>FC4-10-FGVVS-&lt;Support Bundle&gt;-02-DD</td>
<td>Subscriptions license for FortiGate-VM (8 vCPU cores)</td>
</tr>
<tr>
<td>FortiGate-VM16-S</td>
<td>FC5-10-FGVVS-&lt;Support Bundle&gt;-02-DD</td>
<td>Subscriptions license for FortiGate-VM (16 vCPU cores)</td>
</tr>
<tr>
<td>FortiGate-VM32-S</td>
<td>FC6-10-FGVVS-&lt;Support Bundle&gt;-02-DD</td>
<td>Subscriptions license for FortiGate-VM (32 vCPU cores)</td>
</tr>
<tr>
<td>FortiGate-VMUL-S</td>
<td>FC7-10-FGVVS-&lt;Support Bundle&gt;-02-DD</td>
<td>Subscriptions license for FortiGate-VM (Unlimited vCPU cores)</td>
</tr>
</tbody>
</table>

### Support Bundle

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>258</td>
<td>FortiCare services (only) included</td>
</tr>
<tr>
<td>815</td>
<td>Enterprise Bundle included</td>
</tr>
<tr>
<td>820</td>
<td>360 Protection Bundle included</td>
</tr>
<tr>
<td>990</td>
<td>UTP Bundle included</td>
</tr>
</tbody>
</table>

FortiOS 6.2.3+ and 6.4.0+ support the FortiGate-VM S-series. The FortiGate-VM S-series does not have RAM restrictions on all vCPU levels. FortiManager 6.2.3+ and 6.4.0+ support managing FortiGate-VM S-series devices.
BUNDLES

<table>
<thead>
<tr>
<th>Bundles</th>
<th>360 Protection</th>
<th>Enterprise Protection</th>
<th>Unified Threat Protection</th>
<th>Advanced Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>ASE 1</td>
<td>24×7</td>
<td>24×7</td>
<td>24×7</td>
</tr>
<tr>
<td>FortiGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IPS Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Web and Video Filtering Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Antispam Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Security Rating Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IoT Detection Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiConverter Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Orchestrator Entitlement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Cloud Assisted Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Overlay Controller VPN Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet SOCaaS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiAnalyzer Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiManager Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. 24×7 plus Advanced Services Ticket Handling  
2. Available when running FortiOS 7.0

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.