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

Security
- Protects against known exploits and malware using continuous threat intelligence provided by FortiGuard Labs security services
- Identify thousands of applications including cloud applications for deep inspection into network traffic
- Protects against unknown attacks using dynamic analysis and provides automated mitigation to stop targeted attacks

Performance
- Delivers industry’s best threat protection performance with DPDK+vNP offloading and SR-IOV technologies

Certification
- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICSA, Virus Bulletin and AV Comparatives

Networking
- Delivers extensive routing, switching, and VPN capabilities to consolidate networking and security functionality

Management
- Ability to manage virtual appliances and physical appliances from a single pane of glass management platform
- Wide array of licensing choices to fit any infrastructure requirement
- VDOM-enabled models for multi-tenant environments

Security Fabric
- Enables Fortinet and Fabric-ready partners’ products to collaboratively integrate and provide end-to-end security across the entire attack surface
- Out-of-the-box integration and orchestration with leading SDN platforms
Deployment

Next Generation Virtual Firewall (NGVFW)

- Combines threat prevention security capabilities into single power virtual appliance instance
- Reduces complexity by creating campus topology view and providing granular visibility of devices, users and threat information
- Identifies and stops threats with powerful intrusion prevention beyond port and protocol that examines the actual content of your network traffic
- Extends security capabilities with Security Fabric integration

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 VFs; virtual functions), consisting of an ESXi virtual network pool of adapters, which can be used by local host processors or directly by virtual machines like FG-VM. VM then talks directly to the network adapters through DMA (Direct Memory Access) by bypassing virtualization transports, which will improve north-south network performance.

DPDK (Data Plane Development Kit) and vNP Offloading

DPDK and vNP enhance FortiGate-VM performance by offloading part of packet processing to user space while bypassing kernel within the operating system. The capability must be enabled and configured with FortiGate CLI commands.

Currently the feature is available only on the special build. Please refer to documentation for more detail.

Fortinet Security Fabric

Today’s Challenges

- Conventional network infrastructure lacks flexibility due to physical entities ranging from wires, servers, to rack spaces. This type of network cannot easily respond to evolving security threats.
- Multi-clouds are still co-existent isolated sets of private clouds, public clouds, and physical entities requiring different security management methodologies which have become burdens to administrators.
- Dramatically increasing number of instantiated entities with elastic workloads raises risks of unattended vulnerabilities.
- Inconsistent security management with assortment of security solutions at different sites and tenants.
Fortinet Security Fabric

Security Fabric
The Security Fabric delivers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. All this is tied together under a single pane of glass management for significantly thereby delivering leading security capabilities across your entire environment while also significantly reducing complexity.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.

FortiOS
Control all security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce complexity, costs, and response time with a truly consolidated next-generation security platform.

- A truly consolidated platform with a single OS and pane-of-glass for all security and networking services across all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance. Ability to leverage 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.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated AI-driven breach prevention and advanced threat protection.
- Fulfill your networking needs with extensive routing, switching, and SD-WAN capabilities along with intent-based segmentation.
- Utilize SPU hardware acceleration to boost security capability performance.

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™ 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
## Specifications

<table>
<thead>
<tr>
<th></th>
<th>FORTIGATE-VM01/01V</th>
<th>FORTIGATE-VM02/02V</th>
<th>FORTIGATE-VM04/04V</th>
<th>FORTIGATE-VM08/08V</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Specifications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCPU Support (Minimum / Maximum)</td>
<td>1 / 1</td>
<td>1 / 2</td>
<td>1 / 4</td>
<td>1 / 8</td>
</tr>
<tr>
<td>Network Interface Support (Minimum / Maximum)</td>
<td>1 / 10</td>
<td>1 / 10</td>
<td>1 / 10</td>
<td>1 / 10</td>
</tr>
<tr>
<td>Memory Support (Minimum / Maximum)</td>
<td>1 GB / 2 GB</td>
<td>1 GB / 4 GB</td>
<td>1 GB / 6 GB</td>
<td>1 GB / 12 GB</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>
<td>32 GB / 2 TB</td>
</tr>
<tr>
<td>Wireless Access Points Controlled (Tunnel / Global)</td>
<td>32 / 64</td>
<td>32 / 128</td>
<td>256 / 512</td>
<td>1,024 / 4,096</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum)*</td>
<td>10 / 10</td>
<td>10 / 25</td>
<td>10 / 50</td>
<td>10 / 500</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>1,000</td>
<td>1,000</td>
<td>5,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Maximum Number of Registered Endpoints</td>
<td>2,000</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>
<td>Yes</td>
</tr>
<tr>
<td><strong>System Performance</strong></td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
</tr>
<tr>
<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>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td>1.0 Million</td>
<td>2.6 Million</td>
<td>4.3 Million</td>
<td>8.5 Million</td>
</tr>
<tr>
<td>New Sessions / Second (TCP)</td>
<td>85,000</td>
<td>100,000</td>
<td>125,000</td>
<td>150,000</td>
</tr>
<tr>
<td>iPSec VPN Throughput (AES256-SHA1, 512 Byte)</td>
<td>1.0 Gbps</td>
<td>1.2 Gbps</td>
<td>2.0 Gbps</td>
<td>4.2 Gbps</td>
</tr>
<tr>
<td>Gateway-to-Gateway iPSec VPN Tunnels</td>
<td>2,000</td>
<td>6,000</td>
<td>20,000</td>
<td>40,000</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>1.5 Gbps</td>
<td>3.5 Gbps</td>
<td>6.5 Gbps</td>
<td>10.5 Gbps</td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users (Recommended Maximum)</td>
<td>1,000</td>
<td>2,000</td>
<td>5,000</td>
<td>10,000</td>
</tr>
<tr>
<td><strong>IPS Throughput</strong></td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
</tr>
<tr>
<td>IPS Throughput</td>
<td>0.7 Gbps</td>
<td>1.0 Gbps</td>
<td>2.2 Gbps</td>
<td>4.5 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>2.1 Gbps</td>
<td>3.5 Gbps</td>
<td>5.7 Gbps</td>
<td>8.9 Gbps</td>
</tr>
<tr>
<td><strong>NGFW Throughput</strong></td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPSec VPN Tunnels</td>
<td>17.0 Gbps</td>
<td>17.5 Gbps</td>
<td>18.5 Gbps</td>
<td>22.5 Gbps</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>8.0 Gbps</td>
<td>10.0 Gbps</td>
<td>12.0 Gbps</td>
<td>14.0 Gbps</td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users (Recommended Maximum)</td>
<td>1,000</td>
<td>2,000</td>
<td>5,000</td>
<td>10,000</td>
</tr>
<tr>
<td><strong>IPS HTTP 1M</strong></td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>6.0 Gbps</td>
<td>9.0 Gbps</td>
<td>15.0 Gbps</td>
<td>21.0 Gbps</td>
</tr>
<tr>
<td><strong>IPsec VPN Throughput (AES256-SHA1, 512 Byte)</strong></td>
<td>8.6 Gbps</td>
<td>25.2 Gbps</td>
<td>28.8 Gbps</td>
<td>52.5 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>3.5 Gbps</td>
<td>5.4 Gbps</td>
<td>8.8 Gbps</td>
<td>13.5 Gbps</td>
</tr>
<tr>
<td><strong>Application Control Throughput</strong></td>
<td>2.0 Gbps</td>
<td>2.7 Gbps</td>
<td>5.2 Gbps</td>
<td>8.5 Gbps</td>
</tr>
<tr>
<td><strong>NGFW Throughput</strong></td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPSec VPN Tunnels</td>
<td>17.0 Gbps</td>
<td>17.5 Gbps</td>
<td>18.5 Gbps</td>
<td>22.5 Gbps</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>8.0 Gbps</td>
<td>10.0 Gbps</td>
<td>12.0 Gbps</td>
<td>14.0 Gbps</td>
</tr>
<tr>
<td>IPS Throughput</td>
<td>0.7 Gbps</td>
<td>1.0 Gbps</td>
<td>2.2 Gbps</td>
<td>4.5 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>2.1 Gbps</td>
<td>3.5 Gbps</td>
<td>5.7 Gbps</td>
<td>8.9 Gbps</td>
</tr>
<tr>
<td><strong>NGFW Throughput</strong></td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPSec VPN Tunnels</td>
<td>17.0 Gbps</td>
<td>17.5 Gbps</td>
<td>18.5 Gbps</td>
<td>22.5 Gbps</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>8.0 Gbps</td>
<td>10.0 Gbps</td>
<td>12.0 Gbps</td>
<td>14.0 Gbps</td>
</tr>
<tr>
<td>IPS Throughput</td>
<td>0.7 Gbps</td>
<td>1.0 Gbps</td>
<td>2.2 Gbps</td>
<td>4.5 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>2.1 Gbps</td>
<td>3.5 Gbps</td>
<td>5.7 Gbps</td>
<td>8.9 Gbps</td>
</tr>
<tr>
<td><strong>IPsec VPN Throughput (AES256-SHA1, 512 Byte)</strong></td>
<td>8.6 Gbps</td>
<td>25.2 Gbps</td>
<td>28.8 Gbps</td>
<td>52.5 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>3.5 Gbps</td>
<td>5.4 Gbps</td>
<td>8.8 Gbps</td>
<td>13.5 Gbps</td>
</tr>
<tr>
<td><strong>Application Control Throughput</strong></td>
<td>2.0 Gbps</td>
<td>2.7 Gbps</td>
<td>5.2 Gbps</td>
<td>8.5 Gbps</td>
</tr>
<tr>
<td><strong>NGFW Throughput</strong></td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
<td>Non-DPDK+vNP offloading</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPSec VPN Tunnels</td>
<td>17.0 Gbps</td>
<td>17.5 Gbps</td>
<td>18.5 Gbps</td>
<td>22.5 Gbps</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>8.0 Gbps</td>
<td>10.0 Gbps</td>
<td>12.0 Gbps</td>
<td>14.0 Gbps</td>
</tr>
<tr>
<td>IPS Throughput</td>
<td>0.7 Gbps</td>
<td>1.0 Gbps</td>
<td>2.2 Gbps</td>
<td>4.5 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput</td>
<td>2.1 Gbps</td>
<td>3.5 Gbps</td>
<td>5.7 Gbps</td>
<td>8.9 Gbps</td>
</tr>
</tbody>
</table>

Actual performance may vary depending on the network and system configuration. Performance metrics were observed using a DELL R740 (CPU Intel Xeon Platinum 8168 @ 2.7 Ghz, 96 cores, Intel X710 network adapters). Non-DPDK numbers were measured on FG-VMv6.1. iPSec numbers were measured on the special build of FG-VMv6.1. SR-IOV is enabled. Tested with VMware vSphere 6.5. Update 1. 1. IPS performance is measured using Enterprise Traffic Mix and 1Mbyte HTTP. 2. Application Control performance is measured with 64Kbyte 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. 5. *Not applicable to FG-VMv6.x series as VDOMs are not supported. FG-VMv6.0.0 is an exception, which supports VDOM addition with separately purchased VDOM licenses. See ORDER INFORMATION for VDOM SKUs.*
## Specifications

<table>
<thead>
<tr>
<th>Technical Specifications</th>
<th>FORTIGATE-VM02/02V</th>
<th>FORTIGATE-VM04/04V</th>
<th>FORTIGATE-VM08/08V</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>Network Interface Support (Minimum / Maximum)</td>
<td>1 / 10</td>
<td>1 / 10</td>
<td>1 / 10</td>
</tr>
<tr>
<td>Memory Support (Minimum / Maximum)</td>
<td>1 GB / 4 GB</td>
<td>1 GB / 6 GB</td>
<td>1 GB / 6 GB</td>
</tr>
<tr>
<td>Storage Support (Minimum / Maximum)</td>
<td>32 GB / 1 TB</td>
<td>32 GB / 1 TB</td>
<td>32 GB / 1 TB</td>
</tr>
<tr>
<td>Wireless Access Points Controlled (Tunnel / Global)</td>
<td>256 / 512</td>
<td>256 / 512</td>
<td>1,024 / 4,096</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum)</td>
<td>10 / 25</td>
<td>10 / 50</td>
<td>10 / 500</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>1,000,000</td>
<td>10,000,000</td>
<td>200,000,000</td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>1,000</td>
<td>5,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Maximum Number of Registered Endpoints</td>
<td>2,000</td>
<td>5,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Unlimited User License</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### System Performance

<table>
<thead>
<tr>
<th>Performance</th>
<th>FORTIGATE-VM02/02V</th>
<th>FORTIGATE-VM04/04V</th>
<th>FORTIGATE-VM08/08V</th>
</tr>
</thead>
<tbody>
<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 Throughput 1</td>
<td>2.5 Gbps</td>
<td>4.7 Gbps</td>
<td>8.6 Gbps</td>
</tr>
<tr>
<td>IPS HTTP 1M</td>
<td>16.5 Gbps</td>
<td>32.0 Gbps</td>
<td>32.0 Gbps</td>
</tr>
<tr>
<td>Application Control Throughput 2</td>
<td>4.0 Gbps</td>
<td>7.4 Gbps</td>
<td>12.5 Gbps</td>
</tr>
<tr>
<td>NSFW Throughput 3</td>
<td>1.9 Gbps</td>
<td>5.6 Gbps</td>
<td>8.5 Gbps</td>
</tr>
<tr>
<td>Threat Protection Throughput 4</td>
<td>1.5 Gbps</td>
<td>5.0 Gbps</td>
<td>5.6 Gbps</td>
</tr>
</tbody>
</table>

* Actual performance may vary depending on the network and system configuration. 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.

** IPS performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.

*** Application Control performance is measured with 64 Kbyte HTTP traffic.

1. IPS performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
2. NGFW performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.

** It is highly recommended to allocate as much RAM size as the licensed limit for maximum performance.

---

* It is highly recommended to allocate as much RAM size as the licensed limit for maximum performance.

** Not applicable to FG-VMxxV series as VDOMs are not supported. FG-VMxV 6.0.0 is an exception, which supports VDOM addition with separately purchased VDOM licenses. See ORDER INFORMATION for VDOM SKUs.

---

1. IPS performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
2. Application Control performance is measured with 64 Kbyte HTTP traffic.
3. NGFW performance is measured with IPS and Application Control and Malware protection 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.

---

*** 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.
Order Information

The following SKUs adopt perpetual licensing scheme:

<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 and (up to) 2 GB RAM. 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 and (up to) 4 GB RAM. 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 and (up to) 6 GB RAM. 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 and (up to) 12 GB RAM. 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 and up to 24 GB RAM. 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 and up to 48 GB RAM. 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 and RAM. No VDOM by default for FG-VMULV model.</td>
</tr>
</tbody>
</table>

Optional Accessories

Virtual Domain License Add 5  FG-VDOM-5-UG Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 15 FG-VDOM-15-UG Upgrade license for adding 15 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 25 FG-VDOM-25-UG Upgrade license for adding 25 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 50 FG-VDOM-50-UG Upgrade license for adding 50 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.
Virtual Domain License Add 240 FG-VDOM-240-UG Upgrade license for adding 240 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity.

FG-VMxx”V” 6.0.0 supports VDOM by adding separate VDOM licenses. 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.

Bundles

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.

<table>
<thead>
<tr>
<th>Bundles</th>
<th>Threat Protection</th>
<th>UTM</th>
<th>Enterprise Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCASB SaaS-only Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Security Rating Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Antispam</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Web Filtering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, C0R©, Virus Outbreak Protection* and FortiSandbox Cloud Service*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IPS Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FritiCare + FortiGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Available when running FortiOS 6.0.1 and above  
With new Q3-2018 SKUs