FortiGate® Virtual Appliances
Consolidated Security for Virtualized Environments

Complete end-to-end security ecosystem for the Software Defined Data Center. Fortinet enables and facilitates the enterprise’s journey through the Data Center consolidation process.

Fortinet delivers both physical and virtualized security appliances to secure unique data planes. It offers on one side, unmatched performance and security capabilities while allowing for the growth and evolution of the consolidating Data Center with no service degradation or bottlenecks, no compromise on security, and with an unmatched ROI — fulfilling the outcomes of a robust software-defined security framework.

FortiGate Virtual Appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

FortiGate virtual appliances offer protection from a broad array of threats, with support for all of the security and networking services offered by the FortiOS operating system. In addition, the appliances offer:

- Increased visibility within virtualized infrastructure
- Rapid deployment capability
- Ability to manage virtual appliances and physical appliances from a single pane of glass management platform
- Simple licensing with no per-user fees
- Support for multiple virtualization and Cloud platforms
- Full support for FortiHypervisor deployments enabling line-speed security in vCPE requirement
- Wide array of licensing choices to fit any infrastructure requirement
- VDOM-enabled models for multi-tenant environments

Fortinet’s comprehensive security virtual appliance lineup supports in excess of 16 solutions.
PLATORM

Choice of Form Factor
Few organizations use 100% hardware or 100% virtual IT infrastructure today, creating a need for both hardware appliances and virtual appliances in your security strategy. Fortinet allows you to build the security solution that’s right for your environment with hardware and virtual appliances to secure the core, the edge and increase visibility and control over communications within the virtualized infrastructure. FortiManager virtual or physical appliances allow you to easily manage and update your Fortinet security assets — hardware, virtual or both — from a single pane of glass.

Multi-Threat Security
Using the advanced FortiOS™ operating system, FortiGate appliances effectively neutralize a wide range of security threats facing your virtualized environment. Whether deployed at the edge as a front-line defense, or deep within the virtual infrastructure for inter-zone security, FortiGate appliances protect your infrastructure with some of the most effective security available today by enabling security features you need.

DEPLOYMENT

All Inter-VM traffic in Bravo Zones are subject to full UTM scan through L2 VDOM. Inter-Zone traffic subject to full Next Gen Firewall and UTM scan by L3 VDOM. Alpha Zone VMs can all talk to each other freely.

Choice of Form Factor
Few organizations use 100% hardware or 100% virtual IT infrastructure today, creating a need for both hardware appliances and virtual appliances in your security strategy. Fortinet allows you to build the security solution that’s right for your environment with hardware and virtual appliances to secure the core, the edge and increase visibility and control over communications within the virtualized infrastructure. FortiManager virtual or physical appliances allow you to easily manage and update your Fortinet security assets — hardware, virtual or both — from a single pane of glass.

Multi-Threat Security
Using the advanced FortiOS™ operating system, FortiGate appliances effectively neutralize a wide range of security threats facing your virtualized environment. Whether deployed at the edge as a front-line defense, or deep within the virtual infrastructure for inter-zone security, FortiGate appliances protect your infrastructure with some of the most effective security available today by enabling security features you need.
FORTINET SECURITY FABRIC

Security Fabric
The Security Fabric 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.

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 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.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated advanced threat protection.
- Fulfill your networking needs with extensive routing, switching, and SD-WAN capabilities.
- Utilize SPU hardware acceleration to boost security capability performance.

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 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

### FORTIGATE-VM00

<table>
<thead>
<tr>
<th>Specification</th>
<th>FORTIGATE-VM00</th>
<th>FORTIGATE-VM01/01V</th>
<th>FORTIGATE-VM02/02V</th>
<th>FORTIGATE-VM04/04V</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU Support</td>
<td>1 / 1</td>
<td>1 / 1</td>
<td>1 / 2</td>
<td>1 / 4</td>
</tr>
<tr>
<td>Memory Support</td>
<td>1 GB / 2 GB</td>
<td>1 GB / 2 GB</td>
<td>1 GB / 4 GB</td>
<td>1 GB / 6 GB</td>
</tr>
<tr>
<td>Storage Support</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</td>
<td>32 / 32</td>
<td>32 / 64</td>
<td>256 / 512</td>
<td>256 / 512</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>25,000</td>
<td>50,000 / 100,000</td>
<td>50,000 / 100,000</td>
<td>50,000 / 100,000</td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>1,000</td>
<td>1,000</td>
<td>1,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Maximum Number of Registered Endpoints</td>
<td>N/A</td>
<td>2,000</td>
<td>2,000</td>
<td>8,000</td>
</tr>
<tr>
<td>Unlimited User License</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### System Performance

<table>
<thead>
<tr>
<th>Specification</th>
<th>FORTIGATE-VM00</th>
<th>FORTIGATE-VM01/01V</th>
<th>FORTIGATE-VM02/02V</th>
<th>FORTIGATE-VM04/04V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (UDP Packets, SR-IOV Enabled)</td>
<td>12 Gbps</td>
<td>12 Gbps</td>
<td>15 Gbps</td>
<td>28 Gbps</td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td>2 Million</td>
<td>2 Million</td>
<td>2.6 Million</td>
<td>4.3 Million</td>
</tr>
<tr>
<td>New Sessions / Second (TCP)</td>
<td>85,000</td>
<td>85,000</td>
<td>100,000</td>
<td>125,000</td>
</tr>
<tr>
<td>IPsec VPN Throughput (AES256-SHA1, 512 Byte)</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1.5 Gbps</td>
<td>3 Gbps</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPsec VPN Tunnels</td>
<td>1,024 / 4,096</td>
<td>1,024 / 4,096</td>
<td>1,024 / 4,096</td>
<td>1,024 / 4,096</td>
</tr>
<tr>
<td>Virtual Domains</td>
<td>10 / 50</td>
<td>10 / 50</td>
<td>10 / 25</td>
<td>10 / 50</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>50,000</td>
<td>50,000</td>
<td>50,000</td>
<td>50,000</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>N/A</td>
<td>2,000</td>
<td>2,000</td>
<td>8,000</td>
</tr>
<tr>
<td>Unlimited User License</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Actual Performance

- 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, Intel X710 network adapters), running FOS v5.6.3. Tested with VMware vSphere 6.5 Enterprise Plus. SR-IOV is enabled.
- 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix.
- 2. Application Control Throughput 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.

**Applicable to VM running on 5.6 and above.**

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

### VENDOR
**Private Clouds (Hypervisors)**
- VMware ESX v5.5 / v6.0 / v6.1 / v6.5 / v7.0 / v7.1
- Citrix XenServer v5.6 sp2, v6.0, v6.2 and later
- Open source Xen v3.3, v4.1 and later
- KVM qemu 0.12.1 & libvirt 0.10.2 and later for Red Hat Enterprise Linux / CentOS 6.4 and later / Ubuntu 16.04 LTS (generic kernel)
- KVM qemu 2.3.1 for SUSE Linux Enterprise Server 12 SP1 LTSS

### VENDOR
**Public Clouds (Market Places)**
- Amazon AWS (Amazon Web Services)
- VMware Cloud on AWS
- Microsoft Azure
- Google GCP (Google Cloud Platform)
- Oracle OCI and OCI-Classic

Note: Virtualization/Cloud Platform Support varies by model and FortiOS builds. Please refer to appropriate release notes. FG-VMxxV series require FortiOS 5.4.8+ / 5.6.1+ / 6.0.0.

### ORDER INFORMATION

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate-VM00</td>
<td>FG-VM00</td>
<td>FortiGate-VM Virtual appliances: 1x vCPU core, (up to) 2 GB RAM. No Extreme DB support.</td>
</tr>
<tr>
<td>FortiGate-VM01</td>
<td>FG-VM01, FG-VM01V</td>
<td>FortiGate-VM Virtual appliances: 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 appliances: 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 appliances: 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 appliances: 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 appliances: 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 appliances: 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 appliances: 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.

**Note:** FG-VMxxV series 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.