The FortiGate-VM on Microsoft Azure delivers next generation firewall (NGFW) capabilities for organizations of all sizes, with the flexibility to be deployed as NGFW and/or VPN gateway. 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 firewall and threat protection performance using software-based, purpose-built virtual security processor (vSPU) technology
- 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, multitency, 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 and 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
- APIs for automation and orchestration with cloud and SDN extensions

**Security Fabric**
- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation
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

**VPN Gateway**
- VPN gateways for FortiGate inter-vNET VPN
- Hybrid cloud site-to-site IPsec VPN
- Remote access VPN

---

---

**Public Cloud**

- Fabric Connectors
- VNF Orchestration
- Cloud Init

---

**Advanced Security**
- SD-WAN
- VPN
- IPS
- Carrier-FW
- Threat intel
- URL Filtering
- AV
- Sandboxing
- Intent-based / Micro Segmentation

---

**Enterprise Edge**

**MSSP**

---

**Gain comprehensive visibility and apply consistent control**

---

**Azure Integration**
- FortiOS embeds the latest autoscaling functionality, providing automation based on resource demand from your cloud workloads.
- Designed to ensure easy, consistent deployment for the most efficient systems and applications uptime with minimal disruption using Azure load balancing and two FortiGate-VMs.
- FortiOS works with Azure Traffic Manager to provide local access for customers for low latency while providing redundancy.
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 and 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, enables the convergence of high performing networking and security across the Fortinet Security Fabric, delivering consistent and context-aware security posture across network endpoints 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 1000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.
With a multitude of deployment methods supported across various private and public cloud deployments, FortiGate-VM for Microsoft Azure supports both on-demand (PAYG) and bring your own license (BYOL) licensing models.

On-demand licensing is a highly flexible option for both initial deployments and growing them as needed. With a wide selection of supported instance types, there is a solution for every use case. This license offers FortiOS with a UTP bundle.

BYOL is ideal for migration use cases, where an existing private cloud deployment is migrated to a public cloud deployment. When using an existing license, the only additional cost is the price for the Microsoft Azure instances.

You can deploy FortiGate-VM in regional Azure such as Azure Government, Germany, and China.

FortiGate-VM also supports Azure Stack (BYOL only).

### SPECIFICATIONS

<table>
<thead>
<tr>
<th>System Requirement</th>
<th>VM-01/01V/01S</th>
<th>VM-02/02V/02S</th>
<th>VM-04/04V/04S</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU (Minimum/Maximum)</td>
<td>1/1</td>
<td>1/2</td>
<td>1/4</td>
</tr>
</tbody>
</table>

#### Technical Specifications

<table>
<thead>
<tr>
<th>Network Interface Support (Minimum/Maximum)</th>
<th>1/24</th>
<th>1/24</th>
<th>1/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDOMs (Default/Maximum)</td>
<td>1/10</td>
<td>1/25</td>
<td>1/50</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>10,000</td>
<td>10,000</td>
<td>20,000</td>
</tr>
</tbody>
</table>

#### System Performance

- **Instance Shape to be Measured**
  - DS2_v2 (2vCPU)
  - D4s_v3 (4vCPU)
- **Firewall Throughput (UDP Packets) in Mbps**
  - 1100
  - 1600
  - 1380
  - 2000
- **New Sessions/Second (TCP)**
  - 5800
  - 4200
  - 5900
  - 4500
- **IPS Throughput in Mbps**
  - 640
  - 1480
  - 930
  - 1950
- **IPS HTTP 1M in Mbps**
  - 680
  - 1490
  - 1010
  - 1980
- **SSL Inspection Throughput in Mbps**
  - 520
  - 1040
  - 700
  - 1670
- **Application Control Throughput in Mbps**
  - 690
  - 1480
  - 1000
  - 1975
- **NGFW Throughput**
  - 590
  - 660
  - 630
  - 800
- **IPsec VPN throughput (SHA2-256) with UDP 1518 bytes**
  - 950
  - 1600
  - 1250
  - 1800

#### Note:
All performance values are “up to” and vary depending on system configuration. PAYG supports only up to 32 vCPU instances. 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. Different versions of the document may note the discrepancy in the performance numbers so ensure that you refer to the latest datasheets. Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.0.1.

- FG-VMxV and FG-VMxS 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.
- The latest information about Microsoft Azure bandwidth is found on https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general.
- IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
- Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).
- Application Control performance is measured with 64 Kbyte HTTP traffic.
- NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
- Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
### SPECIFICATIONS

<table>
<thead>
<tr>
<th></th>
<th>VM-08/08V/08S</th>
<th>VM-16/16V/16S</th>
<th>VM-32/32V/32S</th>
<th>VM-UL/ULV/ULS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Requirement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCPU (Minimum/Maximum)</td>
<td>1/8</td>
<td>1/16</td>
<td>1/32</td>
<td>1/Unlimited</td>
</tr>
<tr>
<td><strong>Technical Specifications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Interface Support (Minimum/Maximum)</td>
<td>1/24</td>
<td>1/24</td>
<td>1/24</td>
<td>1/24</td>
</tr>
<tr>
<td>VDOMs (Default/Maximum)</td>
<td>10/500</td>
<td>10/500</td>
<td>10/500</td>
<td>10/500</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>200 000</td>
<td>200 000</td>
<td>200 000</td>
<td>200 000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>System Performance</strong></th>
<th>Accelerated Networking OFF</th>
<th>Accelerated Networking ON</th>
<th>Accelerated Networking OFF</th>
<th>Accelerated Networking ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Shape to be Measured</td>
<td>D8s_v3 (8vCPU)</td>
<td>D16s_v3 (16vCPU)</td>
<td>D32s_v3 (32vCPU)</td>
<td></td>
</tr>
<tr>
<td>Azure Expected Bandwidth</td>
<td>4000 Mbps</td>
<td>8000 Mbps</td>
<td>16 000 Mbps</td>
<td></td>
</tr>
<tr>
<td>Firewall Throughput (UDP Packets) in Mbps</td>
<td>1550</td>
<td>4000</td>
<td>1870</td>
<td>7800</td>
</tr>
<tr>
<td>New Sessions/Second (TCP)</td>
<td>8000</td>
<td>6500</td>
<td>13 500</td>
<td>11 100</td>
</tr>
<tr>
<td>IPS Throughput in Mbps</td>
<td>1100</td>
<td>3900</td>
<td>1150</td>
<td>7560</td>
</tr>
<tr>
<td>IPS HTTP 1M in Mbps</td>
<td>1150</td>
<td>3910</td>
<td>1200</td>
<td>7620</td>
</tr>
<tr>
<td>SSL Inspection Throughput in Mbps</td>
<td>780</td>
<td>2160</td>
<td>830</td>
<td>3500</td>
</tr>
<tr>
<td>Application Control Throughput in Mbps</td>
<td>1150</td>
<td>3900</td>
<td>1200</td>
<td>7550</td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>800</td>
<td>1770</td>
<td>1100</td>
<td>2350</td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>790</td>
<td>1770</td>
<td>1100</td>
<td>2550</td>
</tr>
<tr>
<td>IPsec VPN Throughput (SHA2-256) with UDP 1518 bytes</td>
<td>1400</td>
<td>4000</td>
<td>1800</td>
<td>6500</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 FortiGate-VM BYOL instances using FOS v7.01.

1. Applicable to 6.4.0+. The actual working number of consumable network interfaces varies depending on Microsoft Azure instance types/sizes and may be less.
2. FG-VMxV and FG-VMxS 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.
4. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
5. Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).
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.
ORDERING INFORMATION

The following are SKUs that can be acquired for the BYOL scheme. For the PAYG/On-Demand subscription, various instance/VM types are available on the Marketplace. BYOL is perpetual licensing, as opposed to PAYG/On-Demand, which is an hourly subscription available with marketplace-listed products.

<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>
</tbody>
</table>

The number of configurable VDOMs can be stacked up to the maximum number of supported VDOMs per vCPU model. 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>

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. FortManager 6.2.3+ and 6.4.0+ support managing FortiGate-VM S-series devices.
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>Enterprise Protection</th>
<th>Unified Threat Protection</th>
<th>Advanced Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</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>
</tr>
<tr>
<td>FortiGuard IPS Service</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>
</tr>
<tr>
<td>FortiGuard Web and Video Filtering Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Antispam 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 IoT Detection Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiConverter Service</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Available when running FortiOS 7.0