The FortiGate-VM on Microsoft Azure delivers next generation firewall capabilities for organizations of all sizes, with the flexibility to be deployed as next generation firewall and/or VPN gateway. 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

**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 (VDOM is supported with BYOL only)
- APIs for automation and orchestration with cloud and SDN extensions

**Security Fabric**
- Enables Fortinet and Fabric-ready partners’ products to collaboratively integrate and provide end-to-end security across the entire attack surface

Fortinet’s comprehensive security virtual appliance lineup supports on Microsoft Azure
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

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

Microsoft Azure Integration
- FortiOS embeds the latest Auto Scaling 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 LB and two virtual machines of FortiGate.
- FortiOS works with Azure Traffic Manager to provide local access for customers for low latency while providing redundancy.
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 ties 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.
- Fulfil 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
**Licensing**

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 UTM 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 would be the price for the Microsoft Azure instances.

FortiGate-VM can also be deployed in regional Azure such as Azure Government, Germany, and China. AzureStack is also supported (BYOL only).

**Specifications**

The following is the system requirement for BYOL licenses:

<table>
<thead>
<tr>
<th>System Requirement</th>
<th>VM-00</th>
<th>VM-01/01V</th>
<th>VM-02/02V</th>
<th>VM-04/04V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core (Minimum / Maximum)</td>
<td>1 / 1</td>
<td>1 / 1</td>
<td>1 / 2</td>
<td>1 / 4</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum) **</td>
<td>2 / 2</td>
<td>10 / 10</td>
<td>10 / 25</td>
<td>10 / 50</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Requirement</th>
<th>VM-08/08V</th>
<th>VM-16/16V</th>
<th>VM-32/32V</th>
<th>VM-UL/ULV*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core (Minimum / Maximum)</td>
<td>1 / 8</td>
<td>1 / 16</td>
<td>1 / 32</td>
<td>1 / Unlimited</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum) **</td>
<td>10 / 500</td>
<td>10 / 500</td>
<td>10 / 500</td>
<td>10 / 500</td>
</tr>
</tbody>
</table>

** PAYG supports only up to 32 vCPU instances.
** Not applicable to FG-VMxV series as VDOMs are not supported by default. VDOMs can be added with separately purchased VDOM licenses. See ORDER INFORMATION for VDOM SKUs.

For sizing guide, please refer to the sizing document available on www.fortinet.com
Order Information

The following are SKUs that can be acquired for BYOL scheme. For PAYG/On-Demand subscription, various instance/VM types are available on 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-VM00</td>
<td>FG-VM00</td>
<td>FortiGate-VM virtual appliance. 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 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-VM-32V 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-VM-32V 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. |

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.

Bundles

- **FortiGuard Labs**
- **FortiGuard Security Rating Service**
- **FortiGuard Antispyware**
- **FortiGuard Web Filtering**
- **FortiGuard Advanced Malware Protection (AMP)** — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection* and FortiSandbox Cloud Service*
- **FortiGuard IPS Service**
- **FortiCare + FortiGuard App Control Service**

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