FortiGate®-VM on Microsoft Azure

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

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

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

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 Firewall (NGFW)
- 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 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.

Fabric Connectors provide open, API based integration and orchestration of FortiGate or FortiManager with multiple SDN, cloud and partner technology platforms, thus automate security and simplify management in complex Hybrid Networks.

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.
- Manage public cloud and on-premises assets from a single pane of glass using FortiManager
- Support high availability on public cloud infrastructure

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.

For more information, please refer to forti.net/fortiguard

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/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 (BYOL) can also be deployed in regional Azure such as Azure Government, Germany, and China.

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-VMxxV 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 Licensing, various Azure instance type are available on Microsoft Azure Marketplace.

<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</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</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</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</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</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</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</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-U UPG, FortiGate-VM virtual appliance, unlimited vCPU cores, No VDOM by default for FG-VM-32V model.
- **Virtual Domain License Add 15**: FG-VDOM-15-U, FortiGate-VM virtual appliance, unlimited vCPU cores, No VDOM by default for FG-VM-32V model.
- **Virtual Domain License Add 25**: FG-VDOM-25-U, FortiGate-VM virtual appliance, unlimited vCPU cores, No VDOM by default for FG-VM-32V model.
- **Virtual Domain License Add 50**: FG-VDOM-50-U, FortiGate-VM virtual appliance, unlimited vCPU cores, No VDOM by default for FG-VM-32V model.
- **Virtual Domain License Add 240**: FG-VDOM-240-U, FortiGate-VM virtual appliance, unlimited vCPU cores, No VDOM by default for FG-VM-32V model.

FG-VMv6 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.

**FortiGuard Bundle**

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.

**FortiGuard Labs**

- FortiCASB SaaS-only Service
- FortiGuard Industrial Service
- FortiGuard Security Rating Service
- FortiGuard Antispm
- FortiGuard Web Filtering
- FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, COF, Virus Outbreak Protection and FortiSandbox Cloud Service
- FortiGuard IPS Service
- FortiCare + FortiGuard App Control Service

**Bundles**

<table>
<thead>
<tr>
<th><strong>Bundles</strong></th>
<th><strong>Threat Protection</strong></th>
<th><strong>UTM</strong></th>
<th><strong>Enterprise Protection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGuard Labs</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>FortiCare + 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

---

**GLOBAL HEADQUARTERS**

Fortinet Inc.  
899 KIFER ROAD  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
www.fortinet.com/sales

**EMEA SALES OFFICE**

EMEA SALES OFFICE  
905 rue Albert Einstein  
06560 Valbonne  
France  
Tel: +33.4.8987.0500

**APAC SALES OFFICE**

APAC SALES OFFICE  
8 Temasek Boulevard  
#12-01 Suntec Tower Three  
Singapore 038988  
Tel: +65.6395.2788

**LATIN AMERICA SALES OFFICE**

LATIN AMERICA SALES OFFICE  
Sawgrass Lakes Center  
13450 W. Sunrise Blvd., Suite 430  
Sunrise, FL 33323  
United States  
Tel: +1.954.368.9990