Automated, Advanced Security for VMware NSX-T Data Center Environments

FortiGate-VM next generation firewall is a virtual appliance that integrates with NSX-T security for VMware ESXi and other hypervisors and container orchestration platforms in SDDCs, private clouds, and public clouds. FortiGate-VM augments the microsegmentation that NSX-T 3.0 / 3.1 / 3.2 / 4.0 provides with advanced L7 security and zero-trust segmentation for complete protection against the most sophisticated threats and vulnerabilities.

Security Features
- Advanced (L7) threat protection integrated with VMware NSX-T Data Center environments in SDDCs as well as private and public clouds
- Zero-trust segmentation to protect against lateral threats
- Streamlined SecOps, with automation and orchestration via Fortinet Fabric Connectors
- Single-pane-of-glass management through VMware NSX Manager, with full visibility in FortiManager

Certification
- FortiGate-VM is certified with VMware's Service Chaining for NSX-T Data Center (Firewall) and Edge Service Insertion for NSX-T Data Center (Firewall). For the compatibility matrix, go to VMware Compatibility Guide

Management
- Ability to manage virtual 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

Fortinet's comprehensive security virtual appliance lineup supports VMware NSX-T

FortiManager  FortiAnalyzer
The FortiGate-VM provides interoperability with NSX-T Data Center through service insertion as a third-party edge firewall (Figure 1).

Core capabilities include:

- By means of Fabric Connectors activated from the FortiManager console, FortiGate-VM integrates with NSX-T Data Center to register both east-west and north-south service insertions.
- From that point on, security can be managed from the NSX-T dashboard and is automatically carried through to the FortiGate-VM instances running in the NSX-T Data Center.
- Fortinet Fabric Connector automatically updates security policies associated with dynamic objects in NSX-T whenever changes are made to underlying IP addresses, application metadata, and annotations. This capability, which also extends to public cloud infrastructures (such as AWS, Azure, and GCP), relieves organizations of the need to manually update security policies, freeing up their time for other business-critical duties.
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 & 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 enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, 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.
## SPECIFICATIONS

### FORTIGATE-VM01/01V
- **vCPU Support (Minimum / Maximum):** 1 / 1
- **Memory Support (Minimum):** 2 GB
- **Storage Support (Minimum / Maximum):** 32 GB / 2 TB
- **Wireless Access Points Controlled (Tunnel / Global):** 32 / 64
- **Virtual Domains (Default / Maximum):** 10 / 10
- **Firewall Policies:** 10,000
- **Maximum Number of Registered Endpoints:** 2,000
- **Unlimited User License:** Yes

### FORTIGATE-VM02/02V
- **vCPU Support (Minimum / Maximum):** 1 / 2
- **Memory Support (Minimum):** 2 GB
- **Storage Support (Minimum / Maximum):** 32 GB / 2 TB
- **Wireless Access Points Controlled (Tunnel / Global):** 512 / 1024
- **Virtual Domains (Default / Maximum):** 10 / 25
- **Firewall Policies:** 10,000
- **Maximum Number of Registered Endpoints:** 2,000
- **Unlimited User License:** Yes

### FORTIGATE-VM04/04V
- **vCPU Support (Minimum / Maximum):** 1 / 4
- **Memory Support (Minimum):** 2 GB
- **Storage Support (Minimum / Maximum):** 32 GB / 2 TB
- **Wireless Access Points Controlled (Tunnel / Global):** 512 / 1024
- **Virtual Domains (Default / Maximum):** 10 / 50
- **Firewall Policies:** 10,000
- **Maximum Number of Registered Endpoints:** 8,000
- **Unlimited User License:** Yes

### FORTIGATE-VM08/08V
- **vCPU Support (Minimum / Maximum):** 1 / 8
- **Memory Support (Minimum):** 2 GB
- **Storage Support (Minimum / Maximum):** 32 GB / 2 TB
- **Wireless Access Points Controlled (Tunnel / Global):** 1,024 / 4,096
- **Virtual Domains (Default / Maximum):** 10 / 500
- **Firewall Policies:** 20,000
- **Maximum Number of Registered Endpoints:** 20,000
- **Unlimited User License:** Yes

### FORTIGATE-VM16/16V
- **vCPU Support (Minimum / Maximum):** 1 / 16
- **Memory Support (Minimum):** 2 GB
- **Storage Support (Minimum / Maximum):** 32 GB / 2 TB
- **Wireless Access Points Controlled (Tunnel / Global):** 1,024 / 4,096
- **Virtual Domains (Default / Maximum):** 10 / 500
- **Firewall Policies:** 20,000
- **Maximum Number of Registered Endpoints:** 20,000
- **Unlimited User License:** Yes

### FORTIGATE-VM32/32V
- **vCPU Support (Minimum / Maximum):** 1 / 32
- **Memory Support (Minimum):** 2 GB
- **Storage Support (Minimum / Maximum):** 32 GB / 2 TB
- **Wireless Access Points Controlled (Tunnel / Global):** 1,024 / 4,096
- **Virtual Domains (Default / Maximum):** 10 / 500
- **Firewall Policies:** 20,000
- **Maximum Number of Registered Endpoints:** 20,000
- **Unlimited User License:** Yes

### FORTIGATE-VMUL/ULV
- **vCPU Support (Minimum / Maximum):** 1 / unlimited
- **Memory Support (Minimum):** 2 GB
- **Storage Support (Minimum / Maximum):** 32 GB / 2 TB
- **Wireless Access Points Controlled (Tunnel / Global):** 1,024 / 4,096
- **Virtual Domains (Default / Maximum):** 10 / 500
- **Firewall Policies:** 20,000
- **Maximum Number of Registered Endpoints:** 20,000
- **Unlimited User License:** Yes

### Network Interface Support
The maximum number of network interfaces consumable by a FortiGate instance is 24 starting with FortiGate version 6.4.0. Prior versions allow 18. The minimum number is 1. The actual number of network interfaces attachable to instances varies depending on cloud platforms and instance types, and they may not allow you to attach the greater number of interfaces to an instance than their maximum limits even while FortiGate allows up to 24.

**FG-VMxxV and FG-VMxxS 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. Special licenses for offline network environments are available for VMxxV series (01V to ULV), and they have the same specifications as those of VMxxV shown in the table above. For ordering offline licenses, please consult Fortinet sales representatives.**

### System Requirements
NSX-T integration requires a deployment of FortiManager (as a physical appliance or VM instance) with a valid license/entitlement in addition to a FortiGate-VM. See the FortiManager datasheet for the spec for details: [https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf)

FortiGate-VM 6.4.3 GA can be upgraded to 6.4.9+ GA. FortiGate-VM 7.0.6 GA can be upgraded to 7.2.0+ GA.

### Software Compatibility Matrix

<table>
<thead>
<tr>
<th>NSX-T</th>
<th>FortiGate-VM</th>
<th>FortiManager</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>7.0.6</td>
<td>7.0.5/7.21</td>
</tr>
<tr>
<td>3.0/3.1</td>
<td>7.0.6</td>
<td>7.0.5/7.21</td>
</tr>
<tr>
<td>3.0/3.1</td>
<td>6.4.3</td>
<td>6.4.4+</td>
</tr>
</tbody>
</table>

### CERTIFICATIONS

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Partner Product and Version</th>
<th>Certification Date</th>
<th>Listing URL</th>
</tr>
</thead>
</table>
**ORDERING INFORMATION**

<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 unlimited 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 unlimited 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 unlimited 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 unlimited 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 unlimited 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 unlimited 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.                          |

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.

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>

**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.

**FortiCare**

FortiGate S Series

- **FortiCare**
  - **Enterprise Protection**: 24x7
  - **Unified Threat Protection**: 24x7
  - **Advanced Threat Protection**: 24x7

1. Available when running FortiOS 7.0

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims any warranties, whether express or implied, except as may be contained in written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet expresses no warranty whatsoever in any way, directly or indirectly, to any purchaser herein, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet declines in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet’s products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).