

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 Appliance Benefits

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

- Increased visibility within virtualized infrastructure monitoring
- 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.

Platforms

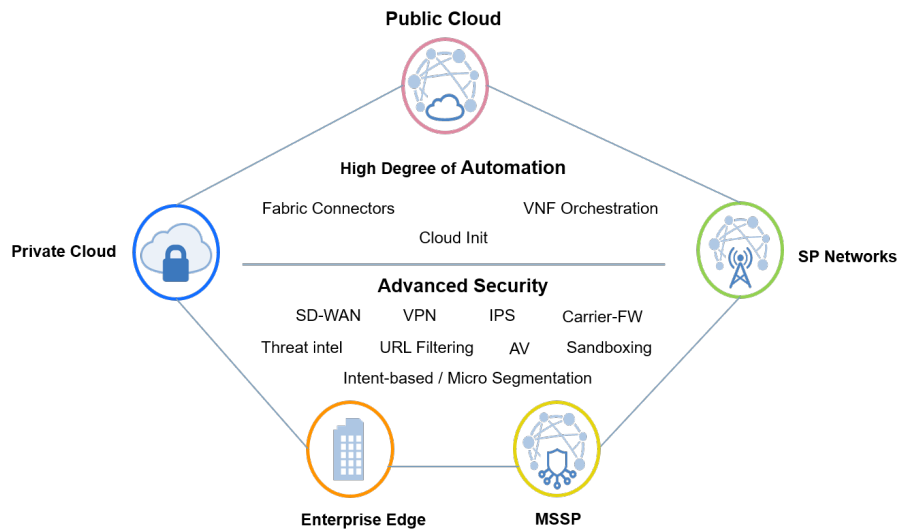
Choice of Form Factor

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 FortiOSTM 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



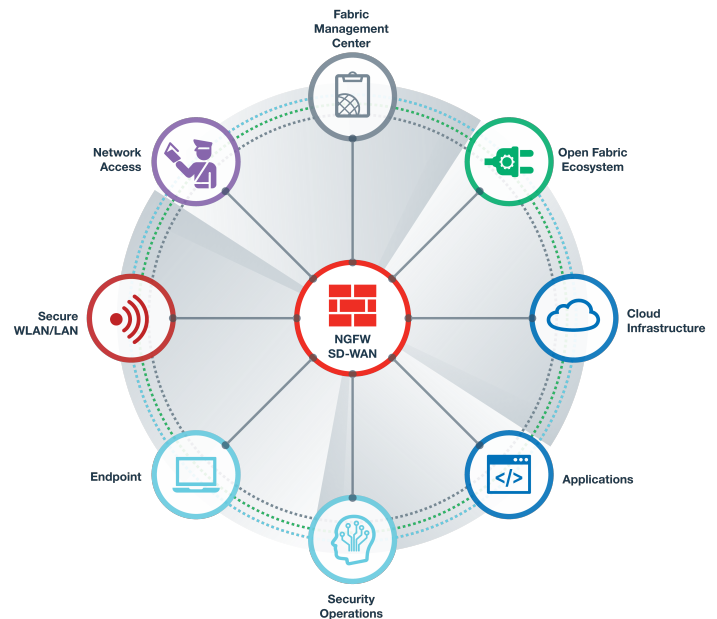
Gain comprehensive visibility and apply consistent control

Fortinet Security Fabric

Security Fabric

The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric covers the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off of the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats



FortiOS

FortiGates are the foundation of the Fortinet Security Fabric—the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Leverage the 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.
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection.
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation.
- Utilize virtual SPU hardware acceleration to boost network security performance.

Services



FortiGuard™ Security Services

FortiGuard Labs offer 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-VM01/01V/01S	FORTIGATE-VM02/02V/02S	FORTIGATE-VM04/04V/04S	FORTIGATE-VM08/08V/08S
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 1	1 / 2	1 / 4	1 / 8
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	32 / 64	256 / 512	256 / 512	1,024 / 4,096
Virtual Domains (Default / Maximum) *	10 / 10	10 / 25	10 / 50	10 / 500
Firewall Policies	10,000	10,000	10,000	200,000
Maximum Number of Registered Endpoints	2,000	2,000	8,000	20,000
Unlimited User License	Yes	Yes	Yes	Yes

	FORTIGATE-VM16/16V/16S	FORTIGATE-VM32/32V/32S	FORTIGATE-VMUL/ULV/ULS
Technical Specifications			
vCPU Support (Minimum / Maximum)	1 / 16	1 / 32	1 / unlimited
Storage Support (Minimum / Maximum)	32 GB / 2 TB	32 GB / 2 TB	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096
Virtual Domains (Default / Maximum) *	10 / 500	10 / 500	10 / 500
Firewall Policies	200,000	200,000	200,000
Maximum Number of Registered Endpoints	20,000	20,000	20,000
Unlimited User License	Yes	Yes	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 will vary 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.

* Not applicable to FG-VMxV and FG-VMxS series, which does not support VDOMs by default. See ORDER INFORMATION for VDOM addition SKUs if you require multiple VDOMs on your FortiGate-VM.

VENDOR
Private Clouds (Hypervisors)
VMware ESXi v5.5 / v6.0 / v6.5 / v6.7
VMware NSX-T v2.3*
Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019**
Microsoft AzureStack
Citrix Xen XenServer v5.6 sp2, v6.0, v6.2 and later
Open source Xen v3.4.3, 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
Nutanix AHV (AOS 5.10, Prism Central 5.10)***
Cisco Cloud Services Platform 2100***
Cisco ENCS (NFVIS 3.12.3)****

* FortiGate-VM 6.0.4+ supports VMware NSX-T.
 ** FortiGate-VM 6.2.3+ supports Microsoft Hyper-V 2019.
 *** FortiGate-VM 6.0.3+ supports Nutanix AHV and Cisco CSP 2100.
 **** FortiGate-VM 6.2.3+ supports Cisco NFVIS 3.12.3.

VENDOR
Public Clouds (Market Places)
Amazon AWS (including GovCloud and AWS China)
VMware Cloud on AWS*
VMware Cloud on Dell EMC**
Microsoft Azure (including regional Azure: US Gov, Germany, and China) and AzureStack syndication
Google GCP (Google Cloud Platform)
Oracle OCI
Alibaba Cloud (AliCloud)
Virtualization/Cloud Platform Support varies by model and FortiOS builds. Please refer to appropriate release notes. FG-VMxV series require FortiOS 5.4.8+ / 5.6.1+ / 6.0.0+.
* FortiGate-VM 6.0.4+ supports VMware Cloud on AWS.
** FortiGate-VM 6.2.3+ supports VMware Cloud on Dell EMC.

Order Information

The following SKUs adopt the perpetual licensing scheme:

Product	SKU	Description
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM 'virtual appliance'. 1x vCPU core and unlimited RAM. No VDOM by default for FG-VM01V model.
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM 'virtual appliance'. 2x vCPU cores and unlimited RAM. No VDOM by default for FG-VM02V model.
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM 'virtual appliance'. 4x vCPU cores and unlimited RAM. No VDOM by default for FG-VM04V model.
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM 'virtual appliance'. 8x vCPU cores and unlimited RAM. No VDOM by default for FG-VM08V model.
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM 'virtual appliance'. 16x vCPU cores and unlimited RAM. No VDOM by default for FG-VM016V model.
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM 'virtual appliance'. 32x vCPU cores and unlimited RAM. No VDOM by default for FG-VM032V model.
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores and RAM. No VDOM by default for FG-VMULV model.

FortiGate-VM 6.2.2 no longer has RAM restriction on all vCPU models while prior versions still restrict RAM sizes per model. Upgrade to 6.2.2 is necessary to remove the restriction.

Order Information

The following SKUs adopt the perpetual licensing scheme:

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.

FortiGate-VM 6.2.2 no longer has RAM restriction on all vCPU models while prior versions still restrict RAM sizes per model. Upgrade to 6.2.2 is necessary to remove the restriction.

The following SKUs adopt the annual subscription licensing scheme:

Product	SKU	Description
FortiGate-VM01-S	FC1-10-FGWS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (1 vCPU core)
FortiGate-VM02-S	FC2-10-FGWS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (2 vCPU cores)
FortiGate-VM04-S	FC3-10-FGWS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (4 vCPU cores)
FortiGate-VM08-S	FC4-10-FGWS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (8 vCPU cores)
FortiGate-VM16-S	FC5-10-FGWS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (16 vCPU cores)
FortiGate-VM32-S	FC6-10-FGWS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (32 vCPU cores)
FortiGate-VMUL-S	FC7-10-FGWS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (Unlimited vCPU cores)
Support Bundle		
258	FortiCare services (only) included	
815	Enterprise Bundle included	
820	360 Protection Bundle included	
990	UTM Bundle included	

FortiOS 6.2.3+ and 6.4.0+ support the FortiGate-VM S-series. It also does not have RAM restriction on all vCPU levels.

Bundles



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.

Bundles	360 Protection	Enterprise Protection	UTM	Threat Protection
FortiCare	ASE 1	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection, and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	•
FortiGuard Antispam Service	•	•	•	•
FortiGuard Security Rating Service	•	•	•	•
FortiGuard Industrial Service	•	•	•	•
FortiGuard IoT Detection Service 2	•	•	•	•
FortiConverter Service	•	•	•	•
IPAM Cloud 2	•	•	•	•
SD-WAN Orchestrator Entitlement 2	•	•	•	•
SD-WAN Cloud Assisted Monitoring	•	•	•	•
SD-WAN Overlay Controller VPN Service	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
FortiManager Cloud	•	•	•	•

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.4

