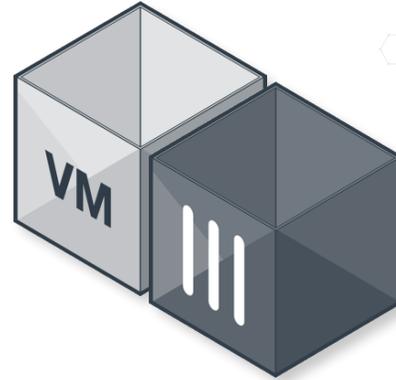


FortiGate® Virtual Appliances

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 offered by the FortiOS operating system. In addition, the appliances offer:

- Increased visibility within virtualized infrastructure
- 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.

PLATFORM

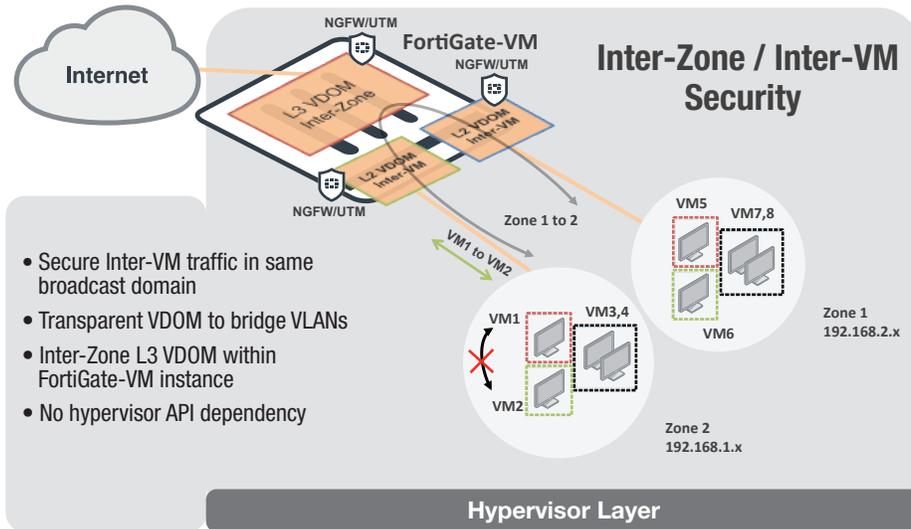
Choice of Form Factor

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.

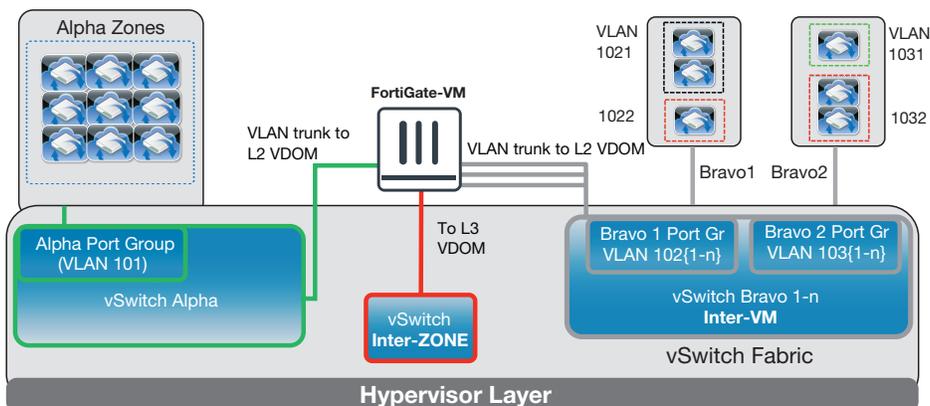
Multi-Threat Security

Using the advanced FortiOS™ 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



All Inter-VM traffic in Bravo Zones are subject to full UTM scan through L2 VDOM. Inter-Zone traffic subject to full Next Gen Firewall and UTM scan by L3 VDOM. Alpha Zone VMs can all talk to each other freely.



FORTINET SECURITY FABRIC

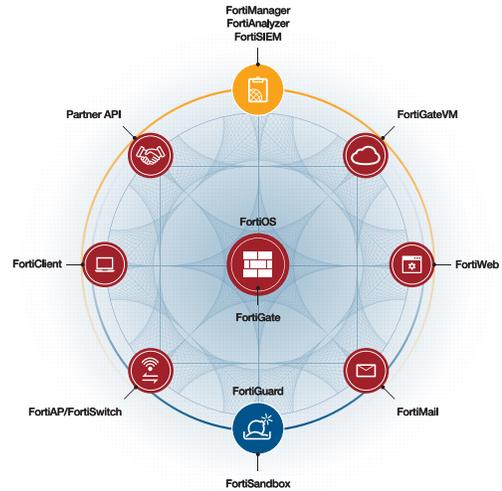
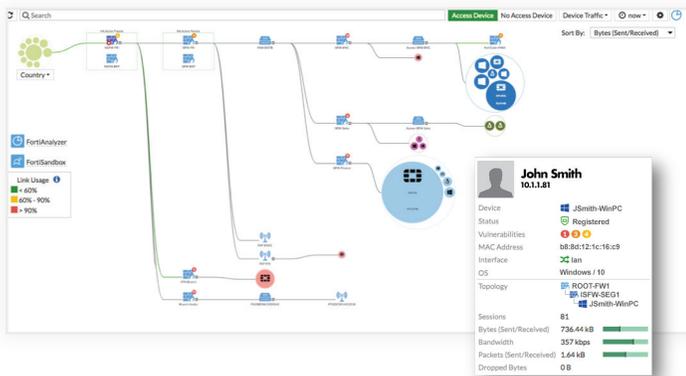
Security Fabric

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.

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 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.
- Fulfill your networking needs with extensive routing, switching, and SD-WAN capabilities.
- Utilize SPU hardware acceleration to boost security capability performance.

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.

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-VM00	FORTIGATE-VM01/01V	FORTIGATE-VM02/02V	FORTIGATE-VM04/04V
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 1	1 / 1	1 / 2	1 / 4
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10
Memory Support (Minimum / Maximum)	1 GB / 2 GB *	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB
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 / 32	32 / 64	256 / 512	256 / 512
Virtual Domains (Default / Maximum) **	2 / 2	10 / 10	10 / 25	10 / 50
Firewall Policies (VDOM / System)	5,000	20,000 / 40,000	50,000 / 100,000	50,000 / 100,000
Maximum Number of FortiTokens	1,000	1,000	1,000	5,000
Maximum Number of Registered Endpoints	200	2,000	2,000	8,000
Unlimited User License	Yes	Yes	Yes	Yes
System Performance				
Firewall Throughput (UDP Packets)	12 Gbps	12 Gbps	15 Gbps	28 Gbps
Concurrent Sessions (TCP)	1.0 Million	1.0 Million	2.6 Million	4.3 Million
New Sessions / Second (TCP)	85,000	85,000	100,000	125,000
IPsec VPN Throughput (AES256+SHA1, 512 Byte)	1 Gbps	1 Gbps	1.5 Gbps	3 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000	2,000	2,000	2,000
Client-to-Gateway IPsec VPN Tunnels	6,000	6,000	12,000	20,000
SSL-VPN Throughput	800 Mbps	800 Mbps	830 Mbps	2 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	1,000	1,000	2,000	4,500
IPS Throughput (HTTP / Enterprise Mix) ¹	3.5 Gbps / 1 Gbps	3.5 Gbps / 1 Gbps	5.5 Gbps / 1.5 Gbps	8 Gbps / 3 Gbps
Application Control Throughput ²	2 Gbps	2 Gbps	2.6 Gbps	4.5 Gbps
NGFW Throughput ³	850 Mbps	850 Mbps	1.5 Gbps	2.5 Gbps
Threat Protection Throughput ⁴	700 Mbps	700 Mbps	1.2 Gbps	2 Gbps

	FORTIGATE-VM08/08V	FORTIGATE-VM16/16V	FORTIGATE-VM32/32V	FORTIGATE-VMUL/ULV
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 8	1 / 16	1 / 32	1 / unlimited
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10
Memory Support (Minimum / Maximum)	1 GB / 12 GB	1 GB / 24 GB	1 GB / 48 GB	1 GB / Unlimited GB
Storage Support (Minimum / Maximum)	32 GB / 2 TB			
Wireless Access Points Controlled (Tunnel / Global)	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096	1,024 / 4,096
Virtual Domains (Default / Maximum) **	10 / 500	10 / 500	10 / 500	10 / 500
Firewall Policies (VDOM / System)	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000
Maximum Number of FortiTokens	5,000	5,000	5,000	5,000
Maximum Number of Registered Endpoints	20,000	20,000	20,000	20,000
Unlimited User License	Yes	Yes	Yes	Yes
System Performance				
Firewall Throughput (UDP Packets)	33 Gbps	36 Gbps	50 Gbps	
Concurrent Sessions (TCP)	8.5 Million	18.0 Million	38.0 Million	
New Sessions / Second (TCP)	150,000	175,000	200,000	
IPsec VPN Throughput (AES256+SHA1, 512 Byte)	5.5 Gbps	6.5 Gbps	7 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40,000	40,000	40,000	
Client-to-Gateway IPsec VPN Tunnels	40,000	50,000	64,000	
SSL-VPN Throughput	4.5 Gbps	8.5 Gbps	8.6 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum)	10,000	25,000	40,000	
IPS Throughput (HTTP / Enterprise Mix) ¹	15.5 Gbps / 6 Gbps	25 Gbps / 12 Gbps	29 Gbps / 19 Gbps	
Application Control Throughput ²	9 Gbps	17 Gbps	17.5 Gbps	
NGFW Throughput ³	4.5 Gbps	9 Gbps	16.5 Gbps	
Threat Protection Throughput ⁴	3.5 Gbps	7 Gbps	13 Gbps	

Actual performance may vary depending on the network and system configuration. Performance metrics were observed using a DELL R740 (CPU Intel Xeon Platinum 8168 2.7 GHz, Intel X710 network adapters), running FOS v5.6.3. Tested with VMware vSphere 6.5 Enterprise Plus. SR-IOV is enabled. 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix. 2. Application Control performance is measured with 64 Kbytes HTTP traffic. 3. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 4. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.

* Applicable to VM running on 5.6 and above.

** Not applicable to FG-VMxV series as VDOMs are not supported. FG-VMxV 6.0.0 is an exception, which supports VDOM addition with separately purchased VDOM licenses. See ORDER INFORMATION for VDOM SKUs.

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

SPECIFICATIONS

VENDOR
Private Clouds (Hypervisors)
VMware ESXi v5.0 / v5.1 / v5.5 / v6.0 / v6.5
Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016
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

VENDOR
Public Clouds (Market Places)
Amazon AWS (including GovCloud and AWS China)
VMware Cloud on AWS
Microsoft Azure (including regional Azure: US Gov, Germany, and China)
Google GCP (Google Cloud Platform)
Oracle OCI
Aliyun (Alibaba Cloud)
Note: 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+.

ORDER INFORMATION

Product	SKU	Description
FortiGate-VM00	FG-VM00	FortiGate-VM 'virtual appliance'. 1x vCPU core, (up to) 2 GB RAM. No Extreme DB support.
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM 'virtual appliance'. 1x vCPU core and (up to) 2 GB RAM. No VDOM by default for FG-VM01V model.
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM 'virtual appliance'. 2x vCPU cores and (up to) 4 GB RAM. No VDOM by default for FG-VM02V model.
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM 'virtual appliance'. 4x vCPU cores and (up to) 6 GB RAM. No VDOM by default for FG-VM04V model.
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM 'virtual appliance'. 8x vCPU cores and (up to) 12 GB RAM. No VDOM by default for FG-VM08V model.
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM 'virtual appliance'. 16x vCPU cores and (up to) 24 GB RAM. No VDOM by default for FG-VM016V model.
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM 'virtual appliance'. 32x vCPU cores and (up to) 48 GB 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.
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.

FG-VMxV™ 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.



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

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

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

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