

FortiGate® Virtual Appliances

Consolidated Security for Virtual Environments

Via a complete end-to-end security ecosystem for the Data Center, Fortinet enables and facilitates the enterprise's journey through the Data Center consolidation process.



The delivery of both physical and virtual planes security appliances it offers on one side, and the unmatched performance and security capabilities it provides on the other side, allow 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.



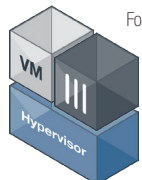
FortiGate Virtual Appliance Benefits

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 platforms



FortiGate-VM



FortiADC-VM



FortiAnalyzer-VM



FortiAuthenticator-VM



FortiCache-VM



FortiRecorder-VM



FortiMail-VM



FortiManager-VM



FortiSandbox-VM



FortiVoice-VM



FortiWeb-VM

Fortinet comprehensive virtual appliance offerings

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.

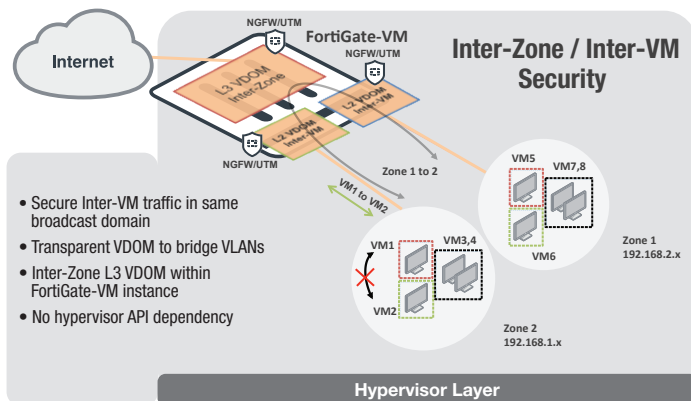
Supported Hypervisor

VENDOR	HYPERVISOR	FORTIGATE-VM			
Private Cloud Platforms					
VMware	ESX v4.0, v4.1 ESXi v5.0, v5.1, v5.5, v6.0	FG-VM00	FG-VM01	FG-VM02	FG-VM04
Citrix	XenServer v5.6 sp2, v6.0 and later	FG-VM00-Xen	FG-VM01-Xen	FG-VM02-Xen	FG-VM04-Xen
Microsoft	Hyper-V Server 2008 R2, 2012, 2012 R2	FG-VM00-HV	FG-VM01-HV	FG-VM02-HV	FG-VM04-HV
KVM	CentOS 6.4 (qemu 0.12.1) and later	FG-VM00-KVM	FG-VM01-KVM	FG-VM02-KVM	FG-VM04-KVM
Open Source Xen	v3.4.3, v4.1 and later	FG-VM00-Xen	FG-VM01-Xen	FG-VM02-Xen	FG-VM04-Xen
Public Cloud Platform					
Amazon	Amazon Web Services (AWS)*	—	FG-VM01-AWS	FG-VM02-AWS	FG-VM04-AWS
Microsoft	Azure	—	—	FG-VM02-AZ	FG-VM04-AZ

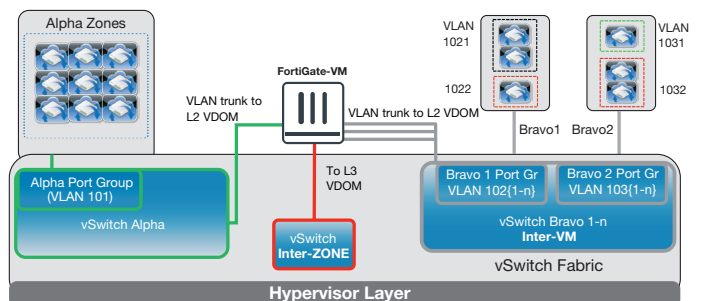
VENDOR	HYPERVISOR	FORTIGATE-VM			
Private Cloud Platforms					
VMware	ESX v4.0, v4.1 ESXi v5.0, v5.1, v5.5, v6.0	FG-VM08	FG-VM16	FG-VM32	FG-VMUL
Citrix	XenServer v5.6 sp2, v6.0 and later	FG-VM08-Xen	FG-VM16-Xen	FG-VM32-Xen	FG-VMUL-Xen
Microsoft	Hyper-V Server 2008 R2, 2012, 2012 R2	FG-VM08-HV	FG-VM16-HV	FG-VM32-HV	FG-VMUL-HV
KVM	CentOS 6.4 (qemu 0.12.1) and later	FG-VM08-KVM	FG-VM16-KVM	FG-VM32-KVM	FG-VMUL-KVM
Open Source Xen	v3.4.3, v4.1 and later	FG-VM08-Xen	FG-VM16-Xen	FG-VM32-Xen	FG-VMUL-Xen
Public Cloud Platforms					
Amazon	Amazon Web Services (AWS)*	FG-VM08-AWS	FG-VM16-AWS	FG-VM32-AWS	FG-VMUL-AWS
Microsoft	Azure	FG-VM08-AZ	FG-VM16-AZ	FG-VM32-AZ	FG-VMUL-AZ

Hypervisor Support varies according to FortiOS builds. Please refer to appropriate release notes.
 * Available as Pay-As-You-Go or Bring-Your-Own-License (BYOL). Purchase from AWS Marketplace.

DEPLOYMENT



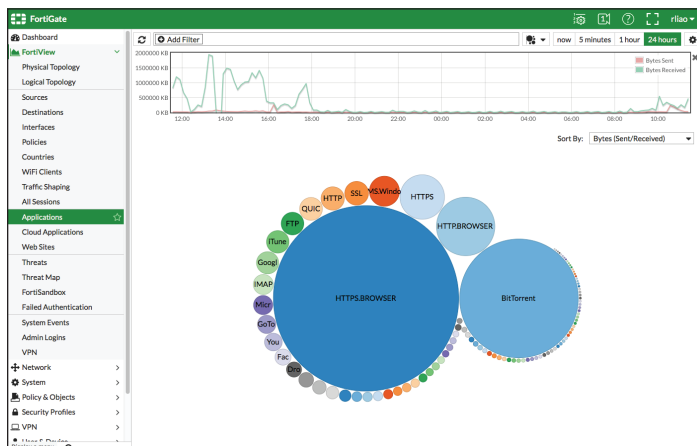
All Inter-VM traffic in Bravo Zones are subject to full UTM scan through L2 VDOM. Inter-Zone traffic subject to full Next Gen Firewall and UTM scan by L3 VDOM. Alpha Zone VMs can all talk to each other freely.



SOFTWARE

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.
- Detect, contain and block advanced attacks automatically in minutes with integrated advanced threat protection framework.
- Solve your networking needs with extensive routing, switching, WiFi, LAN and WAN capabilities.
- Activate all the SPU-booster capabilities you need on the fastest firewall platform available.



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, other network and security vendors, as well as law enforcement agencies:

- **Real-time Updates** — 24x7x365 Global Operations research security intelligence, distributed via Fortinet Distributed Network to all Fortinet platforms.
- **Security Research** — FortiGuard Labs have discovered over 170 unique zero-day vulnerabilities to date, totaling millions of automated signature updates monthly.
- **Validated Security Intelligence** — Based on FortiGuard intelligence, Fortinet's network security platform is tested and validated by the world's leading third-party testing labs and customers globally.

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:

- **Enhanced Support** — For customers who need support during local business hours only.
- **Comprehensive Support** — For customers who need around-the-clock mission critical support, including advanced exchange hardware replacement.
- **Advanced Services** — For global or regional customers who need an assigned Technical Account Manager, enhanced service level agreements, extended software support, priority escalation, on-site visits and more.
- **Professional Services** — For customers with more complex security implementations that require architecture and design services, implementation and deployment services, operational services and more.



Enterprise 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 the FortiGuard Enterprise Bundle. This bundle contains the full set of FortiGuard security services plus FortiCare service and support offering the most flexibility and broadest range of protection all in one package.

SPECIFICATIONS

	FORTIGATE-VM00	FORTIGATE-VM01	FORTIGATE-VM02	FORTIGATE-VM04
Technical Specifications				
Hypervisor Support	VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Citrix XenServer 5.6 SP2/6.0 or later, Open Source Xen 3.4.3/4.1 or later, Microsoft Hyper-V Server 2008 R2/2012/2012 R2, KVM, AWS (Amazon Web Services), Microsoft Azure			
vCPU Support (Minimum / Maximum)	1 / 1	1 / 1	1 / 2	1 / 4
Network Interface Support (Minimum / Maximum)	2 / 10	2 / 10	2 / 10	2 / 10
Memory Support (Minimum / Maximum)	1 GB / 1.5 GB	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB
Storage Support (Minimum / Maximum)	30 GB+ / 2 TB	30 GB+ / 2 TB	30 GB+ / 2 TB	30 GB+ / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	32 / 32	32 / 64	256 / 512	256 / 512
Virtual Domains (Default / Maximum)	1	10 / 10	10 / 25	10 / 50
Firewall Policies (VDOM / System)	5,000	20,000 / 40,000	50,000 / 100,000	50,000 / 100,000
Unlimited User License	Yes	Yes	Yes	Yes

	FORTIGATE-VM08	FORTIGATE-VM16	FORTIGATE-VM32	FORTIGATE-VMUL
Technical Specifications				
Hypervisor Support	VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Citrix XenServer 5.6 SP2/6.0 or later, Open Source Xen 3.4.3/4.1 or later, Microsoft Hyper-V Server 2008 R2/2012/2012 R2, KVM, AWS (Amazon Web Services), Microsoft Azure			
vCPU Support (Minimum / Maximum)	1 / 8	1 / 16	1 / 32	1 / Unlimited
Network Interface Support (Minimum / Maximum)	2 / 10	2 / 10	2 / 10	2 / 10
Memory Support (Minimum / Maximum)	1 GB / 12 GB	1 GB / 24 GB	1 GB / 48 GB	1 GB / Unlimited
Storage Support (Minimum / Maximum)	30 GB+ / 2 TB	30 GB+ / 2 TB	30 GB+ / 2 TB	30 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 / 250	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
Unlimited User License	Yes	Yes	Yes	Yes

PERFORMANCE REFERENCE

VM-08	VMWARE ESXI	CITRIX XEN	MICROSOFT HYPER-V	XEN	KVM
Maximum System Performance					
Firewall Throughput (UDP Packets)	4.0 Gbps	1.8 Gbps	1.8 Gbps	1.8 Gbps	2.2 Gbps
Concurrent Sessions (TCP)	11.0 Million	11.0 Million	11.0 Million	11.0 Million	11.0 Million
New Sessions/Second (TCP)	90,000	45,000	90,000	45,000	75,000
IPsec VPN Throughput (AES256+SHA1)	500 Mbps	235 Mbps	500 Mbps	235 Mbps	250 Mbps
Gateway-to-Gateway IPsec VPN Tunnels (VDOM / System)	5,000 / 10,000	5,000 / 10,000	5,000 / 10,000	5,000 / 10,000	5,000 / 10,000
Client-to-Gateway IPsec VPN Tunnels	64,000	64,000	64,000	64,000	64,000
SSL-VPN Throughput	2.25 Gbps	1.2 Gbps	2.0 Gbps	1.2 Gbps	2.5 Gbps
Concurrent SSL-VPN Users	25,000	25,000	25,000	25,000	25,000
IPS Throughput	5.0 Gbps	850 Mbps	2.5 Gbps	850 Mbps	2.0 Gbps
Antivirus Throughput	2.2 Gbps	750 Mbps	1.1 Gbps	750 Mbps	1.5 Gbps

Actual performance values may vary depending on the network and system configuration. Performance metrics were observed using a Dell R730 Server (Intel Xeon E5-2687W 3.1 GHz, 2x 10 GE interfaces), running FOS v5.2.3 and latest virtualization platform versions. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1.

ORDER INFORMATION

Product	SKU	Description
FortiGate-VM00	FG-VM00(-Xen/HV/KVM)	FortiGate-VM 'virtual appliance' designed for [Platform], 1x vCPU core, (up to) 1.5 GB RAM and Extreme DB NOT supported.
FortiGate-VM01	FG-VM01(-Xen/HV/KVM/AWS)	FortiGate-VM 'virtual appliance' designed for [Platform], 1x vCPU core and (up to) 2 GB RAM.
FortiGate-VM02	FG-VM02(-Xen/HV/KVM/AWS/AZ)	FortiGate-VM 'virtual appliance' designed for [Platform], 2x vCPU cores and (up to) 4 GB RAM.
FortiGate-VM04	FG-VM04(-Xen/HV/KVM/AWS/AZ)	FortiGate-VM 'virtual appliance' designed for [Platform], 4x vCPU cores and (up to) 6 GB RAM.
FortiGate-VM08	FG-VM08(-Xen/HV/KVM/AWS/AZ)	FortiGate-VM 'virtual appliance' designed for [Platform], 8x vCPU cores and (up to) 12 GB RAM.
FortiGate-VM16	FG-VM16(-Xen/HV/KVM/AWS)	FortiGate-VM 'virtual appliance' designed for [Platform], 16x vCPU cores and (up to) 24GB RAM.
FortiGate-VM32	FG-VM32(-Xen/HV/KVM/AWS)	FortiGate-VM 'virtual appliance' designed for [Platform], 32x vCPU cores and (up to) 48 GB RAM.
FortiGate-VMUL	FG-VMUL(-Xen/HV/KVM/AWS)	FortiGate-VM 'virtual appliance' designed for [Platform], Unlimited vCPU cores and unlimited RAM.
Optional Accessories		
Virtual Domain License 11-25	FG-VDOM-25	Single Blade VDOM License Key 11–25 Virtual Domain Upgrade.
Virtual Domain License 26-50	FG-VDOM-50	Single Blade VDOM License Key 26–50 Virtual Domain Upgrade.
Virtual Domain License 51-100	FG-VDOM-100	Single Blade VDOM License Key 51–100 Virtual Domain Upgrade.
Virtual Domain License 101-250	FG-VDOM-250	Single Blade VDOM License Key 101–250 Virtual Domain Upgrade.
Virtual Domain License 251-500	FG-VDOM-500	Single Blade VDOM License Key 251–500 Virtual Domain Upgrade.
Virtual Domain License 11-250	FG-VDOM	Single Blade VDOM License Key 11–250 Virtual Domain Upgrade.



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
300 Beach Road 20-01
The Concourse
Singapore 199555
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