DATA SHEET

FortiGate® Virtual Appliances

Consolidated Security
for Virtual Environments

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 — fullfilling 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.

Fortinet comprehensive virtual appliance offerings

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 these benefits:

- 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

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.

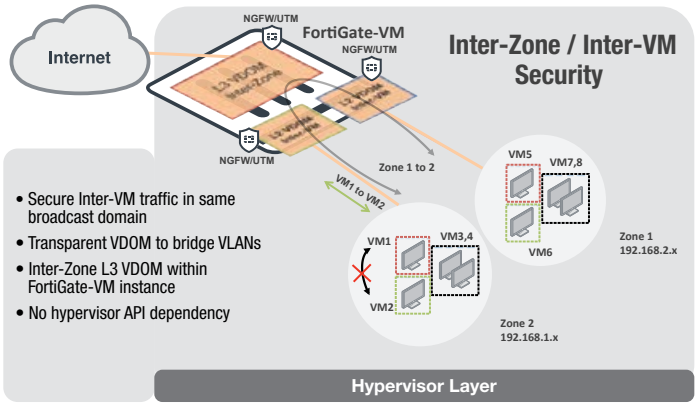
Supported Hypervisor

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	FG-VM08
Citrix	Xen Server V5.6 SP2, V6.0 and later	FG-VM00-Xen	FG-VM01-Xen	FG-VM02-Xen	FG-VM04-Xen	FG-VM08-Xen
Linux KVM	CentOS 6.4 (qemu 0.12.1) and later	FG-VM00-KVM	FG-VM01-KVM	FG-VM02-KVM	FG-VM04-KVM	FG-VM08-KVM
Microsoft	Hyper-V Server 2008 R2, 2012, and 2012 R2	FG-VM00-HV	FG-VM01-HV	FG-VM02-HV	FG-VM04-HV	FG-VM08-HV
Open Source	XenServer V3.4.3, V4.1 and later	FG-VM00-Xen	FG-VM01-Xen	FG-VM02-Xen	FG-VM04-Xen	FG-VM08-Xen
Public Cloud Platforms						
Amazon	Amazon Web Services (AWS)*	—	FG-VM01-AWS	FG-VM02-AWS	FG-VM04-AWS	FG-VM08-AWS
Microsoft	Azure	—	—	FG-VM02-AZ	FG-VM04-AZ	FG-VM08-AZ

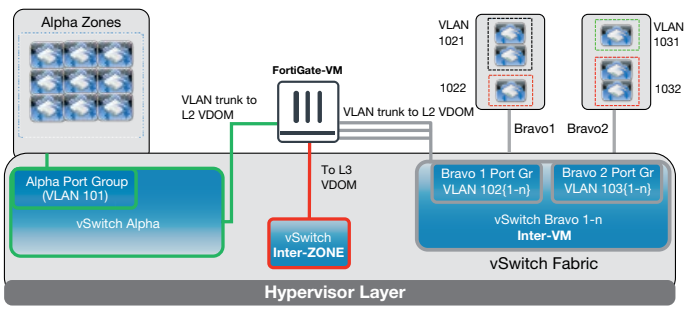
Hypervisor Support varies according to FortiOS builds. Please refer to appropriate release notes.

* 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 Managment UI — FortiView and Application Control Panel

FortiOS

FortiOS helps you protect your organization against advanced threats, configure and deploy your network security faster and see deep into what's happening inside your network. It enables organization to set up policies specific to types of devices, users and applications with industry-leading security capabilities. The feature set is consistent for both virtual and physical appliance and can be managed on a single centralized platform. In essence, FortiOS delivers:

- **Comprehensive Security** — Control thousands of applications and stop more threats with NSS Labs Recommended IPS, sandboxing, VB100 certified antimalware and more.
- **Superior Control and Visibility** — Stay in control with rich visibility over network traffic, granular policy control, and intuitive, scalable security and network management.
- **Robust Networking Capabilities** — Optimize your network with extensive switching and routing, high availability, WAN optimization, embedded WiFi controller, and a range of virtual options.

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.

For more information, please refer to http://forti.net/guard

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.
- **Premium 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.

For more information, please refer to http://forti.net/care

SPECIFICATIONS

	FORTIGATE-VM00	FORTIGATE-VM01	FORTIGATE-VM02	FORTIGATE-VM04	FORTIGATE-VM08
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 2008 R2/2012/2012 R2, KVM, AWS (Amazon Web Services), Microsoft Azure				
vCPU Support (Minimum / Maximum)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
Network Interface Support (Minimum / Maximum)	2 / 10	2 / 10	2 / 10	2 / 10	2 / 10
Memory Support (Minimum / Maximum)	1 GB / 1 GB	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB	1 GB / 12 GB
Storage Support (Minimum / Maximum)	30 GB / 2 TB	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	1,024 / 4,096
Virtual Domains (Default / Maximum)	1	10 / 10	10 / 25	10 / 50	10 / 250
Firewall Policies (VDOM / System)	5,000	20,000 / 40,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000
Unlimited User License	Yes	Yes	Yes	Yes	Yes

	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, 1 GB RAM only 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.
Optional Accessories		
Virtual Domain (VDOM) Upgrade License 11-25	FG-VDOM-25	Single Blade VDOM License Key 11 to 25 Virtual Domain Upgrade.
Virtual Domain (VDOM) Upgrade License 26-50	FG-VDOM-50	Single Blade VDOM License Key 26 to 50 Virtual Domain Upgrade.
Virtual Domain (VDOM) Upgrade License 51-100	FG-VDOM-100	Single Blade VDOM License Key 51 to 100 Virtual Domain Upgrade.
Virtual Domain (VDOM) Upgrade License 101-250	FG-VDOM-250	Single Blade VDOM License Key 101 to 250 Virtual Domain Upgrade.
Virtual Domain (VDOM) Upgrade License 11-250	FG-VDOM	Single Blade VDOM License Key 11 to 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
Valbonne 06560
Alpes-Maritimes, 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

FORTINET

Fortinet Product Matrix

產品	效能	Description	作業版本
Fortinet 標準版資安防護系統 一年授權	防護系統 一年授權	提供防火牆控管存取政策，使用者身份辨識，IPSEC VPN，SSL VPN, SLB(主機負載平衡）及 無線網路控制器（Wireless Controller）	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
Fortinet 標準版資安防護系統 防護升級模組 一年授權	防護升級模組 一年授權		
Fortinet 高階版資安防護系統 一年授權	高階版防護系統 一年授權	提供防火牆控管存取政策，使用者身份辨識，IPSEC VPN，SSL VPN, SLB(主機負載平衡）， 無線網路控制器（Wireless Controller），入侵防禦，應用程式控管，防毒，不當網頁過濾，防垃圾郵件	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
Fortinet 高階版資安防護系統 防護升級模組 一年授權	高階版資安防護系統 防護升級模組 一年授權		
FMG-VM-Base Fortinet 集中管理系統	集中管理系統 10 台設備	Fortinet 防火牆管理，設定和集中派送（政策，資安防禦資料庫）的中央管理系統 r, 支援 10 台設備	Vmware Hyper-V AWS
FMG-VM-10-UG Fortinet 集中管理系統	集中管理平台設備 數量升級 - 10 台設備		
FAZ-VM-BASEFortinet 集中日誌報表系統	集中日誌報表系統	Fortinet 防火牆的集中日誌報表管理系統	Vmware Hyper-V AWS
FAZ-VM-GB1 Fortinet 集中日誌報表系統 紀錄數量升級 - 1 GB/Day	集中日誌報表系統 紀錄數量升級 - 1 GB/Day		
FSA-VM Fortinet 先進威脅防護系統 (ATP)	先進威脅防護系統 (ATP)	即時執行沙箱檢測，提供虛擬的運行環境來分析高風險或可疑的程式，研判威脅完整的生命周期，協助用戶智慧地立即偵測出既存與新興的 網路威脅。	VMware
FWB-Base Fortinet 網站應用程式防火牆(WAF) 25Mbps	網站應用程式防火牆(WAF) 25Mbps	提供網站應用程式防火牆功能（WAF）， 網頁防置換，網頁自動備份及回復等功能	Vmware Hyper-V Citrix Xen Open Xen AWS
FWB-100-UG Fortinet 網站應用程式防火牆(WAF) 頻寬升級 100Mbps	網站應用程式防火牆(WAF) 頻寬升級 100Mbps		

FWB-VM01/VM02/VM04/VM08 Fortinet 網站應用程式防火牆(WAF) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	網站應用程式防火牆(WAF) 支援 1 CPU		
FAD-Base Fortinet 主機負載平衡系統 (SLB) 1Gbps	主機負載平衡系統(SLB) 1Gbps	支援網路的主機負載平衡，全球服務負載平衡（GSLB）及線路負載平衡（LLB）等功能	VMware
FAD-1000-UG Fortinet 主機負載平衡系統 (SLB) 頻寬升級 1Gbps	主機負載平衡系統(SLB) 頻寬升級 1Gbps		
FAD-VM01/VM02/VM04/VM08 Fortinet 主機負載平衡系統(SLB) (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	主機負載平衡系統(SLB) 支援 1 CPU		
FML-Base Fortinet 反垃圾郵件及郵件保全系統 100 人版	反垃圾郵件及郵件保全系統 100 人版	提供電子郵件主機功能、過濾並攔截垃圾郵件	VMware Hyper-V Citrix Xen KVM
FML-300-UG Fortinet 反垃圾郵件及郵件保全系統 使用者數量升級 300 人	反垃圾郵件及郵件保全系統 使用者數量升級 300 人		
FML-VM01/VM02/VM04/VM08 Fortinet 反垃圾郵件及郵件保全系統 (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	反垃圾郵件及郵件保全系統 支援 1 CPU		
FAC-VM-Base Fortinet 身份認證系統 (Authenticator) 100 人版	身份認證系統(Authenticator) 100 人版	整合 RADIUS、LDAP 伺服器，提供標準及安全的雙因子認證	VMWare Hyper-V
FAC-VM-100-UGFortinet 身份認證系統 (Authenticator) 使用者數量升級 100 人	身份認證系統(Authenticator) 使用者數量升級 100 人		