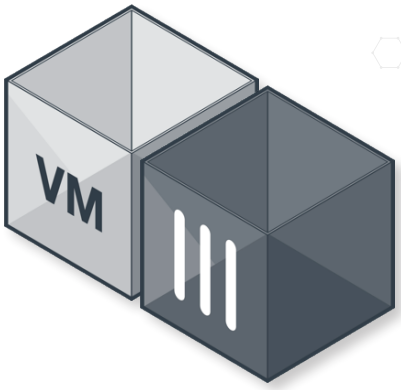
FortiGate® Virtual Appliances

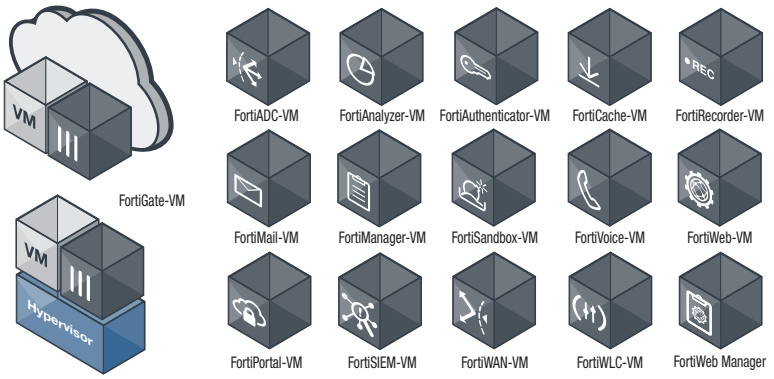
Consolidated Security for Virtualized Environments

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.



Fortinet's comprehensive security virtual appliance lineup supports in excess of 16 solutions.

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

PLATFORM

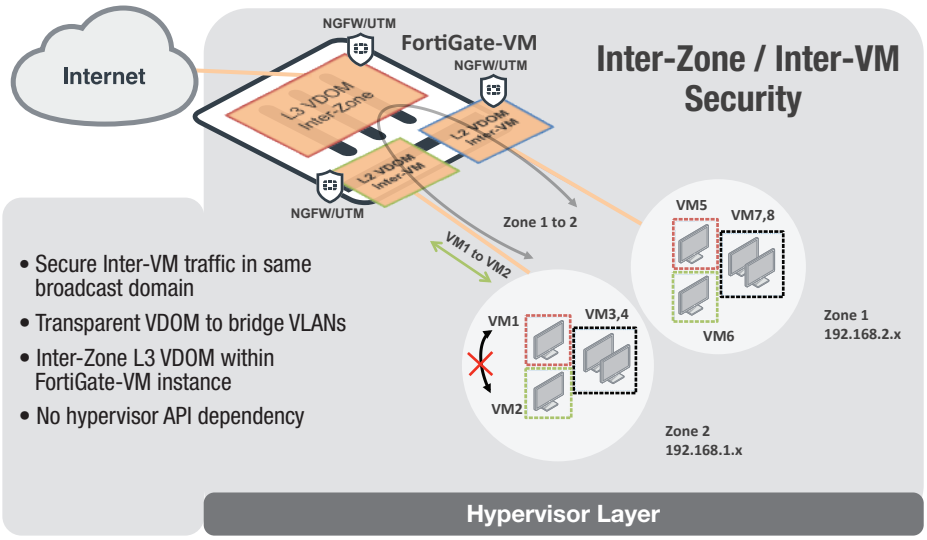
Choice of Form Factor

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.

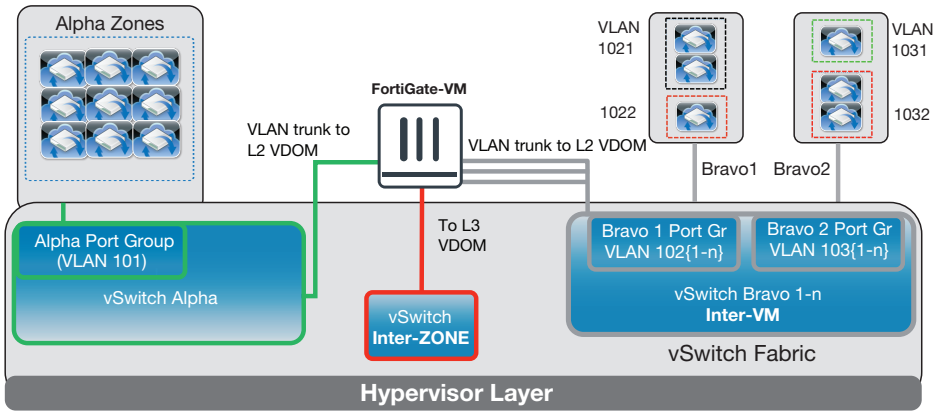
Multi-Threat Security

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



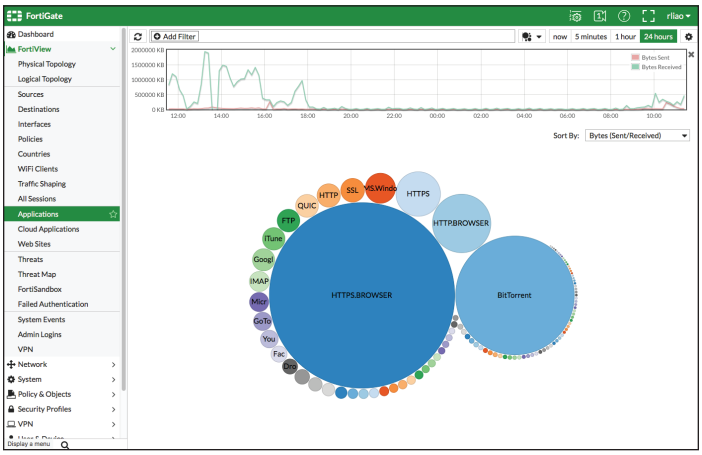
All Inter-VM traffic in Bravo Zones are subject to full UTM scan through L2 VDOM. Inter-Zone traffic subject to full Next Gen Firewall and UTM scan by L3 VDOM. Alpha Zone VMs can all talk to each other freely.



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-boosted 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-VM01/01V	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)	1 / 1	1 / 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	N/A	2,000	2,000	8,000
Unlimited User License	Yes	Yes	Yes	Yes
System Performance				
Firewall Throughput (UDP Packets, SR-IOV Enabled)		9.0 Gbps	11.5 Gbps	15.0 Gbps
Concurrent Sessions (TCP)		1.0 Million	2.6 Million	4.3 Million
New Sessions / Second (TCP)		85,000	100,000	125,000
IPsec VPN Throughput (AES256+SHA1, 512 Byte)		850 Mbps	1.15 Gbps	2.65 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		2,000	2,000	2,000
Client-to-Gateway IPsec VPN Tunnels		6,000	12,000	20,000
SSL-VPN Throughput		500 Mbps	750 Mbps	1.5 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)		1,000	2,000	4,500
IPS Throughput (HTTP / Enterprise Mix) [1]		3.0 Gbps / 950 Mbps	4.4 Gbps / 1.7 Gbps	7.5 Gbps / 3.0 Gbps
Application Control Throughput [2]		1.5 Gbps	2.6 Gbps	4.0 Gbps
NGFW Throughput [3]		550 Mbps	1.3 Gbps	2.2 Gbps
Threat Protection Throughput [4]		450 Mbps	1.0 Gbps	1.7 Gbps
CAPWAP Throughput [5]		1.0 Gbps	1.6 Gbps	2.4 Gbps

	FORTIGATE-VM08/08V	FORTIGATE-VM16/16V	FORTIGATE-VM32/32V	FORTIGATE-VMUL/ULV
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 8	1 / 16	1 / 16	1 / 16
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	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	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
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, SR-IOV Enabled)	20.0 Gbps	25.0 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)	5.2 Gbps	6.25 Gbps	6.85 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	3.5 Gbps	6.0 Gbps	7.3 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum)	10,000	25,000	40,000	
IPS Throughput (HTTP / Enterprise Mix) [1]	13.5 Gbps / 5.5 Gbps	16.5 Gbps / 9.5 Gbps	18.3 Gbps / 15.5 Gbps	
Application Control Throughput [2]	8.0 Gbps	11.0 Gbps	14.0 Gbps	
NGFW Throughput [3]	4.0 Gbps	5.5 Gbps	11.0 Gbps	
Threat Protection Throughput [4]	3.2 Gbps	4.5 Gbps	8.8 Gbps	

Actual performance may vary depending on the network and system configuration. Performance metrics were observed using a Del R730 Server (Intel E5-2687W 3.1 GHz, 2x 10 GE interfaces) running FOS v5.6. 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.

SPECIFICATIONS

VENDOR	
Private Cloud Platforms	
Fortinet	FortiHypervisor v1.0 and newer
VMware	ESXi v4.0 and newer
Citrix	XenServer v6.0 and newer
Microsoft	Hyper-V 2008R2 and newer
KVM	CentOS v6.4 (qemu 0.12.1) and newer

VENDOR	
Public Cloud Platforms	
Amazon	AWS (Amazon Web Services)
Microsoft	Azure and Azure Stack
Oracle	OPC (Oracle Public Cloud)
Google	GCP (Google Cloud Platform)

Note: Virtualization/Cloud Platform Support varies by model and FortiOS builds. Please refer to appropriate release notes.

ORDER INFORMATION

Product	SKU	Description
FortiGate-VM00	FG-VM00	FortiGate-VM 'virtual appliance'. 1x vCPU core, (up to) 2 GB RAM. No VDOM or Extreme DB support.
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM 'virtual appliance'. 1x vCPU core and (up to) 2 GB RAM. No VDOM support 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 support 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 support 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 support 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 support 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 support for FG-VM032V model.
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores and RAM. No VDOM support FG-VMULV model.
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

FST-PROD-DS-GTVMR4

FG-VM-DAT-R15-201708