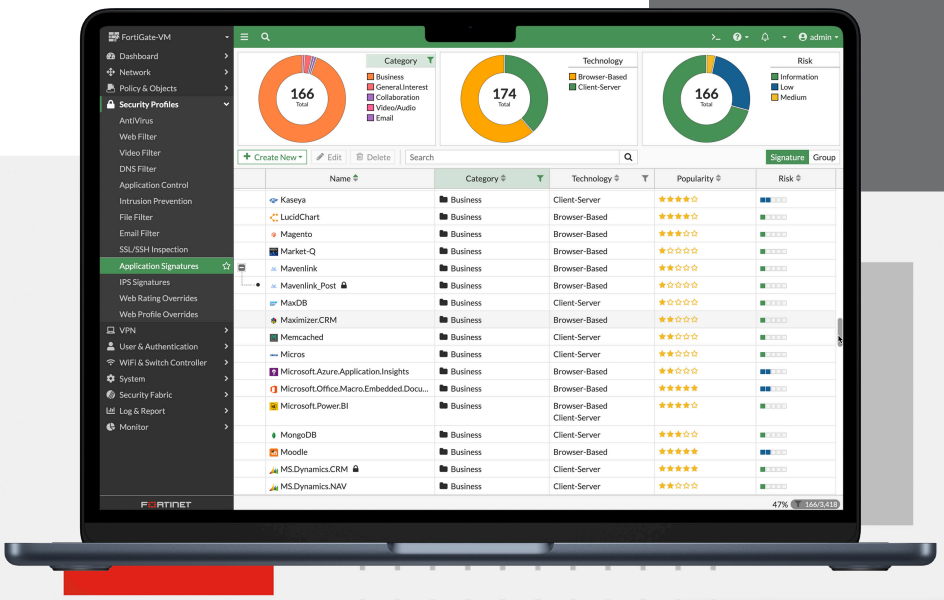
FortiGate®-VM on Linux KVM



Highlights

- Comprehensive network security functions, including firewall, VPN, intrusion prevention, web filtering, anti-virus, and anti-malware protection
- A high degree of flexibility and scalability to meet the changing needs
- Can be easily and quickly deployed in a virtual environment, reducing hardware costs and increasing operational efficiency
- Support high availability configurations to ensure network security and uptime

Delivering Next Generation Firewall Capabilities

The FortiGate-VM on Linux KVM delivers next-generation firewall capabilities for organizations of all sizes, with the flexibility to be deployed as next-generation firewall or VPN gateway. It protects against cyber threats with high performance, security efficacy, and deep visibility.

FortiGate VM allows administrators to easily and quickly deploy network security in a virtual environment, providing a high level of flexibility and scalability to meet the changing needs. It offers the benefits of virtualization, such as reduced hardware costs, increased operational efficiency, and easier disaster recovery and business continuity.

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's advanced operating system

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

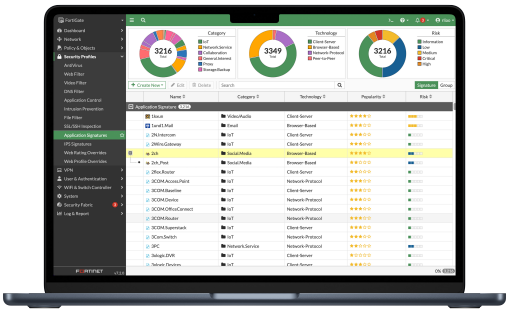
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations



Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Migration Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.



FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

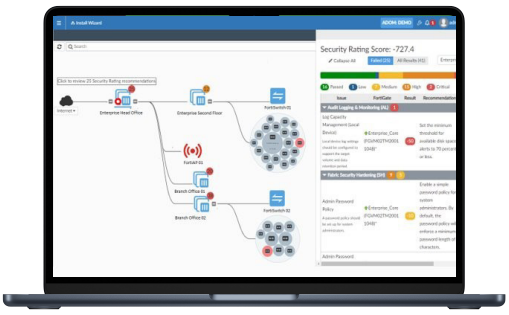
Advanced Virtual Security Processing Units (vSPUs)

Virtual firewalls are commonly used to protect virtualized environments in software-defined data centers and multi-cloud environments on the basis that they are the least expensive and the most portable, enabling users to easily move a virtual firewall from cloud to cloud. One disadvantage of most virtual firewalls is that they deliver significantly lower network throughput as compared with physical firewalls, creating bottlenecks throughout the network and reducing business agility and performance.

FortiGate virtual firewalls (FortiGate-VM), featuring advanced virtual security processing units (vSPUs), overcome the throughput barrier to provide top performance in private and public clouds. With FortiGate-VM, organizations can securely migrate any application and support a variety of use cases, including highly available large-scale virtual private networks (VPNs) in the cloud."

FortiGate-VM removes the cost-performance barriers to adopting virtual NGFWs, with several industry-leading features:

- The FortiGate-VM vSPU is a unique technology that enhances performance by offloading part of packet processing to user space, while using a kernel bypass solution within the operating system. With vSPU enabled, FortiGate-VM can achieve more than triple the throughput for a UDP firewall rule
- Support for Intel QuickAssist Technology (Intel QAT), working on the latest QuickAssist Adapters, accelerates traffic processing through site-to-site IPSec VPNs. With QAT enabled, FortiGate-VM can achieve two to three times throughput improvements depending on the packet frame size
- Fortinet is the first NGFW vendor to support AWS C5n instances, which enables organizations to use a virtual firewall to secure compute-heavy applications in the cloud



Intuitive view and clear insights into network security posture with FortiManager

Centralized Network and Security Management at Scale

FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving as the fundamental component for deploying Hybrid Mesh Firewalls.

Deployment

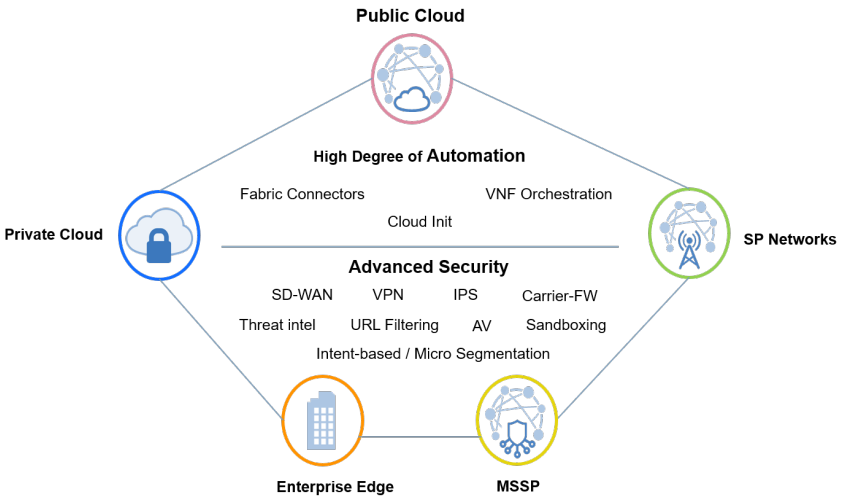
Next Generation Firewall (NGFW)

- Reduce complexity by combining threat protection security capabilities into single high-performance network security appliances
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Deliver the industry's highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection

VPN Gateway

- Direct Connect utilizing FortiGate firewalls for SSL and IPsec VPNs into and out of the AWS VPCs
- VGW to FortiGate VPN between VPCs
- Hybrid cloud site to site IPsec VPN
- Remote access VPN

Gain Comprehensive Visibility and Apply Consistent Control



Technologies

SR-IOV (Single Root I/O Virtualization)

In enabling SR-IOV on the KVM host, a single physical network controller can be partitioned into multiple virtual interfaces (called virtual functions (VFs)), consisting of an ESXi virtual network pool of adapters, which can be used by local host processors or directly by virtual machines like the FortiGate-VM. The VM then talks directly to the network adapters through Direct Memory Access (DMA) by bypassing virtualization transports, which will improve north-south network performance.

Data Plane Development Kit (DPDK) and vNP Offloading

DPDK and vNP enhance FortiGate-VM performance by offloading part of packet processing to userspace while bypassing kernel within the operating system. The capability must be enabled and configured with FortiGate CLI commands.

Specifications

	FortiGate-VM01S		FortiGate-VM02S	
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 1		1 / 2	
Memory Support (Minimum)	2 GB		2 GB	
Network Interface Support (Minimum / Maximum) [1]	1 / 24		1 / 24	
Storage Support (Minimum / Maximum)	32 GB / 2 TB		32 GB / 2 TB	
Wireless Access Points Controlled (Tunnel / Global)	32 / 64		512 / 1024	
Virtual Domains (Default / Maximum) [2]	2 / 10		2 / 25	
Firewall Policies	10 000		10 000	
Maximum Number of Registered Endpoints	2000		2000	
Unlimited User License	Yes		Yes	
System Performance	**SR-IOV/vSPU-off**	**SR-IOV/vSPU-on**	**SR-IOV/vSPU-off**	**SR-IOV/vSPU-on**
Firewall Throughput (UDP Packets, 1518 Byte)	10.5 Gbps	N/A [8]	15.7 Gbps	40.2 Gbps
Firewall Throughput (UDP Packets, 512 Byte)	4.5 Gbps	N/A [8]	6.8 Gbps	13.1 Gbps
Firewall Throughput (UDP Packets, 64 Byte)	0.9 Gbps	N/A [8]	1.2 Gbps	1.9 Gbps
IPSec VPN UDP Throughput-1360 (AES256GCM)	0.6 Gbps	N/A [8]	1 Gbps	10.8 Gbps
New Sessions / Second (TCP)	100K	N/A [8]	151K	99K
Concurrent Connections (TCP)	1.5M (RAM: 4GB)	N/A [8]	3.5M (RAM: 8GB)	1.5M (RAM: 8GB)
Application Control Throughput (HTTP 64K)	1.5 Gbps	N/A [8]	2.8 Gbps	3 Gbps
IPS Throughput (Enterprise Mix)	0.9 Gbps	N/A [8]	1.9 Gbps	2.2 Gbps
IPS Throughput (HTTP 1M)	1.3 Gbps	N/A [8]	2.3 Gbps	2.4 Gbps
NGFW Throughput (Enterprise Mix)	0.7 Gbps	N/A [8]	1.5 Gbps	1.6 Gbps
Threat Protection Throughput (Enterprise Mix)	0.4 Gbps	N/A [8]	1.1 Gbps	1.2 Gbps
SSL VPN Throughput	1.5 Gbps	N/A [8]	1.6 Gbps	N/A
Inline SSL IPS HTTPS Throughput (TLS v1.2)	0.5 Gbps	N/A [8]	0.9 Gbps	1.2 Gbps

Note. All performance values are “up to“ and vary depending on system configuration.

Datasheet numbers should only be used as a guidance for VM sizing, rather than a definitive information since performance measures vary quite significantly based up on the selected testbed (hardware + host OS), FortiOS version and configuration, as well as the tunning applied to achieve more performance. For numbers alinged with your own environment, make sure you engage with one of our pre-sales representatives for specific guidance before purchasing any licenses.

Actual performance may vary depending on the network and system configuration. Note that these metrics are updated periodically as the product performance keeps improving through internal testing. The discrepancy in the performance numbers may be noted in different versions of the document so ensure that you refer to the latest datasheets.

Performance metrics were observed using DELL R740 (CPU Intel Xeon Platinum 8268 CPU, 192G memory), with SRIVO NIC Intel X710. Tested with FortiOS 7.0.6 running on KVM/ RedHat 8.4.

vSPU refers to the combination of FortiOS vNP and DPDK libraries in the FortiGate-VM. vNP is the software emulation of a subset of Fortinet’s Network Processor (NP).

1. Applicable to 7.0.6+. The actual working number of consumable network interfaces varies depending on the Linux RedHat KVM instance types/sizes and may be less.
2. FG-VMxxS series do not come with a multi-VDOM feature by default. You can add it by applying separate VDOM addition perpetual/subscription licenses. See ORDER INFORMATION for VDOM SKUs.
3. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
4. Application Control performance is measured with 64 Kbyte HTTP traffic.
5. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
6. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix
7. SSL-VPN does not support vSPU in the tested firmware.
8. vSPU requires at least 2vCPUs.

Specifications

	FortiGate-VM04S		FortiGate-VM08S	
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 4		1 / 8	
Memory Support (Minimum)	2 GB		2 GB	
Network Interface Support (Minimum / Maximum) [1]	1 / 24		1 / 24	
Storage Support (Minimum / Maximum)	32 GB / 2 TB		32 GB / 2 TB	
Wireless Access Points Controlled (Tunnel / Global)	512 / 1024		1024 / 4096	
Virtual Domains (Default / Maximum) [2]	2 / 50		2 / 500	
Firewall Policies	10 000		200 000	
Maximum Number of Registered Endpoints	8000		20 000	
Unlimited User License	Yes		Yes	
System Performance	**SR-IOV/vSPU-off**	**SR-IOV/vSPU-on**	**SR-IOV/vSPU-off**	**SR-IOV/vSPU-on**
Firewall Throughput (UDP Packets, 1518 Byte)	30 Gbps	71.2 Gbps	44.2 Gbps	110.3 Gbps
Firewall Throughput (UDP Packets, 512 Byte)	12.8 Gbps	26.3 Gbps	19.7 Gbps	36.8 Gbps
Firewall Throughput (UDP Packets, 64 Byte)	2.2 Gbps	2.6 Gbps	3.8 Gbps	4.5 Gbps
IPSec VPN UDP Throughput-1360 (AES256GCM)	2.2 Gbps	20 Gbps	5.5 Gbps	32.5 Gbps
New Sessions / Second (TCP)	122K	160K	380K	251K
Concurrent Connections (TCP)	6M (RAM: 12GB)	2.5M (RAM: 12GB)	12M (RAM: 24GB)	6.5M (RAM: 24GB)
Application Control Throughput (HTTP 64K)	5.4 Gbps	5.7 Gbps	11 Gbps	11.8 Gbps
IPS Throughput (Enterprise Mix)	3.5 Gbps	3.8 Gbps	6.1 Gbps	6.5 Gbps
IPS Throughput (HTTP 1M)	4.3 Gbps	4.7 Gbps	8.1 Gbps	11.5 Gbps
NGFW Throughput (Enterprise Mix)	2.9 Gbps	3.1 Gbps	5 Gbps	4.8 Gbps
Threat Protection Throughput (Enterprise Mix)	1.9 Gbps	1.9 Gbps	3.8 Gbps	4.2 Gbps
SSL VPN Throughput	3.9 Gbps	N/A	7.9 Gbps	N/A
Inline SSL IPS HTTPS Throughput (TLS v1.2)	1.7 Gbps	2.3 Gbps	3.3 Gbps	4.5 Gbps

Note. All performance values are “up to“ and vary depending on system configuration.

Datasheet numbers should only be used as a guidance for VM sizing, rather than a definitive information since performance measures vary quite significantly based up on the selected testbed (hardware + host OS), FortiOS version and configuration, as well as the tunning applied to achieve more performance. For numbers alinged with your own environment, make sure you engage with one of our pre-sales representatives for specific guidance before purchasing any licenses.

Actual performance may vary depending on the network and system configuration. Note that these metrics are updated periodically as the product performance keeps improving through internal testing. The discrepancy in the performance numbers may be noted in different versions of the document so ensure that you refer to the latest datasheets.

Performance metrics were observed using DELL R740 (CPU Intel Xeon Platinum 8268 CPU, 192G memory), with SRIVO NIC Intel X710. Tested with FortiOS 7.0.6 running on KVM/ RedHat 8.4.

vSPU refers to the combination of FortiOS vNP and DPDK libraries in the FortiGate-VM. vNP is the software emulation of a subset of Fortinet’s Network Processor (NP).

1. Applicable to 7.0.6+. The actual working number of consumable network interfaces varies depending on the Linux RedHat KVM instance types/sizes and may be less.
2. FG-VMxxS series do not come with a multi-VDOM feature by default. You can add it by applying separate VDOM addition perpetual/subscription licenses. See ORDER INFORMATION for VDOM SKUs.
3. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
4. Application Control performance is measured with 64 Kbyte HTTP traffic.
5. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
6. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix
7. SSL-VPN does not support vSPU in the tested firmware.
8. vSPU requires at least 2vCPUs.

Specifications

	FortiGate-VM16S		FortiGate-VM32S	
Technical Specifications				
vCPU Support (Minimum / Maximum)	1 / 16		1 / 32	
Memory Support (Minimum)	2 GB		2 GB	
Network Interface Support (Minimum / Maximum) [1]	1 / 24		1 / 24	
Storage Support (Minimum / Maximum)	32 GB / 2 TB		32 GB / 2 TB	
Wireless Access Points Controlled (Tunnel / Global)	1024 / 4096		1024 / 4096	
Virtual Domains (Default / Maximum) [2]	2 / 500		2 / 500	
Firewall Policies	200 000		200 000	
Maximum Number of Registered Endpoints	20 000		20 000	
Unlimited User License	Yes		Yes	
System Performance	**SR-IOV/vSPU-off**	**SR-IOV/vSPU-on**	**SR-IOV/vSPU-off**	**SR-IOV/vSPU-on**
Firewall Throughput (UDP Packets, 1518 Byte)	65.3 Gbps	110.7 Gbps	96.7 Gbps	111.9 Gbps
Firewall Throughput (UDP Packets, 512 Byte)	33.8 Gbps	37.5 Gbps	44 Gbps	41.3 Gbps
Firewall Throughput (UDP Packets, 64 Byte)	5 Gbps	4.9 Gbps	7.4 Gbps	6 Gbps
IPSec VPN UDP Throughput-1360 (AES256GCM)	6.9 Gbps	42.3 Gbps	11.1 Gbps	47.3 Gbps
New Sessions / Second (TCP)	684K	520K	822K	423K
Concurrent Connections (TCP)	27M (RAM: 48GB)	14M (RAM: 48GB)	55.3M (RAM: 96GB)	29M (RAM: 96GB)
Application Control Throughput (HTTP 64K)	21.5 Gbps	22.6 Gbps	27.6 Gbps	36.1 Gbps
IPS Throughput (Enterprise Mix)	11.1 Gbps	12.7 Gbps	16.1 Gbps	22.5 Gbps
IPS Throughput (HTTP 1M)	11.7 Gbps	18.4 Gbps	16.9 Gbps	22.8 Gbps
NGFW Throughput (Enterprise Mix)	9.3 Gbps	10.6 Gbps	14.6 Gbps	16.8 Gbps
Threat Protection Throughput (Enterprise Mix)	7.2 Gbps	7.8 Gbps	11.5 Gbps	13.5 Gbps
SSL VPN Throughput	8.5 Gbps	N/A	11.7 Gbps	N/A
Inline SSL IPS HTTPS Throughput (TLS v1.2)	6.6 Gbps	8.8 Gbps	10 Gbps	11 Gbps

	FortiGate-VMULS
Technical Specifications	
vCPU Support (Minimum / Maximum)	1 / unlimited
Memory Support (Minimum)	2 GB
Network Interface Support (Minimum / Maximum) [1]	1 / 24
Storage Support (Minimum / Maximum)	32 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	1024 / 4096
Virtual Domains (Default / Maximum) [2]	2 / 500
Firewall Policies	200 000
Maximum Number of Registered Endpoints	20 000
Unlimited User License	Yes

Note. All performance values are “up to“ and vary depending on system configuration.

Datasheet numbers should only be used as a guidance for VM sizing, rather than a definitive information since performance measures vary quite significantly based up on the selected testbed (hardware + host OS), FortiOS version and configuration, as well as the tunning applied to achieve more performance. For numbers alinged with your own environment, make sure you engage with one of our pre-sales representatives for specific guidance before purchasing any licenses.

Actual performance may vary depending on the network and system configuration. Note that these metrics are updated periodically as the product performance keeps improving through internal testing. The discrepancy in the performance numbers may be noted in different versions of the document so ensure that you refer to the latest datasheets.

Performance metrics were observed using DELL R740 (CPU Intel Xeon Platinum 8268 CPU, 192G memory), with SRIVO NIC Intel X710. Tested with FortiOS 7.0.6 running on KVM/ RedHat 8.4.

vSPU refers to the combination of FortiOS vNP and DPDK libraries in the FortiGate-VM. vNP is the software emulation of a subset of Fortinet’s Network Processor (NP).

1. Applicable to 7.0.6+. The actual working number of consumable network interfaces varies depending on the Linux RedHat KVM instance types/sizes and may be less.
2. FG-VMxxS series do not come with a multi-VDOM feature by default. You can add it by applying separate VDOM addition perpetual/subscription licenses. See ORDER INFORMATION for VDOM SKUs.
3. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
4. Application Control performance is measured with 64 Kbyte HTTP traffic.
5. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
6. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix
7. SSL-VPN does not support vSPU in the tested firmware.
8. vSPU requires at least 2vCPUs.

Ordering Information

The following SKUs adopt the annual subscription licensing scheme:

Product	SKU	Description
FortiGate-VM01-S	FC1-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (1 vCPU core).
FortiGate-VM02-S	FC2-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (2 vCPU cores).
FortiGate-VM04-S	FC3-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (4 vCPU cores).
FortiGate-VM08-S	FC4-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (8 vCPU cores).
FortiGate-VM16-S	FC5-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (16 vCPU cores).
FortiGate-VM32-S	FC6-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (32 vCPU cores).
FortiGate-VMUL-S	FC7-10-FGVVS-<Support Bundle>-02-DD	Subscriptions license for FortiGate-VM (Unlimited vCPU cores).

FortiOS 6.2.3+ and 6.4.0+ support the FortiGate-VM S-series. The FortiGate-VM S-series does not have RAM restrictions on all vCPU levels.
FortiManager 6.2.3+ and 6.4.0+ support managing FortiGate-VM S-series devices.

Optional Accessories/Spares	SKU	Description
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.

For the sizing guide, please refer to the sizing document available on www.fortinet.com

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles: Enterprise Protection	Bundles: Unified Threat Protection	Bundles: Advanced Threat Protection	Bundles: SD-WAN
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•	
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct, AI-based Heurestic AV, FortiGate Cloud Sandbox[1]	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video Filtering, Malicious Certificate[1]	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP)[2]	•	•			
	IoT Security — IoT Device Detection, IoT Vulnerability Correlation, and Virtual Patching[3]		•			•
	Security Rating (and Outbreak Check)[3]		•			•
	OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS[2]	•				
	Application Control	----------included with FortiCare Subscription----------				
	Inline CASB[1]	----------included with FortiCare Subscription----------				
SD-WAN and SASE Services	SD-WAN SLA Database					•
	SD-WAN Underlay and Application Monitoring Service					•
	SD-WAN Overlay Orchestration Service					•
	SD-WAN Connector for FortiSASE Secure Private Access					•
	FortiSASE Starter Kit for n* Users[4]					•
	One Year Cloud-based Log Retention					•
	FortiTelemetry Cloud					•
NOC and SOC Services	FortiConverter Service for One Time Configuration Conversion	•	•			
	Managed FortiGate Service—Available 24×7, with Fortinet NOC Experts Performing Device Setup, Network, And Policy Change Management	•				
	FortiManagement Cloud—Management, Analysis, and One Year Log Retention	•				
	FortiManager Cloud	•				
	FortiAnalyzer Cloud	•				
	FortiGuard SOCaaS—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service	•				
Hardware and Software Support	FortiCare Essentials	Desktop models only				
	FortiCare Premium[3]	•	•	•	•	•
	FortiCare Elite	•				
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing	----------included with FortiCare Subscription----------				

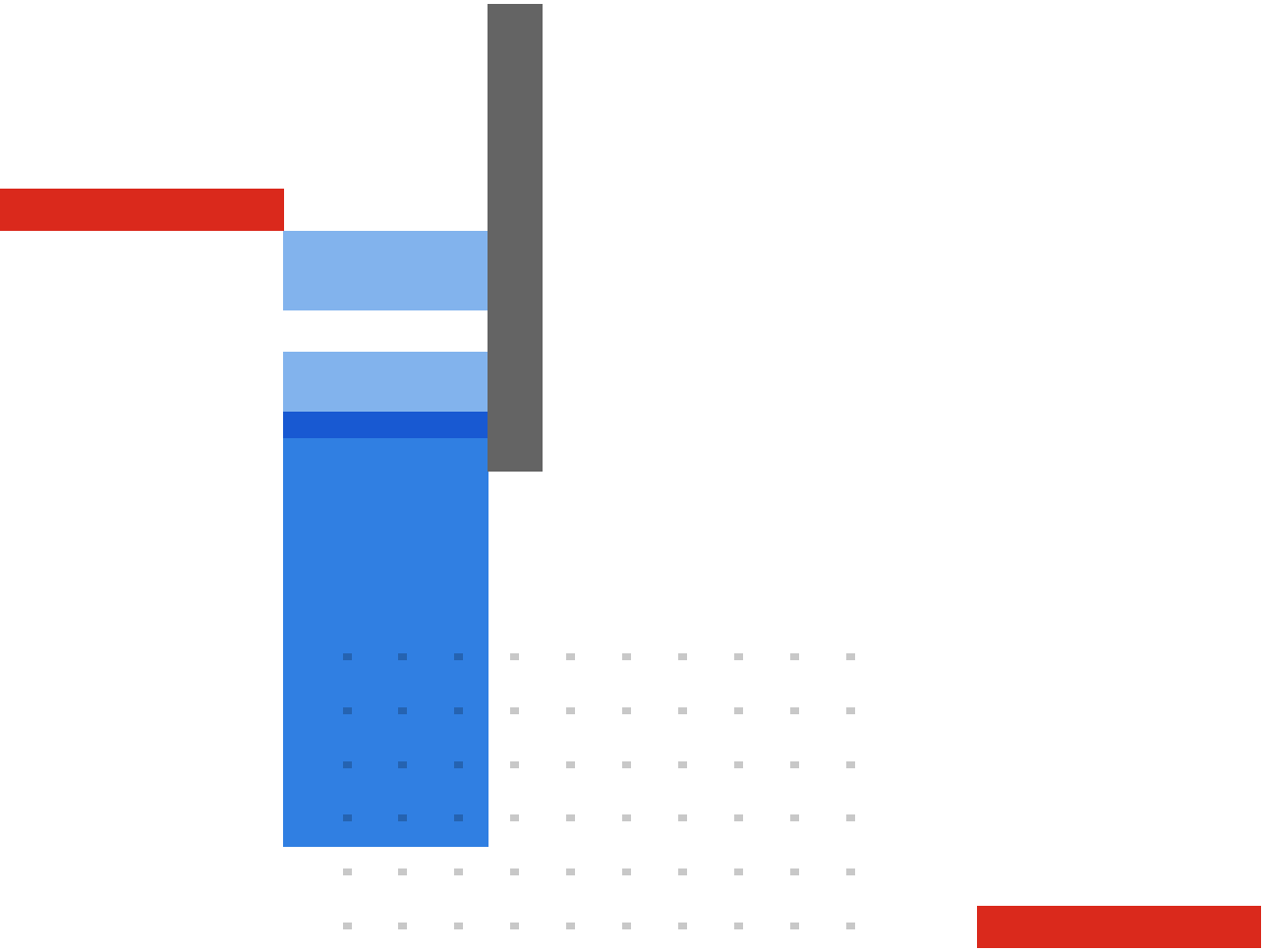
1. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Not available for SD-WAN Bundle SKU FC-10-XXXXX-1387-02-DD.
4. Only supported on FortiGate/FortiWiFi models from the 70F (F-series and all later series) and FGR-60G onwards. See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

FortiGuard AI-Powered Security Bundles offer curated security services to combat known, unknown, zero-day, and emerging AI threats. They protect against malicious content, web threats, and secure IT/OT/IoT devices, applications, users, and data. All bundles include FortiCare Premium Services with 24×7×365 support, one-hour critical response, and next-business-day noncritical response.

Fortinet's FortiCare Services support the Security Fabric throughout its lifecycle—Design, Deploy, Operate, Optimize, and Evolve. FortiCare Elite delivers enhanced SLAs, rapid issue resolution, dedicated support, 18 months of extended engineering support, and a unified portal for device and security health, improving operational efficiency and deployment performance.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

October 1, 2026

FG-VM-KVM-DAT-R31-20261001