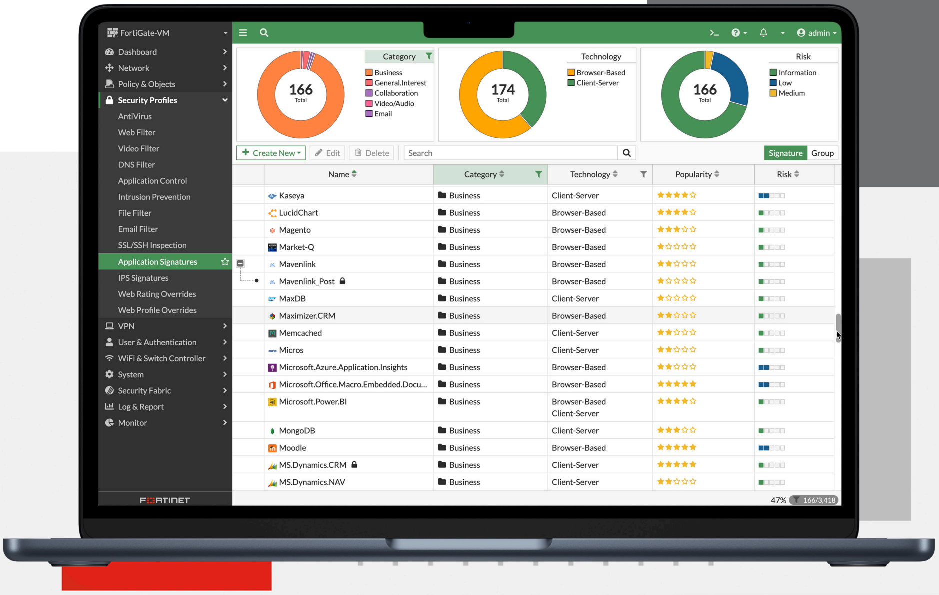
FortiGate®-VM on Google Cloud



Name	Category	Technology	Popularity	Risk
Kaseya	Business	Client-Server	★★★★☆	■■□□□
LucidChart	Business	Browser-Based	★★★★☆	■□□□□
Magento	Business	Browser-Based	★★★☆☆	■□□□□
Market-Q	Business	Browser-Based	★☆☆☆☆	■□□□□
Mavenlink	Business	Browser-Based	★★☆☆☆	■□□□□
Mavenlink_Post	Business	Browser-Based	★☆☆☆☆	■□□□□
MaxDB	Business	Client-Server	★☆☆☆☆	■□□□□
Maximizer.CRM	Business	Browser-Based	★★☆☆☆	■□□□□
Memcached	Business	Client-Server	★★☆☆☆	■□□□□
Micros	Business	Client-Server	★★☆☆☆	■□□□□
Microsoft.Azure.Application.Insights	Business	Browser-Based	★★☆☆☆	■■□□□
Microsoft.Office.Macro.Embedded.Docu...	Business	Browser-Based	★★★★★	■■□□□
Microsoft.Power.BI	Business	Browser-Based Client-Server	★★★★☆	■□□□□
MongoDB	Business	Client-Server	★★★☆☆	■□□□□
Moodle	Business	Browser-Based	★★★★★	■■□□□
MS.Dynamics.CRM	Business	Client-Server	★★★★★	■□□□□
MS.Dynamics.NAV	Business	Client-Server	★★☆☆☆	■□□□□

47% 166/3,418

Highlights

- Securely connect to your application workloads without performance bottlenecks
- Move at cloud speed without compromising security
- Seamlessly scale your cloud protection without increasing operational burden
- Secure your cloud transformation without impacting business outcomes, with flexible consumption models

Adaptive Multi-Cloud Security with AI-Powered Advanced Threat Protection

The FortiGate-VM on Google Cloud 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 delivers protection from a broad array of network security threats. It offers the same security and networking services included in the FortiOS operating system and is available for public cloud, private cloud, and Telco Cloud (VNFs). With a consistent operational model across hybrid cloud, multi-cloud, and service provider environments, it reduces the training burden on security teams.

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

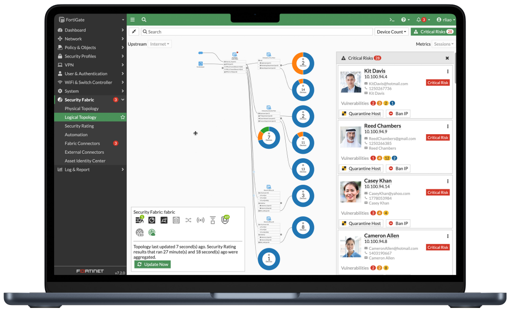
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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.

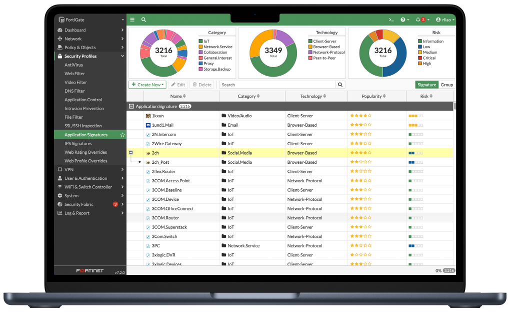
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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

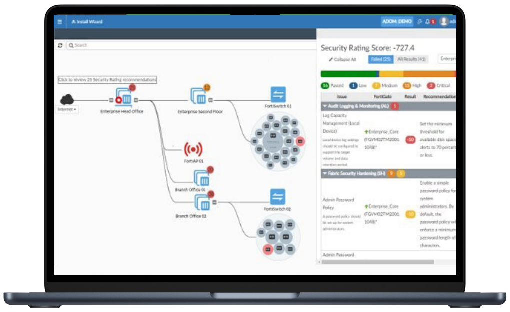
Advanced Virtual Security Processing Units (vSPUs)

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 a particular industry-leading feature:

- 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.



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

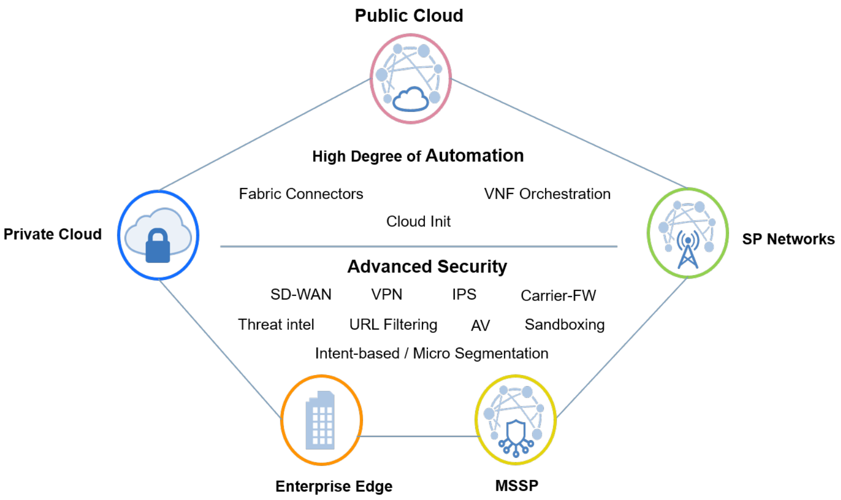
Next Generation Firewall (NGFW)

- 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 GCP VPCs
- VGW to FortiGate VPN between VPCs
- Hybrid cloud site to site IPsec VPN
- Remote access VPN

Gain Comprehensive Visibility and Apply Consistent Control



Specifications

The FortiGate-VM supports multiple instance families that leverage x64 processors from Intel and AMD as well as ARM64 processors such as the Google Axion Processor. For a full list of supported instance families, see the Fortigate GCP Administration Guide.

Specifications

The following shows the performance of x64 C4-Standard instance family with the BYOL License type.

DEVICE PERFORMANCE DATA												
	VM-01/01S	VM-02/02S		VM-04/04S		VM-08/08S		VM-16/16S		VM-32/32S		VM-UL/ ULS
SYSTEM REQUIREMENT												
vCPU (Minimum / Maximum)	1 / 1	1 / 2		1 / 4		1 / 8		1 / 16		1 / 32		1 / Unlimited
TECHNICAL SPECIFICATIONS												
Network Interface Support (Minimum / Maximum)1	1 / 24	1 / 24		1 / 24		1 / 24		1 / 24		1 / 24		1 / 24
Virtual Domains (Default / Maximum)2	10 / 10	10 / 50		10 / 50		10 / 50		10 / 500		10 / 500		10 / 500
Firewall Policies	10 000	10 000		10 000		200 000		200 000		200 000		200 000
SYSTEM PERFORMANCE												
Instance Shape to be Measured		C4-Standard-2		C4-Standard-4		C4-Standard-8		C4-Standard-16		C4-Standard-32		
Google Cloud Expected Bandwidth [3]		Up to 10 Gbps		Up to 23 Gbps		Up to 23 Gbps		Up to 23 Gbps		Up to 23 Gbps		
(Gigabit per second) [3]		stand alone	IPSEC	stand alone	IPSEC	stand alone	IPSEC	stand alone	IPSEC	stand alone	IPSEC	
Firewall Throughput (UDP Packets) in Mbps - 1280 bytes		10 200	3250	22 000	6000	22 000	7000	21 900	8000	21 900	8700	
Firewall Throughput (UDP Packets) in Mbps - 512 bytes		6650	1950	10 000	2900	10 300	3500	15 500	4000	12 000	4370	
Firewall Throughput (UDP Packets) in Mbps - 64 bytes		1100	390	1600	600	2000	625	2350	780	2400	790	
New Sessions / Second (TCP)		125 000		175 000	-	250 000	-	340 000	-	330 000	-	
HTTP Throughput w/ Application profile (64K size)[4] in Mbps		10 150		18 800	-	20 000	-	20 500	-	21 300	-	
HTTP Throughput w/ IPS profile (44K size) [5] in Mbps		10 150		18 200	-	20 800	-	20 800	-	21 500	-	
HTTP Throughput w/ IPS profile (1M size) [5] in Mbps		10 190		18 500	-	21 000	-	21 000	-	21 600	-	
NGFW Throughput (Mbps) [6]		965		2200	-	4100	-	8100	-	13 100	-	
Threat Protection Throughput (Mbps) [7]		945		2180	-	4050	-	8000	-	13 000	-	
SSL Inspection throughput (Mbps) [8]		2540		5200	-	9900	-	16 000	-	17 600	-	

Notes.

Actual performance may vary depending on the network and system configuration.
Please 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 please make sure to refer to the latest datasheets.
Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.6.1.

1. Applicable to 7.6.1+. The actual working number of consumable network interfaces varies depending on GCP 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 additional perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. The latest information about GCP bandwidth is found on https://cloud.google.com/compute/docs/network-bandwidth.
4. Application Control performance is measured with 64 Kbyte HTTP traffic.
5. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
6. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
7. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
8. SSL Inspection Throughput is measured using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

Specifications

The following shows the performance of DPDK x64 C4-Standard instance family with the BYOL License type.

DEVICE PERFORMANCE DATA							
	VM-01S	VM-02S	VM-04S	VM-08S	VM-16S	VM-32S	VM-ULS
SYSTEM REQUIREMENT							
vCPU (Minimum / Maximum)	1 / 1	1 / 2	1 / 4	1 / 8	1 / 16	1 / 32	1 / Unlimited
TECHNICAL SPECIFICATIONS							
Network Interface Support (Minimum / Maximum)1	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24
Virtual Domains (Default / Maximum)2	10 / 10	10 / 25	10 / 50	10 / 50	10 / 500	10 / 500	10 / 500
Firewall Policies	10 000	10 000	10 000	200 000	200 000	200 000	200 000

SYSTEM PERFORMANCE										
Instance Shape to be Measured	C4-Standard-2		C4-Standard-4		C4-Standard-8		C4-Standard-16		C4-Standard-32	
Google Cloud Expected Bandwidth [3]	10 Gbps		Up to 23 Gbps		Up to 23 Gbps		Up to 23 Gbps		Up to 23 Gbps	
(Gigabit per second) [3]	DPDK stand alone	DPDK IPSEC	DPDK stand alone	DPDK IPSEC	DPDK stand alone	DPDK IPSEC	DPDK stand alone	DPDK IPSEC	DPDK stand alone	DPDK IPSEC
Firewall Throughput (UDP Packets) in Mbps - 1280 bytes	10 500	2500	21 000	5200	21 000	6500	24 000	7800	23 000	9500
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	9900	1290	11 000	2600	10 800	3200	13 000	4000	11 800	4500
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	2000	235	2500	500	2300	620	2500	780	2500	840
New Sessions / Second (TCP)	110 000	-	200 000	-	320 000	-	400 000	-	440 000	-
HTTP Throughput w/ Application profile (64K size)[4] in Mbps	10 265	-	17 500	-	20 500	-	23 000	-	20 800	-
HTTP Throughput w/ IPS profile (44K size) [5] in Mbps	10 270	-	17 500	-	20 500	-	22 500	-	21 200	-
HTTP Throughput w/ IPS profile (1M size) [5] in Mbps	10 300	-	17 200	-	20 600	-	22 400	-	21 800	-
NGFW Throughput (Mbps) [6]	1070	-	2500	-	4900	-	9200	-	13 500	-
Threat Protection Throughput (Mbps) [7]	1050	-	2450	-	4800	-	9000	-	13 200	-
SSL Inspection throughput (Mbps) [8]	5560	-	10 000	-	15 500	-	18 000	-	18 000	-

Notes.

Actual performance may vary depending on the network and system configuration.
Please 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 please make sure to refer to the latest datasheets.
Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.6.1.

1. Applicable to 7.6.1+. The actual working number of consumable network interfaces varies depending on GCP 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 additional perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. The latest information about GCP bandwidth is found on https://cloud.google.com/compute/docs/network-bandwidth.
4. Application Control performance is measured with 64 Kbyte HTTP traffic.
5. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
6. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
7. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
8. SSL Inspection Throughput is measured using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

Specifications

The following shows the performance of C4A-Standard ARM instance family with the BYOL License type.

DEVICE PERFORMANCE DATA							
	VM-01S	VM-02S	VM-04S	VM-08S	VM-16S	VM-32S	VM-ULS
SYSTEM REQUIREMENT							
vCPU (Minimum / Maximum)	1 / 1	1 / 2	1 / 4	1 / 8	1 / 16	1 / 32	1 / Unlimited
TECHNICAL SPECIFICATIONS							
Network Interface Support (Minimum / Maximum)1	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24	1 / 24
Virtual Domains (Default / Maximum)2	10 / 10	10 / 25	10 / 50	10 / 50	10 / 500	10 / 500	10 / 500
Firewall Policies	10 000	10 000	10 000	200 000	200 000	200 000	200 000

SYSTEM PERFORMANCE										
Instance Shape to be Measured	C4A-Standard-2		C4A-Standard-4		C4A-Standard-8		C4A-Standard-16		C4A-Standard-32	
Google Cloud Expected Bandwidth [3]	Up to 10 Gbps		Up to 23 Gbps		Up to 23 Gbps		Up to 23 Gbps		Up to 23 Gbps	
(Gigabit per second) [3]	stand alone	IPSEC	stand alone	IPSEC	stand alone	IPSEC	stand alone	IPSEC	stand alone	IPSEC
Firewall Throughput (UDP Packets) in Mbps - 1280 bytes	4450	2380	10 000	4500	10 100	4750	10 300	8500	15 800	9250
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	4500	1700	9000	3000	10 300	3280	10 400	4350	11 200	4850
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	1050	470	1800	620	2500	650	2650	860	2800	900
New Sessions / Second (TCP)	130 000	—	270 000	—	300 000	—	320 000	—	390 000	—
HTTP Throughput w/ Application profile (64K size)[4] in Mbps	10 100	—	17 500	—	20 000	—	20 500	—	21 300	—
HTTP Throughput w/ IPS profile (44K size) [5] in Mbps	10 050	—	17 000	—	20 800	—	20 800	—	21 500	—
HTTP Throughput w/ IPS profile (1M size) [5] in Mbps	10 080	—	17 000	—	21 000	—	21 000	—	21 600	—
NGFW Throughput (Mbps) [6]	1220	—	2300	—	4500	—	8550	—	14 500	—
Threat Protection Throughput (Mbps) [7]	1200	—	2250	—	4430	—	8350	—	14 500	—
SSL Inspection throughput (Mbps) [8]	2900	—	5550	—	10 850	—	18 500	—	21 000	—

Notes.
FortiGate-VM on ARM instances do not currently support DPDK.
All performance values are "up to" and vary depending on system configuration.
Actual performance may vary depending on the network and system configuration.
Please 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 please make sure to refer to the latest datasheets.
Performance metrics were observed using FortiGate-VM BYOL instances using FOS v7.6.2.

1. Applicable to 7.6.2+. The actual working number of consumable network interfaces varies depending on GCP 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 additional perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. The latest information about GCP bandwidth is found on https://cloud.google.com/compute/docs/network-bandwidth.
4. Application Control performance is measured with 64 Kbyte HTTP traffic.
5. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
6. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
7. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
8. SSL Inspection Throughput is measured using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

Licensing

With a multitude of deployment methods supported across various private and public cloud deployments, FortiGate-VM for Google Cloud supports the bring-your-own-license (BYOL) licensing model.

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.

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.

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

Download

You can download the Google Cloud new deployment file on www.support.fortinet.com.

Go to Download > VM Images from the top menu and choose FortiGate from the Product dropdown list and Google from the Platform dropdown list. Create a FortiGate-VM instance from Custom Images on the Compute Engine portal.

Subscriptions

			Bundles		
Service Category	Service Offering	A-la-carte	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heuristic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		------------included with FortiCare Subscription------------		
	Inline CASB [3]		------------included with FortiCare Subscription------------		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	Models up to FG/ FWF-60F series			
	SD-WAN Underlay and Application Monitoring Service	FG-70F series and above			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE expansion for SD-WAN (SD-WAN SPA Connector license plus FortiSASE starter kit for n* users) [2]	Selected models only[2]			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth)	Desktop models only			
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	•			
	FortiGate 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	•	•	•	•
	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] Full features available when running FortiOS 7.4.1.

[2] See the FortiSASE Ordering Guide for supported models and their associated number of user licenses.

[3] Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.

FortiGuard Bundles

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 one of these FortiGuard Bundles.

FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an Extended End-of-Engineering-Support of 18 months, providing flexibility. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet 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.

www.fortinet.com

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.

July 25, 2025