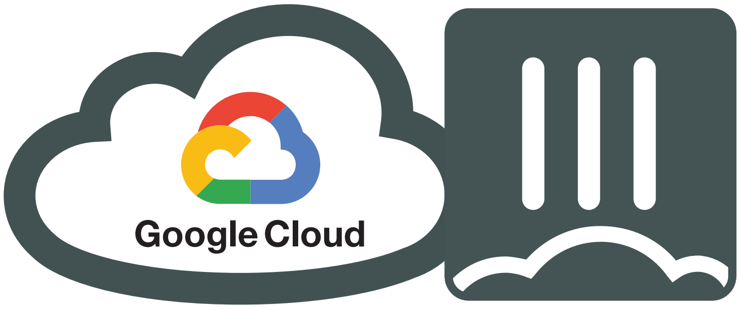
FORTINET

DATA SHEET

FortiGate®-VM on Google Cloud

Next Generation Firewall
VPN Gateway



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

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevents and detects against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance

- Delivers industry's best firewall and threat protection performance using software-based, purpose-built virtual security processor (vSPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multitenancy, and effective utilization of resources (only BYOL supports VDOM)
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's single pane of glass management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Fortinet's comprehensive security virtual appliance lineup supports Google Cloud

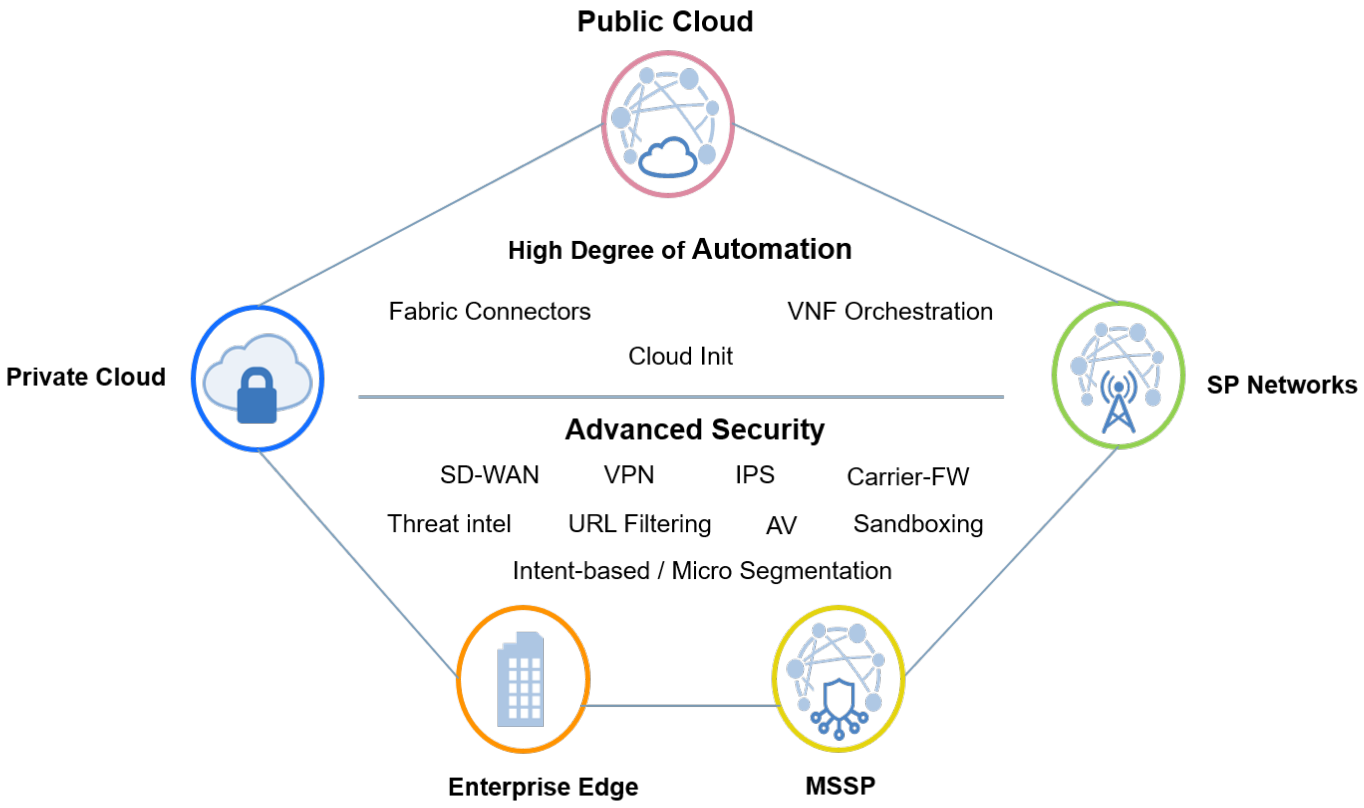
DEPLOYMENT

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
- Delivers the industry's highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- Proactively blocks newly discovered sophisticated attacks in real-time with advanced threat protection

VPN Gateway

- FortiGate firewalls for SSL and IPsec VPNs into and out of the VPCs
- Cloud VPN to FortiGate inter-VPC VPN
- Hybrid cloud site-to-site IPsec VPN
- Remote access VPN



Gain comprehensive visibility and apply consistent control

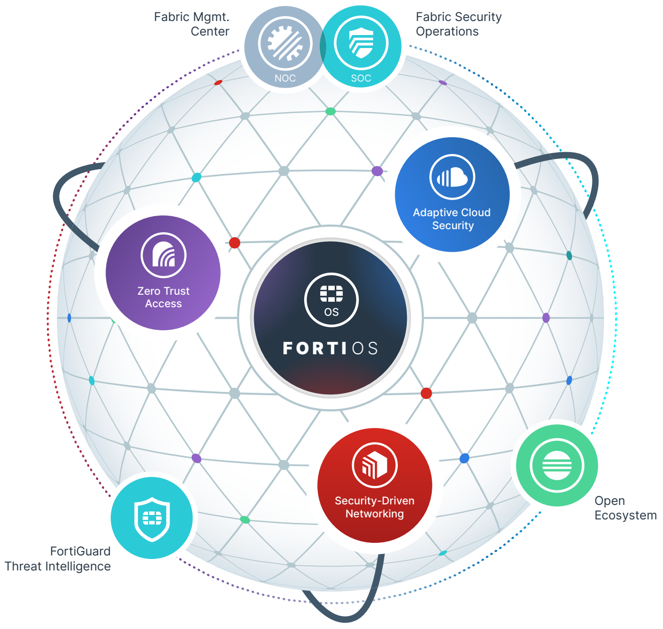
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad**: Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints, and users
- **Integrated**: Integrated and unified security, operation, and performance across different technologies, locations, deployment options, and the richest ecosystem
- **Automated**: Context-aware and self-healing network and security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Security Fabric

The Security Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system, enables the convergence of high performing networking and security across the Fortinet Security Fabric. It delivers consistent and context-aware security posture across the network, endpoints, and clouds. Its organically-built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection by supporting seamless scalability and simplifying innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models running on appliances, software, and as-a-service with SASE, ZTNA, and other emerging cybersecurity solutions.

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

FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

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.

SPECIFICATIONS

DEVICE PERFORMANCE DATA							
	VM-01 /01V /01S	VM-02/ 02V/ 02S	VM-04/ 04V /04S	VM-08/ 08V/ 08S	VM-16/ 16V/ 16S	VM-32/ 32V/ 32S	VM-UL/ ULV/ 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	200 000	200 000	200 000	200 000	200 000

SYSTEM PERFORMANCE										
Instance Shape to be Measured	N2-Standard-2		N2-Standard-4		N2-Standard-8		N2-Standard-16		N2-Standard-32	
Google Cloud Expected Bandwidth[3]	10 Gbps		10 Gbps		16 Gbps		32 Gbps		32 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	4000	1360	5350	2000	7000	2300	15 000	3500	20 000	7600
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	2500	720	3000	1000	5000	1200	7000	1900	8500	3350
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	350	160	500	190	900	210	1500	450	1600	650
New Sessions / Second (TCP)	85 000	-	120 000	-	180 000	-	280 000	-	335 000	-
HTTP Throughput w/ Application profile (64K size) [4]	5750	-	7900	-	9600	-	14 700	-	17 000	-
HTTP Throughput w/ IPS profile (44K size) [5]	5700	-	7850	-	9500	-	14 700	-	17 000	-
HTTP Throughput w/ IPS profile (1M size) [5]	5800	-	7900	-	9600	-	14 700	-	17 000	-
NGFW Throughput (Mbps) [6]	680	-	1140	-	2240	-	4250	-	8000	-
Threat Protection Throughput (Mbps) [7]	680	-	1140	-	2240	-	4250	-	8000	-
SSL Inspection throughput (Mbps) [8]	1370	-	2000	-	3800	-	7000	-	10 500	-

Notes.

All performance values are up to and vary depending on system configuration. Actual performance may vary depending on the network and system configuration. These metrics are updated periodically as the product performance keeps improving through internal testing. Different versions of the document may note the discrepancy in the performance numbers, so ensure that you refer to the latest datasheets.

Performance metrics were observed using FortiGate-VM BYOL instances using FortiOS 7.0.1.

1. Applicable to 6.4.0+. The actual working number of consumable network interfaces varies depending on Google Cloud instance types/sizes and may be less.
2. FG-VMxxV and FG-VMxxS series do not come with a multi-VDOM feature by default. You can add it by applying separate VDOM addition perpetual licenses. See ORDER INFORMATION for VDOM SKUs.
3. You can find the latest information about Google Cloud bandwidth at https://cloud.google.com/compute/docs/machine-types#n2_standard_machine_types.
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).

ORDERING INFORMATION

The following are SKUs that can be acquired for the BYOL scheme. For the PAYG/On-Demand subscription, various instance/VM types are available on the marketplace. BYOL is perpetual licensing, as opposed to PAYG/On-Demand, which is an hourly subscription available with marketplace-listed products.

Product	SKU	Description
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM 'virtual appliance'. 1x vCPU core. No VDOM by default for FG-VM01V model.
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM 'virtual appliance'. 2x vCPU cores. No VDOM by default for FG-VM02V model.
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM 'virtual appliance'. 4x vCPU cores. No VDOM by default for FG-VM04V model.
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM 'virtual appliance'. 8x vCPU cores. No VDOM by default for FG-VM08V model.
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM 'virtual appliance'. 16x vCPU cores. No VDOM by default for FG-VM016V model.
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM 'virtual appliance'. 32x vCPU cores. No VDOM by default for FG-VM032V model.
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores. No VDOM by default for FG-VMULV model.
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.

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.

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.

BUNDLES

FortiGuard 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 one of these FortiGuard Bundles.

Bundles	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•
FortiGuard IPS Service	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•
FortiGuard Web and Video[1] Filtering Service	•	•	
FortiGuard Antispam Service	•	•	
FortiGuard Security Rating Service	•		
FortiGuard IoT Detection Service	•		
FortiGuard Industrial Service	•		
FortiConverter Service	•		

[1] Available when running FortiOS 7.0

Google Cloud

GLOBAL

Partner of the Year

Security

2020

www.fortinet.com

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 censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).