DATA SHEET

FortiGate®-VM on Amazon Web Services

Next Generation Firewall
VPN Gateway

The FortiGate-VM on AWS delivers next generation firewall capabilities for organizations of all sizes, with the flexibility to be deployed as next generation firewall 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
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services
- Automates incident response and threat intelligence from AWS GuardDuty threat detection service

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
- AWS Security Competency partner

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy 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
- Design for high availability using AWS health checks

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
- Map your security postures to scale up and down with your EC2

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 AWS

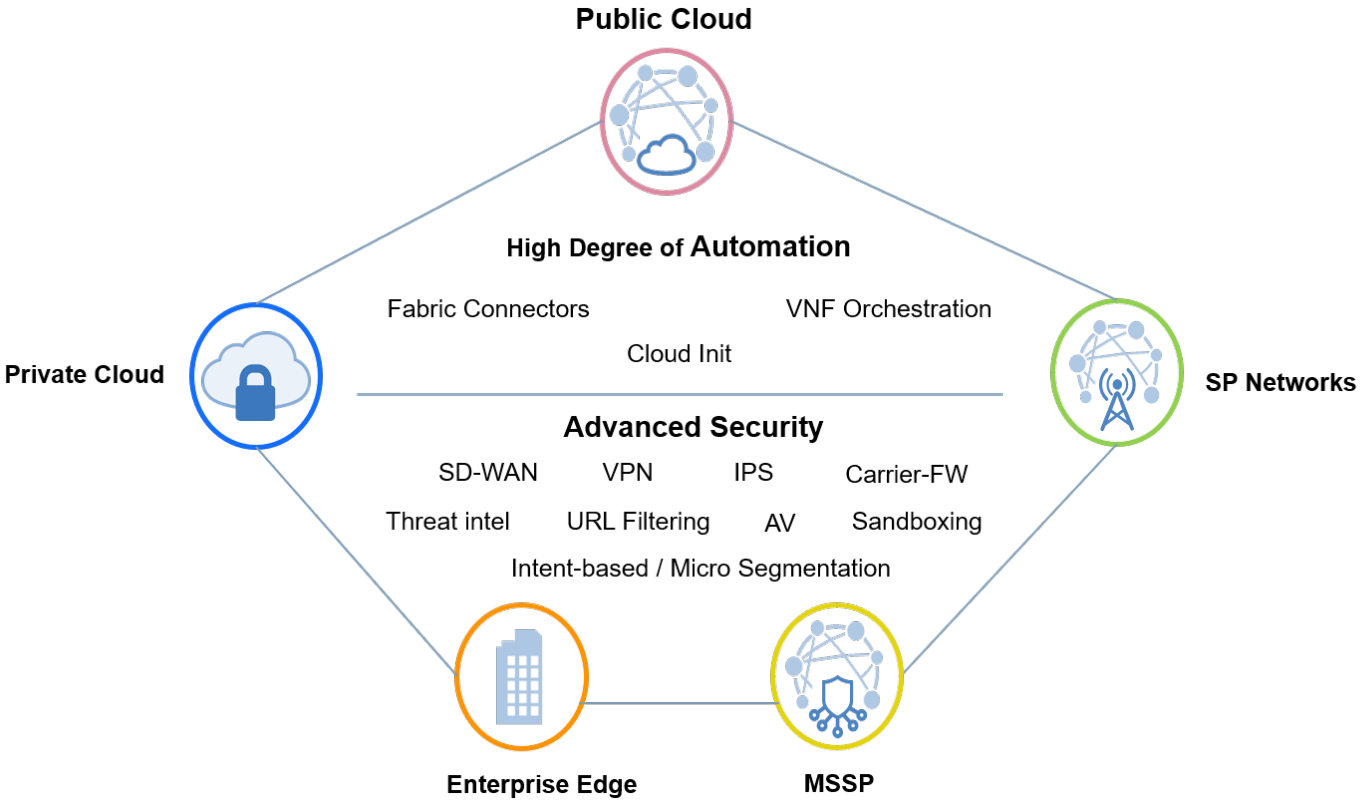
DEPLOYMENT

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

AWS Integration

- Fortinet embeds the latest AWS Auto Scaling functionality and FortiGate CloudFormation template configuration into our cloud Security Fabric, providing automation based on resource demand from your cloud workloads
- Accelerate time-to-protection for new threats detected by AWS GuardDuty by deploying native AWS scripting to automatically push malicious IP or DNS addresses into dynamic FortiGate policies
- Provide service resiliency with AWS native load balancer

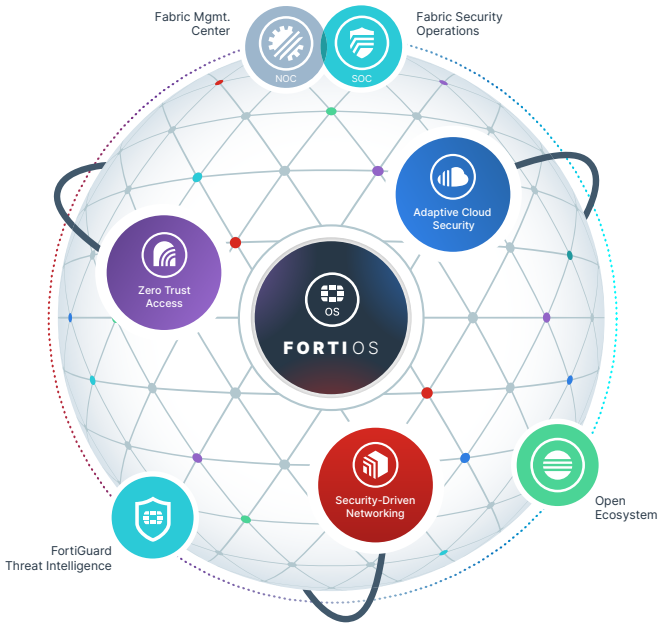
FORTINET SECURITY FABRIC

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, location, deployment options, and the richest Ecosystem
- **Automated**: Context aware, 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 Fabric

The 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 delivering consistent and context-aware security posture across network endpoint and clouds. The organically-built, best-of-breed capabilities and unified approach allow organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models 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 1,000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

SPECIFICATIONS

The C6i instance family leverages the Intel IceLake Processors. FortiGate-VM is available for purchase in all regions, including AWS GovCloud and AWS China. The following is the system requirement for BYOL licenses:

	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 / 500		10 / 500		10 / 500		10 / 500
Firewall Policies	10 000	10 000		200 000		200 000		200 000		200 000		200 000
System Performance		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		**ENA Driver - Yes**		
Instance Shape to be Measured		**C6I.LARGE**		**C6I.XLARGE**		**C6I.2XLARGE**		**C6I.4XLARGE**		**C6I.8XLARGE**		
AWS Bandwidth [3]		**Up to 12.5 Gbps**		**Up to 12.5 Gbps**		**Up to 12.5 Gbps**		**Up to 12.5 Gbps**		**12.5 Gbps**		
		Native	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	**Native**	**IPSEC**	
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes		12360	1950	12360	4000	12690	5100	12690	11200	12690	11480	
Firewall Throughput (UDP Packets) in Mbps - 512 bytes		4270	1360	4270	2150	5350	2830	6420	6300	8540	6600	
Firewall Throughput (UDP Packets) in Mbps - 64 bytes		670	290	670	450	840	600	1000	1000	1340	1100	
New Sessions / Second (TCP)		162K	-	200K	-	234K	-	235K	-	245K	-	
HTTP Throughput w/ Application profile (64K size) [4]		3500	-	7710	-	9640	-	11570	-	12510	-	
HTTP Throughput w/ IPS profile (44K size) [4]		3900	-	7550	-	9435	-	11330	-	12520	-	
HTTP Throughput w/ IPS profile (1M size) [4]		3900	-	7750	-	9690	-	11660	-	12540	-	
NGFW Throughput [5]		870	-	1900	-	3520	-	6200	-	10000	-	
Threat Protection Throughput [6]		870	-	1900	-	3520	-	6000	-	9500	-	
SSL Inspection Throughput in Mbps [7]		1010	-	3850	-	4950	-	6200	-	8350	-	

Note: 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 v7.2.0.

1. Applicable to 6.4.0+. The actual working number of consumable network interfaces varies depending on AWS 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. The latest information about AWS bandwidth is found on https://aws.amazon.com/ec2/instance-types/.
4. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
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. Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

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

SPECIFICATIONS

The C6g instance family leverages the AWS Graviton (ARM-based) Processors. FortiGate-VM is available for purchase in all regions, including AWS GovCloud and AWS China. The following is the system requirement for BYOL licenses:

	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 / 500	10 / 500	10 / 500	10 / 500
Firewall Policies	10 000	10 000	200 000	200 000	200 000	200 000	200 000
System Performance		**ENA Driver - Yes**	**ENA Driver - Yes**	**ENA Driver - Yes**	**ENA Driver - Yes**	**ENA Driver - Yes**	
Instance Shape to be Measured		**C6g.LARGE**	**C6g.XLARGE**	**C6g.2XLARGE**	**C6g.4XLARGE**	**C6g.8XLARGE**	
AWS Bandwidth [3]		**Up to 10 Gbps**	**Up to 10 Gbps**	**Up to 10 Gbps**	**Up to 10 Gbps**	**12 Gbps**	
		Native / **IPSEC**	**Native** / **IPSEC**	**Native** / **IPSEC**	**Native** / **IPSEC**	**Native** / **IPSEC**	
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes		9800 / 1360	10000 / 2540	10120 / 3100	10120 / 4580	12000 / 5400	
Firewall Throughput (UDP Packets) in Mbps - 512 bytes		3400 / 900	3700 / 1640	4500 / 2000	4500 / 2900	5000 / 3500	
Firewall Throughput (UDP Packets) in Mbps - 64 bytes		540 / 250	650 / 410	720 / 550	720 / 680	800 / 680	
New Sessions / Second (TCP)		120K / -	130K / -	140K / -	135K / -	130K / -	
HTTP Throughput w/ Application profile (64K size) [4]		6100 / -	7550 / -	8700 / -	9000 / -	9800 / -	
HTTP Throughput w/ IPS profile (44K size) [4]		6000 / -	7550 / -	8250 / -	8900 / -	9650 / -	
HTTP Throughput w/ IPS profile (1M size) [4]		6200 / -	7750 / -	8500 / -	9000 / -	9900 / -	
NGFW Throughput in Mbps [5]		770 / -	1700 / -	2900 / -	5300 / -	6100 / -	
Threat Protection Throughput in Mbps [6]		770 / -	1700 / -	2900 / -	5300 / -	6100 / -	
SSL Inspection Throughput in Mbps [7]		1300 / -	2500 / -	4000 / -	5000 / -	5700 / -	

Note: 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 v7.0.6

1. Applicable to 7.0.6+. The actual working number of consumable network interfaces varies depending on AWS 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. The latest information about AWS bandwidth is found on https://aws.amazon.com/ec2/instance-types/.
4. IPS performance is measured using Enterprise Traffic Mix and 1 Mbyte HTTP.
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. Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

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

LICENSING

With a multitude of deployment methods supported across various private and public cloud deployments, FortiGate-VM for AWS supports both on-demand (PAYG) and bring-your-own-license (BYOL) licensing models.

On-demand licensing is a highly flexible option for both initial deployments and growing them as needed. With a wide selection of supported instance types, there is a solution for every use case. This license offers FortiOS with a UTP bundle.

BYOL is ideal for migration use cases, where an existing private cloud deployment is migrated to a public cloud deployment. When using an existing license, the only additional cost would be the price for the AWS instances.

ORDERING INFORMATION

The following are SKUs that can be acquired for BYOL scheme. For PAYG/On-Demand subscription, various instance/VM types are available on 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.

FG-VMxx"V" 6.0.0 supports VDOM by adding separate VDOM licenses. 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.

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

www.fortinet.com