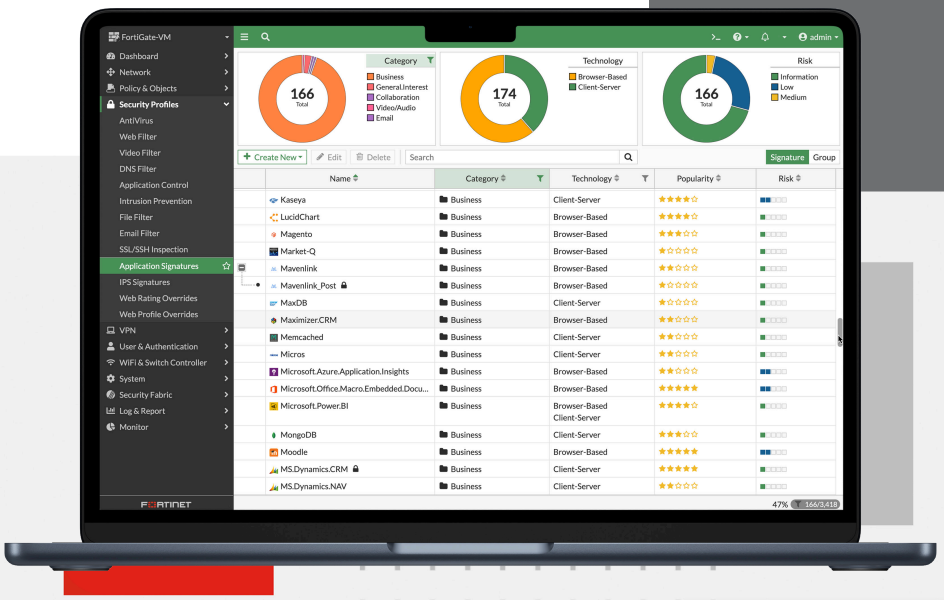
FortiGate®-VM on Oracle Cloud Infrastructure

ORACLE
Cloud Infrastructure



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 Oracle Cloud Infrastructure (OCI) 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.

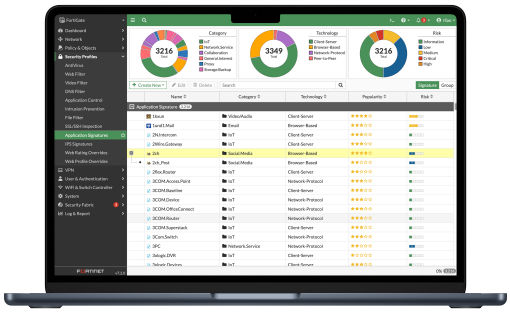
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed 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

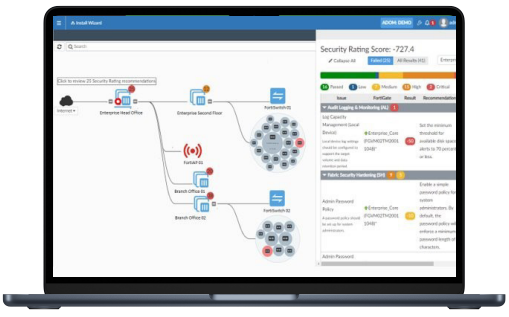
Advanced Virtual Security Processing Units (vSPUs)

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 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

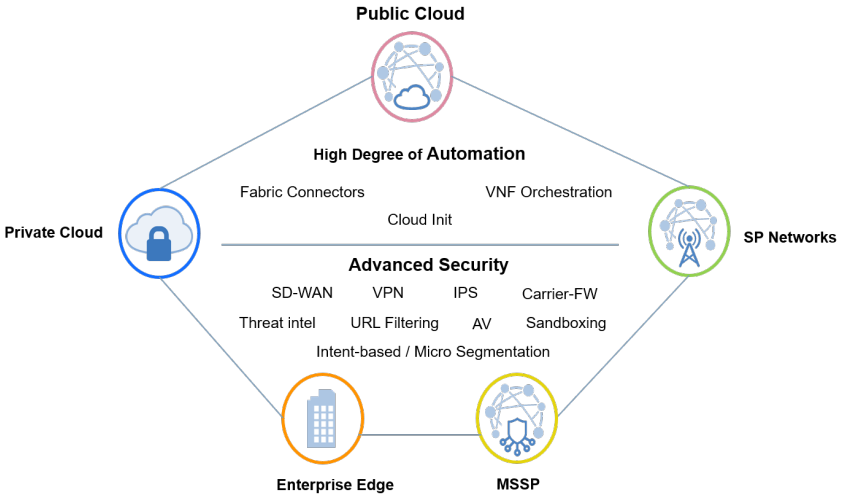
Next Generation Firewall (NGFW)

- 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



Specifications

The FortiGate-VM supports multiple instance families that leverage Intel and AMD-based x64 processors as well as the VM.Standard.A1.Flex instance family that leverages the Ampere® Altra® Arm-based processor.

For a full list of supported instance families See OCI Administration Guide: Instance type Support.

The following shows performance of ARM64 VM.Standard.A1.Flex and VM64 VM.Standard3.Flex Instance families with BYOL licenses.

ARM64 Specifications

	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 / 24		1 / 24		1 / 24		1 / 24		1 / 24		1 / 24	1 / 24
Virtual Domains (Default / Maximum) [1]	10 / 10		10 / 25		10 / 50		10 / 500		10 / 500		10 / 500	10 / 500
OCPU	1		2		4		8		16		32	Unlimited
Firewall Policies	10 000		10 000		10 000		200 000		200 000		200 000	
System Performance												
Instance Shape to be Measured	VM.StandardA1.Flex (1 OCPU)		VM.StandardA1.Flex (2 OCPU)		VM.StandardA1.Flex (4 OCPU)		VM.StandardA1.Flex (8 OCPU)		VM.StandardA1.Flex (16 OCPU)			
OCI Bandwidth [2]	1 Gbps		2 Gbps		4.1 Gbps		8.2 Gbps		16.4 Gbps			
	VFIO	IPSEC	VFIO	IPSEC	VFIO	IPSEC	VFIO	IPSEC	VFIO	IPSEC		
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes	1000	450	2000	650	4000	1350	8300	2200	12000	2950		
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	393	200	800	500	1680	630	3120	1150	4500	1500		
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	60	30	140	120	280	125	560	200	820	290		
New Sessions / Second (TCP)	19000	-	27000	-	50000	-	110000	-	150000	-		
HTTP Throughput w/ Application profile (64K size) in Mbps	780	-	2000	-	4000	-	8100	-	10200	-		
HTTP Throughput w/ IPS profile (44K size) in Mbps	760	-	2000	-	4000	-	8100	-	10000	-		
HTTP Throughput w/ IPS profile (1M size) in Mbps	780	-	2000	-	4000	-	8100	-	10200	-		
NGFW Throughput in Mbps [3]	195	-	400	-	860	-	1790	-	3100	-		
Threat Protection Throughput in Mbps [4]	195	-	395	-	850	-	1780	-	3000	-		
SSL Inspection Throughput in Mbps [5]	200	-	500	-	1270	-	2800	-	5350	-		

Notes.

PAYG supports only up to 24 OCPU (48 vCPU) instances.

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 measured using FortiOS v7.4.3

1. 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.
2. The latest information about OCI bandwidth is found on https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm#vm-standard
3. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
4. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
5. Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

VM64 Specifications

LICENSE TYPE : VM-02/02S

System Requirement						
vCPU (Minimum / Maximum)	1 / 2					
Technical Specifications						
Network Interface Support (Minimum / Maximum)	1 / 24					
Virtual Domains (Default / Maximum) [1]	10 / 25					
Firewall Policies	10 000					
OCPU [2]	1					
System Performance						
Instance Shape to be Measured	VM.Standard3.Flex (1 OCPU)					
OCI Bandwidth [3]	1 Gbps					
	SR-IOV				PARAVIRTUALIZED	IPSEC
	VFIO	IPSEC	VFIO DPDK	IPSEC		
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes	1280	1250	1280	1250	1270	1000
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	1300	1000	1300	1000	1120	460
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	1100	300	1020	200	180	85
New Sessions / Second (TCP)	142000	-	92000	-	55000	-
HTTP Throughput w/ Application profile (64K size) in Mbps	1030	-	1030	-	1030	-
HTTP Throughput w/ IPS profile (44K size) in Mbps	1030	-	1030	-	1030	-
HTTP Throughput w/ IPS profile (1M size) in Mbps	1040	-	1040	-	1040	-
NGFW Throughput in Mbps [4]	760	-	830	-	455	-
Threat Protection Throughput in Mbps [5]	740	-	820	-	450	-
SSL Inspection throughput (Mbps) [6]	1030	-	1030	-	630	-

LICENSE TYPE : VM-04/04S

System Requirement						
vCPU (Minimum / Maximum)	1 / 4					
Technical Specifications						
Network Interface Support (Minimum / Maximum)	1 / 24					
Virtual Domains (Default / Maximum) [1]	10 / 50					
Firewall Policies	10 000					
OCPU [2]	2					
System Performance						
Instance Shape to be Measured	VM.Standard3.Flex (2 OCPU)					
OCI Bandwidth [3]	2 Gbps					
	SR-IOV				PARAVIRTUALIZED	IPSEC
	VFIO	IPSEC	VFIO DPDK	IPSEC		
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes	2500	2190	2500	2090	2500	1980
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	2600	1000	2600	1030	2300	850
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	1100	300	1100	250	400	150
New Sessions / Second (TCP)	180000	-	155000	-	90000	-
HTTP Throughput w/ Application profile (64K size) in Mbps	2070	-	2070	-	2070	-
HTTP Throughput w/ IPS profile (44K size) in Mbps	2070	-	2070	-	2070	-
HTTP Throughput w/ IPS profile (1M size) in Mbps	2070	-	2070	-	2070	-
NGFW Throughput in Mbps [4]	1390	-	1550	-	990	-
Threat Protection Throughput in Mbps [5]	1380	-	1500	-	980	-
SSL Inspection throughput (Mbps) [6]	2060	-	2060	-	2060	-

Notes.

PAYG supports only up to 24 OCPU (48 vCPU) instances.

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 measured using FortiOS v7.4.4.

1. 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.
2. 1 OCPU equates to 2vCPU applies only for x64 instance types. FortiGate-VM BYOL licenses are based on vCPUs, so plan accordingly.
3. The latest information about OCI bandwidth is found on https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm#vm-standard
4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
6. Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

VM64 Specifications

LICENSE TYPE : VM-08/08S

System Requirement						
vCPU (Minimum / Maximum)	1 / 8					
Technical Specifications						
Network Interface Support (Minimum / Maximum)	1 / 24					
Virtual Domains (Default / Maximum) [1]	10 / 500					
Firewall Policies	200 000					
OCPU [2]	4					
System Performance						
Instance Shape to be Measured	VM.Standard3.Flex (4 OCPU)					
OCI Bandwidth [3]	4.1 Gbps					
	SR-IOV				PARAVIRTUALIZED	IPSEC
	VFIO	IPSEC	VFIO DPDK	IPSEC		
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes	5120	4280	5100	4280	4050	3700
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	3950	2150	5000	2150	2600	1800
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	1100	400	1100	390	450	340
New Sessions / Second (TCP)	180000	-	175000	-	130000	-
HTTP Throughput w/ Application profile (64K size) in Mbps	4130	-	4130	-	4130	-
HTTP Throughput w/ IPS profile (44K size) in Mbps	4140	-	4140	-	4130	-
HTTP Throughput w/ IPS profile (1M size) in Mbps	4140	-	4140	-	4140	-
NGFW Throughput in Mbps [4]	2720	-	3300	-	2300	-
Threat Protection Throughput in Mbps [5]	2700	-	3300	-	2300	-
SSL Inspection throughput (Mbps) [6]	3750	-	3880	-	3560	-

LICENSE TYPE : VM-16/16S

System Requirement						
vCPU (Minimum / Maximum)	1 / 16					
Technical Specifications						
Network Interface Support (Minimum / Maximum)	1 / 24					
Virtual Domains (Default / Maximum) [1]	10 / 500					
Firewall Policies	200 000					
OCPU [2]	8					
System Performance						
Instance Shape to be Measured	VM.Standard3.Flex (8 OCPU)					
OCI Bandwidth [3]	8.2 Gbps					
	SR-IOV				PARAVIRTUALIZED	IPSEC
	VFIO	IPSEC	VFIO DPDK	IPSEC		
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes	10200	5500	9500	6000	10200	4100
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	4000	2500	3300	2480	4200	1950
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	850	460	850	440	700	350
New Sessions / Second (TCP)	275000	-	285000	-	240000	-
HTTP Throughput w/ Application profile (64K size) in Mbps	8270	-	8270	-	8270	-
HTTP Throughput w/ IPS profile (44K size) in Mbps	8270	-	8270	-	8270	-
HTTP Throughput w/ IPS profile (1M size) in Mbps	8300	-	8300	-	8270	-
NGFW Throughput in Mbps [4]	4500	-	7000	-	3890	-
Threat Protection Throughput in Mbps [5]	4450	-	6800	-	3820	-
SSL Inspection throughput (Mbps) [6]	6900	-	7150	-	5600	-

Notes.

PAYG supports only up to 24 OCPU (48 vCPU) instances.

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 measured using FortiOS v7.4.4.

1. 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.
2. 1 OCPU equates to 2vCPU applies only for x64 instance types. FortiGate-VM BYOL licenses are based on vCPUs, so plan accordingly.
3. The latest information about OCI bandwidth is found on https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm#vm-standard
4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
6. Using TLS ECDHE RSA WITH AES 256 GCM SHA384 (2K).

VM64 Specifications

LICENSE TYPE : VM-32/32S

System Requirement						
vCPU (Minimum / Maximum)	1 / 32					
Technical Specifications						
Network Interface Support (Minimum / Maximum)	1 / 24					
Virtual Domains (Default / Maximum) [1]	10 / 500					
Firewall Policies	200 000					
OCPU [2]	16					
System Performance						
Instance Shape to be Measured	VM.Standard3.Flex (16 OCPU)					
OCI Bandwidth [3]	16.4 Gbps					
	SR-IOV				PARAVIRTUALIZED	
	VFIO	IPSEC	VFIO DPDK	IPSEC		IPSEC
Firewall Throughput (UDP Packets) in Mbps - 1518 bytes	18000	5500	18000	5500	19400	4280
Firewall Throughput (UDP Packets) in Mbps - 512 bytes	6250	2500	6200	2540	6740	2300
Firewall Throughput (UDP Packets) in Mbps - 64 bytes	970	460	970	460	1050	460
New Sessions / Second (TCP)	280000	-	285000	-	275000	-
HTTP Throughput w/ Application profile (64K size) in Mbps	12100	-	12000	-	12100	-
HTTP Throughput w/ IPS profile (44K size) in Mbps	11900	-	12000	-	12030	-
HTTP Throughput w/ IPS profile (1M size) in Mbps	12200	-	12300	-	12300	-
NGFW Throughput in Mbps [4]	10000	-	10500	-	7000	-
Threat Protection Throughput in Mbps [5]	10000	-	10500	-	6950	-
SSL Inspection throughput (Mbps) [6]	7000	-	7200	-	6820	-

LICENSE TYPE : VM-UL/ULS

System Requirement	
vCPU (Minimum / Maximum)	1 / Unlimited
Technical Specifications	
Network Interface Support (Minimum / Maximum)	1 / 24
Virtual Domains (Default / Maximum) [1]	10 / 500
OCPU [2]	Unlimited

Notes.

PAYG supports only up to 24 OCPU (48 vCPU) instances.

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 measured using FortiOS v7.4.4.

1. 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.
2. 1 OCPU equates to 2vCPU applies only for x64 instance types. FortiGate-VM BYOL licenses are based on vCPUs, so plan accordingly.
3. The latest information about OCI bandwidth is found on https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm#vm-standard
4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix.
5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.
6. 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

Download

You can download the OCI 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 Oracle from the Platform dropdown list. Create a FortiGate-VM instance from Custom Images on the Compute Engine portal.

For information on how to setup VFIO and DPDK for FortiOS on Oracle cloud click here.

Ordering Information

The following SKUs adopt the perpetual licensing scheme:

Product	SKU	Description
FortiGate-VM02	FG-VM02	FortiGate-VM 'virtual appliance'. 2x vCPU cores.
FortiGate-VM04	FG-VM04	FortiGate-VM 'virtual appliance'. 4x vCPU cores.
FortiGate-VM08	FG-VM08	FortiGate-VM 'virtual appliance'. 8x vCPU cores.
FortiGate-VM16	FG-VM16	FortiGate-VM 'virtual appliance'. 16x vCPU cores.
FortiGate-VM32	FG-VM32	FortiGate-VM 'virtual appliance'. 32x vCPU cores.
FortiGate-VMUL	FG-VMUL	FortiGate-VM 'virtual appliance'. Unlimited vCPU cores.
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.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			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 Heurestic 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

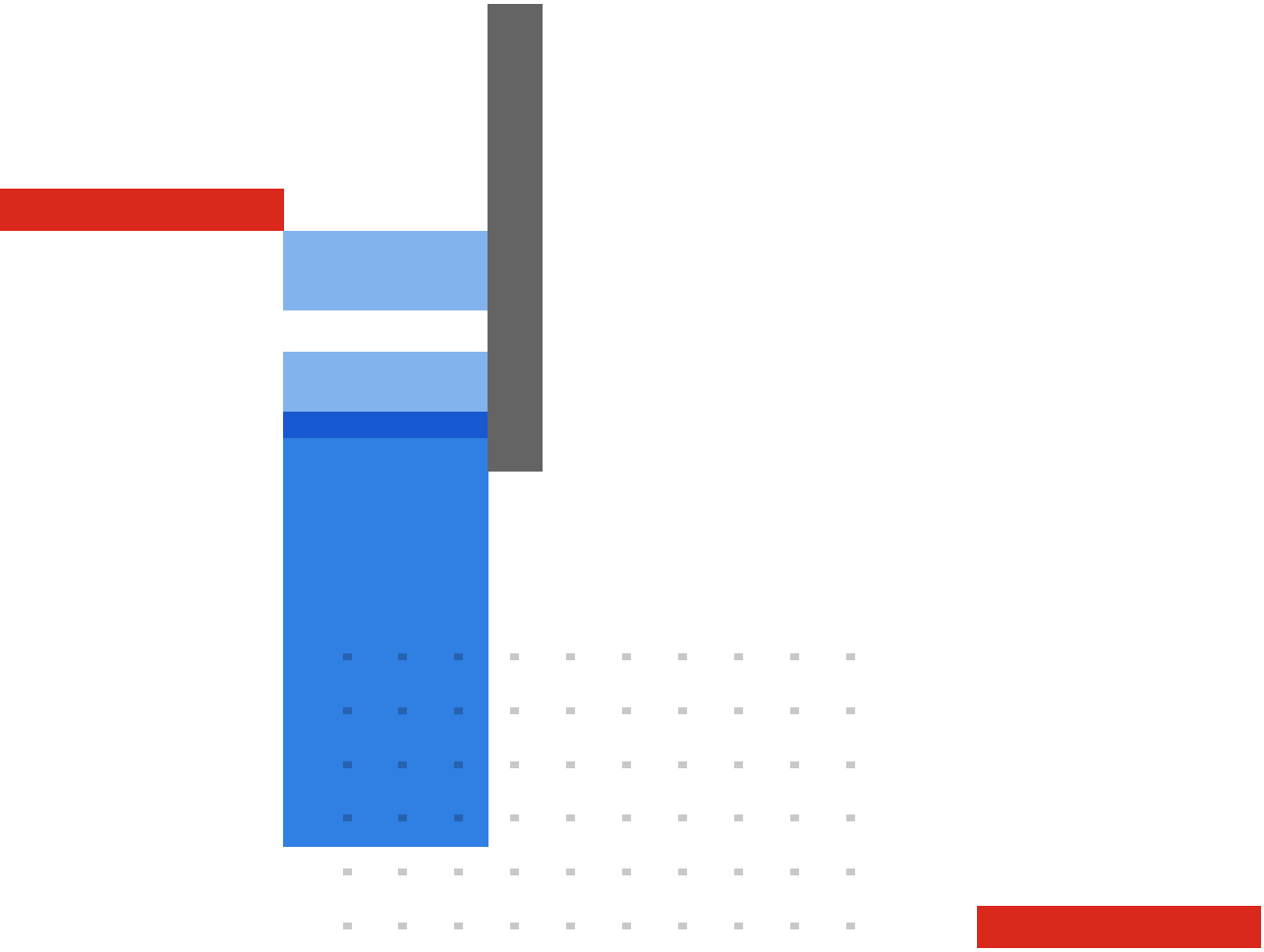
FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

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.



FORTINET

www.fortinet.com

April 7, 2025

FG-VM-OCI-DAT-R31-20250407