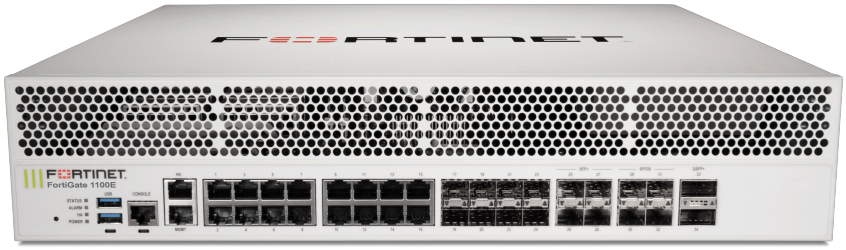
DATA SHEET

FortiGate® 1100E Series

FG-1100E and 1101E

Next Generation Firewall
Segmentation
IPS
Mobile Security



The FortiGate 1100E series delivers high-performance threat protection and SSL inspection for large enterprises and service providers, with the flexibility to be deployed at the enterprise/cloud edge, in the data center core or internal segments. The multiple high-speed interfaces, high port density, superior security efficacy and high throughput of the 1100E series keep your network connected and secure.

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 threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated best 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, multi-tenancy and effective utilization of resources
- 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 & visibility.
- Provides Zero Touch Integration with 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
80 Gbps	**12.5 Gbps**	**9.8 Gbps**	**7.1 Gbps**	Multiple GE RJ45, GE SFP, 10 GE SFP+, 25 GE SFP28, and 40 GE QSFP+ slots

Refer to specification table for details

Deployment

Next Generation Firewall (NGFW)

- Reduce complexity by combining threat protection security capabilities into the single high-performance network security appliance
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Delivers 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

Segmentation

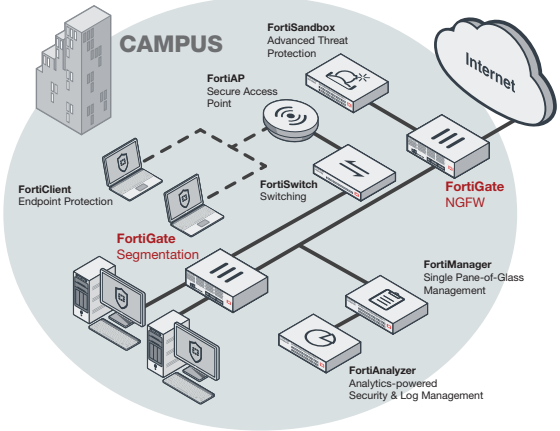
- Intent-based Segmentation builds a robust security framework while proactively reducing risk, cost, and complexity
- Integrates with Security Fabric seamlessly to allow third-party solutions and continuous trust assessment and thereby prevent sophisticated attacks
- Protects critical business applications and helps implement any compliance without network redesigns

IPS

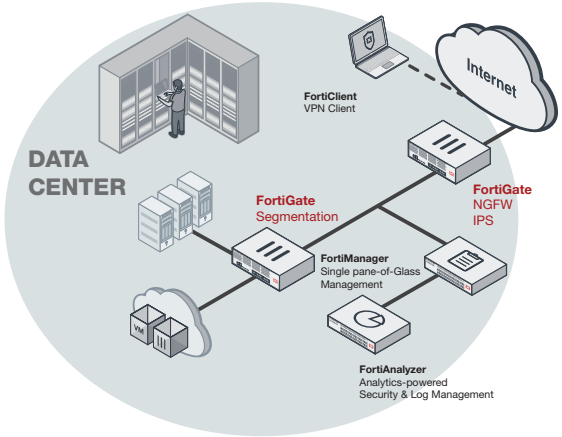
- Highly cost-effective mitigation of unpatched vulnerability for hard-to-patch systems such as IOT, ICS, and Scada
- Protect sensitive data to achieve various regulatory compliance such as PCI, HIPPA, PII, GDPR
- Multiple inspection engines, threat intelligence feeds and advanced threat protection options to defend against unknown threats in real-time
- Best of breed intrusion prevention with high-performance SSL inspection

Mobile Security for 4G, 5G and IOT

- SGi LAN security powered by multiple SPUs to provide high performance CGNAT and accelerate IPv4 and IPv6 traffic
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- Various high-speed interfaces to enable deployment flexibility



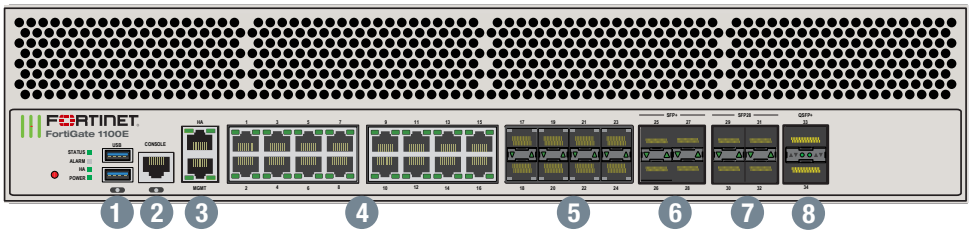
FortiGate 1100E deployment in large campus networks (NGFW, Intent-based Segmentation)

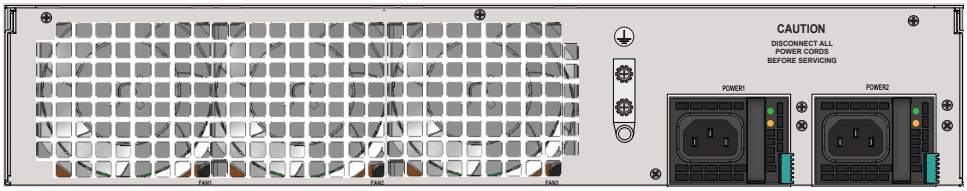


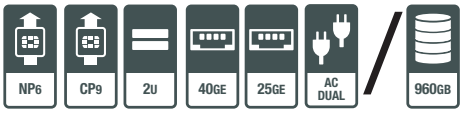
FortiGate 1100E deployment in data center (IPS/NGFW, Intent-based Segmentation)

Hardware

FortiGate 1100E/1101E







Interfaces

1. 2x USB Ports
2. Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 8x GE SFP Slots
6. 4x 10 GE SFP+ Slots
7. 4x 25 GE SFP28 / 10 GE SFP+ Slots
8. 2x 40 GE QSFP+ Slots

Powered by SPU

- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

Network Processor

Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency down to 2 microseconds
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

Fortinet's new, breakthrough SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection of computationally intensive security features:

- Enhanced IPS performance with the unique capability of full signature matching at SPU
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

High-Speed Connectivity

High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 1100E series provides 40 GE and 25 GE interfaces, simplifying network designs without relying on additional devices to bridge desired connectivity.

Fortinet Security Fabric

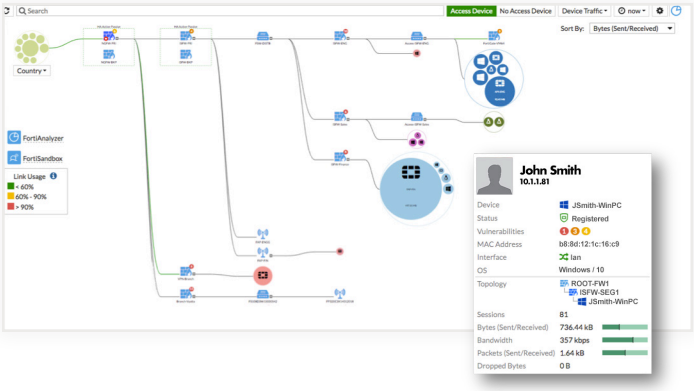
Security Fabric

The Security Fabric delivers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. All this is tied together under a single pane of glass management to deliver leading security capabilities across your entire environment while also significantly reducing complexity.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.

FortiOS

Control all security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce complexity, costs, and response time with a truly consolidated next-generation security platform.



- A truly consolidated platform with a single OS and pane-of-glass for all security and networking services across all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance. Ability to leverage latest technologies such as deception-based security.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated AI-driven breach prevention and advanced threat protection.
- Improved user experience with innovative SD-WAN capabilities and ability to detect, contain and isolate threats with Intent-based Segmentation.
- Utilize SPU hardware acceleration to boost security capability performance.

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™ Support Services

Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.

For more information, please refer to forti.net/fortiguard and forti.net/forticare

Specifications

	FORTIGATE 1100E	FORTIGATE 1101E
Interfaces and Modules		
Hardware Accelerated 40 GE QSFP+ Slots	2	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots	4	
Hardware Accelerated 10 GE SFP+ Slots	4	
Hardware Accelerated GE SFP Slots	8	
Hardware Accelerated GE RJ45 Ports	16	
GE RJ45 Management / HA Ports	2	
USB Ports (Client / Server)	1 / 2	
Console Port	1	
Onboard Storage	0	2x 480 GB SSD.
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	12.5 Gbps	
NGFW Throughput [2, 4]	9.8 Gbps	
Threat Protection Throughput [2, 5]	7.1 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 45 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 45 Gbps	
Firewall Latency (64 byte, UDP)	3 µs	
Firewall Throughput (Packet per Second)	67.5 Mpps	
Concurrent Sessions (TCP)	8 Million	
New Sessions/Second (TCP)	500,000	
Firewall Policies	100,000	
IPsec VPN Throughput (512 byte) [1]	48 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	20,000	
Client-to-Gateway IPsec VPN Tunnels	100,000	
SSL-VPN Throughput	8.4 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	10.0 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	6,500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	780,000	
Application Control Throughput (HTTP 64K) [2]	26 Gbps	
CAPWAP Throughput (HTTP 64K)	43 Gbps	
Virtual Domains (Default / Maximum)	10 / 250	
Maximum Number of FortiSwitches Supported	128	
Maximum Number of FortiAPs (Total / Tunnel)	4,096 / 2,048	
Maximum Number of FortiTokens	20,000	
Maximum Number of Registered FortiClients	20,000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 1100E	FORTIGATE 1101E
Dimensions and Power		
Height x Width x Length (inches)	3.5 x 17.44 x 17.62	
Height x Width x Length (mm)	88.9 x 443 x 447.4	
Weight	24.9 lbs (11.3 kg)	25.4 lbs (11.55 kg)
Form Factor	Rack Mount, 2 RU	
AC Power Supply	100–240V AC, 50–60 Hz	
Power Consumption (Average / Maximum)	217 W / 336 W	222 W / 346 W
Current (Maximum)	6A@120V, 3A@240V	
Heat Dissipation	1147 BTU/h	1181 BTU/h
Redundant Power Supplies	Yes, Hot swappable	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	66.7 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	

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

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.
4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Order Information

Product	SKU	Description
FortiGate 1100E	FG-1100E	2x 40 GE QSFP+ slots, 4x 25 GE SFP28 slots, 4x 10 GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, and 2 AC power supplies.
FortiGate 1101E	FG-1101E	2x 40 GE QSFP+ slots, 4x 25 GE SFP28 slots, 4x 10 GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, 960 GB SSD onboard storage, and 2 AC power supplies.

Optional Accessories/Spares	SKU	Description
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
25 GE SFP28 Transceiver Module, Long Range	FG-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for all systems with SFP28 slots.
25 GE/10 GE Dual Rate SFP28 Transceiver Module, Short Range	FG-TRAN-SFP28-SR	25 GE/10 GE dual rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots.
40 GE QSFP+ Transceivers, Short Range	FG-TRAN-QSFP+SR	40 GE QSFP+ transceivers, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceivers, Short Range, BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceivers, short range BiDi for systems with QSFP+ slots.
40 GE QSFP+ Transceivers, Long Range	FG-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.
40 GE QSFP+ to 4x 10GE SFP+ Optical Breakout	FG-TRAN-QSFP+4XSFP	40GE QSFP+ Parallel Breakout Active Optical Cable with 1m length for all systems with QSFP+ slots.
QSFP+ to 4xSFP+ Optical breakout 5m	FG-TRAN-QSFP+4SFP-5	40G QSFP+ Parallel Breakout MPO to 4xLC connectors, 5m reach, transceivers not included.
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1100/1101E, FG-1200D, FG-1500D/-DC, FG-2000E, FG-2500E, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
AC Power Supply	SP-FG300E-PS	AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FG-1100/1101E, FAZ-200F/FAZ-300F/FMG-200F and FAZ-800F/FMG-300F.

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	360 Protection	Enterprise Protection	UTM	Threat Protection
FortiCare	ASE [1]	24x7	24x7	24x7
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 Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiCASB SaaS-only Service	•	•		
FortiConverter Service	•			
SD-WAN Cloud Assisted Monitoring [2]	•			
SD-WAN Overlay Controller VPN Service [2]	•			
FortiAnalyzer Cloud [2]	•			
FortiManager Cloud [2]	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2

www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, 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. 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.