The FortiGate 400E series provides an application-centric, scalable, and secure SD-WAN solution with Next Generation Firewall (NGFW) capabilities for mid-sized to large enterprises deployed at the campus or branch level. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet’s Security-Driven Networking approach provides tight integration of the network to the new generation of security.

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

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 and 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

<table>
<thead>
<tr>
<th>Firewall</th>
<th>IPS</th>
<th>NGFW</th>
<th>Threat Protection</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 Gbps</td>
<td>7.8 Gbps</td>
<td>6 Gbps</td>
<td>5 Gbps</td>
<td>Multiple GE RJ45 and GE SFP Slots</td>
</tr>
</tbody>
</table>

Refer to specification table for details
DEPLOYMENT

Next Generation Firewall (NGFW)
- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, and applications across the entire attack surface, and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

Secure SD-WAN
- Consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport
- Accelerated multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage.
- Simplified and intuitive workflow with FortiManger for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identifies anomalies
- Strong security posture with next generation firewall and real-time threat protection

Secure Web Gateway (SWG)
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URLs and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web
HARDWARE

FortiGate 400E/401E

Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 16x GE SFP Slots

Hardware Features

Powered by SPU
- Fortinet's 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
  - VPN, CAPWAP and IP tunnel acceleration
  - Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
  - Traffic shaping and priority queuing

Content Processor
Fortinet's ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.
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 user
- **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 enable 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 allows 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 of HW, Software and As-a-Service with SASE and ZTNA, among others.

SERVICES

**FortiGuard™ Security Services**

FortiGuard Labs offer 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.
SPECSIFICATIONS

<table>
<thead>
<tr>
<th>Interfaces and Modules</th>
<th>FG-400E</th>
<th>FG-401E/DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>Hardware Accelerated GE RJ45 Interfaces</td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>USB Ports</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>RJ45 Console Port</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Onboard Storage</td>
<td>2x 240 GB SSD</td>
<td></td>
</tr>
</tbody>
</table>

Included Transceivers
2x SFP (SX 1 GE)

System Performance — Enterprise Traffic Mix

| IPS Throughput | 7.8 Gbps |
| NGFW Throughput | 6 Gbps |
| Threat Protection Throughput | 5 Gbps |

IPv4 Firewall Throughput
32 / 24 Gbps

Firewall Latency (64 byte, UDP)
2.14 μs

Firewall Throughput (Packet per Second)
36 Mpps

Concurrent Sessions (TCP)
4 Million

New Sessions/Second (TCP)
450 000

Firewall Rules
10 000

IPsec VPN Throughput (512 byte)
20 Gbps

Gateway-to-Gateway IPsec VPN Tunnels
2000

Client-to-Gateway IPsec VPN Tunnels
50 000

SSL-VPN Throughput
4.5 Gbps

Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)
5000

SSL Inspection Throughput
4.8 Gbps

SSL Inspection COPS (IPS, avg. HTTPS)
100 000

SSL Inspection Concurrent Session (IPS, avg. HTTPS)
300 000

Application Control Throughput (HTTP 64K)
12 Gbps

CAPWAP Throughput (HTTP 64K)
14.8 Gbps

Virtual Domains (Default / Maximum)
10 / 10

Maximum Number of FortiSwitches Supported
72

Maximum Number of FortiSwitches (Total / Tunnel)
512 / 256

Maximum Number of FortiAPs
5000

High Availability Configurations
Active-Active, Active-Passive, Clustering

Dimensions and Power

<table>
<thead>
<tr>
<th>FG-400E</th>
<th>FG-401E/DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
<td>1.75 x 17.0 x 15.0</td>
</tr>
<tr>
<td>Weight</td>
<td>16.4 lbs (7.4 kg)</td>
</tr>
<tr>
<td>Form Factor</td>
<td>Rack Mount, 1 RU</td>
</tr>
<tr>
<td>AC Power Input</td>
<td>100-240V AC, 50/60Hz</td>
</tr>
</tbody>
</table>

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 | 48 dBA |
| Airflow | Side and Front to Back |

Certifications

ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6 IPv6

Note:

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.
## DATA SHEET | FortiGate® 400E Series

### ORDERING INFORMATION

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>SKU</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 400E</td>
<td>FG-400E</td>
<td>18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 16x GE SFP slots, SPU NP6 and CP9 hardware accelerated.</td>
</tr>
<tr>
<td>FortiGate 401E</td>
<td>FG-401E</td>
<td>18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 16x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2x 240 GB onboard SSD storage.</td>
</tr>
<tr>
<td>FortiGate 401E-DC</td>
<td>FG-401E-DC</td>
<td>18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 16 x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2x 240GB onboard SSD storage, 1 DC power supply.</td>
</tr>
</tbody>
</table>

**Optional Accessories**

| 1GE SFP LX Transceiver Module | FN-TRAN-LX | 1GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1GE SFP RJ45 Transceiver Module | FN-TRAN-GC | 1GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots. |
| 1GE SFP SX Transceiver Module | FN-TRAN-SX | 1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots. |

**Optional Power Supply**

| SF-PG300E-PS | AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FAZ-200F/300F/800F and FMG-200F/300F. |
| SP-FG300E-DC-PS | DC power supply for FG-401E-DC and FG-1100E-DC. |

### 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.

<table>
<thead>
<tr>
<th>Bundles</th>
<th>Enterprise Protection</th>
<th>Unified Threat Protection</th>
<th>Advanced Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IPS Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Available when running FortiOS 7.0