FortiGate® 300E Series
FortiGate 300E and 301E

The FortiGate 300E 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 enterprise 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
- Prevents and detects against known attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services
- Proactively blocks unknown sophisticated attacks in real-time with the Fortinet Security Fabric integrated AI-powered FortiSandbox

Performance
- Engineered for Innovation using Fortinet’s purpose-built security processors (SPU) to deliver the industry’s best threat protection performance and ultra-low latency
- Provides industry-leading performance and protection for SSL encrypted traffic including the first firewall vendor to provide TLS 1.3 deep inspection

Certification
- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICSA, Virus Bulletin, and AV Comparatives

Networking
- Dynamic Path Selection over any WAN transport to provide better application experience based on self-healing SD-WAN capabilities
- Advanced routing, Scalable VPN, multi-cast and IPV4/IPV6 forwarding powered by purpose-built network processors

Management
- SD-WAN Orchestration provides intuitive and simplified workflow for centralized management and provisioning of business policies in a few easy clicks
- Expedited deployment with Zero touch provisioning well-suited for large and distributed infrastructure
- Automated VPN tunnels for flexible hub-to-spoke and full-mesh deployment at scale to provide bandwidth aggregation and encrypted WAN paths
- Predefined compliance checklists analyze the deployment and highlight best practices to improve the 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
- Automatically builds Network Topology visualizations which discover IoT devices and provide complete visibility into Fortinet and Fabric-ready partner products

<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>5 Gbps</td>
<td>3.5 Gbps</td>
<td>3 Gbps</td>
<td>Multiple GE RJ45 and GE SFP Slots</td>
</tr>
</tbody>
</table>

Refer to the specifications 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, 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 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 URL’s 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

**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 SD-WAN Orchestrator for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identify anomalies
- Strong security posture with next generation firewall and real-time threat protection

---

FortiGate 300E deployment in Campus (NGFW)

FortiGate 300E SWG deployment

FortiGate 300E deployment in Enterprise Branch (Secure SD-WAN)
Hardware

FortiGate 300E/301E

Interfaces
1. USB Port
2. Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 16x GE SFP 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 unique capability of full signature matching at ASIC
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading
Fortinet Security Fabric

Security Fabric
The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric covers the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off of the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats

FortiOS
FortiGates are the foundation of the Fortinet Security Fabric—the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Leverage the 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.
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection.
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation.
- Utilize SPU hardware acceleration to boost network security performance.

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™ 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

<table>
<thead>
<tr>
<th>Interfaces and Modules</th>
<th>FORTIGATE 300E</th>
<th>FORTIGATE 301E</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE RJ45 Interfaces</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>GE SFP Slots</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RJ45 Console Port</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Local Storage</td>
<td>2x 240 GB SSD</td>
<td>2x 380 GB SSD</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>2x SFP (SX 1 GE)</td>
<td>2x SFP (SX 1 GE)</td>
</tr>
</tbody>
</table>

### System Performance — Enterprise Traffic Mix
- IPS Throughput: 2.5 Gbps
- NGFW Throughput: 3.5 Gbps (2x)
- Threat Protection Throughput: 3.0 Gbps (2x)

### System Performance and Capacity
- IPv4 Firewall Throughput: 32 / 2 / 20 Gbps
- IPv6 Firewall Throughput: 32 / 2 / 20 Gbps
- Firewall Latency: 64 byte, UDP
- Firewall Throughput (Packet per Second): 4 Million
- New Sessions/Second (TCP): 3 Million
- Firewall Policies: 10,000
- IPSec VPN Throughput (512 byte): 20 Gbps
- Gateway-to-Gateway IPSec VPN Tunnels: 2,000
- Client-to-Gateway IPSec VPN Tunnels: 2,000
- SSL-VPN Throughput: 2.5 Gbps
- Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode): 10,000
- SSL Inspection Throughput (IPS, avg. HTTPS): 3.6 Gbps
- SSL Inspection DPI (IPS, avg. HTTPS): 2.5 Gbps
- SSL Inspection Concurrent Session (IPS, avg. HTTPS): 3,000
- Application Control Throughput (HTTP 64K): 7 Gbps
- CAPWAP Throughput (1444 byte, UDP): 5 Gbps
- Virtual Domains (Default / Maximum): 10 / 10
- Maximum Number of FortiSwitches Supported: 72
- Maximum Number of FortiSwitches (Total / Tunnel): 512 / 256
- Maximum Number of FortiTokens: 5,000
- High Availability Configurations: Active-Active, Active-Active, Active-Passive, Dualaring

### Dimensions and Power
<table>
<thead>
<tr>
<th>Dimensions and Power</th>
<th>FORTIGATE 300E</th>
<th>FORTIGATE 301E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
<td>1.75 x 17.0 x 15.0</td>
<td>1.75 x 17.0 x 15.0</td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
<td>44.45 x 432 x 380</td>
<td>44.45 x 432 x 380</td>
</tr>
<tr>
<td>Weight (LBs)</td>
<td>16.1</td>
<td>16.6</td>
</tr>
<tr>
<td>Weight (Kgs)</td>
<td>7.3</td>
<td>7.6</td>
</tr>
<tr>
<td>Form Factor (supports EIA / non-EIA standards)</td>
<td>Rack Mount, 1 RU</td>
<td>Rack Mount, 1 RU</td>
</tr>
<tr>
<td>Power Consumption (Average / Maximum)</td>
<td>90 W / 173 W</td>
<td>90 W / 180 W</td>
</tr>
<tr>
<td>Power Input</td>
<td>100–240V AC, 50–60Hz</td>
<td>100–240V AC, 50–60Hz</td>
</tr>
<tr>
<td>Current (Maximum)</td>
<td>6A</td>
<td>6A</td>
</tr>
<tr>
<td>Heat Dissipation</td>
<td>570 BTU/h</td>
<td>614 BTU/h</td>
</tr>
<tr>
<td>Redundant Power Supplies (Hot Swappable)</td>
<td>optional</td>
<td>optional</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
- Operating Altitude: Up to 7,400 ft (2,250 m)
- Compliance: FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
- IC Certified: 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 is measured with AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW, and Threat Protection are measured with Logging enabled.
3. SSL inspection performance uses 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.

---

FORTIGATE 300E

---

FORTIGATE 301E
## Order Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 300E</td>
<td>FG-300E</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 301E</td>
<td>FG-301E</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, 480 GB onboard SSD storage.</td>
</tr>
</tbody>
</table>

### Optional Accessories

<table>
<thead>
<tr>
<th>Module Type</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GE SFP LX Transceiver Module</td>
<td>FN-TRAN-LX</td>
<td>1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>1 GE SFP RAS Transceiver Module</td>
<td>FN-TRAN-RC</td>
<td>1 GE SFP RAS transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>1 GE SFP SX Transceiver Module</td>
<td>FN-TRAN-SX</td>
<td>1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
</tbody>
</table>

### Optional Power Supply

<table>
<thead>
<tr>
<th>Module Type</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC power supply for FG-300/301E and FG-500/501E</td>
<td>SP-FG300E-PS</td>
<td>AC power supply for FG-300/301E and FG-500/501E.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Bundles</th>
<th>360 Protection</th>
<th>Enterprise Protection</th>
<th>Unified Threat Protection</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td></td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IPS Service</td>
<td></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>
<td></td>
</tr>
<tr>
<td>FortiGuard Web Filtering Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Antispam Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Security Rating Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IoT Detection Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiConverter Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPAM Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Orchestrator Entitlement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Cloud Assisted Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD-WAN Overlay Controller VPN Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiAnalyzer Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiManager Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. 24x7 plus Advanced Services Ticket Handling  
2. Available when running FortiOS 6.4