The FortiGate 3200D 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 3200D 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 the 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>80 Gbps</td>
<td>26 Gbps</td>
<td>24 Gbps</td>
<td>15 Gbps</td>
<td>Multiple GE RJ45 and 10 GE SFP+ / GE SFP slots</td>
</tr>
</tbody>
</table>

Refer to specification table for details
**Deployment**

**Next Generation Firewall (NGFW)**
- Reduce complexity by combining threat protection security capabilities into 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 SPU 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)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- Signaling security to inspect various protocols such as SCTP, Diameter, GTP-C, SIP and provide protection against attacks
- High-speed interfaces to enable deployment flexibility
Hardware

FortiGate 3200D

1. USB Management Port
2. USB Port
3. Console Port
4. 2x GE RJ45 Management Ports
5. 48x 10 GE SFP+ / GE SFP Slots

Interfaces

- **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**
  - The SPU CP8 content processor works outside of the direct flow of traffic, providing high-speed cryptography and content inspection services including:
    - Signature-based content inspection acceleration
    - Encryption and decryption offloading

- **10 GE Connectivity for Network Segmentation**
  - High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3200D provides the highest 10 GE port densities in the market, 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

<table>
<thead>
<tr>
<th>Interfaces and Modules</th>
<th>FORTIGATE 3200D</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 GE SFP+ / GE SFP Slots</td>
<td>48</td>
</tr>
<tr>
<td>GE K/L4S Management Ports</td>
<td>1</td>
</tr>
<tr>
<td>USB Ports (client / server)</td>
<td>1</td>
</tr>
<tr>
<td>Console Port</td>
<td>1</td>
</tr>
<tr>
<td>Internal Storage</td>
<td>2x 480 GB SSD</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>2x SFP+ (SR 100G)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Performance — Enterprise Traffic Mix</th>
<th>FORTIGATE 3200D</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Throughput</td>
<td>26 Gbps</td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>24 Gbps</td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>15 Gbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Performance and Capacity</th>
<th>FORTIGATE 3200D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (1518 / 512 / 64 byte, UDP)</td>
<td>80 / 80 / 50 Gbps</td>
</tr>
<tr>
<td>(1518 / 512 / 86 byte, UDP)</td>
<td>75 Gbps</td>
</tr>
<tr>
<td>Firewall Throughput (Packet per Second)</td>
<td>75 Mpps</td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td>40 Million</td>
</tr>
<tr>
<td>New Sessions/Second (TCP)</td>
<td>400,000</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>200,000</td>
</tr>
<tr>
<td>IPsec VPN Throughput (512 byte)</td>
<td>50 Gbps</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPsec VPN Tunnels</td>
<td>50 Gbps</td>
</tr>
<tr>
<td>Client-to-Gateway IPsec VPN Tunnels</td>
<td>50 Gbps</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>8 Gbps</td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users</td>
<td>30,000</td>
</tr>
<tr>
<td>Application Control Throughput (HTTP 64K)</td>
<td>51 Gbps</td>
</tr>
<tr>
<td>CAPNAP Throughput (1444 byte, UDP)</td>
<td>22 Gbps</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum)</td>
<td>10 / 500</td>
</tr>
<tr>
<td>Maximum Number of FortiSwitches Supported</td>
<td>256</td>
</tr>
<tr>
<td>Maximum Number of FortiAPs (Total / Tunnel Mode)</td>
<td>4,096 / 2,048</td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>20,000</td>
</tr>
<tr>
<td>Maximum Number of Registered FortiClients</td>
<td>20,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dimensions and Power</th>
<th>FORTIGATE 3200D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
<td>3.5 x 17.4 x 21.9</td>
</tr>
<tr>
<td>Height x Width x Length (mm)</td>
<td>89 x 442 x 555</td>
</tr>
<tr>
<td>Weight</td>
<td>37.9 lbs (17.2 kg)</td>
</tr>
<tr>
<td>AC Power Supply</td>
<td>100–240V AC, 50–60 Hz</td>
</tr>
<tr>
<td>Power Consumption (Average / Maximum)</td>
<td>350 W / 938 W</td>
</tr>
<tr>
<td>Redundant Power Supplies</td>
<td>Yes, Hot Swappable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating Environment and Certifications</th>
<th>FORTIGATE 3200D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Temperature</td>
<td>32–104°F (0–40°C)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-31–158°F (-35–70°C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>10–90% non-condensing</td>
</tr>
<tr>
<td>Noise Level</td>
<td>50 dBA</td>
</tr>
<tr>
<td>Operating Altitude</td>
<td>Up to 7,400 ft (2,250 m)</td>
</tr>
<tr>
<td>Compliance</td>
<td>FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB</td>
</tr>
<tr>
<td>Certifications</td>
<td>ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6</td>
</tr>
<tr>
<td>High Availability Configurations</td>
<td>Active / Active / Passive / Clustering</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 3200D</td>
<td>FG-3200D</td>
<td>48x 10 GE SFP+ slots, 2x GE RJ45 Management, SPU NP6 and CP8 hardware accelerated, 960 GB SSD onboard storage, and dual AC power supplies.</td>
</tr>
</tbody>
</table>

Optional Accessories

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10 GE SFP+ Transceiver Module, Short Range</td>
<td>FG-TRAN-SFP+SPR</td>
<td>10 GE SFP + transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10 GE SFP+ Transceiver Module, Long Range</td>
<td>FG-TRAN-SFP+PLX</td>
<td>10 GE SFP + transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>1 GE SFP LX Transceiver Module</td>
<td>FG-TRAN-LX</td>
<td>1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft</td>
<td>SP-CABLE-A4KSF+</td>
<td>10 GE SFP+ active direct attach cables, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>AC Power Supply</td>
<td>SP-FG3600C-PS</td>
<td>AC power supply for FG-3000D, FG-3100D, FG-3200D, FG-3600C and FG-3240C.</td>
</tr>
</tbody>
</table>

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>360 Protection</th>
<th>Enterprise Protection</th>
<th>UTM Protection</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGTGuard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FGTGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FGTGuard IPS Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FGTGuard 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>FGTGuard Web Filtering Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FGTGuard AntiSpam Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FGTGuard Security Rating Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FGTGuard Industrial Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FGTGuard Saas-only Service</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>FGTAnalyzer Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FGTManager 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 6.2

Copyright © 2019 Fortinet, Inc. All rights reserved. FortiGate®, FortiGuard®, FortiCASB® and FortiAnalyzer®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet marks 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 explicitly states that the applicable 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.