

# FortiGate® 3900E Series

FortiGate 3980E/-DC and 3960E/-DC Series

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3900E series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network's performance. 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, ICISA, Virus Bulletin, and AV Comparatives

### Networking

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Model	FG-3980E/-DC	FG-3960E/-DC
Firewall	1.05 Tbps	620 Gbps
IPS	32 Gbps	30 Gbps
NGFW	28 Gbps	22 Gbps
Threat Protection	20 Gbps	13.5 Gbps
Network Interfaces	Multiple 40/100 GE QSFP+/QSFP28, 10 GE SFP+ and GE RJ45	Multiple 40/100 GE QSFP+/QSFP28, 10 GE SFP+ and GE RJ45

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 security effectiveness, 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



### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns



### 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



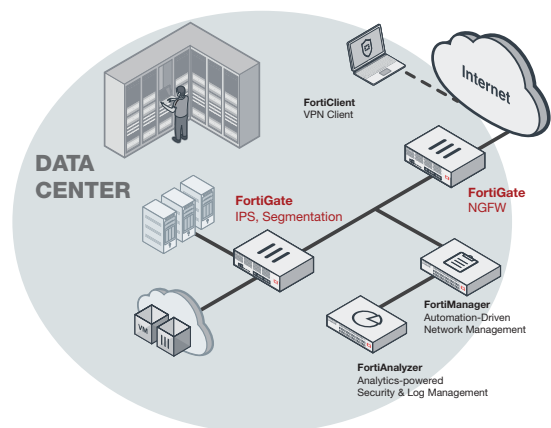
### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric



### Mobile Security for 4G, 5G, and IOT

- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- 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
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility

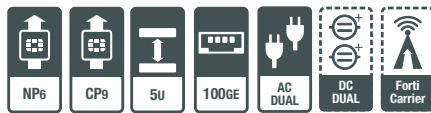
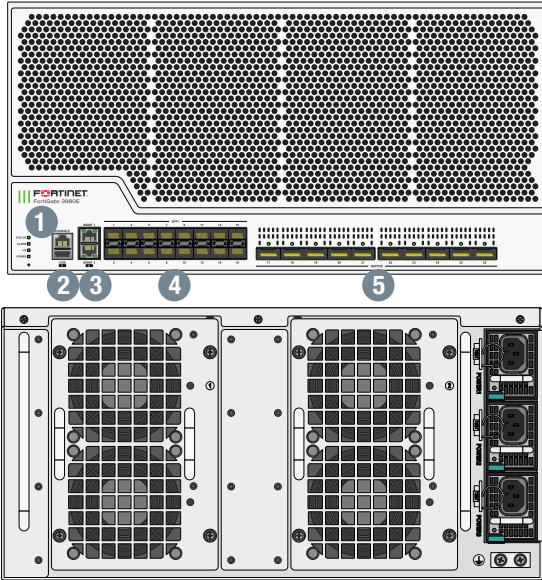


FortiGate 3900E deployment in data center (NGFW, IPS, and Intent-based Segmentation)



## Hardware

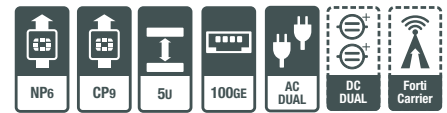
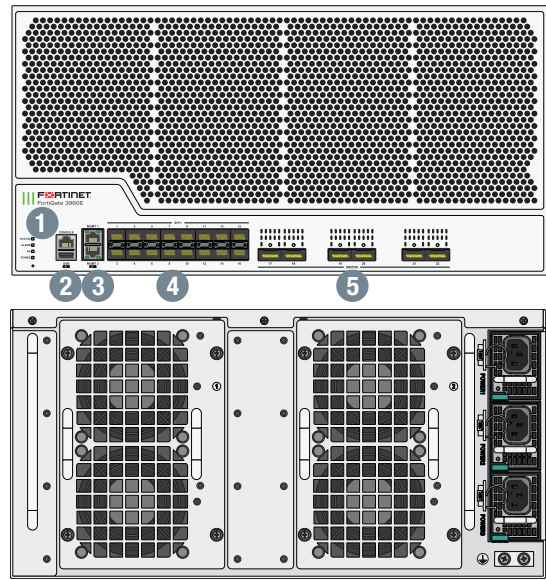
### FortiGate 3980E/-DC



#### Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45 Management Ports
4. 16x 1/10 G SFP/SFP+ Slots
5. 10x 40/100 GE QSFP+/QSFP28 Slots

### FortiGate 3960E/-DC



#### Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45 Management Ports
4. 16x 1/10 G SFP/SFP+ Slots
5. 6x 40/100 GE QSFP+/QSFP28 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:

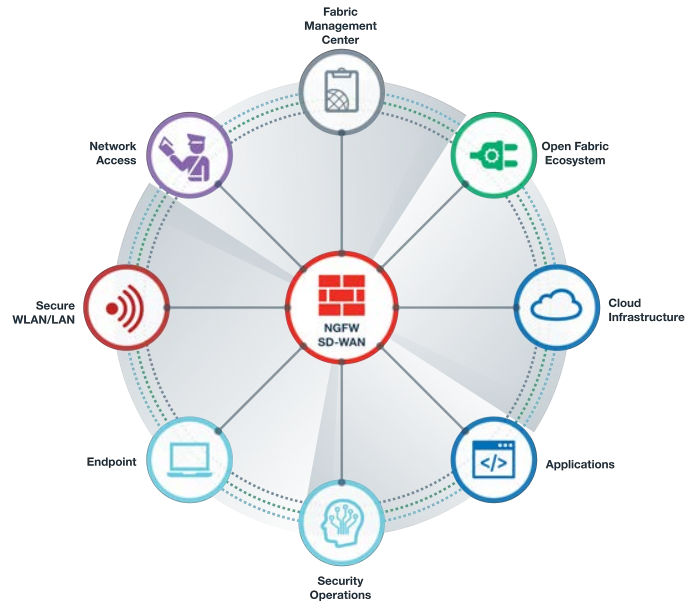
- Enhanced IPS performance with unique capability of full signature matching at SPU
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

## 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

	FG-3980E/-DC	FG-3960E/-DC
<b>Interfaces and Modules</b>		
40/100 GE QSFP+/QSFP28 Slots	10	6
10 GE SFP+ Slots		16
GE RJ45 Management Ports		2
USB Ports		1
Console Port		1
Internal Storage		–
Included Transceivers		2x SFP+ (SR 10 GE)
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>	32 Gbps	30 Gbps
NGFW Throughput <sup>2,4</sup>	28 Gbps	22 Gbps
Threat Protection Throughput <sup>2,5</sup>	20 Gbps	13.5 Gbps
<b>System Performance and Capacity</b>		
Firewall Throughput (1518 / 512 / 64 byte, UDP)	1.05 Tbps / 1.05 Tbps / 680 Gbps	620 Gbps / 610 Gbps / 370 Gbps
Firewall Latency (64 byte, UDP)		3 µs
Firewall Throughput (Packet per Second)	1,020 Mpps	555 Mpps
Concurrent Sessions (TCP)		160 Million
New Sessions/Sec (TCP)		550,000
Firewall Policies		200,000
IPsec VPN Throughput (512 byte) <sup>1</sup>	400 Gbps	280 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		40,000
Client-to-Gateway IPsec VPN Tunnels		200,000
SSL-VPN Throughput	9.5 Gbps	9 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	26 Gbps	23 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	17,000	14,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	12 Million	12 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>	55 Gbps	40 Gbps
CAPWAP Throughput (1444 byte, UDP)	14 Gbps	13.5 Gbps
Virtual Domains (Default / Maximum)		10 / 500
Maximum Number of FortiSwitches Supported		256
Maximum Number of FortiAPs (Total / Tunnel Mode)		8,192 / 2,048
Maximum Number of FortiTokens		20,000
High Availability Configurations		Active / Active, Active / Passive, Clustering

	FG-3980E/-DC	FG-3960E/-DC
<b>Dimensions and Power</b>		
Height x Width x Length (inches)	8.8 x 17.2 x 27.3	
Height x Width x Length (mm)	222 x 437 x 695	
Weight	106.3 lbs (48.2 kg)	100.8 lbs (45.8 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 5 RU	
AC Power Supply	100–240V AC, 50–60 Hz	
Power Consumption (Average / Maximum)	1172 / 2350 W	960 / 2110 W
AC Current (Maximum)	12A@100V, 10A@240V	
Heat Dissipation	8,019 BTU/h	7,200 BTU/h
DC Power Supply (FG-3980E-DC, FG-3960E-DC)	-48V DC	
DC Current (Maximum)	30A per feed (2+1)	
Redundant Power Supplies	Yes, Hot Swappable	
<b>Operating Environment and Certifications</b>		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	63 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	
NEBS Certified	–	

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, NGF, 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 3980E	FG-3980E	10x 100 GE QSFP28 slots and 16x 10 GE SFP+ slots, 2x GE RJ45 management ports, SPU NP6 and CP9 hardware accelerated, and 3 AC power supplies.
FortiGate 3980E-DC	FG-3980E-DC	10x 100 GE QSFP28 slots and 16x 10 GE SFP+ slots, 2x GE RJ45 management ports, SPU NP6 and CP9 hardware accelerated, and 3 DC power supplies.
FortiGate 3960E	FG-3960E	6x 100 GE QSFP28 slots and 16x 10 GE SFP+ slots, 2x GE RJ45 management ports, SPU NP6 and CP9 hardware accelerated, and 3 AC power supplies.
FortiGate 3960E-DC	FG-3960E-DC	6x 100 GE QSFP28 slots and 16x 10 GE SFP+ slots, 2x GE RJ45 management ports, SPU NP6 and CP9 hardware accelerated, and 3 DC power supplies.
Optional Accessories		
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots.
100 GE QSFP28 Transceivers, Short Range	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, Long Range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, CWDM4	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.
AC Power Supply	FG-7040E-PS-AC	1500 W AC power supply module for FG-7030E, FG-7040E, FG-6300/6301F, FG-6500/6501F, FG-3960E, FG-3980E (not compatible for use with FG-7060E).

## 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	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	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	•	•	•	•
FortiGuard IoT Detection Service <sup>2</sup>	•	•	•	•
FortiConverter Service	•	•	•	•
IPAM Cloud <sup>2</sup>	•	•	•	•
SD-WAN Orchestrator Entitlement <sup>2</sup>	•	•	•	•
SD-WAN Cloud Assisted Monitoring	•	•	•	•
SD-WAN Overlay Controller VPN Service	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
FortiManager Cloud	•	•	•	•

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



# FortiGate® 3800D Series

FortiGate 3800D/-DC

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3800D series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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, ICASA, Virus Bulletin, and AV Comparatives

### Networking

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
<b>320 Gbps</b>	<b>30 Gbps</b>	<b>20 Gbps</b>	<b>13 Gbps</b>	Multiple 100 GE CFP2, 40 GE QSFP+, 10 GE SFP+ and/or multiple GE SFP/RJ45 depending on variants

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 security effectiveness, 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

### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns

### Secure Web Gateway (SWG)

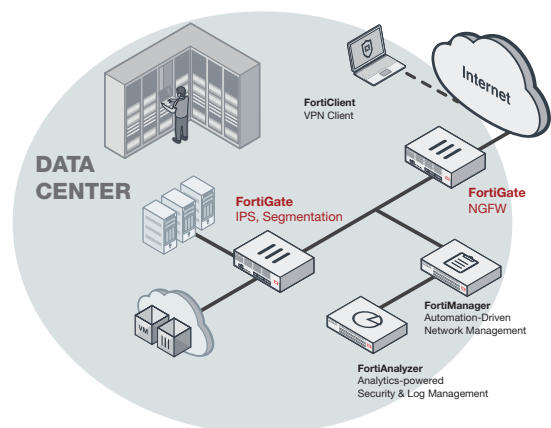
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to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

### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

### Mobile Security for 4G, 5G, and IOT

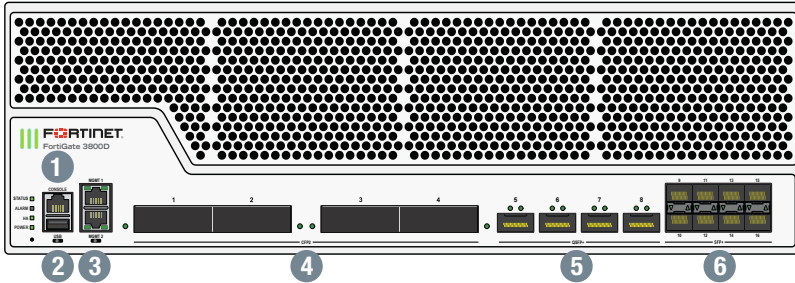
- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGi LAN and 5G N6 security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility



FortiGate 3800D deployment in data center (NGFW, IPS, and Intent-based Segmentation)

## Hardware

### FortiGate 3800D/-DC



## Interfaces

- |                                |                               |
|--------------------------------|-------------------------------|
| 1. Console Port                | 4. 4x 100 GE CFP2 Slots       |
| 2. USB Port                    | 5. 4x 40 GE QSFP+ Slots       |
| 3. 2x GE RJ45 Management Ports | 6. 8x 10 GE SFP+/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

The SPU CP8 content processor works outside of the direct flow of traffic, providing high-speed cryptography, and content inspection services including:

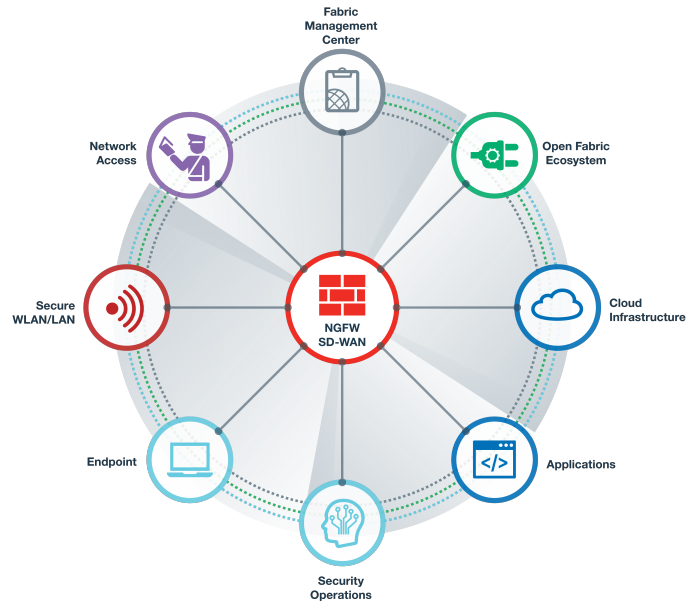
- Signature-based content inspection acceleration
- Encryption and decryption offloading

## 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

	FG-3800D	FG-3800D-DC
<b>Interfaces and Modules</b>		
100 GE CFP2 Slots		4
40 GE QSFP+ Slots		4
10 GE SFP+ Slots	8 (supports GE SFP)	
GE RJ45 Management Ports		2
USB Ports		1
Console Port		1
Internal Storage	2x 480 GB SSD	
Included Transceivers	2x SFP+ (SR 10 GE)	
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		30 Gbps
NGFW Throughput <sup>2,4</sup>		20 Gbps
Threat Protection Throughput <sup>2,5</sup>		13 Gbps
<b>System Performance and Capacity</b>		
Firewall Throughput (1518 / 512 / 64 byte, UDP)	320 / 300 / 150 Gbps	
Firewall Latency (64 byte, UDP)	5 µs	
Firewall Throughput (Packet per Second)	262.5 Mpps	
Concurrent Sessions (TCP)	95 Million	
New Sessions/Sec (TCP)	480,000	
Firewall Policies	200,000	
IPsec VPN Throughput (512 byte) <sup>1</sup>	135 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40,000	
Client-to-Gateway IPsec VPN Tunnels	200,000	
SSL-VPN Throughput	10 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000	
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	14.4 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	9,000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	7 Million	
Application Control Throughput (HTTP 64K) <sup>2</sup>	44 Gbps	
CAPWAP Throughput (1444 byte, UDP)	22 Gbps	
Virtual Domains (Default / Maximum)	10 / 500	
Maximum Number of FortiSwitches Supported	256	
Maximum Number of FortiAPs (Total / Tunnel Mode)	4,096 / 2,048	
Maximum Number of FortiTokens	20,000	
High Availability Configurations	Active / Active, Active / Passive, Clustering	

	FG-3800D	FG-3800D-DC
<b>Dimensions and Power</b>		
Height x Width x Length (inches)		5.2 x 17.4 x 26.5
Height x Width x Length (mm)		133 x 442 x 673
Weight		51 lbs (23.0 kg)
Form Factor (supports EIA / non-EIA standards)		Rack Mount, 3 RU
AC Power Supply	100–240V AC, 50–60 Hz	
Power Consumption (Average / Maximum)		537.6 / 748.8 W
AC Current (Maximum)	12A@100V, 9A@240V	–
Heat Dissipation		2,560 BTU/h
DC Power Supply	–	-48V DC
DC Current (Maximum)	–	30A
Redundant Power Supplies		Yes, Hot Swappable
<b>Operating Environment and Certifications</b>		
Operating Temperature		32–104°F (0–40°C)
Storage Temperature		-31–158°F (-35–70°C)
Humidity		10–90% non-condensing
Noise Level		60 dBA
Operating Altitude		Up to 7,400 ft (2,250 m)
Compliance		FCC Part 15 Class A, RCM, 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 3800D	FG-3800D	4x 100 GE CFP2 slots, 4x 40 GE QSFP+ slots, 8x 10 GE SFP+ slots, 2x GE RJ45 Management ports, SPU NP6 and CP8 hardware accelerated, 960 GB onboard storage, and dual AC power supplies.
FortiGate 3800D-DC	FG-3800D-DC	4x 100 GE CFP2 slots, 4x 40 GE QSFP+ slots, 8x 10 GE SFP+ slots, 2x GE RJ45 Management ports, SPU NP6 and CP8 hardware accelerated, 960 GB onboard storage, and dual DC power supplies.

Optional Accessories	SKU	Description
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots.
100 GE CFP2 Transceivers, Short Range	FG-TRAN-CFP2-SR10	100 GE CFP2 transceivers, 10 channel parallel fiber, short range for all systems with CFP2 slots.
100 GE CFP2 Transceivers, Long Range	FG-TRAN-CFP2-LR4	100 GE CFP2 transceivers, long range, over single mode fiber, for all systems with CFP2 slots.
100 GE SR10 to 10x 10 GE Fan Out Cable	FG-CABLE-SR10-SFP+	100 GE SR10 to 10x 10 GE SFP+ 1M fan out cable.
AC Power Supply	SP-FG3800D-PS	AC power supply for FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D.
DC Power Supply	SP-FG3800D-DC-PS	DC power supply for FG-3700D-DC, and FG-3700D-DC-NEBS.
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D, FG-3100D, FG-3200D, FG-3700D/-DC, FG-3700DX, FG-3810D and FG-3950B/-D.

## 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	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	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	•	•	•	•
FortiGuard IoT Detection Service <sup>2</sup>	•	•	•	•
FortiConverter Service	•	•	•	•
IPAM Cloud <sup>2</sup>	•	•	•	•
SD-WAN Orchestrator Entitlement <sup>2</sup>	•	•	•	•
SD-WAN Cloud Assisted Monitoring	•	•	•	•
SD-WAN Overlay Controller VPN Service	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
FortiManager Cloud	•	•	•	•

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





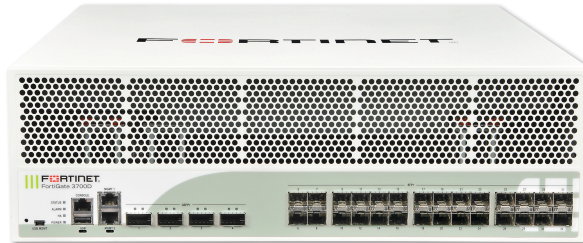


DATA SHEET

# FortiGate® 3700D

FortiGate 3700D and 3700D-DC

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3700D series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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, ICASA, Virus Bulletin, and AV Comparatives

### Networking

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
160 Gbps	28 Gbps	20 Gbps	13 Gbps	Multiple 40 GE QSFP+, 10 GE SFP+ and GE SFP

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 security effectiveness, 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



### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns



### 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



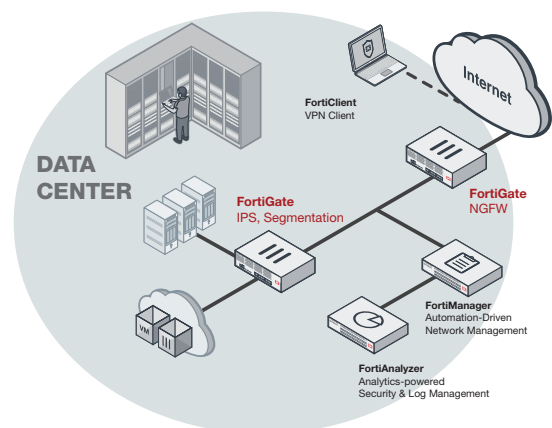
### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric



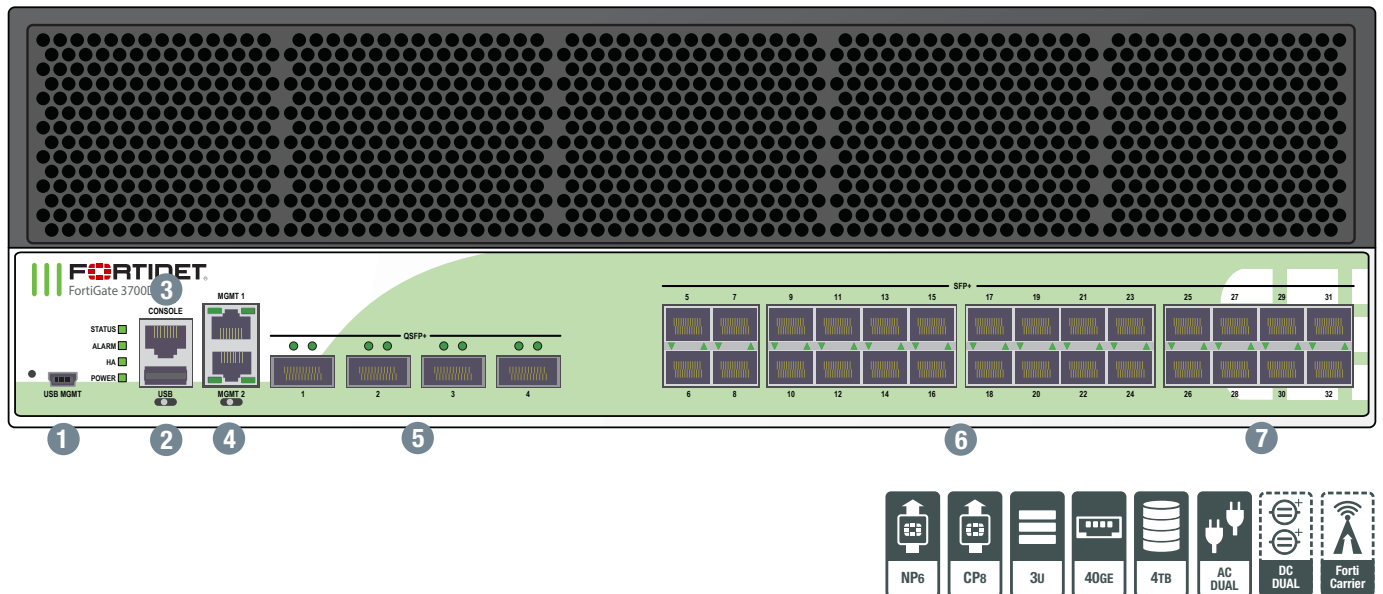
### Mobile Security for 4G, 5G, and IOT

- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- 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
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility



FortiGate 3700D deployment in data center (NGFW, IPS, and Intent-based Segmentation)

## Hardware



## Interfaces

1. USB Management Port
2. USB Port
3. Console Port
4. 2x GE RJ45 Management Ports
5. 4x 40 GE QSFP Slots

6. 20x 10 GE SFP+ / GE SFP Slots
7. 8x 10 GE SFP+ Slots (Ultra-low latency)

### 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

### 40 GE Connectivity for Core Infrastructure

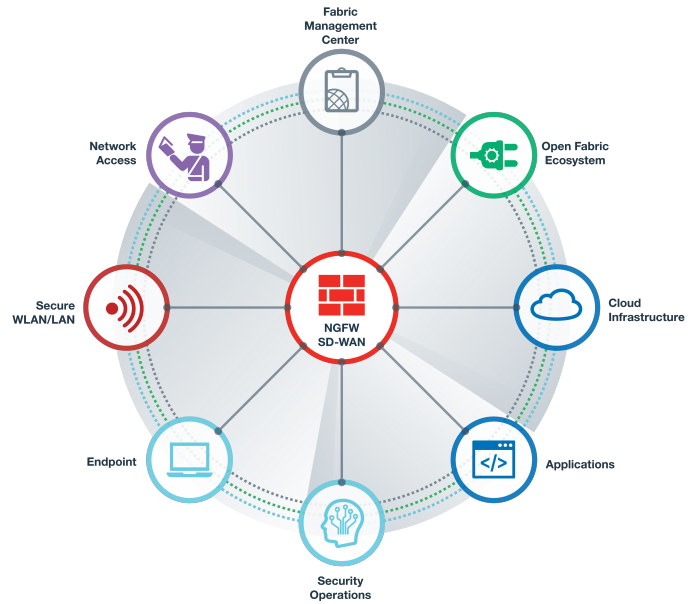
High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3700D provides one of the highest 40 GE and 10 GE port densities in the market, simplifying network designs without relying on additional devices to bridge desired connectivity.

# Fortinet Security Fabric

## Security Fabric

The Security Fabric 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

	FG-3700D	FG-3700D-DC
<b>Interfaces and Modules</b>		
40 GE QSFP Slots		4
10 GE SFP+ / GE SFP Slots		20
10 GE SFP+ Slots (Ultra-low Latency)		8
GE RJ45 Management Ports		2
USB Ports (Client / Server)		1 / 1
Console Port		1
Internal Storage		2x 2 TB HDD
Included Transceivers		2x SFP+ (SR 10GE)
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		28 Gbps
NGFW Throughput <sup>2,4</sup>		20 Gbps
Threat Protection Throughput <sup>2,5</sup>		13 Gbps
<b>System Performance and Capacity</b>		
Firewall Throughput (1518 / 512 / 64 byte, UDP)		160 / 160 / 110 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		160 / 160 / 110 Gbps
Firewall Latency (64 byte, UDP)		2 µs
Firewall Throughput (Packet per Second)		165 Mpps
Concurrent Sessions (TCP)		50 Million
New Sessions/Second (TCP)		400,000
Firewall Policies		200,000
IPsec VPN Throughput (512 byte) <sup>1</sup>		100 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		40,000
Client-to-Gateway IPsec VPN Tunnels		200,000
SSL-VPN Throughput		10 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		15.5 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		8,500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		3.5 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>		40 Gbps
CAPWAP Throughput (1444 byte, UDP)		22 Gbps
Virtual Domains (Default / Maximum)		10 / 500
Maximum Number of FortiSwitches Supported		256
Maximum Number of FortiAPs (Total / Tunnel Mode)		4,096 / 2,048
Maximum Number of FortiTokens		20,000
High Availability Configurations		Active / Active, Active / Passive, Clustering

	FG-3700D	FG-3700D-DC
<b>Dimensions and Power</b>		
Height x Width x Length (inches)		5.25 x 17.2 x 22.8
Height x Width x Length (mm)		133 x 437 x 579
Weight		46.9 lbs (21.3 kg)
Form Factor (supports EIA/non-EIA standards)		Rack Mount, 3 RU
AC Power Supply		100–240V AC, 50–60 Hz
AC Current (Maximum)		12A@100V, 5A@240V
Power Consumption (Average / Maximum)		609.6 W / 840 W
Heat Dissipation		2,871 BTU/h
DC Power Supply (FG-3700D-DC)	–	–48V DC
DC Current (Maximum)	–	17.5A
Redundant Power Supplies		Yes, Hot Swappable
<b>Operating Environment and Certifications</b>		
Operating Temperature		32–104°F (0–40°C)
Storage Temperature		-31–158°F (-35–70°C)
Humidity		10–90% non-condensing
Noise Level		60 dBA
Operating Altitude		Up to 7,400 ft (2,250 m)
Compliance		FCC Part 15 Class A, RCM, 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 3700D	FG-3700D	4x 40 GE QSFP+ slots, 28x 10 GE SFP+ slots, 2x GE RJ45 Management, SPU NP6 and CP8 hardware accelerated, 4 TB (2x 2TB) HDD onboard storage, and dual AC power supplies.
FortiGate 3700D-DC	FG-3700D-DC	4x 40 GE QSFP+ slots, 28x 10 GE SFP+ slots, 2x GE RJ45 Management, SPU NP6 and CP8 hardware accelerated, 4 TB (2x 2 TB) HDD onboard storage, and dual DC power supplies.
Optional Accessories		
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D/DG, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots.
AC Power Supply	SP-FG3800D-PS	AC power supply for FG-3700D, FG-3700DX, FG-3810D and FG-3815D.
DC Power Supply	SP-FG3800D-DC-PS	DC power supply for FG-3700D-DC, FG-3810D-DC, FG-3815D-DC.

## 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	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	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	•	•		
FortiGuard IoT Detection Service <sup>2</sup>	•	•		
FortiConverter Service	•	•		
IPAM Cloud <sup>2</sup>	•			
SD-WAN Orchestrator Entitlement <sup>2</sup>	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

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



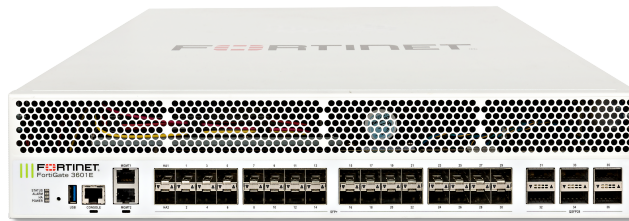


DATA SHEET

# FortiGate® 3600E Series

FG-3600E/-DC and 3601E

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3600E series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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, ICASA, Virus Bulletin, and AV Comparatives

### Networking

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
240 Gbps	55 Gbps	40 Gbps	30 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100 GE QSFP28 / 40 GE QSFP+ slots

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 security effectiveness, 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



### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns



### 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



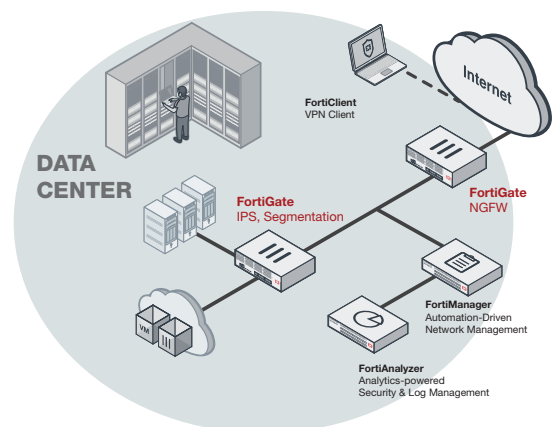
### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric



### Mobile Security for 4G, 5G, and IOT

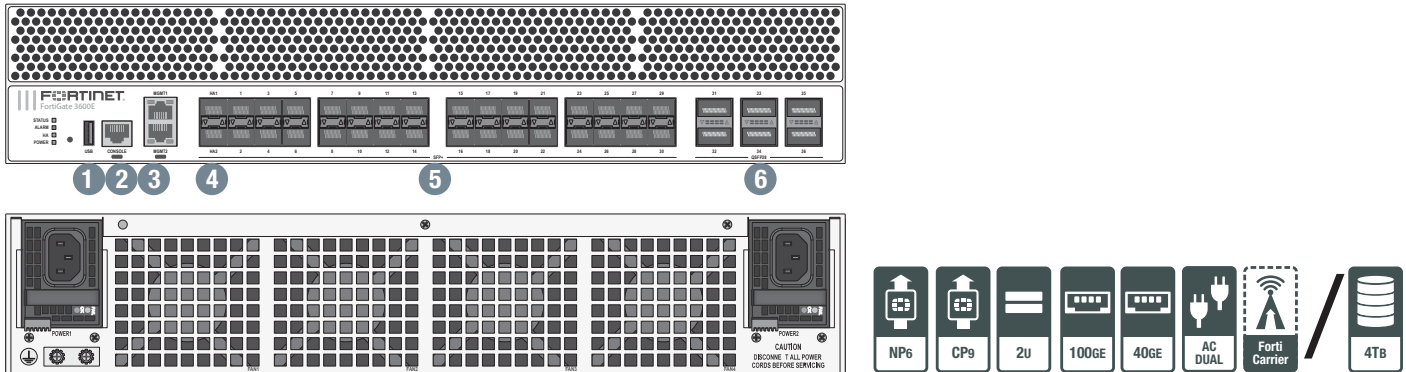
- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility



FortiGate 3600E deployment in data center (NGFW, IPS, and Intent-based Segmentation)

## Hardware

### FortiGate 3600E/-DC and 3601E



## Interfaces

- |  |   |
|--|---|
| <ol style="list-style-type: none"> <li>1. USB Management Port</li> <li>2. Console Port</li> <li>3. 2x GE RJ45 Management Ports (supports 1 GE only)</li> </ol> | <ol style="list-style-type: none"> <li>4. 2x 25 GE SFP28 / 10 GE SFP+ / GE SFP HA Slots</li> <li>5. 30x 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots</li> <li>6. 6x 100 GE QSFP28 / 40 GE QSFP+ Slots</li> </ol> |
|--|---|

### 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 SPU
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

### 100 GE Connectivity for Network

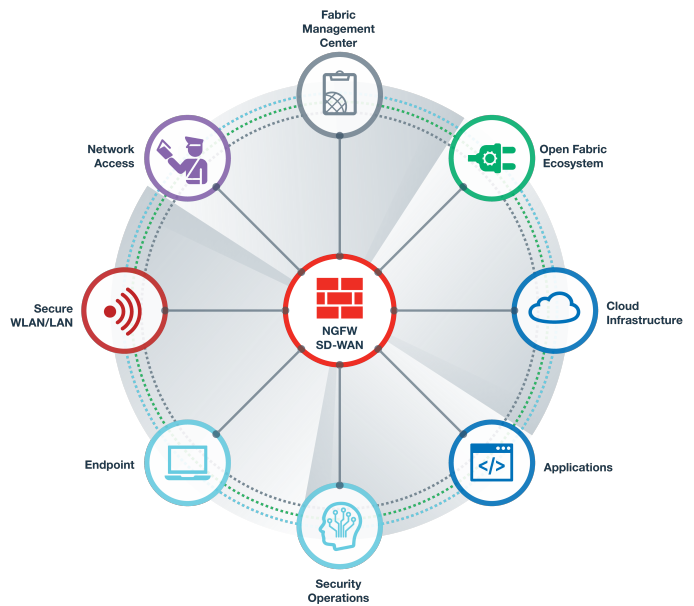
High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3600E provides multiple 100 GE QSFP28 slots, simplifying network designs without relying on additional devices to bridge desired connectivity.

## 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)



## Specifications

	FG-3600E/-DC	FG-3601E
<b>Interfaces and Modules</b>		
100 GE QSFP28 / 40 GE QSFP+ Slots		6
25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		32
GE RJ45 Management Ports	2 (supports 1 GE only)	
USB Ports (Client / Server)	1 / 1	
Console Port	1	
Internal Storage	–	2x 2TB SSD
Included Transceivers	2x SFP+ (SR 10GE)	
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		55 Gbps
NGFW Throughput <sup>2,4</sup>		40 Gbps
Threat Protection Throughput <sup>2,5</sup>		30 Gbps
<b>System Performance and Capacity</b>		
Firewall Throughput (1518 / 512 / 64 byte, UDP)	240 / 240 / 150 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	240 / 240 / 150 Gbps	
Firewall Latency (64 byte, UDP)	4 µs	
Firewall Throughput (Packet per Second)	225 Mpps	
Concurrent Sessions (TCP)	50 Million	
New Sessions/Second (TCP)	460,000	
Firewall Policies	200,000	
IPsec VPN Throughput (512 byte) <sup>1</sup>	145 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40,000	
Client-to-Gateway IPsec VPN Tunnels	200,000	
SSL-VPN Throughput	12 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000	
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	34 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	19,000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	5.2 Million	
Application Control Throughput (HTTP 64K) <sup>2</sup>	95 Gbps	
CAPWAP Throughput (HTTP 64K)	57 Gbps	
Virtual Domains (Default / Maximum)	10 / 500	
Maximum Number of FortiSwitches Supported	256	
Maximum Number of FortiAPs (Total / Tunnel Mode)	4,096 / 2,048	
Maximum Number of FortiTokens	20,000	
High Availability Configurations	Active / Active, Active / Passive, Clustering	

	FG-3600E/-DC	FG-3601E
<b>Dimensions and Power</b>		
Height x Width x Length (inches)	3.5 x 17.4 x 21.9	
Height x Width x Length (mm)	89 x 443 x 556	
Weight	43.1 lbs (19.6 kg)	44.5 lbs (20.2 kg)
Form Factor (supports EIA / non-EIA standards)	Rack Mount, 2 RU	
AC Power Supply	100–240V AC, 50–60 Hz	
AC Current (Maximum)	12A@120V, 9A@240V	
Power Consumption (Average / Maximum)	672 W / 977 W	
Heat Dissipation	3334 BTU/h	
DC Power Supply (FG-3600E-DC)	-48V DC	–
DC Current (Maximum)	17.8A	–
Redundant Power Supplies	Yes, Hot Swappable	
<b>Operating Environment and Certifications</b>		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	60 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, RCM, 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 3600E	FG-3600E	6x 100 GE QSFP28 slots and 32x 25 GE SFP28 slots (including 30x ports, 2x HA ports), 2x GE RJ45 Management Ports, SPU NP6 and CP9 hardware accelerated, and 2 AC power supplies.
FortiGate 3600E-DC	FG-3600E-DC	6x 100 GE QSFP28 slots and 32x 25 GE SFP28 slots (including 30x ports, 2x HA ports), 2x GE RJ45 Management Ports, SPU NP6 and CP9 hardware accelerated, and 2 DC power supplies.
FortiGate 3601E	FG-3601E	6x 100 GE QSFP28 slots and 32x 25 GE SFP28 slots (including 30x ports, 2x HA ports), 2x GE RJ45 Management Ports, SPU NP6 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 AC power supplies.
Optional Accessories		
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D/DC, 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-FG3800D-PS	AC power supply for FG-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D.
DC power supply	SP-FG3800D-DC-PS	DC power supply for FG-3400/3401E-DC, FG-3600E-DC, FG-3700D-DC, FG-3700D-DC-NEBS, FG-3810D-DC, FG-3815D-DC.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended 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, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range for all systems with SFP28 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.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceiver module, short range BiDi for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots.
100 GE QSFP28 Transceivers, Short Range	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, Long Range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, CWDM4	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.

## 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	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	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	•	•		
FortiGuard IoT Detection Service <sup>2</sup>	•	•		
FortiConverter Service	•	•		
IPAM Cloud <sup>2</sup>	•			
SD-WAN Orchestrator Entitlement <sup>2</sup>	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

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



www.fortinet.com

Copyright © 2020 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.

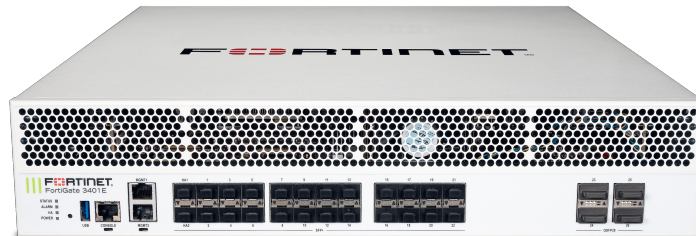


DATA SHEET

# FortiGate® 3400E Series

FG-3400E/-DC and 3401E/-DC

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3400E series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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, ICASA, Virus Bulletin, and AV Comparatives

### Networking

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
240 Gbps	44 Gbps	34 Gbps	23 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100 GE QSFP28 / 40 GE QSFP+ slots

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 security effectiveness, 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

### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns

### Secure Web Gateway (SWG)

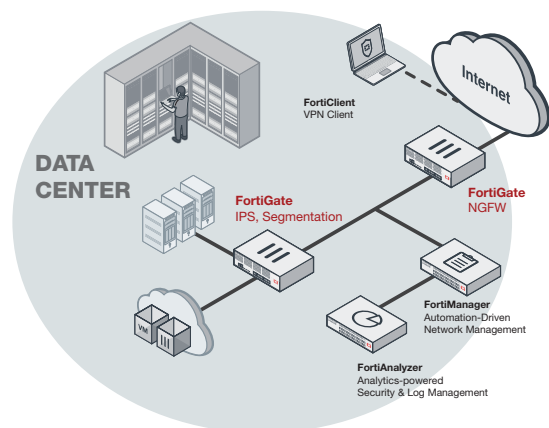
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to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

### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

### Mobile Security for 4G, 5G, and IOT

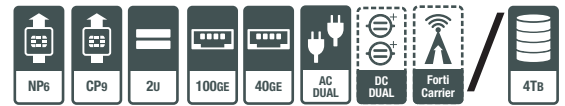
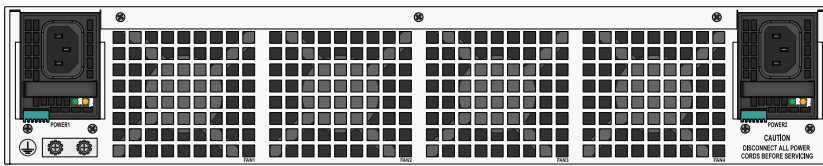
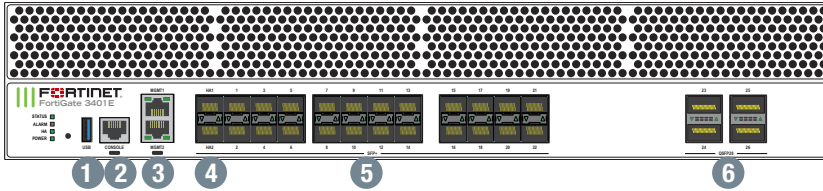
- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility



FortiGate 3400E deployment in data center (NGFW, IPS, and Intent-based Segmentation)

## Hardware

### FortiGate 3400E/-DC and 3401E/-DC



## Interfaces

- |                                |  |
|--------------------------------|--|
| 1. USB Management Port         | 4. 2x 25 GE SFP28 / 10 GE SFP+ / GE SFP HA Slots |
| 2. Console Port                | 5. 22x 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots   |
| 3. 2x GE RJ45 Management Ports | 6. 4x 100 GE QSFP28 / 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 unique capability of full signature matching at SPU
- SSL Inspection capabilities based on the latest industry mandated cipher suites
- Encryption and decryption offloading

### 100 GE Connectivity for Network

High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3400E provides multiple 100 GE QSFP28 slots, simplifying network designs without relying on additional devices to bridge desired connectivity.

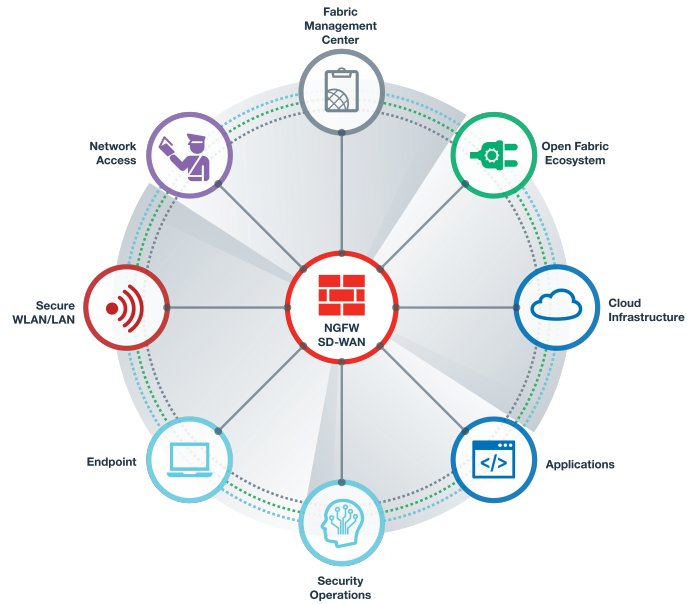


## Fortinet Security Fabric

### 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)



## Specifications

	FG-3400E/-DC	FG-3401E/-DC
<b>Interfaces and Modules</b>		
100 GE QSFP28 / 40 GE QSFP+ Slots		4
25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		24
GE RJ45 Management Ports		2
USB Ports (Client / Server)		1 / 1
Console Port		1
Internal Storage	–	2x 2TB SSD
Included Transceivers		2x SFP+ (SR 10 GE)
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		44 Gbps
NGFW Throughput <sup>2,4</sup>		34 Gbps
Threat Protection Throughput <sup>2,5</sup>		23 Gbps
<b>System Performance and Capacity</b>		
Firewall Throughput (1518 / 512 / 64 byte, UDP)		240 / 238 / 150 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		240 / 238 / 150 Gbps
Firewall Latency (64 byte, UDP)		4 µs
Firewall Throughput (Packet per Second)		225 Mpps
Concurrent Sessions (TCP)		50 Million
New Sessions/Second (TCP)		460,000
Firewall Policies		200,000
IPsec VPN Throughput (512 byte) <sup>1</sup>		140 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		40,000
Client-to-Gateway IPsec VPN Tunnels		200,000
SSL-VPN Throughput		11 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		30 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		14,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		4.9 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>		86 Gbps
CAPWAP Throughput (HTTP 64K)		57 Gbps
Virtual Domains (Default / Maximum)		10 / 500
Maximum Number of FortiSwitches Supported		256
Maximum Number of FortiAPs (Total / Tunnel Mode)		4,096 / 2,048
Maximum Number of FortiTokens		20,000
High Availability Configurations		Active / Active, Active / Passive, Clustering

	FG-3400E/-DC	FG-3401E/-DC
<b>Dimensions and Power</b>		
Height x Width x Length (inches)		3.5 x 17.44 x 21.89
Height x Width x Length (mm)		88.9 x 443 x 556
Weight	42.9 lbs (19.5 kg)	44.3 lbs (20.1 kg)
Form Factor (supports EIA/non-EIA standards)		Rack Mount, 2 RU
AC Power Supply		100–240V AC, 50/60 Hz
Power Consumption (Average / Maximum)	513 W / 728 W	519 W / 750 W
AC Current (Maximum)		12A@120V, 9A@240V
Heat Dissipation	2484 BTU/h	2560 BTU/h
DC Power Supply		-48V DC
DC Current (Maximum)		17.8A
Redundant Power Supplies		Yes, Hot Swappable
<b>Operating Environment and Certifications</b>		
Operating Temperature		32–104°F (0–40°C)
Storage Temperature		-31–158°F (-35–70°C)
Humidity		10–90% non-condensing
Noise Level		63 dBA
Operating Altitude		Up to 7,400 ft (2,250 m)
Compliance		FCC Part 15 Class A, RCM, 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 3400E	FG-3400E	4x 100 GE QSFP28 slots and 24x 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, and 2 AC power supplies.
FortiGate 3400E-DC	FG-3400E-DC	4x 100 GE QSFP28 slots and 24x 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, and 2 DC power supplies.
FortiGate 3401E	FG-3401E	4x 100 GE QSFP28 slots and 24x 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 AC power supplies.
FortiGate 3401E-DC	FG-3401E-DC	4x 100 GE QSFP28 slots and 24x 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 DC power supplies.
Optional Accessories		
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D/DC, 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-FG3800D-PS	AC power supply for FG-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D.
DC power supply	SP-FG3800D-DC-PS	DC power supply for FG-3400/3401E-DC, FG-3700D-DC, FG-3700D-DC-NEBS, FG-3810D-DC, FG-3815D-DC.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended 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, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range for all systems with SFP28 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.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceiver module, short range BiDi for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots.
100 GE QSFP28 Transceivers, Short Range	FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, Long Range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots.
100 GE QSFP28 Transceivers, CWDM4	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.

## 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	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	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	•	•		
FortiGuard IoT Detection Service <sup>2</sup>	•	•		
FortiConverter Service	•	•		
IPAM Cloud <sup>2</sup>	•			
SD-WAN Orchestrator Entitlement <sup>2</sup>	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

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



www.fortinet.com

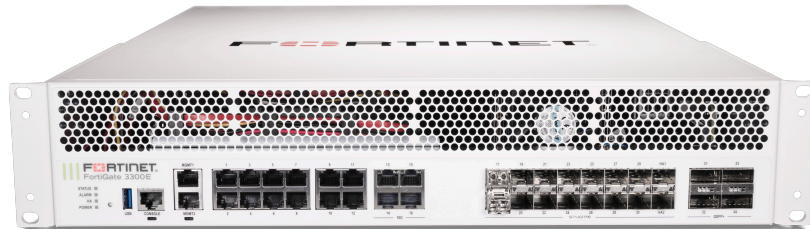


DATA SHEET

# FortiGate® 3300E Series

FG-3300E and 3301E

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3300E series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
160 Gbps	27 Gbps	23 Gbps	17 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ and 40 GE QSFP+ slots

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 security effectiveness, 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

### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns

### Secure Web Gateway (SWG)

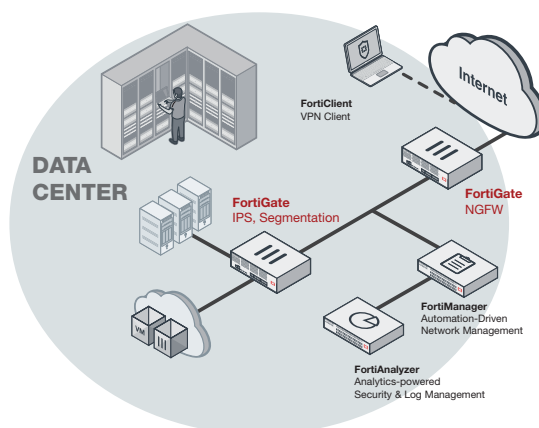
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to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

### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

### Mobile Security for 4G, 5G, and IOT

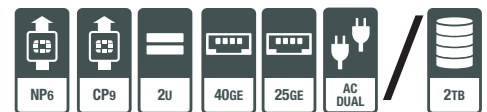
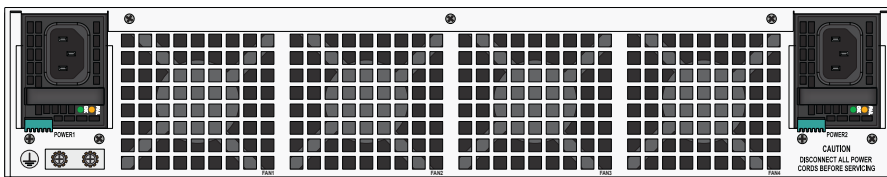
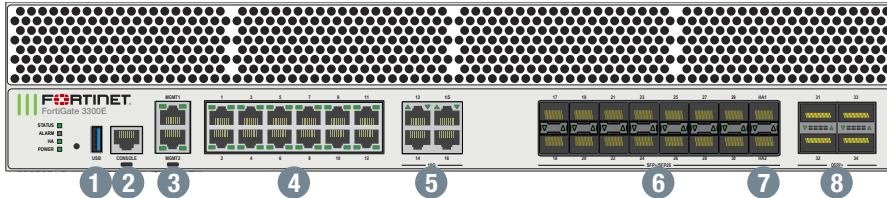
- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility



FortiGate 3300E deployment in data center (NGFW, IPS, and Intent-based Segmentation)

## Hardware

### FortiGate 3300E and 3301E



### Interfaces

- |                           |   |
|---------------------------|---|
| 1. USB Management Port    | 5. 4x 10 GE RJ45 Ports                  |
| 2. Console Port           | 6. 14x 25 GE SFP28 / 10 GE SFP+ Slots   |
| 3. 2x GE RJ45 MGMT/ Ports | 7. 2x 25 GE SFP28 / 10 GE SFP+ HA Slots |
| 4. 12x GE RJ45 Ports      | 8. 4x 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 3300E series provides 40 GE and 25 GE interfaces, simplifying network designs without relying on additional devices to bridge desired connectivity

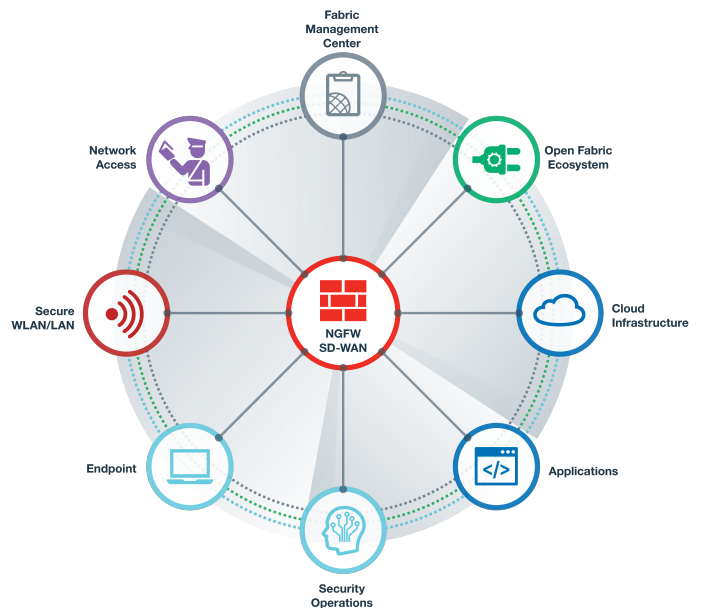


## Fortinet Security Fabric

### Security Fabric

The Security Fabric 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

	FG-3300E	FG-3301E
<b>Interfaces and Modules</b>		
40 GE QSFP+ Slots		4
25 GE SFP28 / 10 GE SFP+ HA Slots		2
25 GE SFP28 / 10 GE SFP+ Slots		14
10 GE RJ45 Ports		4
GE RJ45 Ports		12
GE RJ45 Management/HA Ports		2
USB Ports (Client / Server)		1 / 1
Console Port		1
Internal Storage	–	2x 1 TB SSD
Included Transceivers		2x SFP+ (SR 10 GE)
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		27 Gbps
NGFW Throughput <sup>2,4</sup>		23 Gbps
Threat Protection Throughput <sup>2,5</sup>		17 Gbps
<b>System Performance and Capacity</b>		
Firewall Throughput (1518 / 512 / 64 byte, UDP)		160 / 158 / 100 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		160 / 158 / 100 Gbps
Firewall Latency (64 byte, UDP)		4 µs
Firewall Throughput (Packet per Second)		150 Mpps
Concurrent Sessions (TCP)		50 Million
New Sessions/Second (TCP)		460,000
Firewall Policies		200,000
IPsec VPN Throughput (512 byte) <sup>1</sup>		98 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		40,000
Client-to-Gateway IPsec VPN Tunnels		200,000
SSL-VPN Throughput		10 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		21 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		11,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		4 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>		70 Gbps
CAPWAP Throughput (HTTP 64K)		55 Gbps
Virtual Domains (Default / Maximum)		10 / 500
Maximum Number of FortiSwitches Supported		256
Maximum Number of FortiAPs (Total / Tunnel Mode)		4,096 / 2,048
Maximum Number of FortiTokens		20,000
High Availability Configurations		Active / Active, Active / Passive, Clustering

	FG-3300E	FG-3301E
<b>Dimensions and Power</b>		
Height x Width x Length (inches)	3.5 x 17.44 x 21.89	
Height x Width x Length (mm)	88.9 x 443 x 556	
Weight	42.9 lbs (19.5 kg)	44.3 lbs (20.1 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2 RU	
AC Power Supply	100–240V AC, 60–50 Hz	
Power Consumption (Average / Maximum)	492 W / 610 W	496 W / 617 W
Maximum Current	12@100V, 9A@240V	
Heat Dissipation	2097 BTU/h	2105 BTU/h
Redundant Power Supplies	Yes, Hot Swappable	
<b>Operating Environment and Certifications</b>		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	70 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, RCM, 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 3300E	FG-3300E	4x 40 GE QSFP+ slots, 16x 25 GE SFP28 slots (including 14x ports, 2x HA ports), 14x GE RJ45 ports (including 12x ports, 2x management ports), 4x 10GBase-T ports, SPU NP6 and CP9 hardware accelerated, and dual AC power supplies.
FortiGate 3301E	FG-3301E	4x 40 GE QSFP+ slots, 16x 25 GE SFP28 slots (including 14x ports, 2x HA ports), 14x GE RJ45 ports (including 12x ports, 2x management ports), 4x 10GBase-T ports, SPU NP6 and CP9 hardware accelerated, and dual AC power supplies, with 2x 1 TB SSD onboard storage.
Optional Accessories		
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D/DC, 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-FG3800D-PS	AC power supply for FG-2200/2201E, FG-3300/3301E, FG-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D and FG-3815D.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended 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, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range for all systems with SFP28 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.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Short Range BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceiver module, short range BiDi for all systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, 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.

## 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.

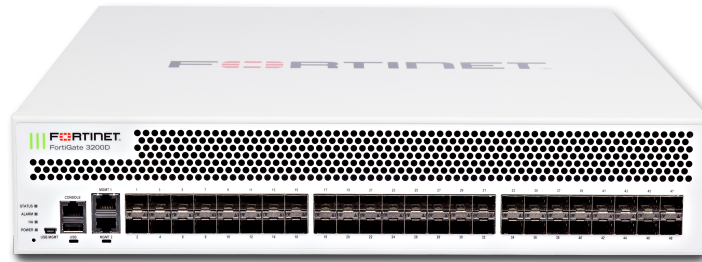
Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiGuard IoT Detection Service <sup>2</sup>	•	•		
FortiConverter Service	•	•		
IPAM Cloud <sup>2</sup>	•			
SD-WAN Orchestrator Entitlement <sup>2</sup>	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

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



# FortiGate® 3200D

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3200D series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
80 Gbps	26 Gbps	24 Gbps	15 Gbps	Multiple GE RJ45 and 10 GE SFP+ / GE SFP slots

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 security effectiveness, 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

### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns

### Secure Web Gateway (SWG)

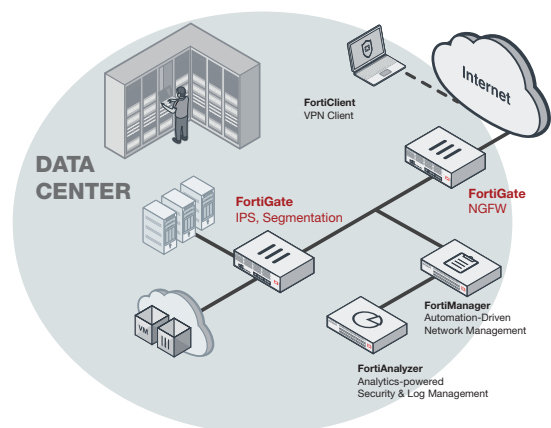
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to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

### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

### Mobile Security for 4G, 5G, and IOT

- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- 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
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility

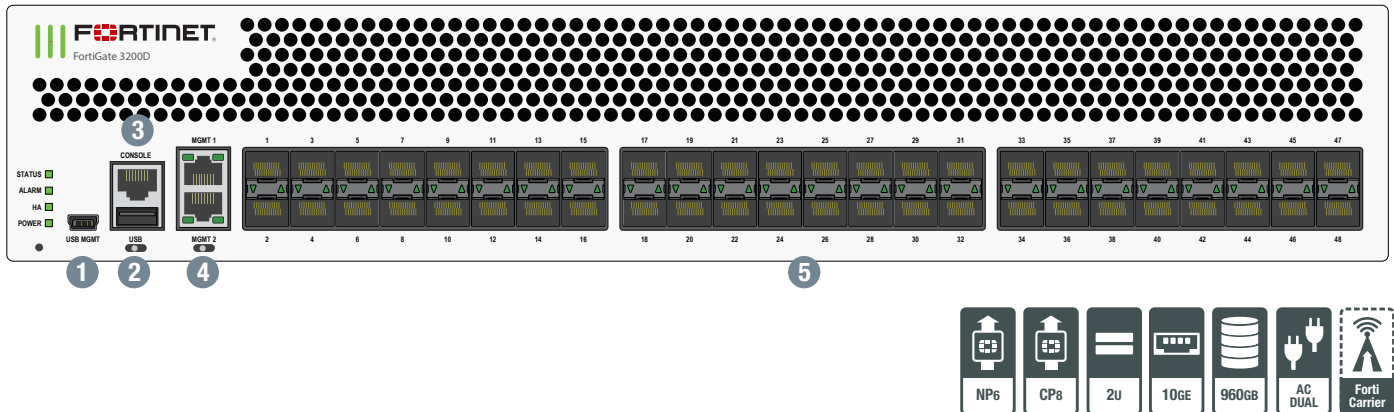


FortiGate 3200D deployment in data center (NGFW, IPS, and Intent-based Segmentation)



# Hardware

## FortiGate 3200D



### Interfaces

- |  |  |
|--|--|
| <ol style="list-style-type: none"> <li>1. USB Management Port</li> <li>2. USB Port</li> <li>3. Console Port</li> </ol> | <ol style="list-style-type: none"> <li>4. 2x GE RJ45 Management Ports</li> <li>5. 48x 10 GE SFP+ / GE SFP Slots</li> </ol> |
|--|--|

### 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

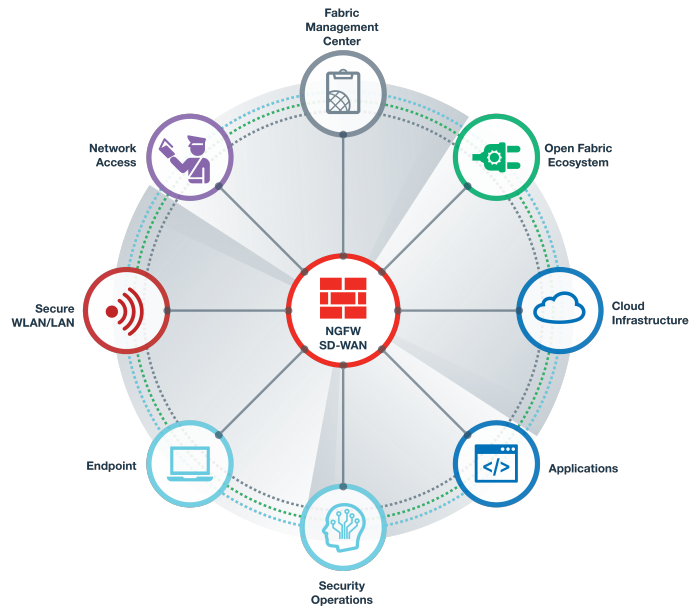
High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3200D provides the highest 10 GE port densities in the market, simplifying network designs without relying on additional devices to bridge desired connectivity.

## Fortinet Security Fabric

### Security Fabric

The Security Fabric 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

FORTIGATE 3200D	
<b>Interfaces and Modules</b>	
10 GE SFP+ / GE SFP Slots	48
GE RJ45 Management Ports	2
USB Ports (Client / Server)	1 / 1
Console Port	1
Internal Storage	2x 480 GB SSD
Included Transceivers	2x SFP+ (SR 10GE)
<b>System Performance — Enterprise Traffic Mix</b>	
IPS Throughput <sup>2</sup>	26 Gbps
NGFW Throughput <sup>2,4</sup>	24 Gbps
Threat Protection Throughput <sup>2,5</sup>	15 Gbps
<b>System Performance and Capacity</b>	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 50 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 50 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	75 Mpps
Concurrent Sessions (TCP)	50 Million
New Sessions/Second (TCP)	400,000
Firewall Policies	200,000
IPsec VPN Throughput (512 byte) <sup>1</sup>	50 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40,000
Client-to-Gateway IPsec VPN Tunnels	200,000
SSL-VPN Throughput	8 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	17 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	11,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	3.5 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>	50 Gbps
CAPWAP Throughput (1444 byte, UDP)	22 Gbps
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiSwitches Supported	256
Maximum Number of FortiAPs (Total / Tunnel Mode)	4,096 / 2,048
Maximum Number of FortiTokens	20,000
High Availability Configurations	Active / Active, Active / Passive, Clustering

FORTIGATE 3200D	
<b>Dimensions and Power</b>	
Height x Width x Length (inches)	3.5 x 17.4 x 21.9
Height x Width x Length (mm)	88 x 442 x 555
Weight	37.9 lbs (17.2 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2 RU
Power Input	100–240V AC, 50–60 Hz
Current Maximum	10A@100V, 5A@240V AC
Power Consumption (Average / Maximum)	350 W / 598 W
Heat Dissipation	2041 BTU/h
Redundant Power Supplies	Yes, Hot Swappable
<b>Operating Environment and Certifications</b>	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	10–90% non-condensing
Noise Level	50 dBA
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, RCM, 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 3200D	FG-3200D	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.
<b>Optional Accessories</b>		
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D, FG-3100D, FG-3200D, FG-3700D/-DC, FG-3700DX, FG-3810D and FG-3950B/-DC.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended 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.
AC Power Supply	SP-FG3600C-PS	AC power supply for FG-3000D, FG-3100D, FG-3200D, FG-3600C and FG-3240C.

## 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	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	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	•	•		
FortiGuard IoT Detection Service <sup>2</sup>	•	•		
FortiConverter Service	•	•		
IPAM Cloud <sup>2</sup>	•			
SD-WAN Orchestrator Entitlement <sup>2</sup>	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

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

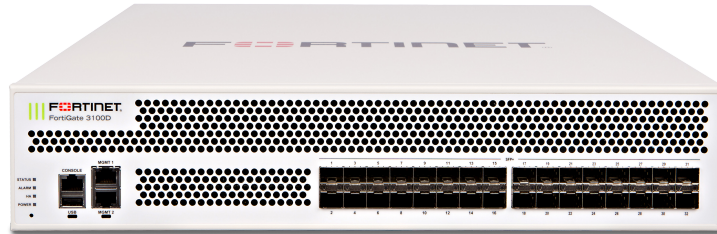




DATA SHEET

# FortiGate® 3100D

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3100D series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
<b>80 Gbps</b>	<b>22 Gbps</b>	<b>18 Gbps</b>	<b>13 Gbps</b>	Multiple 10 GE SFP+   Multiple GE SFP and GE RJ45

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 security effectiveness, 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



### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns



### 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



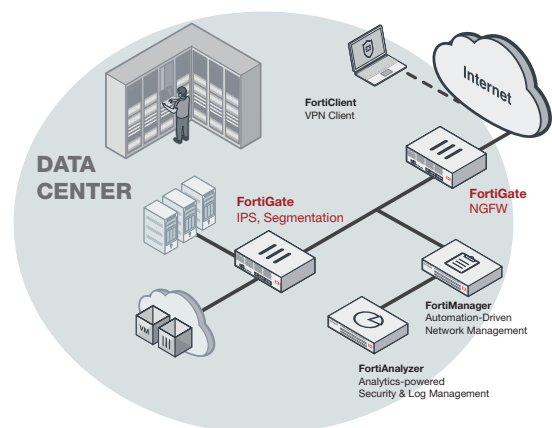
### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric



### Mobile Security for 4G, 5G, and IOT

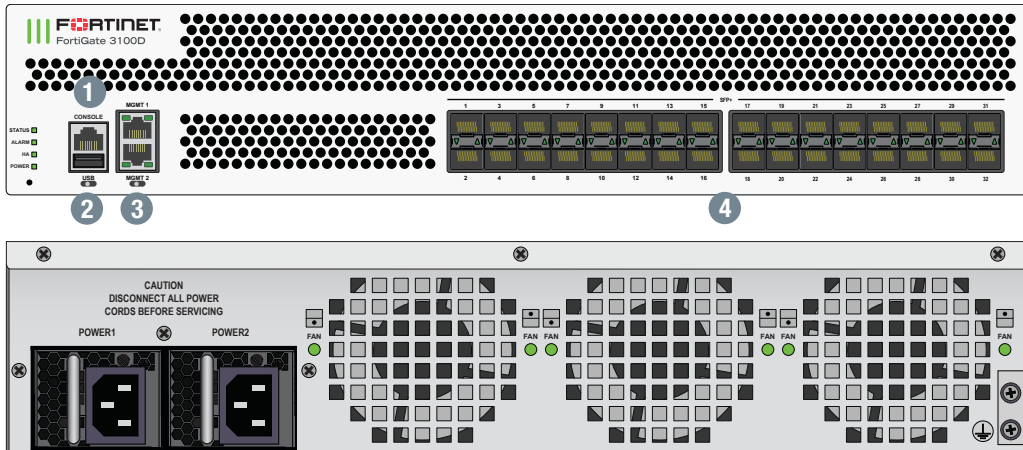
- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility



FortiGate 3100D deployment in data center (NGFW, IPS, and Intent-based Segmentation)

# Hardware

## FortiGate 3100D



### Interfaces

- |   |  |
|---|--|
| <ol style="list-style-type: none"> <li>1. Console Port</li> <li>2. USB Management Port</li> </ol> | <ol style="list-style-type: none"> <li>3. 2x GE RJ45 Management Ports</li> <li>4. 32x 10G SFP+/GE SFP Slots</li> </ol> |
|---|--|

### 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

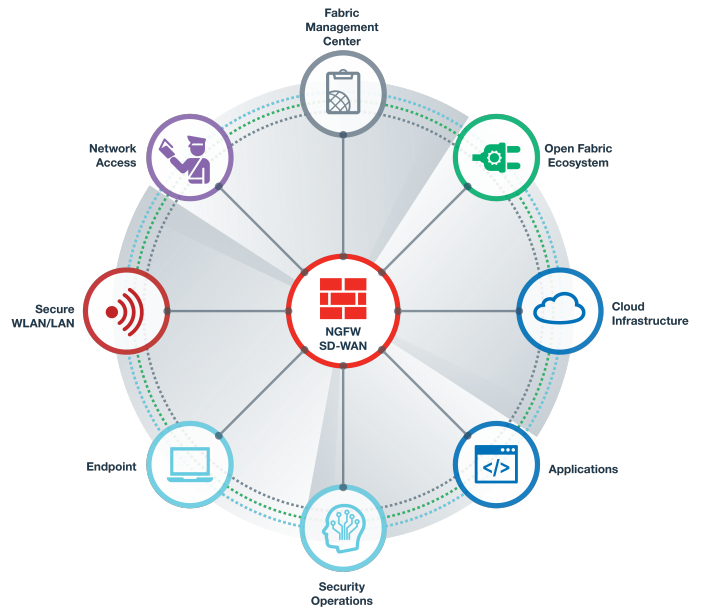
High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3100D provides the highest 10 GE port densities in the market, simplifying network designs without relying on additional devices to bridge desired connectivity.

# Fortinet Security Fabric

## Security Fabric

The Security Fabric 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

FORTIGATE 3100D	
<b>Interfaces and Modules</b>	
10 GE SFP+ / GE SFP Slots	32
GE RJ45 Management Ports	2
USB Ports (Client / Server)	1 / 1
Console Port	1
Internal Storage	1x 480 GB SSD
Included Transceivers	2x SFP+ (SR 10 GE)
<b>System Performance — Enterprise Traffic Mix</b>	
IPS Throughput <sup>2</sup>	22 Gbps
NGFW Throughput <sup>2,4</sup>	18 Gbps
Threat Protection Throughput <sup>2,5</sup>	13 Gbps
<b>System Performance and Capacity</b>	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 50 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 50 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	75 Mpps
Concurrent Sessions (TCP)	50 Million
New Sessions/Second (TCP)	400,000
Firewall Policies	200,000
IPsec VPN Throughput (512 byte) <sup>1</sup>	50 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40,000
Client-to-Gateway IPsec VPN Tunnels	200,000
SSL-VPN Throughput	8 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	16 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	10,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	3.5 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>	40 Gbps
CAPWAP Throughput (1444 byte, UDP)	22 Gbps
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiSwitches Supported	256
Maximum Number of FortiAPs (Total / Tunnel Mode)	4,096 / 2,048
Maximum Number of FortiTokens	20,000
High Availability Configurations	Active/Active, Active/Passive, Clustering

FORTIGATE 3100D	
<b>Dimensions and Power</b>	
Height x Width x Length (inches)	3.5 x 17.4 x 21.9
Height x Width x Length (mm)	88 x 442 x 555
Weight	37.69 lbs (17.1 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2 RU
Power Input	100–240V AC, 50–60 Hz
Current (Maximum)	10A@100VAC, 5A@240VAC
Power Consumption (Average / Maximum)	337 W / 520 W
Heat Dissipation	1775 BTU/h
Redundant Power Supplies	Yes, Hot Swappable
<b>Operating Environment and Certifications</b>	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	10–90% non-condensing
Noise Level	50 dBA
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, RCM, 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 3100D	FG-3100D	32x 10 GE SFP+ slots 10G ports (2 SFP+ SR-type transceivers included), SPU NP6 and CP8 hardware accelerated, 480 GB SSD internal storage, and dual AC power supplies.
<b>Optional Accessories</b>		
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D, FG-3100D, FG-3200D, FG-3700D/-DC, FG-3700DX, FG-3810D and FG-3950B/-DC.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended 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.
AC Power Supply	SP-FG3600C-PS	AC power supply for FG-3000D, FG-3100D, FG-3200D, FG-3600C and FG-3240C.

## 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	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	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	•	•		
FortiGuard IoT Detection Service <sup>2</sup>	•	•		
FortiConverter Service	•	•		
IPAM Cloud <sup>2</sup>	•			
SD-WAN Orchestrator Entitlement <sup>2</sup>	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

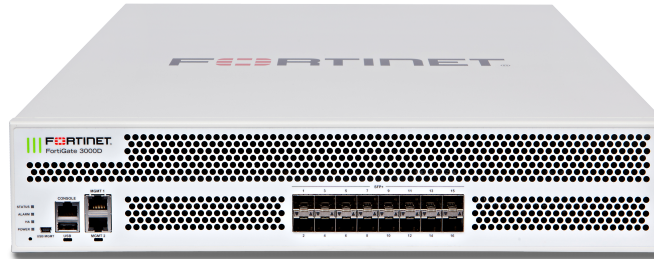
1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.4





# FortiGate® 3000D

Next Generation Firewall  
Segmentation  
Secure Web Gateway  
IPS  
Mobile Security



The FortiGate 3000D series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density, and high-throughput, ideal deployments are at the enterprise edge, hybrid data center core, and across internal segments. Leverage industry-leading IPS, SSL inspection, and advanced threat protection to optimize your network’s performance. 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

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- 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

Firewall	IPS	NGFW	Threat Protection	Interfaces
<b>80 Gbps</b>	<b>23 Gbps</b>	<b>22 Gbps</b>	<b>13 Gbps</b>	Multiple 10 GE SFP+   Multiple GE SFP and GE RJ45

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 security effectiveness, 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



### Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns



### 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



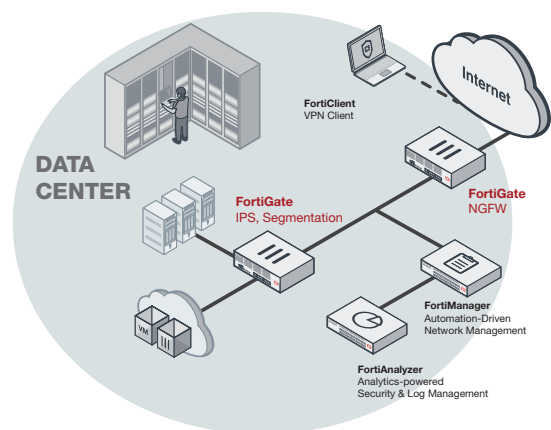
### IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric



### Mobile Security for 4G, 5G, and IOT

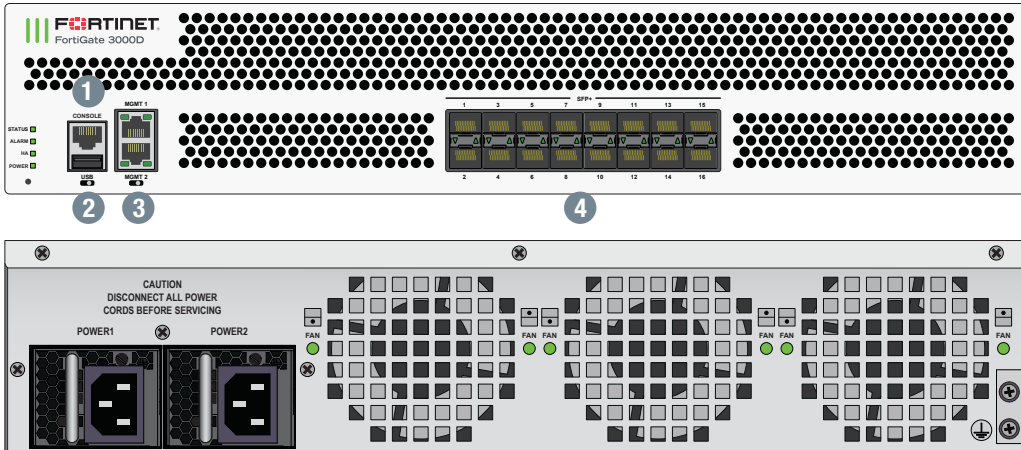
- SPU accelerated, high performance CGNAT and IPv4 and IPv6 traffic, for 4G SGI LAN and 5G N6 security
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G and 5G security for user and data plane traffic SCTP, GTP-U/C and SIP that provides protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility



FortiGate 3000D deployment in data center (NGFW, IPS, and Intent-based Segmentation)

## Hardware

### FortiGate 3000D



### Interfaces

1. Console Port
2. USB Management Port
3. 2x GE RJ45 Management Ports
4. 16x 10G SFP+/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

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

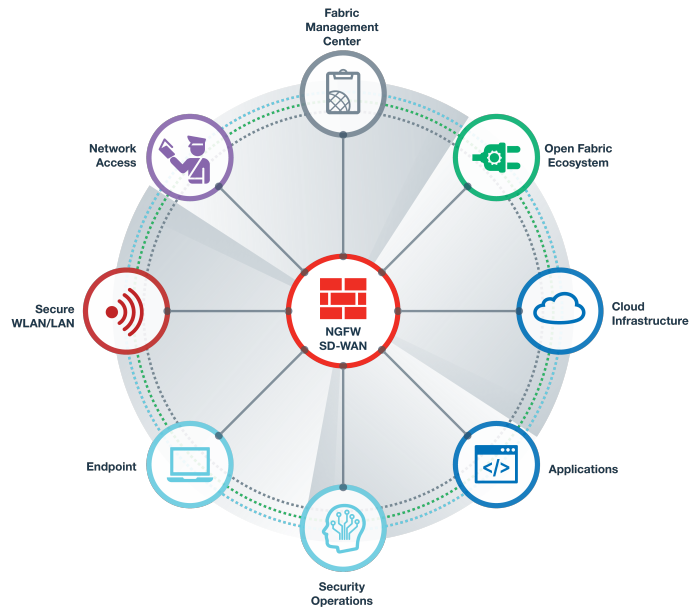
High-speed connectivity is essential for network security segmentation at the core of data networks. The FortiGate 3000D provides the highest 10 GE port densities in the market, simplifying network designs without relying on additional devices to bridge desired connectivity.

# Fortinet Security Fabric

## Security Fabric

The Security Fabric 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 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.



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](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

FORTIGATE 3000D	
<b>Interfaces and Modules</b>	
10 GE SFP+ / GE SFP Slots	16
GE RJ45 Management Ports	2
USB Ports (Server)	1
Console Port	1
Internal Storage	1x 480 GB SSD
Included Transceivers	2x SFP+ (SR 10GE)
<b>System Performance — Enterprise Traffic Mix</b>	
IPS Throughput <sup>2</sup>	23 Gbps
NGFW Throughput <sup>2,4</sup>	22 Gbps
Threat Protection Throughput <sup>2,5</sup>	13 Gbps
<b>System Performance and Capacity</b>	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 50 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 50 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	75 Mpps
Concurrent Sessions (TCP)	50 Million
New Sessions/Second (TCP)	400,000
Firewall Policies	200,000
IPsec VPN Throughput (512 byte) <sup>1</sup>	50 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40,000
Client-to-Gateway IPsec VPN Tunnels	200,000
SSL-VPN Throughput	8 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	15 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	8,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	3.5 Million
Application Control Throughput (HTTP 64K) <sup>2</sup>	40 Gbps
CAPWAP Throughput (1444 byte, UDP)	22 Gbps
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiSwitches Supported	256
Maximum Number of FortiAPs (Total / Tunnel Mode)	4,096 / 2,048
Maximum Number of FortiTokens	20,000
High Availability Configurations	Active / Active, Active / Passive, Clustering

FORTIGATE 3000D	
<b>Dimensions and Power</b>	
Height x Width x Length (inches)	3.5 x 17.4 x 21.9
Height x Width x Length (mm)	88 x 442 x 555
Weight	37.5 lbs (17.0 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2 RU
Power Input	100–240V AC, 50–60 Hz
Power Consumption (Average / Maximum)	310 W / 427 W
Current (Maximum)	10A@100VAC, 5A@240VAC
Heat Dissipation	1457 BTU/h
Redundant Power Supplies	Yes, Hot Swappable
<b>Operating Environment and Certifications</b>	
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Humidity	10–90% non-condensing
Noise Level	50 dBA
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, RCM, 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 3000D	FG-3000D	16x 10 GE SFP+ slots, 2x GE RJ45 Management, SPU NP6 and CP8 hardware accelerated, 480 GB SSD onboard storage, and dual AC power supplies.
<b>Optional Accessories</b>		
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1200D, FG-1500D, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D, FG-3100D, FG-3200D, FG-3700D/-DC, FG-3700DX, FG-3810D and FG-3950B/-DC.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended 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.
AC Power Supply	SP-FG3600C-PS	AC power supply for FG-3000D, FG-3100D, FG-3200D, FG-3600C and FG-3240C.

## 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	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	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	•	•		
FortiGuard IoT Detection Service <sup>2</sup>	•	•		
FortiConverter Service	•	•		
IPAM Cloud <sup>2</sup>	•			
SD-WAN Orchestrator Entitlement <sup>2</sup>	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

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

