The FortiGate 7121F 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 performance. Fortinet’s security-driven networking approach provides tight integration with the new security generation.

### Security
- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

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

### Certification
- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

### Networking
- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

### Management
- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet’s Security Fabric Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

### Security Fabric
- Enables Fortinet and Fabric-ready partners’ products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

<table>
<thead>
<tr>
<th>FIREWALL</th>
<th>IPS</th>
<th>NGFW</th>
<th>THREAT PROTECTION</th>
<th>NETWORK INTERFACES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.89 Tbps</td>
<td>675 Gbps</td>
<td>550 Gbps</td>
<td>520 Gbps</td>
<td>25 GE SFP28 / 10 GE SFP+ / GE SFP 100 GE QSFP28 / 40 GE QSFP+ 400 GE QSFP-DD</td>
</tr>
</tbody>
</table>
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.

**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.

**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.

**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.
- 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.

---

**Data Center Deployment**

- FortiGate NGFW
- IPS
- Segmentation
- FortiManager Single Pane-of-Glass Management
- FortiAnalyzer Analytics-powered Security & Log Management
- FortiClient VPN Client

---

(Data Center Deployment (IPS/NGFW, Intent-based Segmentation))
FORTINET SECURITY FABRIC

Security Fabric
The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad**: Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints, and users
- **Integrated**: Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest ecosystem
- **Automated**: Context aware, self-healing network and security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.

FortiOS™ Operating System
FortiOS, Fortinet’s leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric’s ability to deliver consistent security across hybrid deployment models of Hardware, Software, and Software As-a-Service with SASE and ZTNA, among others.

SERVICES

**FortiGuard™ Security Services**
FortiGuard Labs offer real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet’s solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world’s leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

**FortiCare™ Services**
Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.
HARDWARE

FortiGate 7121F

Content Processor
Fortinet’s ninth generation custom SPU CP9 content processor works outside of the direct flow of traffic and accelerates the inspection.

Network Processor
Fortinet’s new, breakthrough SPU NP7 network processor works inline with FortiOS functions delivering:
- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

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

Trusted Platform Module (TPM)
The FortiGate 7121F Series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.
## HARDWARE

### Fortinet Interface Module FIM-7921F and FIM-7941F

### Hardware Features

![Hardware Features Diagram]

### Specifications

<table>
<thead>
<tr>
<th>Hardware Interfaces</th>
<th>FIM-7921F</th>
<th>FIM-7941F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Accelerated 400 GE QSFP-DD / 100 GE QSFP28 / 40 GE QSFP+ Slots</td>
<td>2&lt;sup&gt;1&lt;/sup&gt;</td>
<td>2&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Management/HA Slots</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ SFP Management/HA Slots</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>USB Ports</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Console Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Onboard Storage</td>
<td>2 x 4 TB SSD</td>
<td>2 x 4 TB SSD</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>2 x 10 GE SFP+ SR</td>
<td>2 x 10 GE SFP+ SR</td>
</tr>
</tbody>
</table>

### Dimensions and Power

<table>
<thead>
<tr>
<th>Dimensions and Power</th>
<th>FIM-7921F</th>
<th>FIM-7941F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height x Width x Length (inches)</td>
<td>20.8 x 17.1 x 18.56</td>
<td>20.8 x 17.1 x 18.56</td>
</tr>
<tr>
<td>Weight</td>
<td>21.48 lbs (9.75 kg)</td>
<td>25.66 lbs (11.65 kg)</td>
</tr>
<tr>
<td>Power Consumption (Average / Maximum)</td>
<td>568 W / 597 W</td>
<td>598 W / 630 W</td>
</tr>
<tr>
<td>Current (Maximum)</td>
<td>50A</td>
<td>53A</td>
</tr>
<tr>
<td>Heat Dissipation (Average)</td>
<td>2036 BTU/h</td>
<td>2149 BTU/h</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>-32°F to 104°F (-35°C to 40°C)</td>
<td>-32°F to 104°F (-35°C to 40°C)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-31°F to 158°F (-35°C to 70°C)</td>
<td>-31°F to 158°F (-35°C to 70°C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>10-90% non-condensing</td>
<td>10-90% non-condensing</td>
</tr>
</tbody>
</table>

### Compliance

- FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB

---

1. Both ports 19 and 20 can be configured as split ports
2. Ports 1-8 can be configured as split ports
3. Ports 1-18 can be configured as split ports
Fortinet Processor Module FPM-7620F

Specifications

<table>
<thead>
<tr>
<th>Hardware Interfaces</th>
<th>FPM-7620F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots</td>
<td>2</td>
</tr>
<tr>
<td>Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots</td>
<td>8</td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td>1</td>
</tr>
<tr>
<td>Console Ports</td>
<td>1</td>
</tr>
</tbody>
</table>

System Performance and Capacity

- IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP packets): 396 / 395 / 263 Gbps
- IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP packets): 396 / 395 / 263 Gbps
- Firewall Latency (64 byte, UDP): 7.50 μs
- Firewall Throughput (Packet per Second): 39 286 Mpps
- Concurrent Sessions (TCP): 100 Million
- New Sessions/Sec (TCP): 300K
- Firewall Policies: 200 000 (system wide)
- IPSec VPN Throughput (512 byte): 63 Gbps
- Gateway-to-Gateway IPSec VPN Tunnels: 4000
- Client-to-Gateway IPSec VPN Tunnels: 26 000
- SSL-VPN Throughput: 13.7 Gbps
- Concurrent SSL-Users (Recommended Maximum): 3000
- IPS Throughput (Enterprise Mix): 67.5 Gbps
- SSL Inspection Throughput: 54 Gbps
- SSL Inspection CPS (IPS, avg. HTTPS): 48 000
- SSL Inspection Concurrent Session (IPS, avg. HTTPS): 10 Million
- Application Control Throughput: 150 Gbps
- NGFW Throughput: 55 Gbps
- Threat Protection Throughput: 52 Gbps
- CAPWAP Throughput: N.A.
- Virtual Domains (Default / Maximum): 10 / 1500
- Maximum Number of FortiTokens: 2000
- Maximum Number of FortiSwitches Supported: 300
- Maximum Number of FortiAPs (Total / Tunnel Mode): N.A.

High Availability Configurations

- Active-Passive, Active-Active

Hardware Features

- Dimensions and Power
  - Height x Width x Length (inches): 16.9 x 17.11 x 18.56
  - Height x Width x Length (mm): 43 x 435 x 471
  - Weight: 16.19 lb. (7.35 kg)
  - Power Consumption (Average / Maximum): 675 W / 716 W
  - Current (Maximum): 60A
  - Heat Dissipation (Average): 2442 BTU/h
  - Operating Temperature: 32–104°F (0–40°C)
  - Storage Temperature: -13–158°F (-25–70°C)
  - Humidity: 20–90% non-condensing

- Compliance
  - Certifications: FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB

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, URL filtering, and Malware Protection with sandboxing enabled.
7. Measured on single FPM only.
**SPECIFICATIONS**

<table>
<thead>
<tr>
<th>Interfaces and Modules</th>
<th>FG-7121F+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Accelerated 400 GE QSFP-DD / 100 GE QSFP28 / 40 GE QSFP+ Slots</td>
<td>4</td>
</tr>
<tr>
<td>Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots</td>
<td>56</td>
</tr>
<tr>
<td>Hardware Accelerated Management/HA Slots</td>
<td>4</td>
</tr>
<tr>
<td>Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots</td>
<td>80</td>
</tr>
<tr>
<td>System Management/HA Slots</td>
<td>4</td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td>14</td>
</tr>
<tr>
<td>GE SFP+ Management/HA Slots</td>
<td>4</td>
</tr>
<tr>
<td>GE SFP+ Management/HA Slots</td>
<td>4</td>
</tr>
<tr>
<td>GE RJ45 Management Ports</td>
<td>14</td>
</tr>
<tr>
<td>USB Ports</td>
<td>2</td>
</tr>
<tr>
<td>Console Ports</td>
<td>14</td>
</tr>
<tr>
<td>Onboard Storage</td>
<td>4 x 4 TB SSD</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>4 x 10 GE SFP+ SR</td>
</tr>
</tbody>
</table>

**System Performance - Enterprise Traffic Mix**

- **IPS Throughput**
  - 675 Gbps
- **NGFW Throughput**
  - 550 Gbps
- **Threat Protection Throughput**
  - 520 Gbps

**System Performance and Capacity**

- **IPv4 Firewall Throughput**
  - (1518 / 512 / 64 byte, UDP packets) 1.89 / 1.68 / 1.129 Tbps
- **IPv6 Firewall Throughput**
  - (1518 / 512 / 64 byte, UDP packets) 1.89 / 1.68 / 1.129 Tbps
- **Firewall Latency (64 byte, UDP)**
  - 7.50 μs
- **Firewall Throughput (Packet per Second)**
  - 1680 Mpps

- **Concurrent Sessions (TCP)**
  - 1 Billion
- **New Sessions/Sec (TCP)**
  - 9 Million
- **Firewall Policies**
  - 200 000
- **IPsec VPN Throughput**
  - 830 Gbps
- **Gateway-to-Gateway IPsec VPN Tunnels**
  - 40 000
- **SSL-VPN Throughput**
  - 30 000
- **Concurrent SSL-VPN Users**
  - (Recommended Maximum) 13.7 Gbps
- **IPES Throughput (Enterprise Mix)**
  - 675 Gbps
- **SSL Inspection Throughput**
  - 540 Gbps
- **SSL Inspection CPS (IPS, avg. HTTPS)**
  - 480 000
- **SSL Inspection Concurrent Session (IPS, avg. HTTPS)**
  - 100 Million
- **Application Control Throughput**
  - 1.5 Tbps
- **NGFW Throughput**
  - 550 Gbps
- **Threat Protection Throughput**
  - 520 Gbps
- **CAPWAP Throughput**
  - N.A.

**Operating Environment and Certifications**

- **Operating Temperature**
  - 32–104°F (0–40°C)
- **Storage Temperature**
  - 31–158°F (-35–70°C)
- **Humidity**
  - 20–90% non-condensing
- **Compliance Certifications**
  - FCC, ICES, CE, RCM, VCCI, BSMI, UL2200C, CB

**Dimensions and Power**

- **Height x Width x Length (inches)**
  - 28.63 x 17.33 x 26.8
- **Height x Width x Length (mm)**
  - 727.2 x 440 x 675.5
- **Weight (maximum)**
  - 447.36 lbs (203.1 kg)
- **Form Factor**
  - 16 RU
  - (supports EIA/non-EIA standards)
  - 10 Slots for FPM and 2 Slots for FIM (default configuration 2xFPM-7620F and 2xFIM-7921F)
- **Power Required**
  - 200 to 240 VAC (50/60 Hz)
- **Power Consumption**
  - (Maximum / Average) 9754 W / 8296 W
- **Heat Dissipation (Maximum)**
  - 33 261 BTU/h

*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, URL filtering, and Malware Protection with sandboxing enabled.
6. Power Consumption measured with VPN load balancing.
7. Measured on single FPM only.

*Performance specifications for FG-7121F are based on 10 FPM combination.*
# ORDER INFORMATION

## PRODUCT

<table>
<thead>
<tr>
<th>SKU</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FG-7121F*</td>
<td>16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7941F I/O Module, 2x Management Module and 8x hot swappable redundant PSU.</td>
</tr>
<tr>
<td>FG-7121F-2</td>
<td>16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7941F I/O Module, 2x Management Module and 8x hot swappable redundant PSU.</td>
</tr>
<tr>
<td>FG-7121F-DC</td>
<td>16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7941F I/O Module, 2x Management Module and 8x hot swappable redundant PSU 2KW DC-DC (without DC combiner).</td>
</tr>
</tbody>
</table>

## OPTIONAL / SPARE ITEMS

<table>
<thead>
<tr>
<th>SKU</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPM-7620F Module</td>
<td>Hot swappable processing module for 7xxxF series - FortiASIC NP7 and CP9 hardware accelerated. 2x QSFP28 and 8x SFP28 ports.</td>
</tr>
<tr>
<td>FIM-7921F Module**</td>
<td>Hot swappable i/o module for 7xxxF series - FortiASIC NP7 hardware accelerated. 2x GE RJ45 Management ports, 2x QSFP-DD ports, 20x QSFP28 ports, 2x SFP28 ports. 2x 4TB local log storage.</td>
</tr>
<tr>
<td>FIM-7941F Module**</td>
<td>Hot swappable i/o module for 7xxxF series - FortiASIC NP7 hardware accelerated. GE RJ45 Management ports, 2x QSFP-DD ports, 20x QSFP28 ports, 2x SFP28 ports. 2x 4TB local log storage.</td>
</tr>
<tr>
<td>Fan Module</td>
<td>FG-7121F-FAN FG-7121F Fan module.</td>
</tr>
<tr>
<td>Power Supply</td>
<td>FG-7121F-PS-2KAC FG-7121F power supply 2KW AC.</td>
</tr>
<tr>
<td>FortiGate-7121F-AC-Chassis</td>
<td>FG-7121F-CH FG-7121F chassis with 2x system management module, 8x PSU and 6x FAN module.</td>
</tr>
<tr>
<td>FortiGate-7121F-DC-Chassis</td>
<td>FG-7121F-DC-CH FG-7121F chassis with 2x system management module, 8x DC PSU and 6x FAN module, 8x DC input cable.</td>
</tr>
<tr>
<td>FG-7121F-DC-Combiner</td>
<td>FG-7121F-DC-COMBINER 1U rack mounted chassis containing 8x DC combiner module to support A+B input redundancy for FG-7121F-DC.</td>
</tr>
<tr>
<td>1GE SFP RJ45 transceiver module</td>
<td>FN-TRAN-GC 1GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>1GE SFP SX transceiver module</td>
<td>FN-TRAN-SX 1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>1GE SFP LX transceiver module</td>
<td>FN-TRAN-LX 1GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10GE copper SFP+ RJ45 Transceiver (30m range)</td>
<td>FN-TRAN-SFP+GC 10GE copper SFP+ RJ45 Fortinet Transceiver (30m range) for systems with SFP+ slots.</td>
</tr>
<tr>
<td>10Base-ER SFP+ transceivers</td>
<td>FN-TRAN-SFP+ER 10Base-ER SFP+ transceivers for FortiSwitch and FortiGate, 1550nm. Single Mode. 40km range for systems with SFP+ slots.</td>
</tr>
<tr>
<td>40GE QSFP+ transceivers, long range</td>
<td>FN-TRAN-QSFP+SR 40GE QSFP+ transceivers, long range for all systems with QSFP+ slots.</td>
</tr>
<tr>
<td>100GE QSFP28 transceivers</td>
<td>FN-TRAN-QSFP28-2SR 100GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.</td>
</tr>
<tr>
<td>100GE QSFP28 transceivers, long range</td>
<td>FN-TRAN-QSFP28-LR 100GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots.</td>
</tr>
<tr>
<td>100GE QSFP28 transceivers</td>
<td>FN-TRAN-QSFP28-CWDM4 100GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.</td>
</tr>
</tbody>
</table>

* The FG-7121F has Chassis-based pricing. Individual and bundled FortiGuard security services and FortiCare support subscription services such as Threat Protection Bundle, UTM Bundle, Enterprise Bundle, and FortiCare360 are on a chassis-based pricing. License such as VDOM and Endpoint Compliance are also included in the chassis-based pricing.
** Each FIM is packed individually and comes with 2x 10 GE SFP+ SR transceivers at no charge.

NOTE: All optional/spare components are for replacement usage and should not be used to assemble a bundle as only bundles have the necessary subscriptions.
## BUNDLES

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

<table>
<thead>
<tr>
<th>Bundles</th>
<th>Enterprise Protection</th>
<th>Unified Threat Protection</th>
<th>Advanced Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCare</td>
<td>24x7</td>
<td>24x7</td>
<td>24x7</td>
</tr>
<tr>
<td>FortiGuard App Control Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IPS Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Web and Video Filtering Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Antispam Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Security Rating Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard IoT Detection Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiGuard Industrial Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FortiConverter Service</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Available when running FortiOS 7.0

---

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet’s products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet D.U.A (https://www.fortinet.com/content/dam/fortinet/assets/legal/dual-use.pdf) and report any suspected violations of the D.U.A via the procedures outlined in the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domains/fortinet/media/201775/Whistleblower_Policy.pdf).