FortiGate 600F Series
FG-600F and FG-601F

AI/ML Security and Deep Visibility

The FortiGate 600F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 600F Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks.

Universal ZTNA automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast Threat Protection and SSL Inspection provides security at the edge you can see without impacting performance.

<table>
<thead>
<tr>
<th>IPS</th>
<th>NGFW</th>
<th>Threat Protection</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 Gbps</td>
<td>11.5 Gbps</td>
<td>10.5 Gbps</td>
<td>Multiple 25GE SFP28, 10GE SFP+, GE SFP Slots and GE RJ45</td>
</tr>
</tbody>
</table>
FortiOS Everywhere

FortiOS, Fortinet’s advanced operating system

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

• Interactive drill-down and topology viewers that display real-time status
• On-click remediation that provides accurate and quick protection against threats and abuses
• Unique threat score system correlates weighted threats with users to prioritize investigations

FortiConverter Migration Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

Intuitive easy to use view into the network and endpoint vulnerabilities
Visibility with FOS Application Signatures
FortiGuard Services

FortiGuard Al-Powered Security
FortiGuard’s rich suite of security services counter threats in real time using AI-powered, coordinated protection designed by FortiGuard Labs security threat researchers, engineers, and forensic specialists.

Web Security
Advanced cloud-delivered URL, DNS (Domain Name System), and Video Filtering providing complete protection for phishing and other web born attacks while meeting compliance.
Additionally, its dynamic inline CASB (Cloud Access Security Broker) service is focused on securing business SaaS data, while inline ZTNA traffic inspection and ZTNA posture check provide per-sessions access control to applications. It also integrates with the FortiClient Fabric Agent to extend protection to remote and mobile users.

Content Security
Advanced content security technologies enable the detection and prevention of known and unknown threats and file-based attack tactics in real-time. With capabilities like CPRL (Compact Pattern Recognition Language), AV, inline Sandbox, and lateral movement protection make it a complete solution to address ransomware, malware, and credential-based attacks.

Device Security
Advanced security technologies are optimized to monitor and protect IT, IIoT, and OT (Operational Technology) devices against vulnerability and device-based attack tactics. Its validated near-real-time IPS intelligence detects, and blocks known and zero-day threats, provides deep visibility and control into ICS/OT/SCADA protocols, and provides automated discovery, segmentation, and pattern identification-based policies.

Advanced Tools for SOC/NOC
Advanced NOC and SOC management tools attached to your NGFW provide simplified and faster time-to-activation.

SOC-as-a-Service
Includes tier-one hunting and automation, log location, 24×7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

Fabric Rating Security Best Practices
Includes supply chain virtual patching, up-to-date risk and vulnerability data to deliver quicker business decisions, and remediation for data breach situations.
Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today’s content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet’s custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage

Network Processor 7 NP7
Network Processors operate inline to deliver unmatched performance and scalability for critical network functions. Fortinet’s breakthrough SPU NP7 network processor works in line with FortiOS functions to deliver:

- Hyperscale firewall, accelerated session setup, and ultra-low latency
- Industry-leading performance for VPN, VXLAN termination, hardware logging, and elephant flows

Content Processor 9 CP9
Content Processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing

FortiCare Services
Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer’s operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.
Use Cases

Next Generation Firewall (NGFW)
- FortiGuard Labs’ suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet’s patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection

Secure SD-WAN
- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

Universal ZTNA
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access—every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

Segmentation
- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services detects and prevents known, zero-day, and unknown attacks
Hardware

FortiGate 600F Series

Interfaces

1. 2 x USB Ports
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 16 x GE RJ45 Slots
5. 8 x GE SFP Slots
6. 4 x 10GE/GE SFP+/SFP Slots
7. 4x 25GE/10GE SFP28/SFP+ Ultra Low Latency Slots

Hardware Features

Trusted Platform Module (TPM)

The FortiGate 600F 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.

Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.
## Specifications

### Interfaces and Modules

<table>
<thead>
<tr>
<th>FG-600F</th>
<th>FG-601F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Accelerated GE RJ45 Interfaces</td>
<td>16</td>
</tr>
<tr>
<td>Hardware Accelerated GE SFP Slots</td>
<td>8</td>
</tr>
<tr>
<td>Hardware Accelerated 10GE SFP+ / GE SFP Slots</td>
<td>4</td>
</tr>
<tr>
<td>Hardware Accelerated 25GE SFP28/10GE SFP+ Ultra Low Latency Slots</td>
<td>4</td>
</tr>
<tr>
<td>GE RJ45 MGMT/HA Ports</td>
<td>2</td>
</tr>
<tr>
<td>USB Ports</td>
<td>2</td>
</tr>
<tr>
<td>RJ45 Console Port</td>
<td>1</td>
</tr>
<tr>
<td>Onboard Storage</td>
<td>0</td>
</tr>
<tr>
<td>Included Transceivers</td>
<td>2x SFP (SX 1 GE)</td>
</tr>
</tbody>
</table>

### System Performance — Enterprise Traffic Mix

<table>
<thead>
<tr>
<th>FG-600F</th>
<th>FG-601F</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS Throughput</td>
<td>14 Gbps</td>
</tr>
<tr>
<td>NGFW Throughput</td>
<td>11.5 Gbps</td>
</tr>
<tr>
<td>Threat Protection Throughput</td>
<td>10.5 Gbps</td>
</tr>
</tbody>
</table>

### System Performance and Capacity

<table>
<thead>
<tr>
<th>FG-600F</th>
<th>FG-601F</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)</td>
<td>139 / 137.5 / 70 Gbps</td>
</tr>
<tr>
<td>IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)</td>
<td>139 / 137.5 / 70 Gbps</td>
</tr>
<tr>
<td>Firewall Latency (64 byte, UDP)</td>
<td>412 μs / 2.5 μs*</td>
</tr>
<tr>
<td>Firewall Throughput (Packet per Second)</td>
<td>105 Mpps</td>
</tr>
<tr>
<td>Concurrent Sessions (TCP)</td>
<td>8 Million</td>
</tr>
<tr>
<td>New Sessions/Second (TCP)</td>
<td>550 000</td>
</tr>
<tr>
<td>Firewall Policies</td>
<td>10 000</td>
</tr>
<tr>
<td>IPsec VPN Throughput (512 byte)</td>
<td>55 Gbps</td>
</tr>
<tr>
<td>Gateway-to-Gateway IPsec VPN Tunnels</td>
<td>2000</td>
</tr>
<tr>
<td>Client-to-Gateway IPsec VPN Tunnels</td>
<td>50 000</td>
</tr>
<tr>
<td>SSL-VPN Throughput</td>
<td>4.3 Gbps</td>
</tr>
<tr>
<td>Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)</td>
<td>10 000</td>
</tr>
<tr>
<td>SSL Inspection Throughput (IPS, avg. HTTPS)</td>
<td>9 Gbps</td>
</tr>
<tr>
<td>SSL Inspection CPS (IPS, avg. HTTPS)</td>
<td>7500</td>
</tr>
<tr>
<td>SSL Inspection Concurrent Session (IPS, avg. HTTPS)</td>
<td>840 000</td>
</tr>
<tr>
<td>Application Control Throughput (HTTP 64K)</td>
<td>32 Gbps</td>
</tr>
<tr>
<td>CAPWAP Throughput (HTTP 64K)</td>
<td>64.5 Gbps</td>
</tr>
<tr>
<td>Virtual Domains (Default / Maximum)</td>
<td>10 / 10</td>
</tr>
<tr>
<td>Maximum Number of FortiSwitches Supported</td>
<td>96</td>
</tr>
<tr>
<td>Maximum Number of FortiAPs (Total / Tunnel)</td>
<td>1024 / 512</td>
</tr>
<tr>
<td>Maximum Number of FortiTokens</td>
<td>5000</td>
</tr>
</tbody>
</table>

### High Availability Configurations

Active-Active, Active-Passive, Clustering

---

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.
# Ordering Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate 600F</td>
<td>FG-600F</td>
<td>4x 25G SFP28 slots, 4x 10GE SFP+ slots, 18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, SPU NP7 and CP9 hardware accelerated, dual AC power supplies.</td>
</tr>
<tr>
<td>FortiGate 601F</td>
<td>FG-601F</td>
<td>4x 25G SFP28 slots, 4x 10GE SFP+ slots, 18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, SPU NP7 and CP9 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies.</td>
</tr>
</tbody>
</table>

## Optional Accessories

<table>
<thead>
<tr>
<th>Description</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1GE SFP LX Transceiver Module</td>
<td>FN-TRAN-LX</td>
<td>1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>1GE SFP RJ45 Transceiver Module</td>
<td>FN-TRAN-GC</td>
<td>1 GE 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</td>
<td>1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10GE SFP+ RJ45 Transceiver Module</td>
<td>FN-TRAN-SFP+GC</td>
<td>10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.</td>
</tr>
<tr>
<td>10GE SFP+ Transceiver Module, Short Range</td>
<td>FN-TRAN-SFP+SR</td>
<td>10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10GE SFP+ Transceiver Module, Long Range</td>
<td>FN-TRAN-SFP+LR</td>
<td>10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10GE SFP+ Transceiver Module, Extended Range</td>
<td>FN-TRAN-SFP+ER</td>
<td>10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.</td>
</tr>
<tr>
<td>10GE SFP+ Transceiver Module, 30 km Long Range</td>
<td>FN-TRAN-SFP+BD27</td>
<td>10GE SFP+ transceiver module, 30KM long range single Bidi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately)</td>
</tr>
<tr>
<td>10GE SFP+ Transceiver Module, 30 km Long Range</td>
<td>FN-TRAN-SFP+BD33</td>
<td>10GE SFP+ transceiver module, 30KM long range single Bidi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately)</td>
</tr>
<tr>
<td>AC Power Supply</td>
<td>SP-FG400F-PS</td>
<td>AC power supply for FG-400/401F, FG-600/601F, power cable SP-FGPCOR-XX sold separately.</td>
</tr>
</tbody>
</table>

8
## Subscriptions

<table>
<thead>
<tr>
<th>Service Category</th>
<th>Service Offering</th>
<th>A-la-carte</th>
<th>Bundles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enterprise Protection</td>
</tr>
<tr>
<td>Security Services</td>
<td>FortiGuard IPS Service</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Web Security — URL and web content, Video and Secure DNS Filtering</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Anti-Spam</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard IoT Detection Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Industrial Security Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiCloud AI-based Inline Sandbox Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Anti-Spam</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Industrial Security Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiCloud AI-based Inline Sandbox Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiCloud AI-based Inline Sandbox Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Anti-Spam</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Industrial Security Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiCloud AI-based Inline Sandbox Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>NOC Services</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Cloud (SMB Logging + Cloud Management)</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Security Fabric Rating &amp; Compliance Monitoring Service</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiConverter Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>SOCs Services</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiAnalyzer Cloud</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiAnalyzer Cloud with SOCaaS</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Hardware and Software Support</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Hardware and Software Support</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Application Control</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiCloud ZTNA inline CASB Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Internet Service (SaaS) DB Updates</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>GeoIP DB Updates</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Device/OS Detection Signatures</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Trusted Certificate DB Updates</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>DDNS (v4/v6) Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Base Services</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiGuard Application Control</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>FortiCloud ZTNA inline CASB Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Internet Service (SaaS) DB Updates</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>GeoIP DB Updates</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Device/OS Detection Signatures</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>Trusted Certificate DB Updates</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>DDNS (v4/v6) Service</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td><strong>FortiGuard Bundles</strong></td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>

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.

### FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE’s) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

### Fortinet CSR Policy

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 illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

1. Available when running FortiOS 7.2