NALE SYSTEM INTEGRATOR
Experienced, Certified Engineers.
Trusted and Reliable Partner.

PT Nale System Integrator
JL. Panji Suroso, Puri Kartika Asri
Blok R 6-7, Blimbing, Malang - 65125
(0341) 435 97 23
PT Nale System Integrator | nale.co.id | www.nale.co.id

**PROPOSAL PENAWARAN**

Kepada Yth,
Bagian Pengadaan
CV. Primakom Mandiri Jaya
Jl. Lawy Barat, Ruko No. 08 Papahan
Kabupaten Karanganyar
Jawa Tengah
57722

| | |
|---|---|
| Proposal Number : | 85672 |
| Proposal Date : | Maret 9, 2026 |
| Payment Method : | Transfer Bank |
| Bank : | BSI [ 451 ] |
| No Rekening : | 7106842517 |
| Marketing Sales : | Ibu Nisa - 081235303729 |

Dengan Hormat,

Sehubungan dengan adanya kebutuhan project di instansi Bapak/Ibu, bersama ini kami tawarkan list produk di bawah ini:

| Produk | Kuantitas | Unit Price | Total |
|---|---|---|---|
| Fortinet FortiGate-101F<br>SKU: FG-101F | 1 | Rp68.873.074 | Rp68.873.074 |
| Fortinet Fortigate FG-101F License FC-10-F101F-950-02-12<br>SKU: FC-10-F101F-950-02-12 | 1 | Rp51.919.702 | Rp51.919.702 |
| Fortinet Fortigate FG-101F FG-101F-85-12 Fortinet Distributor RMA Replacement Service<br>SKU: FG-101F-85-12 | 1 | Rp8.264.768 | Rp8.264.768 |
| Fortinet FortiGate-61F<br>SKU: FG-61F | 1 | Rp19.034.786 | Rp19.034.786 |
| Fortinet FortiGate 61F License FC-10-0061F-950-02-12<br>SKU: FC-10-0061F-950-02-12 | 1 | Rp14.349.301 | Rp14.349.301 |
| Fortinet Fortigate FG-61F FG-61F-85-12 Fortinet Distributor RMA Replacement Service<br>SKU: FG-61F-85-12 | 1 | Rp2.284.175 | Rp2.284.175 |
| Mikrotik Router RB1100AHx4<br>SKU: RB1100AHx4 | 2 | Rp5.927.400 | Rp11.854.800 |

| | |
|---|---|
| **Subtotal** | Rp176.580.606 |
| **Grand Total** | **Rp176.580.606** |

***Harga Sudah Termasuk PPN**

**Catatan Pelanggan**

Site Project : RS. BHAYANGKARA SURABAYA

– Price valid 7 days

– Indent 8 – 12 weeks

– Term of Payment :

* Termin I = DP 50% saat PO/SPK diterima

* Termin II = 50% Sebelum barang akan dikirim

– Exclude Delivery Cost

– Exclude Installation

– FG-101F 22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10G SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy.

– FC-10-F101F-950-02-12 Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) 1 Year(s)

– FG-101F-85-12 NBD 8×5 Premium Hardware Replacement Services for Fortinet 1 Year(s)

*Approval by TAC Fortinet (RMA’s Ticket) Required

*NBD 8×5 SLA for Jakarta Area

– FG-61F 10 x GE RJ45 ports (including 2 x WAN Ports, 1 x DMZ Port, 7 x Internal Ports), 128GB SSD onboard storage. –

– FC-10-0061F-950-02-12 Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) 1 Year(s)

– FG-61F-85-12 NBD 8×5 Premium Hardware Replacement Services for Fortinet 1 Year(s)

*Approval by TAC Fortinet (RMA’s Ticket) Required

*NBD 8×5 SLA for Jakarta Area

Besar harapan, proposal penawaran yang kami berikan sesuai kebutuhan di instansi Bapak. Apabila terdapat hal-hal yang belum menjawab kebutuhan, mohon kiranya dapat menghubungi kami untuk membicarakannya lebih lanjut.

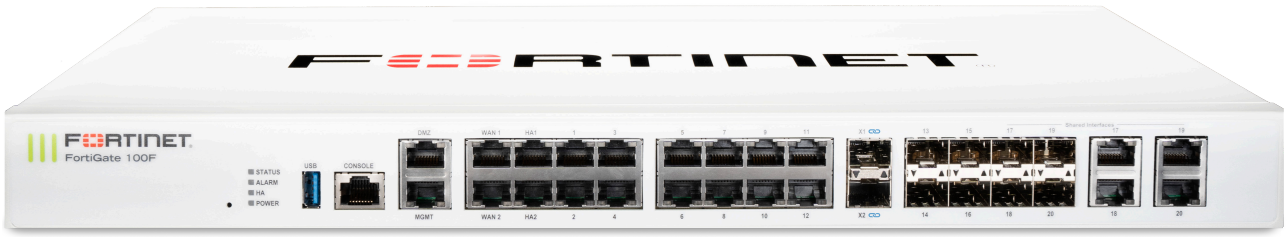
Terima kasih atas perhatiannya. Kami menunggu respon positif dari Bapak/Ibu.

Hormat Kami,

Marketing

**Branch Office Surabaya :** Bumi Mandiri Tower 2 Level 12, Jalan Panglima Sudirman
Kav.66 - 68, Genteng Kota Surabaya - Jawa Timur
0811-3503-797

# FortiGate 100F Series




## Highlights

**Gartner® Magic Quadrant™ Leaders** for both Network Firewalls and WAN Edge Infrastructure

**Secure Networking** with FortiOS for converged networking and security

**State-of-the-art unparalleled performance** with Fortinet's patented SPU and vSPU processors

**Enterprise security** with consolidated AI/ML-powered FortiGuard services

**Deep visibility** into applications, users, and devices beyond traditional firewall techniques

## Artificial Intelligence, Machine Learning Security with Deep Visibility

The FortiGate 100F series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) 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 100F 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. This security fabric seamlessly extends across your entire environment, including a Hybrid Mesh Firewall architecture, ensuring consistent policy enforcement and threat protection across all network segments.

Universal zero-trust network access (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.

| IPS | NGFW | Threat Protection | Interfaces |
|---|---|---|---|
| 2.6 Gbps | 1.6 Gbps | 1 Gbps | Multiple GE RJ45, GE SFP and 10 GE SFP+ slots |

## 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, malware, zero days, and sophisticated AI-powered 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 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 hybrid working 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 data center 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

## FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

### Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

### Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

### SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

### Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

### OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Available in

Appliance

Virtual

Hosted

Cloud

Container

# FortiOS Everywhere

**FortiOS, Fortinet's Real-Time Network Security Operating System**

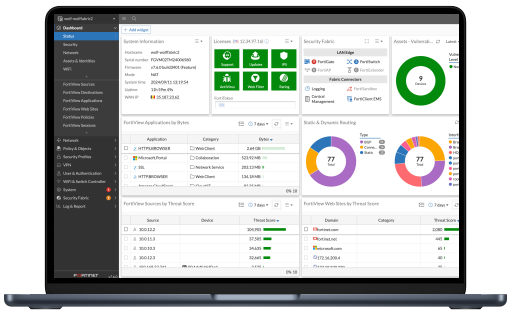
FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integrating generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

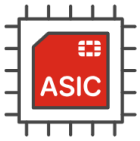
Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

*Intuitive easy to use view into the network and endpoint vulnerabilities*



*Comprehensive view of network performance, security, and system status*

## Fortinet ASICs: Unrivaled Security, Unprecedented Performance




### Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

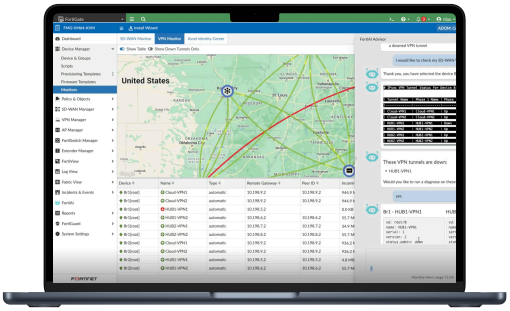
### Secure SD-WAN ASIC SP4

- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Delivers the industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for the best user experience on direct internet access
- Enables best-of-breed NGFW security and deep SSL inspection with high performance
- Extends security to the access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

## FortiManager

**Centralized management at scale for distributed enterprises**

FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.




*GenAI in FortiManager helps manage networks effortlessly—generates configuration and policy scripts, troubleshoots issues, and executes recommended actions.*

## FortiConverter Service

**Migration to FortiGate NGFW made easy**

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. 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.

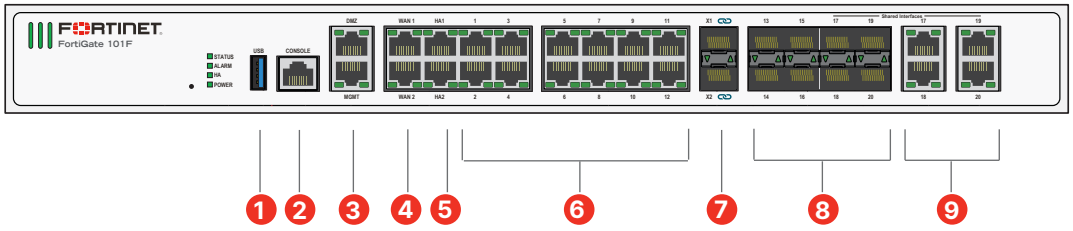
## FortiCare Services

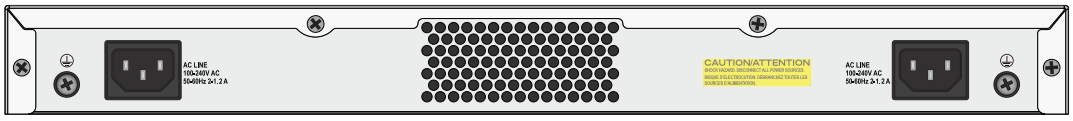
**Expertise at your service**

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

# Hardware

## FortiGate 100F Series




### Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/DMZ Ports
4. 2 x GE RJ45 WAN Ports
5. 2 x GE RJ45 HA Ports
6. 12 x GE RJ45 Ports
7. 2 × 10 GE SFP+ FortiLink Slots
8. 4 x GE SFP Slots
9. 4 x GE RJ45/ SFP Shared Media Pairs

### Hardware Features

SP4 | 1RU | DUAL AC | 480GB

### Dual power supply

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100F series offers dual built-in non-hot swappable power supplies.

### Access layer security

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

# Specifications

| | FORTIGATE 100F | FORTIGATE 101F |
|---|---|---|
| **Interfaces and Modules** | | |
| Hardware Accelerated GE RJ45 Ports | 12 | |
| Hardware Accelerated GE RJ45 Management/ HA/ DMZ Ports | 1 / 2 / 1 | |
| Hardware Accelerated GE SFP Slots | 4 | |
| Hardware Accelerated 10 GE SFP+ FortiLink Slots (default) | 2 | |
| GE RJ45 WAN Ports | 2 | |
| GE RJ45 or SFP Shared Ports * | 4 | |
| USB Port | 1 | |
| Console Port | 1 | |
| Onboard Storage | 0 | 1× 480 GB SSD |
| Trusted Platform Module (TPM) | — | |
| Bluetooth Low Energy (BLE) | — | |
| Signed Firmware Hardware Switch | — | |
| Included Transceivers | 0 | |
| **System Performance — Enterprise Traffic Mix** | | |
| IPS Throughput [2] | 2.6 Gbps | |
| NGFW Throughput [2, 4] | 1.6 Gbps | |
| Threat Protection Throughput [2, 5] | 1 Gbps | |
| **System Performance and Capacity** | | |
| IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) | 20 / 18 / 10 Gbps | |
| Firewall Latency (64 byte, UDP) | 4.97 µs | |
| Firewall Throughput (Packet per Second) | 15 Mpps | |
| Concurrent Sessions (TCP) | 1.5 Million | |
| New Sessions/Second (TCP) | 56 000 | |
| Firewall Policies | 10 000 | |
| IPsec VPN Throughput (512 byte) [1] | 11.5 Gbps | |
| Gateway-to-Gateway IPsec VPN Tunnels | 2000 | |
| Client-to-Gateway IPsec VPN Tunnels | 16 000 | |
| SSL-VPN Throughput | 1 Gbps | |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | 500 | |
| SSL Inspection Throughput (IPS, avg. HTTPS) [3] | 1 Gbps | |
| SSL Inspection CPS (IPS, avg. HTTPS) [3] | 1800 | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3] | 135 000 | |
| Application Control Throughput (HTTP 64K) [2] | 2.2 Gbps | |
| CAPWAP Throughput (HTTP 64K) | 15 Gbps | |
| Virtual Domains (Default / Maximum) | 10 / 10 | |
| Maximum Number of FortiSwitches Supported | 32 | |
| Maximum Number of FortiAPs (Total / Tunnel) | 128 / 64 | |
| Maximum Number of FortiTokens | 5000 | |
| High Availability Configurations | Active-Active, Active-Passive, Clustering | |

| | FORTIGATE 100F | FORTIGATE 101F |
|---|---|---|
| **Dimensions and Power** | | |
| Height x Width x Length (inches) | 1.73 × 17 × 10 | |
| Height x Width x Length (mm) | 44 × 432 × 254 | |
| Weight | 7.25 lbs (3.29 kg) | 7.56 lbs (3.43 kg) |
| Form Factor (supports EIA/non-EIA standards) | Rack Mount, 1 RU | |
| AC Power Supply | 100–240V AC, 50/60 Hz | |
| Power Consumption (Average / Maximum) | 26.5 W / 29.5 W | 35.3 W / 39.1 W |
| Current (Maximum) | 100V / 1A, 240V / 0.5A | |
| Heat Dissipation | 100.6 BTU/h | 121.13 BTU/h |
| Redundant Power Supplies | Yes (Default dual non-swappable AC PSU for 1+1 Redundancy) | |
| Power Supply Efficiency Rating | 80Plus Compliant | |
| **Operating Environment and Certifications** | | |
| Operating Temperature | 32°F to 104°F (0°C to 40°C) | |
| Storage Temperature | -31°F to 158°F (-35°C to 70°C) | |
| Humidity | 10% to 90% non-condensing | |
| Noise Level | 40.4 dBA | |
| Forced Airflow | Side to Back | |
| Operating Altitude | Up to 10 000 ft (3048 m) | |
| Compliance | FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI | |
| Certifications | USGv6/IPv6 | |

* Latency based on Ultra Low Latency (ULL ports)

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.

[6] Uses RSA-2048 certificate.

# Subscriptions

| Service Category | Service Offering | A-la-carte | Bundles: Enterprise Protection | Bundles: Unified Threat Protection | Bundles: Advanced Threat Protection | Bundles: SD-WAN |
|---|---|---|---|---|---|---|
| FortiGuard Security Services | IPS — IPS, Malicious/Botnet URLs | • | • | • | • | |
| | Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct[1], AI-based Heurestic AV, FortiGate Cloud Sandbox | • | • | • | • | |
| | URL, DNS and Video Filtering — URL, DNS and Video[1] Filtering, Malicious Certificate | • | • | • | | |
| | Anti-Spam | | • | • | | |
| | AI-based Inline Malware Prevention [1] | • | • | | | |
| | Data Loss Prevention (DLP) [2] | • | • | | | |
| | Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check | | • | | | • |
| | OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS [2] | • | | | | |
| | Application Control | | ----------included with FortiCare Subscription---------- | | | |
| | Inline CASB[1] | | ----------included with FortiCare Subscription---------- | | | |
| SD-WAN and SASE Services | SD-WAN SLA Database | | | | | • |
| | SD-WAN Underlay and Application Monitoring Service | | | | | • |
| | SD-WAN Overlay Orchestration Service | | | | | • |
| | SD-WAN Connector for FortiSASE Secure Private Access | | | | | • |
| | FortiSASE Starter Kit for n* Users[3] | | | | | • |
| | FortiGate Cloud One Year Cloud-based Log Retention | | | | | • |
| | FortiTelemetry Cloud | | | | | • |
| NOC and SOC Services | FortiConverter Service for One Time Configuration Conversion | • | • | | | |
| | Managed FortiGate Service—Available 24×7, with Fortinet NOC Experts Performing Device Setup, Network, And Policy Change Management | • | | | | |
| | FortiGate Cloud—Management, Analysis, and One Year Log Retention | • | | | | |
| | FortiManager Cloud | • | | | | |
| | FortiAnalyzer Cloud | • | | | | |
| | FortiGuard SOCaaS—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service | • | | | | |
| Hardware and Software Support | FortiCare Essentials | Desktop models only | | | | |
| | FortiCare Premium | • | • | • | • | • |
| | FortiCare Elite | • | | | | |
| Base Services | Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing | | ----------included with FortiCare Subscription---------- | | | |

1. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Only supported on G-series FortiGate models above 120G. See the FortiSASE Ordering Guide for supported models and their associated number of user licenses.

### FortiGuard AI-Powered Security Bundles for FortiGate

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

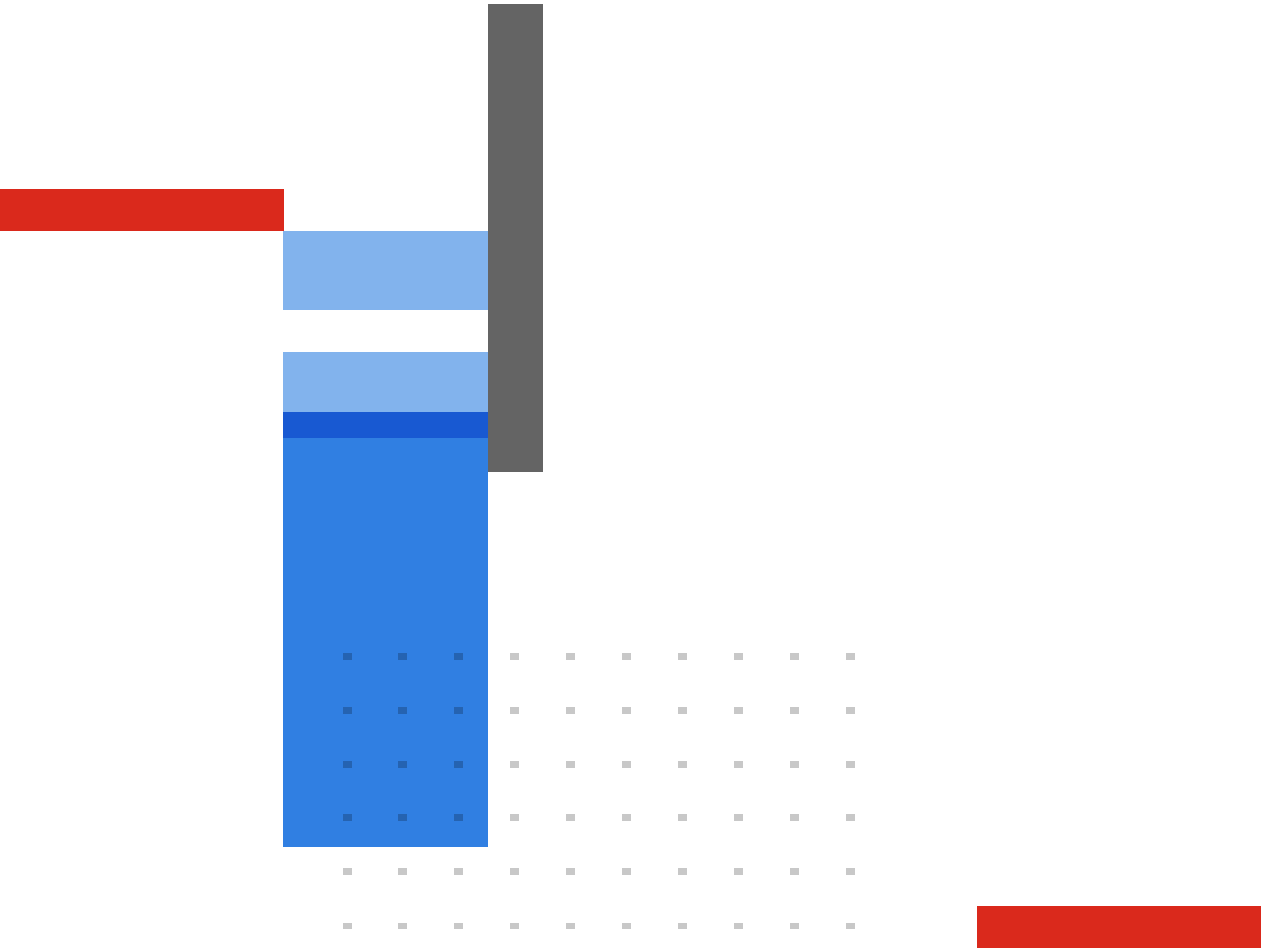
# Ordering Information

| Product | SKU | Description |
|---|---|---|
| **FortiGate 100F** | FG-100F | 22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2× 10 GE SFP+ FortiLinks, dual power supplies redundancy. |
| **FortiGate 100F** | FG-100F-HA | 22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2× 10G SFP+ FortiLinks, dual power supplies redundancy. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts. |
| **FortiGate 101F** | FG-101F | 22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2× 10 GE SFP+ FortiLinks, 480 GB onboard storage, dual power supplies redundancy. |
| **FortiGate 101F** | FG-101F-HA | 22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2× 10G SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts. |
| **Transceivers** | | |
| **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. |
| **1 GE SFP LX Transceiver Module** | FN-TRAN-LX | 1 GE SFP LX 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+ Transceiver Module, 80km Extreme Long Range** | FN-TRAN-SFP+ZR | 10 GE SFP+ transceiver module, 80km extreme long range, for systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Transceiver Module, 30 km Long Range** | FN-TRAN-SFP+BD27 | 10 GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately). |
| **10 GE SFP+ Transceiver Module, 30 km Long Range** | FN-TRAN-SFP+BD33 | 10 GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately). |
| **Cables** | | |
| **10 GE SFP+ Passive Direct Attach Cable 1m** | FN-CABLE-SFP+1 | 10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Passive Direct Attach Cable 3m** | FN-CABLE-SFP+3 | 10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots. |
| **10 GE SFP+ Passive Direct Attach Cable 5m** | FN-CABLE-SFP+5 | 10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots. |

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

## Fortinet Corporate Social Responsibility 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.



FORTINET

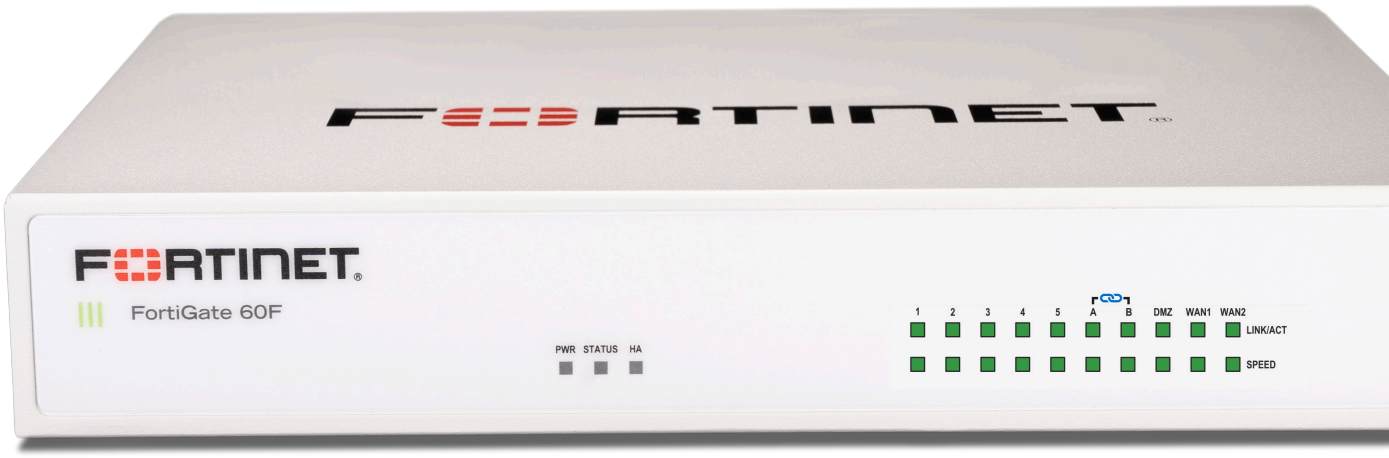
www.fortinet.com



February 3, 2026

FG-100F-DAT-R43-20260203

# FortiGate FortiWiFi 60F Series




## Highlights

**Gartner® Magic Quadrant™ Leaders** for both Network Firewalls and SD-WAN

**Unparalleled performance** enabled by Fortinet's patented ASIC and the FortiOS operating system

**Enterprise-grade protection** with FortiGuard AI-Powered Security Services

**Simplified operations** with centralized management for networking and security, automated workflows, deep analytics, and self-healing

**Inclusive SD-WAN** and wireless controller in every FortiGate appliance at no extra cost

**Rich portfolio** for any business budget and need

## Converged Next-Generation Firewall and SD-WAN

The FortiGate and FortiWiFi 60F series integrate firewalling, SD-WAN, and security in one appliance, making them perfect for building secure networks at distributed enterprise sites and transforming WAN architecture at any scale.

The 60F series runs on FortiOS, the industry's first converged networking and security operating system. This single OS approach enables businesses to gain benefits of operational efficiency and unified protection from the seamless integration of Fortinet Solutions within a Hybrid Mesh Firewall architecture.

As a cornerstone of the Fortinet Security Fabric platform, the FortiGate NGFW works seamlessly with FortiGuard AI-Powered Security Services to deliver coordinated, automated, end-to-end threat protection in real time.

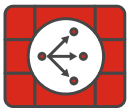
The 60F family is built on the patented SD-WAN-based ASIC, which delivers unmatched performance over traditional CPUs with lower cost and reduced power consumption. This application-specific design and embedded multi-core processor further accelerate the convergence of networking and security functions in the 60F family to optimize secure connections and deliver a robust user experience at branch locations.

| IPS | NGFW | Threat Protection | Interfaces |
|---|---|---|---|
| 1.4 Gbps | 1 Gbps | 700 Mbps | Multiple GE RJ45 \| Variants with internal storage \| WiFi variants |

# Use Cases

### Perimeter Protection

- Protect networks from malicious traffic, guard against file-based threats, block web-based attacks, and secure applications and data with natively integrated FortiGuard AI-Powered Security Services
- Inspect and control incoming and outgoing traffic based on defined security policies
- Perform real-time SSL inspection (including TLS 1.3) with full visibility into users, devices, and applications across the attack surface
- Accelerate performance, protection, and energy efficiency with Fortinet's patented SPU with converged security and networking technologies



### Secure SD-WAN

- FortiGate enables best-of-breed WAN edge with integrated SD-WAN, WAN optimization, security, and unified management from a single FortiOS operating system
- FortiGate, built on a patented SD-WAN-based ASIC, delivers faster application identification to avoid delays in accessing applications and accelerates overlay performance regardless of location
- Enhances hybrid working with a comprehensive SASE solution by integrating cloud-delivered SD-WAN with security service edge (SSE)
- Achieves operational efficiencies at any scale through automation, deep analytics, and self-healing

### Secure Branch

- The Fortinet Security Fabric platform enables FortiGate NGFWs to automatically discover and secure IoT devices for faster branch onboarding
- Fully integrated with FortiSwitch secure Ethernet switches and FortiAP access points, FortiGate easily extends security to WAN, LAN, and WLAN at branch offices for unified protection and reliable connectivity
- FortiGate and Fortinet products work seamlessly with FortiManager to centralize visibility and simplify management across locations for IT teams
- FortiGate HA support ensures continuous network protection and minimizes downtime in the event of hardware failures or network disruptions

## FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

### Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

### Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

### SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

### Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

### OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Available in

Appliance

Virtual

Hosted

Cloud

Container

# FortiOS Everywhere

**FortiOS, Fortinet's Real-Time Network Security Operating System**

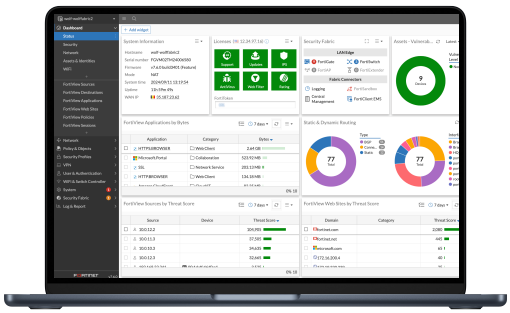
FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integrating generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

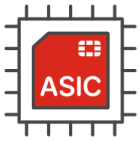
Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

*Intuitive easy to use view into the network and endpoint vulnerabilities*



*Comprehensive view of network performance, security, and system status*

## Fortinet ASICs: Unrivaled Security, Unprecedented Performance




### Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

### Secure SD-WAN ASIC SP4

- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Delivers the industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for the best user experience on direct internet access
- Enables best-of-breed NGFW security and deep SSL inspection with high performance
- Extends security to the access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

# Unified Management for Optimal Security and Efficiency

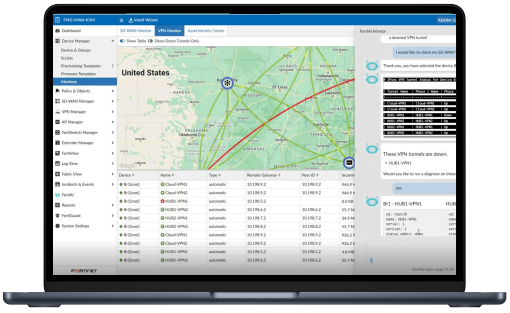
Whether you are a small business or a large enterprise, Fortinet provides centralized control, visibility, and automation for your security infrastructure.

### FortiManager: Centralized management at scale for distributed enterprises

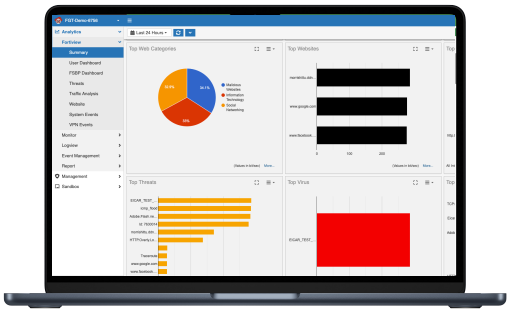
FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.

### FortiGate Cloud: Simplified management for small and mid-size businesses

FortiGate Cloud is a SaaS service offering simplified management, security analytics, and reporting for Fortinet FortiGate NGFWs to help you more efficiently manage your devices and reduce cyber risk. It simplifies the initial deployment, setup, and ongoing management of FortiGates and downstream connected devices such as FortiAP, FortiSwitch, and FortiExtender, with zero-touch provisioning. It provides real-time and historical visibility into traffic analytics and security threats to reduce risks and improve security posture. View various threats, web traffic, and system events stored in the cloud for up to a year, with predefined reports to meet compliance and deliver actionable insights.



*GenAI in FortiManager helps manage networks effortlessly—generate configuration and policy scripts, troubleshoot issues, and execute recommended actions.*



*FortiGate Cloud provides intuitive management and analytics solution with end-to-end visibility, logging and reporting for SMB.*

# FortiConverter Service

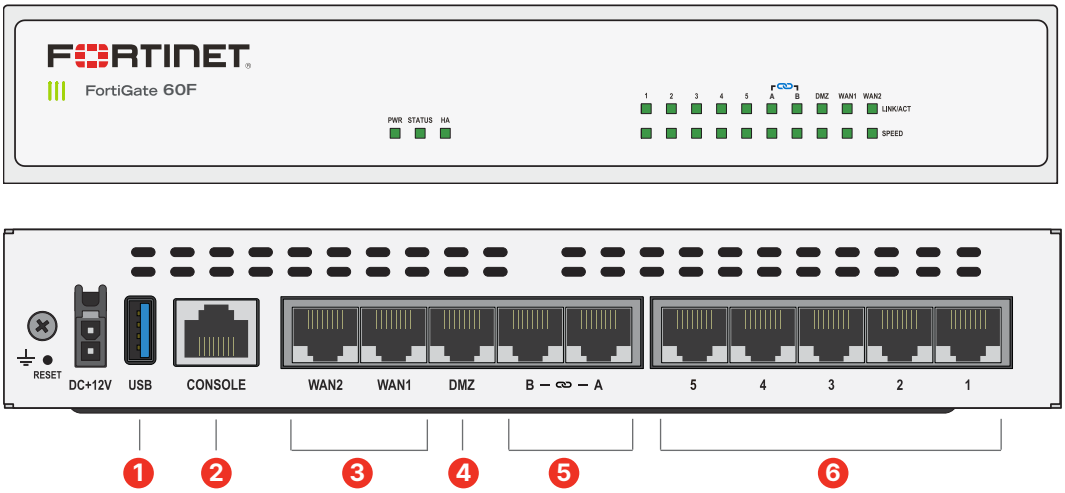
### Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. 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.

# Hardware

## FortiGate FortiWiFi 60F/61F

SoC4 DESKTOP a/b/g/n/ac-W2 128GB




### Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 WAN Ports
4. 1 x GE RJ45 DMZ Port
5. 2 x GE RJ45 FortiLink Ports
6. 5 x GE RJ45 Internal Ports

### Hardware Features

#### Access layer security

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

#### Compact and reliable form factor

Designed for small environments, the FortiGate can be on a desktop or wall-mounted. It is small, lightweight, yet highly reliable with superior meantime between failures, minimizing the chance of network disruption.

# Specifications

| | FORTIGATE 60F | FORTIGATE 61F | FORTIWIFI 60F | FORTIWIFI 61F |
|---|---|---|---|---|
| **Hardware Specifications** | | | | |
| GE RJ45 WAN / DMZ Ports | 2 / 1 | 2 / 1 | 2 / 1 | 2 / 1 |
| GE RJ45 Internal Ports | 5 | 5 | 5 | 5 |
| GE RJ45 FortiLink Ports (Default) | 2 | 2 | 2 | 2 |
| Wireless Interface | — | — | Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2 | Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2 |
| USB Ports | 1 | 1 | 1 | 1 |
| Console (RJ45) | 1 | 1 | 1 | 1 |
| Internal Storage | — | 1 × 128 GB SSD | — | 1 × 128 GB SSD |
| Trusted Platform Module (TPM) | — | — | — | — |
| Bluetooth Low Energy (BLE) | — | — | — | — |
| Signed Firmware Hardware Switch | — | — | — | — |
| **System Performance — Enterprise Traffic Mix** | | | | |
| IPS Throughput [2] | 1.4 Gbps | | | |
| NGFW Throughput [2, 4] | 1 Gbps | | | |
| Threat Protection Throughput [2, 5] | 700 Mbps | | | |
| **System Performance** | | | | |
| Firewall Throughput (1518 / 512 / 64 byte UDP packets) | 10/10/6 Gbps | | | |
| Firewall Latency (64 byte UDP packets) | 3.3 µs | | | |
| Firewall Throughput (Packets Per Second) | 9 Mpps | | | |
| Concurrent Sessions (TCP) | 700 000 | | | |
| New Sessions/Second (TCP) | 35 000 | | | |
| Firewall Policies | 2000 | | | |
| IPsec VPN Throughput (512 byte) [1] | 6.5 Gbps | | | |
| Gateway-to-Gateway IPsec VPN Tunnels | 200 | | | |
| Client-to-Gateway IPsec VPN Tunnels | 500 | | | |
| SSL-VPN Throughput[6] | 900 Mbps | | | |
| Concurrent SSL-VPN Users[6] (Recommended Maximum, Tunnel Mode) | 200 | | | |
| SSL Inspection Throughput (IPS, avg. HTTPS) [3] | 630 Mbps | | | |
| SSL Inspection CPS (IPS, avg. HTTPS) [3] | 400 | | | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3] | 55 000 | | | |
| Application Control Throughput (HTTP 64K) [2] | 1.8 Gbps | | | |
| CAPWAP Throughput (HTTP 64K) | 8 Gbps | | | |
| Virtual Domains (Default / Maximum) | 10 / 10 | | | |
| Maximum Number of FortiSwitches Supported | 24 | | | |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | 64 / 32 | | | |
| Maximum Number of FortiTokens | 500 | | | |
| High Availability Configurations | Active-Active, Active-Passive, Clustering | | | |
| **Dimensions** | | | | |
| Height x Width x Length (inches) | 1.5 × 8.5 × 6.3 | | | |
| Height x Width x Length (mm) | 38.5 × 216 × 160 mm | | | |
| Weight | 2.23 lbs (1.01 kg) | | | |
| Form Factor | Desktop | | | |

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.

[6] SSL VPN not supported on FortiOS 7.6.0 and above.

# Specifications

| | FORTIGATE 60F | FORTIGATE 61F | FORTIWIFI 60F | FORTIWIFI 61F |
|---|---|---|---|---|
| **Operating Environment and Certifications** | | | | |
| **Power Rating** | 12Vdc, 3A | | | |
| **Power Required** | Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz | | | |
| **Maximum Current** | 100Vac/1.0A, 240Vac/0.6A | | | |
| **Power Consumption (Average / Maximum)** | 10.17 W / 12.43 W | 17.2 W / 18.7 W | 17.2 W / 18.7 W | 17.5 W / 19.0 W |
| **Heat Dissipation** | 42.4 BTU/hr | 42.4 BTU/hr | 63.8 BTU/hr | 64.8 BTU/hr |
| **Operating Temperature** | 32°F to 104°F (0°C to 40°C) | | | |
| **Storage Temperature** | -31°F to 158°F (-35°C to 70°C) | | | |
| **Humidity** | 10% to 90% non-condensing | | | |
| **Noise Level** | Fanless 0 dBA | | | |
| **Operating Altitude** | Up to 7400 ft (2250 m) | | | |
| **Compliance** | FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB | | | |
| **Certifications** | USGv6/IPv6 | | | |
| **Radio Specifications** | | | | |
| **Multiple User (MU) MIMO** | — | — | 3×3 | |
| **Maximum Wi-Fi Speeds** | — | — | 1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz | |
| **Maximum Tx Power** | — | — | 20 dBm | |
| **Antenna Gain** | — | — | 3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz | |

# Subscriptions

| Service Category | Service Offering | A-la-carte | Bundles: Enterprise Protection | Bundles: Unified Threat Protection | Bundles: Advanced Threat Protection | Bundles: SD-WAN |
|---|---|---|---|---|---|---|
| FortiGuard Security Services | IPS — IPS, Malicious/Botnet URLs | • | • | • | • | |
| | Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct[1], AI-based Heurestic AV, FortiGate Cloud Sandbox | • | • | • | • | |
| | URL, DNS and Video Filtering — URL, DNS and Video[1] Filtering, Malicious Certificate | • | • | • | | |
| | Anti-Spam | | • | • | | |
| | AI-based Inline Malware Prevention [1] | • | • | | | |
| | Data Loss Prevention (DLP) [2] | • | • | | | |
| | Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check | | • | | | • |
| | OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS [2] | • | | | | |
| | Application Control | | ----------included with FortiCare Subscription---------- | | | |
| | Inline CASB[1] | | ----------included with FortiCare Subscription---------- | | | |
| SD-WAN and SASE Services | SD-WAN SLA Database | | | | | • |
| | SD-WAN Underlay and Application Monitoring Service | | | | | • |
| | SD-WAN Overlay Orchestration Service | | | | | • |
| | SD-WAN Connector for FortiSASE Secure Private Access | | | | | • |
| | FortiSASE Starter Kit for n* Users[3] | | | | | • |
| | FortiGate Cloud One Year Cloud-based Log Retention | | | | | • |
| | FortiTelemetry Cloud | | | | | • |
| NOC and SOC Services | FortiConverter Service for One Time Configuration Conversion | • | • | | | |
| | Managed FortiGate Service—Available 24×7, with Fortinet NOC Experts Performing Device Setup, Network, And Policy Change Management | • | | | | |
| | FortiGate Cloud—Management, Analysis, and One Year Log Retention | • | | | | |
| | FortiManager Cloud | • | | | | |
| | FortiAnalyzer Cloud | • | | | | |
| | FortiGuard SOCaaS—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service | • | | | | |
| Hardware and Software Support | FortiCare Essentials | Desktop models only | | | | |
| | FortiCare Premium | • | • | • | • | • |
| | FortiCare Elite | • | | | | |
| Base Services | Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing | | ----------included with FortiCare Subscription---------- | | | |

1. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Only supported on G-series FortiGate models above 120G. See the FortiSASE Ordering Guide for supported models and their associated number of user licenses.

## FortiGuard AI-Powered Security Bundles for FortiGate

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

## FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

# Ordering Information

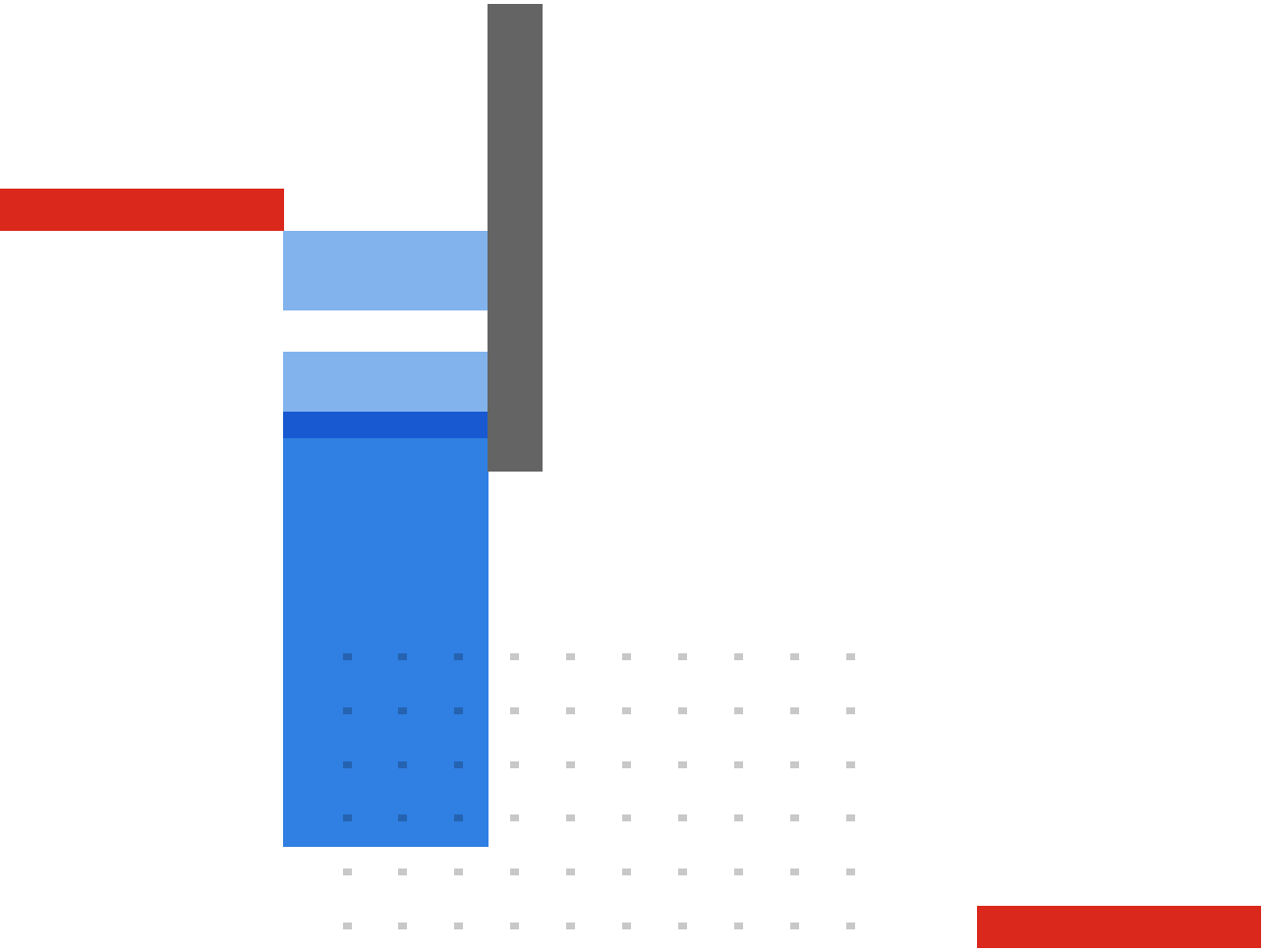
| Product | SKU | Description |
|---|---|---|
| **FortiGate 60F** | FG-60F | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port). |
| **FortiGate 60F** | FG-60F-HA | 10 x GE RJ45 ports (including 2 x WAN Ports, 1 x DMZ Port, 7 x Internal Ports), 128GB SSD onboard storage. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts (limited to Enterprise, UTP, and ATP bundles only). |
| **FortiGate 61F** | FG-61F | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage. |
| **FortiGate 61F** | FG-61F-HA | 10 x GE RJ45 ports (including 2 x WAN Ports, 1 x DMZ Port, 7 x Internal Ports), 128GB SSD onboard storage. FG-XX-HA SKUs must be bought in pairs and entitle HA pair to leverage single service contracts. |
| **FortiWiFi 60F** | FWF-60F-[RC] | 10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2). |
| **FortiWiFi 61F** | FWF-61F-[RC] | 10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2), 128GB SSD onboard storage. |
| **Optional Accessories** | | |
| **Rack Mount Tray** | SP-RACKTRAY-02 | Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com. |
| **AC Power Adaptor** | SP-FG60E-PDC-5 | Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 70/71F, 70/71G, 80E/81E, 80/81F, 90/91G and FDC-100G.<br>Power cable SP-FG60CPCOR-XX sold separately. |
| **Wall Mount Kit** | SP-FG60F-MOUNT-20 | Pack of 20 wall mount kits for FG/FWF-60F and FG/FWF-80F series. |

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

## Fortinet Corporate Social Responsibility 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.



FORTINET

www.fortinet.com



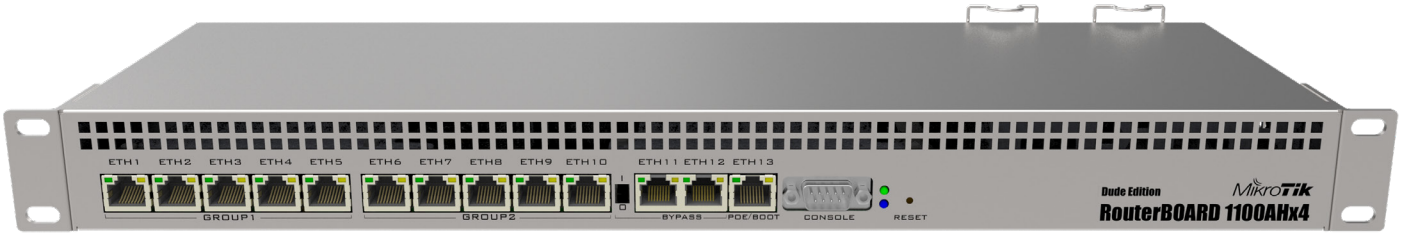
February 3, 2026

FGFWF-60F-DAT-R48-20260203

# RB1100AHx4 series

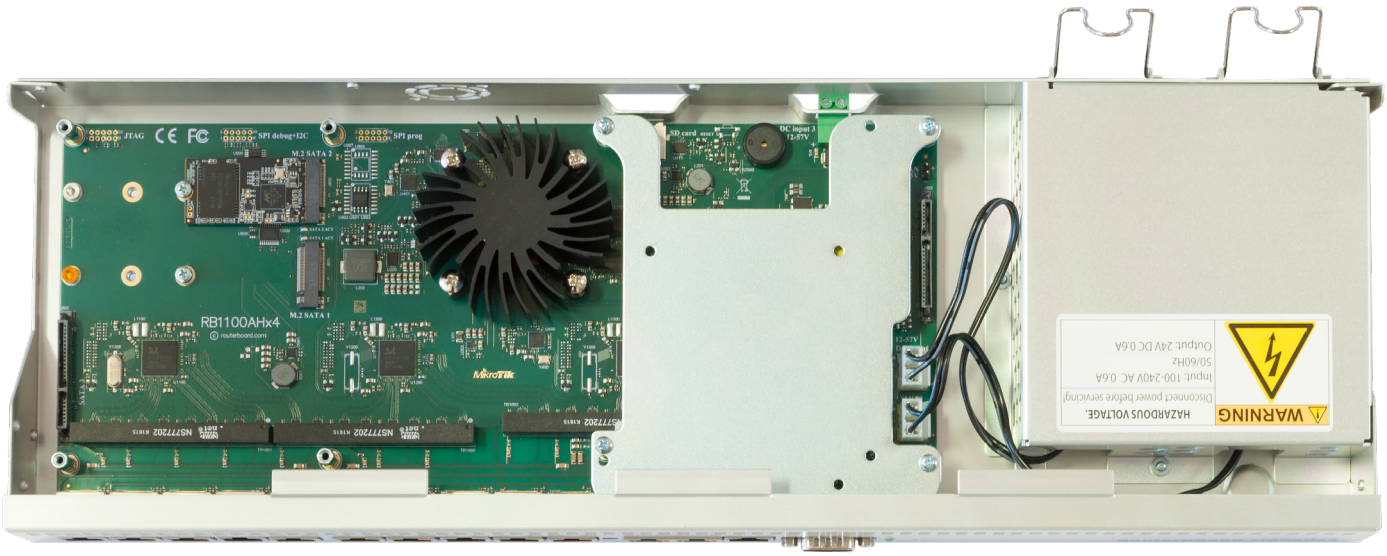
The new RB1100AHx4 series of devices uses a new quad core Cortex A15 chip from Annapurna labs, an Amazon company, The chip is clocked at 1.4 GHz, for a maximum throughput of up to 7.5 Gbit.

Two models are available, with the RB1100AHx4 Dude edition featuring several high speed storage connectors (two SATA and two M.2) for using a Dude database, proxy cache or any other storage intensive feature. The Dude edition includes a 60 GB M.2 drive already installed.




The devices support IPsec hardware acceleration and are faster at it than any previous RouterBOARD device.

The RB1100AHx4 feature two IEC failover power connectors, support 802.3at PoE input and also have a DC telecom power connector for -48 V DC powering.



# Specifications

| | | |
|---|---|---|
| Product code | RB1100AHx4 Dude edition | RB1100AHx4 |
| CPU | AL21400, 4 cores, 1.4G Hz | AL21400, 4 cores, 1.4 GHz |
| Size of RAM | 1 GB | 1 GB |
| Storage type | NAND | NAND |
| Storage size | 128 MB + 60 GB m.2 SATA 3 drive included | 128 MB |
| 10/100/1000 Ethernet ports | 13 | 13 |
| Ethernet bypass | Ethernet 11/12 | Ethernet 11/12 |
| Power jack | 2x IEC. 100 V - 240 V | 2x IEC. 100 V - 240 V |
| DC telecom power | 20 V - 57 V (-48 V supported) | 20 V - 57 V (-48 V supported) |
| PoE input | Passive, 802.3at. 20 V - 57 V | Passive, 802.3at. 20 V - 57 V |
| Redundant power supply | Yes | Yes |
| Voltage monitor | Yes | Yes |
| PCB temperature monitor | Yes | Yes |
| Current monitor | Yes | Yes |
| Dimensions | 443 x 148 x 44 mm | 443 x 148 x 44 mm |
| Operating temperature | -40°C .. +70°C tested | -40°C .. +70°C tested |
| Operating system | RouterOS, level 6 license | RouterOS, level 6 license |
| Max Power consumption | 25 W | 20 W |
| microSD | 1 | 1 |
| SATA | 2x 2.5 inch SATA 3 | - |
| M.2 slots | 2x SATA 3 compatible<br>(supports 2242, 2260 and 2280 sizes, M-key) | - |
| Serial port | RS232 | RS232 |
| Beeper | Yes | Yes |



SATA cables


K-10 R2 screw kit


Rack ears


2x IEC cord


M.2 SSD 60 GB