



Office of the Chief Executive Officer Shri Mata Vaishno Devi Shrine Board,

Central Office, Jammu Road, Katra (J&K – UT) - 182301

No.CO/Pur/Electronics/657/21

Dated: 06.04.2026

Request for Inviting Quotations (RFIQ)

For and on behalf of Shri Mata Vaishno Devi Shrine Board; through Chief Executive Officer (herein after referred as SMVDSB), offers are hereby invited from reputed manufacturers / distributors / dealers / suppliers only for furnishing the rates for SITC of Network Setup as per specifications, Brand and Make mentioned in Annexure-“A”:

Terms and conditions:

1. **Document to be submitted:**

- i) GST Certificate.
- ii) Earnest Money Deposit as per Clause no: 16 (i) for the RFIQ.
- iii) Certification w.r.t. authorized manufacturer / distributor / dealer, (if any).
- iv) Data Sheets in respect of Network firewall, 24 & 16 Managed port PoE switch with SFP, PoE wifi Access Points and OFC Transceivers along with the offer. Failure to submit the same may lead to rejection of the bid at any stage, even after bid opening.
- v) Copy of the RFIQ document duly signed and stamped accepting all the terms and conditions.

2. **Last date for submission of sealed quotation:**

By or before **15.04.2026 upto 03:00 PM** at Central Office, Katra through Speed Post / Registered Post / reputed courier /by hand.

3. **Validity:** The validity of quotation should be 30 days from the last date prescribed for submission.

4. Quantity mentioned in RFIQ is indicative and can be increased or decreased as per requirement.

5. **Rates:**

- i) The rates should be NET inclusive of GST, loading, unloading, labour charges, toll tax, freight and other taxes / charges / F.O.R. Engineering Store, Banganga.
- ii) The participating firms are advised to quote rates as per Annexure B (inclusive of all), strictly as per the specifications and Brand/Make mentioned in the RFIQ.

6. Location for Installation of Network setup at **Heliport at Hutt village, Shergpur, Katra.**

7. Before submitting the offer, the participating firm is advised to visit and inspect the installation site to assess the actual conditions, scope of work, and any other factors that may affect the execution of the work. No claim whatsoever on account of lack of site knowledge shall be entertained at a later stage.

8. **Delivery:** The SITC shall be completed within a period of **25** days from the date of issuance of respective Order. Before participating, the competing firm must ensure that it has the capacity to meet the delivery period criteria. The Shrine Board may or may not extend the delivery period.

9. The conditional, illegible, ambiguous quotation (s) and quotation (s) received after the stipulated date and time shall be out rightly rejected.

10. The material to be supplied strictly should be from the brands / makes / specifications mentioned in the RFIQ. No change in the Brand / Make shall be accepted. No deviation or change in the specified Brand/Make shall be entertained after the issuance of the Work Order.

11. The rate of the successful firm shall be considered on an L-1 basis.

12. The participating firms are required to clearly mention the Brand/Make of the items to be offered in the Annexure – B i.e. Price Bid. Incomplete information or failure to specify the Brand/Make against any item may lead to the rejection of the bid at any stage, even after opening of bids.

13. The successful firm is responsible for replacing the cameras as well as related accessories with same approved brand / make material only within the warranty period. Any deviation from the same leads to the rejection of the supplied material alongwith forfeiting of EMD and debarring from any further dealing with SMVDSB for a period of 03 years.

14. The successful firm shall ensure the replacement of faulty component within a period of 05 days failing which same shall be replaced by the SMVDSB at its own and the cost of the same shall be deducted from the pending payment / EMD of the firm.

15. **INSPECTION / LIFTING BACK OF REJECTED SUPPLIES:**

- a. On receipt, the material shall be inspected / checked by our Inspection Committee and if found of inferior quality/defective, the same will be rejected and the Board shall be at liberty to have the same procured from open market at the risk & cost of the supplier whereby the original supplier shall be liable to pay the extra cost, if any, involved in the process. The Competent Authority, however, may accept the replaced material within the delivery period if it conforms to the approved specifications.
- b. The rejected material shall have to be lifted by the supplier at his own risk and cost within a week's time, failing which storage charges @ 2% per day shall be imposed against the supplier for a period of one week. Beyond one month the material shall be auctioned and storage charges shall be recovered from the supplier @ 2% per day. The amount acquired on account of auctioning shall be deposited to SMVDSB Account.

16. **Earnest Security Deposit (EMD):**

- a. The participating firm shall have to furnish the EMD in the shape of CDR/FDR amounting to **₹ 10,000/- (Rupees Ten Thousand only)** pledged to FA/CAO, SMVDSB payable at Katra along with the offer. The participating firms may also deposit the EMD amount through NEFT/RTGS in the official A/c of Shri Mata Vaishno Devi Shrine Board, Bank Name: The J&K Bank, Account No. Account No. 0235040500001804, IFSC – JAKA0KATTRA ("0" Zero).
- b. EMD in the shape of Demand Draft shall not be accepted. Also, no exemption for non-submission of EMD is allowed.
- c. It shall be noted that if any bidder did not enclose EMD (in original) of stipulated amount or furnish CDR/FDR of an amount less than the stipulated amount as mentioned, the bid/offer submitted by the firm shall be rejected outrightly and the rates of the said firm shall not be considered even after opening.
- d. The EMD of the successful bidder shall be retained as Security Deposit which shall be released after the expiry of warranty period, subject to receipt of satisfactory performance report from the concerned Unit Heads and IT Section.
- e. The EMD of the unsuccessful bidder shall be released after issuance of work order in favour of successful bidder.

17. **Penalty:** Following penalties (calculated on the value of unsupplied material) shall be imposed for delay beyond the prescribed delivery/installation period, unless exempted by the competent authority for valid reasons to be brought on record.

- a) upto 7 days @ 0.5%
- b) From 8th day to 15th day @ 1%
- c) From 16th day to 22nd day @ 1.5% and
- d) From 23rd day to 30th day @ 2% shall be imposed on each pending item as per the approved rate/quantity mentioned in the purchase order of the value of the pending supplies.
- e) After 30 days of delay, the purchase order shall be deemed to have been cancelled to the extent of unsupplied material and the material shall be procured from alternative sources at risk and cost of vendor.

Note: Despite cancellation of Purchase Order as stated above; for any valid reason to be brought on record, the Competent Authority may grant extension in the stipulated delivery period; with or without penalty. (Amount to be decided by the Competent Authority).

18. **Force Majeure:**

Any failure or omission to carry out the provisions of the order shall not give rise to any claim by one party against the other, if such failure or omission arises from an "Act of God" which shall include all acts of Natural Calamities such as fire, flood, earthquakes, hurricanes, pandemics or any pestilences or from civil strikes, compliances with any statute or regulations of the Government lock outs and strikes, riots, embargoes or from any other reasons beyond the control of the parties.

19. All disputes arising hereto are subject to Jurisdiction of the Courts of Law at Katra / Reasi.

20. **Payment:**

- a) No Advance payment shall be made.
- b) 70% Payment shall be released after the successful delivery of material at Engineering store, Banganga, Katra.

- c) 20% payment shall be released after the successful installation and commissioning of work i.e. supply/installation/testing/commissioning (SITC) of Network setup, subject to satisfactory report received from concerned unit I/c and I/c IT Wing, SMVDSB.
- d) 10% Payment shall be released after the expiring of DLP period of 02 year.
21. **Warranty:**
- The successful firm shall provide onsite warranty on the items specified in the Annexure - A.
 - The warranty shall start from the date of commissioning of Network at Site(s).
 - The successful firm shall be responsible for providing Guarantee / Warranty to SMVDSB on the supplied material. Warranty / Guarantee Certificate shall be furnished at the time of supply of material. The supplier shall be fully responsible for any manufacturing defects and shall provide onsite warranty / guarantee service after sales.
22. **Defect Liability Period:** The firm shall be responsible for providing a Defect Liability Period (DLP) of two (02) years for the entire Supply, Installation, Testing, and Commissioning (SITC) work of the Network Setup, including all allied accessories, commencing from the date of successful commissioning.
23. **Rights reserved by SMVDSB:** The Competent authority of SMVDB reserves the right:
- To cancel / terminate the RFIQ / Purchase Order during the period of its validity without assigning any reason thereof.
 - To forfeit the CDR/FDR of defaulter supplier.
 - Debarring any defaulter firm from any further dealing with Shrine Board for a period of three years.
 - Grant of extension with or without imposing penalty, as deemed fit.
 - To visit the premises of the bidder to verify the production capacity of the bidder / quality of products.
 - The Board reserves the right to establish reasonability of rates, to negotiate with the L-1 bidder for each item or to bifurcate the Purchase Order amongst more than one bidder (on L-1/negotiated rates).
24. This is just a RFIQ and not a Purchase Order.
25. The broad terms and conditions have been included. However, other standard terms and conditions of supply may be incorporated in the Purchase Order to be issued in due course.
26. Conditional, illegible, ambiguous quotation(s) and quotation(s) received after the stipulated date and time shall be out rightly rejected.
27. **Procedure for submission of Bid:**
- Bidders are required to submit their bids under a Two-Bid System, comprising:
- Cover – I: Technical Bid
 - Cover – II: Price Bid
- (A) Cover – I: Technical Bid:**
The technical bid shall include all supporting documents as per Clause 1 of the RFIQ document.
- (B) Cover – II: Price Bid:**
- The Price Bid must be submitted as per Annexure – “B”.
 - The Price Bid must be absolute and unconditional.
 - Conditional bids shall be summarily rejected.
 - The Price Bid will only be opened for bidders who have qualified in the technical bid evaluation.
 - Rates must be quoted strictly as per the prescribed format without any deviation.
- (C) Submission Method:**
Both the Technical Bid (Cover – I) and the Price Bid (Cover – II) must be sealed in separate envelopes super scribed as “**Quotation for SITC of Network Setup at Heliport at Hutt village**” against RFIQ No. CO/Pur/Electronics/657/21 dated: 06.04.2026 and submitted in-

person at the office of SMVDSB, Katra by 3:00 PM (15:00 Hrs) on 11.02.2026 or sent via Registered Post /Speed Post/ Courier addressed to:

Asstt. Chief Executive Officer (VB)
Shri Mata Vaishno Devi Shrine Board
Central Office, Jammu Road, Katra (J&K) – 182301

Bids received after the due date and time will not be considered under any circumstance.

28. All such offers, along with the terms and conditions duly signed, and enveloped as described above, must be submitted in person in the office of the SMVDSB, Katra by 03:00 PM (1500 hrs) on **15.04.2026**. Alternatively the sealed offer may be sent by Registered Post /Speed Post / Courier addressed to the office of the Chief Executive Officer, Central Office, Jammu Road, Katra (J&K) - 182301 so as to reach by 03:00 PM (1500 hrs) on **15.04.2026**. The offer(s) received after the due date and time shall not be considered under any circumstance.
29. The quotations shall be opened by the Committee, at the Office of Chief Executive Officer, SMVDSB, Katra in the presence of the bidders who may choose to be present.
30. The Shrine Board shall not be responsible for any delay in submission of quotation whatsoever. Any conditional offer or offers which are not appropriately sealed as per the format, as explained above, or offers received after the stipulated date and time, shall not be entertained. Any cutting or overwriting in the Documents will also make the bid liable for rejection.

Sd/-
(Vipan Bhagat), JKAS
Asstt. Chief Executive Officer

Seal and Sign. of the firm

(Please read all the contents of the RFIQ before the submission of the quotation)



**Office of the Chief Executive Officer
Shri Mata Vaishno Devi Shrine Board,**

Central Office, Jammu Road, Katra (J&K – UT) - 182301

**Annexure – “A” to this office RFIQ No.CO/Pur/Electronics/657/21
dated: 15.04.2026**

Detail of material to be installed at SITE:

S. No.	Description of items	Qty.	Make and Specifications	Minimum Warranty period
1.	Next Gen. Firewall	01	Make: Fortinet Fortiwifi 60F	12 months
2.	24 Managed Port PoE Switch with SFP	02	Make: D-Link / Cisco / Tp-Link / HP	24 months
3.	16 Managed Port PoE Switch with SFP	01	Make: D-Link / Cisco / Tp-Link / HP	24 months
4.	Network Rack 12 U	01	Make: ValRack / Comrac / President	12 months
5.	Network Rack 9 U	01		12 months
6.	PoE Wifi Access Points	05	Make: Cisco / D-Link / TP-Link	36 months
7.	LAN Points	27	--	OEM warranty
8.	CAT 6 Cable (305 mtr. Roll)	04	Make: Honeywell / D-Link / Molex	OEM warranty
9.	OFC Transceivers	02	OFC Transceivers SFP 1G Make: Cisco / D-Link / TP-Link	24 months
10.	Fiber Patch Cord 1m LC to SC Duplex	04	Make: Molex / D-Link / Schneider Electric (Actassi)	OEM warranty
11.	LIU 6 port	02	Make: D-Link / Molex / Comrack / Valrack / Schneider Electric (Actassi)	12 months
12.	OFC Armoured 2 Core SM	150 mtr.	Make: Honeywell / D-Link / Molex	OEM warranty

**Sd/-
(Vipan Bhagat), JKAS
Asstt. Chief Executive Officer**

(On the letter head of the firm)

PRICE BID

To,

The Asstt. Chief Executive Officer (VB),
Shri Mata Vaishno Devi Shrine Board,
Katra.

Subject: Quotation for SITC of Network setup.**RFIQ No. CO/Pur/Electronics/657/ 21 dated: 06.04.2026**

Sir,

I, _____ representative / proprietor of M/s _____ hereby submit my following rates for SITC of CCTV camera and allied accessories at the locations mentioned at Clause no: 7 of the RFIQ, as per the specification / UOM / requirement of Shrine Board:

S. No.	Description of items	Qty.	Model / Brand offered	Net Rate inclusive of all taxes, and SITC at SITE including Defect Liability Period of 02 years
1.	Next Gen. Firewall	01		
2.	24 Managed Port PoE Switch with SFP	02		
3.	16 Managed Port PoE Switch with SFP	01		
4.	Network Rack 12 U	01		
5.	Network Rack 9 U	01		
6.	PoE Wifi Access Points	05		
7.	LAN Points	27		
8.	CAT 6 Cable (305 mtr. Roll)	04		
9.	OFC Transceivers	02		
10.	Fiber Patch Cord 1m LC to SC Duplex	04		
11.	LIU 6 port	02		
12.	OFC Armoured 2 Core SM	150 mtr.		

Notwithstanding anything mentioned in our price bid, we hereby accept all the terms and conditions mentioned in the RFIQ which are being signed in token of my acceptance. We hereby undertake and confirm that I/we have understood the specifications properly and shall supply the material as per the required / higher specifications to SMVDSB.

I further affirm that in case, I fail to abide-by the conditions or upto the entire satisfaction of the Shrine Board; I shall be liable to the penalties under rules. I further hereby declare that my firm is not blacklisted.

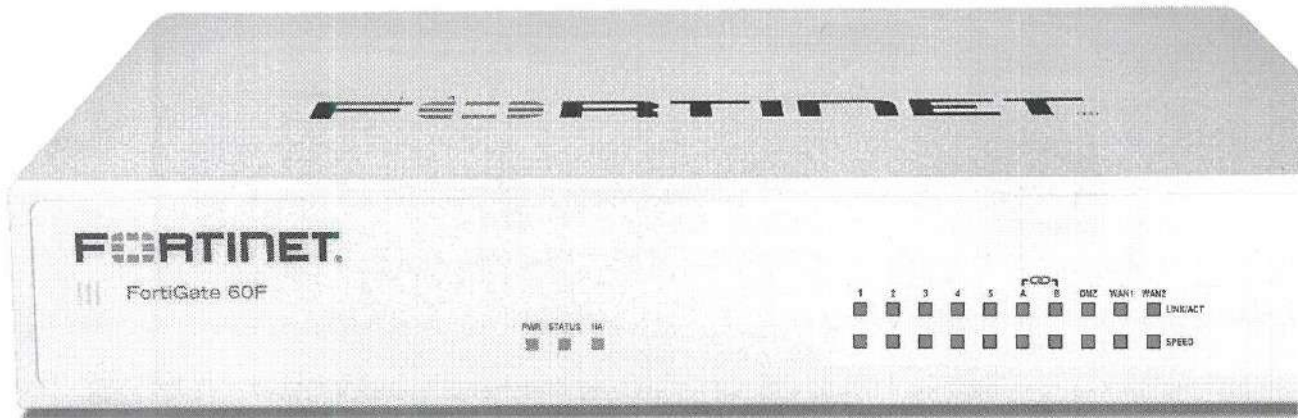
Seal & Signature _____ M/s _____

Full Address _____ Contact Person: _____

Contact Number: _____ E-mail ID: _____

The price to be quoted / offered on the letter head of the firm only as per the Price Bid format.

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.

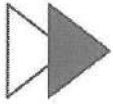
The 60F series runs on FortiOS, the industry's first converged networking and security operating system. This single OS approach enables businesses to gain benefits of operational efficiency and unified protection from the seamless integration of Fortinet Solutions within a Hybrid Mesh Firewall architecture.

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.

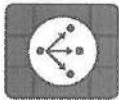
IPS	NGFW	Threat Protection	Interfaces
1.4 Gbps	1 Gbps	700 Mbps	Multiple GE RJ45 Variants with internal storage WiFi variants

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

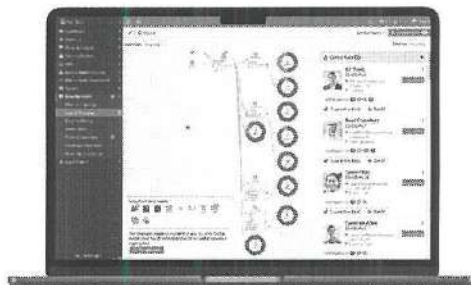
FortiOS, Fortinet's Real-Time Network Security Operating System

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 interoperability across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

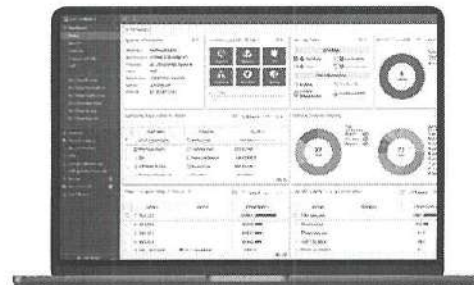
Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances 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>



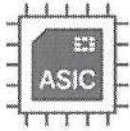
Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status



Fortinet ASICs: Unrivalled 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

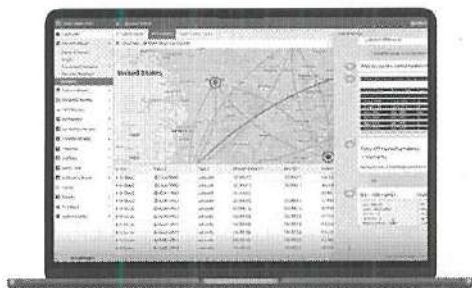


FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides 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.



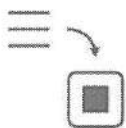
GenAI in FortiManager helps manage networks effortlessly—generate configuration and policy scripts, troubleshoot issues, and execute recommended actions.



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

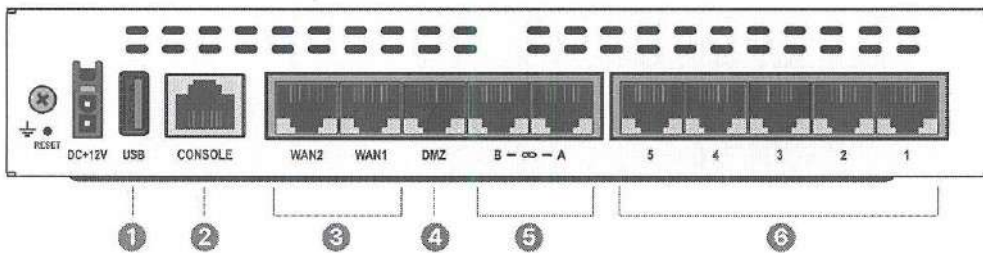
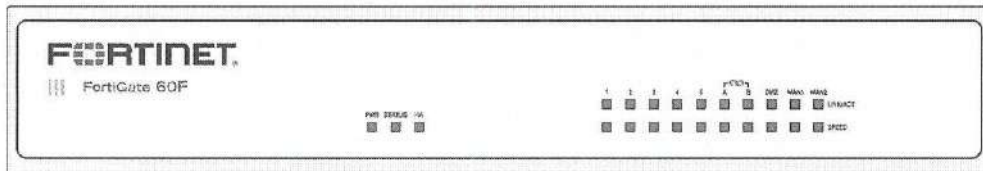


The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations 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 80F	FORTIGATE 61F	FORTIWIIFI 60F	FORTIWIIFI 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)			36 000	
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) ²			630 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) ²			400	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ²			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	---	---	3x3	
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	Bundles				
		A-la-carte	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection	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 Heuristic 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 ³	*				
	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 ³ Users ³					*
	FortiGate Cloud One Year Cloud-based Log Retention					*
NOC and SOC Services	FortiTelemetry Cloud					*
	FortiConverter Service for One Time Configuration Conversion	*	*			
	Managed FortiGate Service—Available 24x7, 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—24x7 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.

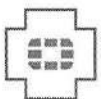
3. Only supported on G-series FortiGate models above 120G. See the FortiSASE Ordering Guide for supported models and their associated number of user licenses.

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 24x7x365 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 adapters for FG/FWF 60E/61E, 60F/61F, 70/71F, 70/71G, 80E/81E, 80/81F, 90/91G and FDC-100G. Power cable SP-FC60C-PCOR-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.

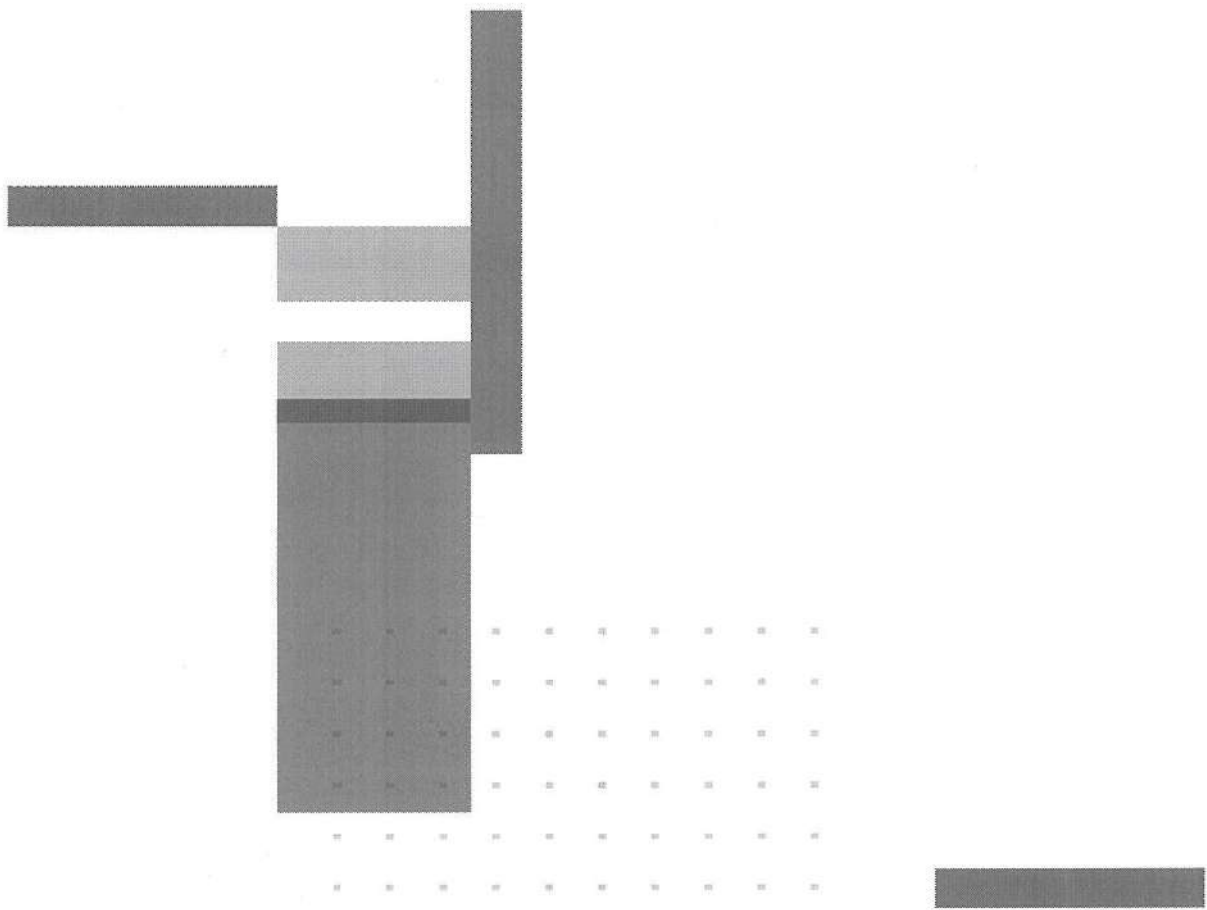
[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y.

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

Copyright © 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGuard®, and FortiSupport®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet marks herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 9, 2016

FOIWF-601-0A1-04A-2016-02

A standard 24-port Layer 2 managed PoE switch with 4 SFP slots generally features the following specifications across major brands like TP-Link, Cisco, and Aruba: [1]

1. Port Interface & Connectivity

- **Ethernet Ports:** 24 RJ45 ports supporting 10/100/1000 Mbps (Gigabit) speeds.
- **SFP Slots:** 4 slots for fiber uplinks, typically 1G SFP or 10G SFP+ depending on the model.
- **Console Port:** 1 RJ45 or Micro-USB port for out-of-band management. [2, 1, 4, 5, 6]

2. Power over Ethernet (PoE) [7]

- **PoE Standard:** Supports IEEE 802.3af (PoE, up to 15.4W) and IEEE 802.3at (PoE+, up to 30W) per port.
- **PoE Budget:** Total power capacity typically ranges from 180W to 410W.
- **PoE Management:** Includes features like priority settings, power scheduling, and remote PoE reset. [1, 5, 7, 8, 9, 10]

3. Layer 2 Management Features

- **VLAN Support:** Supports 802.1Q Tagged VLAN, Guest VLAN, and Voice VLAN for traffic isolation.
- **Spanning Tree:** STP, RSTP, and MSTP to prevent network loops.
- **Link Aggregation:** LACP for combining multiple ports to increase bandwidth.
- **Multicast:** IGMP Snooping (v1/v2/v3) to optimize video and CCTV traffic. [4, 5, 11, 12, 13, 14, 15, 16]

4. Performance & Security

- **Switching Capacity:** Typically between 56 Gbps and 128 Gbps.
- **MAC Table Size:** Usually 8K to 16K entries.
- **Security Protocols:** Access Control Lists (ACL), IP-MAC-Port Binding, DHCP Snooping, 802.1X Port Authentication, and DoS Defend. [2, 5, 11, 12, 16, 17, 18, 19]

5. Physical & Environmental

- **Form Factor:** 1U 19-inch rack-mountable metal chassis.
- **Cooling:** Typically dual built-in fans, though some high-efficiency models are fanless.
- **Operating Temp:** Generally 0°C to 45°C (32°F to 113°F) for standard commercial grades. [1, 1, 5, 20, 21]

A 16-port Layer 2 (L2) managed PoE switch with 2 SFP ports generally provides high-performance connectivity and power for enterprise or small business networks. Common specifications include a switching capacity of **32 Gbps to 40 Gbps** and a total PoE power budget typically ranging from **120W to 250W**.

Core Technical Specifications

- **Port Configuration:**
 - **16 x 10/100/1000Base-T Ports:** Standard RJ45 ports for high-speed Ethernet.
 - **2 x Gigabit SFP Uplink Ports:** Dedicated slots for fiber optic connectivity to expand network reach.
- **PoE Capabilities:**
 - **Standards:** Supports **IEEE 802.3af/at (PoE+)** for powering devices like IP cameras and wireless access points.
 - **Power per Port:** Up to **30W** per PoE port.
 - **Intelligent Management:** Features like **PoE Watchdog** and priority-based power allocation to prevent overload.
- **Performance Metrics:**
 - **Forwarding Rate:** Usually between **23.8 Mpps and 30 Mpps**.
 - **MAC Address Table:** Supports between **8K and 16K** entries.
 - **Packet Buffer:** Typically ranges from **512KB to 4.1MB**.

Layer 2 Management Features

- **Traffic Control:** Supports **802.1Q VLAN** (up to 4,000 groups), Quality of Service (QoS) for prioritizing voice/video, and **IGMP Snooping** for multicast optimization.
- **Redundancy & Reliability:** Includes Spanning Tree Protocols (**STP/RSTP/MSTP**) and **Link Aggregation (LACP)** for high network availability.
- **Security Strategies:** Features like **Access Control Lists (ACL)**, Port Security, **DHCP Snooping**, and **802.1X Authentication**.
- **Management Interfaces:** Configuration via **Web GUI**, Command Line Interface (**CLI**), **SNMP (v1/v2c/v3)**, and **RMON**.

Physical & Environmental

- **Form Factor:** Standard **1U 19-inch rack-mountable** design.
- **Cooling:** Available in both **fanless** (silent) and **dual-fan** models depending on the PoE budget.
- **Operating Environment:** Operating temperature range is typically **0°C to 40°C** or up to **50°C**.

PoE (Power over Ethernet) allows a single Ethernet cable to provide both data and electrical power to a WiFi Access Point (AP), simplifying installation in locations without nearby power outlets.

Core PoE Standards for Access Points

The standard required depends on the AP's power consumption, which typically increases with newer WiFi generations.

- **IEEE 802.3at (PoE+ / Type 2):**
 - **Max Power at PSE:** 30W.
 - **Max Power at AP:** ~25.5W.
 - **Typical Use:** Standard for most **WiFi 6** and **WiFi 6E** APs, especially those