# RG-CF30XS Series

## Next-Generation High-Performance Firewalls

Ruijie Networks Co., Ltd.
All Rights Reserved.

**Datasheet**
V1.0

# 01 Product Overview

## Introduction

As new hot spots such as social networking, cloud computing, and big data have emerged, the Internet has entered an unprecedented era of prosperity. However, the information security problems accompanied have become increasingly complex, bringing huge challenges to the traditional security construction model. Drawing on years of technological expertise and in line with the development trend of next-generation firewalls, Ruijie Networks has unveiled the RG-CF30XS series cloud-managed firewalls to cater for ever-changing demands of today's market. This firewall can be installed in a standard 19-inch rack and features high performance and flexible expansion.

## Product Features and Benefits

The RG-CF30XS series firewalls use a high-performance network forwarding service platform to provide intelligent quick deployment, active asset discovery, intelligent policy manager, one-click fault analysis, and service health diagnosis, simplifying device deployment and O&M. They have rich security functions, including intrusion prevention, antivirus, port scan, traffic learning, application control, and defense against DoS/DDoS attacks. They also support unified management on the cloud platform, data synchronization to the cloud for analysis and reporting, remote monitoring and O&M, policy translation for device replacement, batch configuration, and automatic inspection.

In addition, you can expand the performance of the RG-CF30XS series firewalls by purchasing performance licenses.

| Model | Firewall | IPS | NGFW | Threat Protection | Port |
|---|---|---|---|---|---|
| **RG-CF30XS** | 9 Gbps | 1.8 Gbps | 1.6 Gbps | 1.3 Gbps | 8 x GE RJ45 ports (WAN or LAN)<br>2 x 2.5GE RJ45 ports<br>2 x GE SFP ports<br>2 x 10GE SFP+ ports |

## Applicable Industries and Scenarios

The RG-CF30XS series firewalls can be deployed at an Internet egress, area boundary, data center boundary, and branch egress.

# 02 Product Appearance

## RG-CF30XS

Front View

Rear View

## RG-CF30XS (with the 4G Module Installed)

Front View

Rear View

### Appearance Design

The unique mounting bracket design allows rapid deployment, simplifying the installation process. In a complex equipment room environment, only one person is needed to complete the device installation and securing processes.

### Hardware Security

Different from common software-based defense, the RG-CF30XS series firewalls implement attack defense by using an exclusive built-in anti-DoS/DDoS component on the CPU. This significantly improves the DoS/DDoS attack defense performance and enables more robust and secure networks.

### All-New Hardware Design, Higher Reliability

A voltage or grid exception may incur a storage component failure. To mitigate this risk, the firewalls incorporate monitoring and spare components to enhance the shock resistance of storage components, thereby reducing device damages and data loss.

## 03 Product Highlights

- Built on high-performance hardware, the firewalls offer enhanced encryption and decryption capabilities for full traffic, ensuring robust security.
- Security risks are easier to detect, enabling efficient risk tracing and handling.
- Threat intelligence (TI) databases from leading sources like Google and Kaspersky are integrated to achieve superior risk detection.
- With a built-in AI engine, the firewalls collaborate with cloud-based AI to detect and analyze unknown threats such as polymorphic and slow attacks based on behavior characteristics and contextual correlation, improving threat detection and protection effectiveness by over 20%.
- By transforming the troubleshooting capabilities of senior engineers into product functions, the firewalls provide you with a one-stop troubleshooting wizard.
- In the industry-first policy simulation space, you can foresee the effects of security policy adjustment, realizing zero-risk policy adjustment.
- Simple cloud O&M allows you to manage network and security devices on the entire network via a mobile app.

# 04 Product Features

## High Effectiveness: All-in-One Security

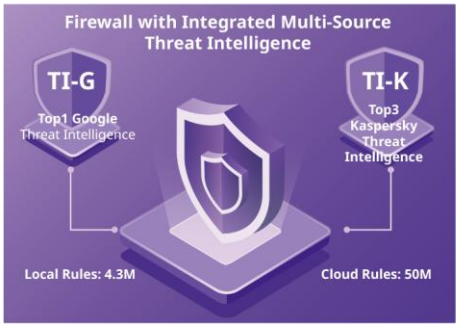
App Control | DNS Inspection | Multi-Source Threat Intelligence | URL Filtering | SSL Decryption | IPS | AV | WAF | Behavior-AI Detection

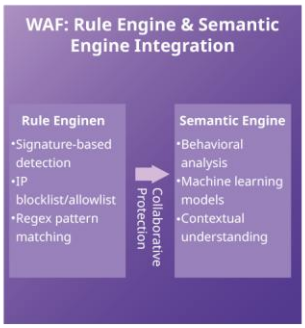
**URL & App filtering:** Top-tier BrightCloud with AI-driven URL detection, improving URL filtering by 20%.

**TI:** Dual TI engines (Google & Kaspersky), improving IP and domain protection by 20%.

**WAF:** Dual-engine WAF (rule + semantic), improving web protection by 30%.

**Abnormal behavior:** Built-in AI engine for behavior-based detection, improving unknown threat protection by 30%.



All-in-One Capabilities: One firewall delivers built-in app control and URL filtering, IPS, AV, Google & Kaspersky threat intelligence, WAF, and AI-based unknown threat detection.

## Lower CapEx and Higher Performance


**CPU Only**
CPU-only decryption slows down performance, leaving 90% of encrypted threats undetected.

**CPU + Fixed Chip**
Any performance upgrade requires hardware replacement.

**CPU + Programmable Chip**
NTOS works seamlessly with FPGA to continuously boost performance.

A firewall delivers over 20% higher decryption and threat protection performance, and seamlessly scales with your business. There is no need to rip and replace infrastructure, saving 10% in procurement costs and over 20% in hardware upgrade costs.

## Easier Security and Lower OpEx

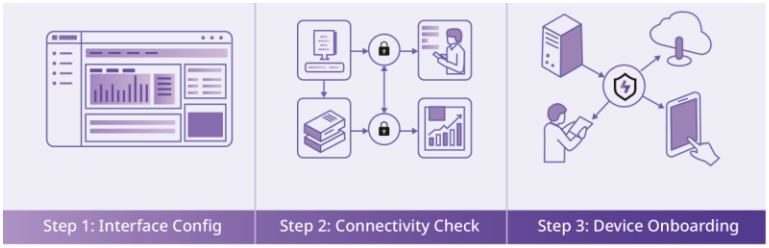

**Analysis:** Smart cloud correlation for massive alerts, automatically generating and pushing event notifications.

**Traceability:** One-click tracing for security incidents, covering events, locations, and root causes.

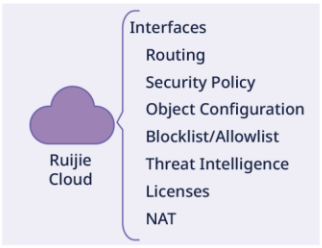
**Control:** Dashboards and reports for network & asset security posture, providing precise improvement recommendations.

No dedicated analyzer product or security experts are required. Event handling time for alert collection, analysis, tracing, and response is reduced from 3 days to just 0.5 days, saving 20% in OpEx.

## Easy O&M and Lower OpEx

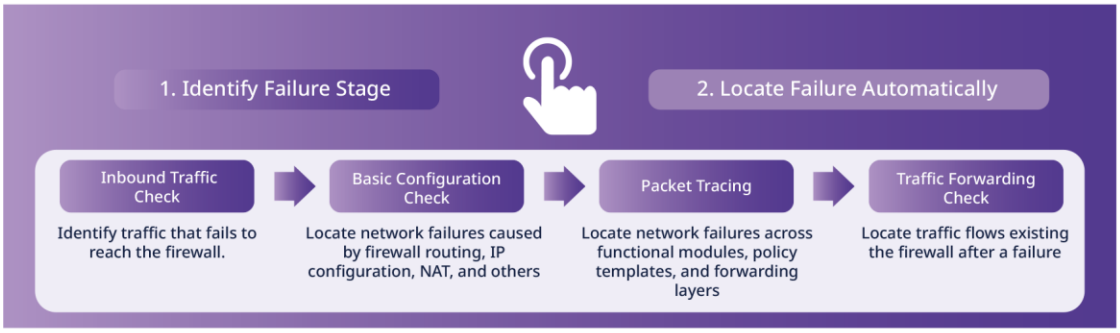



**3-step deployment to go live, reducing onboarding time from 5 hours to 1**

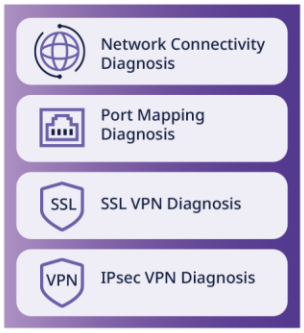



**Remote cloud management, eliminating on-site visits**


**Traffic learning and policy simulation, cutting policy setup time from 8 hours to 1**




**No on-site visits needed. One-click fault diagnosis powered by Cloud AI**




**Firewall Diagnosis Center**

No additional management product is required, reducing deployment time from 3 days to 1 day. Troubleshooting & recovery time is reduced from 1 day to 3 hours, saving 30% in OpEx.

## Intelligent Service Diagnostic Center

- **Fault Analysis**

The RG-CF30XS series firewalls are developed to transform the troubleshooting capabilities of senior engineers into product functions and provide you with a one-stop troubleshooting wizard. In the diagnostic center, automatic troubleshooting can be conducted based on the paths that clients use to access target resources, and fault information and handling suggestions are displayed. This greatly improves the efficiency of troubleshooting and saves additional expenses for troubleshooting.

- **Packet Tracing**

In the diagnostic center, you can also analyze and trace packet processing of each security service module on the device, and check detailed information of packet tracing records to accelerate network fault troubleshooting and locating.

## Port Scan and Traffic Learning, Simple Firewall Onboarding

- **Onboarding Configuration**

To perform firewall onboarding, you can conduct **Port Scan** to automatically identify the IP address and port number of a service system, and then enable **Traffic Learning** to automatically detect the service access relationship on the live network. You can also generate access control policies based on ports with one click, and complete firewall onboarding without professional knowledge.

- **Server Port Check**

In routine O&M, server ports need to be checked to meet high security requirements and formulate refined security policies. In traditional mode, server ports need to be manually verified with the customers, which takes a long time. With port scan and traffic learning, this process can be completed in one day, which greatly improves efficiency and lowers technical thresholds.

### Policy Simulation Space to Foresee Effects, Zero-Risk Policy Adjustment

You can add, delete, and modify a policy in the simulation space, use the policy to match the real traffic to analyze the difference in traffic matching before and after the policy adjustment, and adjust the policy accordingly. In this way, policies can be adjusted without service interruption, and O&M personnel do not need to stay up late to adjust policies in off-peak hours. The risk of policy adjustment is minimized, and refined policy adjustment can be achieved.

## 05 Product Specifications

### Product Performance

| Firewall | IPS[1] | NGFW[1,2] | Threat Protection[1,3] |
|---|---|---|---|
| 9 Gbps | 1.8 Gbps | 1.6 Gbps | 1.3 Gbps |
| Combination of product and performance licenses (Threat Protection):<br>Threat Protection 1.3 Gbps: RG-CF30XS series chassis | | | |

| System Performance and Capacity | RG-CF30XS Series |
|---|---|
| Firewall throughput of IPv4 packets (1518-byte UDP packets)4 | 9 Gbps |
| SSL inspection throughput | 840 Mbps |
| Concurrent sessions (TCP) | 1.5 Million |
| New sessions per second (TCP) | 105,000 |
| Firewall policies | 3,000 |
| SSL VPN throughput | 2.16 Gbps |
| Concurrent SSL VPN users (recommended maximum, tunnel mode) | 1,125 |
| IPsec VPN throughput | 3.7 Gbps |
| Gateway-to-gateway IPsec VPN tunnels | 200 |

**Note:**

All performance values are the maximum values and may vary depending on system configuration.

1. The performance values of IPS (mixed traffic), application control, NGFW, and threat protection are measured with logging enabled.

2. NGFW performance is measured with firewall, IPS, and application control enabled.

3. Threat protection performance is measured with firewall, IPS, application control, and malware protection enabled.

4. Firewall throughput is the maximum forwarding performance (1518-byte UDP packets) of hardware.

## Hardware Specifications

### • Dimensions and Weight

| Dimensions and Weight | RG-CF30XS Series |
|---|---|
| Product dimensions (W x D x H) | 440 mm x 222 mm x 43.6 mm (17.32 in. x 8.74 in. x 1.72 in.) |
| Shipping dimensions (W x D x H) | 540 mm x 345 mm x 153mm (21.26 in. x 13.58 in. x 6.02 in.) |
| Product weight | 2.42 kg (5.34 lbs.) |
| Shipping weight | 3 kg (6.61 lbs.) |
| Form factor | 1 RU rack |

### • Port Specifications

| Port Specifications | RG-CF30XS Series |
|---|---|
| Fixed service port | 8 x 10/100/1000BASE-T ports<br>2 x 10/100/1000/2.5GBASE-T ports<br>2 x 1GE SFP ports<br>2 x 10GE SFP+ ports |
| Fixed management port | 1 x RJ45 MGMT port<br>1 x RJ45 console port (RS-232) |
| USB port | 1 x USB 3.0 ports |

### • Storage Specifications

| Storage | RG-CF30XS Series |
|---|---|
| Hard disk | RG-CF30XS has no hard disk for factory delivery. A 480 GB SSD or a 1 TB HDD expansion module can be added. |

## Storage Specification

| Storage Specification | RG-NSEC-SSD-480G-B-M | RG-NSEC-HDD-1T-B |
|---|---|---|
| Size | 79.2 mm x 109.5 mm x 19.2 mm (3.12 in. x 4.31 in. x 0.76 in.) | 79.2 mm x 109.5 mm x 19.2 mm (3.12 in. x 4.31 in. x 0.76 in.) |
| Port type | SATA | SATA |
| Storage capacity | 480 GB | 1 TB |
| Hard disk type | Solid state drive | Mechanical hard drive |
| Maximum power consumption | 2.4 W | 3.5 W |
| Hot swapping | Not supported | Not supported |
| Product weight | 0.2 kg (0.44 lbs.) | 0.25 kg (0.55 lbs.) |

## LTE Module Specifications

| Model | RG-NSEC-SIC-LTE-S |
|---|---|
| 4G Interface | One 4G interface |
| Connector Type | Two SMA-J interfaces (ANT 1 and ANT 2) for connecting dual antennas |
| Antenna | Two 4G antennas in the standard configuration |
| Supported Rate | FDD-LTE: B1/ 2/ 3/ 4/ 5/ 7/ 8/ 12/ 13 /14/ 17/ 18/ 19/ 20/ 25/ 26/ 28/ 29/ 30 / 32/ 66/ 71<br>TDD-LTE: B34/ 38/ 39/ 40/ 41/ 42/ 43/ 46/ 48<br>WCDMA: B1/ 2/ 3/ 4/ 5/ 6/ 8/ 19 |
| SIM Card | Two Micro SIM cards (Dual SIM single standby) |
| Configuring Module Hot Swapping | Not supported |
| Dimensions (W X D X H) | 103.37 mm x 123 mm x 28 mm (4.07 in. x 4.84 in. x 1.1 in.) |
| Maximum Power Consumption | 5W |

### • Power Supply and Consumption

| Power Supply and Consumption | RG-CF30XS Series |
|---|---|
| Power supply | 1 x fixed power supply:<br>• Rated input voltage: 100–240 V; 50/60 Hz<br>• Rated input current: max 1.5 A |
| Max. power consumption | 30 W |

### • Environment and Reliability

| Environment and Reliability | RG-CF30XS Series |
|---|---|
| Operating temperature | 0°C to 45°C (32°F to 113°F) at altitudes below 1,800 m (5,905.51 ft.) above sea level |
| Storage temperature | –40°C to +70°C (–40°F to +158°F) |
| Operating humidity | 10% RH to 90% RH (non-condensing) |
| Storage humidity | 5% RH to 95% RH (non-condensing) |
| Operating altitude | 0 m to 5,000 m (0 ft. to 16,404.2 ft.) |

### • Regulatory Compliance

| Regulatory Compliance | RG-CF30XS Series |
|---|---|
| RoHS | Yes |
| Safety compliance | IEC 62368-1 |
| EMC | EN 55032, EN 55035, EN 61000-3-3, EN 61000-3-2, EN 301489-1 |

## Software Specifications

### • Network

| Network | RG-CF30XS Series |
|---|---|
| Physical interface | Configuring interfaces as LAN or W WAN ports; three modes for WAN ports: PPPoE, DHCP, and static IP; configuring the routing, transparent, or bypass mode for interfaces |
| Sub-interface | Configuring sub-interfaces and VLAN IDs |
| Bridge interface | Configuring interfaces in transparent mode as bridge interfaces |
| Aggregate interface | Configuring aggregate interfaces |
| Routing | IPv4/IPv6 static and dynamic routing, routing policy, Policy-based Routing (PBR), ISP address library-based routing, application-based routing, and egress load balancing |
| DHCP server | DHCP server functions |
| DNS server | Configuring DNS addresses for devices |
| DDNS | Multiple DDNS service providers supported |
| Link detection | Link detection and link detection logs |
| VPN | SSL VPN and IPsec VPN |
| VRRP | VRRP functions |
| High availability | Deployment with redundancy to achieve automatic switchover between active and passive devices, ensuring service continuity |
| SD-WAN | Integration with cloud platforms to achieve unified orchestration and monitoring of multiple branches |

## Object

| Object | RG-CF30XS Series |
|---|---|
| Address/Address group | Configuring IPv4/IPv6 address objects in IP address/range format |
| Zone | Configuring security zones |
| Application and application group | Configuring application types in application/application group mode |
| Service/Service group | Configuring service objects; common default port services supported |
| Time plan | Configuring time objects; one-off time plans and cyclic time plans supported |
| ISP address library | Default ISP address libraries: China Telecom (CHN), China Mobile (CHN), China Unicom (CHN), CERNET (CHN), and Beijing Teletron (CHN); customizing, importing, and exporting ISP address libraries |
| Virus protection template | Configuring content object templates; antivirus (AV) templates supported; configuring quick scan or deep scan; configuring templates based on protocols and directions; setting excluded viruses |
| Intrusion prevention template | Configuring content object templates; predefined Intrusion Prevention System (IPS) templates supported; customizing IPS templates; configuring rule filters based on objects, severity, protocols, and threat types; setting excluded rules |
| File filtering | Configuring content object templates; file filter templates (filtering by file type) supported |
| URL filtering | URL filtering |
| SSL proxy certificate | Adding, importing, deleting, viewing, and downloading SSL proxy certificates; configuring a global SSL proxy certificate |
| Server certificate | Importing, deleting, viewing, and downloading server certificates |
| Security rule base | Viewing default security rules in the IPS library |
| Content identification | URL category and keyword configuration |
| User authentication | User management, user import, authentication server configuration, real-name user information synchronization, and authentication policy configuration |

## Policy

| Policy | RG-CF30XS Series |
|---|---|
| Traffic learning | Traffic learning to record destination IP addresses and port numbers as well as abnormal traffic; Export of traffic learning logs |
| Network address translation (NAT) | NAT; configuring NAT policies; importing NAT policies in batches; common NAT application-level gateway (ALG) services; server port mapping; viewing NAT address pool status |
| Security policy | Configuring security policies; customizing policies based on parameters including objects, contents, and zones; viewing the policy list; importing security policies in batches |
| Policy simulation | Simulating policy execution in the simulation space to check whether uncertain security policies can achieve expected effects |
| Policy configuration wizard | Security policy configuration wizard for conducting port scan, performing configurations, testing configurations, and other steps to generate security policies |

| Policy | RG-CF30XS Series |
|---|---|
| Policy optimization | Sorting out configured security policies and analyzing policies to identify redundant, expired, and conflicting policies |
| Policy lifecycle | Full lifecycle display of security policies, including detailed records of policy changes |
| Port scan | Port scan of configured IP ranges for all ports or selected ports; policy creation prompt for scan results |
| DoS/DDoS attack defense | Different DDoS attack defense policies in security defense |
| ARP attack defense | Anti-ARP spoofing, ARP flooding suppression, and other functions in security defense |
| Local defense | Configuring local defense policies in security defense |
| Threat intelligence | Enabling or disabling threat intelligence; customizing threat intelligence; managing excluded threats |
| Blocklist/Allowlist | Configuring global blocklists and allowlists |
| SSL proxy policy | Configuring SSL proxy policies; customizing policies based on parameters including objects, contents, and zones; policy list |
| SSL proxy template | Configuring SSL proxy templates; setting the template type to protecting client or server |
| SSL proxy allowlist | Configuring domain name allowlists and application allowlists |
| Behavior analysis | Configuring analysis policies, templates, and allowlists |
| AI-based Threat Detection | AI-powered stealthy attack and abnormal behavior detection |

- System

| System | RG-CF30XS Series |
|---|---|
| Simple Network Management Protocol (SNMP) | Connecting to third-party platforms for management through SNMPv1/v2/v3 |
| Patch installation | Downloading and installing patches for upgrade |
| Cloud management platform | Enabling or disabling unified management on the cloud management platform; log upload to the cloud |
| One-click collection | Collecting fault information with one click |
| Device health | Device health diagnosis |
| Service diagnosis | Service continuity diagnosis |
| System upgrade | System upgrade and rollback |
| Database backup | System database backup and restoration |
| Factory settings restoration | Restoring factory settings on the web UI |
| API | Open APIs facilitate integration and docking with other third-party platform |

- O&M

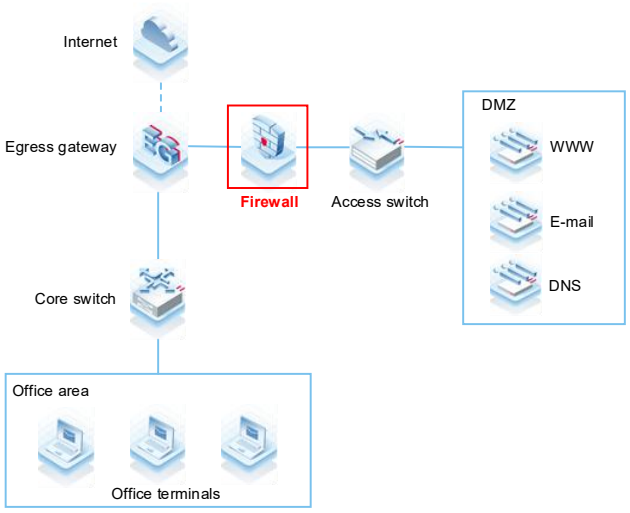
| System | RG-CF30XS Series |
|---|---|
| Dashboard | Providing insights into the network's security status and network operation status |
| Reports | Periodically or regularly generating network status and network security reports |
| Fault diagnosis | Helping quickly locate and resolve network and security issues |

# 06 Typical Applications

## Security Defense at Area Boundary

The RG-CF30XS series firewalls can be deployed at an area boundary to meet LAN application requirements, improve information security, and guarantee LAN service security. The firewalls can bring the following benefits:

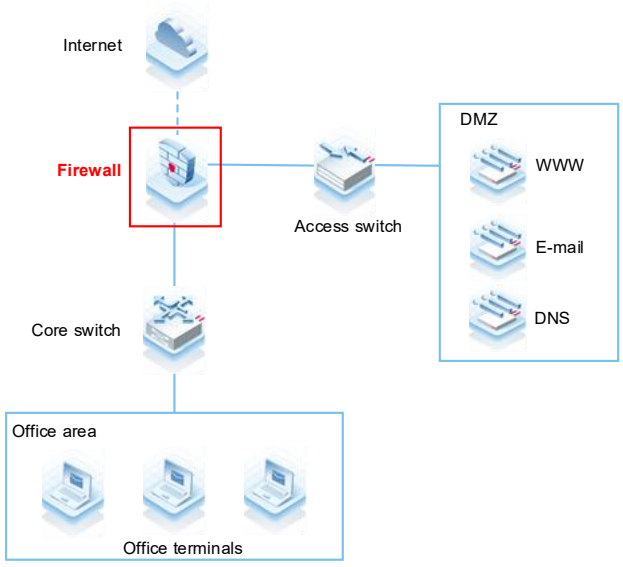
- Generate refined access control policies based on servers.
- Effectively defend against external attacks and viruses to protect key enterprise services.
- Help users identify and control applications.




## Small and Medium-Sized Internet Egress

The RG-CF30XS series firewalls can satisfy the needs of small and medium-sized Internet egress, improve information security, and guarantee egress network security. The firewalls can bring the following benefits:

- Meet the needs of small and medium-sized Internet egress scenarios.
- Effectively defend against external attacks and viruses to protect key services of users.
- Help users identify and control applications.



# 07 Ordering Information

| Model | Description |
|---|---|
| RG-CF30XS | Rack-Mounted Firewall — Threat Protection Throughput: 1.3 Gbps to 1.6 Gbps; 8 x GE RJ45 Ports, 2 x 2.5GE RJ45 Ports, 2 x GE SFP Ports, 2 x 10GE SFP+ Ports; Built-in 64 GB Storage; 1 x Fixed Power Supply; Hard Disk and LTE Expansion Support |
| RG-CF30XS-300M-LIC | RG-CF30 Series Full Threat Protection Throughput License –Each Additional License Increases the T Total Throughput by 300 Mbps, with an Upper Limit of 1.6 Gbps |
| RG-CF30XS-UTP-LIS-1Y | RG-CF30 Series 1-Year All-in-One Security Feature License（IPS+AV+TI-G+TI-K+URL Filtering+App Control+AI+WAF） |
| RG-CF30XS-UTP-LIS-1M | RG-CF30 Series 1-Month All-in-One Security Feature License（IPS+AV+TI-G+TI-K+URL Filtering+App Control+AI+WAF） |
| RG-NSEC-SIC-LTE-S | Rack-Mounted Firewall 4G Plug-in Module – Enables Network Access for Firewalls via 4G Card |
| RG-NSEC-SSD-480G-B-M | 480 GB SSD Expansion Module |
| RG-NSEC-HDD-1T-B | 1 TB HDD Expansion Module |
| RG-CF30XS-1.3G-Bundle-1Y | RG-CF30XS + RG-CF30XS-UTP-LIS-1Y |
| RG-CF30XS-1.3G-Bundle-3Y | RG-CF30XS + 3 x RG-CF30XS-UTP-LIS-1Y |
| RG-CF30XS-1.3G-Bundle-5Y | RG-CF30XS + 5 x RG-CF30XS-UTP-LIS-1Y |

Note:

To ensure syslog security and system stability, please use hard disks from Ruijie. Ruijie will not be responsible for any hardware damage, syslog loss, or performance degradation resulting from the use of third-party hard disks. An unauthorized third-party hard disk does not have a hard disk tray provided by Ruijie, w which w will cause hardware malfunctions. In addition, insufficient hard disk IOPS specifications and improper hard disk partitioning may lead to system failures.

# 08 Ordering Guide

The RG-CF30XS series firewalls provide two GE SFP ports and two 10GE SFP+ ports. The following table lists the optional optical transceivers.

| Model | Description |
|---|---|
| XG-SFP-SR-MM850 | 10G SR module, SFP+ form factor, Duplex LC, 300 m (984.25 ft., with OM3 optical cables) or 400 m (1312.34 ft., with OM4 optical cables) over MMF |
| XG-SFP-LR-SM1310 | 10G LR module, SFP+ form factor, Duplex LC, 10 km ((32,808.40 ft.) over SMF |
| XG-SFP-ER-SM1550 | 10G ER module, SFP+ form factor, Duplex LC, 40 km (131,233.60 ft.) over SMF |
| XG-SFP-ZR-SM1550 | 10G ZR module, SFP+ form factor, Duplex LC, 80 km (262,467.19 ft.) over SMF |
| XG-SFP-LR10-SM1270-BIDI-I | 10G LR module, SFP+ form factor, BIDI LC, 10 km (32,808.40.13 ft.) over SMF |
| XG-SFP-LR10-SM1330-BIDI-I | 10G LR module, SFP+ form factor, BIDI LC, 10 km (32,808.40.13 ft.) over SMF |
| XG-SFP-AOC1M | 10G SFP+ AOC cable, 1 m (3.28 ft.) |
| XG-SFP-AOC3M | 10G SFP+ AOC cable, 3 m (9.84 ft.) |
| XG-SFP-AOC5M | 10G SFP+ AOC cable, 5 m (16.40 ft.) |
| XG-SFP-T | 10G SFP+ copper module, SFP+ form factor, RJ45 connector, 100 m (328.08 ft.) over Cat 6a/7 cable |
| MINI-GBIC-SX-MM850 | 1G SR module, SFP form factor, LC, 550 m (1,804.46 ft.) over MMF |
| MINI-GBIC-LX-SM1310 | 1G LX module, SFP form factor, LC, 10 km (32,808.40 ft.) over SMF |
| Mini-GBIC-GT | 1G SFP copper module, SFP form factor, RJ-45, 100 m (328.08 ft.) over Cat 5e/6/6a |
| MINI-GBIC-LH40-SM1310 | 1G LH module, SFP form factor, LC, 40 km (131,233.60 ft.) over SMF |

# 09 Package Contents

| Item | Quantity |
|---|---|
| RG-CF30XS series chassis (with the nameplate at the bottom) | 1 |
| Power cord | 1 |
| Grounding wire | 1 |
| Rubber pad | 4 |
| L-shaped rack-mount bracket | 2 |
| M4 x 8 mm cross recessed countersunk head screw | 4 |
| Warranty Card | 1 |
| User Manual | 1 |

# 10 Warranty Information

## Security Defense at Area Boundary

For more information about warranty terms and period, visit the official Ruijie website or contact your local sales agency:

- Warranty terms: https://www.ruijie.com/support/servicepolicy
- Warranty period: https://www.ruijie.com/support/servicepolicy/Service-Support-Summany/

Note: The warranty terms are subject to the terms of different countries/regions and distributors.

# 11 More Information

## Security Defense at Area Boundary

For more information about Ruijie Networks, visit the official Ruijie website or contact your local sales agency:

- Ruijie Networks official website: https://www.ruijie.com/
- Online support: https://www.ruijie.com/support
- Hotline support: https://www.ruijie.com/support/hotline
- Email support: service_rj@ruijie.com