GPL-NGFW-3000R

Zero Trust Next Generation Firewall

GPL-NGFW-3000R is a new generation firewall, designed to deliver Advanced Zero Trust security with cutting edge features for protecting the IT networks. It combines advanced security measures, high availability and fine-grain controls minimising the attack surface and reducing the risk of cyber-attacks to meet the needs of modern IT infrastructures.

FEATURES OVERVIEW

Intrusion Detection System (IDS/IPS)

- Real-time monitoring of network traffic for malicious activities
- Alerts administrators of potential threats
- Seamlessly integrates with other security protocols
- Proactively blocks identified threats before they infiltrate your network
- Leverages signature-based and anomaly-based detection techniques

Firewall and Routing

- Stateful packet inspection for robust network defence
- Flexible routing options or complex network architectures
- Support for NAT and port forwarding

High Availability (HA)

- Active-passive and active-active failover configurations
- Ensures uninterrupted network service

Customisable Web categories /Whitelisting

- Predefined and customisable web filtering categories
- Easy to configure whitelisting for trusted sites

DNS-based content filtering

- Blocks access to harmful websites based on DNS requests
- Provides and additional layer of security against malware and phishing

Protection against New Malware/Virus / Phishing Outbreaks

- Regular updates to threat intelligence databases
- Zero-da protection with heuristic analysis

Advanced Zero Trust Network Access

- Eliminates VPN (TLS/SSL)
- Network Lockdown: no open inbound ports, no public IPs
- Complete isolation from the internet and internal networks
- Simplified Firewall rules management
- Continuous, context-aware authentication
- Pre-defined Zero Trust policies based on multi-dimensional authentication
- Efficient networks: optimised bandwidth usage, supports C2C topology, low latency
- Fine-grained controls to manage and monitor application usage

Enhanced Security

- Zero encryption overhead
- Micro-segmentation at service level
- Quantum-Safe security
- Physical unclonable function (PUF)
- Crypto agility for seamless real-time updates

Botnet Filtering

- Detects and blocks communications with malicious botnet servers
- Prevents data exfiltration and unauthorised access

Time-based/ Scheduled Filtering

- Enables granular control over Internet and application access
- Schedules rules to restrict access during specific hours

Blu5 Group
info@blu5group.com
www.blu5group.com

GPL-NGFW-3000R

Zero Trust Next Generation Firewall

HARDWARE FEATURES

Mini Size
Portable

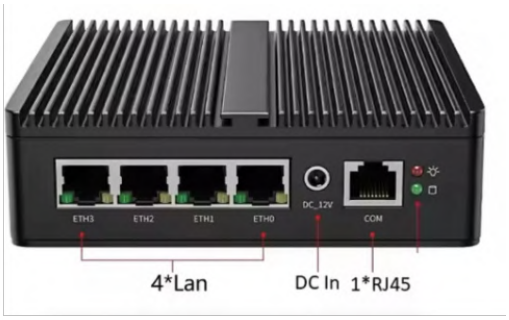
Full aluminium alloy
Excellent cooling

Fan-less
Silent Design

HARDWARE SPECIFICATIONS

The main hardware factors of the GPL-NGFW-3000R setup involved are CPU, RAM, mass storage (disc), the number and quantity of network interface.

FIREWALL THROUGHPUT	MANAGEMENT	LOGGING AND REPORTING
UP TO 300 Mbps	We-based GUI, CLI	Built-in and external server integration



Blu5 Group
info@blu5group.com
www.blu5group.com

GPL-NGFW-3000R

Zero Trust Next Generation Firewall

Specifications and Performance*

Product Performance	
Concurrent service routes	Up to 1024 concurrent ZTNA routes Up to 1022 concurrent ZTNA routes • 510 Client-Server ZTNA routes • 512 Server-Client ZTNA routes
Throughput	Up to 300Mbps
Features	
High availability	Active-Passive High Availability
Disaster Recovery	Smart Disaster Recovery Function
Centralised management	Secure remote web-based configuration, monitoring and logging system
General Specifications	
Processor	ARM Cortex A, Intel onboard Celeron J4215 Processor, FCBGA1090, quad core quad threaded, 2.00GHz Main frequency, 4MB cache, TDP10W processor7, quad core processor
BIOS	AMI EFI BIOS
Network Interface	Design of onboard INTEL I226 2.5G network card chip with 4 network ports
Display Interface	1 DP interface 1 HDMI interface
System Memory	2 x DDR4, SO-DIMM slot, DDR4 2400, maximum memory support of 8GB
Storage Memory	1xSATA interface, 1xM SATA solid state drive interface , 1xM2_2280 solid-state drive interface PCIE2.0 X1
Routing	Proprietary TCP Service-Level Routing
Security	Key Management libraries (generation, update, storage) HW Accelerator for High-Speed AES256 (up to 5Gb/s) SHA256, CMAC-AES256, Elliptic Curves (up to 521-bit) Post Quantum Algorithms (on demand) Mutual Authentication Symmetrical Cryptographic Scheme Inner and Outer Attacks Protection Supply Chain Attacks Protection Software tampering detection SSL/TLS free cryptography Military-grade key derivation functions Simplex and Duplex Session Keys Negotiation process

**Specifications are subject to change without notice to improve reliability, function or design or otherwise. Product performance measured in a controlled laboratory environment, actual performance may vary due to factors such as network traffic and environmental conditions. Results may not be indicative of real-world scenarios.*

Blu5 Group
info@blu5group.com
www.blu5group.com

GPL-NGFW-3000R

Zero Trust Next Generation Firewall

Specifications and Performance

Physical Specifications	
System Fan	Fan-less
Housing	CNC Aluminium Box
Front Panel	4x 2.5G Ethernet port 1x RJ45-COM port 1x power adapter interface 1x power hard disk indicator light
Rear Panel	2 x USB 2.0 ports 2x USB 3.0 ports 1x HDMI (with output audio) + DP 1x power button 1x SIM card slot
Expansion slots	1x Mini PCI-e interface
Unit Dimension	136mm x 126mm x 40mm (W x D x H)
Unit Weight	1.75 Kg (whole machine) 1.15 Kg (bare machine)
Power Specifications	
Power supply	DC 12V -4A 5.5*2.5
Environmental	
Operation Temp.	-0°C ~ 50°C (commercial HDD) -20°C ~ 50°C (industrial SSD) surface air flow
Operating Humidity	5 ~ 90% relative humidity non condensing
Other functions	
Miscellaneous	Power on, times power on, network wakeup, PXE Startup, watchdog
Regulatory	
Approval	CE, CCC, FCC, ROHS

*Specifications are subject to change without notice to improve reliability, function or design or otherwise. Product performance measured in a controlled laboratory environment, actual performance may vary due to factors such as network traffic and environmental conditions. Results may not be indicative of real-world scenarios.

Blu5 Group
info@blu5group.com
www.blu5group.com