PRODUCT BROCHURE / US 1.0.1

zGuardian-NG

KEY FEATURES

- Enhances Protection & Network Security
- Easy Deployment and Simplified Management
- Extensive Data Analysis and Report Generation
- Automatic updates to keep system protected from latest threats
- Freedom to deploy more than one security technologies

PRODUCT OVERVIEW

zGuardian-NG – Cybersecurity Appliance

The zGuardian Cybersecurity Appliance Next-Generation Firewall (NGFW) offers state-of-the-art security protection that is well- suited for small and medium-sized enterprises with down-to- earth pricing.

With advanced features such as on-the-fly malware protection, intrusion prevention, and URL/DNS filtering, it safeguards the entire IT infrastructure without any performance penalties. The zGuardian-NG adopts Unified Threat Management (UTM), integrating multiple security features into a single appliance.

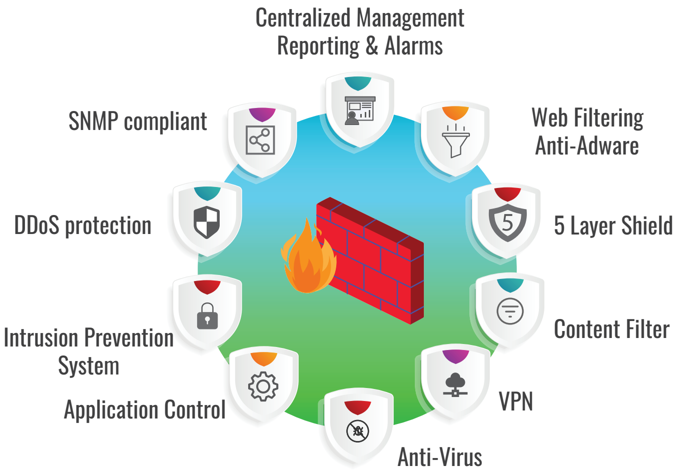
zGuardian-NG Management Station

The zGuardian-NG Management Station is a centralized software designed to manage and monitor zGuardian-NG devices deployed within the network's reach.

Its dashboard displays real-time activities and notifications from the managed zGuardian-NG devices.

zGuardian-NG Functionalities

- URL/DNS Filtering
- Anti-virus detection and virus protection
- Anti-adware and advertisement avoidance
- Intrusion prevention and intrusion detection system
- Stateful firewall and Remote Manageability
- Auto update of virus signatures, web filtering, configuration, IPS-IDS rules, and adware links
- Remote Manageability
- Control of specific applications
- VPN for secured access to IT infrastructure via zero-trust network
- Geo-fencing
- MAC address filtering



Highlighted Features of zGuardian-NG

Enhanced Security

- Intrusion Detection and Prevention (IPS/IDS)
- Protects from Distributed Denial of Service (DDoS)attacks
- On-the-fly virus scanning and protection with more than 8 million of signatures
- Content filtering
- Safeguard from packet flood attacks
- Stateful Firewall
- SSL Inspection
- FQDN filter with allow/block list

Up-to-date Protective Measures

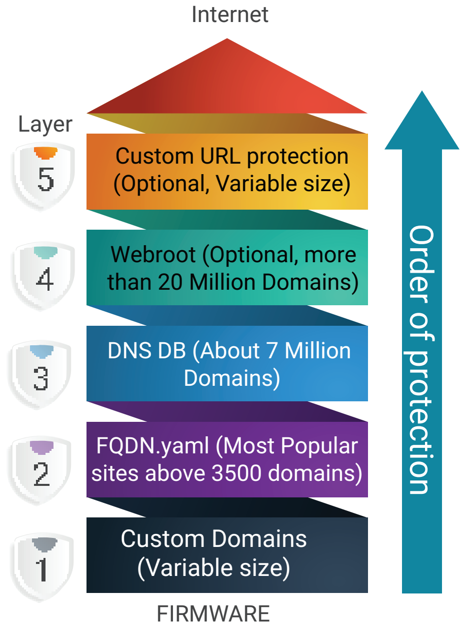
- Periodic updates of new virus signatures to guard your IT infrastructure from the latest virus attacks
- Smart update techniques for categorized domains/URLs from our repository without overloading the network links
- Synchronized rule updates from the common repository to enhance cybersecurity and up-to-date detection and prevention of modern cyber threats
- Demand-based updates of security rules to enhance cybersecurity
- Immediate updates based on policy changes in enterprises

Third-party Domain/URL Database Integration

- Allow or deny billions of sites based on the categories
- Easy configuration option to permit or block sites based on their risk/reputation
- Billions of domains and URLs categorized using modern tools including AI/ML
- Daily updates of databases ensure inclusion/exclusion and category changes of trillions of websites across the globe
- Powerful caching mechanism for high performance
- URL Filtering (Webroot): Web classification and Web reputation services with 87 categories, more than 4 billion IPV4 and IPv6 addresses history, about 1 billion categorized domains, 43 billion evaluated URLs

5 Layer Shield

- Smart high-speed protective layers
- 5 Layer protection scheme ensures complete cyber security without compromising the performance even in low-end zGuardian models
- Quick decision to allow or deny most popular sites using protective layer 2 without entering into layer 3 and above
- More than 7 million of in-built categorized domain database in layer 3
- Access to third-party domain databases of more than 20 billion entries
- Customized rules are allowed in layers 1 and 5


Internet
Layer
5
Custom URL protection (Optional, Variable size)
4
Webroot (Optional, more than 20 Million Domains)
3
DNS DB (About 7 Million Domains)
2
FQDN.yaml (Most Popular sites above 3500 domains)
1
Custom Domains (Variable size)
FIRMWARE
Order of protection

Seamless Network Management with SNMP

- Supports all the standardized SNMP protocols such as SNMPv1, SNMPv2c, and SNMPv3 for versatile, secure, and flexible device management
- Seamlessly monitors critical device parameters (e.g., traffic statistics, status alerts, and resource utilization) via SNMP
- Utilizes SNMPv3's encryption and authentication options to safeguard sensitive network data
- Configures settings and receives alerts for exceeded limits to ensure network reliability
- Works flawlessly with popular SNMP-based monitoring platforms (NMS, MIB browsers, etc.) to streamline IT infrastructure.

Application Control

- Flexibility to allow or deny certain applications based on their protocol
- Administrator can create policies to allow or block application traffic
- Supports application control with more than fifteen protocols such as SSH/FTP/SFTP/SMTP/MySQL/Telnet etc.

Centralized Management Solution (Director)

- Dashboard view of notifications and alerts of edge devices
- Automated or manual grouping of devices for hassle-free monitoring and management
- Bird's-eye view of Topology/Network of deployed ECs for the easiness in manageability of 100s to 1000s of numbers
- Easy edge device configurations and settings with a few clicks
- Real-time traffic statistics and link status
- Leveraging comprehensive analytics and advanced reporting features to provide actionable insights
- Administrator can take snap decisions based on alerts from the managed edge device
- Multi-language support

Network Management Solution (NMS)

- A light-weight management solution via well industry-standard SNMP v1, v2c and v3
- Automatically discovers edge devices via SNMP, ICMP, or custom IP ranges, using rule-based configuration for easy setup
- Organizes monitored devices into logical groups for streamlined management
- Geographic maps offer visualization of global infrastructure
- Custom-defined traps based on various thresholds and monitored values to activate alerts
- A built-in ticketing system for escalating incidents automatically upon receiving an alert
- Enhanced interfacing APIs to richer data exchange with Jira, ServiceNow, AmZetta Support Portal, and other ticketing systems
- Allows for flexible SLA adjustments based on time of day or workload, ensuring accurate SLA tracking
- Historical data reporting provides trend analysis, which aids in capacity planning and identifying performance issues

Productivity Conscious

- Blocks non-productive websites via URL/DNS filtering
- Nullifies lost hours by protecting computers and servers from old and new malware attacks
- Blocks adware which also reduces network traffic
- Protects IT infrastructure from DDoS attacks and hence avoids loss of productivity

Easy Deployment

- Plug-n-play edge deployment assisted by Zero Touch Configuration (ZTC)
- Easy cloning of security settings across multiple deployments using export/import configuration
- Optionally policy-driven configuration
- Hassle-free registration and visibility of edge devices

HW Minimum Requirements:

- Intel x86 CPU with 1.1 GHz
- 8 GB RAM
- 32 GB SSD

How to Get Started?

AmZetta offers free 30-day evaluation with no obligation to purchase. Simply visit https://AmZetta.com/Eval and complete the Evaluation Form. An AmZetta Solutions Engineer will help you get started with your evaluation.

AmZetta
AMZETTA.COM

HEADQUARTERS
AmZetta Technologies
5555 Oakbrook Parkway
Suite 280
Norcross GA 30093

Sales & Support
sales@amzetta.com
1-877-991-1809
support@amzetta.com
1-800-892-6625

INDIA
AmZetta Technologies Pvt. Ltd.
Kumaran Nagar, Semmenchery
Off Rajiv Gandhi Salai (OMR)
Chennai – 600 119

Sales & Support
sales@amzetta.co.in
support@amzetta.co.in
Tel: [91] 44 -61240022
1800-572-4061