

Wi-Jungle®

Unified Network Security Gateway



DataSheet – U350_(Rev1)



WiJungle Web Application Firewall appliance with machine learning architecture secures organizations against emerging network and applications threats. It is ideal for optimizing application performance by offloading compute intensive SSL transactions, and employing caching, compression etc. Being in industry, WiJungle very well understands necessities and challenges of different verticals like Enterprises, Hospitality, Education, Healthcare, BFSI, Transport, Retail, Defence etc. and helps them fulfil dynamic demands in highly cost-effective way along with Best Pre and Post sales services.

Specifications (OS 9.8)

Access/Interface Management

- Static, DHCP, PPPoE, PAP/CHAP Support
- Offers Inbuilt Database along with integration of Radius, TACACS/TACACS+, LDAP, SAML, NTLM, AD with authentication suite & Centralized Auth Solution
- Authentication, Authorization & Accounting, Support Thin Client, Setup multiple VLAN, Zones
- Admin/Users 2FA & 3FA via SMS, Email, GAuth, Twilio Authy etc.
- Software Bypass
- Certificate Management

Web & App Security

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Form Validations & Cookie Protection
- CSRF & Session Hijacking
- IP Reputation & Geo Location
- Data Leak Prevention
- Adaptive Profiling & Exception Heuristics (Positive/Negative Security Model)
- Website Cloaking
- Protocol Checks for HTTP and HTTPS traffic & Granular per Url/Parameter policies
- Web services signatures
- Protocol validations
- Brute Force Protection & Rate Control
- Web Defacement Protection & Suppression function

API Defence

- OWASP Top 10 API Security Risks
- XML/JSON protocol conformance & security
- Brute force Protection

Bot & DDOS Defence

- Web Scraping Protection
- Captcha Support
- Volumetric & Application DDOS Protection

Firewall Management

- Stateful / Stateless Inspection
- Access Rules & Thresholding
- DNS Domain Intelligence & Control
- Load Balancing & Content Routing
- Caching & Compression
- SSL Offloading, TCP Multiplexing & Optimization
- Anti Leech & Custom Scripting
- Auto Signature Update & Virtual Patching
- Multi-Level Policies
- Machine Learning based auto rules
- vLoc Support

Network Management

- Deployment in Router, Transparent, Bridge and Reverse Proxy Mode
- Detect/Prevent Mode, SPAN/TAP Mode, Packet Capturing
- NAT, Dyn. DNS
- Supports IP v4 & v6; NAT66, NAT64, DNS64; tunnel IPv6 over IPv4, IPv4 over IPv6
- Route - Static/Dynamic, OSPF/v3, BGP/v6, RIPv1/v2, IGMP, MLD, PIM, IS-IS, Babel, ECMP
- Layer 4/7 application routing policy and server persistence

Internet Links

- Supports two or more ISP Links
- Deliver combined bandwidth output (LAG)
- Define traffic priority to links (Active-Active)
- Ensure failovers - Redirect traffic to active gateways (Active-Backup)

Load Balancing

- Layer 4 & 7 load balancing
- Default load balancing like round robin, weighted round robin, least connections, shortest response etc
- Adaptive load balancing by CPU load, Memory, URL load etc
- Protocols – DNS, SSH, SMTP, IMAP, POP3, HTTP, HTTPS, FTP, SIP, RDP, RADIUS, MySQL, RTMP, RTSP etc supported
- Inbound and Outbound LLB
- Multiple health check target & Schedule support

Anti-Virus & Advance Threat Protection

- Virus, Worms, Trojan detection & Removal
- Spyware, Malware, Ransomware, Phishing, Bot, Pharming and C&C Attack Protection, IOC Intelligence (Optional)
- Dual Antivirus Engine (Optional), ICAP Integration
- Zero Day Protect: Cloud Sandboxing (Optional)
- Automatic Virus Signature Database Update
- Scans HTTP, HTTPS, FTP, SMTP/S, POP3, IMAP
- Block files based on their type.
- Threat Logs with action.

Intrusion Detection & Prevention

- Signatures: Default (25000+), Custom
- IPS actions: Recommended, Allow & Drop packet
- SCADA aware IPS with pre-defined category for ICS & SCADA signatures.
- Automatic Signature updates via Cloud Protocol Anomaly Detection

User Management

- Create User Groups & apply policies
- Social Media and Mobile No. based login
- ID & Password login - fixed users
- Easy Migration - Import/Export data
- Create users with auto-expiry, Renew & Block
- Live, Blocked and Total Users data
- Switch users from one group to other
- Restrictions based on device and OS.
- Set user session time, IP lease time
- Search sessions of a user via id/name, consolidated user and date wise

Captive Portal Capabilities

- 11 different types of captive portals
- Personalise Captive Page
- Customise captive form input fields
- Mobile/Desktop Responsive
- Social Media Based Login, MAC based auto login
- Promotions and Branding Options

Bandwidth Management

- Define Enhanced Quality of Service (QoS)
- Hierarchical Map

Content Filtering

- Web or URL (DNS and Certificate based) /IP/ Geography/Keyword/Port/Application Filter
- Block predefined categories on specific time Create | Edit | Delete Manual Categories & Add Exception

Alert Management

- Real-time alerts on Server Up/Down etc.
- Real-time alerts to admin on link failure, ISP speed, Remote Access etc.
- Schedule Alerts for specific reports
- Alerts on platforms like Slack, Flock, Skype, Telegram, Trello & Email

Reporting/Monitoring

- Graphical real-time logging and monitoring
- Daily/Weekly/Monthly Inbuilt & Custom Reports
- User, IP, Country, Protocol, Services, Bots, Internet, Threat, overall and user wise analytics
- Custom Query/Script Support
- Formats - PDF, CSV, HTML, Txt etc

Logging

- Connection Logs
- Audit Logs
- Access Logs
- Security logs
- Config Changes Logs
- Admin/User events

Highly User-friendly GUI

- Easy to operate/understand even by Non-Technical
- Create customizable view/dashboard
- English translation of every configuration

High Availability

- Active-Active (Load Share & Network Share)
- Active-Passive with state synchronizations
- Stateful Failover to Keep-Alive Sessions

Vulnerability Assessment (Opt.)

- Scans LAN Devices for vulnerability
- Generates summary and detailed reports of found possible threats

System Management

- System Configuration Backup/Restore/Erase
- Auto/Manual backup of User & Threat Logs
- Enable appliance access
- Set auto/manual firmware updates with rollback support
- Create Child Admins, Account Strength Policies and check logs
- Set Time Zone, NTP, SMTP Email
- Integrate Syslog, SIEM, SOAR, SNMP, Netflow; Port Mirroring
- Access via Web GUI HTTPS, Console, SSH, SFTP, Telnet & Centralized Management (Optional)

Troubleshoot

- Activity Timeline, DHCP Logs, Ping, Traceroute, DNS Lookup, Port Scan

Third Party Integration

- Third party application Integration

Custom Development

- Personalized development on request

Hardware

- Memory - 8 GB or higher
- SSD - 500 GB or higher
- Gbps Ethernet Ports - 8
- 1 Gbps/10 Gbps Fiber Ports (Optional) - 4
- 2 USB Ports, 1 VGA, 1 COM

Power and Reliability

- 220W Power Supply with redundancy (Optional)
- Operating T - (-10°C~60°C), Storage T - (-20°C~80°C)
- Relative humidity - 5%-95%, no condense
- Vibrate - 0.5g rms/5-500HZ/random/operating

Performance

- Inspected L7 Throughput - 42 Gbps
- IMIX L7 Throughput - 26 Gbps
- Max L7 Mitigation Throughput - 10.7 Gbps
- L4 Requests Per Sec - 2,100,000
- L7 Requests Per Sec - 1,000,000
- L4 Concurrent Sessions - 12,400,000
- SSL/TLS TPS – 20K (RSA 2K), 12K (ECDHE)
- Latency – <5 micro seconds

Support

- 24*7 Call, Web Chat and Email Support