

# Wi-Jungle®

Unified Network Security Gateway



## DataSheet – IPS-U500



WiJungle Intrusion Prevention System appliance with machine learning architecture secures organizations against emerging network and applications threats. It inspect complete inbound and outbound layer with its anomaly detection and user behaviour detection system in fast and precise detection and mitigation of threats. 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 11.2)

## Access/Interface Management

- Static, DHCP, PPPoE, PAP/CHAP Support
- Offers Inbuilt Database along with integration of Radius, TACACS/TACACS+, LDAP, SAML, AD with authentication suite & Centralized Auth Solution
- Authentication, Authorization & Accounting, Support Thin Client, Setup multiple VLAN, Zones, 803.1P, 803.1S, Location aware access, BYOD
- Clientless Device, IP-Mac bind, MAC Whitelist/Blacklist with auto-expiry.
- Admin/Users 2FA & 3FA via SMS, Email, GAuth, Twilio Authy etc.
- Software Bypass

## Intrusion Detection & Prevention

- Signatures: Default (35000+) & Custom
- Bi-Directional Inspection
- SCADA aware IPS with pre-defined category for ICS & SCADA signatures.
- Dynamic Context Detection i.e. protocol, application and file type
- Vulnerability Exploit Detection & Prevention
- DDoS Protection, App Aware Policies
- Detection of Port Scan, Callback activities using FFSN, Malware Scan etc
- Reconnaissance i.e. TCP/UDP/ICMP scan, stealth and slow detection in IPv4 and IPv6, Correlation
- Protocol Anomaly Detection
- Drop/Allow/Reject/Alert/Capture Action, HTML response & HTTP redirect
- File Filtering & Reputation , Anti-Evasion
- Passive Endpoint Detection, IOC Intelligence
- Automatic Signature updates via Cloud

## Bot Defence

- Block or Alert users about botnet sites
- Message length sequence analysis

## Access Rules

- IP Intelligence & Control
- Block/Allow Bulk IP Addresses
- Geo Location Control
- DNS Domain Intelligence & Control
- Access Control List

## SSL Inspection (Decryption)

- Advanced TLS Stack
- Hardware acceleration
- Cipher Analysis: RC4, DES, 3DES, AES-CBC, AESGCM, AES-GMAC, RSA, DSA, DH, ECDSA, ECDH, MD5, SHA, SHA2 etc

## Network Management

- Deployment in Gateway and Inline 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
- PB Routing, LLDP, HDLC, Upstream & Web Proxy

## 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

## Load Balancing

- 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)

## High Availability

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

## Anti-Spam

- Inbound and Outbound Scanning
- IP & Domain Black list/White list
- Real time blacklist, MIME header check

## Vulnerability Assessment

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

## 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)
- 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.

## User/Guest 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

## Voucher Management & PMS

- Instant voucher generation in printable formats, Prepaid & Postpaid billing
- PMS/HIS integration
- Create cash & cashless vouchers based on policy
- Voucher generations based on room type
- Switch user from one policy to another on same voucher
- Reporting based on room and voucher

## Bandwidth Management

- Restrict Users based on data, b/w & time
- Define Enhanced Quality of Service (QoS)
- Individual and Shared Bandwidth Quota
- Configure multiple b/w policy on a user at different hours of day

## Package Management

- Create Hourly and Day based Plans
- Set renew as automatic & Manual
- Configure conference/banquet hall plans
- Accounting based on hours, days, data transfer

## Alert Management

- Real-time alerts to user on data consumption limit, voucher expiry 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
- Change Logs, Daily/Weekly/Monthly Reports
- User, IP, Country, Protocol, Services, Bots, Internet, Threat, overall and user wise analytics
- Formats - PDF, CSV, HTML, Txt etc

## Surfing Logs

- Records surfing logs of each user
- Inbuilt storage for a complete year
- Search logs based on time, user, IP and site

## Highly User-friendly GUI

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

## System Management

- System Configuration Backup/Restore/Eraser
- Auto/Manual backup of User & Threat Logs
- Enable appliance & PMS remote access
- Set auto/manual firmware updates
- Create Child Admins and check logs
- Set Time Zone, NTP, SMTP Email
- Integrate Syslog, SIEM, SOAR, SNMP, Netflow; Port Mirroring & Central Management
- Access via Web GUI HTTPS, Console, SSH, SFTP, Telnet

## 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 - 12/16 GB
- HDD/SSD - 500 GB
- 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 IPS Throughput – 11.2 Gbps
- Real World Throughput – 10.6 Gbps
- SSL Inspection Throughput – 8.6 Gbps
- Concurrent Sessions - 20,000,000
- New Sessions Per Sec – 200,000
- Latency – <60 micro seconds

## Support

- 24\*7 Call, Web Chat and Email Support