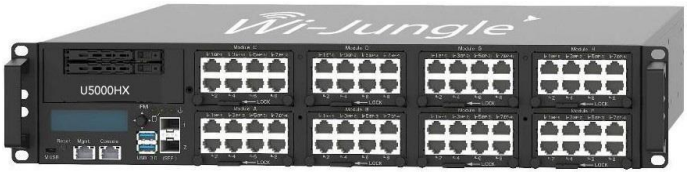
Wi-Jungle®

Unified Network Security Gateway



DataSheet - IPS - U5000HX

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.

www.wijungle.com

Specifications (OS 9.8)

Access/Interface Management
- Static, DHCP, PPPoE, PAP/CHAP Support
- Setup multiple VLAN, Zones
- Clientless Device, IP-Mac bind, MAC Whitelist/Blacklist with auto-expiry.
- Admin 2FA & 3FA via SMS, Email, GAuth, Twilio Authy etc.
- Software Bypass

Intrusion Detection & Prevention
- Signatures: Default (98000+) & Custom
- 65+ Predefined Signature Categories
- 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
- 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 & Behaviour Detection
- Drop/Allow/Reject/Alert/Capture Action, HTML response & HTTP redirect, Host Quarantine
- File Filtering & Reputation, Anti-Evasion, Anti-Spoof, Risk Threat Prioritization
- Passive Endpoint Detection, IOC Intelligence
- MS Office and PDF files specialized deep packet inspection
- Integrated Machine Learning Capabilities with self learning and signature less engines
- Automatic Signature updates via Cloud

Bot Defence
- Block or Alert users about botnet sites
- Message length sequence analysis
- Heuristic Analysis, C2C & DNS Sink Holing

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, Simulate 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

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

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)
- Mobile threat reputation & cloud analysus (Optional)
- Automatic Virus Signature Database Update
- Scans HTTP, HTTPS, FTP, SMTP/S, POP3, IMAP
- Block files based on their type.
- Threat Logs with action.

DoS & DDos Prevention
- Threshold & Heuristic based detection
- Host based connection restrictions

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
- IP, Country, Protocol, Services, Bots, Internet, Threat, overall and user wise analytics
- Formats - PDF, CSV, HTML, Txt etc

Surfing Logs
- Records surfing logs
- Inbuilt storage for a complete year
- Searchable logs

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

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

System Management
- System Configuration Backup/Restore/Erase
- Auto/Manual backup of Threat Logs
- Set auto/manual firmware updates
- Create Child Admins and check logs
- Option to create Dedicated HA Port
- Centralized Management (Opt.)
- Set Time Zone, NTP, SMTP Email
- Integrate Syslog, SIEM, SOAR, SNMP, NetFlow; Port Mirroring
- Access via Web GUI HTTPS, Console, SSH, SFTP, Telnet

Troubleshoot
- DHCP Logs, Ping, Traceroute, DNS Lookup, Port Scan

Third Party Integration
- Third party application Integration

Custom Development
- Personalized development on request

Hardware
- Memory - 80 GB, SSD - 1TB or higher
- Ports - 8*1G Copp., 4*1G SFP incl 4 pair bypass & 2*10G SFP +
- Flexi Slots - 8 (8*1G Copper or SFP/4*1G Copper or SFP/4*1G Copper + 4*1G SFP/4*10G SFP+/2*10SFP+/2*40G QSFP/1*100G QSFP+)
- 2 USB Ports, 1 VGA, 1 COM

Power and Reliability
- 550W with Redundant Supply (Optional)
- Operating T (0°C~40°C), Storage T (-20°C~80°C)
- Relative humidity - 0%-90%, no condense
- Vibrate - 0.5g rms/5-500HZ/random/operating

Performance
- Inspected IPS Throughput – 72 Gbps
- Real World Throughput – 61.6 Gbps
- SSL Inspection Throughput – 27.2 Gbps
- Concurrent Sessions - 70,000,000
- New Sessions Per Sec – 900,000
- Latency – <60 micro seconds

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