WIBORNE, INC.

Wireless LAN Gbits-Based Secure Hotspot Controller: HSG-500

The HSG-500 is a full-featured Wireless LAN Gbits Ethernet security controller that aggregates up to 60 access points (APs), built-in 5000 local accounts / 5000 on-demand accounts and delivers centralized control and security for wireless deployments.

The HSG-500 is designed for applications in which a compact, cost-effective" all-in-one" networking solution is required. The HSG-500 included a policy forced firewall, Intelligent Dual-WAN Load balance; Wireless LAN controller, IP sharing, and 4-Gbits Ethernet switch in a desktop-mount enclosure. This device centralized configuration and management model enables the controllers to be deployed, monitored, and controlled without local IT staff.

The HSG-500 applies to public access network such as WiFi-Hotspot, network management guest access, hospitality deployments – which require reliability, efficiency, and security. It combines an IP Router / Firewall, Multi-WAN / QoS enforcement and Access Controller for use in wireless environments. One single HSG-500 can serve up to 500 simultaneous users, takes control over authentication, authorization, accounting and routing to the Internet as well as to the operating central. Built-in AAA system allows the owners set up public access services without extra RADIUS server.

● Centralized Access Points Management

Through HSG-500, all WiBorne Managed Access Points are managed through a unified Web interface. Make sure all Managed Access Points are under good conditions. It is a simple task to keep the firmware of Managed Access Points up to date. The device management is especially important for a wide area deployment.

- Secure Authentication, Encryption, and Access Control
- Network Management
- Quality of Service
- Centralized Wireless LAN Management

● Wireless and Wired Access Controller

Multiple Authentication Methods and Accounting

HSG-500 Wireless Controller provides authentication, authorization and accounting for a wired/or wireless networks. Hotspot technology allows Internet providers to offer Internet access to customers, while applying certain Internet use rules and limitation. It is convenient for Internet cafes, hotels, airports, schools and universities. The Internet provider gets complete tracking records of per customer time spent on the network, data amount sent / received, real-time accounting and more.

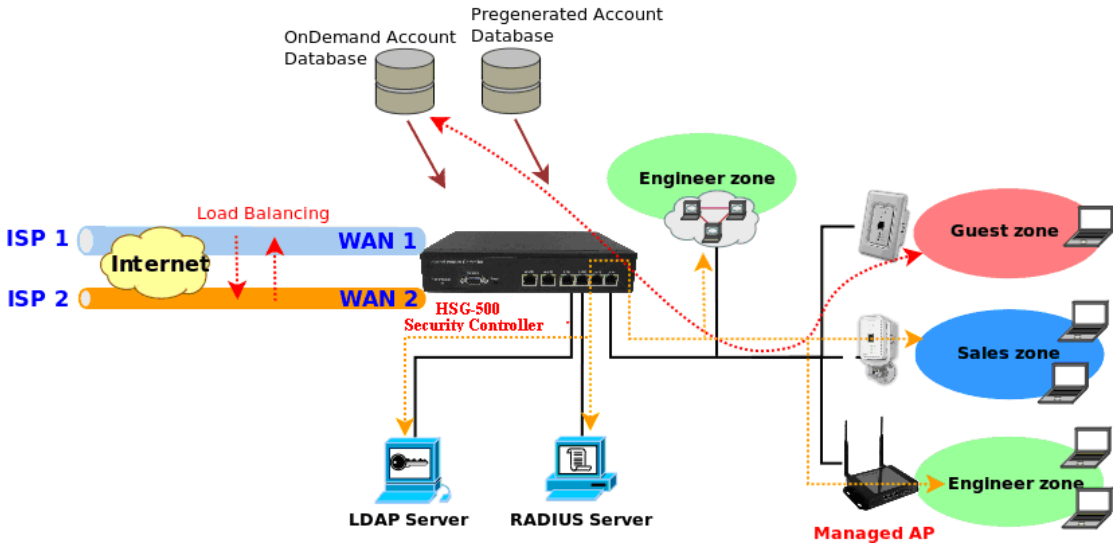
To begin browsing, a client must go through a registration process with the provider, and then enter a Passcode of

WiBorne Take your wireless airborne.
WiBorne, Inc. www.wiborne.com
sales@wiborne.com

USA Office:
4790 Irvine Blvd., Suite105-458,
Irvine, CA 92620
Tel: 1-949-903-8502
Fax:1-949-252-0888

Taiwan Office:
No.5, Qiyan Rd., Beitou District,
Taipei City 112, Taiwan
Tel: 886-2-2898-4050

access ticket in a browser Login window that appears on the attempt to open a webpage. Hotspot technology proposes providers to establish and administrate a user database, which can be useful for enterprise such as airports, hotels or universities that offer wireless or Ethernet Internet connectivity to employees, students, guests or other groups of users.



- **Customizable Login**

Service provider can benefit from the flexible web redirection service. HSG-500 provides a set of location, browser, and user-specific information to the backend system to enable value added personalized service provided by the WISP. Detailed location information is available via HTTPS / XML interfaces. Web pages can be either stored locally on the HSG-500 or remotely on a web portal server.

- **Zero Configuration for Users**

HSG-500 makes Internet access very easy and user-friendly. Users will be redirected to the provider's welcome page automatically regardless of their PC configuration. The IP Plug and Play feature will accept and translate fixed company IP settings and web proxy configurations, so that users do not have to reset their corporate IP or web settings. Outgoing user's e-mails can be redirected to the operator's mail server in order to facilitate to e-mail forwarding for foreign subscribers. The recipient sees the messages as it was sent from the users' home provider.

- **Service Domain**

For Office: A single HSG-500 can manage the wired and wireless network access uniformly. The users from different departments and guests can be partitioned 8 different Service Domain (Virtual Network).

For WISP / Hot Spot Public Area (Multi WISP Roaming): HSG-500 can serve subscribers from multiple service providers through its integrated roaming method. Beyond the RDIUS roaming, HSG-500 supports up to 8 Virtual Network allowing network operators to define AAA or IP policies via WISP/VLAN.

- **Multi-WAN Support**

Outbound Load-Balancing: With real-time load balancing and Optimum Route algorithm, HSG-500 intelligent router engine directs each session or connection to the best available link. It also supports policy-based routing, persistent routing, and traffic scheduling to effectively adapt your business policy into your network policy.

Fault Tolerance: The network health check engine monitors the network around the clock and provides fail-over /fail-back functions.

- Fail-Over: Whenever a link fails or is unstable, traffic is automatically re-routed to other healthy and available links to ensure uninterrupted connectivity
- Fail-back: When the faulty link resumes function, on-line traffic is redistributed across all available connections to optimize the networks.

Flow Control

Policy Based Bandwidth Management: By filtering out unexpected traffic, HSG-500 optimizes bandwidth utilization and ensures the best transmission quality for the transfer of mission-critical data. Built-in QoS function in HSG-500 has the advantage of integrating bandwidth management across Dual WAN links.

Policy-Based Access Control List: Firewall access policies are user definable and can be based on source or destination, type of service, and IP address. It is also implemented in conjunction with traffic scheduling policy. HSG-500supports specific Layer-7 protocols such as P2P, IM, and H.323 for better network management

Protocols Traffic Management: HSG-500 is capable of analyzing and managing many layer-7 protocols such as VoIP protocols (H.323 and SIP), Video Conferencing, ERP, and various IM protocols. With such layer-7 filtering (or scan) capability, HSG-500 empowers business communications and improves efficiency by providing network quality of service management.

Content Blocking / Protection Service: The HSG-500 provides Content Blocking feature to block specific URL, Scrip, IM, P2P and download file. Also, it has built-in Anomaly Flow IP function. This function supports Hackers and Blaster Alerts. An administrator could use this function to watch and track and attacker. Also, the QoS function provides Bandwidth Control and Bandwidth Priority Utilization.

Quota: As broadband usage proliferates coupled with the alarming rise of file sharing trend, in certain cases, it is important to assign quota for user bandwidth consumption, particularly in the education institutions, hot spots, or in a community with shared Internet access provider subsystem.

HSG-500 supports two different quota mechanisms: *prepaid* and *periodical*, in order to meet different real-life business needs. The quota system can also be integrated with external accounting and billing systems.

Auditing

Client Session control, IP and bandwidth monitoring, network latency, serve logs

Firewall

Both the NAT mode and DMZ mode are supported that they can maintain the existing network infrastructure without reconfiguring. The HSG-500 provides policy-based firewall protection and several hacker protections to prevent network managers to enhance the security of local network easily.

Specification

- **Access Point Management and Support**
  - HSG-500 Access Controller Supports:
    - Max: 60 Access Points per Controller
    - Max: 500 wireless client per Controller

- Provide Local Account: 5000

- AP Management -Control-Monitoring
  - Centralized AP Management
    - AP Group management –maintain a set of setting templates that simplify the task to assign the same setting to multiple APs
    - AP-Automatic configuration and provisioning by HSG-500
    - Locally maintained configuration profiles for managed APs
    - Auto discovery for managed APs
    - Automatic recovery of APs in case of system failure
    - Central firmware Upgrade-Select multiple APs and upgrade their firmware at the same time, including bulk upgrade
    - Remote Firmware upgrade
    - Zero configuration technology to restore broken AP's setting onto its replacement AP
  - Central AP Control
    - Provides MAC address Control list of client stations for each managed APs
    - Access Filter
    - Time-based AP access control
    - Single UI for upgrading and restoring managed APs' firmware
    - WLAN Partition – if enabled, WLAN clients are not allowed to exchange data through the AP (WAP-100, WAP-981X, CAP-2410D, CAP-5015D series)
    - Max allowed APs
    - Support Roaming – Intra-Switch, Inter-band, Inter-Switch
  - Central AP Monitoring
    - Monitor AP Status
    - The number of associated clients to the AP
    - The AP RF information
    - Associated Station List
    - Monitoring IP List
    - Load balancing based on number of users
    - Load balancing based on utilzation
    - AP User Statistic –Maintain all wireless clients connection history and depict statics in diagrams
    - Support Monitor IP on third-party APs
    - Alert-Summarize abnormal status in the alert window
    - System alarms and status reports on managed APs: WiBorne Topology Monitor-list monitored device; periodic update on device status
    - AP life check-real time tracking monitors APs status (AP Health Checking)
  - Provide centralized remote management via HTTP/SNMP interface
  - Support MIB's: 802.11, 802.1X, MIBII, RADIUS authentication, RADIUS Accounting
  - SYSLOG support including remote servers
  - Log-system log: operator action log

- Radio Resource Management
  - Automatic Channel Assignment and power setting for controlled APs
  - Simultaneous air monitoring and end user service
  - Self-healing coverage based on dynamic RF condition
  - Dense deployment options for capacity optimizations
  - Multiple BSSID per Radio: 8
  - Hot Standby at AP mode (support fail-over a standby AP)
  - Load Balance to another available AP (Real time users limitation)
  - Radio Management
  - Coverage interference detection

- Convergence
  - 8 Hardware queues per port
  - IEEE802.11p Class of Service/Quality of Service (CoS /QoS)
  - IEEE802.11e Wi-Fi Multimedia (WMM)
  - 8 BSSID per radio
  - Differv Codpoint (DSCP)

- Wireless Encryption
  - WPA personal and enterprise

- WPA2 personal and enterprise
- AES(CCMP): 128bit (FIP-197)
- WEP40/64 and 104/128-bit
- TKIP: RC4-40
- SSL and TLS: RC4 128-bit and RSA1024 and 2048 bit
- EAP-TLS, EAP-TTL/MSCHAPv2

- Wireless Security
  - IEEE802.1X network login user authentication (EAP-MD5/TLS/TTLs)
  - EAP over LAN(EAPoL) transport with PEAP and EAP-TLS authentication
  - RADIUS server authentication (RFC2618)
  - IEEE802.1X user authentication of controller management on controller Telnet and console sessions
  - Multiple access privilege levels
  - Hierarchical management and password protection for management interface
  - EAP offload for AAA server scalability and survivability
  - Stateful 802.1x authentication for standalone APs
  - SSID and Location based authentication
  - Multi-SSID support for operation of Multiple WLANs
  - Simultaneous Centralized and distributed WLAN support
- Identity –Based Security
  - 802.1x Authentication with WPA,WAP2 and 802.11i
  - Local Accounts of 802.1x Authentication
  - Support Radius /LDAP for AAA server
  - User Name and encryption key binding for strong network identity creation
  - Local User Data Base for AAA failover protection
- Wireless Roaming Support
  - Inter AP roaming
  - Fast roaming
  - L2 roaming

- **User Management**
  - Support 500 simultaneous authentication users
  - Max 5000 Pregenerated/ON-demand/Local RADIUS / authentication users
  - Users Session Management
  - Configurable user Black list (with Time-based control)
  - Allows MAC address and user identity binding for local user authentication
  - Authentication methods supported: Pre-generated/On-Demand/local RADIUS, LDAP and Remote RADIUS
  - SSL protected login portal page
  - Session idle timer
  - Login Session idle time out setting
  - Session and account expiration control
  - User Log and traffic statistic notification via automatically email service
  - Login time frame control
  - Session limit
  - Real-Time Online Users Traffic Statistic Reporting
  - Support local account roaming
  - Seamless Mobility: User-centric networking manages wired and wireless users as they roam between ports or wireless APs
- **Service Domain**
  - Integrating with WAP-100, WAP-981X, CAP-5015D, CAP-2410D to have Service Domain feature, each Service Domain can have its own settings: The network is divided into maximum 8 groups, each defined by VLAN Tag and ESSID. Each Domain has its own (1) login portal page (2) authentication options (3) LAN/VLAN interface IP address range (4) Session number limit control (5) Traffic shaping (6) IP Plug and Plan (IP PnP) (7) Multiple Authentication
  - Each Domain allows access to the selected groups
  - Each Domain assigns a network policy to each user group
  - NAT or Router mode
  - Enable DHCP or not, and DHCP address range
  - Enable authentication or not
  - Types of authentication options in one Service Domain (Local, RADIUS, LDAP, On-Demand and

Pre-Generated)
- Web login /logout /redirected page (customizable)
- Default Policy
  - NAT or Route Mode
  - Specific Route (WAN1 or WAN2, or a specified gateway)
  - Login schedule
  - Bandwidth (max. min)

- **Authentication**
  - Authentication: single sign-on (SSO) client with authentication integrated into the local authentication environment through local/domain, LDAP, RADIUS, MAC authentication, and 802.1x.
    - Customizable Login and Logout Portal Pages
    - Customizable Advertisement Links on Login Portal Page
  - User authentication with UAM (Universal Access Method), 802.1x / EAPoLAN, MAC address
  - Allow MAC address and users identity binding for local uer authentication
  - No. Of Registered RADIUS Servers: 2
  - Support MAC control list (ACL)
  - Support Multiple Login service on one Account
  - Support auto-expired guest accounts
  - Users can be divided into user groups
  - Each user group has its own network properties, including bandwidth, QoS, WMM traffic
  - Each group (role) may get different network policies in different srvice zones
  - Max simulanous user session (TCP/UDP) limit
  - Configurable user black list
  - Export/Import local users list to/from a text file
  - Web-based Captive Portal for SSL browser-based authentication
  - Authentication Type
    - IEEE802.1X(EAP,LEAP,EAP-TLS,EAP-TTLS,EAP-GTC,EAP-MD5)
    - RFC2865 RADIUS Authentication
    - RFC3579 RADIUS Support for EAP
    - RFC3748 Extensible Authentication Protocol
    - MAC Adress authentication
    - Web-based captive portal authentication
- **Authorization**
  - Access control to network resource such as protected network with intranet, internet, bandwidth, VPN, and full stateful packet
- **Accounting**
  - Provides billing plans for pre-setting accounts
  - Provides billing plans for on-demand accounts
  - Enables session expiration control for On-demand accounts by time (Hours) and data volume (MB)
  - Detailed per-user traffic history based on time and data volume for both local and on-demand accounts
  - Support local on-demand and external RADIUS server
  - Contain 10 configurable billing plans for on-demand accounts
  - Support credit card billing system by Authorize.net and PayPal
  - Provide session expiration control for on-demand accounts
  - Support automatic email network traffic history
- **Dual WAN**
  - Load Balancing
    - Outbound Fault Tolerance
    - Outbound loadbalance
    - Multiple Domain Support
    - By Traffic
  - Bandwidth Management by individual and users group
  - WAN Connection Detection
- **QoS Enforcement**
  - Packet classification via DSCP (Differentiated Services code Point)
  - Control Policy by IP/IP Ranges/MAC Group/Service
  - No. of Max. Policy setting: 10
  - Layer-7 Protocol Support

- Traffic Analysis and Statistics
- Diff/TOS
- IEEE802.11p/COS
- IEEE 802.1Q Tag VLAN priority control
- IEEE 802.11e WMM
- Automatic mapping of WMM priorities to 802.1p and IP DSCP
- IGMP Snooping for efficient multicast delivery
- Upload and Download Traffic Management

- **Firewall**
  - Built-in DoS attack protection
  - Inspection Full stateful packet filter
  - Access Control List
  - Layer 7 Protocol Blocking
  - Multiple Domain Support
  - Active Firewall Session – 16,000
- **Network**
  - Support NAT or Router Mode
  - Support static IP, Dynamic IP (DHCP Client), PPPoE and PPTP on WAN connection
  - DHCP Server per Interface; Multiple DHCP Networks
  - 802.3 Bridging
  - Proxy DNS/Dynamic DNS
  - Support NAT
    - IP/Port destination redirection
    - DMZ server mapping
    - Virtual server mapping
    - H.323 pass-through
  - Built-in with DHCP server
  - Support Static Routing
  - Binding VLAN with Ethernet and Wireless interface
  - Support MAC Filter
  - Support IP Filter
  - Support Walled garden (free surfing zone)
  - Support MAC-address and IP –address pass through
  - Support IP Plug and Play (IP PnP)
- **System Administration**
  - Three administrator accounts
  - Provide customizable login and logout portal page
  - CLI access (Remote Management) via Telnet and SSH
  - Remote firmware upgrade (via Web)
  - Utilities to backup and restore the system configuration
  - Full Statistics and Status Reporting
  - Real time traffic monitor
  - Ping Watchdog
- **Network Management**
  - Even Syslog
  - Status monitoring of on-line users
  - IP-based monitoring of network devices
  - Interface connection status
  - Support Syslog for diagnosing and troubleshooting
  - User traffic history logging
  - User's session log can be sent to ftp or Syslog server
  - Remote Syslog reporting to external server
  - SNMP v1, v2c, v3
  - SNMP TrAPs to a list of IP Address
  - Support MIB-II
  - NTP Time Synchronization
  - Administrative Access: HTTP / HTTPS

HSG-500 Hardware Specifications	
Base Platform	32-bit, MIPS24K Processor
CPU Clock Speed	680 MHz
Serial Port	1 (DB-9)
USB Port	1 (reserved for ODM request)
Reset Switch Built-in	Push-button momentary contact switch
Ethernet Configuration	10/100/1000 BASE-TX auto-negotiation Ethernet ports x 6 (RJ-45 connector): WAN * 2; LAN * 4
DRAM	On board: 256Mbytes
Flash	On board: 32 Mbytes
CF Socket	1 (reserved for option)
Built-In LED Indicators	1* Power; 1*Status,1 Net Status (for AP management, when system can't detect managed AP)
Environmental & Mechanical Characteristics	
Operating Temperature	0 °C ~ 55 °C
Storage Temperature	-20 °C ~ 75 °C
Operating Humidity	10% to 80% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Power Supply	110 – 220V AC Power ; 12 VDC, 1.5A input.
Unit Dimensions	243 x 150 x 45.5 (mm) (Width x Depth x Height)
Unit Weight	1.4 Kg
Form Factor	Wall Mountable, Metal case
Certifications	FCC / CE

WiBorne
Take your wireless airborne.
WiBorne, Inc. www.wiborne.com
sales@wiborne.com

USA Office:
4790 Irvine Blvd., Suite105-458,
Irvine, CA 92620
Tel: 1-949-903-8502
Fax:1-949-252-0888

Taiwan Office:
No.5, Qiyan Rd., Beitou District,
Taipei City 112, Taiwan
Tel: 886-2-2898-4050