

## Cipherium B3000



**B3000 is a high-performance, cost-effective office network appliance specifically designed for SMBs, branch offices, and remote users, delivering an integrated solution to address the needs for wireless access, remote access, security, and manageability.**

### Key Features –

*Integrated AAA support*

*WAN Failover*

*Multiple authentication methods*

*Guest accounts for visitors*

*Role-based and policy-based access control*

*Per-user bandwidth management*

*Wireless & wired clientless VPN*

*Multiple types of VPN connection*

- Local VPN
- Client-to-site
- Site-to-site

*AP Management*

## Features & Benefits –

### Simplified Deployment and Administration

- Seamless integration into existing wireless and wired network
- No change of configuration is required on client devices
- Customizable login portal page to control the authentication process
- Ability to manage the entire corporate network from a single point
- Ease of maintenance eliminates ongoing administration costs

### Comprehensive Security Features

- Integrated user authentication based on industry standards
- Authorized end-to-end communication for both wireless and wired networks
- Standards-based encryption capabilities ensure data privacy to user's device
- Local VPN termination with clientless approach provides the highest level of wireless security without any hassle
- Clientless approach provides the ease of use to establish remote VPN access (client-to-site)
- Site-to-site VPN connection to provide cost-effective and secure connection among different branch offices
- Configurable packet filtering policies enhance the control of data traffic

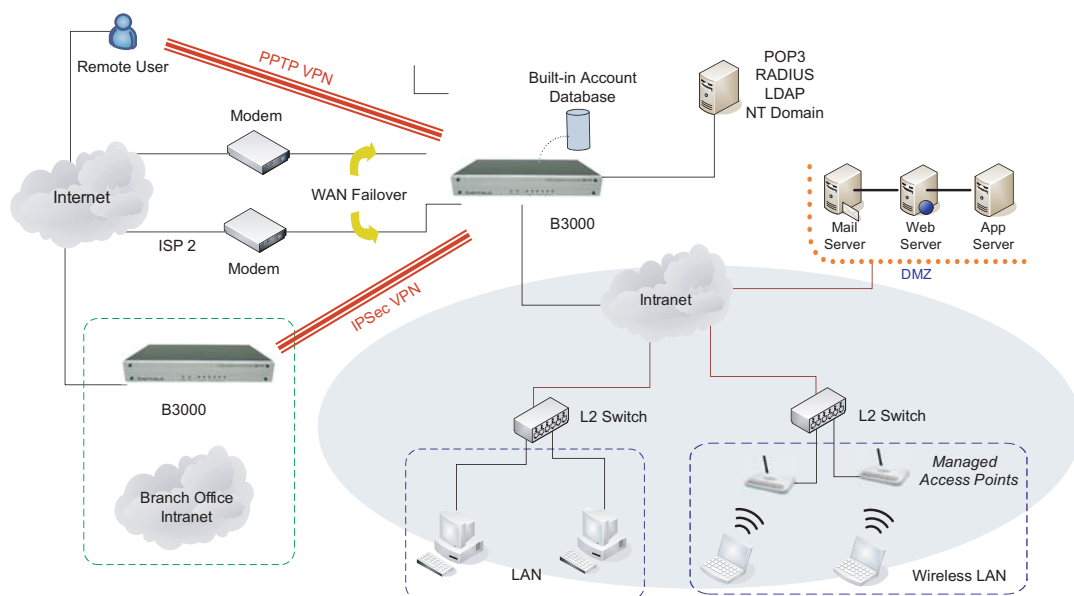
### Effective User Management

- Simultaneous support for internal and external user authentication options
- Easy management of guest access to wireless network
- Policy-based control approach enhances the management of multiple categories of users
- "On-line user list" monitors real-time status of each individual user
- Per-user bandwidth limiting enables flexible traffic control for different scenarios
- Provides detailed per-user traffic history log for analysis and record keeping

### Centralized AP Management

- Centralized remote control of managed APs avoids the need to individually configure each device
- "Automatic discovery" function can identify manageable APs and enroll them to the device list
- Remote status monitoring of managed APs and associated client stations ensures efficient network resource utilization
- Provides system alarms and statistics reports on managed APs

## Target Deployments –



IPsec VPN Encrypted Network

# Multi-Service Business Gateway

## Cipherium B3000

### Networking

- Supports Router, NAT mode
- Supports Static IP, DHCP, PPPoE mode on WAN interface and PPTP (WAN 1 only)
- Controlable LAN ports requiring authentication
- Supports IP Plug and Play (IP PnP)
- Built-in DHCP server and support for DHCP relay
- Supports NAT:
  - (a) IP/Port Destination Redirection
  - (b) DMZ Server Mapping
  - (c) Virtual Server Mapping
  - (d) H.323 Pass-Through
- Supports static route
- Supports SMTP redirection
- Supports WAK on LAN, Dynamic DNS
- Walled Garden (free surfing zone): 20
- Supports MAC Address Pass-Through
- HTTP Proxy Servers: 10
- Supports SIP / NAT pass through (future release)
- Local balancing on dual WANs (future release)

### Security

- Supports data encryption: WEP (64/128-bits), WPA, WPA2
- Supports authentication: WPA-PSK, WPA2-PSK, IEEE 802.1x (EAP-MD5, EAP-TLS, CHAP, PEAP)
- Local VPN of IPSec tunnels to enhance wireless security: 120
- Client-to-stie VPN of PPTP over public Internet: 10
- Site to site IPSec tunnels over public Internet: 10
- Supports VPN Pass-Through (IPSec and PPTP)
- Supports built-in DoS attack protection
- Supports MAC Access Control List
- Supports user Black List: 5 lists x 40 sets
- Allows MAC address and user identity binding for local user authentication
- Supports QoS and WMM (future release)

### AP Management

- Centralized remote management via HTTP interface
- Automatic discovery of managed APs and list of managed APs
- Allows administrators to add and delete APs from the device list
- Allows administrators to enable or disable managed APs
- Provides MAC Access Control List of client stations for each managed AP
- Locally maintained configuration profiles of managed APs
- Single UI for upgrading and restoring managed APs' firmware
- System status monitoring of managed APs and associated client stations
- Automatic recovery of APs in case of system failure
- System alarms and status reports on managed APs
- Supports Monitor IP on third-party APs

### Monitoring and Reporting

- Status monitoring of on-line users
- IP-based monitoring of network devices
- WAN connection failure alert
- Supports SYSLOG for diagnosing and troubleshooting
- User traffic history log
- Detailed per-user traffic history based on time and data volume for both local and guest accounts
- Traffic history report in an automatic email to administrator

### System Administration

- Multi-lingual, web-based management UI
- Customizable login and logout portal page
- SSH remote management
- Remote firmware upgrade
- NTP time synchronization
- Console management interface support (CLI)
- Backup and restore of system configuration
- SNMP v2 support

### User Management

- Simultaneous support for multiple authentication methods (Local, POP3(s), LDAP, RADIUS, and NT Domain)
- Policy-based access control (including Firewall policies, Routing, Login Schedule, and Bandwidth)
- Role-based access control (based on policy setup from above)
- Supports time-based firewall policy (future release)
- User Session Management:
  - (a) SSL protected login portal page
  - (b) Supports multiple logins with one single account
  - (c) Session idle timer
  - (d) Session/account expiration control
  - (e) Notification email to provide a hyperlink to login portal page
  - (f) Windows domain transparent login
  - (g) Configurable login time frame
- Instant guest account generation by authorized users without IT's intervention
- RADIUS class and policy mapping

### Hardware Specifications

- Form Factor: Mini book
- Dimensions (W x D x H): 300 mm x 175 mm x 45 mm
- Weight: 1.4 Kg
- Operating Temperature: 0 ~ 45 °C
- Storage Temperature: 0 ~ 65 °C
- Power: 110~220 VAC, 50/60 HZ
- CPU: Intel IXP 425, 533 Hz
- Flash: 32MB
- SDRAM: 128MB
- WAN Ports: 2 x 10BASE-T/100BASE-TX RJ-45
- LAN Ports: 4 x 10BASE-T/100BASE-TX RJ-45
- Console Port: 1 x RS-232 DB9
- LED indicators: 1 x Power, 1 x Status, 2 x WAN, 4 x LAN
- Certifications: CE, FCC
- RoHS compliance: Yes

### Capacity and Performance

Concurrent Users	120
Local Accounts	500
Guest Accounts	500
Managed Access Points (A300)	12
Monitored 3rd-party Access Points	40
VPN Termination Tunnels	120
VPN 3DES/DES Throughput	30 Mbps

