Secure Extended LANs For Access Control

BeLine
info@belinelocks.com
www.belinelocks.com

Industrial Security Compliances

- FIPS 140-2 - Federal Information Protection Security
  - Encryption, Roles, Physical Security, Operations Security, Attack Mitigation
  - End to End system compliance
- PCI - Payment Card Industry
  - Need to Know Access, Wireless IDS, Auditing, Operations Security
- HIPAA – Healthcare Information Portability and Accountability Act
  - Healthcare Electronic Data Exchange Standards
- GLBA - Graham-Leach Bliley Act – Federal Trade Commission Consumer Information Security Compliance
  - Financial Products, Loans, Real Estate, Taxes

The Common Question

Question: How can installers of access control, biometrics or any other TCP/IP enabled hardware connect to a server running the control and monitoring software at a different site without the difficulties of setting up a standard VPN?

Answer: The Access Point (AP) once configured and plugged into any internet connection will automatically locate the Controller. The AP will securely establish an IPSEC tunnel whereby extending the LAN to any remote location. Simply, the LAN is brought securely to the remote site.

The Network

- Solution to “plug & play” with any access control, biometric system or TCP/IP hardware
- Solution that eliminates typical IT intensive VPN architectures when expanding the system via WAN
- Hardware layer that extends a LAN into any geographical area
- Eliminates time consuming and knowledge intensive “know how” for installers of biometric equipment or any access control system
- Cost effective hardware with scalability
- Any TCP/IP device will work

Common Requirements For IT Usage

- Data Processing Systems Access
- Data Access
- Data Protection Encryption
- User Credentials and Auditing
- Need to Know Access
- Administrative Access and auditing

Common Requirements For Access Control

- Establish remote connectivity into other geographical areas without existing LAN or WAN between sites (or buildings)
- Simplified installation process for field installers of the equipment
- Dedicated network for access control components and server running software
- “Plug and Play” connectivity for any hardware client that is TCP/IP enabled.
- Expansion of network for other access control layers (i.e.. IP cameras, biometrics, etc.)

Expands Your Network For Access Control

Components In An Access Control Layout

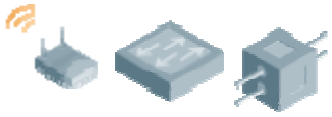
Remote Geographical Area

Biometrics

Wiegand Panels

IP CCTV Cameras

AUTOMATIC SECURE IP TUNNEL LAN EXTENTION



TCP/IP CONNECTIVITY TO ACCESS POINT

ANY INTERNET CONNECTION!

Primary Point For Access Control

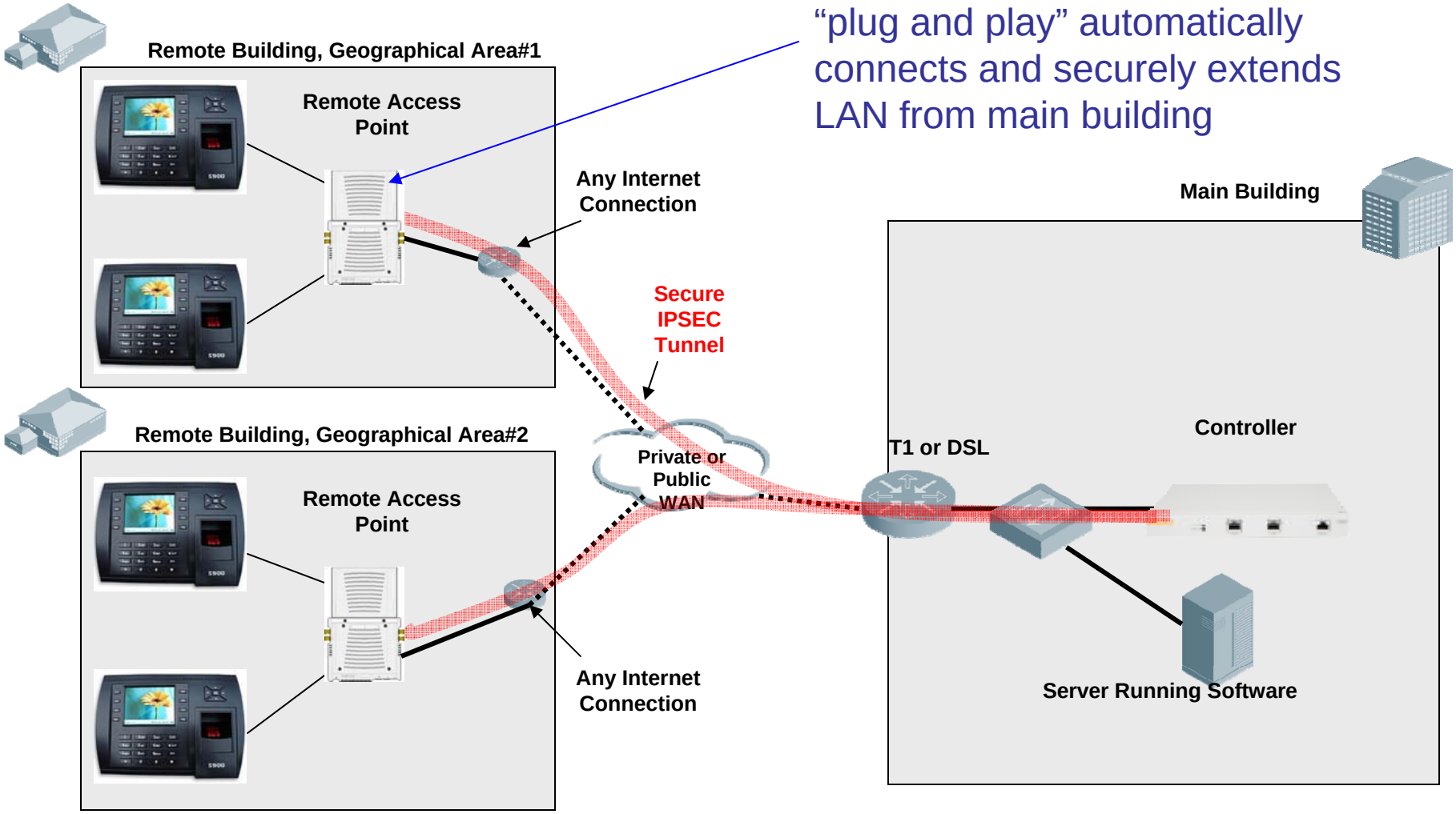
CONTROLLER

ACCESS CONTROL SERVERS ON LAN

LAN BASED HARDWARE DEVICES

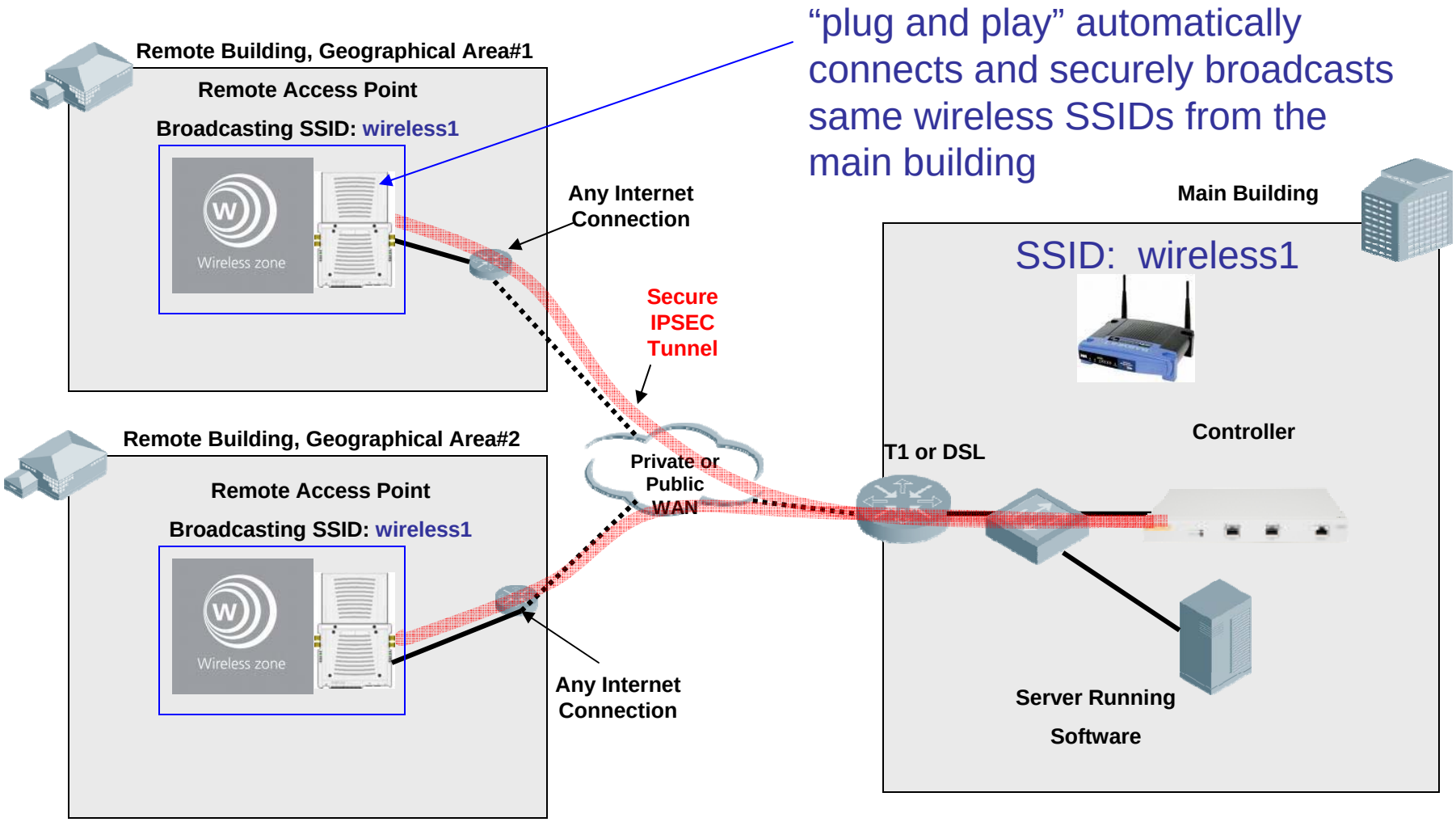
Secure Remote Access Point

Expanded Architecture Using Existing Access Control Products



Broadcasting of Same Wireless SSIDs

Any Broadcasted SSIDs Will Also Be Securely Broadcasted at the Remote Site



Expands Your Product Into Other Geographical Areas

AP AND CONTROLLER

- Establishes an extended and secure LAN
- Device Connection to PC by extended LAN
- ✓Maximum security and data protection
- ✓Low/Medium level of difficulty to establish extended LAN

Typical Hardware Used In An Access Control Installation

RS232 To TCP/IP

- Establishes a TCP/IP connection for RS232 devices
- Connection to PC by LAN
- Network associated security risks
- Low/Medium level of difficulty to establish a network connection on LAN
- High level of difficulty to establish a remote connection (commonly requires an existing LAN or WAN between remote sites

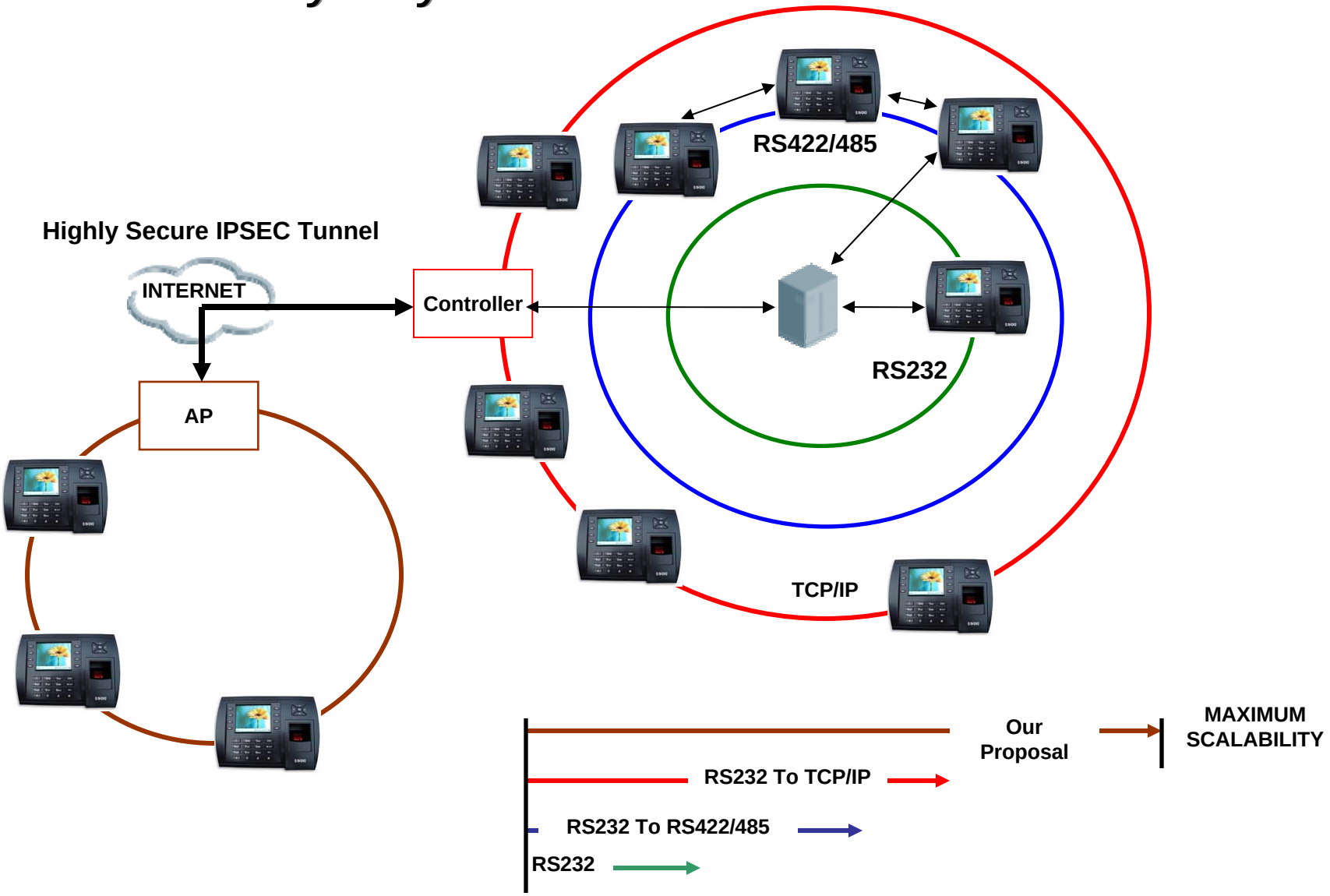
RS232 To RS422/485

- Creates 2 to 4 wire connection among multiple devices
- Direct connection to PC by serial port
- ✓Simple to establish connection

RS232

- Direct connection to PC by serial port
- ✓Simple to establish connection

Connectivity Layers At Work



Closing Statements

✓Any TCP/IP hardware component will operate remotely as if it were operating on the LAN at the “local” site

✓No integration to existing products

✓Installers do not need to setup costly VPN systems that require time and expensive hardware

✓IT personnel will feel secure about the protection of their PC based network operating with other service networks

✓Low/Medium level of difficulty to establish the extended LAN

✓Remote AP plugs into any internet connection and automatically locates the controller

✓No distance limitations

✓Highly secure IPSEC tunnel and other forms of high level encryption

✓Expansion for customer (i.e.. VOIP, IP Paging Systems, IP Cameras, etc.)