

# Specification



*StrongPoint™* Field Security Appliance for Traffic Management Networks

## Specification

The *StrongPoint* Security Network shall create a secure, virtual-network layer connection between the remote user and the traffic control network. *StrongPoint* uses the Uniloc® NetANCHOR™ patented Device Fingerprinting Technology to establish a Secure Private Network between an authorized traffic management system and individual field appliances.

The *StrongPoint* System Process shall be defined, as follows:

The NetANCHOR Device Fingerprinting Technology shall authorize every *StrongPoint* field appliance for exclusive use in a traffic control network, and shall ensure that other unauthorized “network” devices are not allowed to communicate on the *StrongPoint* Secure Private Network. A *StrongPoint* Server shall be located at the Traffic Management Center (TMC). The *StrongPoint* Server shall authenticate the serial numbers and locations of all *StrongPoint* field appliances. Each cabinet contains a *StrongPoint* appliance, which is connected to traffic control devices requiring a network connection. As each appliance is installed and connected, in the field, it shall establish a communications link with the *StrongPoint* Server and shall create its own device-locked point-to-point secure private network.

Throughout its life in the field, the *StrongPoint* appliance shall continuously communicate with the *StrongPoint* Server to verify its operational status.

The *StrongPoint* Security Network shall:

- Provide security for field traffic-control systems by creating a secure, virtual-network layer connection, between the remote user and the traffic control network, thus blocking unauthorized access and external cyber-threats.
- Create a secure, virtual-network layer connection, which enhances traditional router, switch, and firewall security mechanisms.
- Provide Traffic Management Systems with secure private tunneling across public network segments, including, but not exclusive to, wireless (CDMA, GSM, 802.11a/b/g) and the public Internet (802.3, DSL, Cable).
- Provide a point-to-multipoint “Secure Private Network” between the TMC and each field traffic cabinet
- Provide an additional layer of security for detector modules, surveillance cameras, UPS devices, or other cabinet devices, which expose themselves to an Internet Protocol (IP) interface, or in other words, “web-facing” systems.
- Allow network operators to define policies, such as the types of computers or roles of users allowed to access areas of the traffic network. These network usage policies shall be enforced using the *StrongPoint* Management Software.
- Shall enforce network access policies based on authenticated user identities, referred to as Uniloc’s Physical Device Recognition (PDR) technology to grant access to authorized computing devices and communications networks.
- Include device fingerprinting technology to restrict field control access to designated computer terminals at the TMC, or between management centers (Center-to-Center Communications), thus providing only authorized computer terminals exclusive access to the secure private network.

# Specification

The *StrongPoint* Server shall include:

The Server shall allocate permission, manage, and control field security appliances and PC clients from a single remote location. The server application shall monitor status of all network appliances and PC clients participating in the authenticated secure private network. The server shall track and report on all secure private network appliances, PC clients (the System PC and/or the Field PC), and users of the authenticated system.

The server shall define and receive instant status alerts and updates regarding any changes to the secured network, and receive alerts regarding any unauthorized access attempts based on secure private network appliance location.

The server shall include:

- a) The following operating system: RedHat Enterprise Linux 5.x
- b) The following software applications: MySQL 5.x, Apache Tomcat 5.x, OpenVPN, OpenSSL, Uniloc<sup>®</sup> ecoServer, and Uniloc<sup>®</sup> NetAnchor Server
- c) Web-launched Graphic User Interface (GUI), to configure and monitor the secure network
- d) Support for HTML/Web Browsers, Internet Explorer 7 and above (on Windows), Firefox 2.0 and above (on Windows and Linux) and Safari 3.x and above (on Mac OS X 10.5.x)
- e) Complete server-based device management toolset for easy set up and authorized appliance configuration
- f) Complete server-based device management toolset for user roles management
- g) Intrusion detection, location, and notification functionality, including automated alarm and events management system
- h) Intrusion detection, location, and notification functionality, including automated email notice system
- i) Intrusion detection, location, and notification functionality, including system monitoring logs and automated report generation
- j) Cross-platform compatibility with any operating system and field control hardware
- k) Intrusion detection at the *StrongPoint* Appliance Ethernet ports, which includes “Stateful” Packet Inspection (SPI) that keeps track of the state of network connections on the *StrongPoint* Appliance (such as TCP streams or UDP communication) traveling across the *StrongPoint* Appliance ports.

The *StrongPoint* Server shall provide the following minimum hardware requirements:

- 2.0 GHz and above, Dual-Core Intel<sup>®</sup> Xeon<sup>®</sup> Processors
- 70 GB HDD
- 2 GB RAM
- 1 Gigabit Ethernet NIC
- 1 Fast (100 Mbps) Ethernet NIC

# Specification

Technical Support shall include:

- Administrative documentation
- Two-year warranty on hardware
- One-year software upgrade available

The *StrongPoint* Appliance Hardware shall include:

- Self-test on power-up
- LED indicators for power and communications link/activities status
- Auto-Uplink and Stateful Packet Inspection (SPI)
- Shelf-Mount, DIN Rail and Screw-Mount mounting options for easy in-cabinet placement
- 24 VDC, optional 100-240 VAC
- Consumption, current – 8 Watts / 0.3A
- 1 WAN, 4 LAN, RJ45, 10/100 Mbps Ethernet
- -29 F to +165 F (-34 C to +74 C) operating temperature range
- 0 to 95% relative humidity

The *StrongPoint* Appliance internal Processor shall provide, at a minimum:

- Motorola® MPC8321EEC Microprocessor
- 333MHz core processor speed
- 32MB Flash Memory
- 128MB DDR2 Memory
- Up to 18 Mbps Secure Private Network and Virtual Private Network (VPN) Throughput

The field-hardened appliance shall provide the following transportation industry standards certification, at a minimum:

- a) IEEE 802.3, IEEE 802.3u Standards Compliant
- b) NEMA TS2-2003 Certification
- c) FCC Part 15 Certified
- d) ICES-003 (Issue 2) Certified