Secure connectivity for enforcement cameras

Cameras Background

Many countries in the Middle East are trying to improve traffic safety by installing digital radar cameras. Manual collection of the radar camera images is still common, but too dangerous, as the cameras are often installed in the middle of busy roads. Also, there are simply too many sites to go to every day. So, for a large multi-site project in the Middle East, the police and the selected radar camera manufacturer insisted on transferring violation images using wireless data transmission. This case study describes the main technical reasons why Garderos wireless routers were chosen for the data transmission part of this project.

Key requirements for the wireless data transmission equipment

Equipment ruggedization is a key requirement, as summers in the Middle East are amongst the hottest in the world. Hence, only equipment with advanced thermal-hardening could be used. Another key requirement is the ability to survive software faults (“auto-recovery”). It is not acceptable for the wireless equipment to just “hang up”, as this drives up service costs and leads to delays in transmitting the violation images. Furthermore, many of the cameras are in the middle of a busy road, which makes it difficult and dangerous to access them.

3G/4G Cellular Networks

Many of the chosen camera locations had no optical fiber or xDSL cabling available, so it was decided to use the existing high-speed cellular networks, based on 4G technologies, for data connectivity (with future 5G as the next logical step). As busy locations can produce several gigabytes of data per day, the Garderos routers were equipped with 4G interfaces and have proven themselves capable of handling the daily data volumes. Another important part of the technical solution was the use of high-gain cellular antennas and low-loss industrial-grade antenna cabling. This improves cellular signal reception in areas of poor coverage.

Cyber-Security

Due to the sensitive nature of images depicting traffic violations, cyber-security was a key design requirement. The Garderos routers are used together with mobile VPNs, use VPN tunneling and digital certificates to provide a high level of cyber-security.

Router management

It’s important to maintain the software on the routers to keep the level of cyber-security high and to take advantage of new features. However, managing several hundred geographically distributed routers is not an easy task. Garderos routers solve this problem by using Auto-Configuration. The routers “auto-configure” themselves by regularly checking for new configuration files and software updates at a central server. In this way, a consistent configuration is maintained on all routers and patches are easily deployed.