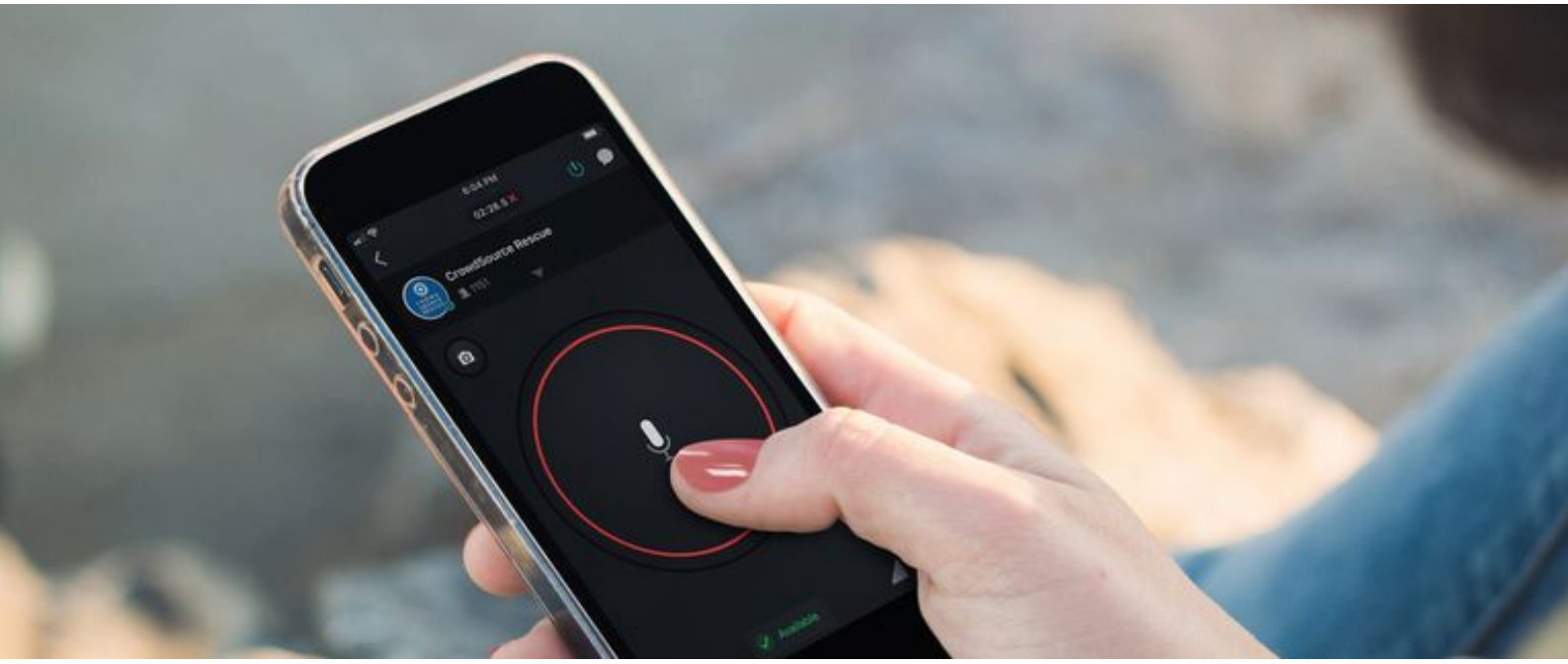
Case Study

Ensuring secure and efficient communications over LTE on Push-to-Talk over Cellular devices



Background

While voice applications remain paramount, data and video based applications are increasingly important during crisis and day-to-day operations of Public Safety Agencies. New network technology generations (i.e., LTE/5G), can drastically enhance the situational awareness and the overall efficiency of operations. Push-to-talk over cellular (PTToC) enhance the most useful aspects of the traditional two-way radio while integrating and supplementing them with the data, video and voice capabilities of mobile phone networks. Ultimately, you can push-to-talk with international users, not just those in close range. Other key benefits are: no infrastructure required, rapid deployments, GPS location tracking. Besides ensuring global connectivity and new capabilities, protecting critical communications from unauthorised access is key to the success of first responders. 5G and cybersecurity are both hot topics in the Critical Communication Sector.

Challenge

Business continuity on critical networks is of vital importance. To achieve this networks must be secure at all times, at all levels, from the endpoint to the data center. With the migration towards more modern, complex and high-performance architectures using the IP protocol, Critical Communication Networks interconnects with commercial environments. Interoperability increases the attack surface and threat vectors facing multiple cyber-risks.

Industry

RoIP
Push-to-Talk over Cellular (PTToC)

Challenge

- Guarantee continuity of operation over poor quality channels
- Ensure optimal protection of endpoints and servers
- Gain complete control and visibility across the Critical Communication ecosystem

Goals

- Establish trusted encrypted channels
- Obtain maximum connections stability
- Seamless security integration for fast setup, deployment and update on multivendor devices, and heterogeneous networks

Solution

SE*link*™ provides a zero trust security model combined with software-defined network segmentation and whitelisting practices. Delivering Data, Device and Network Security and Control in one single solution

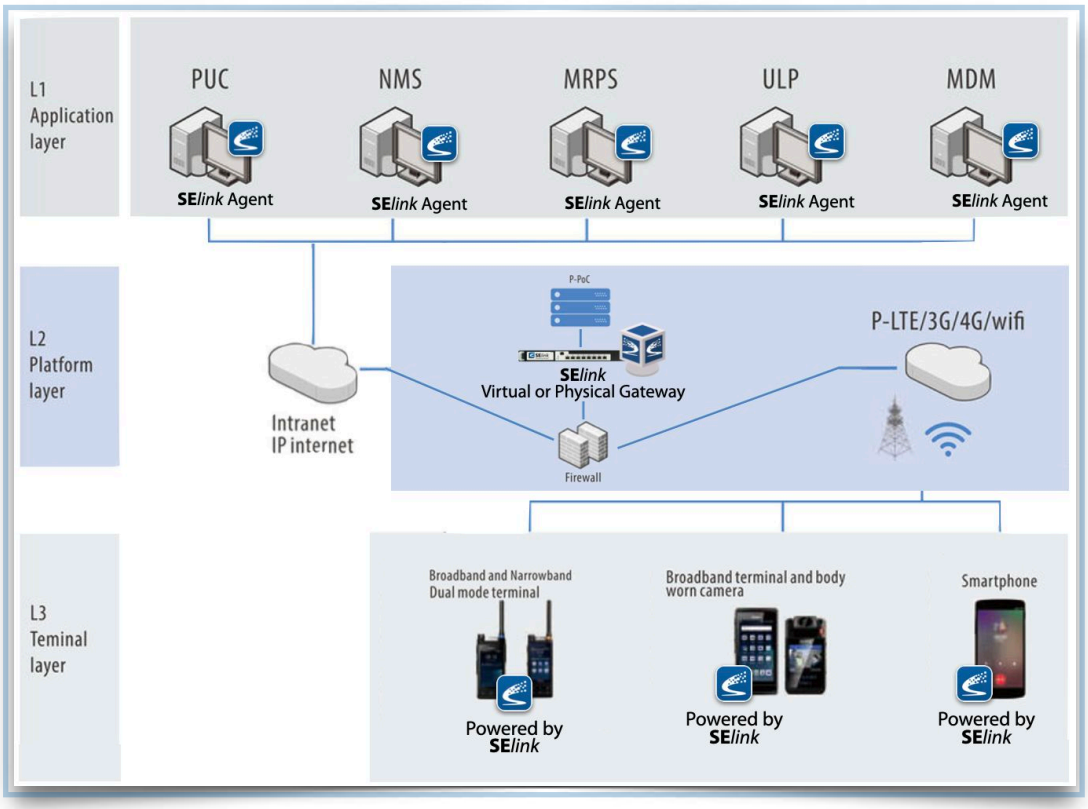
Solution

Broadband for mission-critical creates a whole new set of challenges since broadband can run on commercial cores and protocols increasing the threat surface and reducing the level of control of critical communications users. Blu5 extensive experience in supporting Government and Military Agencies meet their stringent security requirements is a guarantee of in-house resources and expertise to help Public Safety Agencies bridge potential technology gaps.

SE*link*™ is a service-oriented, secure, virtual networking solution to protect end-points (Terminal Layer 1) network (Platform Layer 2) and services (Application Layer 3) alike. Able to replicate heterogenous clients and server behaviours in a seamless way, as in a private LAN; when an endpoint device is connected to the Platform server through SE*link*™, it is virtually relocated in the same Platform server LAN. **The SElink™ Gateway performs endpoint device "virtualisation"**, showing to the server the original MAC address and a unique, registered, identifier for each endpoint device. The advantages are overwhelming. SElink™ protects both the data channel and the access to the communication channel, which can only be used by authorised processes. This ensures that the Platform server is protected even in the event that the endpoint device is compromised. Devices affected by vulnerabilities, even without vendor knowledge, may infect the network with major service disruptions and significant impact on business continuity. Lightweight protocols and zero encryption overhead make band availability and integration of security no longer a limit. Easy integration in any environment, over any protocol, portable, multi-device for a fast deployment of new devices at accident sites without requiring experts to travel to the site. Crypto agility allows SElink™ to migrate to new symmetrical algorithms in a centralised way without any effort. SELink™ is ready to use the Post-Quantum algorithms shortlisted by NIST. A centralised deployment and management security system guarantees control across a large-scale network.

Benefits

1. **Zero Trust Network Access and Assumed Breach model** strategies
2. **Lightweight protocols** for bandwidth sensitive and resource-constrained devices
3. **Low-bandwidth strategies coupled with smart mechanisms** to improve QoS and availability of service
4. **Zero Encryption Overhead** compared to TLS/SSL
5. **Free from third-party vendor dependancies** for the integration of security into heterogeneous devices
6. **Enhanced system longevity and resilience** to quantum attacks
7. **Seamless encryption updates, redesign-free** through Crypto agility



Blu5 Group
info@blu5group.com
www.blu5group.com