



“We were in urgent need of a replacement for our SoR provider. Cellusys has lived up to its #1 position, showing excellence in collaboration and flexibility.”

Natasha Degroote, Head of Roaming, Telenet Group



Customer challenge

The incumbent Steering of Roaming provider discontinued support, leaving Telenet in urgent need of a reliable solution. After a tender process, Cellusys was selected as the best-in-class provider.



Cellusys solution

We deployed our Hybrid & Active Steering of Roaming platform with geo-redundancy and virtualised equipment. The setup accommodated the operator's active-standby requirement, and with strong support from the Cellusys team the solution was fully operational within 12 weeks.



Results

The customer reports that the platform steers traffic very effectively and that adapting steering rules is simple, thanks to the intuitive graphical interface.



“Cellusys Signalling FW is wise. Many actions that could not be done on other networks nodes, could be done on Cellusys SFW.”

Hikmet Yavuzer, Voice Core Operations Manager



Customer challenge

To separate IMSI ranges of Turkey and Cyprus while ensuring legitimate traffic is protected and unwanted traffic blocked.

- ⦿ Unwanted alphanumeric messages within Turkey.
- ⦿ Unintentional roaming in border cells causing bill shock.
- ⦿ Difficulty distinguishing genuine subscriber travel from fraud attempts.



Cellusys solution

Advanced set up of Signalling Firewall to eliminate overlaps in country codes (CCs) and network destination codes (NDCs).

- ⦿ Built regex filters to block unwanted sender IDs and message content.
- ⦿ Inbound roaming rules created to prevent unintentional attaches in border areas.
- ⦿ Travel-time method implemented, a robust solution to thwart fraud attempts.



Results

Turkey and Cyprus signalling traffic is now handled separately, ensuring reliable traffic management and minimising interference.

- ⦿ Unwanted alphanumeric messages were blocked within minutes through precise rule creation.
- ⦿ Subscribers' location data preserved while preventing unintended roaming.
- ⦿ Enhanced processing of CAT3 messages, a level of fraud prevention unmatched by other solutions.



“ Intelligent network selection is a key feature of iBASIS Global Access for Things. In addition to our own patented technology, the Cellusys SoR platform provides a key component for selecting the right network for the right device at the right time. ”

Ajay Joseph, CTO



Customer challenge

IoT devices were struggling with signal strength and firmware issues, preventing them from connecting to the strongest network. Some LPWA devices also required specific power-saving features and needed to be directed to the appropriate network. Customer experience was impacted negatively.



Cellusys solution

Our Steering of Roaming platform offers multiple steering features based on network and device capabilities, along with an extensive API enabling seamless integration with the iBASIS IoT BSS.



Results

Our SoR platform enables iBASIS to efficiently group customer devices based on business needs and customer limitations. The API allows real-time network adjustments, improving device performance and overall customer experience.



“Cellusys Signalling FW was deployed in Ooredoo Oman in 2017.”



Customer challenge

A sharp rise in spoofing was detected in Ooredoo Oman. Fraudsters had started using outbound roaming numbers as Spoofing numbers. Cellusys met with the Telecommunications Regulatory Authority and advised that all operators implement CLI spoofing detection for international calls.



Cellusys solution

A preliminary check determined whether the subscriber was roaming, as received calls do not include exact location information. We then implemented a system with additional rules for handling Oman's signalling traffic. Further rules were introduced to correlate SIP and SS7 signalling.



Results

The enhancement strengthens detection mechanisms and reduces the risks of CLI spoofing. As a result, Ooredoo Oman can better protect its network from fraud, ensuring a more secure communication environment for users.



“Since integrating Cellusys VFW, we have witnessed remarkable improvements in flash call security and fraud prevention.”

Vusal Heybatov, Head of Core Network



Customer challenge

The voice network was witnessing a lot of apparent flash calls. These unwanted calls were neither regulated nor monetised, leading to dissatisfaction among enterprise customers. There was no way to control them, and distinguishing between genuine and fake authentication processes was challenging; no CLI reuse.



Cellusys solution

Advanced Voice Firewall set up using multiple algorithms to detect flash calls. Suitable actions can be taken to block, modify the CLI, or redirect to an IVR. This solution complies with local regulations while offering a range of handling options. Correlation with SMS fallback allows genuine authentication processes to continue, ensuring enterprise customer satisfaction.



Results

Azerconnect reports that the Cellusys Voice Firewall has proven robust and reliable, providing real-time monitoring and analysis of SIP traffic. They highlight Cellusys' exceptional technical support in fine-tuning the system to meet their specific needs. They report that the solution is a vital node in securing the network, and the partnership with Cellusys to enhance network security will continue.

#1