Challenge Sheet

EJIE

Facilitating Initial Configuration and Agile, Secure Diagnosis of Incidents in Complex Network Infrastructures

How might we facilitate both the initial configuration and the agile and secure diagnosis of incidents in complex network infrastructures, improving system visualization and reducing dependency on distributed knowledge, without affecting performance or operational security?

Sub-challenges

- How might we integrate different sources and technologies (firewalls, load balancers, proxies, physical and virtual routers, microsegmentation, NATs, VRFs, PBRs, etc.) into a single visualization interface to facilitate both configuration and incident detection, without modifying the configuration?
- How might we simulate network scenarios to anticipate problems or validate configurations safely, without compromising the operational environment?
- How might we identify the exact point of failure, display it clearly, and generate alerts that are interpretable by technicians with different levels of expertise?

Context

EJIE manages the technological network of the Basque Government, covering critical services such as justice, education, health, and administrative operations. The infrastructure consists of a diverse and constantly evolving network with multiple layers, technologies, and vendors. This complexity makes traceability, coordination among teams, and efficient incident resolution difficult.

The constant need for immediate responses to failures has created an ecosystem where urgent functionality is prioritized over systematization, leading to technical silos, lack of a global view, and a higher risk of errors during interventions. The organization itself acknowledges that there is currently no clear representation of the network ecosystem nor tools that integrate all the components.

The lack of clear and cross-cutting visualization hinders the detection of root causes and slows down resolutions, directly impacting citizen-facing services.

Objectives

- Facilitate the initial configuration of complex infrastructures in a safer and more understandable way.

- Detect the root causes of incidents faster and more accurately.

- Reduce response times without the need for manual testing.

- Improve communication among technical teams currently operating with partial visibility.

- Minimize the citizen impact of poorly managed incidents.

- Increase operational efficiency through a reusable and scalable solution.

- Enable testing in secure environments without affecting the performance of the live system.

What are we looking for?

A GovTech solution that can:

- Visually represent the entire infrastructure, showing layers, devices, and relationships among elements.

- Assist with both initial configuration and diagnosis from a secure, integrated interface with a read-only or passive mode that does not modify devices.

- Integrate hybrid technologies (on-premise and cloud), multiple vendors, and virtualized architectures.

- Launch simulations or test scenarios to predict system behavior without affecting the operational environment.

- Be used by technical staff with varying levels of expertise, including assistants or recommendation systems that help prioritize actions.

- Function as a complement to the current system, not replacing it, but reducing errors due to a lack of context.

Key Considerations

- Any solution must respect cybersecurity and ensure it does not affect the live network.
- Integration with existing tools (monitoring, ticketing, infrastructure management) is highly valued.
- It must not require a complete redesign or forced migration of devices.
- It should allow for progressive deployment in specific areas before scaling.
- Interoperability and technology neutrality are essential.
- The system must support exporting logs, analyses, and technical reports for internal monitoring or audits.
- Ideally, the system should be able to operate partially even if it doesn't have complete visibility of the entire network, providing useful information even with partial integration.

Key Dates and Process

To participate in the challenge, register at this link: **https://bind.spri.eus/govtech-application/**

- Deadline for submitting your proposal: 04/08/2025 at 23:59h
- Semifinalist startups will be announced between 13/10/2025 and 17/10/2025
- Finalist startups will be announced on 30/10/2025
- The winning startup will be announced on 20/11/2025

Selection Process

Phase 1 – Pitches by semifinalist startups with the public entity:
Startups will present their solution in a 10-minute pitch.
→ 3 finalist startups will be selected.
→ This phase will take place from October 27 to 29, 2025.

Phase 2 – Interviews with the finalist startups and the public entity:
Startups will present a deeper version of their proposal.
→ This phase will take place from November 17 to 19, 2025.

What you access

Winning startup

→ Paid pilot of up to €15,000
→ The pilot will begin in January 2026 and will last 6 months