Closed Loop Automation Platform for Intelligent Security Operations with TeraFlowSDN and OSM

Allen Abishek, Ricard Vilalta, Lluís Gifre, Raul Muñoz

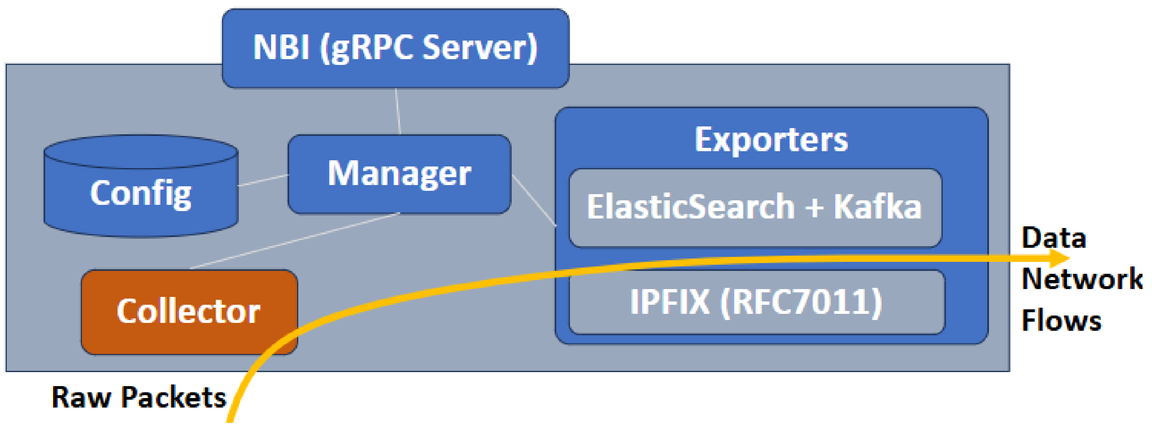
Centre Tecnologic de Telecomunicacions de Catalunya (CTTC-CERCA), Castelldefels (Barcelona), Spain.

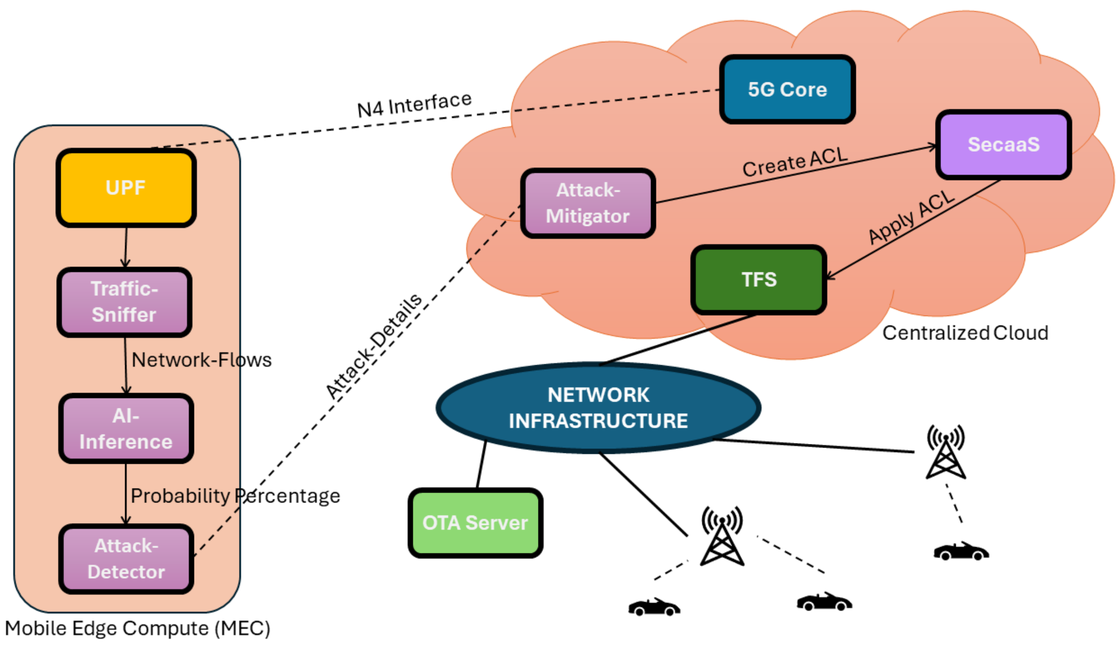
Abstract

The objective is to explore the design of a Closed Loop Automation Platform using SOAR mechanism to provide real-time network security policies and dynamically update security policies based on incoming user plane traffic.

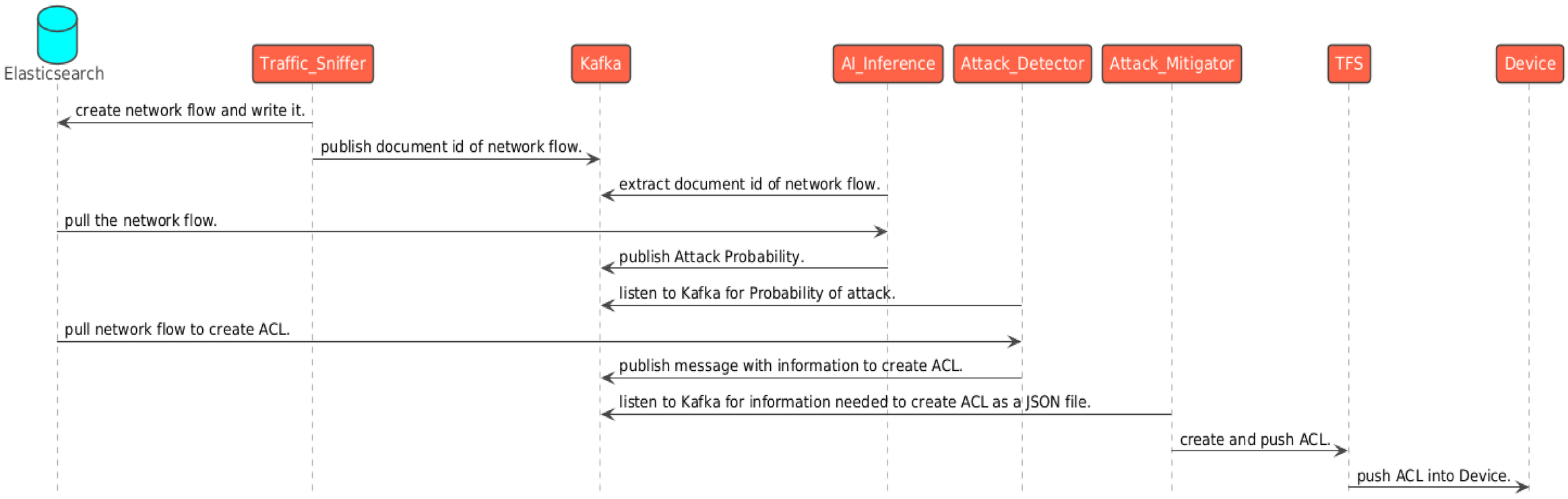
Introduction

1. Capitalizing on SDN, NFV and Cloud Technology to attempt to build a Closed-Loop Automation (CLA) solution based on Security Orchestration, Automation and Response (SOAR) to implement network security policies.
2. This architecture uses 4 main components which are the 'Traffic Sniffer', 'AI-Inference', 'Attack Detector' and 'Attack Mitigator', which is integrated with Teraflow SDN (TFS) controller.
3. The Traffic Sniffer analyzes raw packets and creates reports called 'network flows' that contain contextual information about the network traffic coming into an interface.
4. The AI Inference component classifies network flows(network traffic of a particular type) into 3 types Denial of Service, Ping of Death, Mail-of-Spam and assign a probability for each.
5. The Attack Detector if the probability assigned for each type of attack for each network flow is high enough to be considered as an attack on the network, if it is then the network flow details are sent to the Attack Mitigator.
6. The Attack Mitigator creates an Access Control List (ACL) which is pushed into the Security-as-a-Service (SecaaS) orchestrator.
7. The SecaaS pushes the ACL into the appropriate TFS instance and TFS pushes the ACL into the router/switch that is the closest to the source of the malicious packets entering the network, thus dropping the malicious packets.





CLA Workflow Diagram



References

- R. Vilalta, R. Muñoz, R. Casellas et al., "Teraflow: Secured autonomic traffic management for a tera of sdn flows," in 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE, 2021, pp. 377–382.
- A. Zaalouk, R. Khondoker, R. Marx et al., "Orchsec: An orchestrator-based architecture for enhancing network-security using network monitoring and sdn control functions," in 2014 IEEE Network Operations and Management Symposium (NOMS). IEEE, 2014, pp. 1–9
- R. Asensio-Garriga, P. Alemany, A. M. Zarca et al., "Zsm-based e2e security slice management for ddos attack protection in mec-enabled v2x environments," IEEE Open Journal of Vehicular Technology, 2024

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
UNICO I+D
GOBIERNO DE ESPAÑA
Centre Tecnològic de Telecomunicacions de Catalunya