

A demonstration of a network isolation solution for the computing continuum

Original

A demonstration of a network isolation solution for the computing continuum / Pizzato, Francesco; Bringhenti, Daniele; Cetino, Luca; Sisto, Riccardo; Valenza, Fulvio. - ELETTRONICO. - (2025), pp. 1-2. (2025 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) Athens (GR) 10-12 November 2025) [10.1109/NFV-SDN66355.2025.11349451].

Availability:

This version is available at: 11583/3003407 since: 2026-03-31T12:17:15Z

Publisher:

IEEE

Published

DOI:10.1109/NFV-SDN66355.2025.11349451

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

IEEE postprint/Author's Accepted Manuscript

©2025 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collecting works, for resale or lists, or reuse of any copyrighted component of this work in other works.

(Article begins on next page)

A demonstration of a network isolation solution for the computing continuum

Francesco Pizzato, Daniele Brighenti, Luca Cetino, Riccardo Sisto, Fulvio Valenza
Dip. Automatica e Informatica, Politecnico di Torino, Torino, Italy, Emails: {first.last}@polito.it

Abstract—The computing continuum integrates heterogeneous layers into a unified resource pool, introducing challenges in network-level workload isolation. This demonstration presents an intent-based solution to automate and enforce network isolation across such multi-user and non-uniform environments.

Index Terms—computing continuum, network isolation

I. OVERVIEW

The computing continuum is an innovative paradigm integrating cloud, edge, and IoT resources into a seamless pool of available assets, allowing for the transparent consumption of network, computation, and storage resources [1]. Initiatives like [2] are pushing for an ambitious vision of the continuum, where users are not just consumers of the shared resources, but also providers offering their own resources to other users.

While powerful, the computing continuum introduces significant security challenges. A highly relevant one is enforcing network isolation for workloads deployed within the continuum. In this context, the classical idea of static physical boundaries separating tenants’ resources is not valid anymore. Instead, the dynamism of the continuum transformed them into ephemeral borders, which span across multiple heterogeneous machines and evolve dynamically following user-defined policies or runtime necessities. Within such a dynamic and multi-tenant environment, it is necessary to manage network communications between workloads, safeguarding them from possible interference from the host or other co-located applications.

To address this problem, we developed a novel solution as part of the FLUIDOS [3] project and presented it in [4]. This solution consists in a security orchestrator that automates network isolation in a multi-tenant computing continuum environment by refining high-level user intents into the configuration of low-level primitives, i.e., Kubernetes Network Policies. The designed workflow consists of three main steps: verification, harmonization, and optimization. Their combination allows the intelligent resolution of possible conflicts between users of the continuum and the decoupling of the security definition from its implementation. This demonstration showcases a working prototype [5] of the solution throughout its three main phases.

II. INNOVATION

The main innovations and challenges related to the way our solution aims to address this problem are the following:

High-level security intents. Due to the large scale of the continuum and its heterogeneous composition, the traditional manual approaches based on static configuration are nearly

impossible to adopt. Our solution uses a high-level intent language designed to abstract this complexity away, as tenants express their security needs with a user-friendly but powerful syntax and our solution automatically handles the configuration of network security primitives and their enforcement.

Support for simultaneous and multiple goals. Multiple network isolation goals are simultaneously present within the continuum. The consumers want to be safeguarded from potential interference caused by the host or co-located tenants. Instead, the providers want to be protected from unintentional data exfiltration from hosted applications. Thanks to the designed intent language and multiple types of intents, our solution allows the expression of all these security isolation objectives.

Decoupling from specific implementation. The continuum is inherently heterogeneous, so different components support different network security primitives. The designed approach solves this challenge by decoupling the definition of network isolation intents from the specific implementation, which is carried out within a dedicated phase, i.e., translation, that can be specialized to different backend technologies.

Automated conflict resolutions. The continuum presents multiple and simultaneous network isolation goals. Therefore, conflicts arise between them, e.g., a communication requested by a consumer is not allowed by a provider. The presented solution analysed the set of conflicts that may arise in such environments and defined a resolution strategy for all of them. This is mainly carried out in the harmonization phase.

III. DEMO

The demo proposal follows the architecture and workflow presented in Fig. 1. The setup includes multiple Kubernetes clusters: one consumer cluster runs an e-commerce application, and three providers offer some services and resources, but have different wills in terms of authorized communications for the hosted resources. The clusters are virtualized on a single laptop using KinD [6] and are configured with Calico CNI [7]. Every cluster contains a Secure Border Controller (SCB), i.e., a Kubernetes controller implementing our solution. In the demo setup, each cluster also features external components, which are not part of our proposed solution but necessary for its execution, such as the FLUIDOS Node, developed by the FLUIDOS project for resource advertising and acquisition, and Ligo [8], responsible for the interconnecting fabric.

Intent specification phase. Initially, the consumer specifies a request for resources and the associated network isolation

