ARCADIAN-IoT

UWS B5G HUB

WORKSHOP: NETWORK SELF-PROTECTION LOOP

Pablo Benlloch-Caballero, Antonio Matencio-Escolar, Jose Alcaraz-Calero, Qi Wang
(UWS) http://beyond5ghub.uws.ac.uk

Training session, 26th September 2023, Coimbra

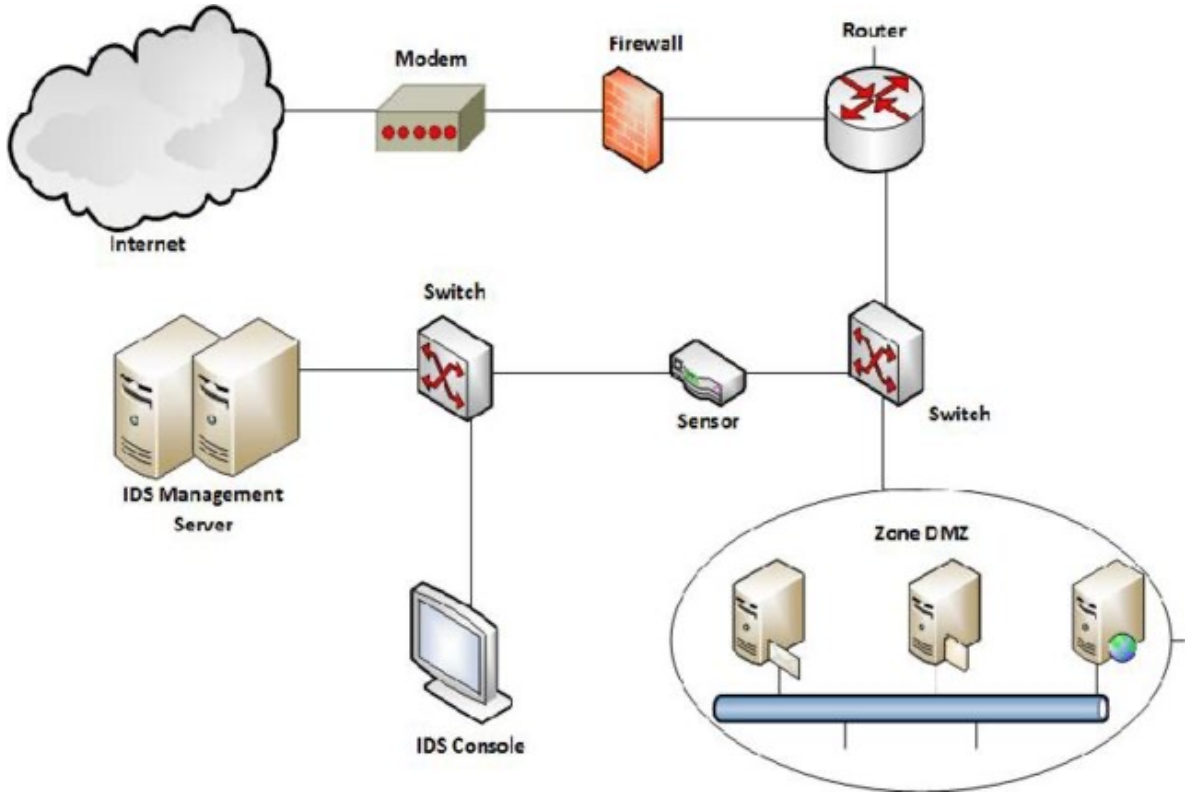
PRESENTATION ROADMAP

1. Motivation
2. What is a Self-protection Loop?
3. Architecture and software components
    1. The Self-protection Cognitive Loop
    2. Network Flow Monitoring
    3. Network Self-healing
    4. Network Self-protection
    5. Integration and communication
4. Threat detection, panning and mitigation
5. Demo
6. Contributions

1. MOTIVATION

HOW NIDS USUALLY WORK

- For a network topology, the security administrators install few components to **monitor** the data incoming to the company services
- Usually, a switch mirrors the traffic so a sensor can detect a threat
- The sensor raises the alerts to the IDS management servers where the **security administrators** can apply mitigation policies
- The **security administrators enforce the mitigation policies** in the firewall to stop the incoming threat

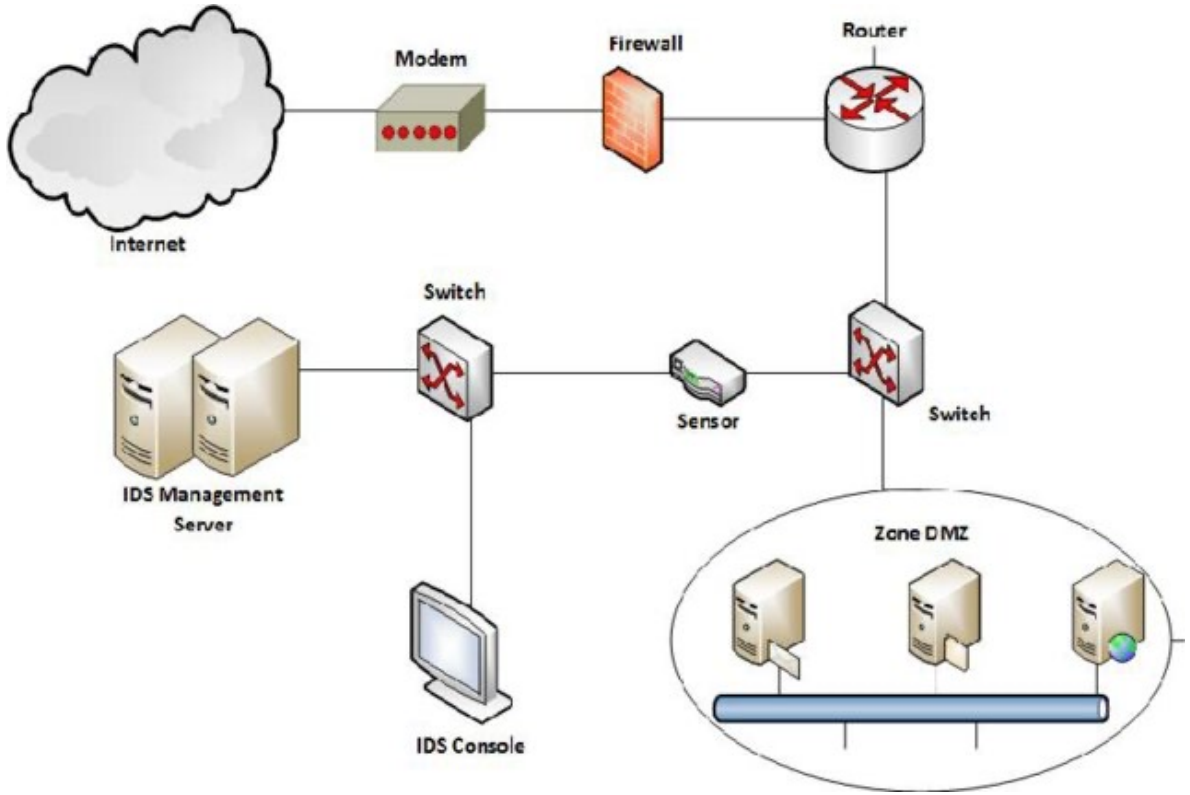


DOI: 10.9781/ijimai.2017.439

HOW NIDS USUALLY WORK

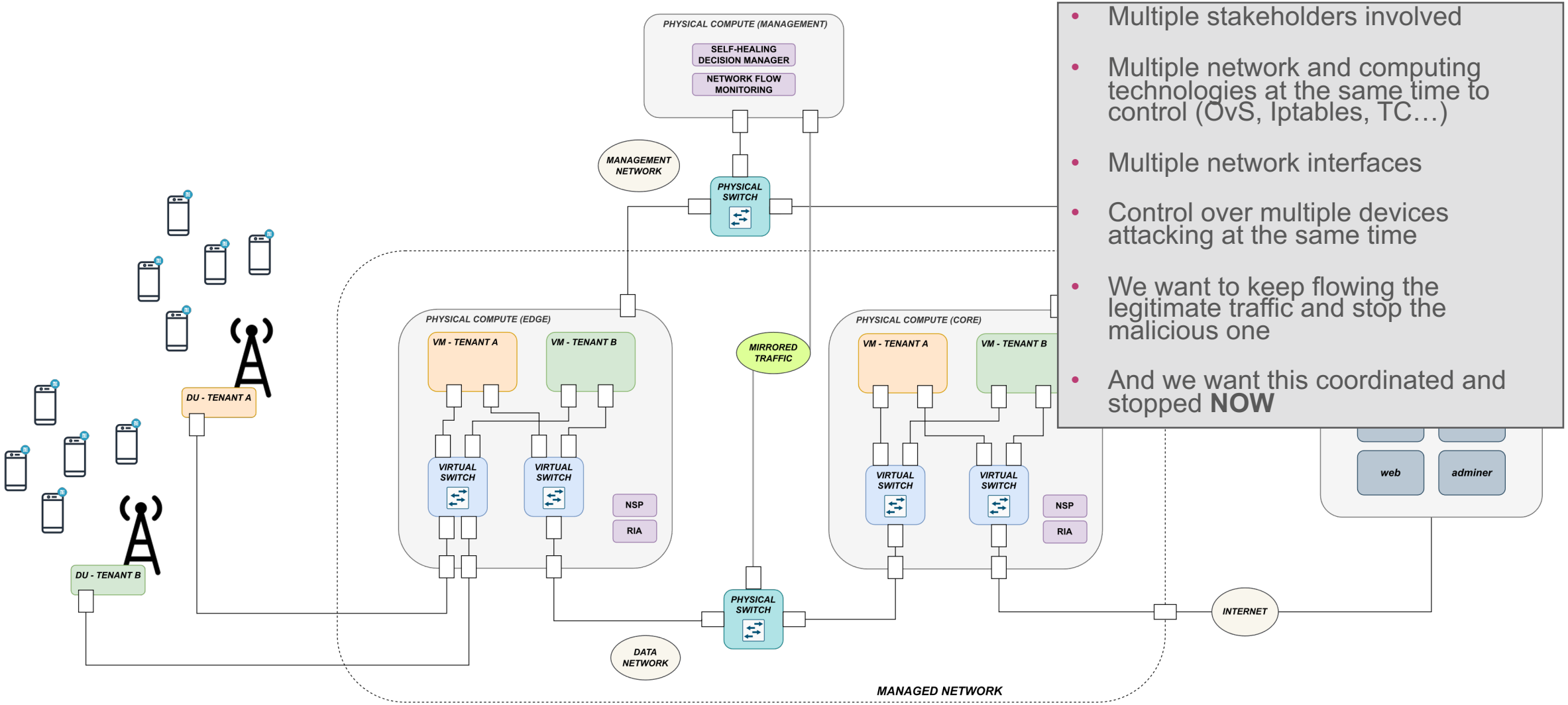
But the real scenarios have more complexity

- Human intervention can cause delay in decisions that can be automated
- These solutions are prepared for single-network scenarios
- Complexity of the network will be directly related to delays on decisions taken by the security administrators
- Usually, the solution is to stop all the user's network traffic



DOI: 10.9781/ijimai.2017.439

MORE COMPLEX SCENARIOS

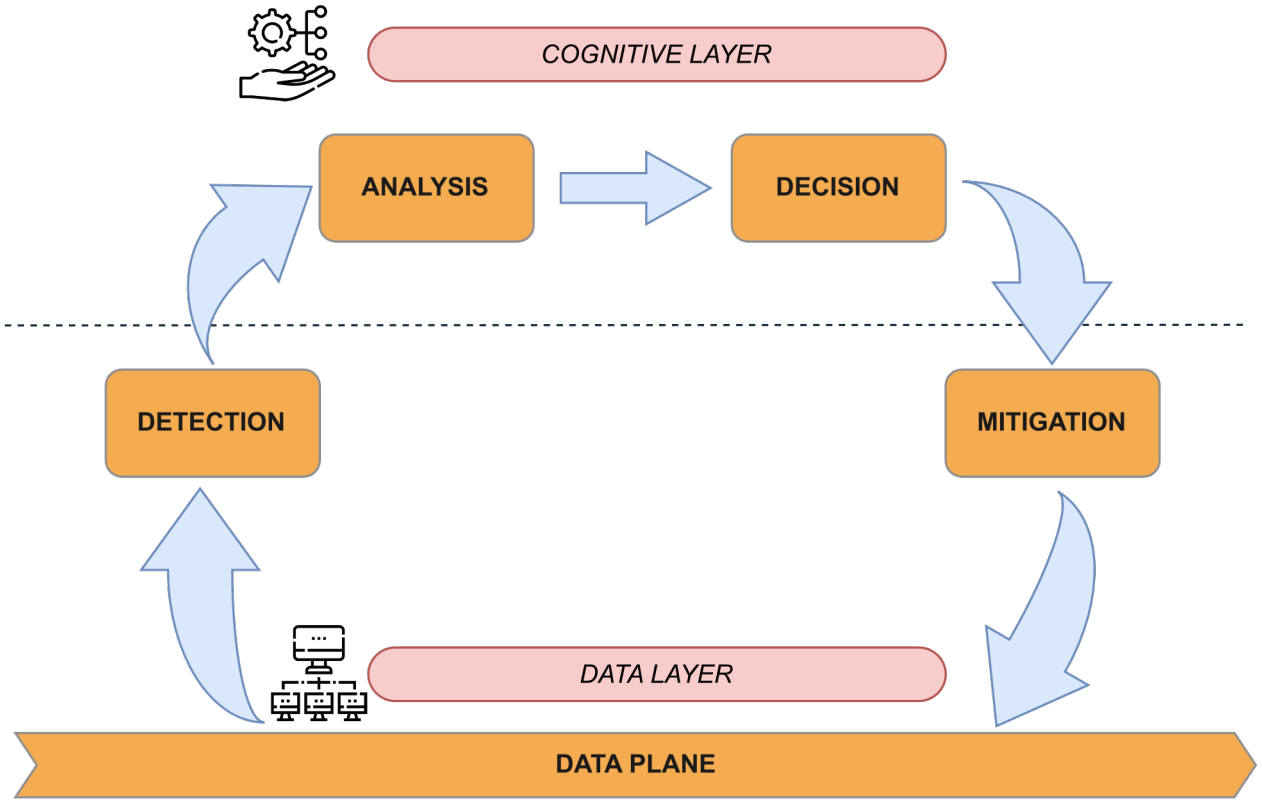


- Multiple stakeholders involved
- Multiple network and computing technologies at the same time to control (OvS, Iptables, TC…)
- Multiple network interfaces
- Control over multiple devices attacking at the same time
- We want to keep flowing the legitimate traffic and stop the malicious one
- And we want this coordinated and stopped **NOW**

2. WHAT IS A SELF-PROTECTION LOOP?

NETWORK SELF-PROTECTION LOOP

- It is called loop because it starts identifying the threat in the dataplane and ends with the mitigation in the dataplane, automatically.
- Has mainly four steps:
  - **Detection**: the system identifies a threat
  - **Analysis**: the system recognises the threat
  - **Decision**: due to previous analysis, a set of decisions are prepared to mitigate the threat
  - **Mitigation**: the system enforces the decisions as actions in the dataplane



WHAT WE AIM TO ACHIEVE

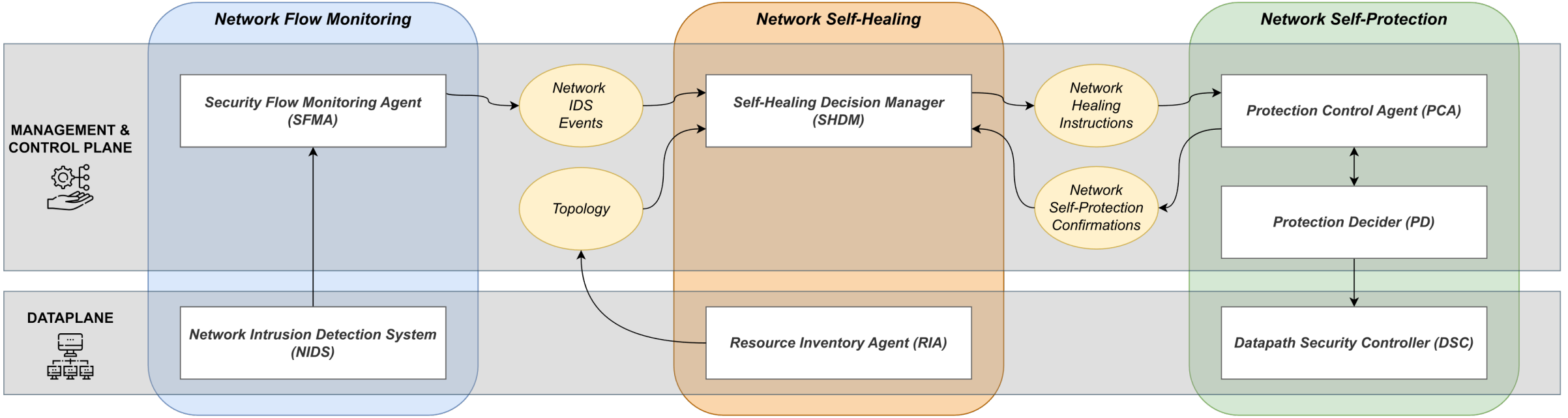
- Detect and identify real-time threats **no matter the complexity of the network topology**
- Provide the **fine grain** metadata **information** about the **flow and the topology** regarding the malicious flow detected
  - What IPs and network encapsulation layers the flow has
  - What are the points of the network that the flow has been detected (draw the flow path)
  - Which are the affected services (related ports and involved stakeholders)
- Provide a set of decisions and actions to be taken to **mitigate** the threat **automatically** for a chosen set of rules
- Enforce the set of actions to **mitigate the threat specifically for the very particular malicious flow**
- Leave the final user with the benign services active with no disruption

3. ARCHITECTURE AND SOFTWARE COMPONENTS

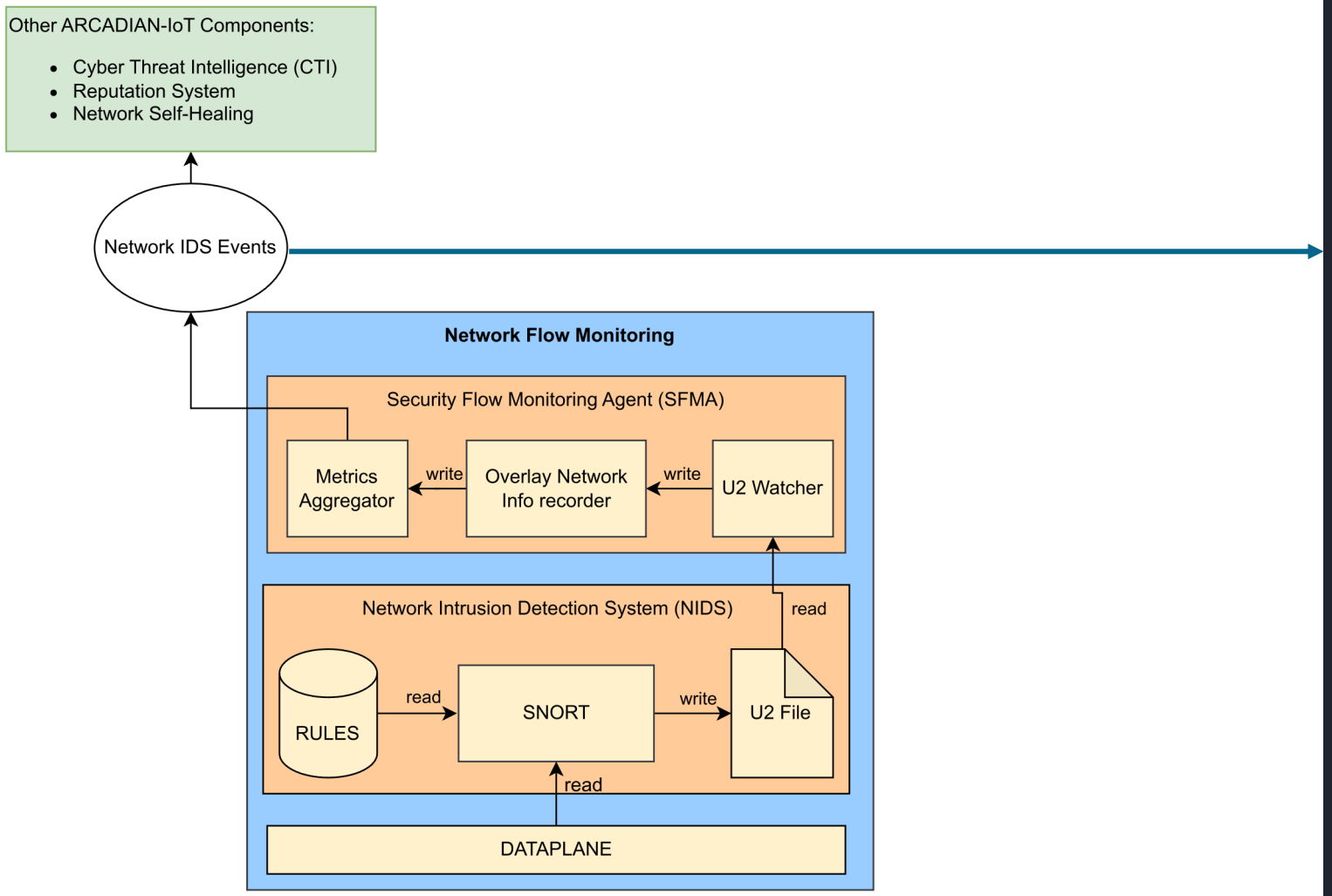
OUR NETWORK SELF-PROTECTION COGNITIVE LOOP

High level integration of the three main Network Self-protection Cognitive Loop components

- Using a message-bus tool as RabbitMQ to exchange information between components
- NFM triggers an **Alert** → NSH takes a decision about **how to perform the mitigation** → NSP **enforces the healing action** in the Dataplane

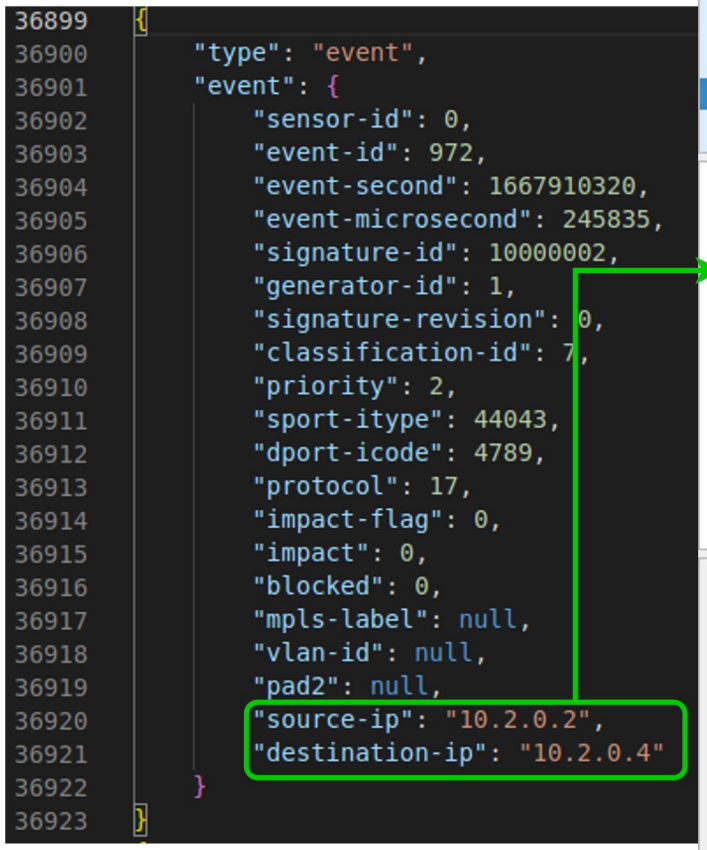


NETWORK FLOW MONITORING

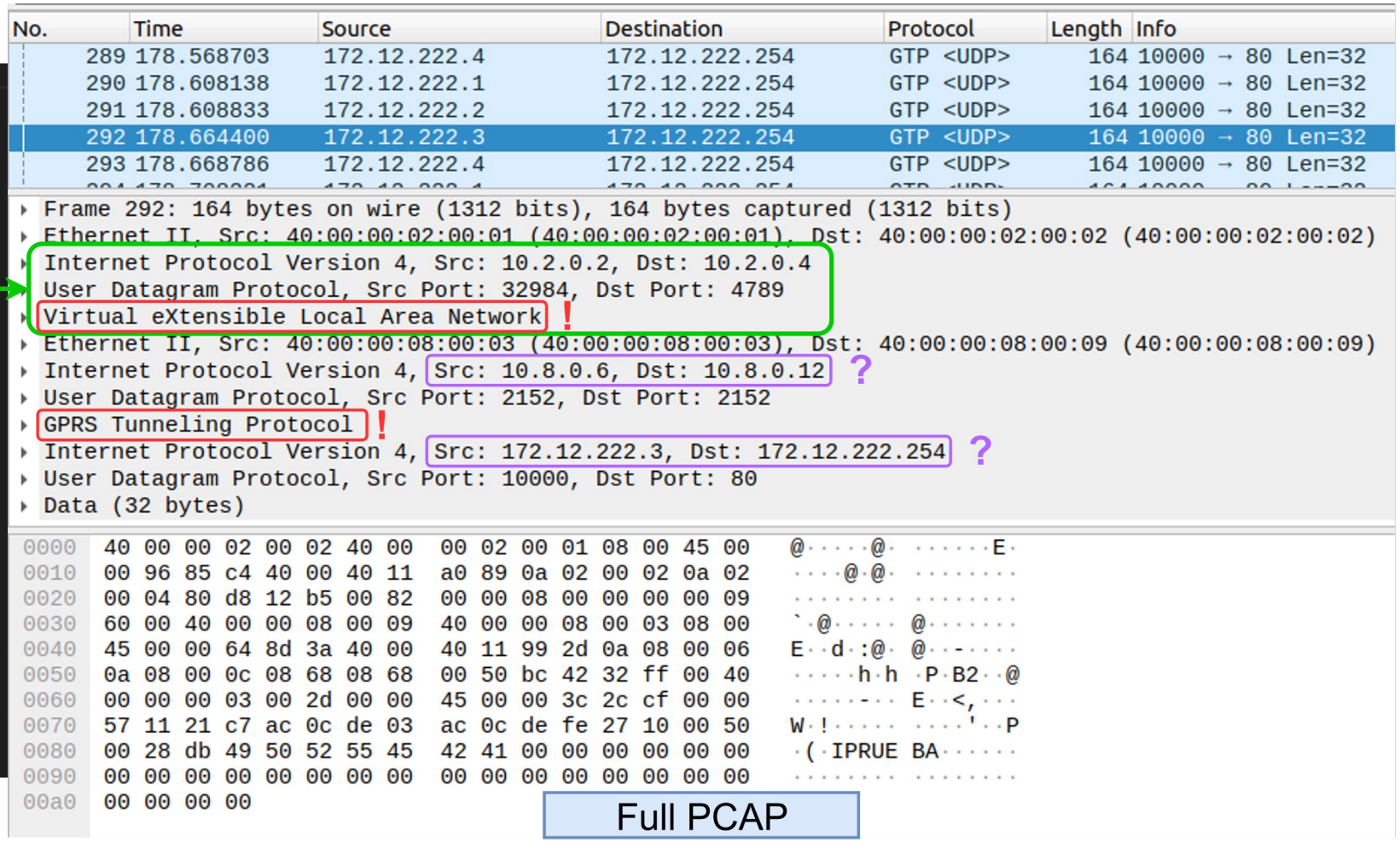



```
{
    "Resources": {
        "flowResourceId": "D7B61291",
        "parentResourceId": "4A10897A",
        "encapsulationLayer": 2,
        "encapsulationID1": "00002904",
        "encapsulationID2": "00000007",
        "encapsulationType1": "vxlan",
        "encapsulationType2": "gtp",
        "sense": "INGRESS",
        "outMacSrc": "40:00:00:02:00:01",
        "outMacDst": "40:00:00:02:00:05",
        "srcIP": "10101100010100101101111000000111",
        "dstIP": "10101100010100101101111011111110",
        "outSrcIP": "00001010000000010000000000000010",
        "outDstIP": "00001010000000010000000000001010",
        "l4Proto": "17",
        "tos": "0",
        "srcPort": "10000",
        "dstPort": "80",
        "resourceAbstractionLayer": "2",
        "resourceId": "4EDD01D3",
        "resourceType": "FLOW_SAMPLE",
        "state": "ACTIVE",
        "serviceInstanceResourceId": "16168DAF",
        "reportedTime": 1669221845231
    },
    "Alert": {
        "alertName": "7",
        "alertReasonId": "10000002",
        "alertAssertionType": "NEGATIVE",
        "alertImpact": 2,
        "alertTime": 1669221843961,
        "resourceId": "D4E23FA9",
        "resourceType": "ALERT",
        "state": "FIRED",
        "serviceInstanceResourceId": "16168DAF",
        "reportedTime": 1669221845235
    }
```

NETWORK FLOW MONITORING

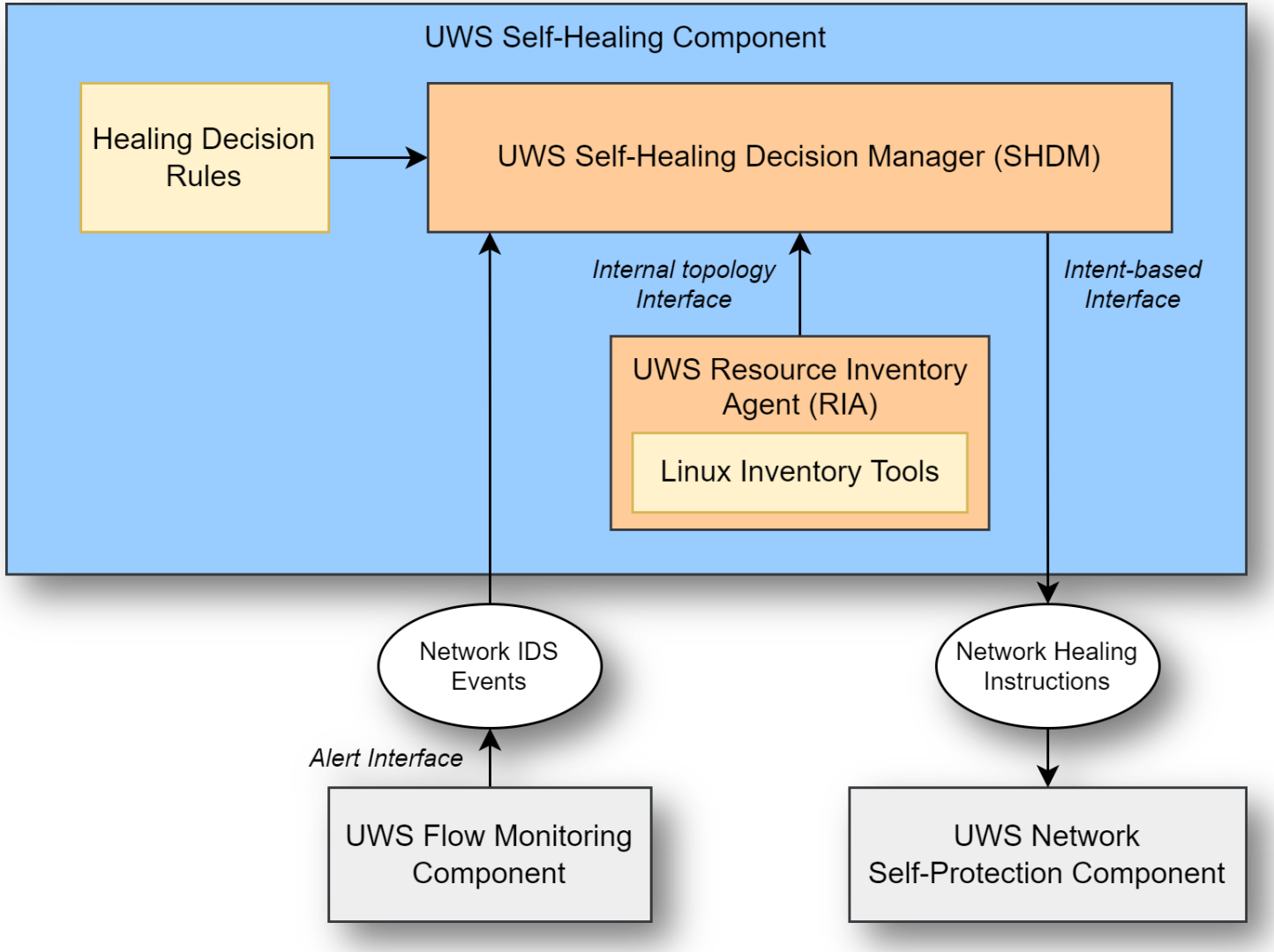


Snort IDS Event

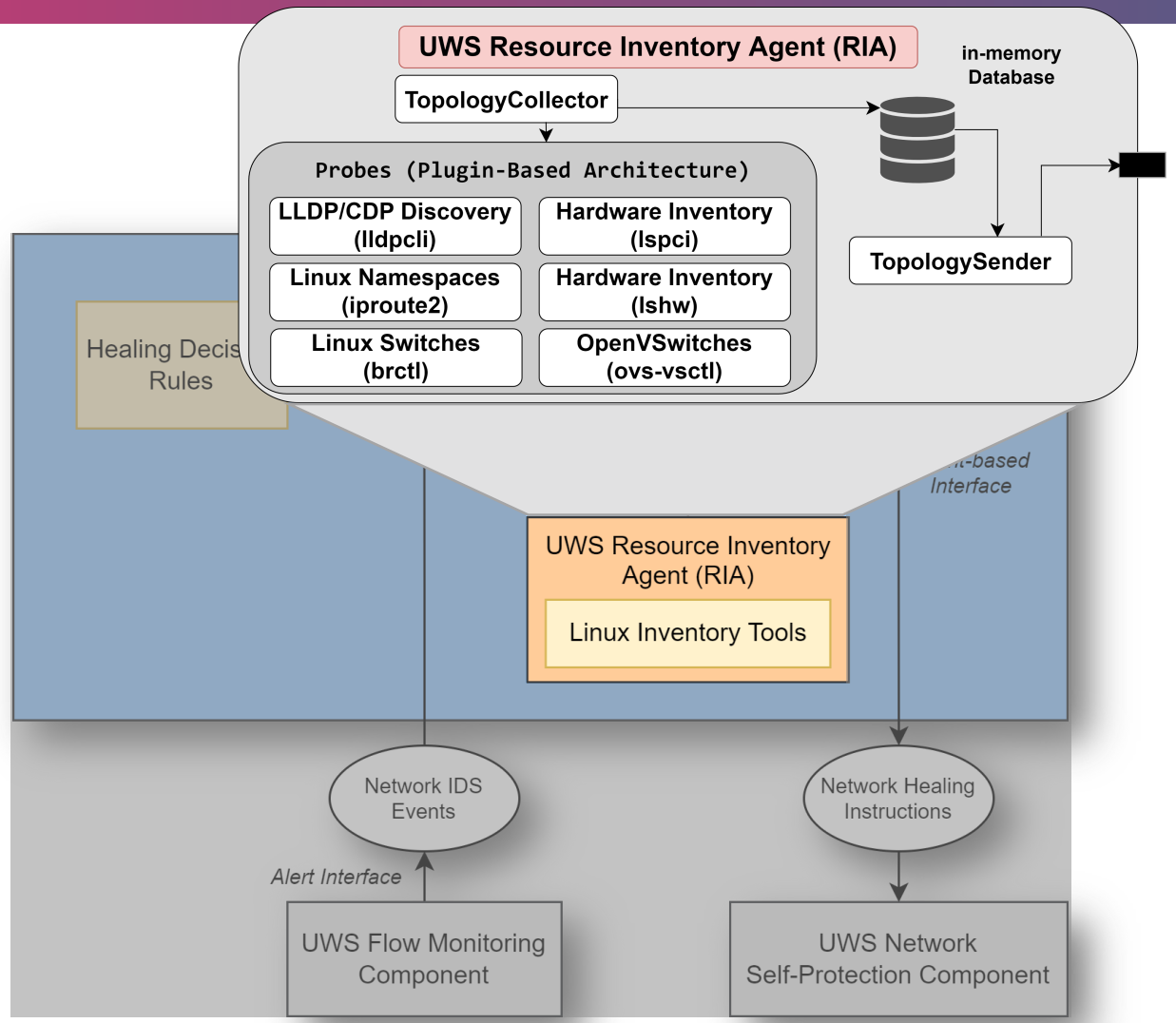


Full PCAP

NETWORK SELF-HEALING



NETWORK SELF-HEALING

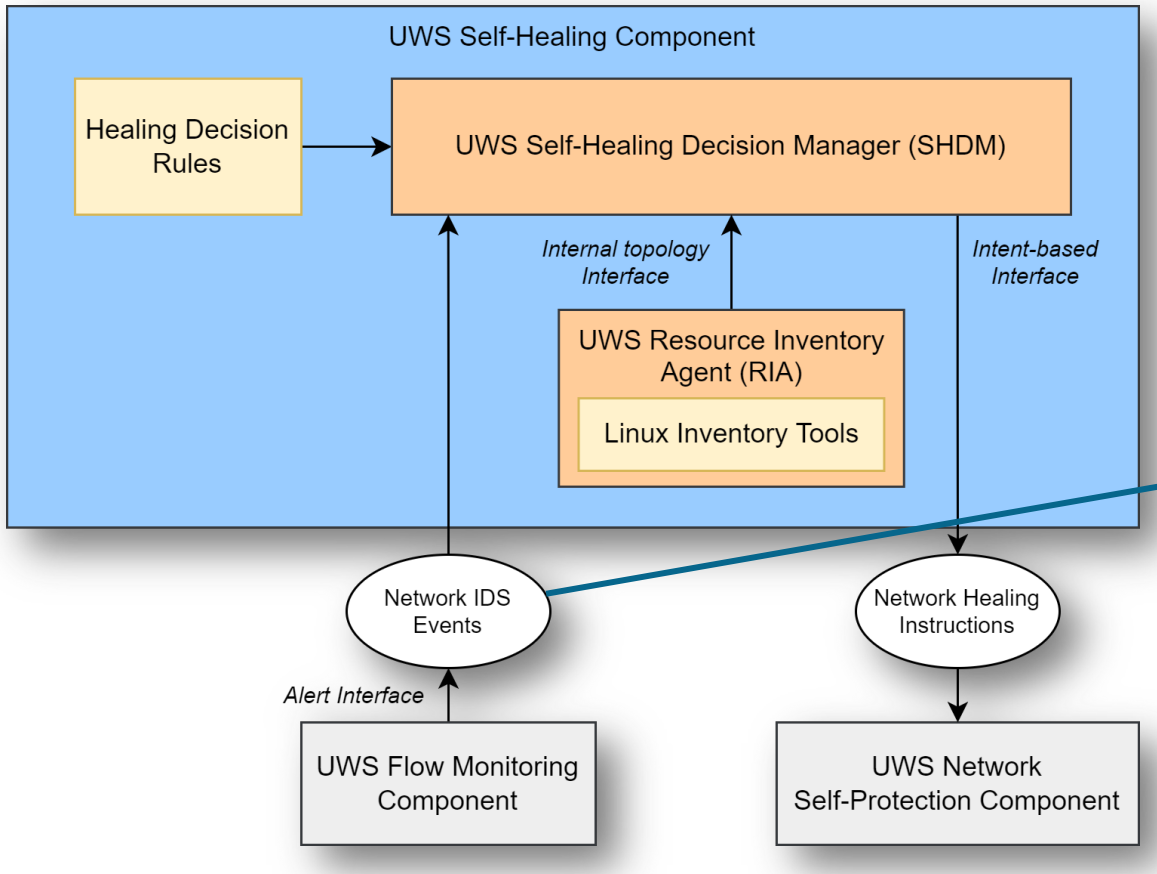


Topology information

Collected by the UWS Resource Inventory Agent (RIA) with supported technologies:

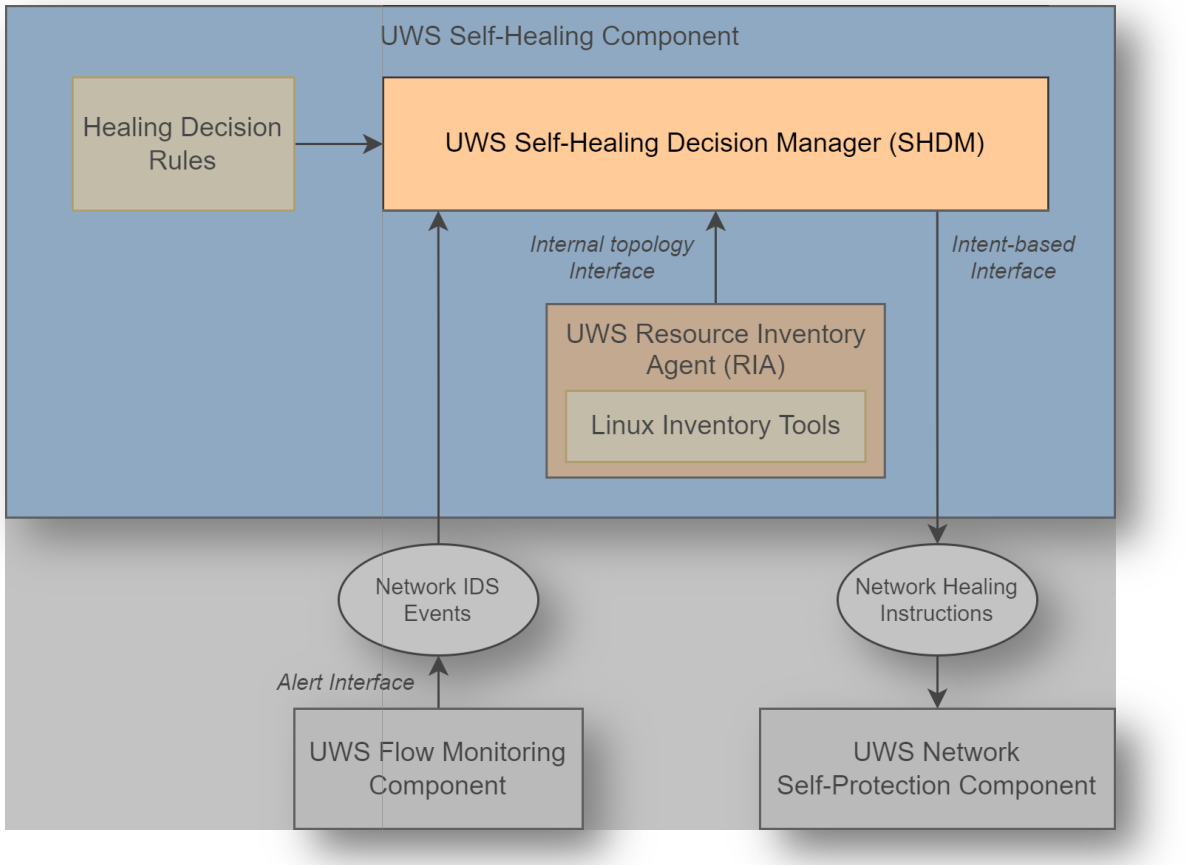
- **lldpcli**: Neighbours inventory
- **lspci**: PCI devices inventory
- **iproute2**: Network interfaces and namespaces
- **lshw**: Host hardware inventory
- **brctl**: Linux bridges inventory
- **ovs-vsctl**: OvS bridges inventory

NETWORK SELF-HEALING




```
{
    "Resources": {
        "flowResourceId": "D7B61291",
        "parentResourceId": "4A10897A",
        "encapsulationLayer": 2,
        "encapsulationID1": "00002904",
        "encapsulationID2": "00000007",
        "encapsulationType1": "vxlan",
        "encapsulationType2": "gtp",
        "sense": "INGRESS",
        "outMacSrc": "40:00:00:02:00:01",
        "outMacDst": "40:00:00:02:00:05",
        "srcIP": "10101100010100101101111000000111",
        "dstIP": "10101100010100101101111011111110",
        "outSrcIP": "00001010000000100000000000000010",
        "outDstIP": "00001010000000100000000000001010",
        "l4Proto": "17",
        "tos": "0",
        "srcPort": "10000",
        "dstPort": "80",
        "resourceAbstractionLayer": "2",
        "resourceId": "4EDD01D3",
        "resourceType": "FLOW_SAMPLE",
        "state": "ACTIVE",
        "serviceInstanceResourceId": "16168DAF",
        "reportedTime": 1669221845231
    },
    "Alert": {
        "alertName": "7",
        "alertReasonId": "10000002",
        "alertAssertionType": "NEGATIVE",
        "alertImpact": 2,
        "alertTime": 1669221843961,
        "resourceId": "D4E23FA9",
        "resourceType": "ALERT",
        "state": "FIRED",
        "serviceInstanceResourceId": "16168DAF",
        "reportedTime": 1669221845235
    }
```

NETWORK SELF-HEALING

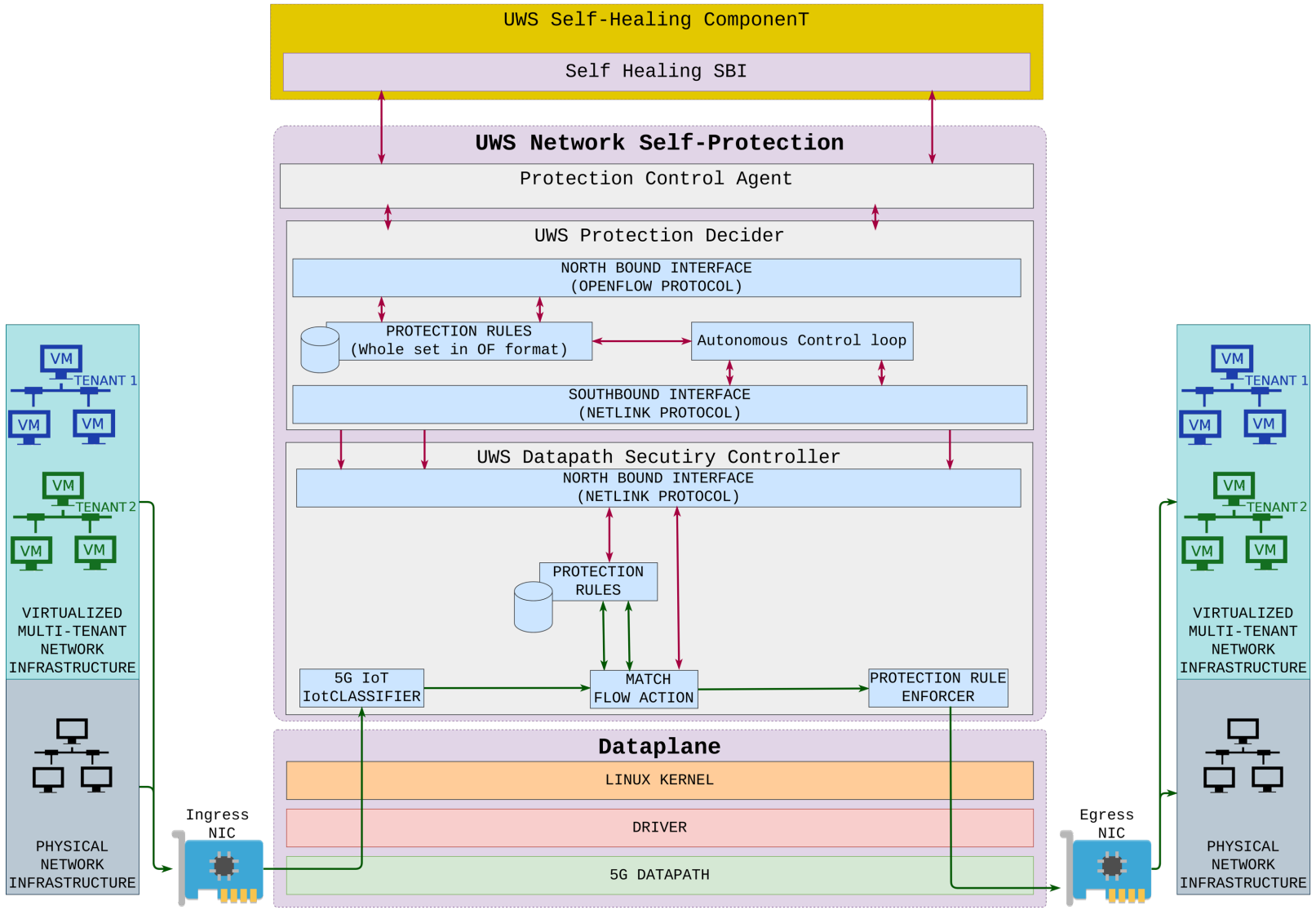


Prescriptive Analytics

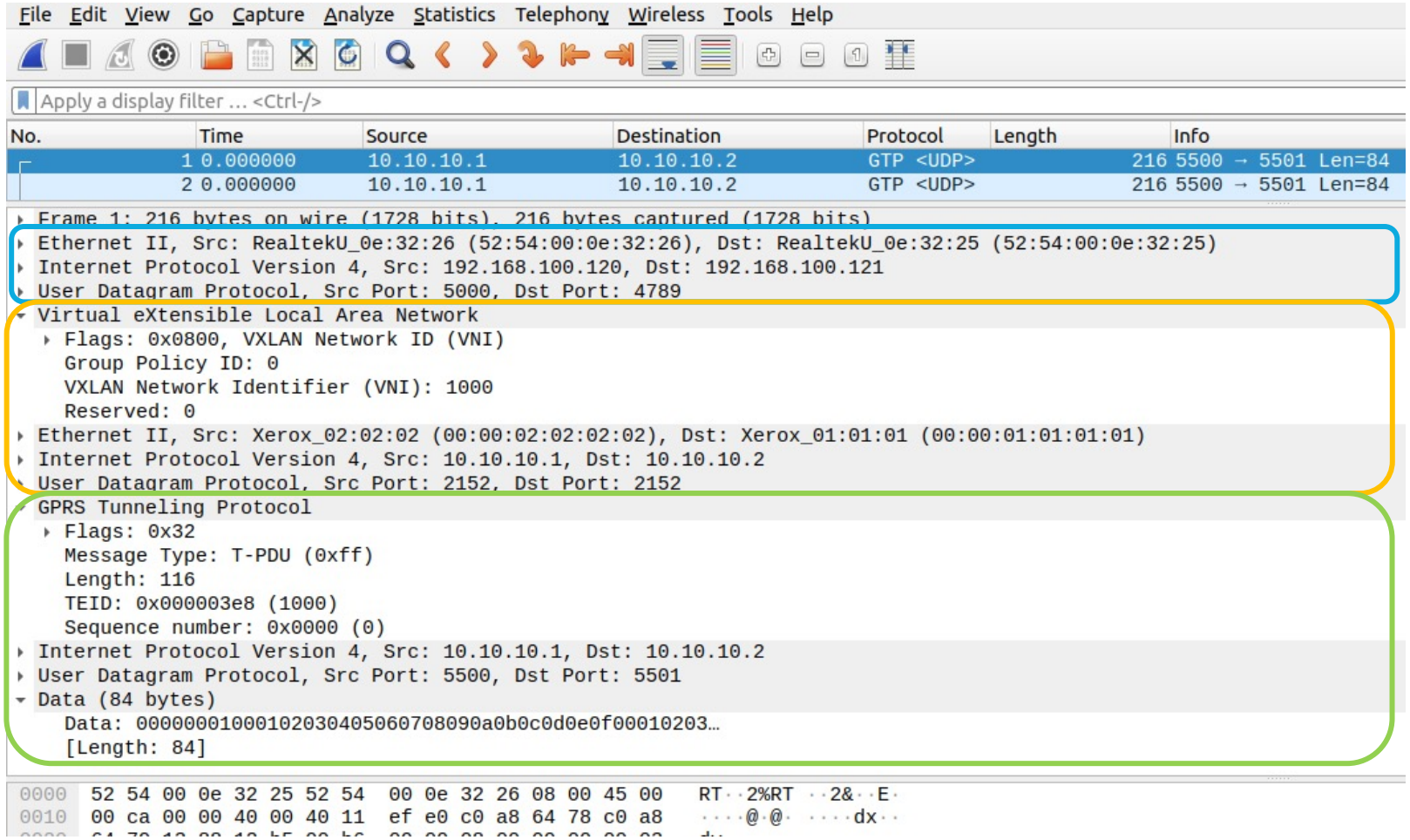
When an attack has been detected, we need to know:

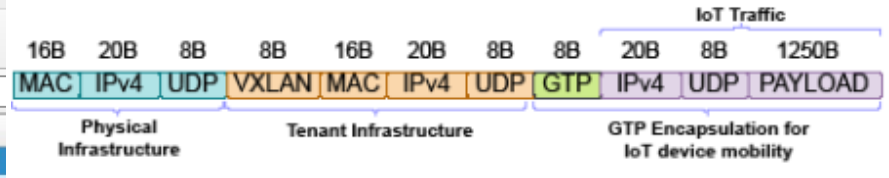
- WHAT action should be taken
- WHERE this action should be enforced
- WHEN it must be enforced
- For HOW LONG it must be active

NETWORK SELF-PROTECTION



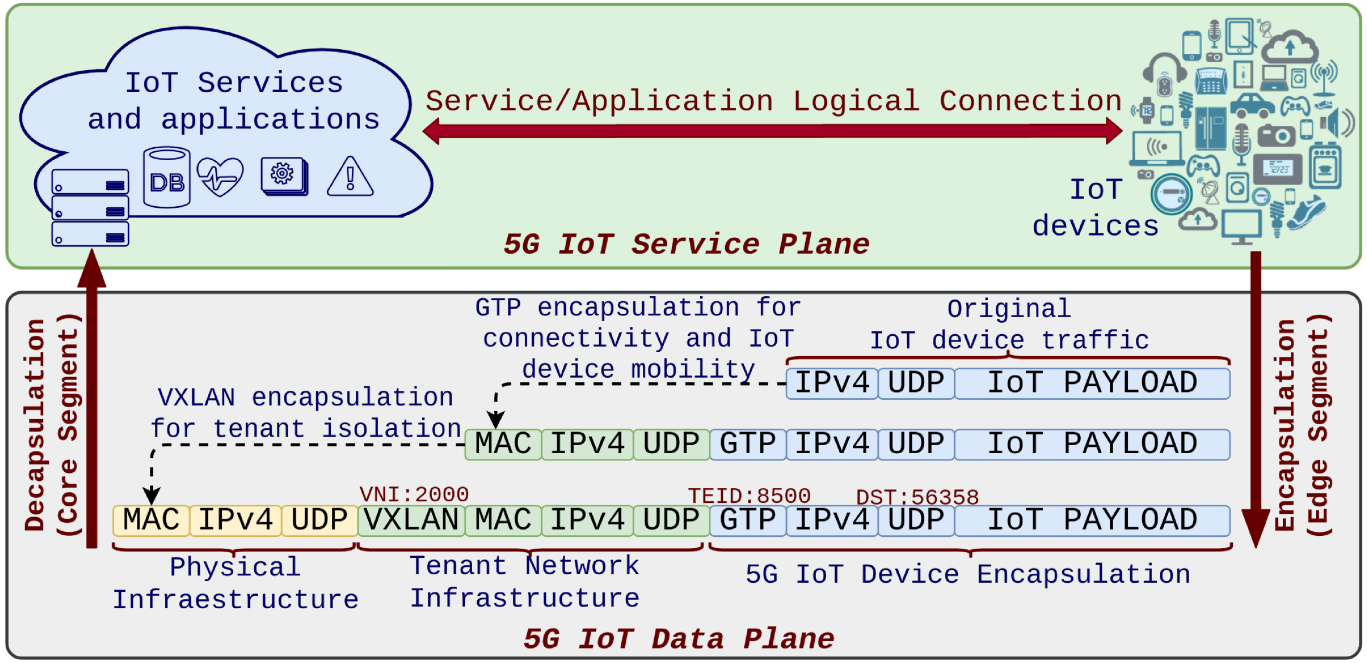
NETWORK SELF-PROTECTION





- Infrastructure traffic
- Tenant traffic (VXLAN for tenant isolation)
- IoT device traffic (VXLAN+GTP headers for user identification and isolation)

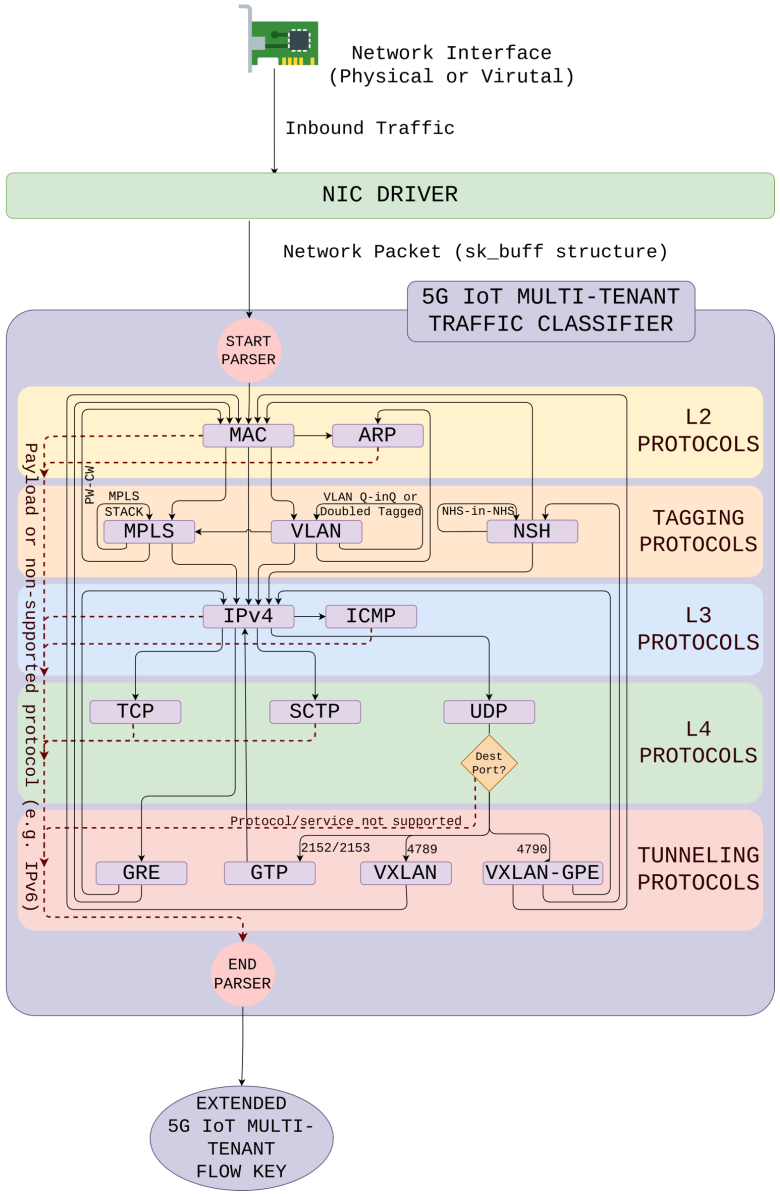
NETWORK SELF-PROTECTION



The same original IoT packet transmitted by an IoT device or sensor can have different packet structure with different encapsulation and tunnelling headers depending on the network segment.

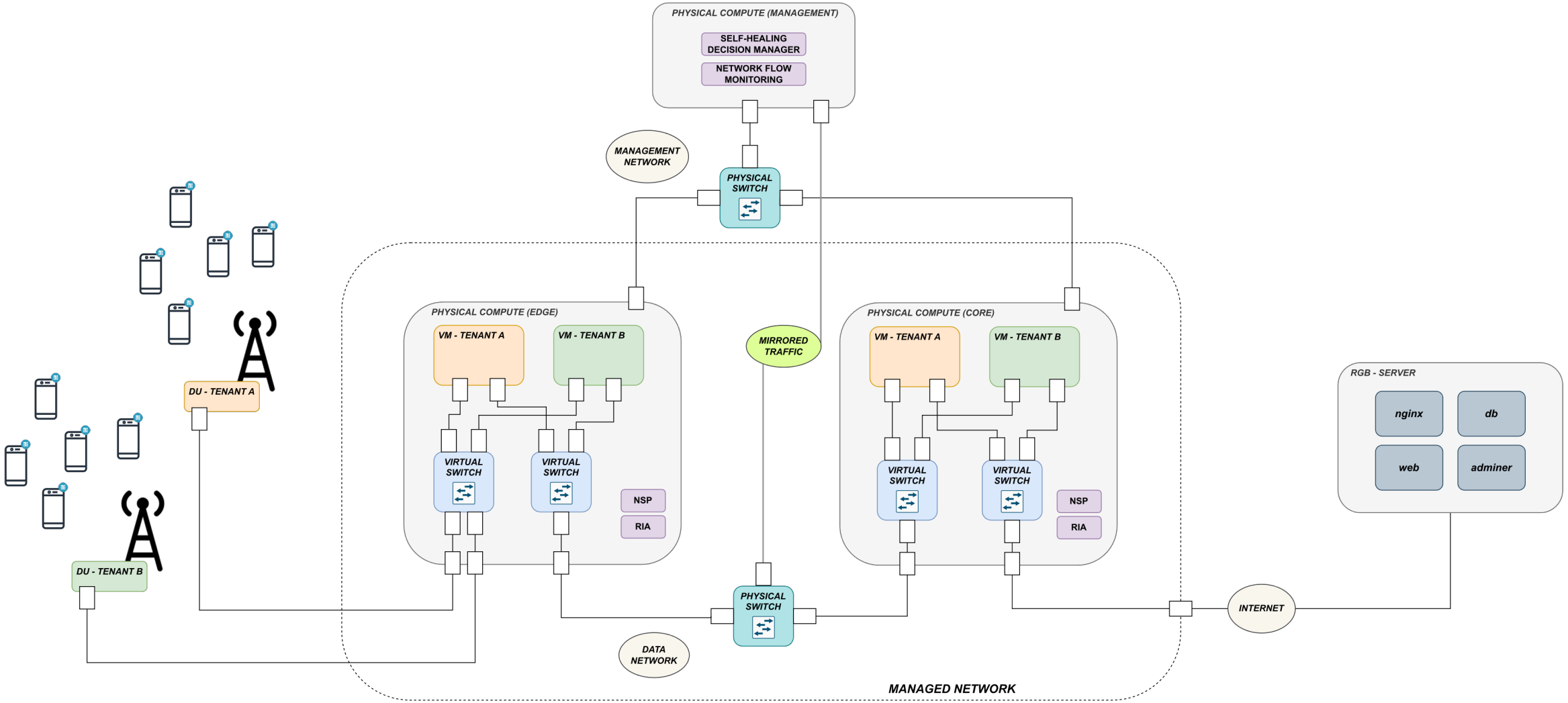
5G IOT MULTI-TENANT CLASSIFIER FEATURES

- Classifier with re-entrance between headers to allow a deep packet inspection for traffic with several levels of encapsulations.
- Support for GTP protocol.
- Support for tunnelling and encapsulation protocols used in overlay networks such as GRE, VXLAN, VXLAN-GTE or VLAN.
- The outcome is an extended *5G-IoT key flow* with information about the inner headers that will allow the enforcement of fine-grained security policies (e.g. stop the IoT traffic from a single IoT device) and in different datapaths expected in 5G multi-tenant networks.
- Modular design allowing for flexible and easy extension to support other network protocols.

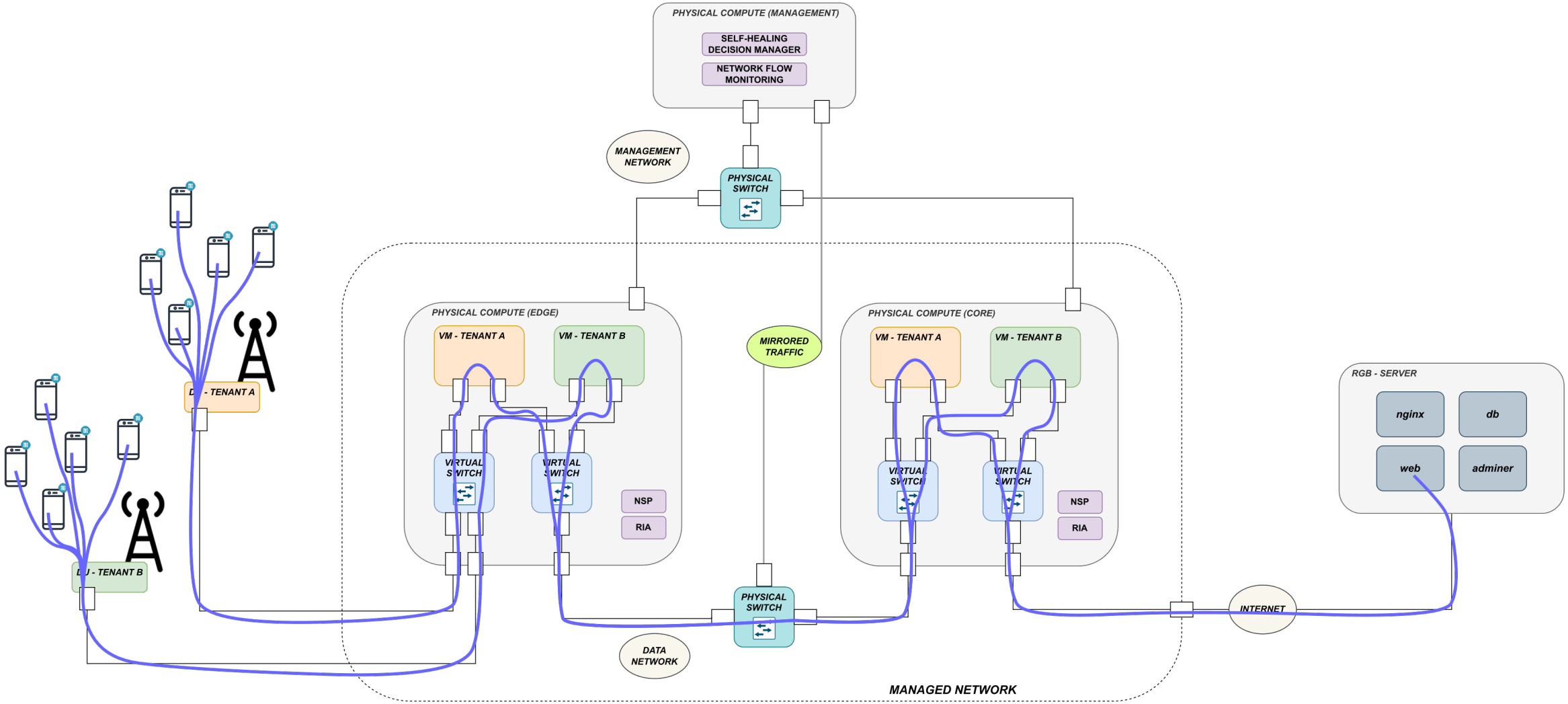


4. THREAT DETECTION, PLANNING AND MITIGATION

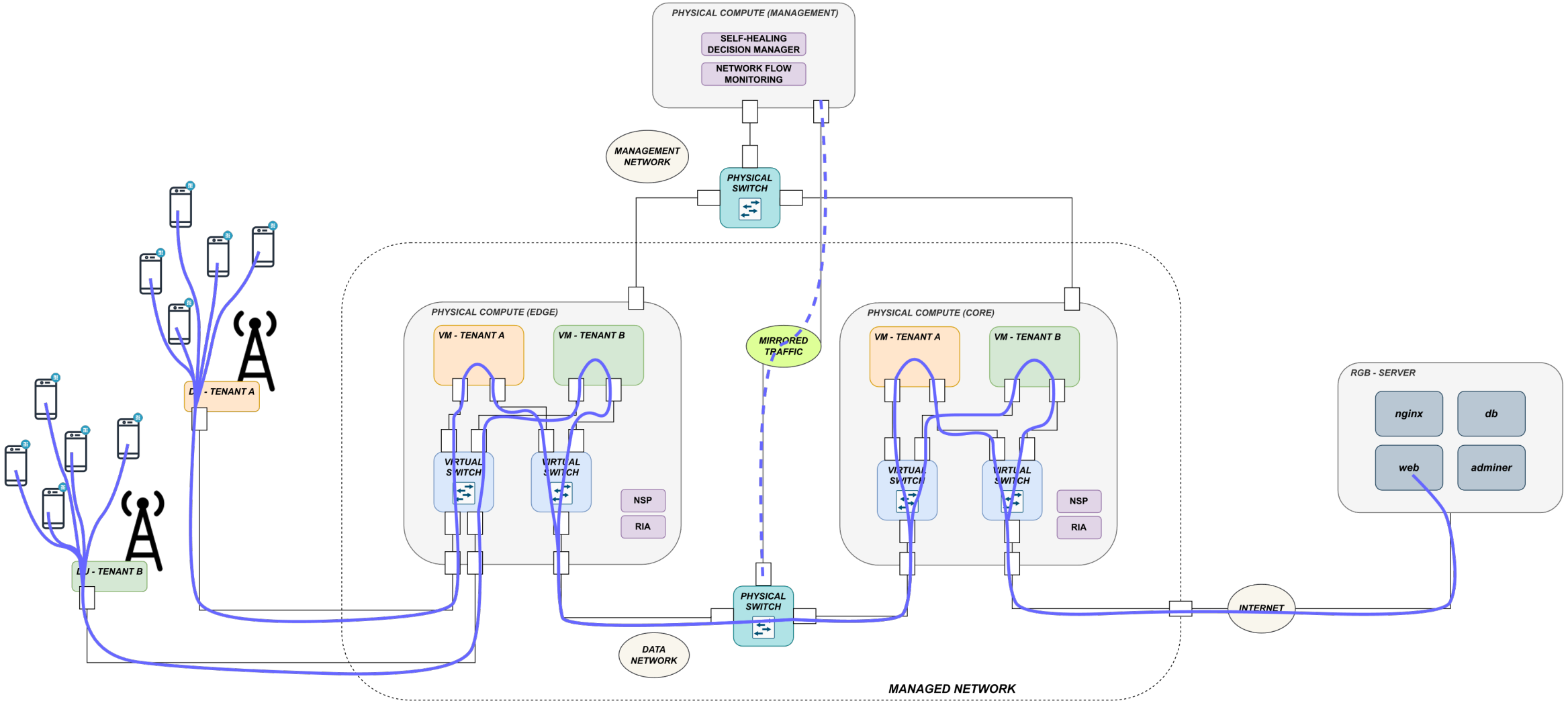
THREAT DETECTION, PLANNING AND MITIGATION



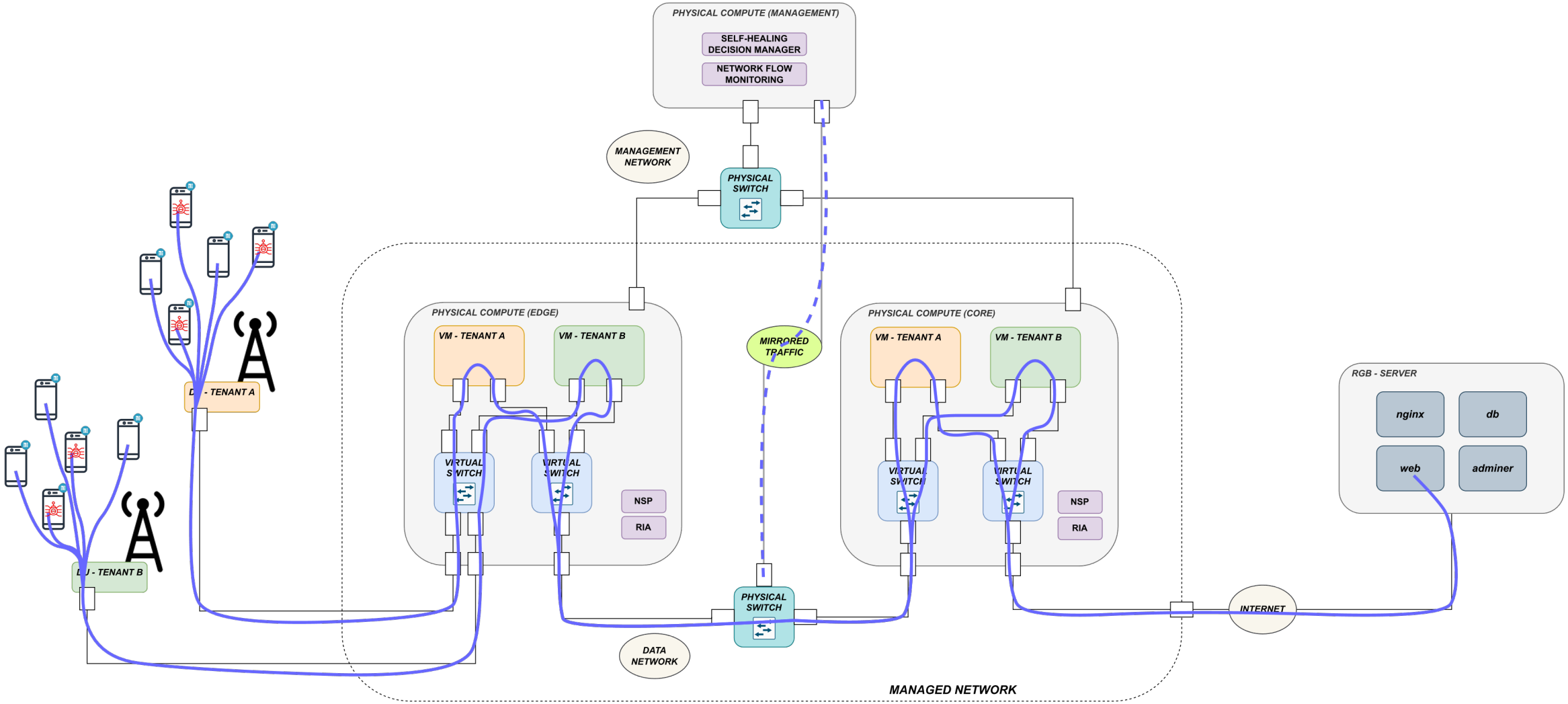
THREAT DETECTION, PLANNING AND MITIGATION



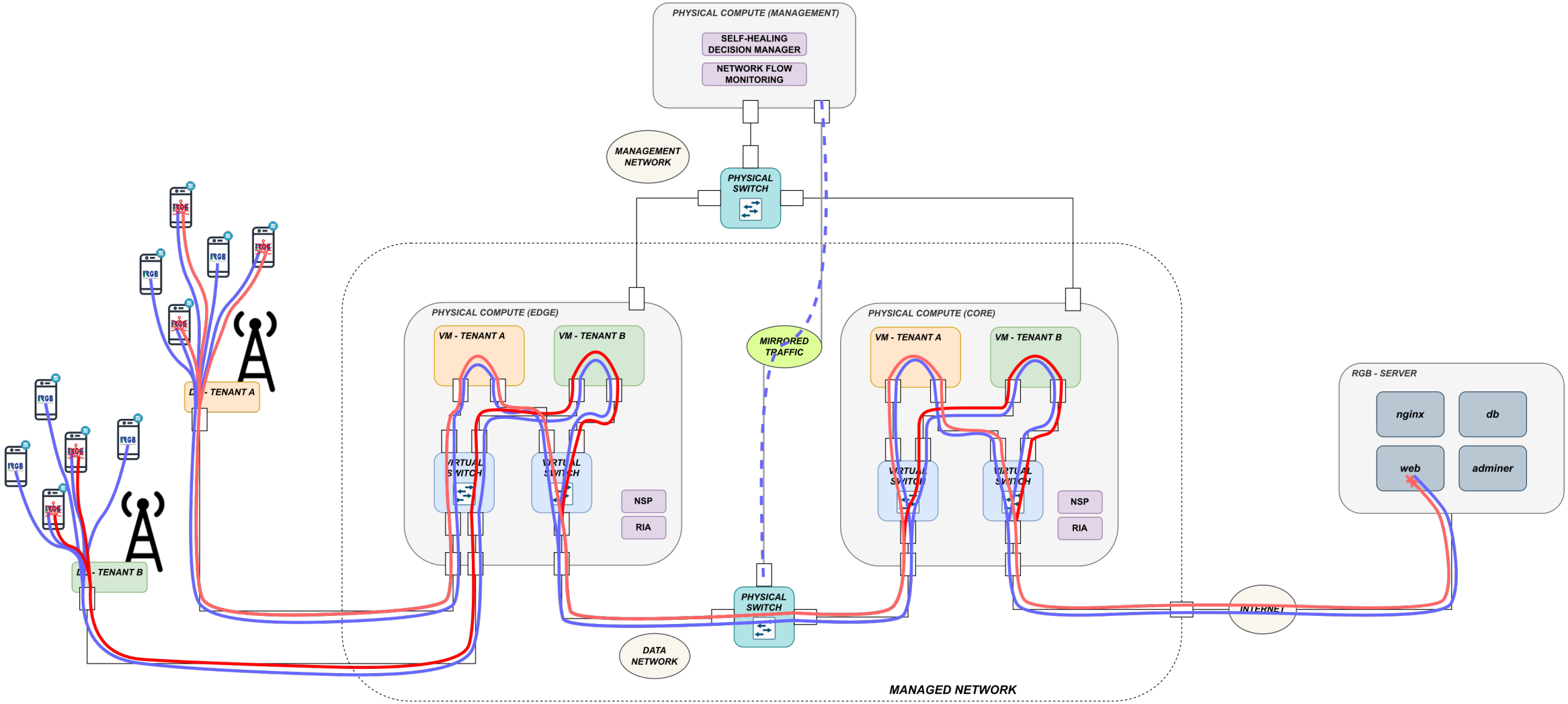
THREAT DETECTION, PLANNING AND MITIGATION



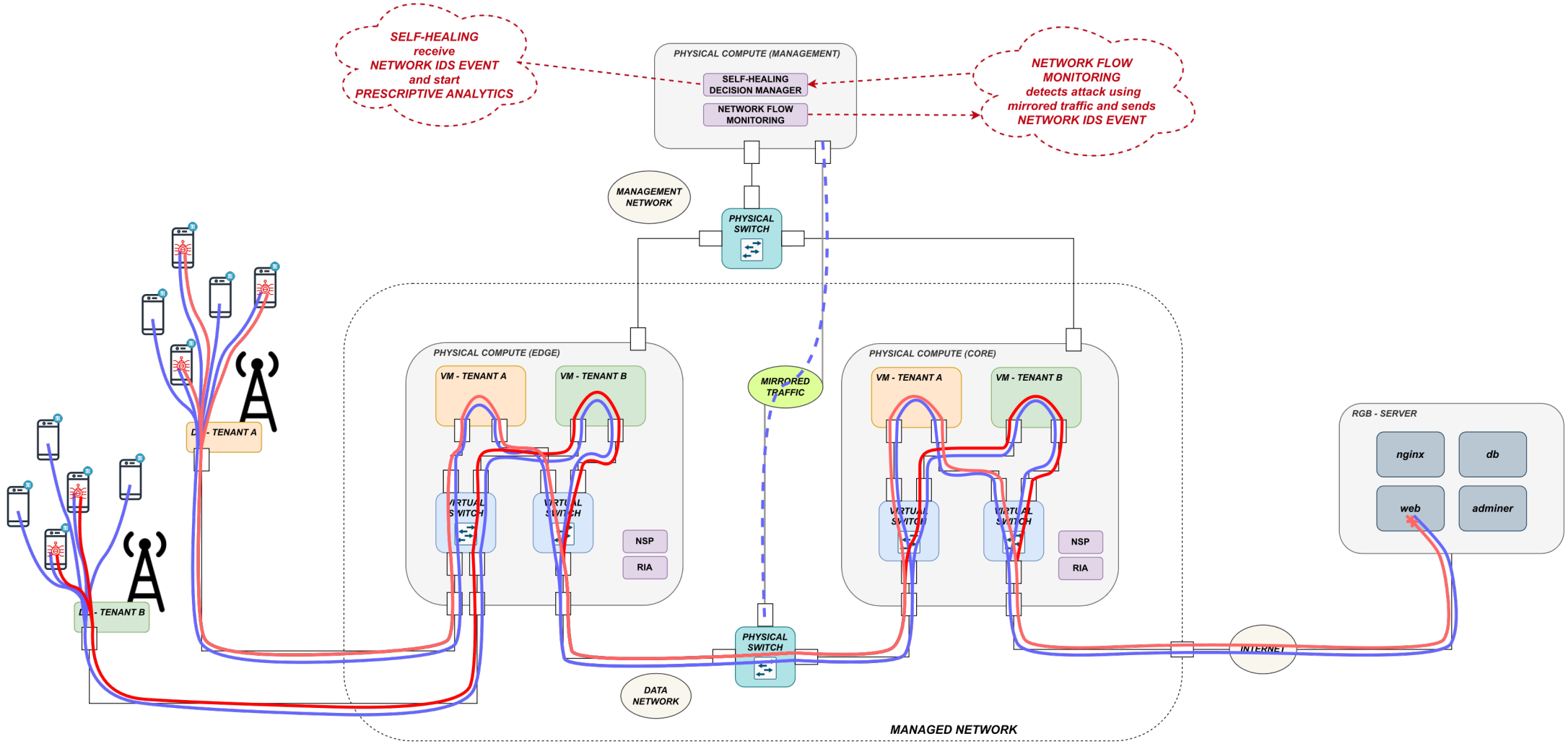
THREAT DETECTION, PLANNING AND MITIGATION



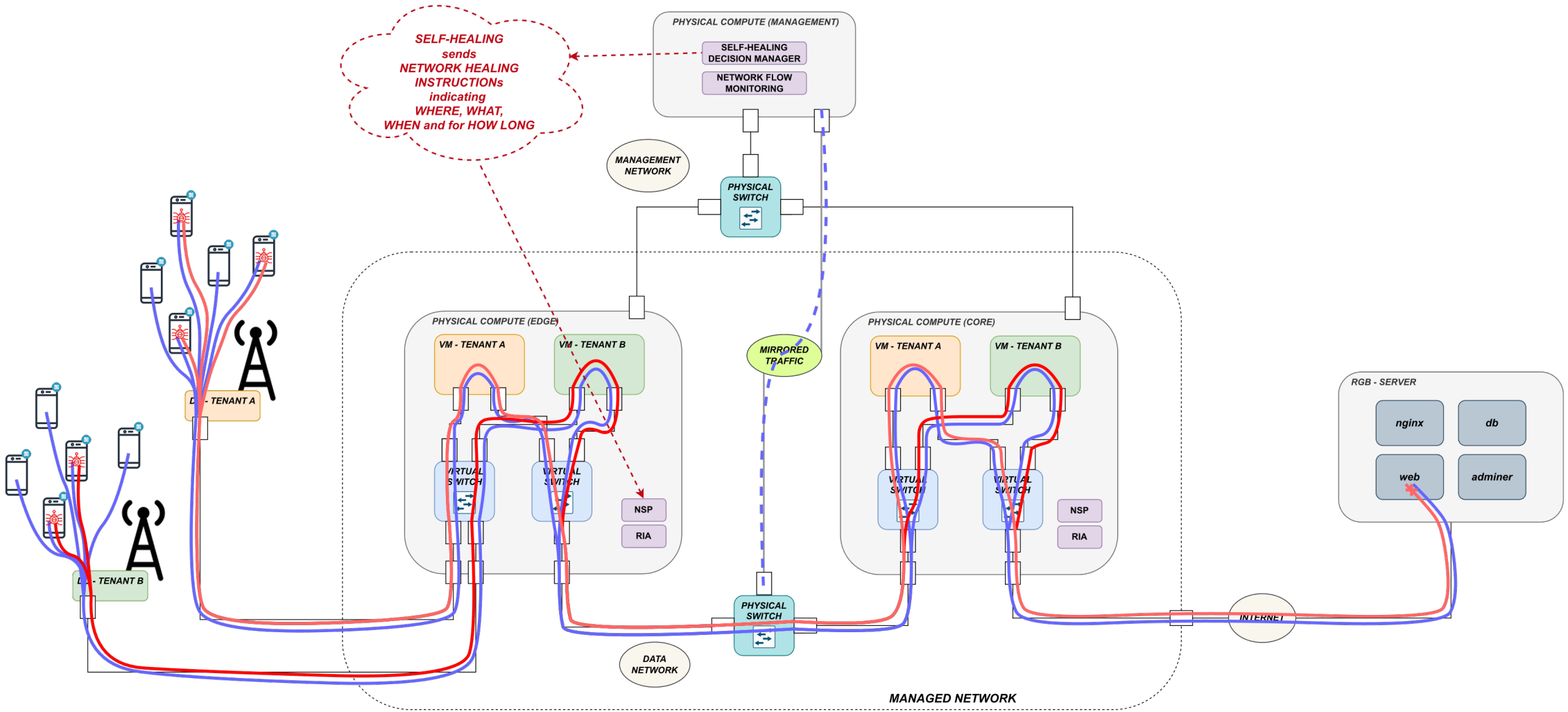
THREAT DETECTION, PLANNING AND MITIGATION



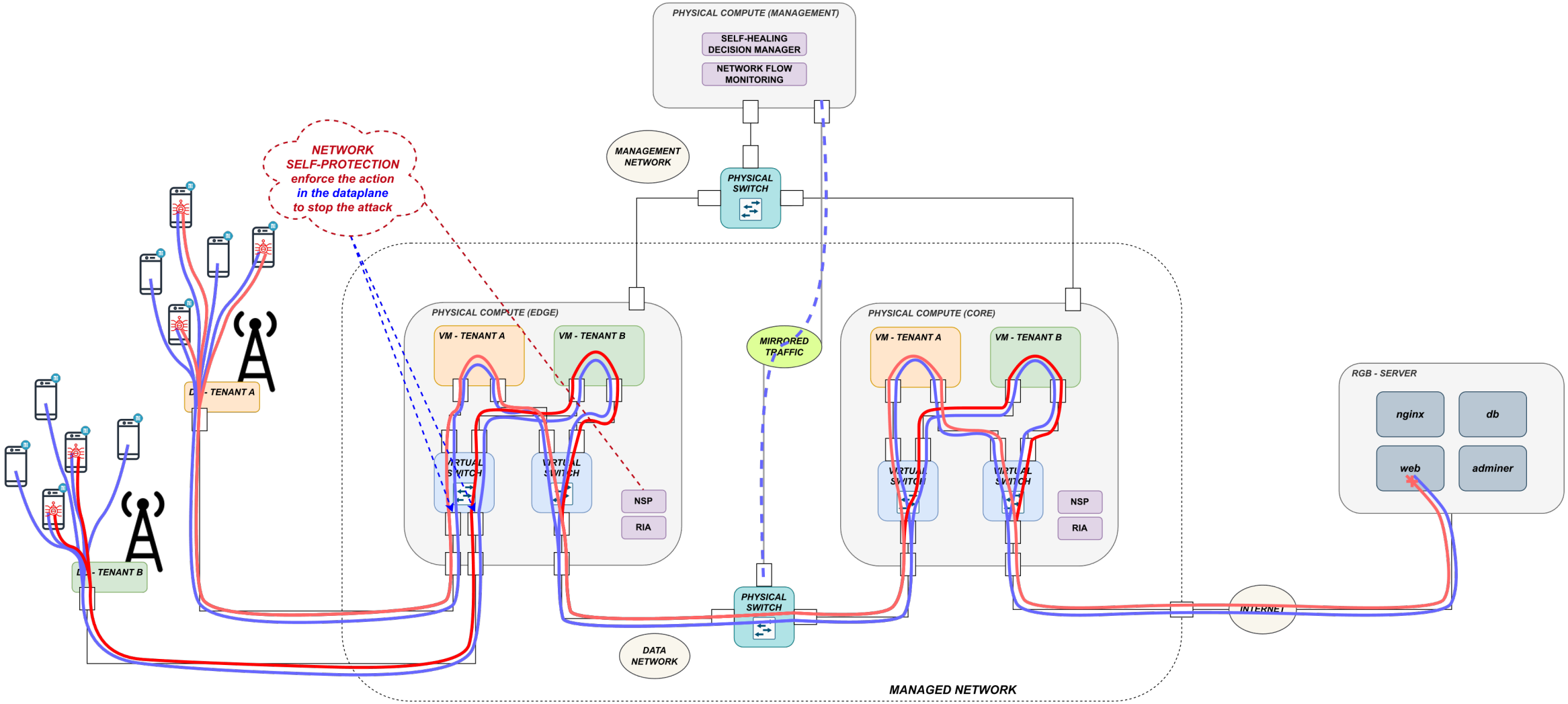
THREAT DETECTION, PLANNING AND MITIGATION



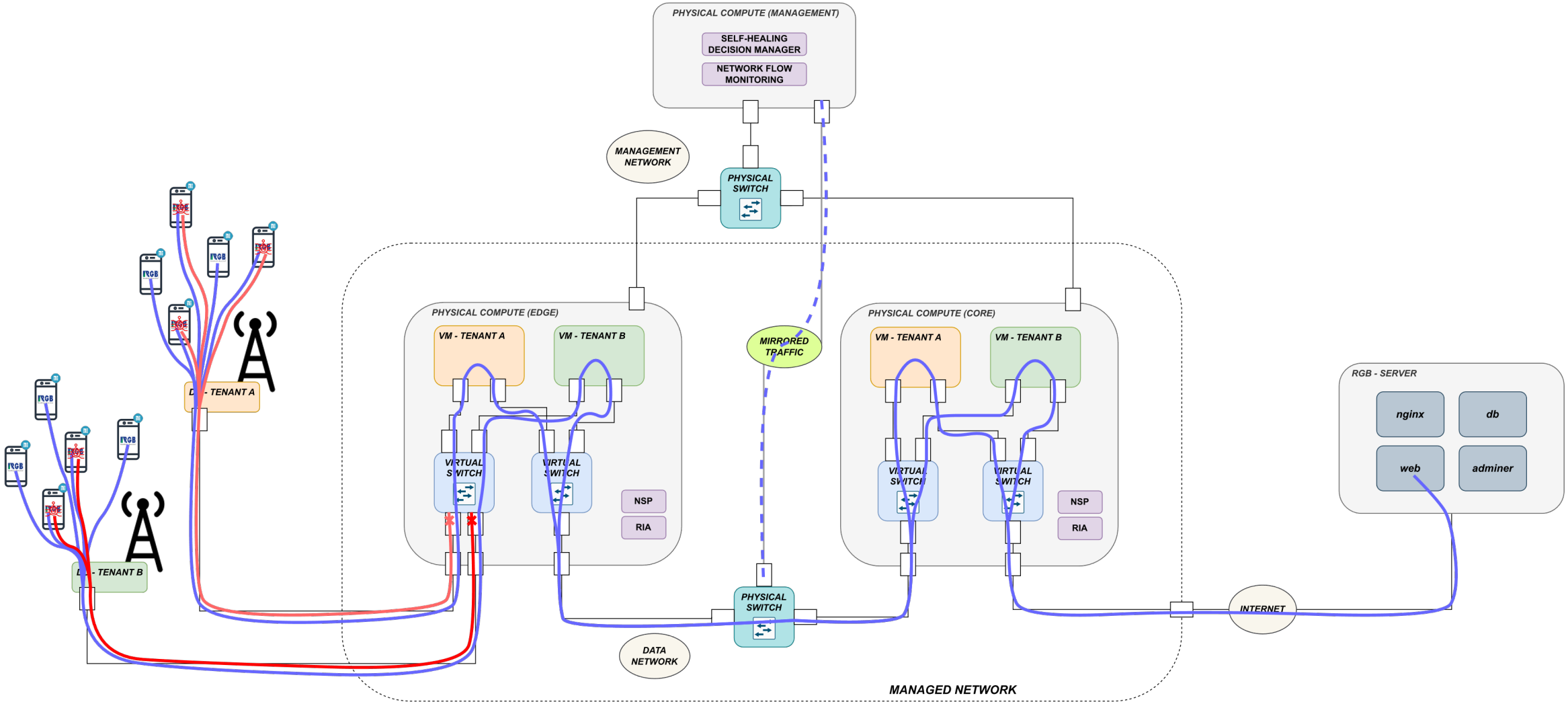
THREAT DETECTION, PLANNING AND MITIGATION



THREAT DETECTION, PLANNING AND MITIGATION



THREAT DETECTION, PLANNING AND MITIGATION



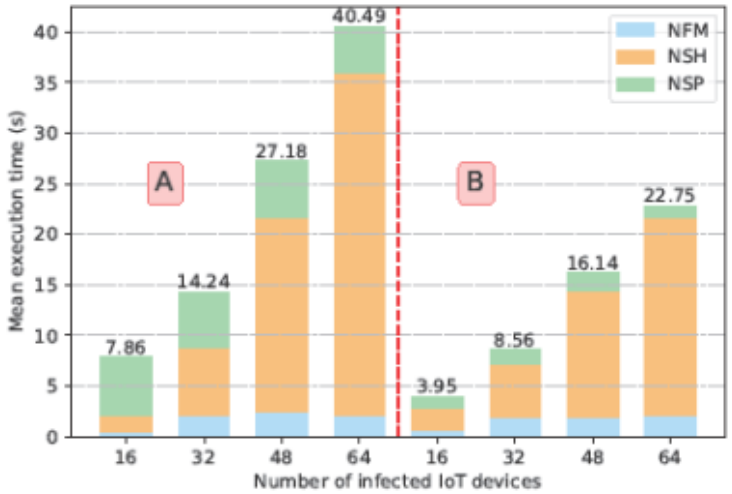
5. DEMO

6. CONTRIBUTIONS

CONTRIBUTIONS

Manuscript for The 31st IEEE International Conference on Network Protocols in Reykjavik, Iceland, October 10-13, 2023

- Shows different experiments that validate the framework proposed as a Self-protection loop within the three main network security components presented in this project
- Shows promising results with respect to time consumed by the framework to detect, plan and mitigate a DDoS threat (less than 47 seconds).



Topology-aware Cognitive Self-protection Framework for Automated Detection and Mitigation of Security and Privacy Incidents in 5G-IoT Networks

1st Pablo Benlloch-Caballero
University of the West of Scotland, UK
Pablo.Benlloch-Caballero@uws.ac.uk

2nd Ignacio Sanchez-Navarro
University of the West of Scotland, UK
ignacio.sanchez@uws.ac.uk

3rd Antonio Matencio-Escolar
University of the West of Scotland, UK
antonio.matencio@uws.ac.uk

4th Jose M. Alcaraz Calero
University of the West of Scotland, UK
Jose.Alcaraz-Calero@uws.ac.uk

5th Qi Wang
University of the West of Scotland,UK
qi.wang@uws.ac.uk

***Abstract*—Internet of Things (IoT) coupled with 5G networks enable unprecedented levels of scalability and performance in the computing industry. These enhanced performance features allow to offer and deploy a wide range of new use cases and services in scenarios such as Smart Cities, Smart Grid or Industry 5.0 just to mention a few. However, the inherent complexity of such networks is a serious concern in terms of security. Furthermore, the vulnerability and low-power constraints of IoT devices make such networks a targeted vector for cyber criminals. In this contribution, authors present an innovative topology-aware Cognitive Self-protection framework able to detect and mitigate attacks in an autonomous way with no human intervention in the wired segments of 5G-IoT multi-tenant networks. Preliminary tests carried out on a realistic emulated testbed show promising results in terms of time spent in stopping DDoS attacks (less than 47 seconds) and scalability for scenarios with different number of tenants and UEs (2 virtual tenants deployed in 4 Edge nodes and up to 64 IoT devices or sensors connected to the infrastructure).**

***Index Terms*—Network Security, IoT, 5G, Zero Touch Network Management.**

I. Introduction

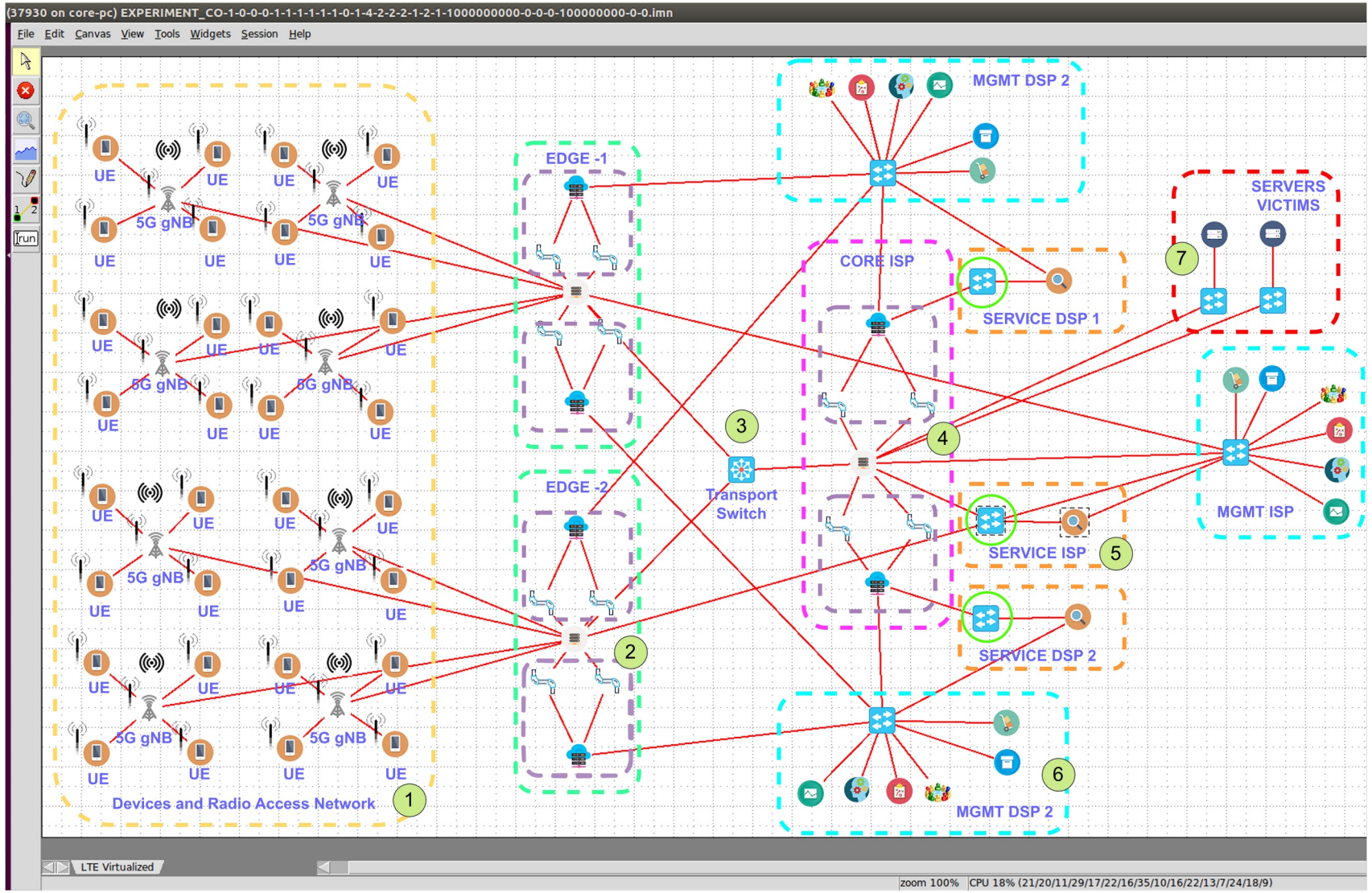
The deployment of IoT systems is growing rapidly worldwide, fuelled by 5G technology [1]. 5G is a key technology able to provide mass connectivity for IoT devices whilst delivering high data rates, higher bandwidth, and low latency in IoT landscapes, allowing it to meet the challenging demands and Quality of Service (QoS) parameters of new use cases otherwise unforeseen in 4G/LTE networks. Similarly, the amount along with more effective mechanisms for attack detection and mitigation.

As defined by 5G PPP in [2], there are different stakeholders involved in the provisioning of network resources in 5G-IoT networks. A major role is played by Digital Service Providers (DSPs), supplying a range of digital services to different verticals, industries, or end-users. Virtualization Infrastructure Service Providers (VISP) provide and operates virtualized physical infrastructure comprising networking and computing resources, offering Infrastructure as a Service (IaaS) to DSPs. Hence, different DSPs can share a common physical multi-tenant infrastructure provided and managed by the same VISP, resulting in savings in Capital Expenditure (CAPEX) and Operational Expenditure (OPEX).

However, the deployment of 5G-IoT multi-tenant networks implies the use of overlay networks with different levels of nested encapsulation to support user mobility, e.g. GPRS Tunnelling protocol (GTP), and tenant isolation, using protocols such as Virtual eXtensive LAN (VXLAN), or Generic Routing Encapsulation (GRE). Therefore, an advanced security solution for this type of network must provide protection not only for traditional IP traffic but also for fine-grained security capabilities to handle the complex network traffic associated with multi-tenant network topologies.

The main contribution of this research work is the design, prototyping, and validation of a novel automated Cognitive Self-protection framework with topology awareness capabili-

CONTRIBUTIONS



ARCADIAN-IoT

THANK YOU FOR YOUR ATTENTION

arcadian-iot.eu

B5GHUB
Powered by the University of the West of Scotland

ARCADIAN-IoT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020259

THIS PROJECT IS PART OF THE NEXT GENERATION IoT
www.ngiot.eu

ARCADIAN-IOT CONSORTIUM