



ARCADIAN-IoT UWSB5GHUB

WORKSHOP: NETWORK SELF-PROTECTION LOOP

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

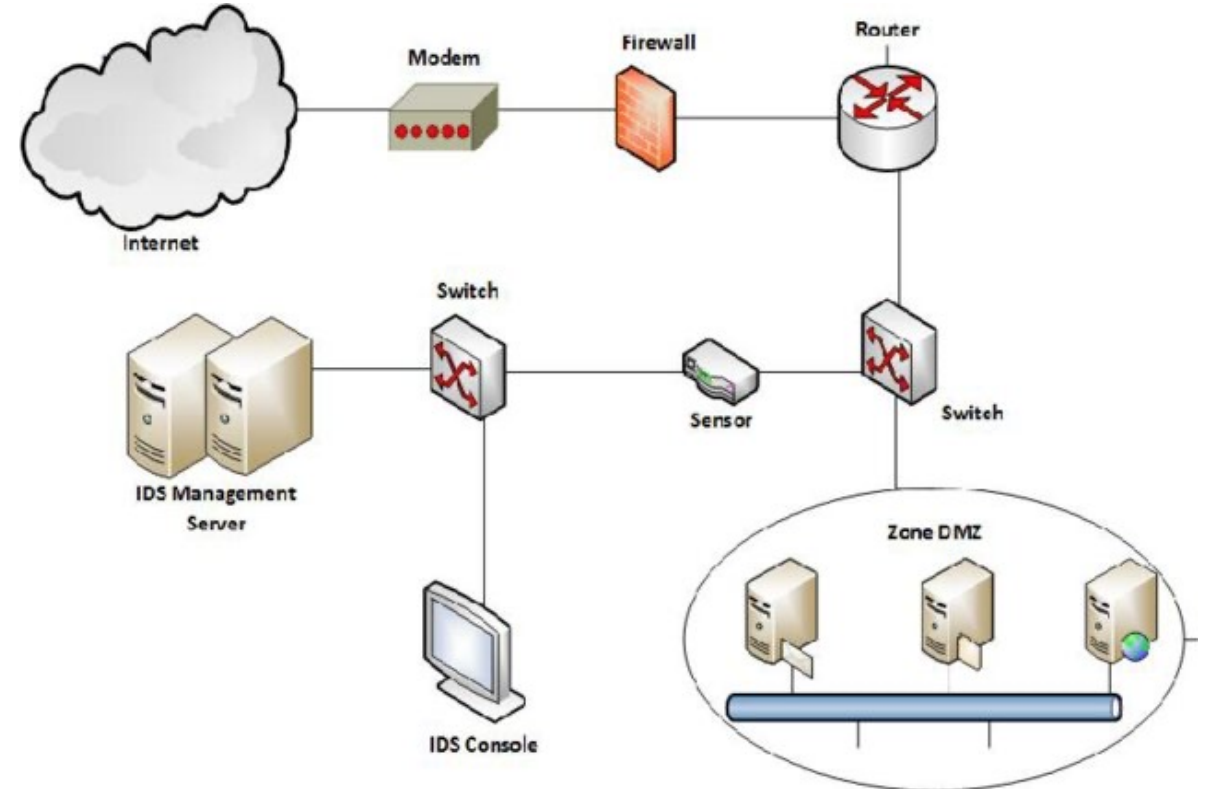
Training session, 26th September 2023, Coimbra

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

The background is a vertical gradient from pink on the left to blue on the right. Three decorative elements are present: a light pink circle with a line extending upwards from the top edge, a light blue circle with a line extending upwards from the top edge, and a light purple circle with a line extending downwards from the bottom edge.

1. MOTIVATION

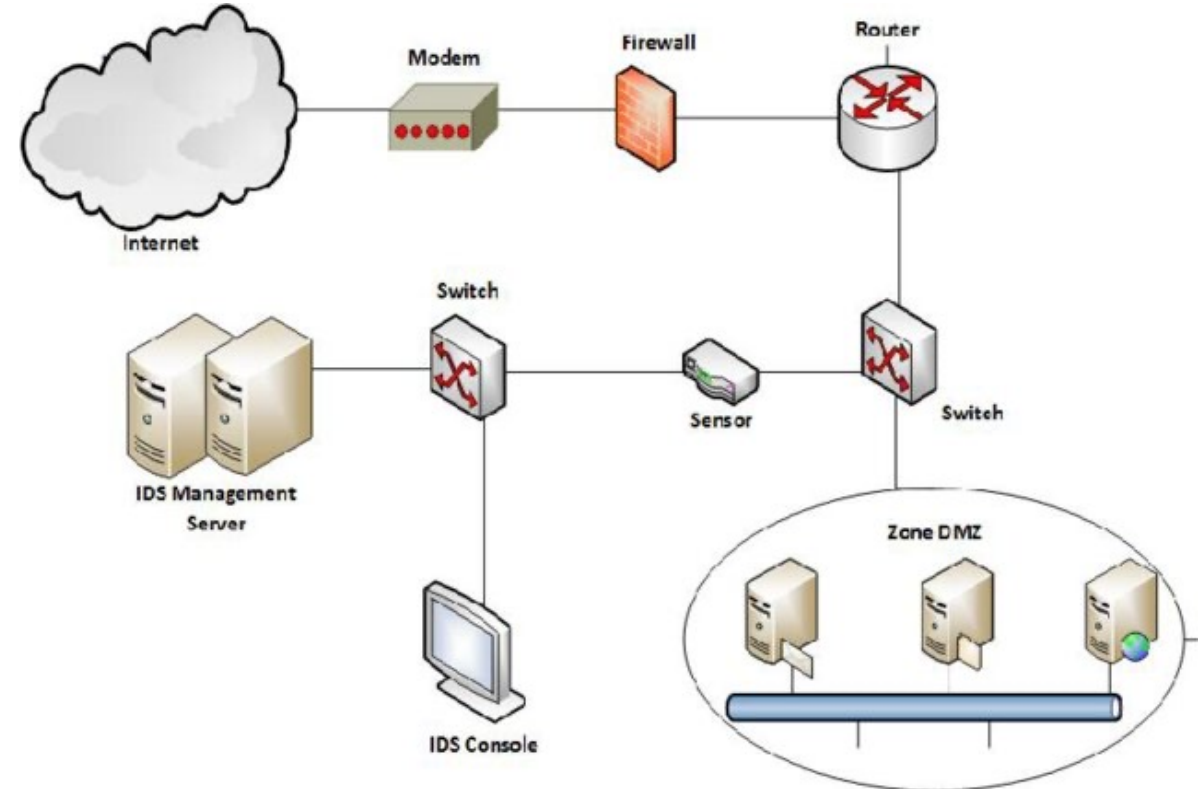
- For a network topology, the security administrators install few components to **monitor** the data incoming to the company services
- Usually, a switch mirrors the traffic so a sensor can detect a threat
- The sensor raises the alerts to the IDS management servers where the **security administrators**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



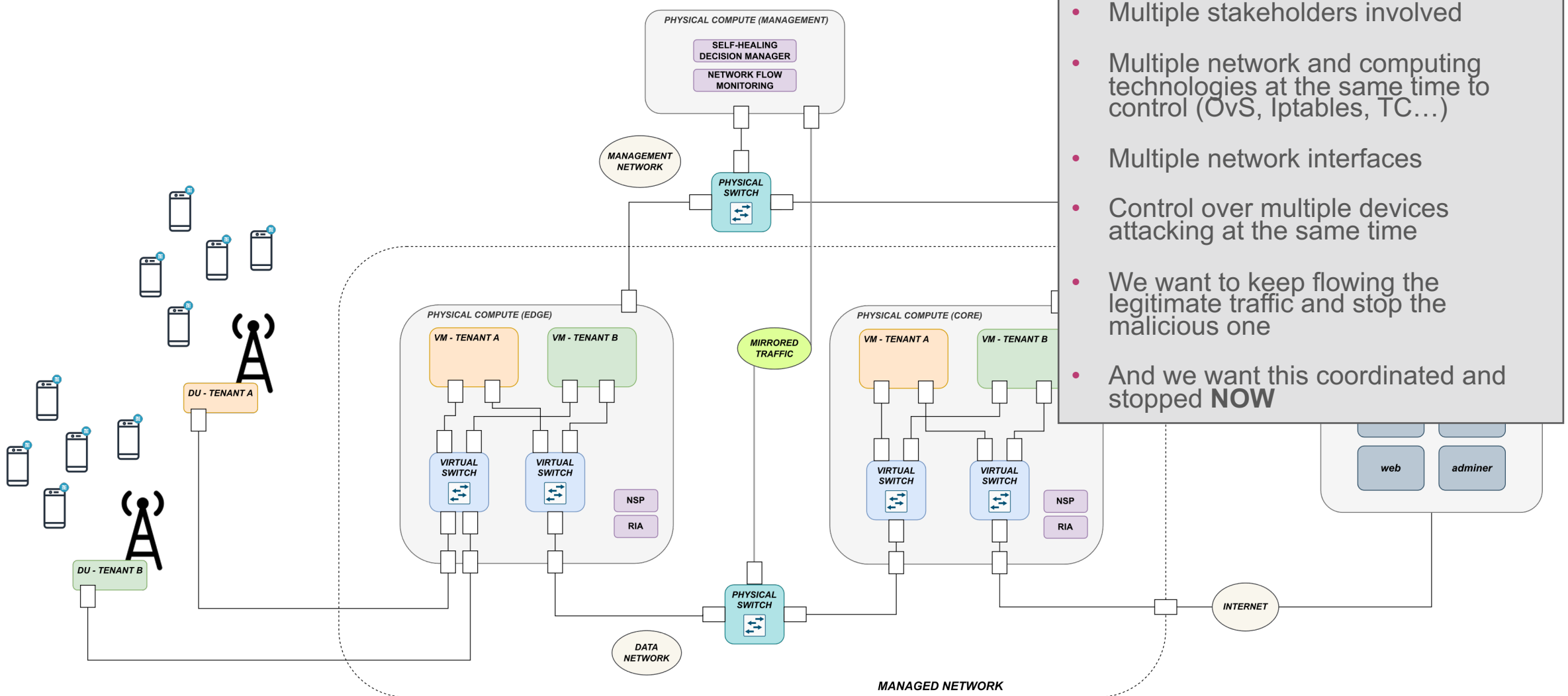
[DOI: 10.9781/ijimai.2017.439](https://doi.org/10.9781/ijimai.2017.439)

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



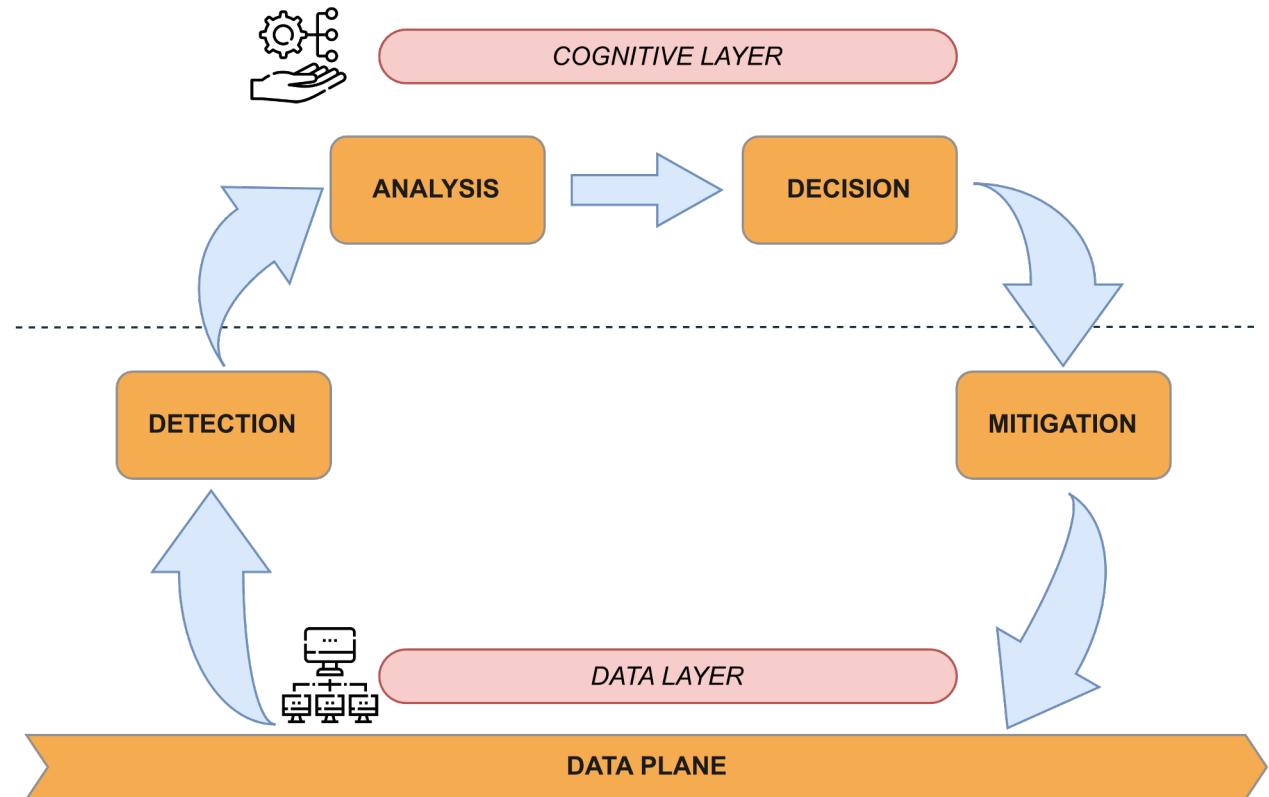
[DOI: 10.9781/ijimai.2017.439](https://doi.org/10.9781/ijimai.2017.439)



The background is a vertical gradient from magenta on the left to dark blue on the right. There are three decorative elements: a light purple circle with a line extending upwards from the top center, a light blue circle with a line extending upwards from the top right, and a light purple circle with a line extending downwards from the bottom center.

2. WHAT IS A 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



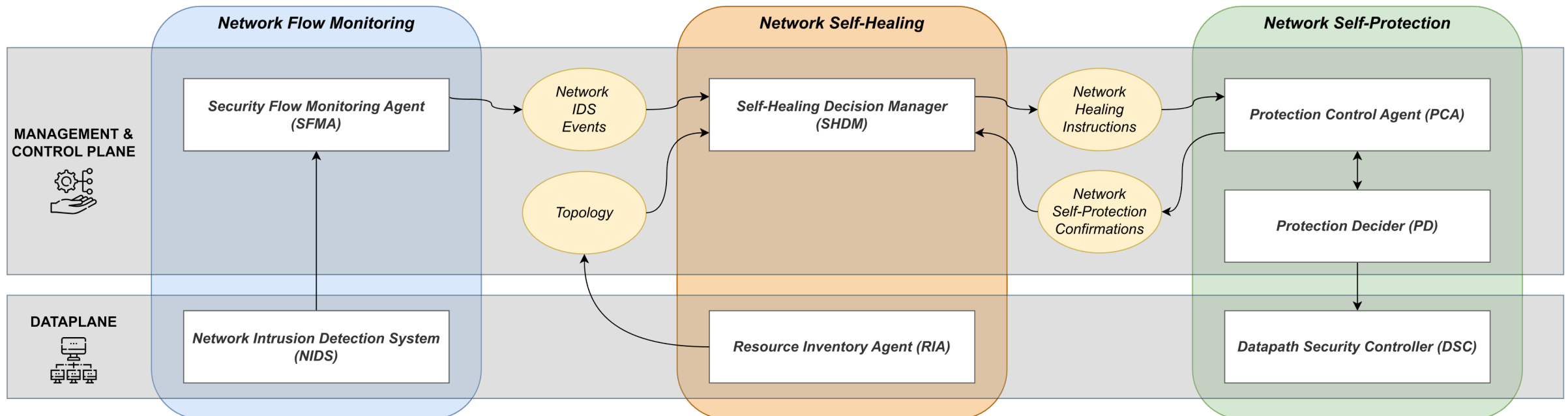
- Detect and identify real-time threats **no matter the complexity of the network topology**
- Provide the **fine grain metadata information** about the **flow and the topology** regarding the malicious flow detected
 - What IPs and network encapsulation layers the flow has
 - What are the points of 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

The background is a vertical gradient from magenta on the left to dark blue on the right. Three decorative elements are present: a light purple circle with a line extending upwards from the top center, a light blue circle with a line extending upwards from the top right, and a light purple circle with a line extending downwards from the bottom center.

3. ARCHITECTURE AND SOFTWARE COMPONENTS

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

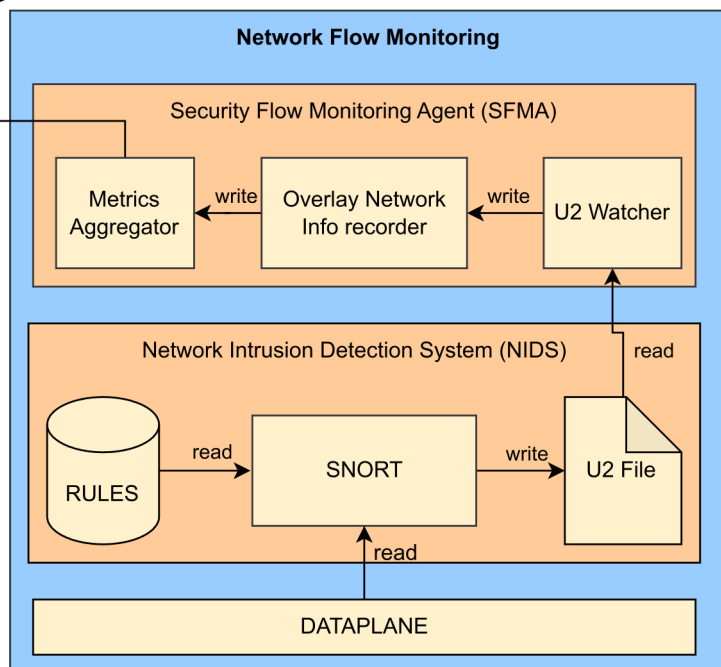
- Using a message-bus tool as RabbitMQ to exchange information between components
- NFM triggers an **Alert** → NSH takes a decision about **how to perform the mitigation** → NSP enforces the **healing action** in the Dataplane



Other ARCADIAN-IoT Components:

- Cyber Threat Intelligence (CTI)
- Reputation System
- Network Self-Healing

Network IDS Events



```
{
  "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": "0000101000000010000000000000010",
    "outDstIP": "000010100000001000000000000001010",
    "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
  }
}
```

```

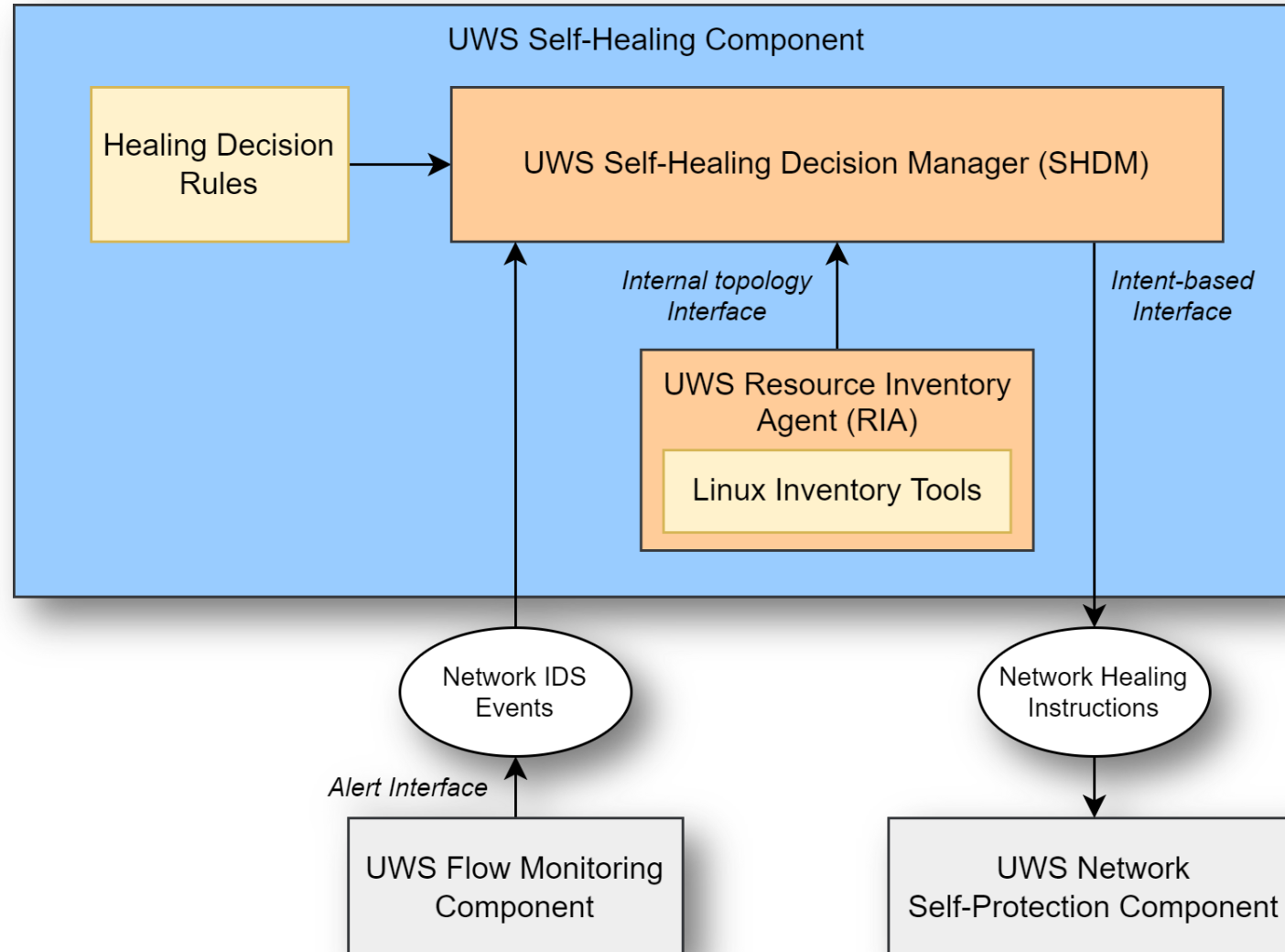
36899 {
36900   "type": "event",
36901   "event": {
36902     "sensor-id": 0,
36903     "event-id": 972,
36904     "event-second": 1667910320,
36905     "event-microsecond": 245835,
36906     "signature-id": 10000002,
36907     "generator-id": 1,
36908     "signature-revision": 0,
36909     "classification-id": 7,
36910     "priority": 2,
36911     "sport-itype": 44043,
36912     "dport-icode": 4789,
36913     "protocol": 17,
36914     "impact-flag": 0,
36915     "impact": 0,
36916     "blocked": 0,
36917     "mpls-label": null,
36918     "vlan-id": null,
36919     "pad2": null,
36920     "source-ip": "10.2.0.2",
36921     "destination-ip": "10.2.0.4"
36922   }
36923 }

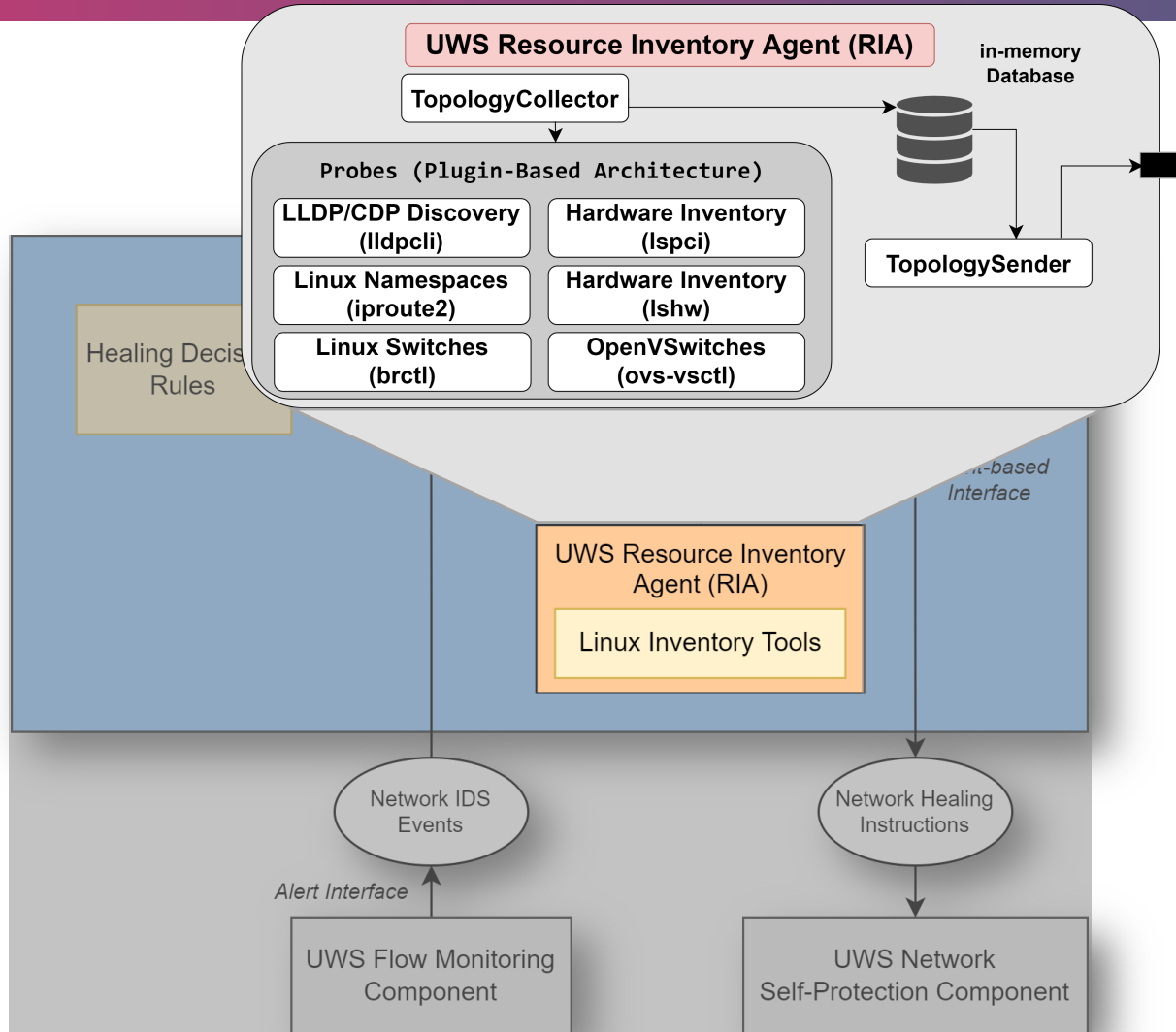
```

Snort IDS Event

No.	Time	Source	Destination	Protocol	Length	Info
289	178.568703	172.12.222.4	172.12.222.254	GTP <UDP>	164	10000 → 80 Len=32
290	178.608138	172.12.222.1	172.12.222.254	GTP <UDP>	164	10000 → 80 Len=32
291	178.608833	172.12.222.2	172.12.222.254	GTP <UDP>	164	10000 → 80 Len=32
292	178.664400	172.12.222.3	172.12.222.254	GTP <UDP>	164	10000 → 80 Len=32
293	178.668786	172.12.222.4	172.12.222.254	GTP <UDP>	164	10000 → 80 Len=32
▶ Frame 292: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0 ▶ Ethernet II, Src: 40:00:00:02:00:01 (40:00:00:02:00:01), Dst: 40:00:00:02:00:02 (40:00:00:02:00:02) ▶ Internet Protocol Version 4, Src: 10.2.0.2, Dst: 10.2.0.4 ▶ User Datagram Protocol, Src Port: 32984, Dst Port: 4789 ▶ Virtual eXtensible Local Area Network ! ▶ Ethernet II, Src: 40:00:00:08:00:03 (40:00:00:08:00:03), Dst: 40:00:00:08:00:09 (40:00:00:08:00:09) ▶ Internet Protocol Version 4, Src: 10.8.0.6, Dst: 10.8.0.12 ? ▶ User Datagram Protocol, Src Port: 2152, Dst Port: 2152 ▶ GPRS Tunneling Protocol ! ▶ Internet Protocol Version 4, Src: 172.12.222.3, Dst: 172.12.222.254 ? ▶ User Datagram Protocol, Src Port: 10000, Dst Port: 80 ▶ Data (32 bytes)						
0000	40 00 00 02 00 02 40 00	00 02 00 01 08 00 45 00	@.....@.E.			
0010	00 96 85 c4 40 00 40 11	a0 89 0a 02 00 02 0a 02	...@.@.			
0020	00 04 80 d8 12 b5 00 82	00 00 08 00 00 00 00 09@.			
0030	60 00 40 00 00 08 00 09	40 00 00 08 00 03 08 00	..@.....@.			
0040	45 00 00 64 8d 3a 40 00	40 11 99 2d 0a 08 00 06	E..d.:@. @.-....			
0050	0a 08 00 0c 08 68 08 68	00 50 bc 42 32 ff 00 40h.h .P.B2..@			
0060	00 00 00 03 00 2d 00 00	45 00 00 3c 2c cf 00 00E.<.,...			
0070	57 11 21 c7 ac 0c de 03	ac 0c de fe 27 10 00 50	W.!.....'..P			
0080	00 28 db 49 50 52 55 45	42 41 00 00 00 00 00 00	.(.IPRUE BA.....			
0090	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00			
00a0	00 00 00 00					

Full PCAP

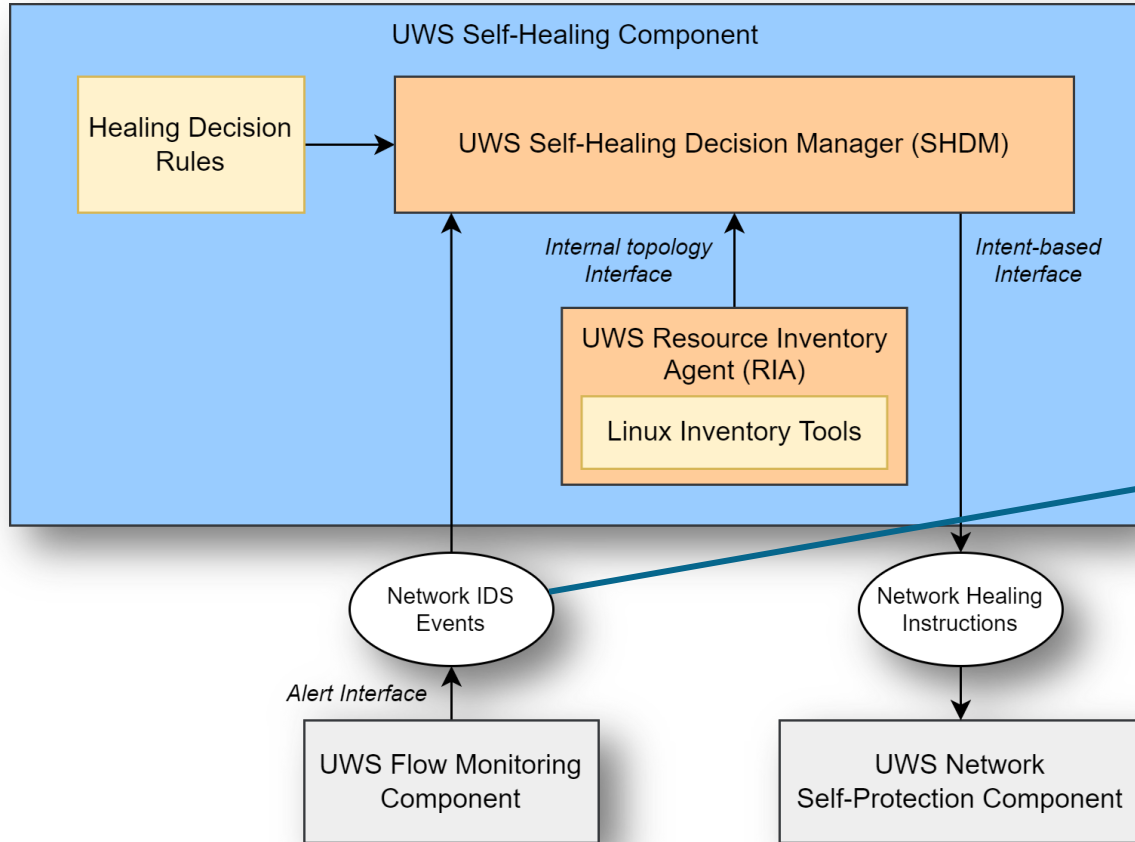




Topology information

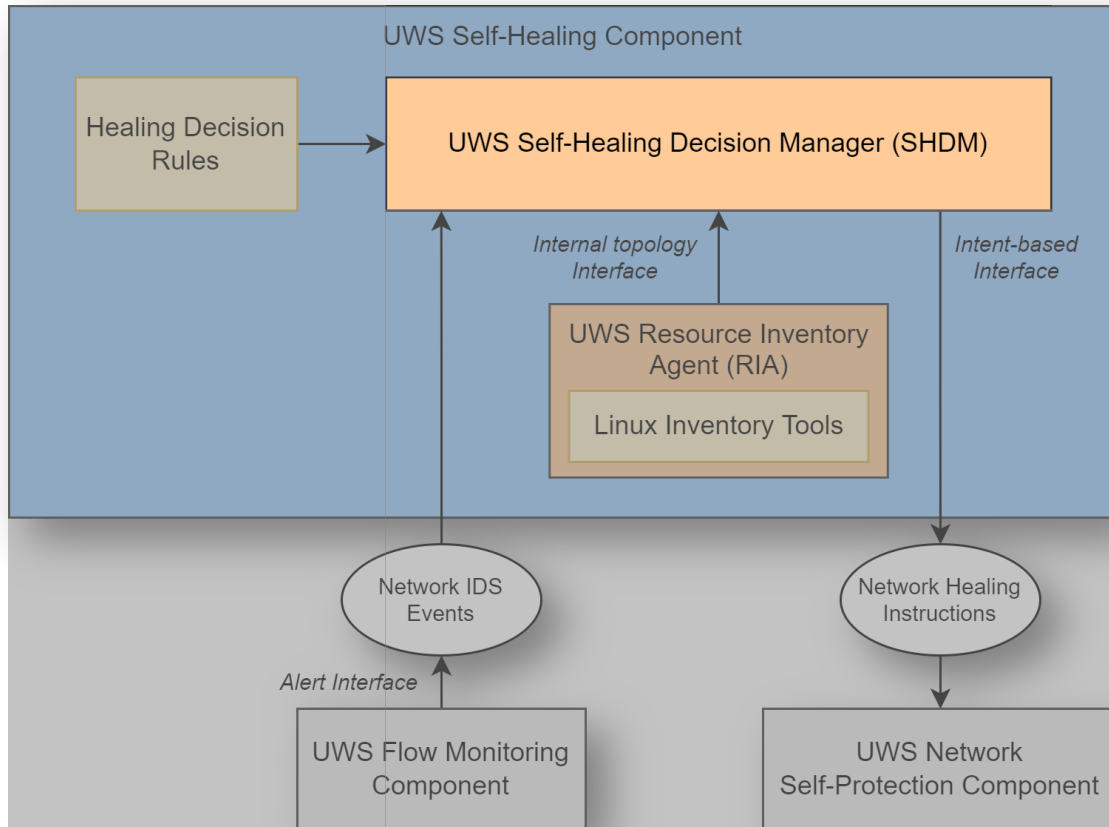
Collected by the UWS Resource Inventory Agent (RIA) with supported technologies:

- **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



```

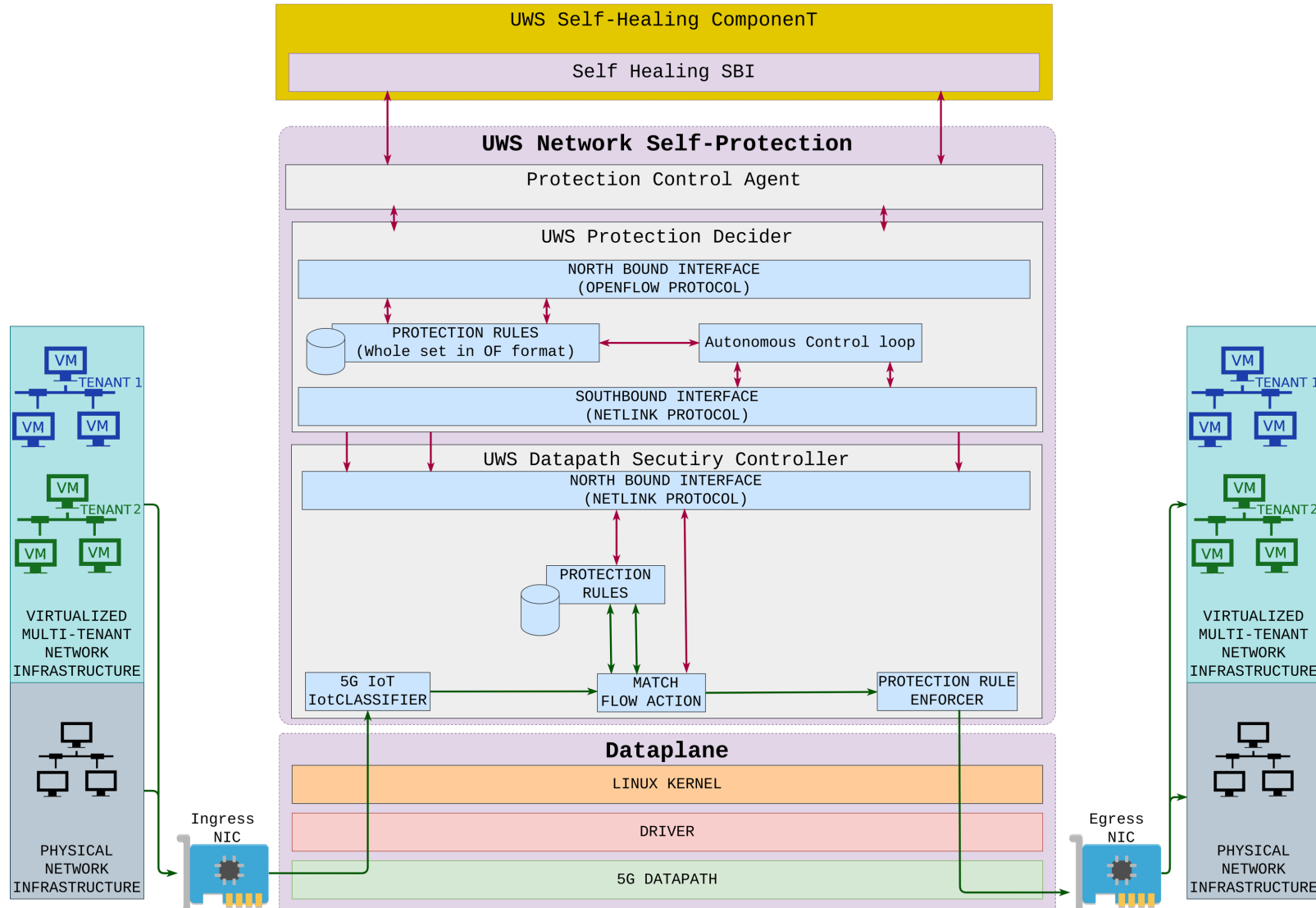
{
  "Resources": {
    "flowResourceId": "D7B61291",
    "parentResourceId": "4A10897A",
    "encapsulationLayer": 2,
    "encapsulationID1": "00002904",
    "encapsulationID2": "00000007",
    "encapsulationType1": "vxlan",
    "encapsulationType2": "gtp",
    "sense": "INGRESS",
    "outMacSrc": "40:00:00:02:00:01",
    "outMacDst": "40:00:00:02:00:05",
    "srcIP": "10101100010100101101111000000111",
    "dstIP": "10101100010100101101111011111110",
    "outSrcIP": "0000101000000010000000000000010",
    "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
  }
}
  
```

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



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

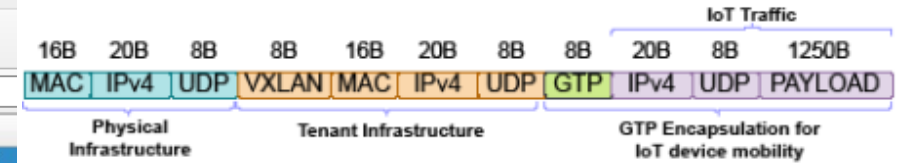
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.10.1	10.10.10.2	GTP <UDP>	216	5500 → 5501 Len=84
2	0.000000	10.10.10.1	10.10.10.2	GTP <UDP>	216	5500 → 5501 Len=84

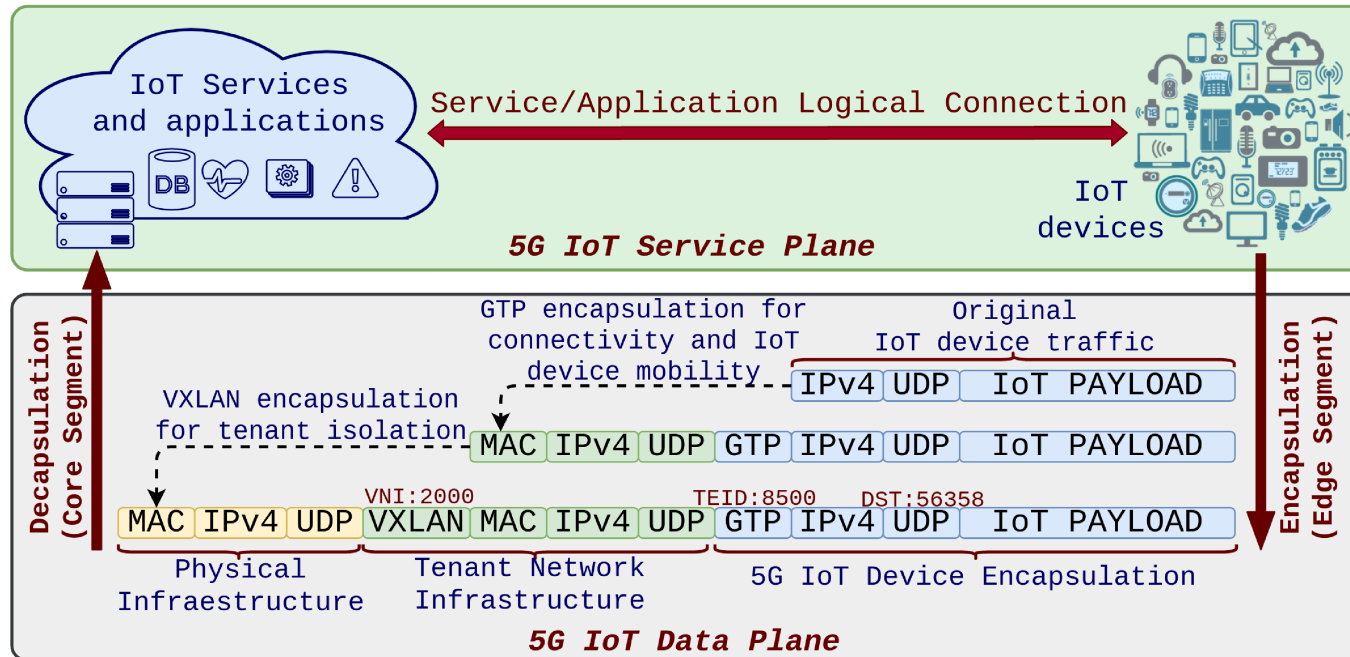
Frame 1: 216 bytes on wire (1728 bits). 216 bytes captured (1728 bits)

- Ethernet II, Src: RealtekU_0e:32:26 (52:54:00:0e:32:26), Dst: RealtekU_0e:32:25 (52:54:00:0e:32:25)
- Internet Protocol Version 4, Src: 192.168.100.120, Dst: 192.168.100.121
- User Datagram Protocol, Src Port: 5000, Dst Port: 4789
- Virtual eXtensible Local Area Network
 - Flags: 0x0800, VXLAN Network ID (VNI)
 - Group Policy ID: 0
 - VXLAN Network Identifier (VNI): 1000
 - Reserved: 0
 - Ethernet II, Src: Xerox_02:02:02 (00:00:02:02:02:02), Dst: Xerox_01:01:01 (00:00:01:01:01:01)
 - Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.2
 - User Datagram Protocol, Src Port: 2152, Dst Port: 2152
 - GPRS Tunneling Protocol
 - Flags: 0x32
 - Message Type: T-PDU (0xff)
 - Length: 116
 - TEID: 0x000003e8 (1000)
 - Sequence number: 0x0000 (0)
 - Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.2
 - User Datagram Protocol, Src Port: 5500, Dst Port: 5501
 - Data (84 bytes)
 - Data: 00000001000102030405060708090a0b0c0d0e0f00010203...
 - [Length: 84]

0000 52 54 00 0e 32 25 52 54 00 0e 32 26 08 00 45 00 RT..2%RT..2&..E.
 0010 00 ca 00 00 40 00 40 11 ef e0 c0 a8 64 78 c0 a8@..dx..

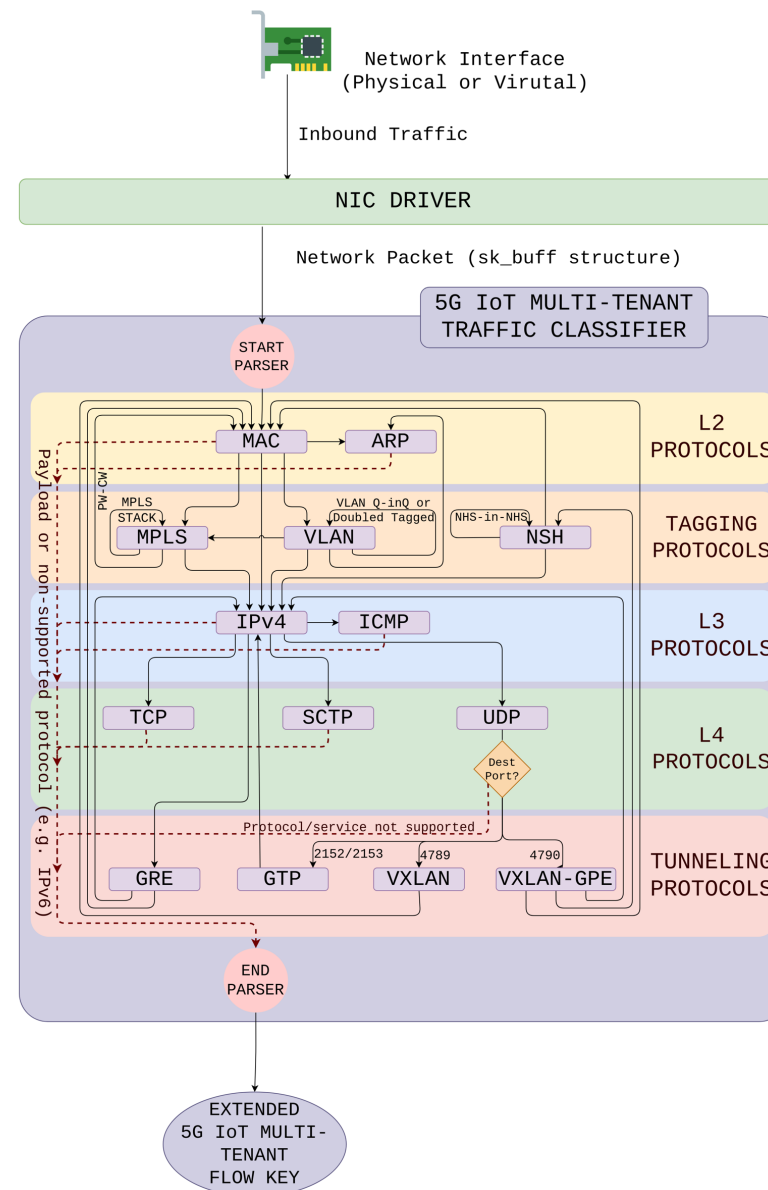


- Infrastructure traffic
- Tenant traffic (VXLAN for tenant isolation)
- IoT device traffic (VXLAN+GTP headers for user identification and isolation)



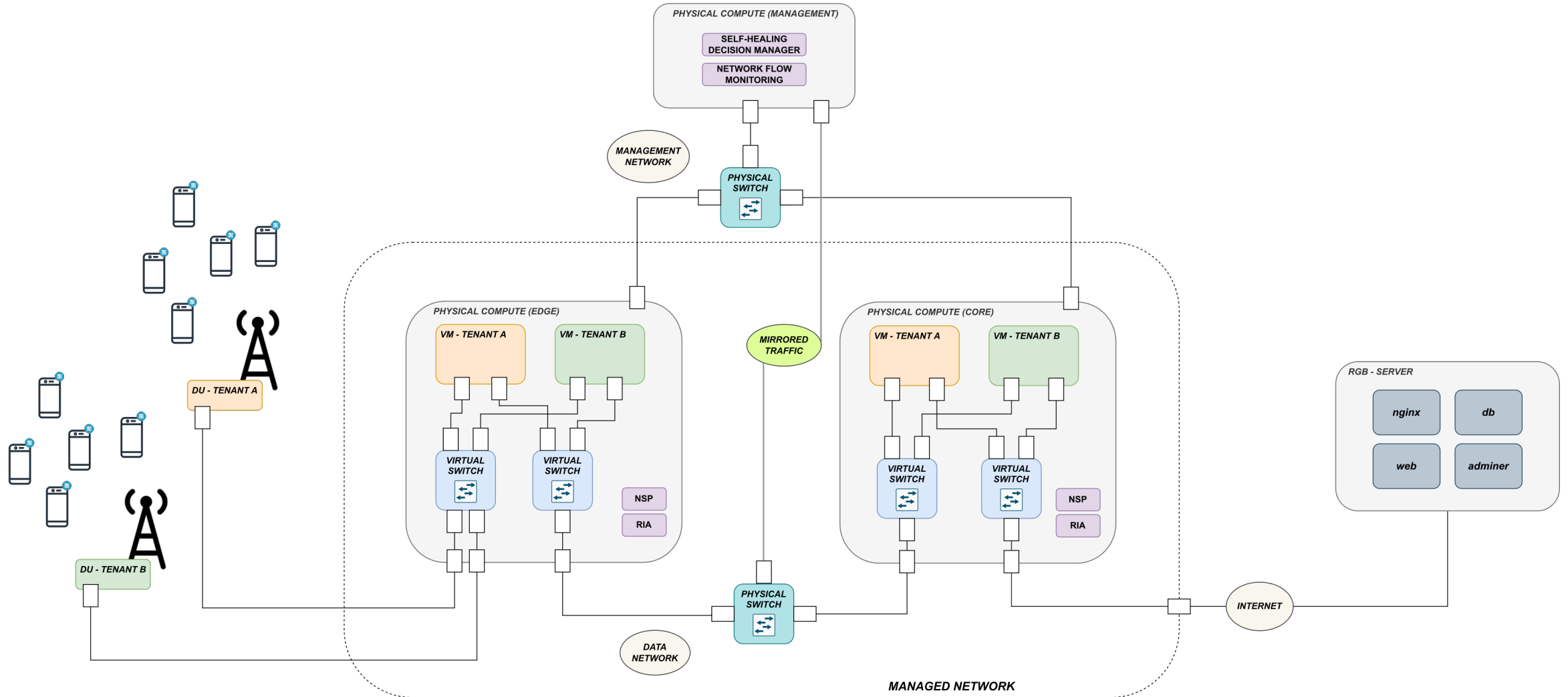
The same original IoT packet transmitted by an IoT device or sensor can have different packet structure with different encapsulation and tunnelling headers depending on the network segment.

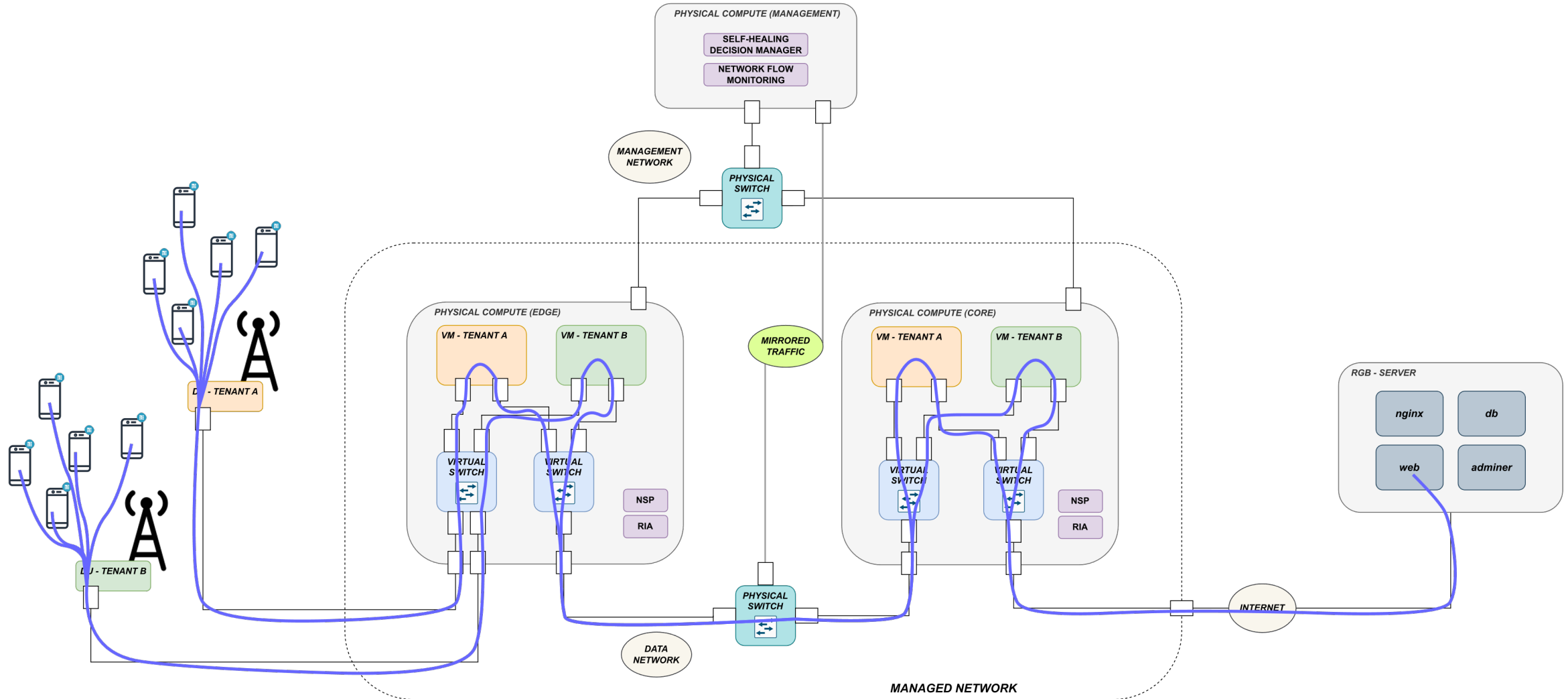
- Classifier with re-entrance between headers to allow a deep packet inspection for traffic with several levels of encapsulations.
- Support for GTP protocol.
- Support for tunnelling and encapsulation protocols used in overlay networks such as GRE, VXLAN, VXLAN-GTE or VLAN.
- The outcome is an extended *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.

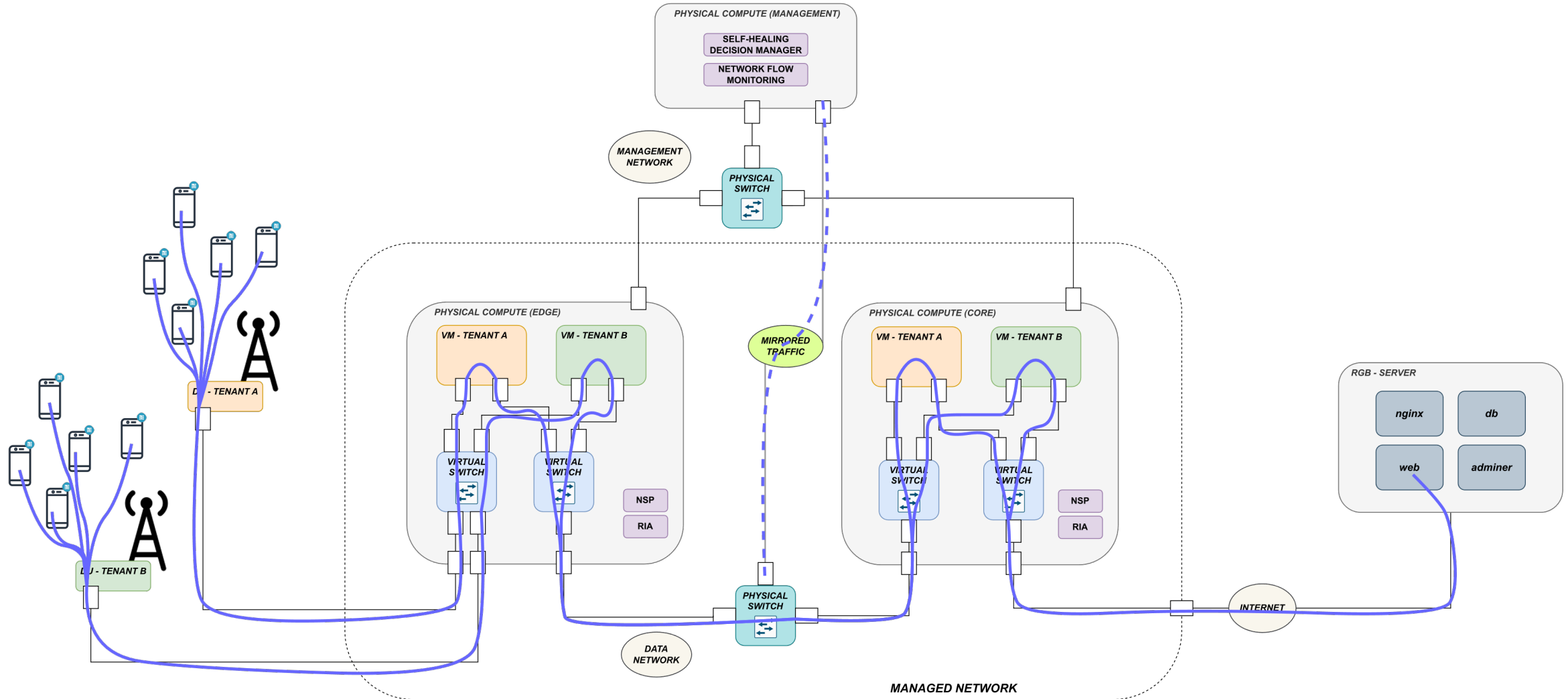


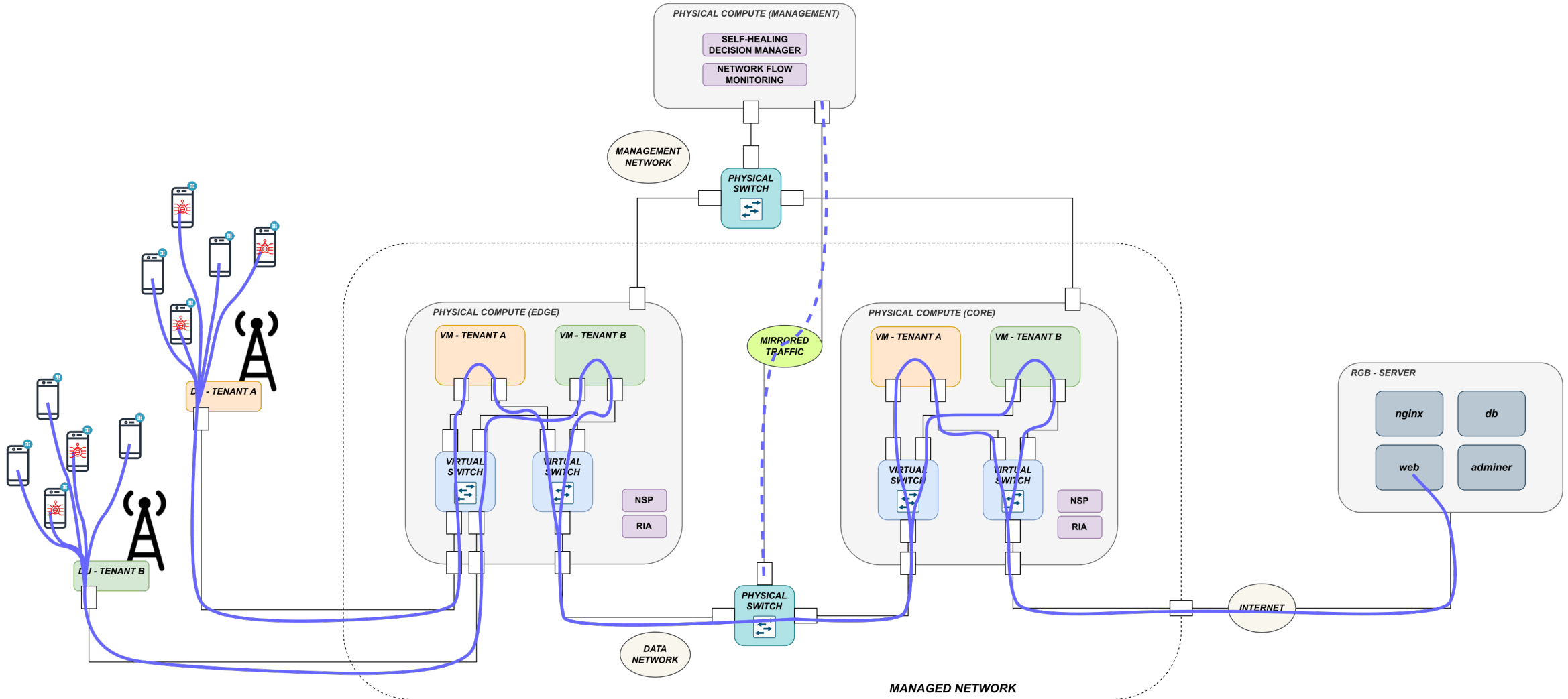


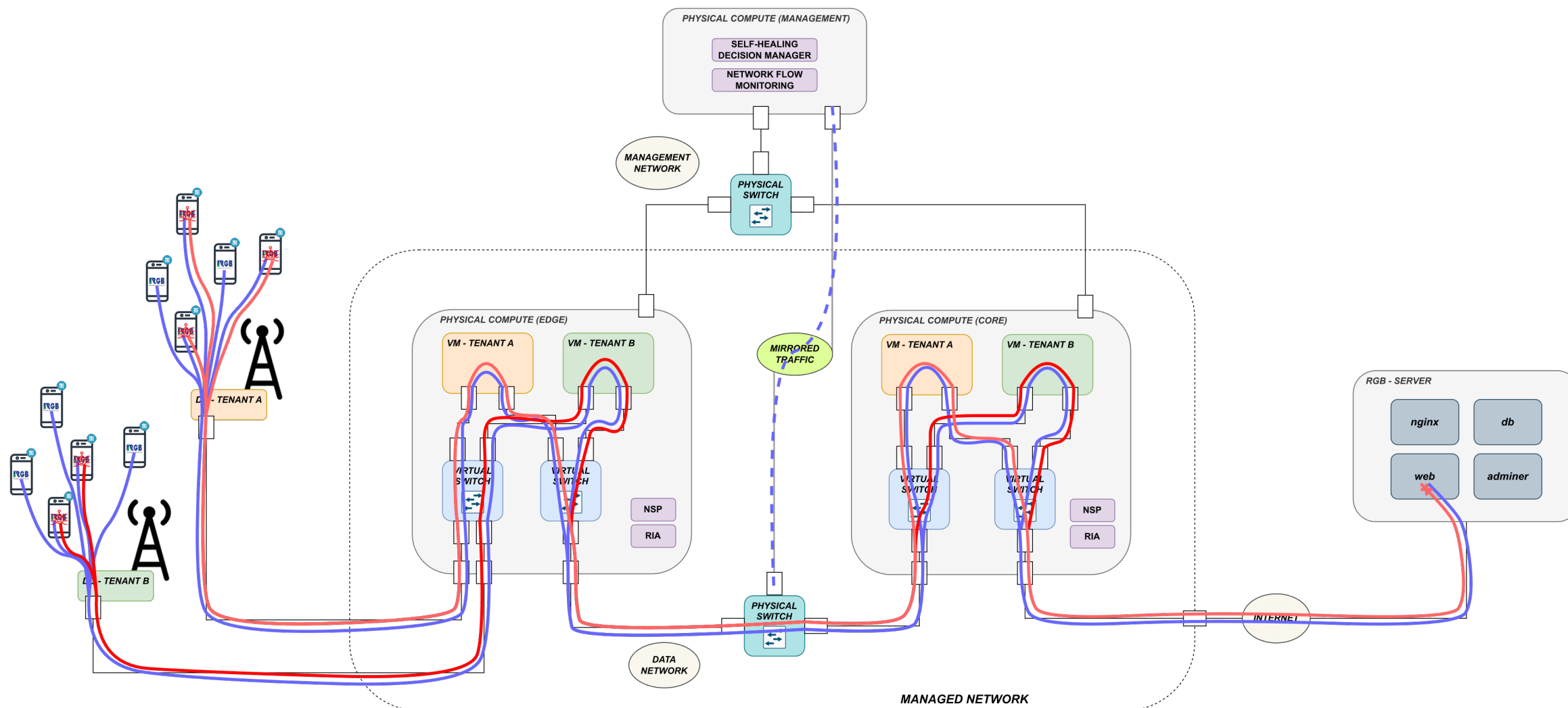
4. THREAT DETECTION, PLANNING AND MITIGATION

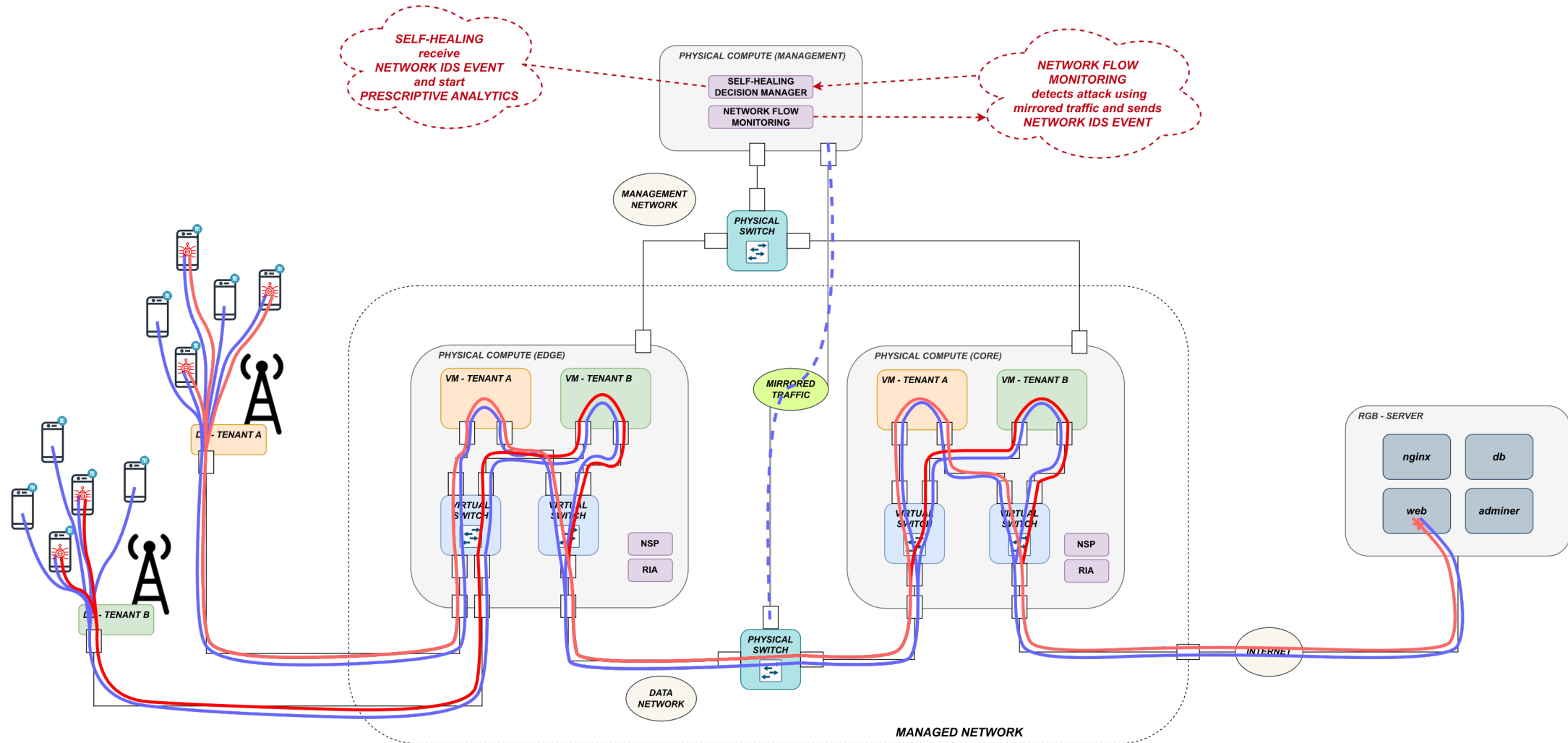


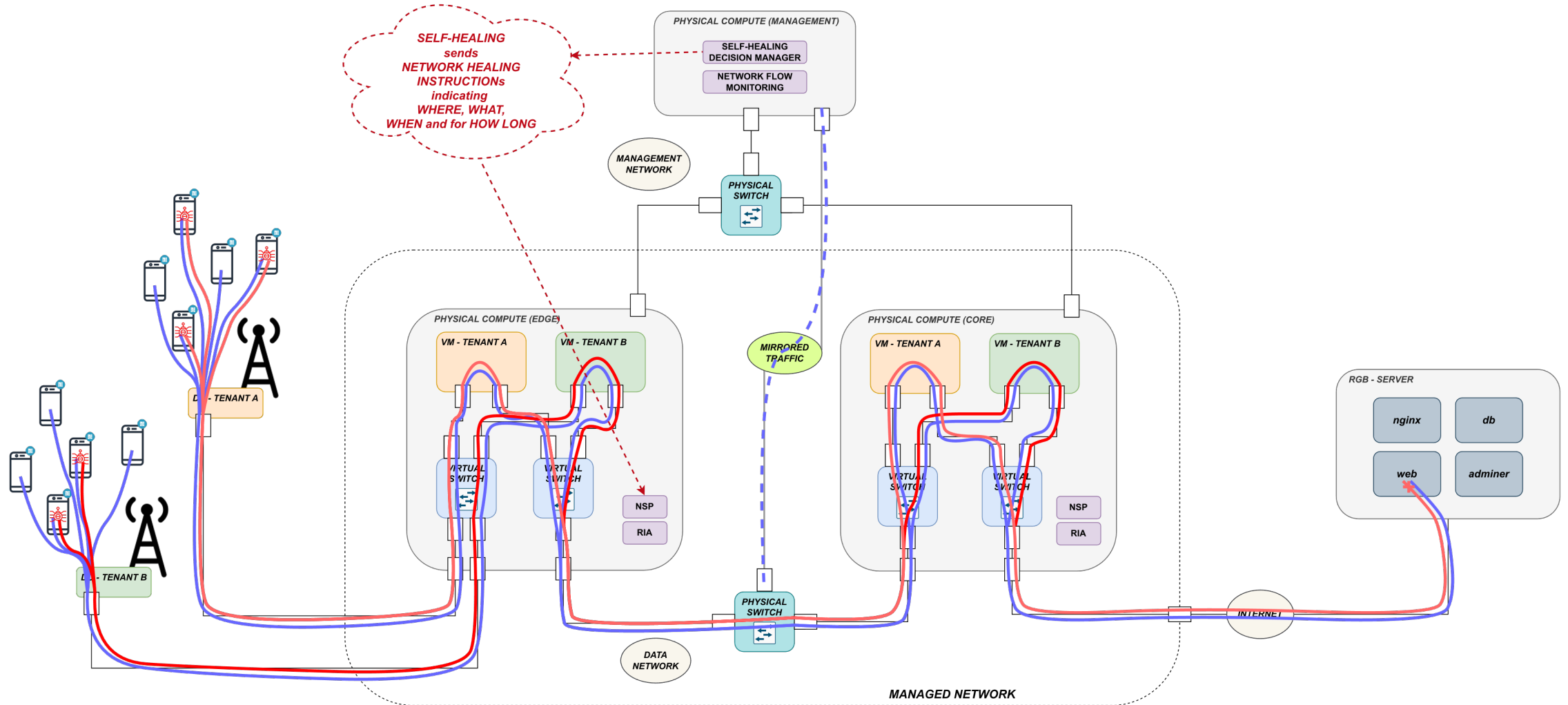


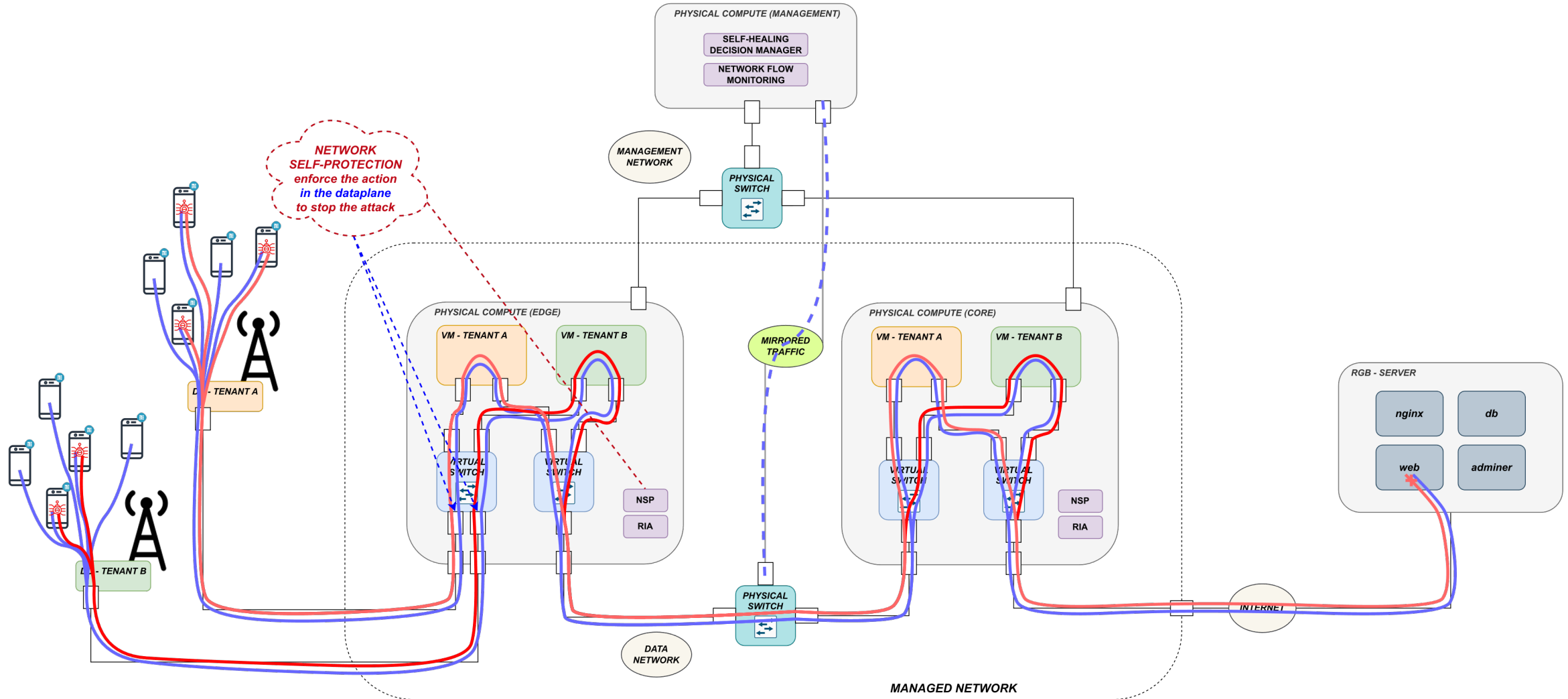


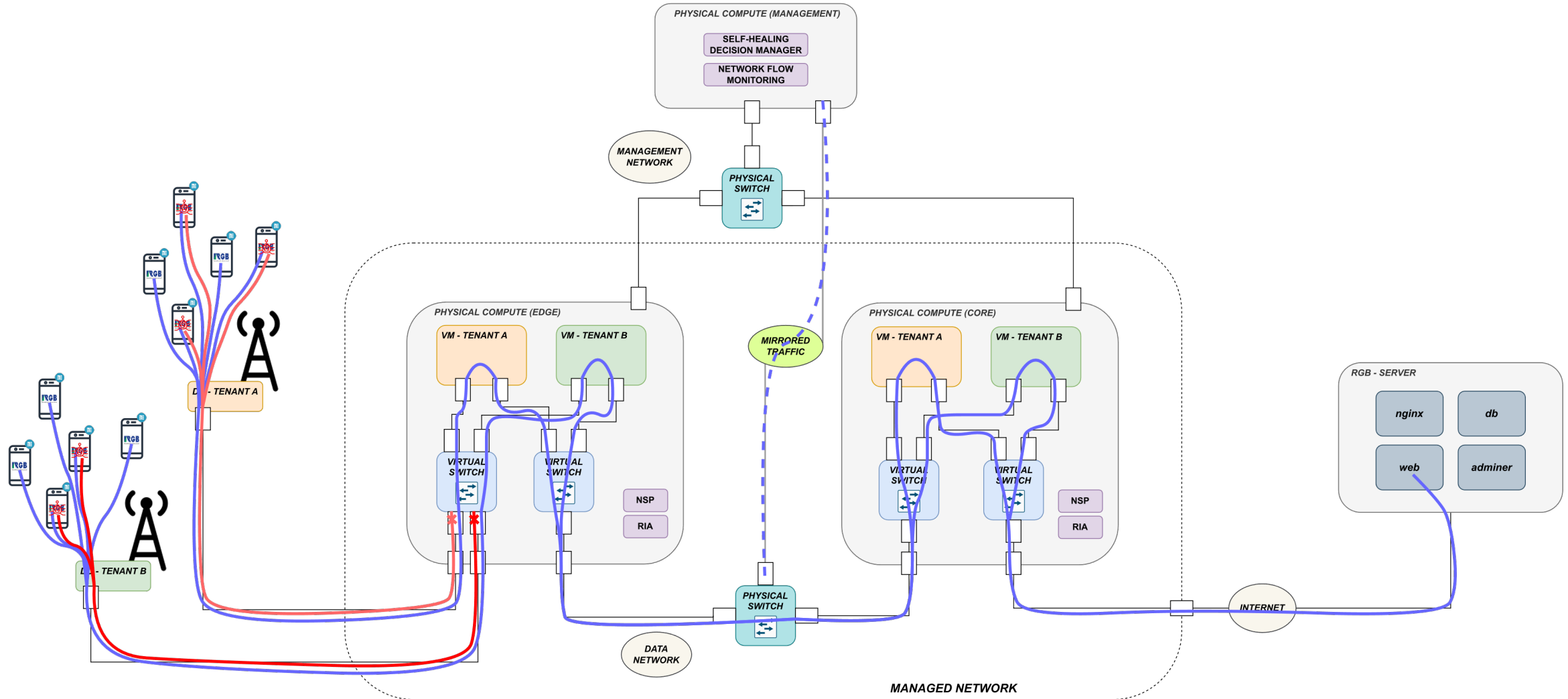












The background is a vertical gradient from pink on the left to blue on the right. Three decorative elements are present: a light pink circle with a line extending upwards from the top edge, a light blue circle with a line extending upwards from the top edge, and a light purple circle with a line extending downwards from the bottom edge.

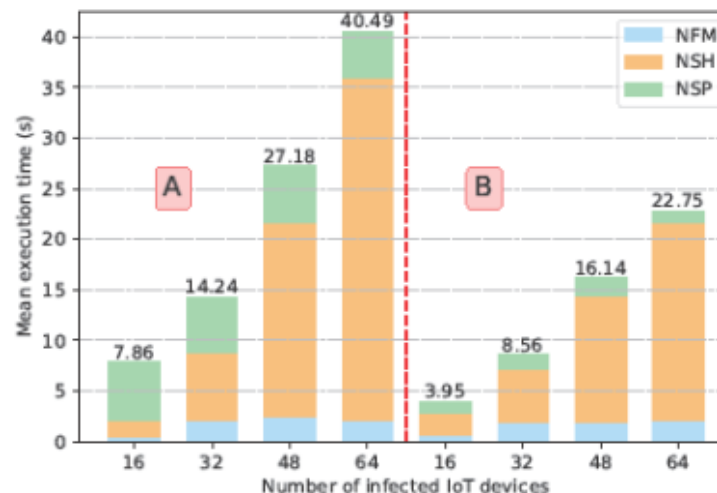
5. DEMO

The background is a vertical gradient from magenta on the left to blue on the right. Three decorative elements are present: a light pink circle with a vertical line extending upwards from its top, located in the upper left; a light blue circle with a vertical line extending upwards from its top, located in the upper right; and a light purple circle with a vertical line extending downwards from its bottom, located in the lower center.

6. 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 (VISPs) 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 Tunneling 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-



ARCADIAN-IoT

THANK YOU FOR YOUR ATTENTION



arcadian-iot.eu



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



