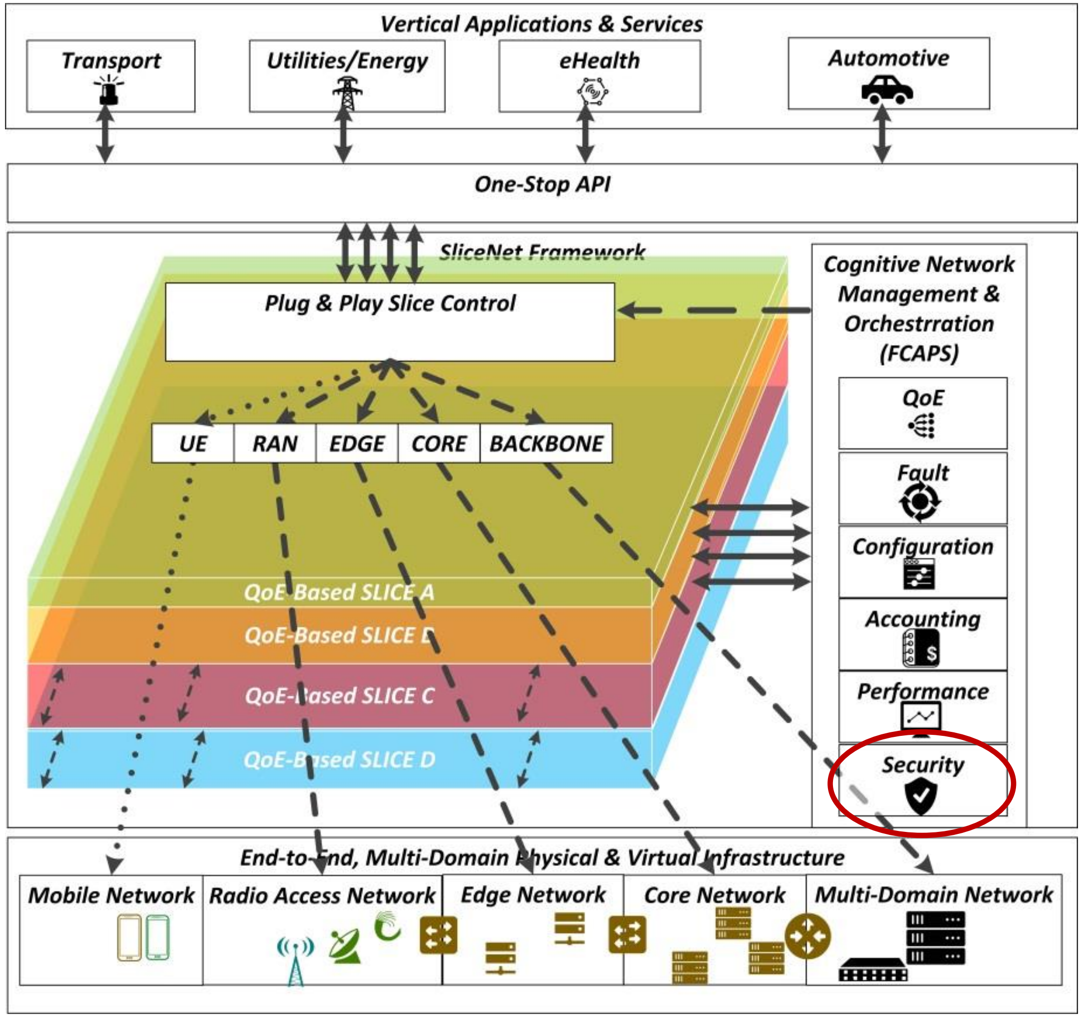
Security Considerations in 5G Network Slicing

Thuy Truong, Zdravko Bozakov, DellEMC

Qi Wang (Presenter), Jose Alcaraz Calero, UWS

SliceNet Overview

1. Achieve an innovative, cognitive, integrated 'one-stop shop' 5G slice management framework for vertical businesses and co-designed by vertical sectors
2. Enable extensible, **end-to-end slice FCAPS management** across multiple planes and operator domains
3. Establish cognitive, agile QoE management of slices for service assurance of vertical businesses
4. Empower orchestration for cross-plane coordination of management, control, service and data planes to achieve system-level slicing control and slice operation



Some Key Security Management Issues in 5G Network Slice

- ❑ End-to-end protection with multi-domain security concerns
- ❑ Inter-slice isolation over a shared physical infrastructure
- ❑ Different security protocols or policies in different slices (differentiated security capabilities for various use cases)
- ❑ Various attacks against Network Slice Manager, Network Slice instance, Host (physical) platforms etc.

- ❑ References
  - ❑ 5G PPP Security WG, 5G PPP Phase1 Security Landscape, Jun 2017
  - ❑ NGMN, 5G Security Recommendations Package #2: Network Slicing, Apr 2016
  - ❑ Huawei, 5G Security: Forward Thinking, 2015

Design and Run-Time Security Considerations in SliceNet

In network slicing, 5G Security can be addressed with two different phases: at the design (static) phase and at the operation (runtime) phase:

- In the design phase for a new slice, primarily composed of Virtual and/or Physical Network Functions (VNFs and PNFs), associated resources and RAN settings, one can add into the slice specific virtualised Security Network Functions (vSNFs) such as vFirewall, vDPI, vIDS, etc. in different locations to have a certain level of security in the slice, depending on the characteristics of the designed slice.
- When this slice is on boarded and instantiated, which will go to the operation/runtime phase where a cognitive mechanism (autonomic security management) could be used for run-time analytics on the chained PNFs/VNFs and associated resources to detect possible threats and prevent or minimize the impact of those detected threats on the system.

SliceNet Slice Security Manager

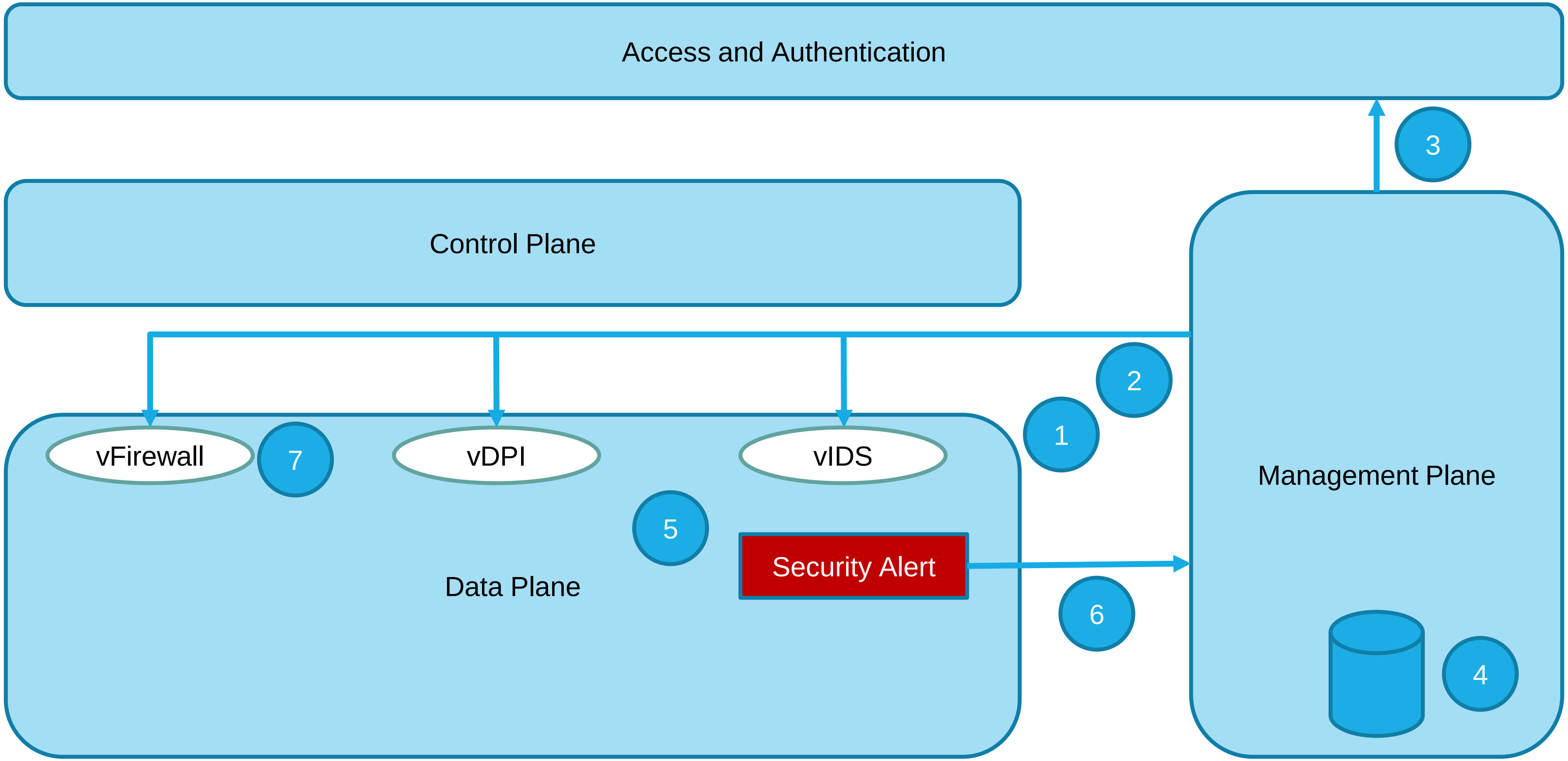
SliceNet proposes a Slice Security Manager component for the following:

- ❑ The Slice Security Manager provides functionality required to secure individual slice instances from each other. Depending on the SLAs, a slice may require end-to-end encryption. To this end, the Slice Security manager will trigger the deployment of predefined de/encryption functions in proximity to, or within the customer's NFVs. The component will interact with other architecture components to distribute required keys.
- ❑ The Slice Security Manager will support the management of security-related network functions (e.g., vFirewall, vDPI, vIDS) utilised by the control loop enforcing policies for detecting and/or mitigating security issues that may degrade or disrupt the slice operation.
- ❑ The Slice Security Manager will coordinate with the Cognition components for run-time analytics on the chained PNFs/VNFs and/or the associated resources to enable proactive detection and/or mitigation. Further analysis (offline) could be conducted for deep analytics.

SliceNet Network Slice Instance Security Management Workflow: An Example

Step	Impacted Architecture Plane	Description
1	Data Plane	Security Network Functions, e.g. DDoS attack detection vDPI, vIDS, vFirewall, etc. are deployed and configured
2	Management Plane	NFs management and/or Infrastructure management (VNFM, EMS, VIM, …) configures access and management rights to deploy infrastructure elements and NFs
3	Management Plane	Access and authentication credentials are exposed to upper layers per NSI/NSSI
4	Management Plane	Access and authentication credentials are stored for further configuration possibilities in security management layer at NSI level.
5	Data Plane	A security threat is detected by relevant NFs. Threat may be resolved at the DP
6	Management Plane	NFs and/or/ Infrastructure management is notified of security threat.
7	Management Plane	Upper layers are notified to determine affected NSIs/NSSIs, and further necessary mitigation actions to be enforced, e.g., replace the affected VNFs, etc.

SliceNet Network Slice Instance Security Management Workflow: An Example



Concluding Remarks

- Network slicing introduces new security concerns that need to be addressed, whilst offering considerable benefits for 5G
- SliceNet considers security issues at both design and run-time phases
- SliceNet, esp. via a Slice Security Manager, enables the coordination of security mechanisms related to the provisioning and operation of secure network slices, considering end-to-end encryption, management of virtual security network functions, cognitive analytics etc.