The Need for Zero Trust in 5G

NSA Center for Cybersecurity Collaboration

28 August 2023

5G FOCUS

- 5G Core
  - Service Based Architecture (SBA)
  - Virtual Machines / Containers
  - Software Defined Networking (SDN)
- 5G Radio Access Network (RAN)
  - Self-Organizing Networks (SON)
  - Heterogeneous Radio Access Technologies
- Resulting in highly configurable 5G Core and RAN
- Eventually manual configuration will give way to AI/ML determined dynamic configuration

NEED FOR VERIFIABLE TRUST

- Analytics need accurate data points for both Quality of Service (QoS) and Security
  - Data poisoning
- Ensure analytics have not been altered and the analytic engine is in a secure state
- Analytic output is appropriately acted upon

NIST SPECIAL PUBLICATION ON ZERO TRUST

CYBERSECURITY

- U. S. National Institute of Standards and Technology (NIST)
- Source: “NIST SP 800-207 Zero Trust Architecture”
- Focused on the enterprise use case
  - User/client-to-server interactions
- 5G System (consisting of a 5G Core and RAN) use case differs from the enterprise
  - Machine-to-machine interactions
- The guidance in SP 800-207 needs to be adjusted for the 5G System

NIST 7 TENETS OF ZERO TRUST

CYBERSECURITY

1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location
3. Access to individual enterprise resources is granted on a per-session basis
4. Access to resources is determined by dynamic policy
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

PEP AND PDP UTILIZING SECURITY CONTROLS

- Policy Enforcement Point/Policy Decision Point (PEP/PDP)

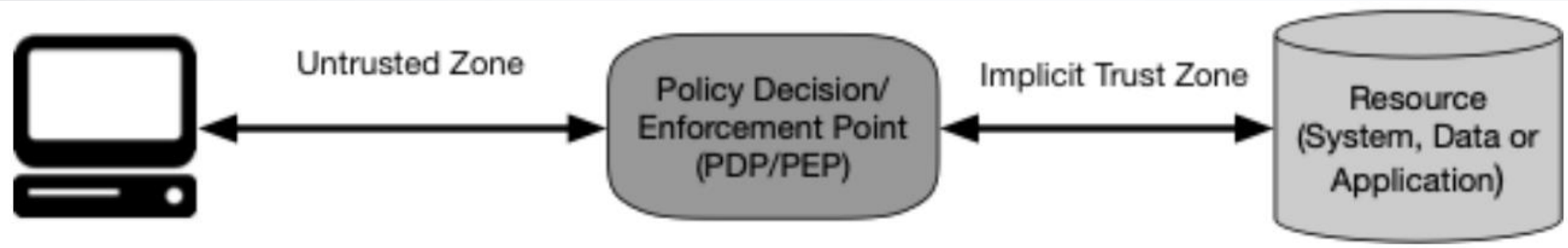

Diagram Source: NIST SP 800-207 Zero Trust Architecture

LAYERS OF ZERO TRUST

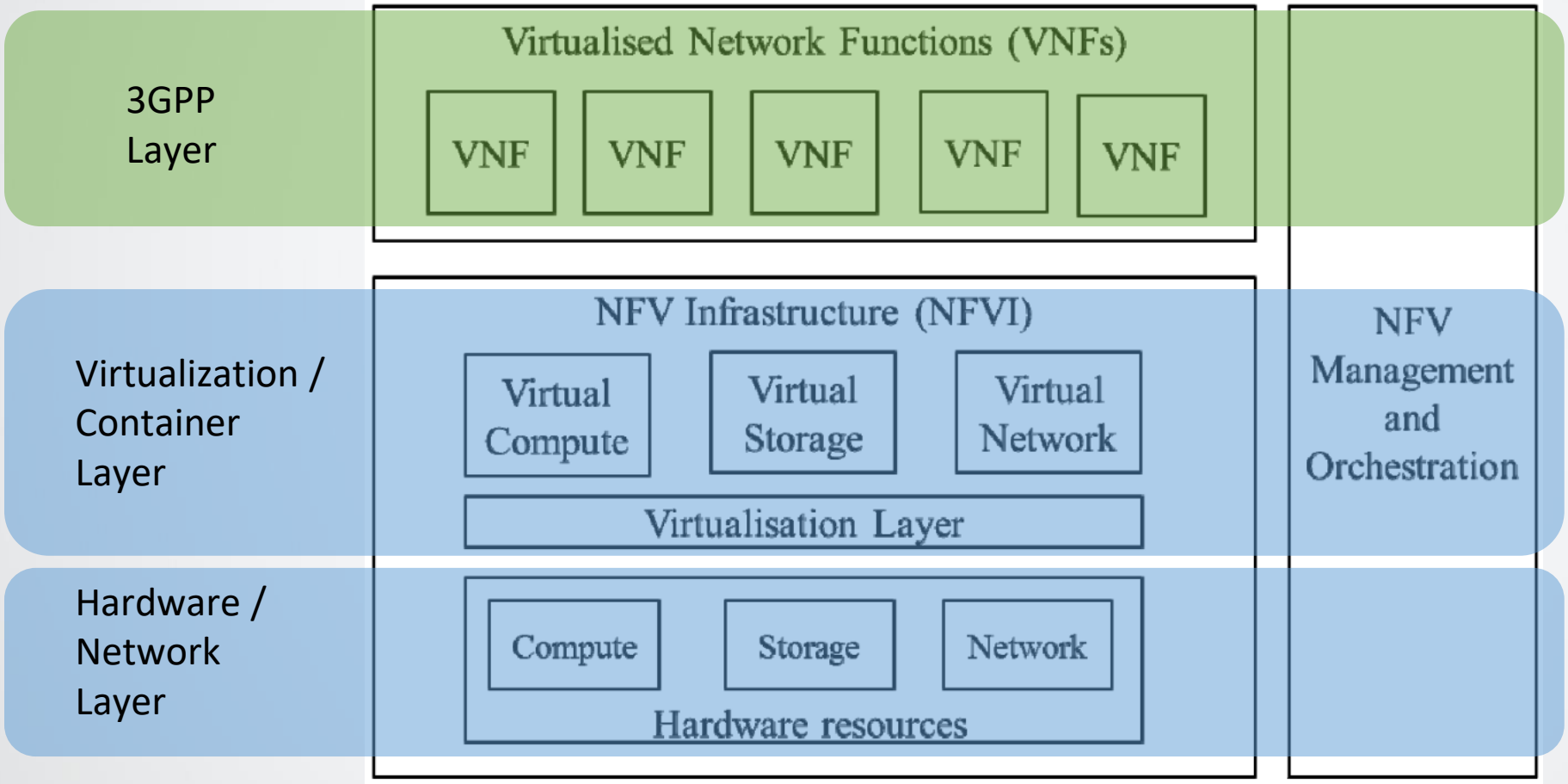

Diagram Source: ETSI GS Network Function Virtualisation (NFV); Architectural Framework

THANK YOU

CYBERSECURITY

https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/