5G - An Opportunity to Get Security Right

Max Iftikhar

Account Director, Service Providers – ANZ

Shain Singh

Cloud/5G Security Architect - APCJ

Our Speakers

Shain Singh

F5

Cloud/5G Security Architect

@shainsingh

Max Iftikhar

F5

Account Director

5G

DELIVERING:

- INFINITE CONNECTIVITY
- HIGH BANDWIDTH
- LOW LATENCY
- ULTRA RELIABILITY
- FAST MOBILITY

Technology Evolution

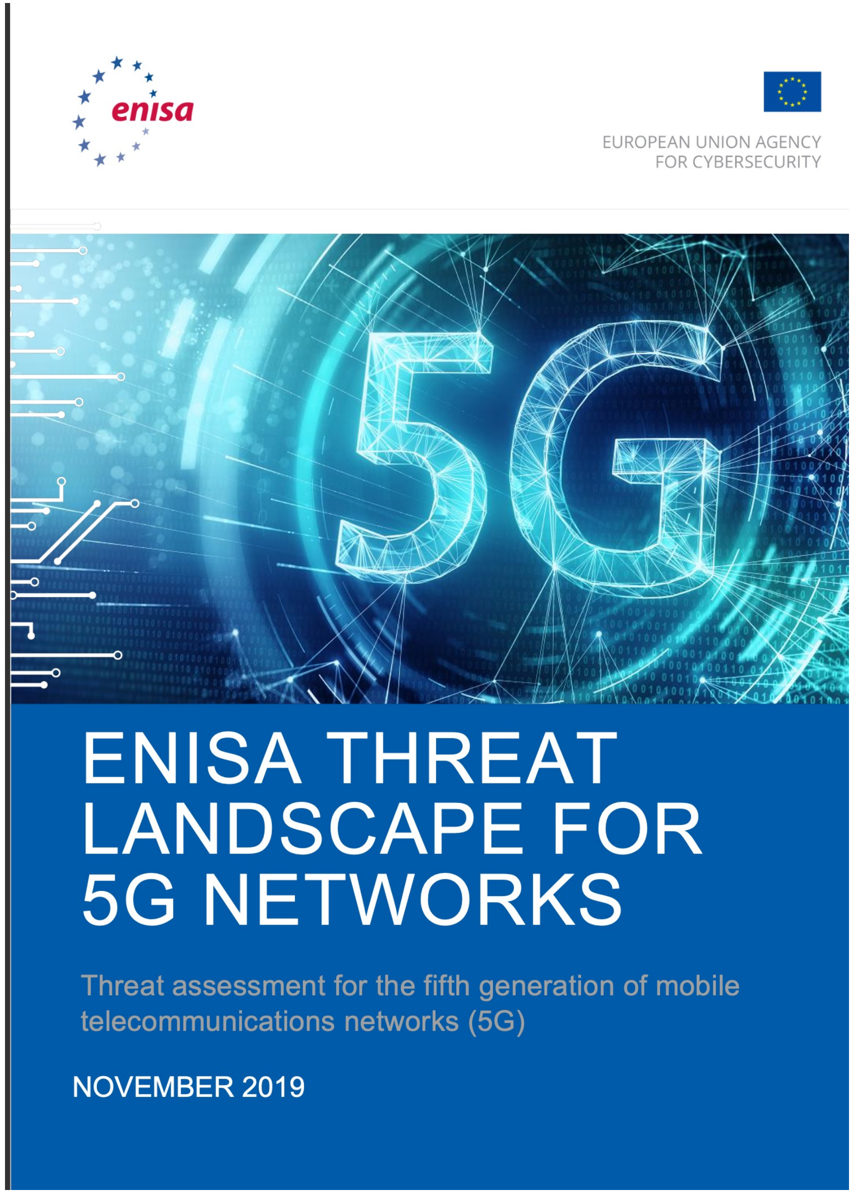
Distributed Data Centers (MEC)

Network Slicing

NFV & SDN

CUPS

Service Based Architecture



enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Threat assessment for the fifth generation of mobile telecommunications networks (5G)

NOVEMBER 2019

Independent market research and
competitive analysis of next-generation
business and technology solutions for
service providers and vendors

HEAVY READING
CUSTOM REPORTS

Heavy Reading's 2019 5G Security Survey

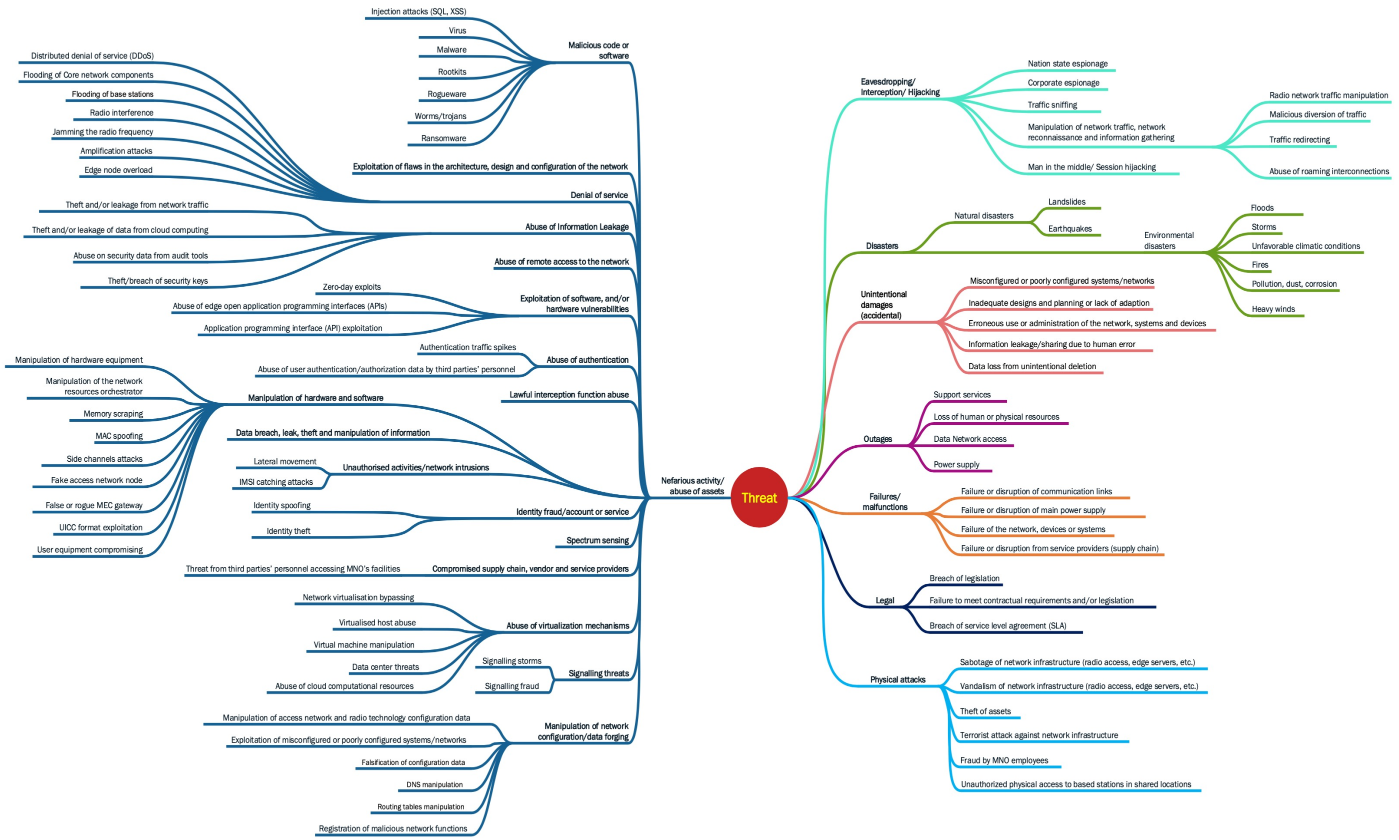
A Custom Research Report Produced for F5 Networks, Fortinet, NetNumber, and Palo Alto Networks

f5
FURTINET
NetNumber
paloalto

AUTHOR: JIM HODGES, PRINCIPAL ANALYST, HEAVY READING

Taxonomy of Threats

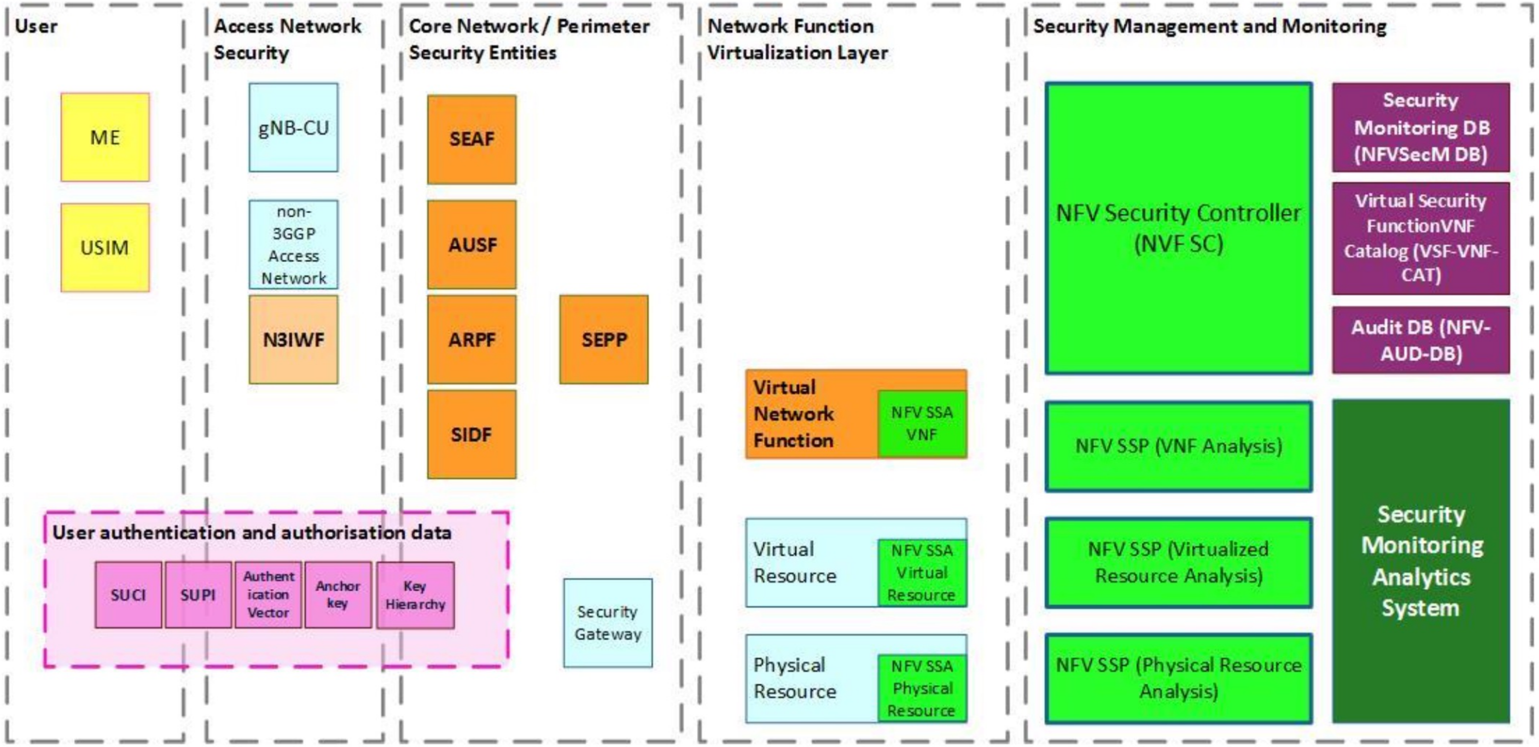
- MULTIPLE THREAT AGENTS
- ATTACK VECTORS ACROSS ACCESS, NETWORK, PHYSICAL COMPONENTS



- Threat
  - Nefarious activity/ abuse of assets
    - Malicious code or software
      - Injection attacks (SQL, XSS)
      - Virus
      - Malware
      - Rootkits
      - Rogueware
      - Worms/trojans
      - Ransomware
    - Exploitation of flaws in the architecture, design and configuration of the network
    - Denial of service
      - Distributed denial of service (DDoS)
      - Flooding of Core network components
      - Flooding of base stations
      - Radio interference
      - Jamming the radio frequency
      - Amplification attacks
      - Edge node overload
    - Abuse of Information Leakage
      - Theft and/or leakage from network traffic
      - Theft and/or leakage of data from cloud computing
      - Abuse on security data from audit tools
      - Theft/breach of security keys
    - Abuse of remote access to the network
    - Exploitation of software, and/or hardware vulnerabilities
      - Zero-day exploits
      - Abuse of edge open application programming interfaces (APIs)
      - Application programming interface (API) exploitation
    - Abuse of authentication
      - Authentication traffic spikes
      - Abuse of user authentication/authorization data by third parties' personnel
    - Lawful interception function abuse
    - Manipulation of hardware and software
      - Manipulation of hardware equipment
      - Manipulation of the network resources orchestrator
      - Memory scraping
      - MAC spoofing
      - Side channels attacks
      - Fake access network node
      - False or rogue MEC gateway
      - UICC format exploitation
      - User equipment compromising
    - Data breach, leak, theft and manipulation of information
    - Unauthorised activities/network intrusions
      - Lateral movement
      - IMSI catching attacks
    - Identity fraud/account or service
      - Identity spoofing
      - Identity theft
    - Spectrum sensing
    - Compromised supply chain, vendor and service providers
      - Threat from third parties' personnel accessing MNO's facilities
    - Abuse of virtualization mechanisms
      - Network virtualisation bypassing
      - Virtualised host abuse
      - Virtual machine manipulation
      - Data center threats
      - Abuse of cloud computational resources
    - Signalling threats
      - Signalling storms
      - Signalling fraud
    - Manipulation of network configuration/data forging
      - Manipulation of access network and radio technology configuration data
      - Exploitation of misconfigured or poorly configured systems/networks
      - Falsification of configuration data
      - DNS manipulation
      - Routing tables manipulation
      - Registration of malicious network functions
  - Eavesdropping/ Interception/ Hijacking
    - Nation state espionage
    - Corporate espionage
    - Traffic sniffing
    - Manipulation of network traffic, network reconnaissance and information gathering
      - Radio network traffic manipulation
      - Malicious diversion of traffic
      - Traffic redirecting
      - Abuse of roaming interconnections
    - Man in the middle/ Session hijacking
  - Disasters
    - Natural disasters
      - Landslides
      - Earthquakes
    - Environmental disasters
      - Floods
      - Storms
      - Unfavorable climatic conditions
      - Fires
      - Pollution, dust, corrosion
      - Heavy winds
  - Unintentional damages (accidental)
    - Misconfigured or poorly configured systems/networks
    - Inadequate designs and planning or lack of adaption
    - Erroneous use or administration of the network, systems and devices
    - Information leakage/sharing due to human error
    - Data loss from unintentional deletion
  - Outages
    - Support services
    - Loss of human or physical resources
    - Data Network access
    - Power supply
  - Failures/ malfunctions
    - Failure or disruption of communication links
    - Failure or disruption of main power supply
    - Failure of the network, devices or systems
    - Failure or disruption from service providers (supply chain)
  - Legal
    - Breach of legislation
    - Failure to meet contractual requirements and/or legislation
    - Breach of service level agreement (SLA)
  - Physical attacks
    - Sabotage of network infrastructure (radio access, edge servers, etc.)
    - Vandalism of network infrastructure (radio access, edge servers, etc.)
    - Theft of assets
    - Terrorist attack against network infrastructure
    - Fraud by MNO employees
    - Unauthorized physical access to based stations in shared locations

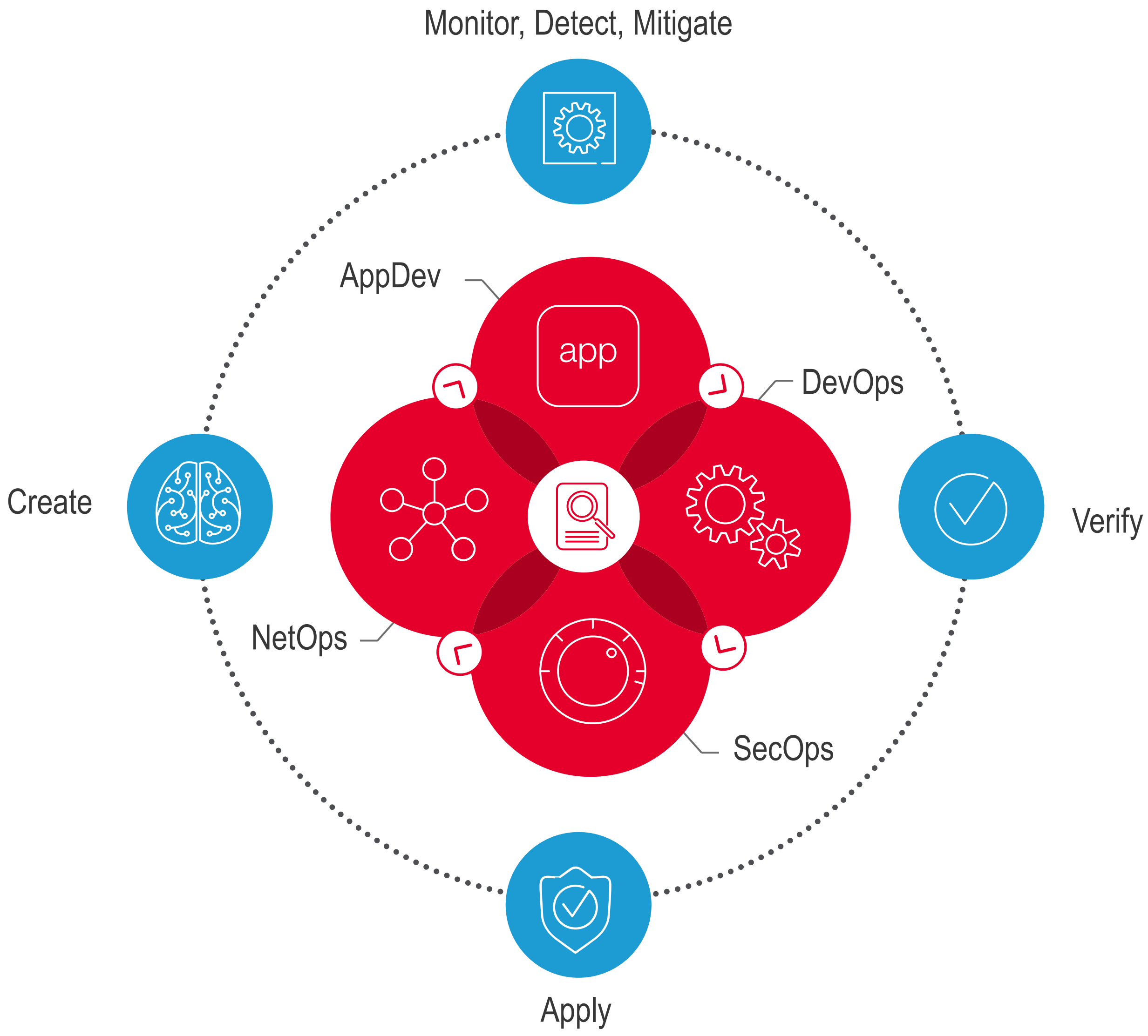
5G Security Architecture

- COVERS ACCESS (RAN), CORE NETWORK AND PERIMETER (EDGE COMPUTING)


User
ME
USIM
Access Network Security
gNB-CU
non-3GGP Access Network
N3IWF
Core Network / Perimeter Security Entities
SEAF
AUSF
ARPF
SEPP
SIDF
Security Gateway
User authentication and authorisation data
SUCI
SUPI
Authentication Vector
Anchor key
Key Hierarchy
Network Function Virtualization Layer
Virtual Network Function
NFV SSA VNF
Virtual Resource
NFV SSA Virtual Resource
Physical Resource
NFV SSA Physical Resource
Security Management and Monitoring
NFV Security Controller (NVF SC)
Security Monitoring DB (NFVSecM DB)
Virtual Security FunctionVNF Catalog (VSF-VNF-CAT)
Audit DB (NFV-AUD-DB)
NFV SSP (VNF Analysis)
NFV SSP (Virtualized Resource Analysis)
NFV SSP (Physical Resource Analysis)
Security Monitoring Analytics System

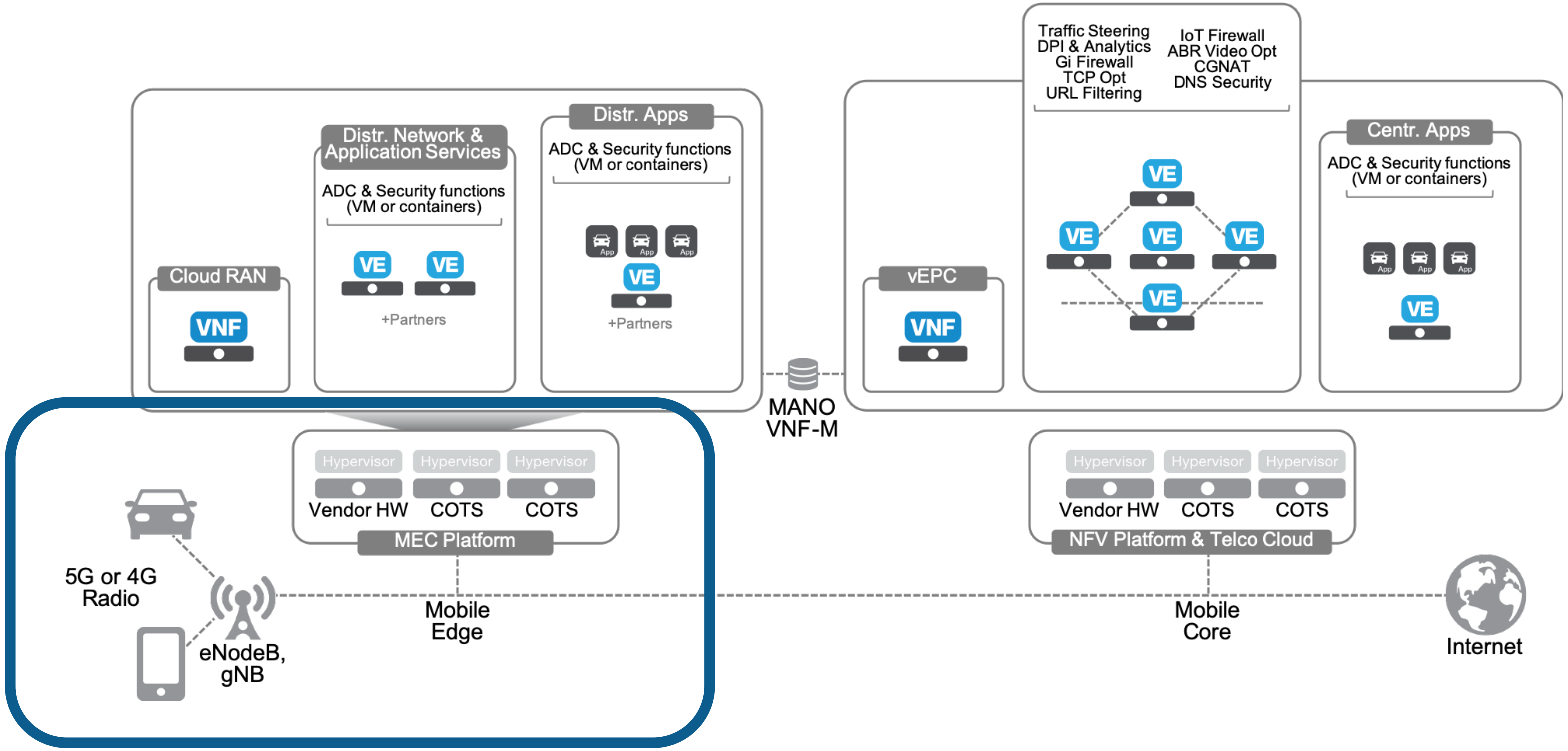
Automate

- MORE SECURITY IN MORE PLACES
- SECOPS CAN BE A BOTTLENECK
- EVEN MINOR EFFICIENCIES PAY OFF
- BUILD ON NFV



Extend Security to the Edge

- DISTRIBUTED 5G DESIGN
- EFFICIENT MITIGATION
- GREATER INTER-DEPENDENCY ON NETWORK AND APPS
- SECURITY AND PERFORMANCE



Go Up the Stack

- NOT JUST BLOCKING IPs AND PORTS
- ADVANCED POLICY IS FURTHER UP
- FOCUS ON BUSINESS LOGIC

DDoS Protection

- Non volumetric attacks
- Application layer attacks
- Advanced attacks (e.g. HTTP/DNS attacks)

WAF

- Data exfiltration
- OWASP Top 10
- Scripting
- Malicious bot activity

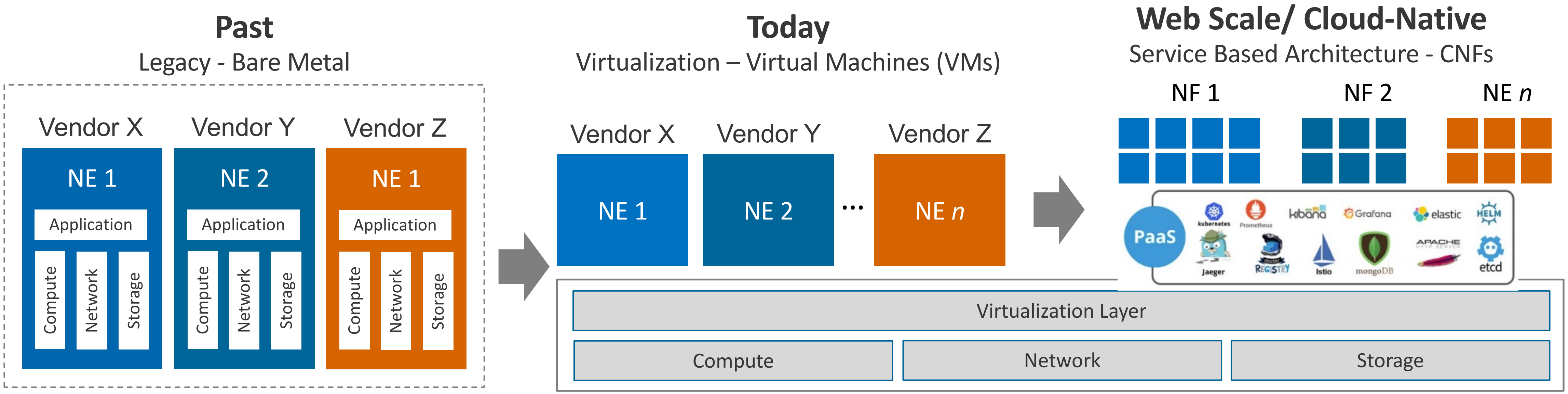
APIs

- Authentication
- Standards enforcement
- Content inspection

Protection on all fronts

- Secure platform
- Functional 3GPP components providing security
- Network and Infrastructure flood and attack protection

Platform Security - PaaS



Past

Legacy - Bare Metal

Today

Virtualization – Virtual Machines (VMs)

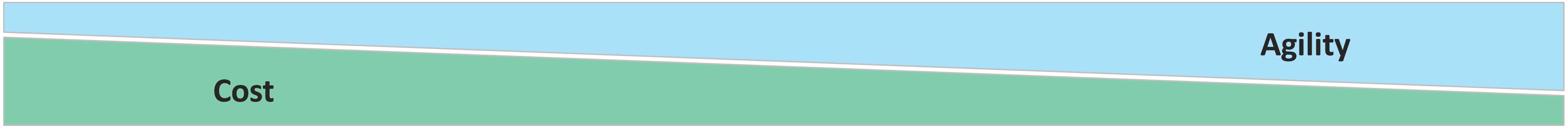
Web Scale/ Cloud-Native

Service Based Architecture - CNFs

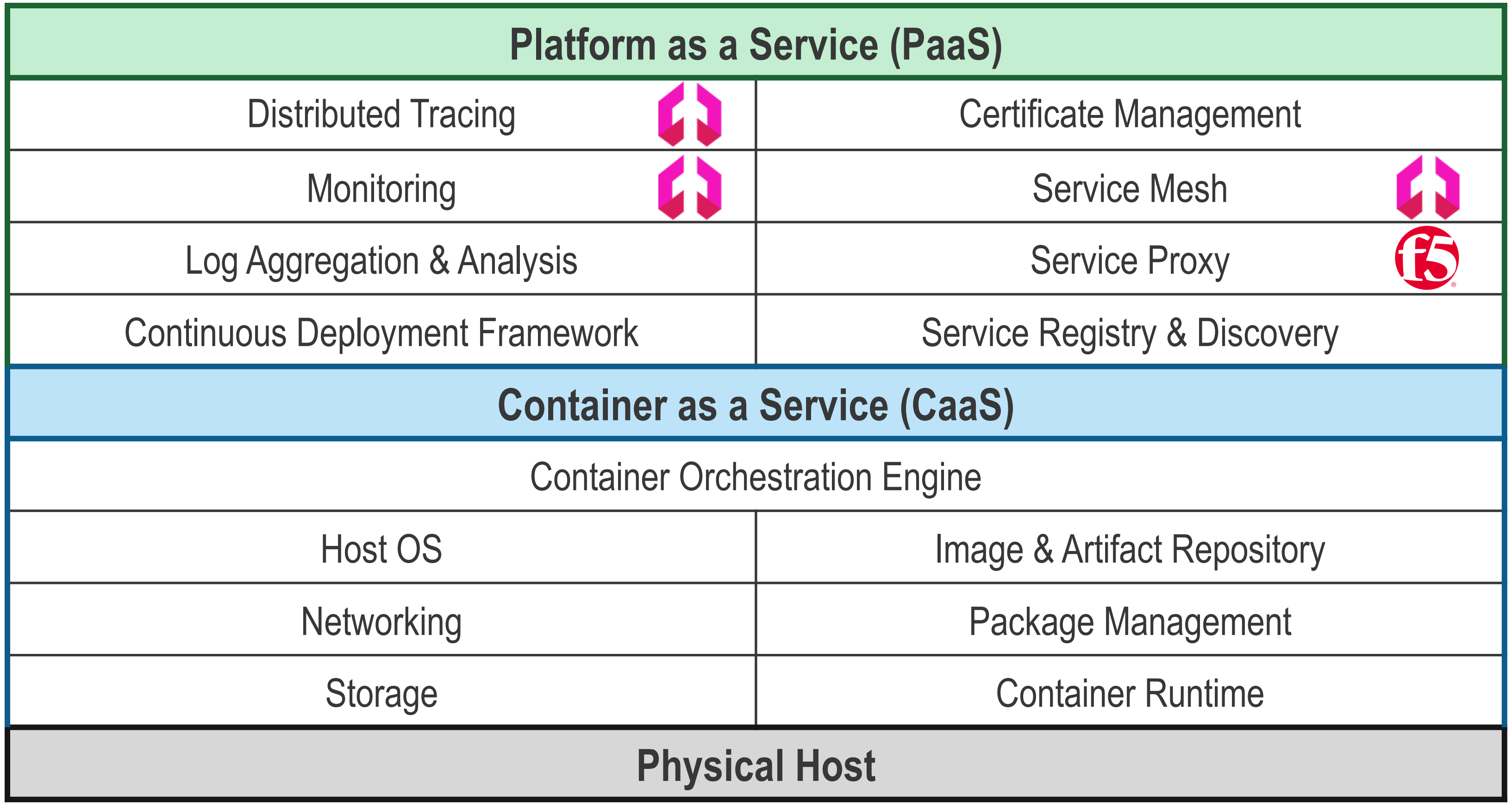
- Bare Metal Servers / Purpose-built HW Appliances
- HW and SW coupling
- Manual MOP-driven Operational Processes

- Eliminate Hardware dependency
- “Software-only” model for vendor VNFs
- Automation and Orchestration
- Multi-tenant: Optimized shared Infrastructure
- Deployment from months to weeks

- "Cloud-Native" Micro-services based architecture for 5G and RAN
- Dynamic network elasticity
- Service orchestration



Web Scale/Cloud-Native Stack



Platform as a Service (PaaS)	
Distributed Tracing	Certificate Management
Monitoring	Service Mesh
Log Aggregation & Analysis	Service Proxy
Continuous Deployment Framework	Service Registry & Discovery
Container as a Service (CaaS)	
Container Orchestration Engine	
Host OS	Image & Artifact Repository
Networking	Package Management
Storage	Container Runtime
Physical Host	

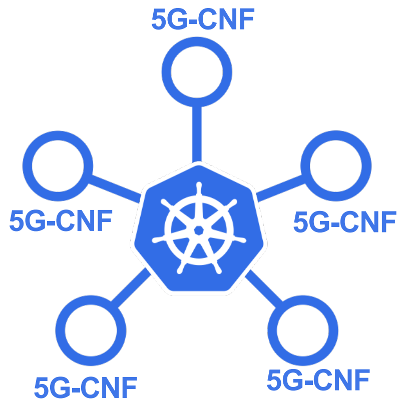
Service Providers are defining CaaS/PaaS architecture utilizing best-of-breed components

Important for Service Providers to own CaaS and PaaS to maintain flexibility, observability and control

F5 Solutions

Part of the PaaS architecture providing industry leading multi-protocol support for 4G & 5G and service mesh with observability, security, and control

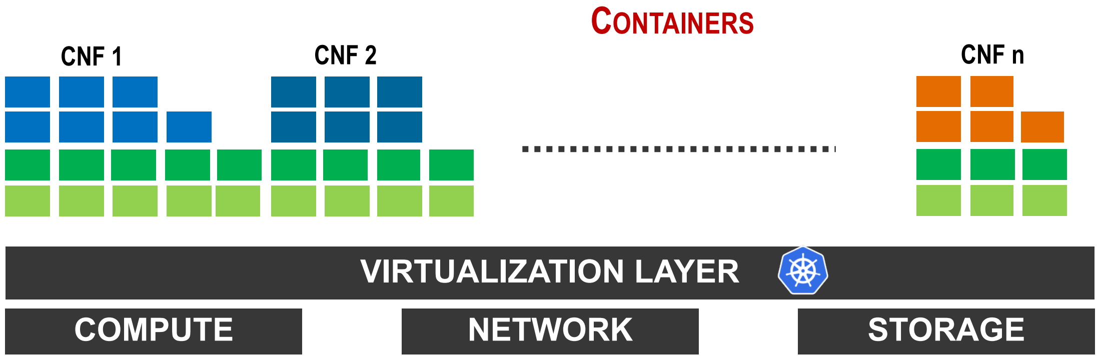
5G Core and Kubernetes (K8s)



K8s flexibility, scalability, and efficiency makes a good choice for cloud native 5G deployments

However K8s was not designed for Service Providers and need to evolve to address the challenges with:

- ➢ Difficultly with protocols that are long lived and have many messages over few connections
- ➢ Lack of security controls
- ➢ Lack of visibility and revenue controls



F5 Service Proxy for K8s

Ingress/Egress Control

per-namespace / per-service proxy

ADC

load balancing for Layer 4 and Layer 7 (TCP, UDP, SCTP, Diameter, GTPcV2)

Secure Proxy

per-service secure firewall

Service Discovery

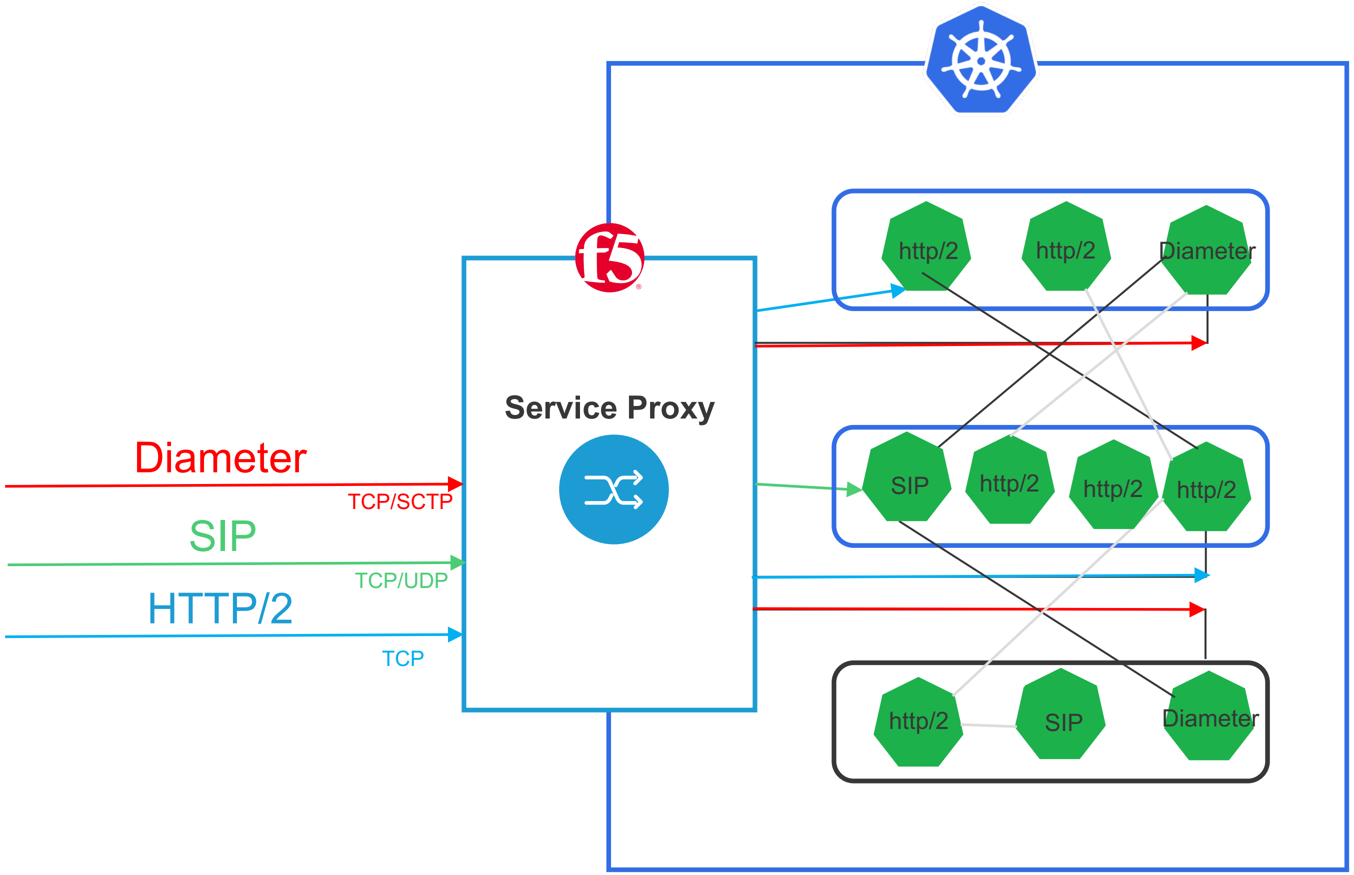
K8s service discovery for automatic configuration of load balancing policies

5G Ingress Use Cases

(4G/5G signaling vision)

Signaling Control

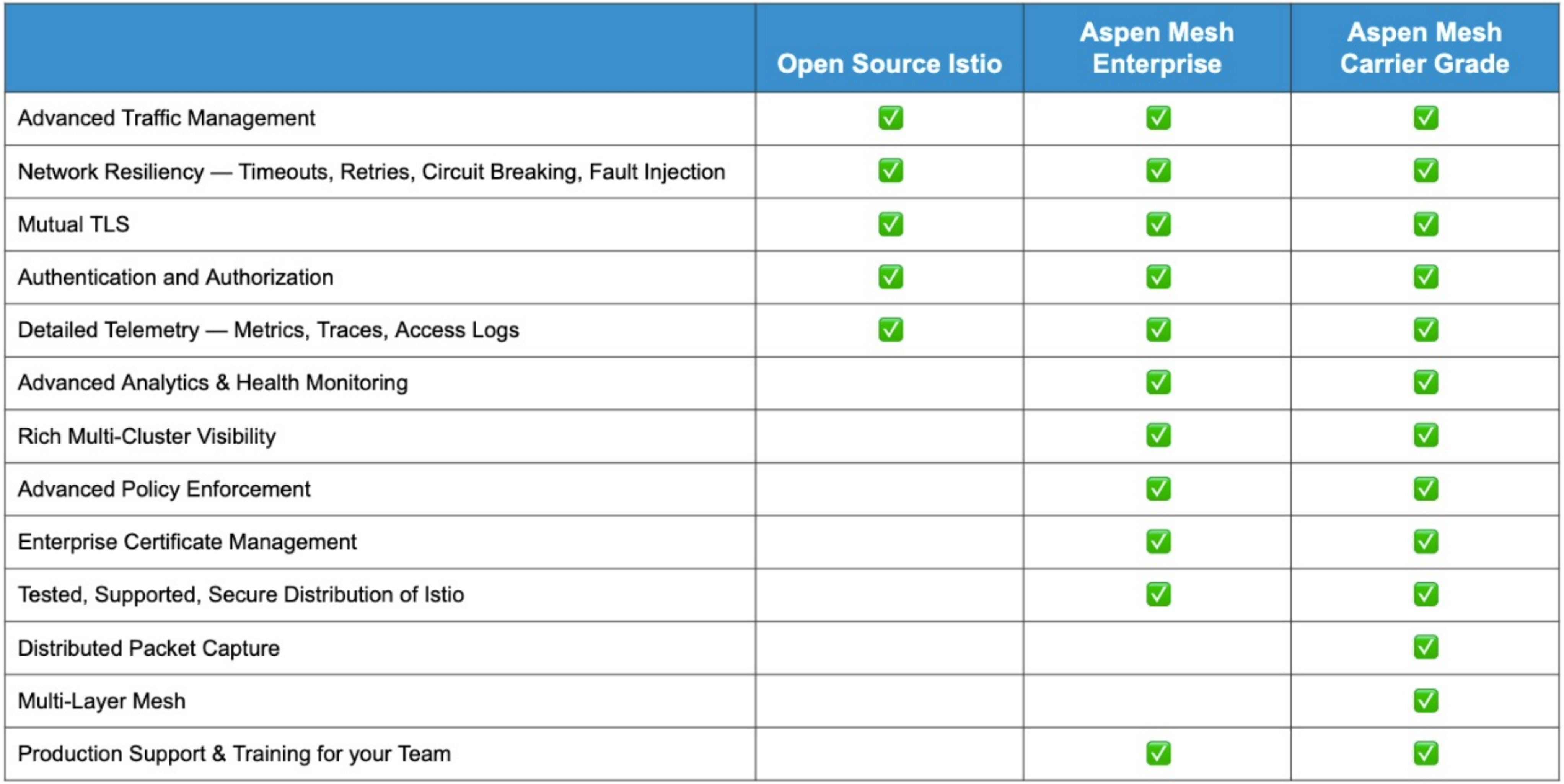
- *routing*
- *load balancing*
- *rate limiting*



K8s has no awareness of telco protocols.

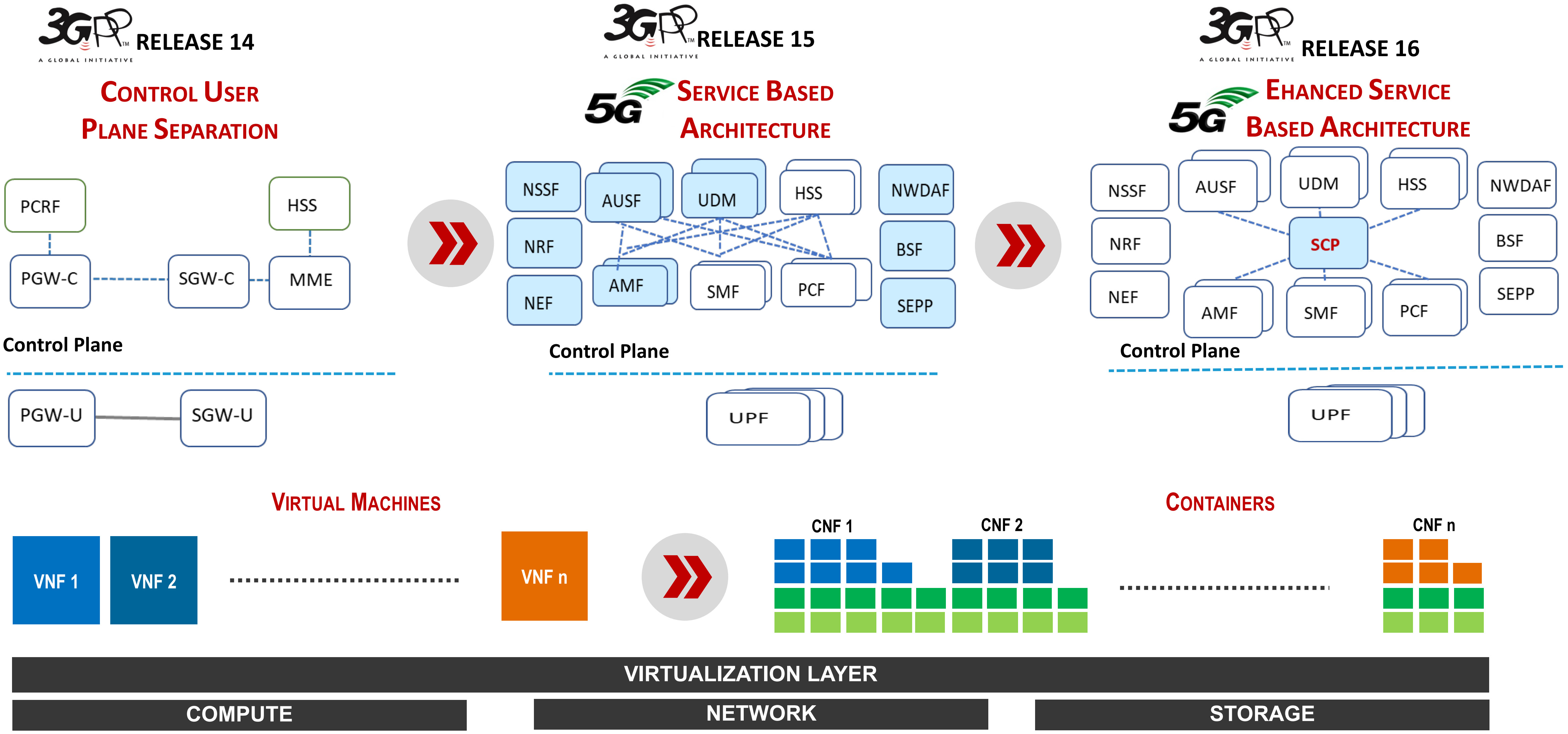
- For example, Diameter is usually a single, big pipe. How to scale multiple, small containers behind it?
- Service Proxy allows for intelligently handling telco messaging protocols.

F5 Aspen Mesh - Istio based Service Mesh



	Open Source Istio	Aspen Mesh Enterprise	Aspen Mesh Carrier Grade
Advanced Traffic Management	✅	✅	✅
Network Resiliency — Timeouts, Retries, Circuit Breaking, Fault Injection	✅	✅	✅
Mutual TLS	✅	✅	✅
Authentication and Authorization	✅	✅	✅
Detailed Telemetry — Metrics, Traces, Access Logs	✅	✅	✅
Advanced Analytics & Health Monitoring		✅	✅
Rich Multi-Cluster Visibility		✅	✅
Advanced Policy Enforcement		✅	✅
Enterprise Certificate Management		✅	✅
Tested, Supported, Secure Distribution of Istio		✅	✅
Distributed Packet Capture			✅
Multi-Layer Mesh			✅
Production Support & Training for your Team		✅	✅

Signalling & Roaming Security



3GPP RELEASE 14

CONTROL USER PLANE SEPARATION

PCRF
HSS
PGW-C
SGW-C
MME

Control Plane

PGW-U
SGW-U

3GPP RELEASE 15

5G SERVICE BASED ARCHITECTURE

NSSF
AUSF
UDM
HSS
NWDAF
NRF
BSF
NEF
AMF
SMF
PCF
SEPP

Control Plane

UPF

3GPP RELEASE 16

5G EHANCED SERVICE BASED ARCHITECTURE

NSSF
AUSF
UDM
HSS
NWDAF
NRF
SCP
BSF
NEF
AMF
SMF
PCF
SEPP

Control Plane

UPF

VIRTUAL MACHINES

VNF 1
VNF 2
VNF n

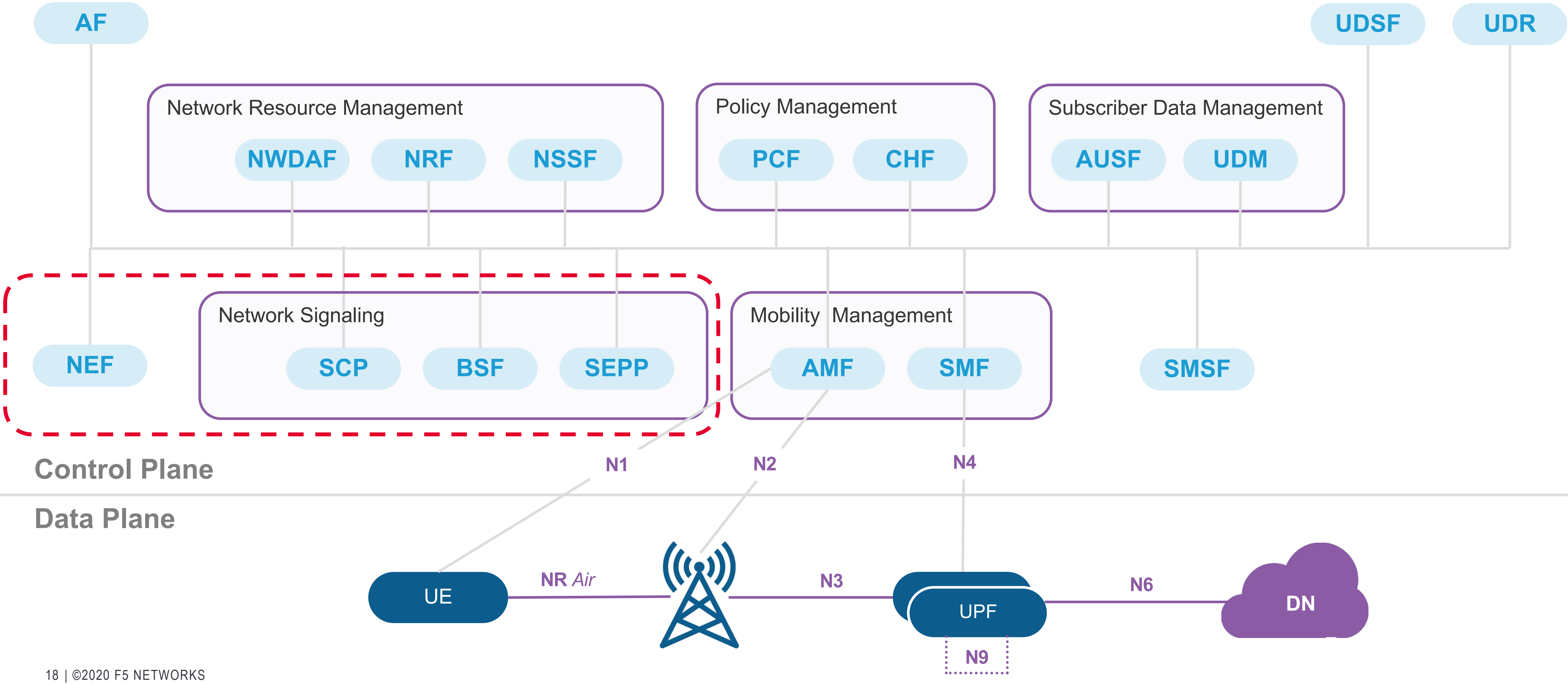
CONTAINERS

CNF 1
CNF 2
CNF n

VIRTUALIZATION LAYER

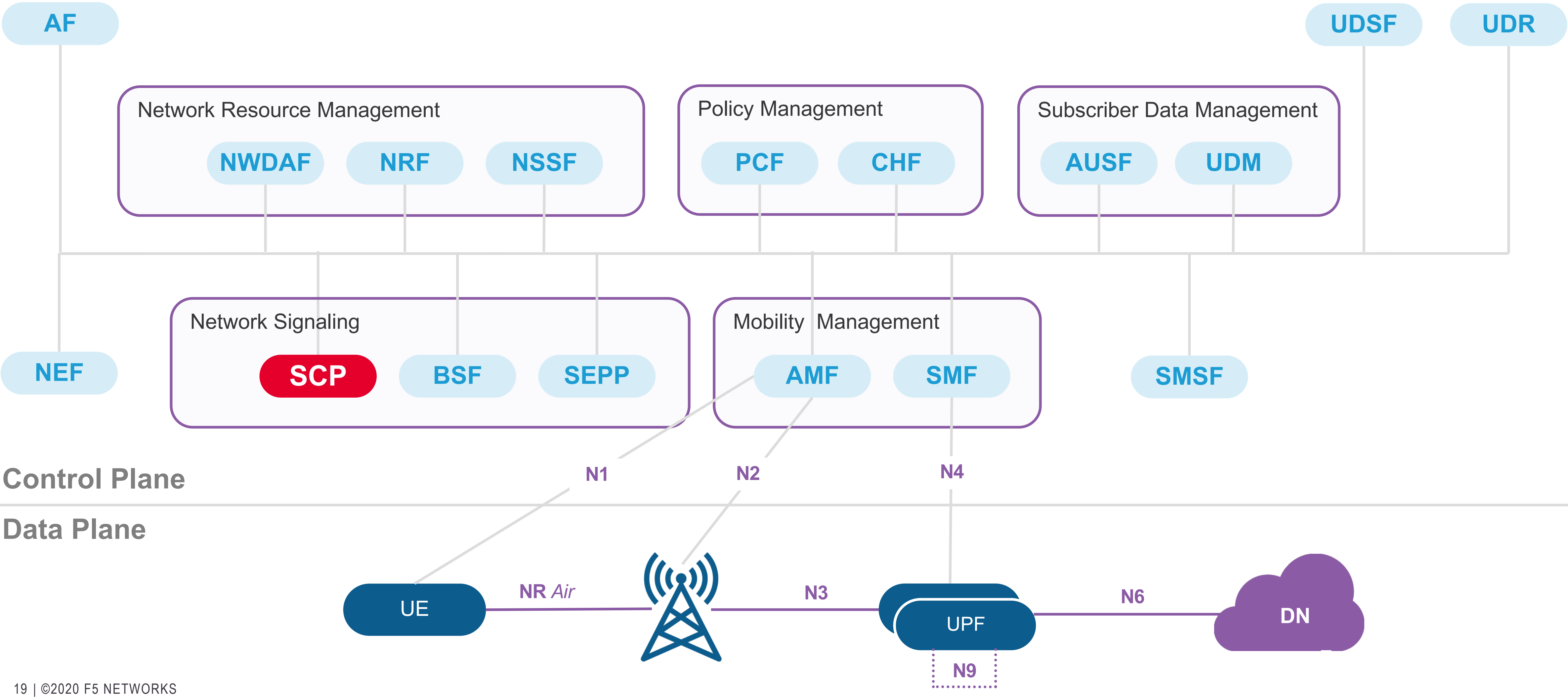
COMPUTE
NETWORK
STORAGE

5G Core Functions

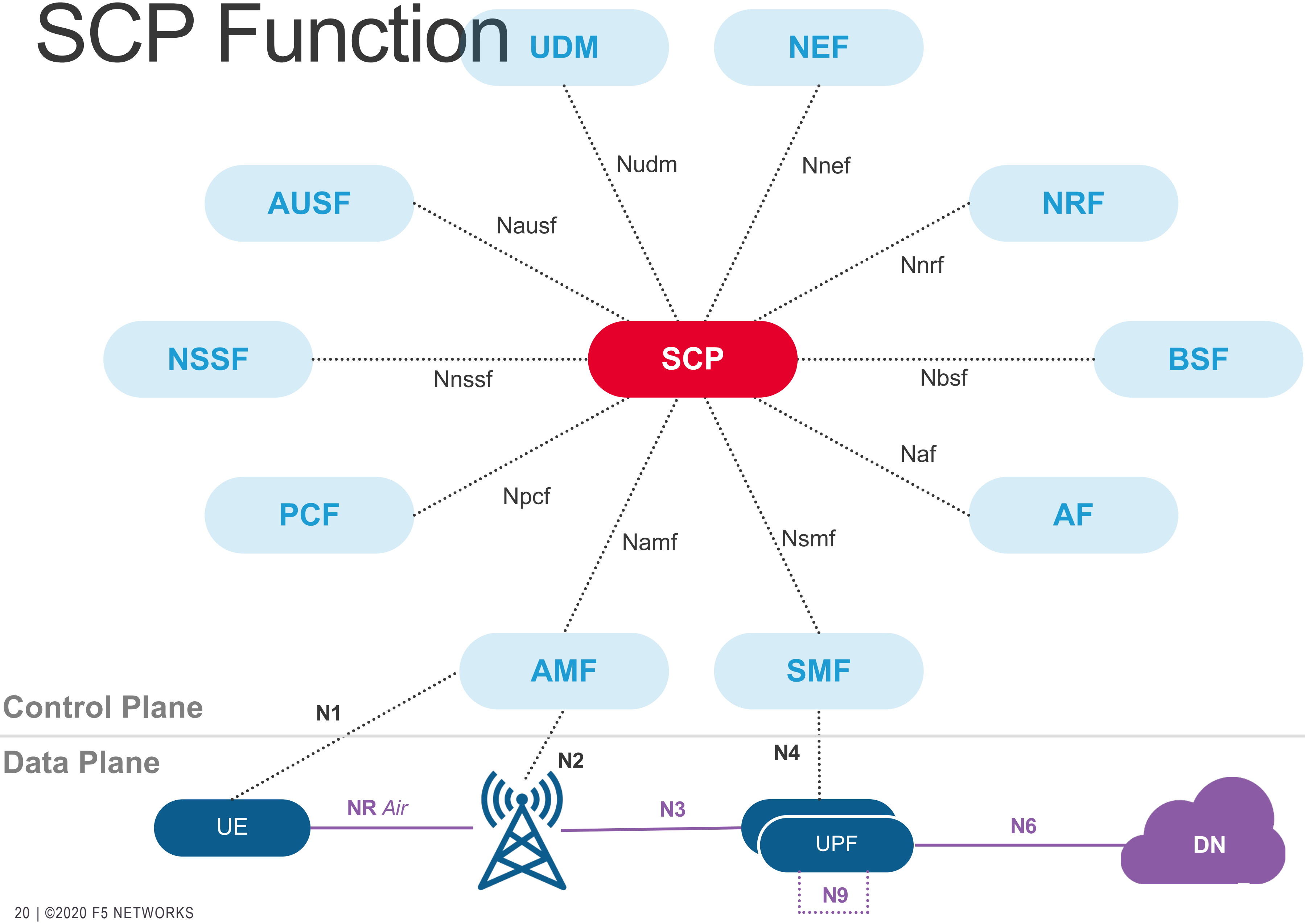


5G Core – Service Communication Proxy

SERVICE COMMUNICATION PROXY (SCP)



SCP Function



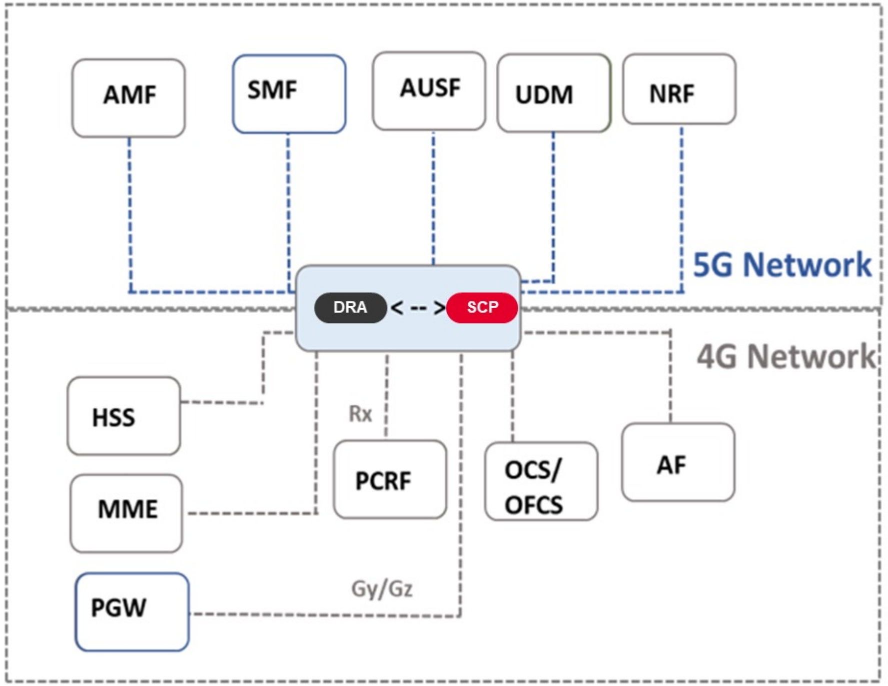
SCP Main Functions

- Routing/Selection
- Load Balancing
- NF Subscription
- NF Degradation and Failures
- Traffic Prioritization
- Congestion and Overload
- Dynamic discovery

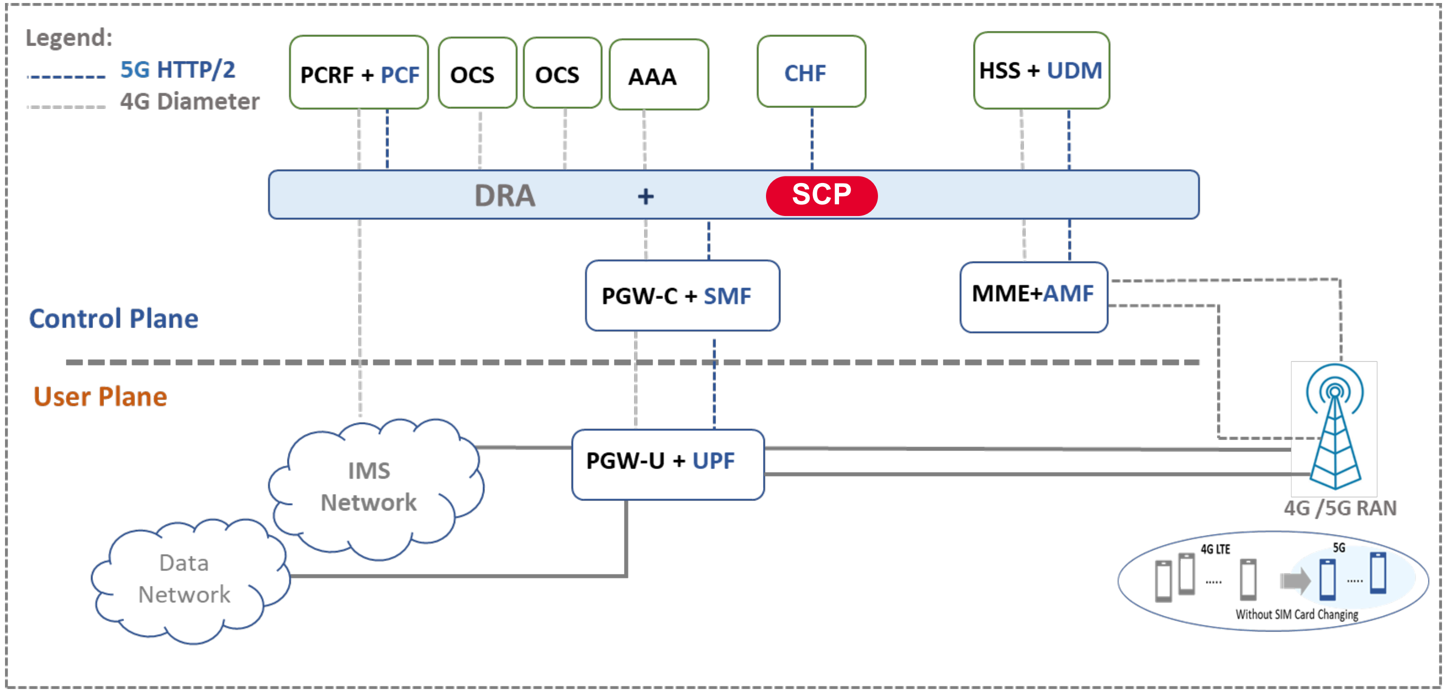
4G/5G Protocol Interworking

SCP provides connectivity with Diameter and HTTP2 protocols translation between 4G and 5G core network functions.

5G Overlay Solution

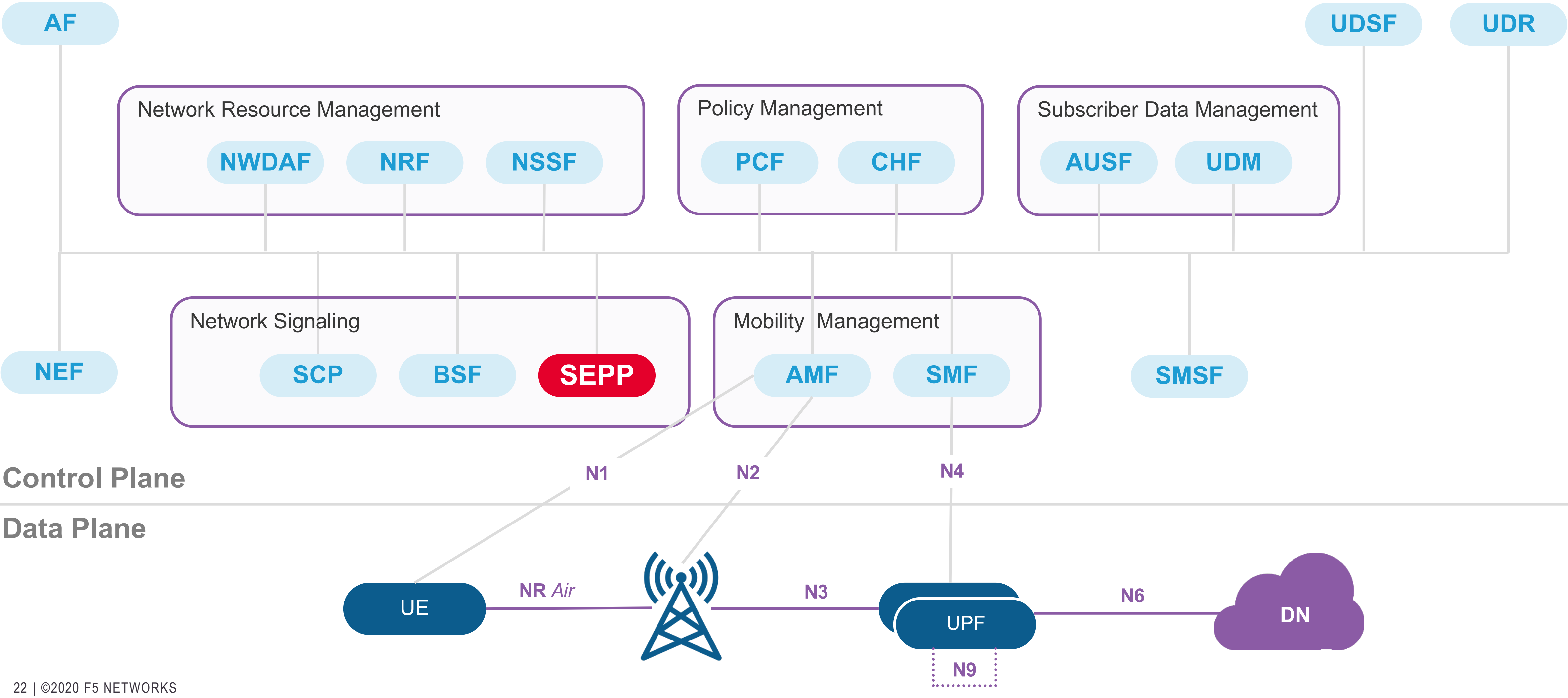


4G/5G Convergent Solution



5G Core – Roaming Security

SECURE EDGE PROTECTION PROXY (SEPP)

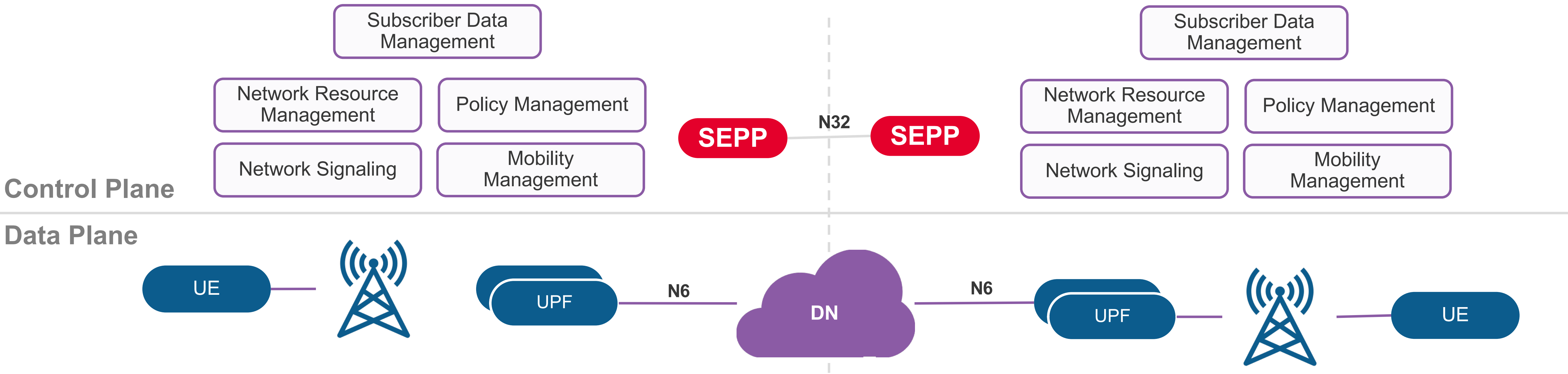


5G Core – Roaming Security

SECURITY EDGE PROTECTION PROXY (SEPP)

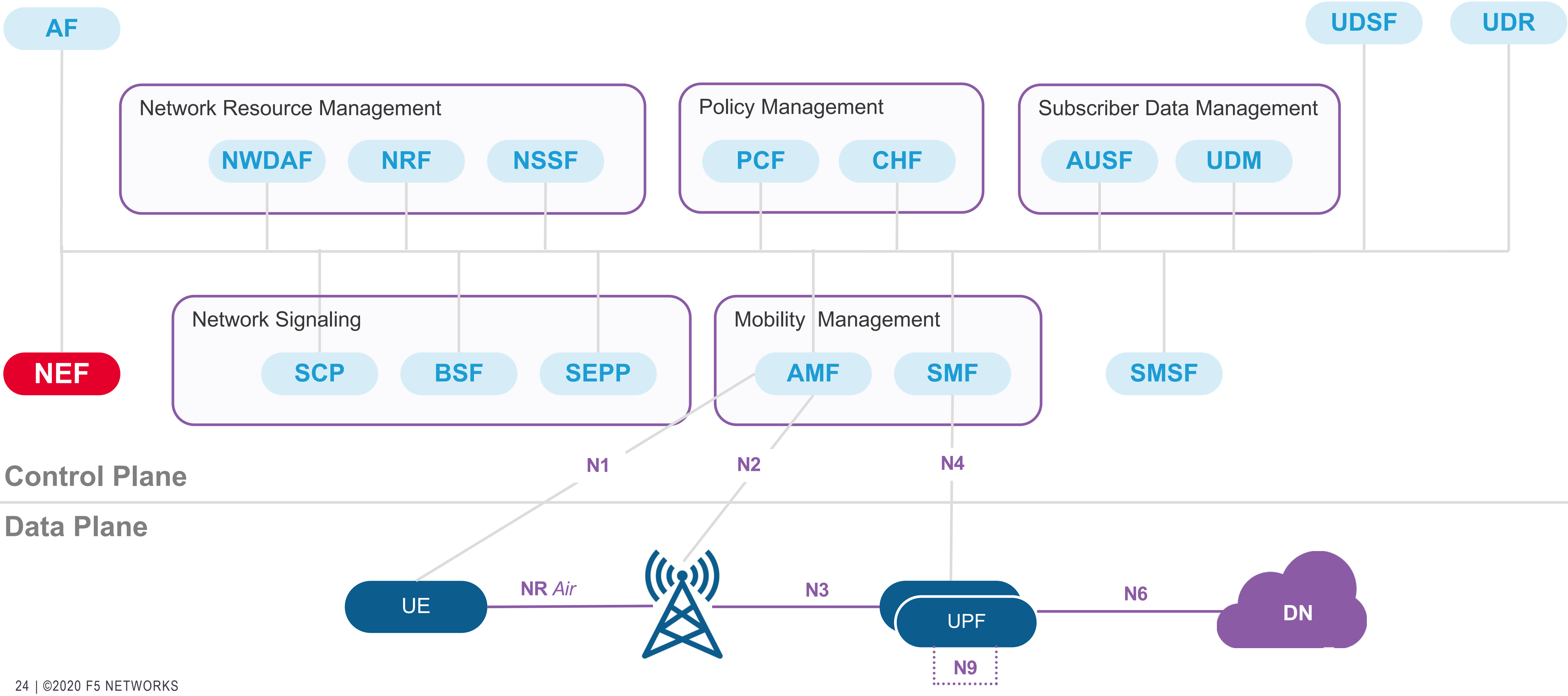
SEPP Main Functions

- Message filtering and policing on inter-PLMN control plane interfaces.
- Topology hiding



5G Core – NF Exposure / API Gateway

NETWORK EXPOSURE FUNCTION (NEF)



DNS Security

Advanced GSLB for multi data center and cloud

Authoritative DNS

DNS caching and resolving

Realtime DNS SEC

Intelligent Global Server Load Balancing

- Traffic steering to the most available and suitable datacenter.
- Integrated solution with LTM.
- Decisions based on real-time health of an LTM protected datacenter.
- Extensible health monitors, including service provider / mobile core
- Built-in database for geo-location traffic steering.

Comprehensive Secure DNS Delivery

- High-performance Authoritative DNS, DNS Caching, and DNS Resolving.
- Real-time DNSSEC.
- Market focus on Security & Service Provider
- Solution well suited to environments susceptible to DDoS attacks

N6 Security

Subscriber Aware Firewall

Carrier Grade NAT

Application Layer Gateways

DDoS Detection & Mitigation

Intrusion Detection & Prevention

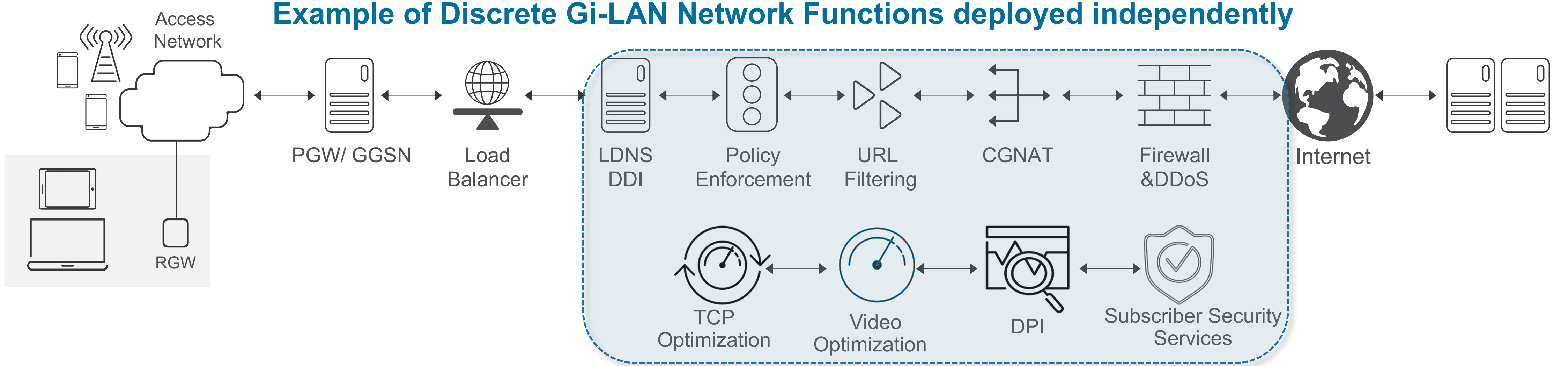
Telco Protocol Firewalls

Dynamic Blacklisting

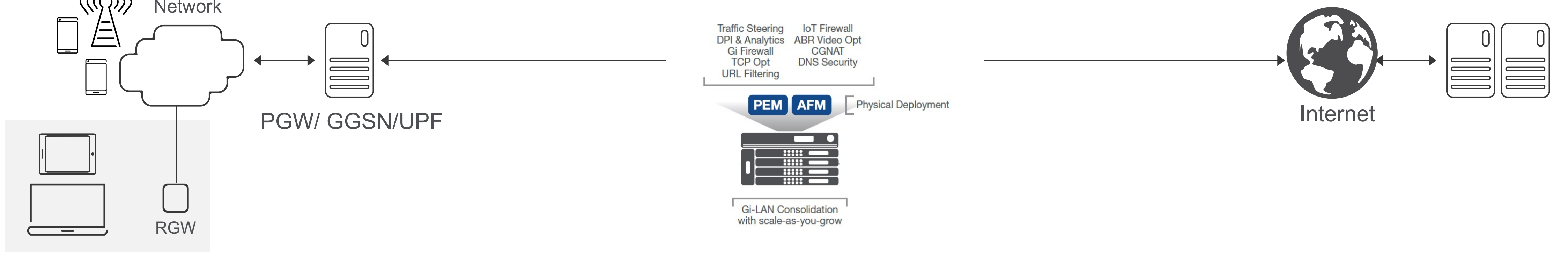
Smart Coprocessor

N6/Gi-LAN Security

Example of Discrete Gi-LAN Network Functions deployed independently

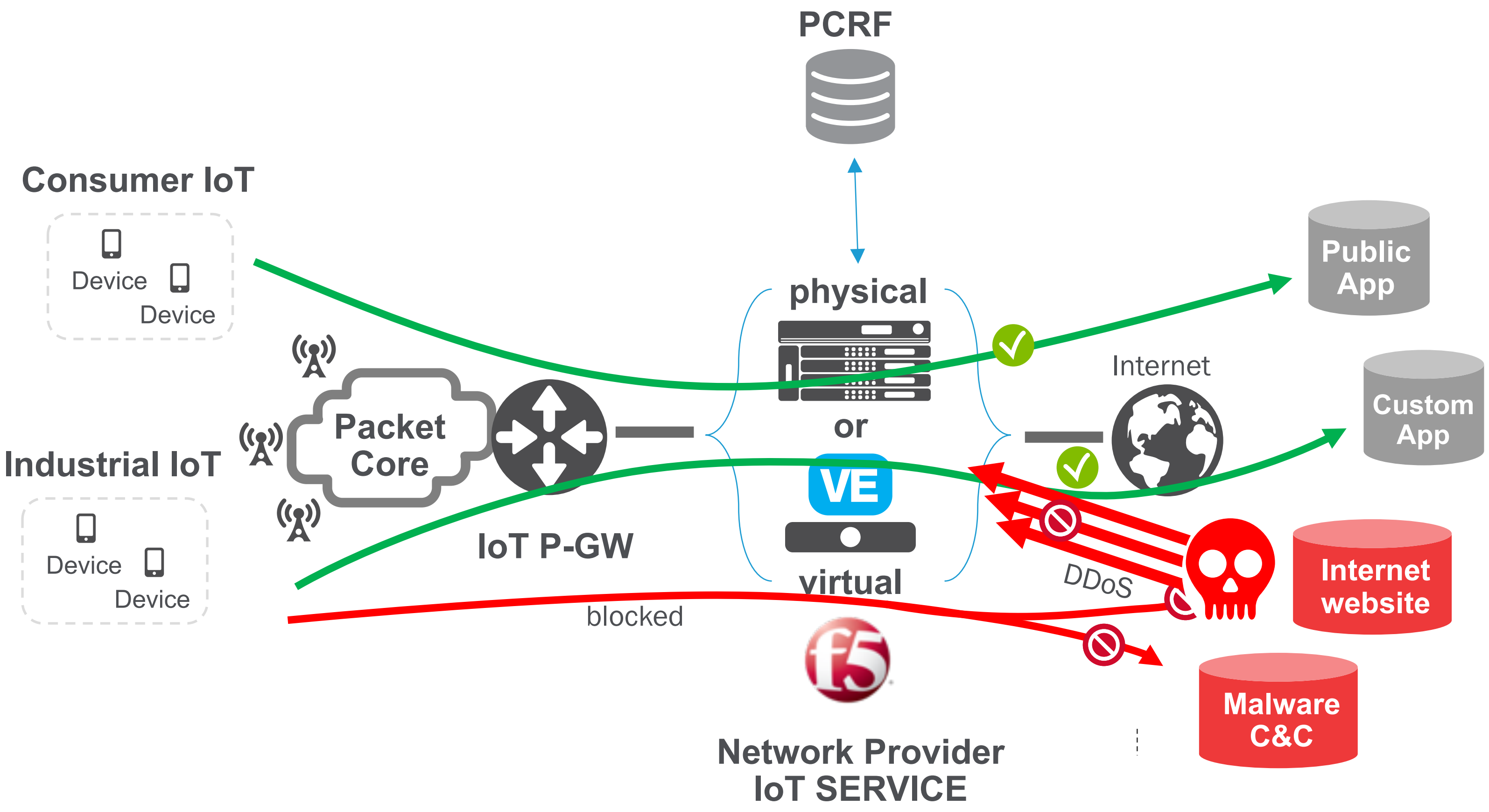


Example of consolidated Gi-LAN NF with F5 VNF



Network-centric IOT Security

DEVICE-AWARE IOT-FW ON GI LAN



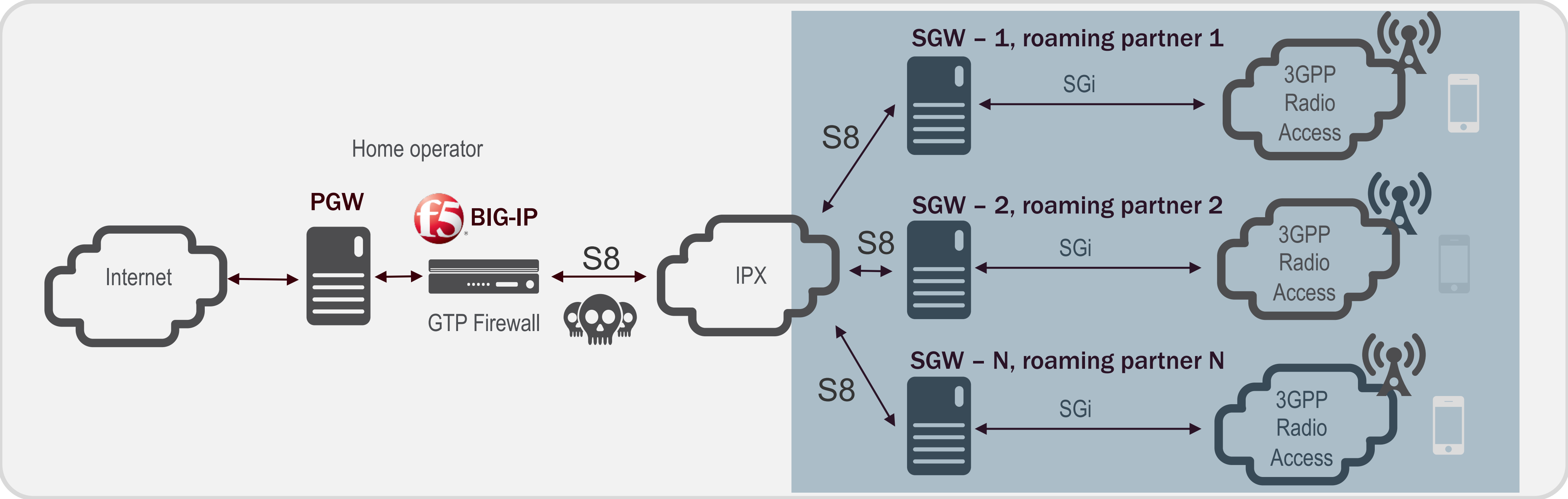
PCRF controlled per-device ACL

Customers want to ensure SIMs purchased for a particular service, such as location tracking, are bound to that service and cannot be used intentionally or otherwise to access general internet services

DDOS & Attack mitigation

IoT devices often lack the performance or connectivity to provide effective security for the device. IoT devices are increasingly targeted by malicious users

GTP Firewall



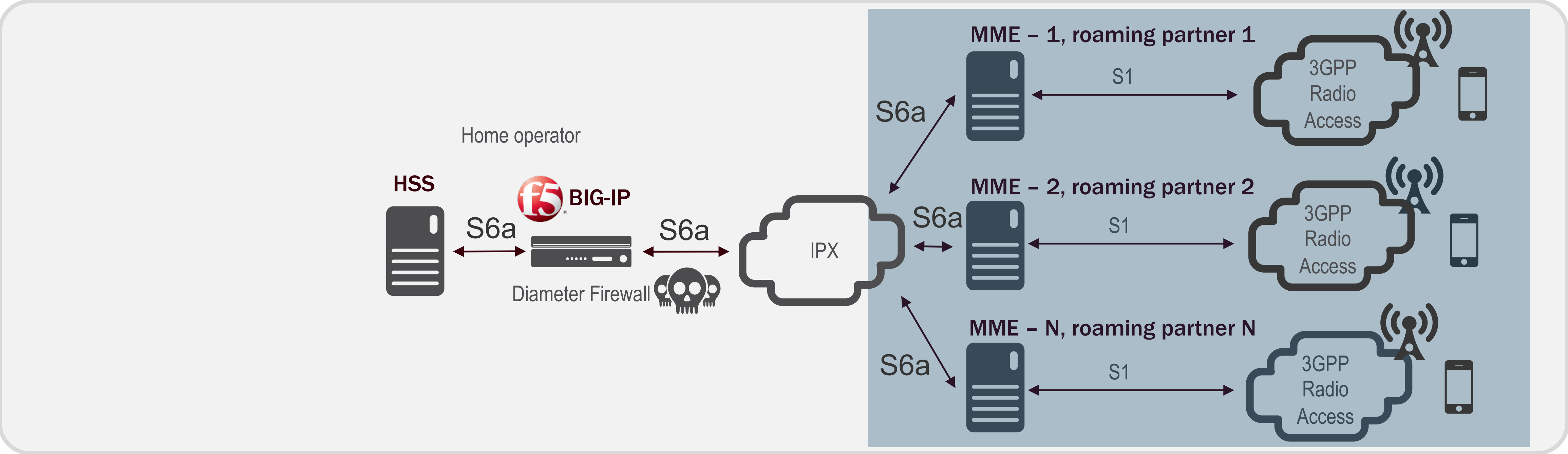
Problem Statement

- If a customer roams, the SGW is in the visited network and both GTP-C (signaling) and GTP-U (User Data) are transported via the S8 interface.
- The home operator has no control on the GTP traffic entering its network

Solution

- GTP-C signaling is checked on protocol conformance
- GTP-C signaling is checked against security rules
- GTP-U user plane traffic is only allowed if TEID was received before, so a pinhole was created
- GTP can be checked in general or for a specific roaming partner

Diameter Firewall



Problem Statement

- If a customer roams, the MME is in the visited network and Diameter S6a (signaling) is transported via the S6a interface of the IPX network.
- The home operator has no control on the Diameter traffic entering its network

Solution

- Diameter S6a signaling is checked on protocol conformance
- Diameter S6a signaling is checked against security rules
- F5's BIG-IP solution consists of the LTM and AFM modules, using respectively MRF and IPS functionalities for Diameter management
  - Compliant with GSMA's FS.19 Diameter Security Cat 0-3
  - Security Rules can be downloaded free-of-charge and/or created by partner/customer