The bridge to possible

Securing Your 5G Network

A Highly Effective and Vendor Agnostic Security Architecture for 5G

Cisco Knowledge Network

Pramod Nair
Security, Cisco

Mr Phil Hyde,
CTO & Evangelist, Accordant

28th Sept 2021

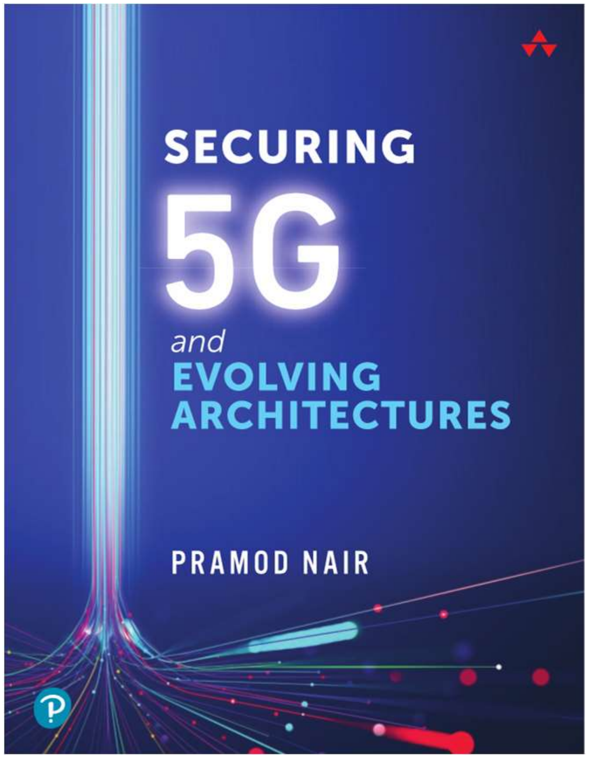
Discussion Topics for today

- Evolution of Networks & Security
- E2E Threats in 5G networks
- 5G Security use cases
- Real Life 5G security deployment
  (by Phil Hyde, CTO & Evangelist, Accordant)
- E2E threats mitigation
- Takeaways

Me…

Lives in Ireland , Works for Security, Focussed on Service Providers
pramonai{at}cisco.com
Co-lead 5G Security 5GAmericas, Works closely with NIST for 5G security

5G Security book



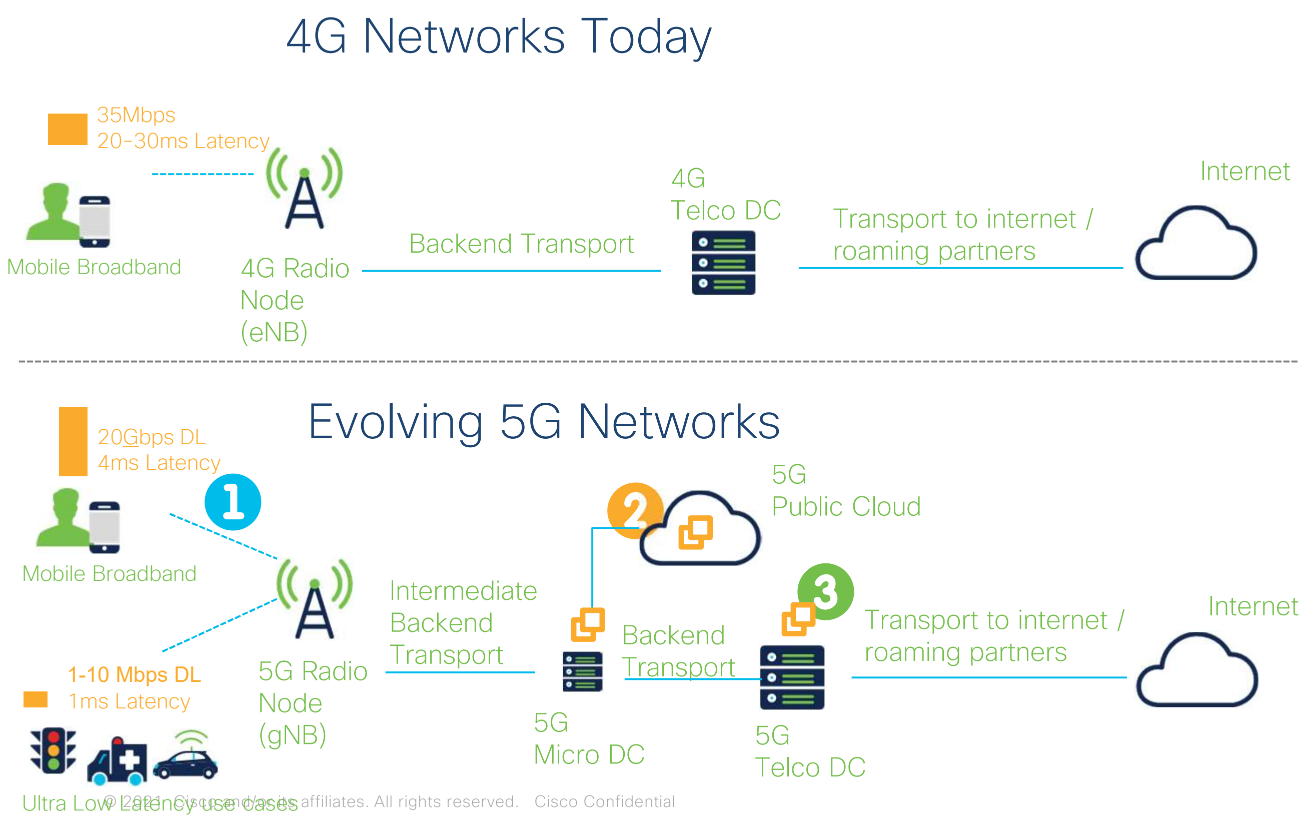
Pre-ordering link:
https://www.amazon.com/Securing-Evolving-Architectures-Pramod-Nair/dp/0137457936/ref=sr_1_1?dchild=1&keywords=securing+5g&qid=1632747776&s=books&sr=1-1

About the book:

A vendor agnostic book covering the following key topics:

- Explore new 5G security challenges–and why you still need external controls, even with recent 3GPP improvements
- Implement network component security controls for RAN, Transport, 5GC, and devices
- Safeguard Multi-Access Edge Compute (MEC), SDNs, virtualized 5G cores, and massive IOT
- Protect Public and Non-Public Networks (Private 5G) deployment scenarios
- Secure Critical Infrastructure, Vehicle to Everything (V2X), and Smart Factory use cases
- Optimize end-to-end 5G security architecture across all 5G domains based on zero trust
- Prioritize 5G security investments in service provider or enterprise environments
- Preview emerging 5G use cases and ML/AI-based security enhancements

Network Evolution



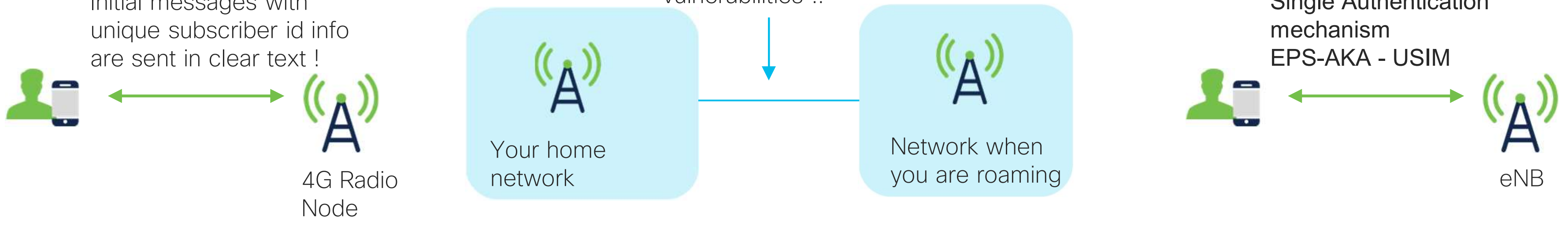
1. Higher throughput, lower latency, sliced network to cater for multiple use cases

2. Disaggregated & Decomposed RAN & Packet Core

3. Virtualized 5GC network functions deployable at public cloud / on-premises

Security Evolution - Simplified

4G Networks



Multiple protocols (Diameter, GTP, SS7) with many known vulnerabilities !!

Initial messages with unique subscriber id info are sent in clear text !

4G Radio Node

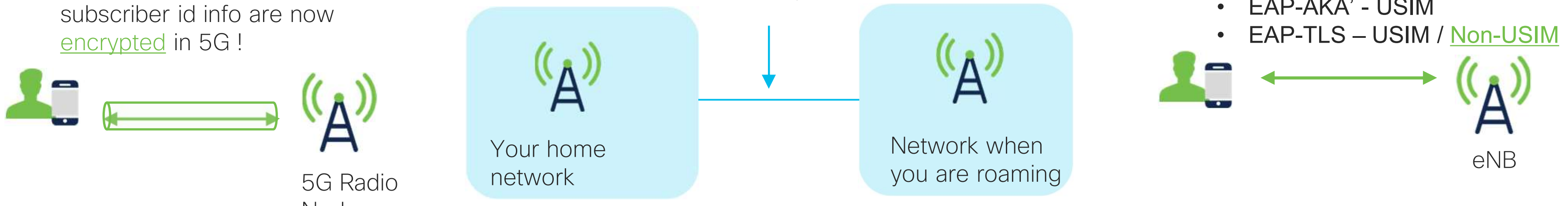
Your home network

Network when you are roaming

Single Authentication mechanism EPS-AKA - USIM

eNB

5G Networks



APIs are used in 5G with a defined network function called Secure edge Protection Proxy (SEPP)

Initial messages with unique subscriber id info are now encrypted in 5G !

5G Radio Node

Your home network

Network when you are roaming

5G allows multiple Authentication mechanism

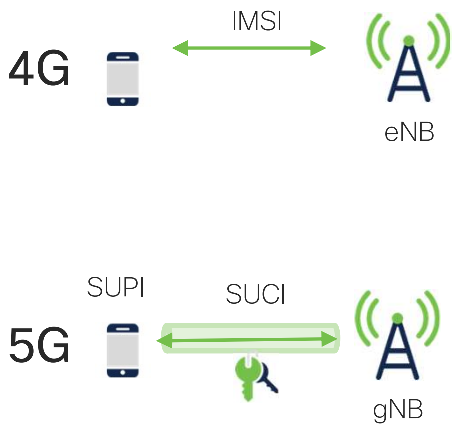
- 5G-AKA - USIM
- EAP-AKA’ - USIM
- EAP-TLS – USIM / Non-USIM

eNB

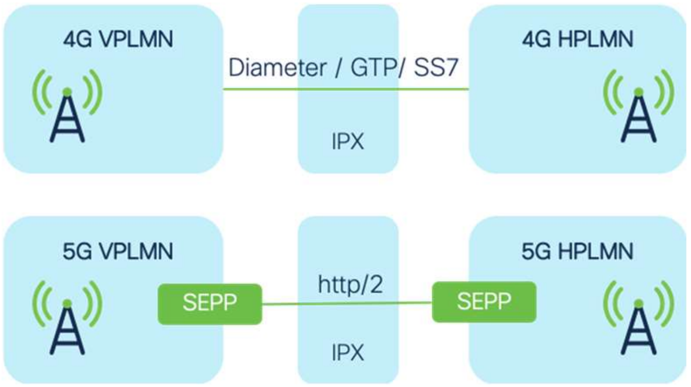
Reference Slide

Security evolution - detailed

Subscriber Security



Roaming & Interconnect



4G Authentication mechanism for user equipment:

- EPS-AKA - USIM

5G Authentication mechanism for user equipment:

- 5G-AKA - USIM
- EAP-AKA' - USIM
- EAP-TLS - USIM / Non-USIM

IMSI: International Mobile Subscriber Identity
SUPI: Subscription Permanent Identifier
SUCI: Subscription Concealed Identifier
VPLMN: Visited Public Land Mobile Network
HPLMN: Home Public Land Mobile Network
IPX: Internetwork Packet Exchange

Reference: 3GPP TS 33.501
http://www.3gpp.org/ftp/specs/archive/33_series/33.501/

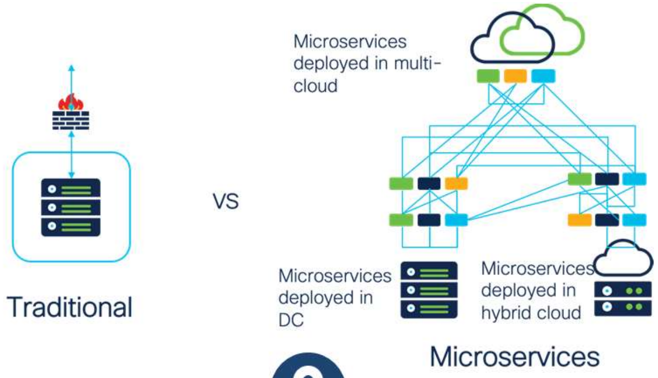
Key Challenges in 5G

IoT & M2M

1

Weak inbuilt security in IoT devices, peer to peer attacks, V2X use cases

Perimeter less deployments



Traditional

VS

Microservices deployed in multi-cloud

Microservices deployed in DC

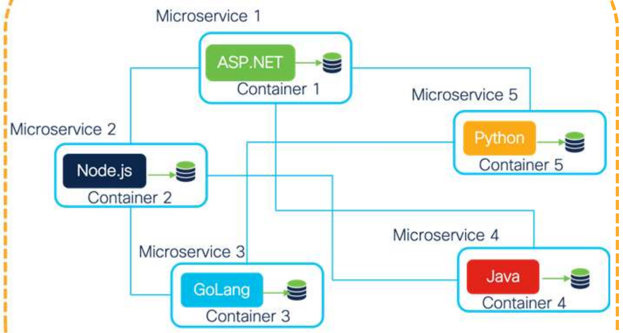
Microservices deployed in hybrid cloud

Microservices

2

5G components can be deployed on-premises and in the cloud, this breaks the concept of perimeter-based deployments. We didn't have to worry about this is 4G

Polyglot architecture



Microservice 1

ASP.NET

Container 1

Microservice 2

Node.js

Container 2

Microservice 3

GoLang

Container 3

Microservice 4

Java

Container 4

Microservice 5

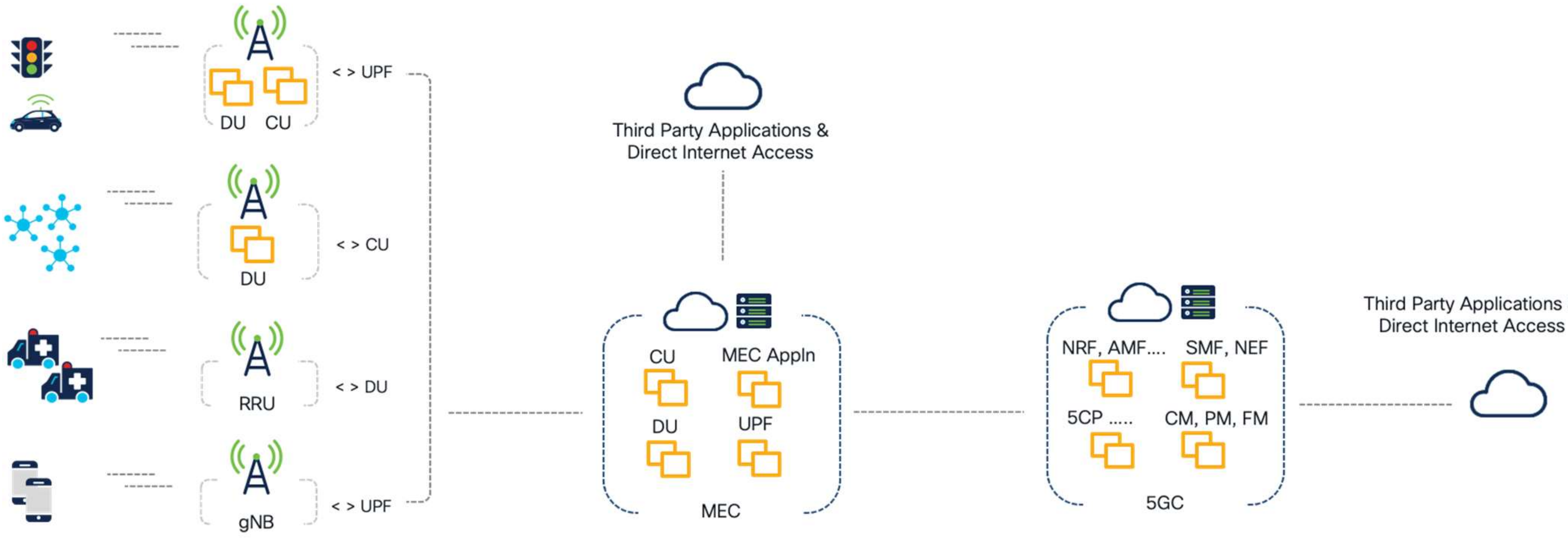
Python

Container 5

3

Virtualized 5G components use open-source programs which introduce vulnerabilities. We didn't have to worry about his in 4G.

Threats in evolving architectures



Device Threats

- Malware
- Bots DDoS
- Firmware Hacks
- Device Tampering
- Sensor Susceptibility
- TFTP MitM attacks

Air Interface Threats

- MitM attack
- Jamming

RAN Threats

- Rogue Nodes
- Insecure S1, X2
- Insecure Xx, Xn

MEC & Backhaul Threats

- DDoS attacks
- LI Vulnerabilities
- Insecure Sx
- Insecure N6
- MEC Backhaul sniff
- Side Channel attacks
- NFVi Vulnerabilities

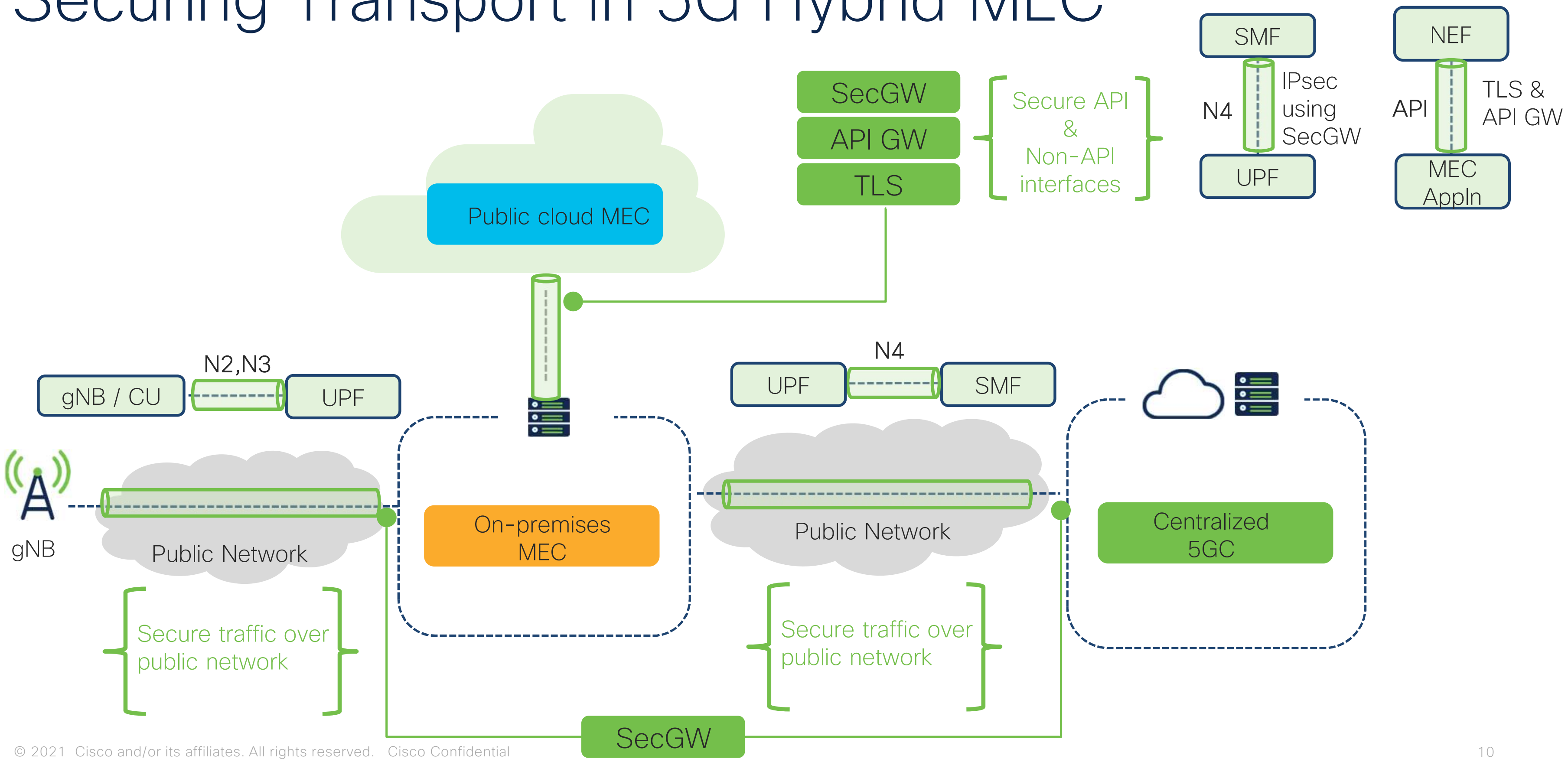
5G Packet Core & OAM Threats

- Virtualisation
- LI Vulnerabilities
- Improper Access Control
- Network Slice security
- API vulnerabilities
- NEF vulnerabilities
- Roaming Partner
- DDoS & DoS attacks

SGi / N6 & External Roaming Threats

- IoT Core integration
- VAS integration
- App server vulnerabilities
- Application vulnerabilities
- API vulnerabilities

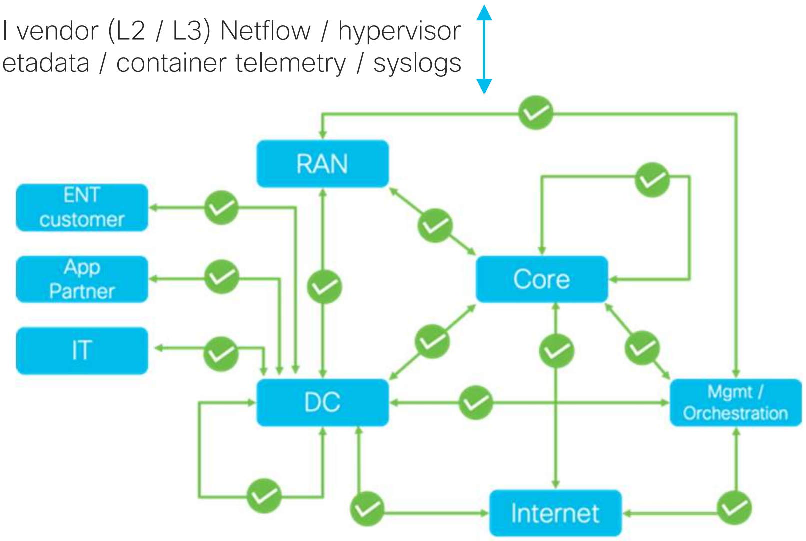
Securing Transport in 5G Hybrid MEC



E2E monitoring for multi-vendor 5G networks

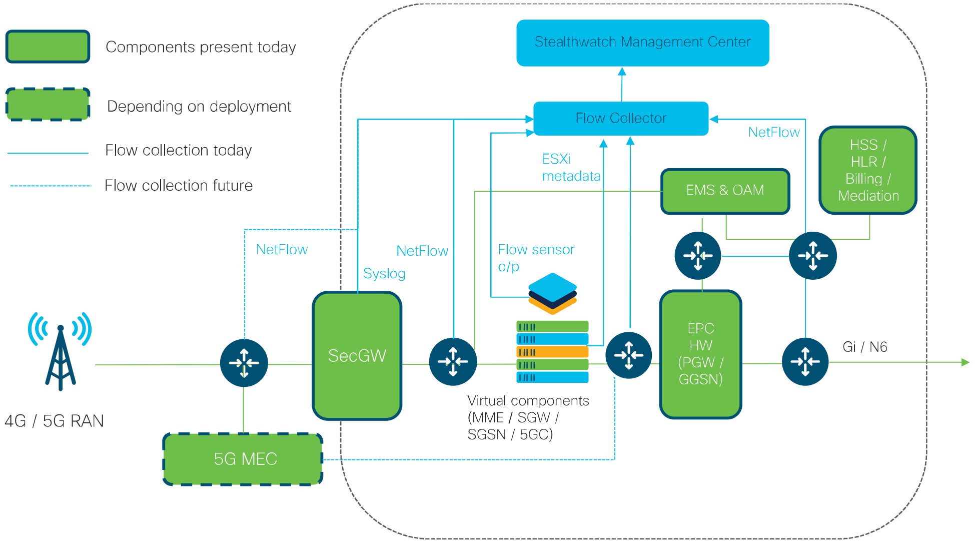
Cisco Stealthwatch

All vendor (L2 / L3) Netflow / hypervisor metadata / container telemetry / syslogs



(actual design for a customer)

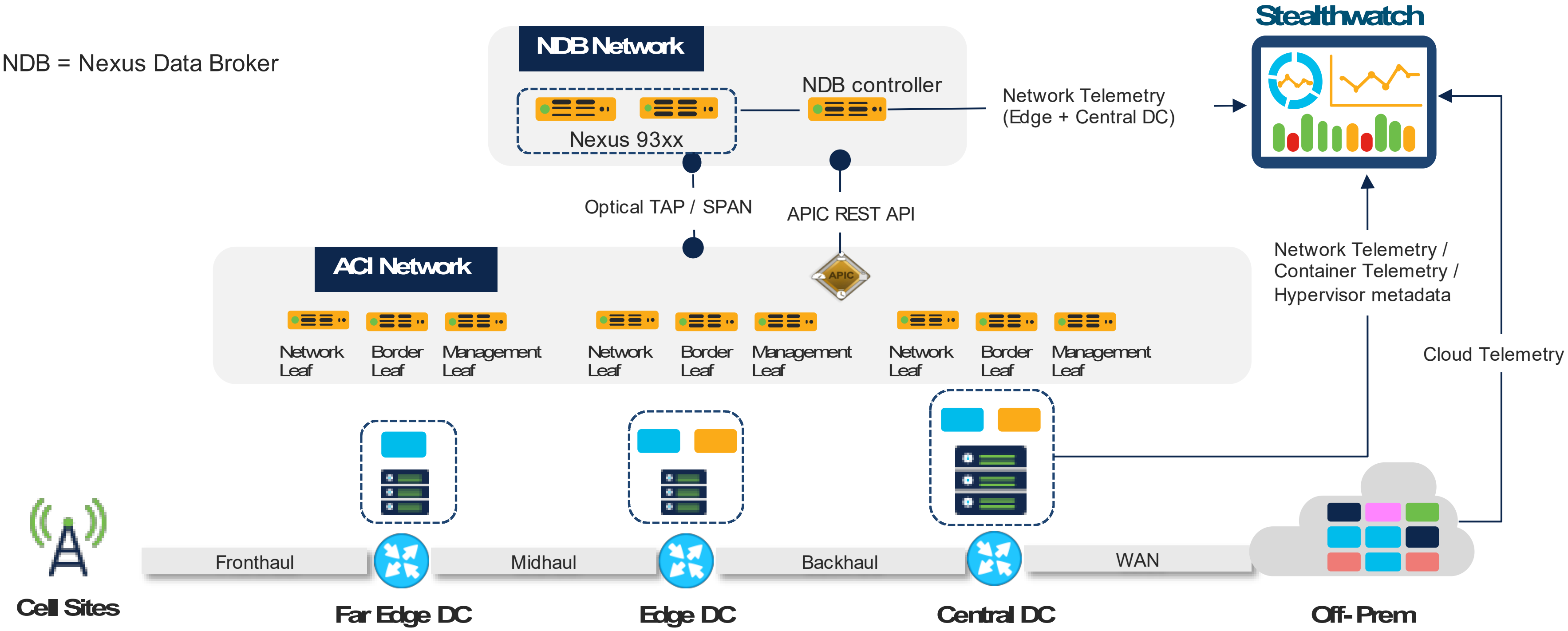
Deployment illustration



5G Telco cloud Analytics - edge and central DC

(actual design for a customer)

NDB = Nexus Data Broker



Nexus Data Broker:
https://www.cisco.com/c/en/us/products/cloud-systems-management/nexus-data-broker/index.html

Secure 5G MEC service chaining

Real network deployment example

Phil Hyde, CTO and Evangelist, Accordant

GET TO KNOW US

Phil Hyde – CTO, Cyber Security Practice Lead and Mentor at Accordant Solutions

Phil.hyde@accordantsolutions.co.uk

8 Years in Cyber Security, specialising in Service Provider, Telco and Defence:

- Former Pro-Wrestler
- Network and Cloud Firewall & IDPS
- NetFlow Analytics
- Cloud Security Internet Gateway
- Security Log Dashboarding

Accordant Solutions – *Harmony In Change*

UK-based Technology Solutions Company, helping people globally improve social value to their Organisation, Cyber Security, Customers, Employees and Planet.

People
Improve customer loyalty and experience
Protect staff and their families

Prosperity
Increase performance
Protect company value
Protect assets

Planet
Reduce environmental impact through digital transformation and product selection

accordantsolutions.co.uk
Accordant Solutions 2021

THE REQUIREMENT FOR 5G MEC SECURITY

TELCO FLAGSHIP SERVICE GOING LIVE – THE NEED FOR SECURITY

- Move content closer to the subscriber; 5G becoming sole-Internet service; reduce the time for content delivery; this does *not* reduce the focus on availability
- Operational Concerns with inline Security devices - latency, user experience and scalability; active/active traffic
- Parent Company Security Requirements – L2-L7 application control, Threat Intelligence blocking,

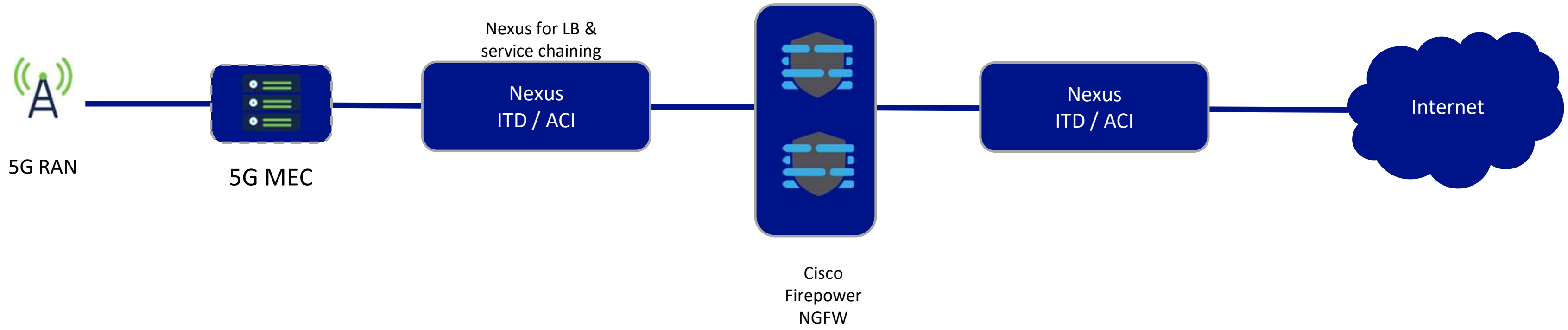
People
Improve access to services and resilience to
improve customer experience

Global Security Sustainability
Align with global security sustainability; Security
Tools that are centrally managed and governed

Prosperity
Increase customer and company value
through availability and security of
services

MEET THE SOLUTION – HIGH LEVEL

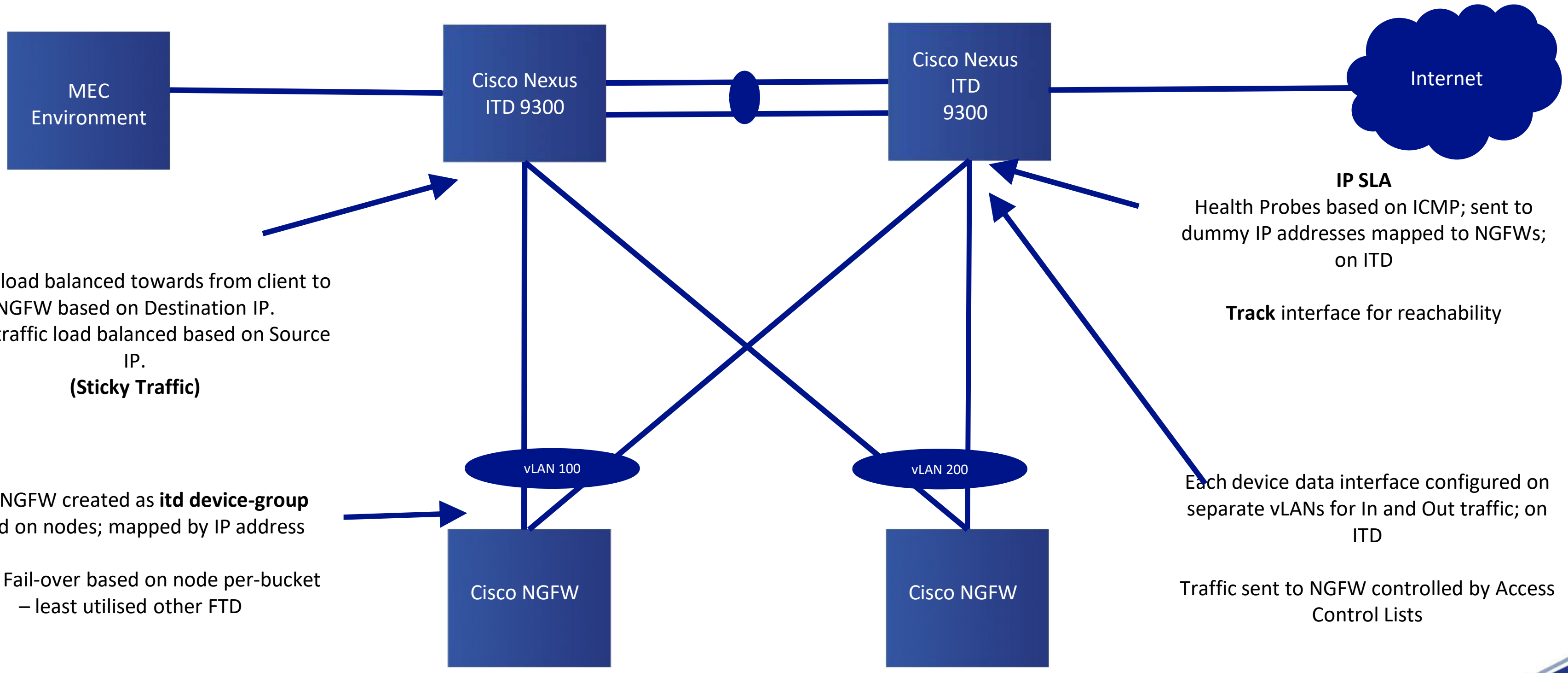
CISCO NEXUS INTELLIGENT TRAFFIC DIRECTOR PACKET BROKER



- Uses Nexus 9300 Switching Portfolio ✓
- Deployed at Layer 2 – simple integration ✓
- Allows the integration of Security Tooling with logical attachment ✓
- Supports Active/Active for load balancing and high-availability of web content ✓
- Control which traffic is sent for Security Inspection on L2-4 ✓
- Flexible Health Probes to detect device failure and allow *the traffic and security to continue* ✓
- No Added L atency ✓

SOLUTION DEEP DIVE – LOW LEVEL

HOW IT WORKS



Traffic load balanced towards from client to NGFW based on Destination IP.
Reply traffic load balanced based on Source IP.
(Sticky Traffic)

Each NGFW created as **itd device-group** based on nodes; mapped by IP address

NGFW Fail-over based on node per-bucket – least utilised other FTD

IP SLA
Health Probes based on ICMP; sent to dummy IP addresses mapped to NGFWs; on ITD

Track interface for reachability

Each device data interface configured on separate vLANs for In and Out traffic; on ITD

Traffic sent to NGFW controlled by Access Control Lists

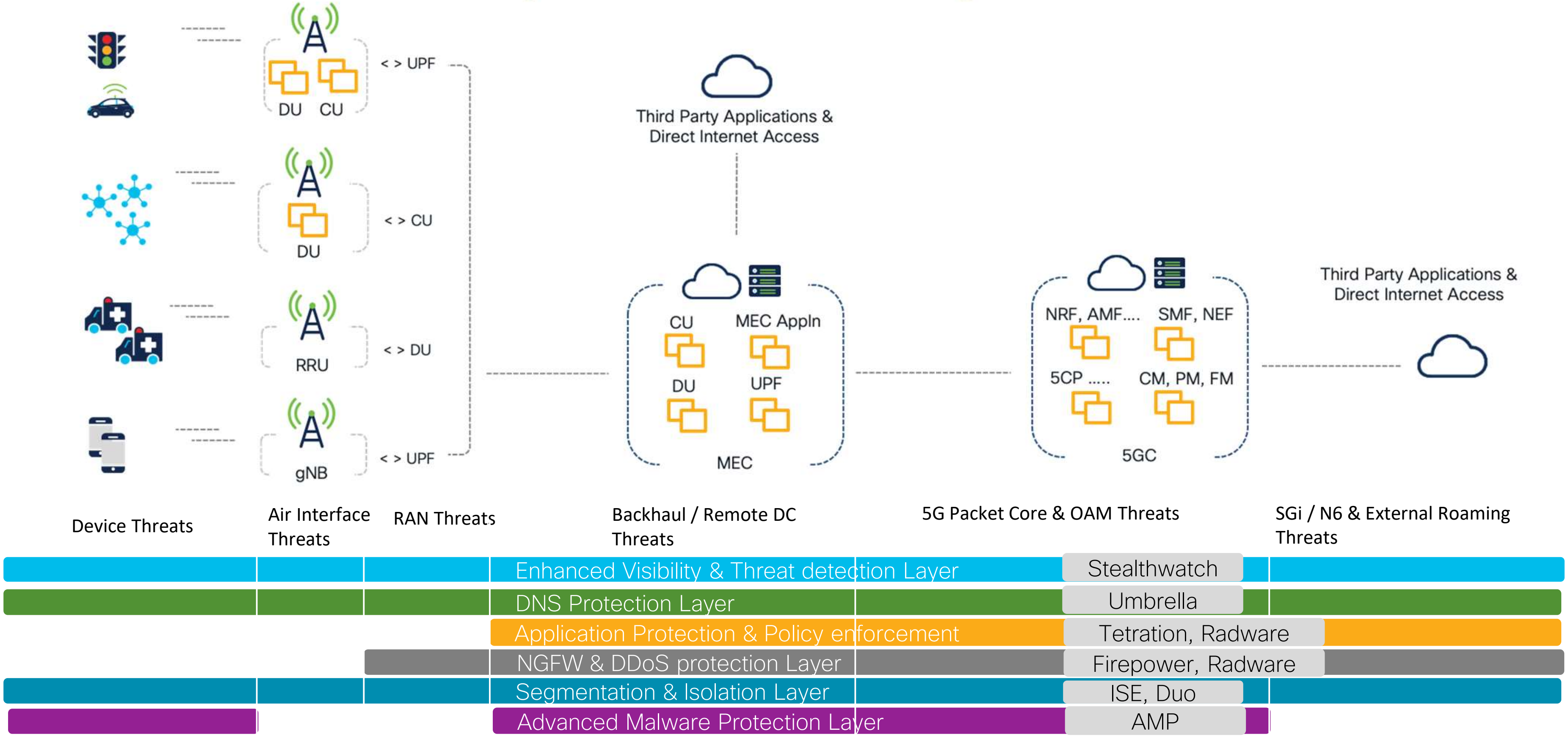
CONCLUSION

- Creates a **Balanced Security and Connectivity**
- The Nexus ITD solution allows the customer's network team to specify which traffic is sent to the NGFW
- Simple integration and supports sticky traffic

THE FUTURE

- Service chain multiple security devices together – SSL Offload -> IPS -> WAF; all aggregated from the Nexus ITD
- Connect passive monitoring tools for enhanced visibility – such as NetFlow
- Support for non-Cisco devices; integrate toolsets from major vendors

End to End Threat Mitigation in 5G & Evolving Networks



DU CU < > UPF

DU < > CU

RRU < > DU

gNB < > UPF

Third Party Applications & Direct Internet Access

CU MEC Appln

DU UPF

MEC

NRF, AMF.... SMF, NEF

5CP ..... CM, PM, FM

5GC

Third Party Applications & Direct Internet Access

Device Threats

Air Interface Threats

RAN Threats

Backhaul / Remote DC Threats

5G Packet Core & OAM Threats

SGi / N6 & External Roaming Threats

Enhanced Visibility & Threat detection Layer — Stealthwatch

DNS Protection Layer — Umbrella

Application Protection & Policy enforcement — Tetration, Radware

NGFW & DDoS protection Layer — Firepower, Radware

Segmentation & Isolation Layer — ISE, Duo

Advanced Malware Protection Layer — AMP

Interesting reads on 5G security..

EU coordinated risk assessment of 5G networks security: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049

5G security blog: https://blogs.cisco.com/sp/5g_secure

Zero Trust 5GC security: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-security-solutions/white-paper-c11-742166.pdf

Innovation in 5G security: https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf

What did I just learn ?

- Different models of deployment will require different security controls

- Integrate full visibility, segmentation and vulnerability detection in all your 5GC workloads

- E2E security of 5G will require multiple layers security controls apart from built-in 3GPP specified security controls

The bridge to possible