Signaling Traffic Management Deep Dive
SIP, Diameter, GTP & DNS

18th May 2016

Peter Nas, Sr Solution Architect Sales

Agenda

Key Service Provider trends

F5's Signaling Strategy for SPs
DNS, GTP, Diameter, SIP

Solutions Can Help

IMS-VoLTE Security

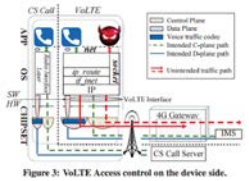
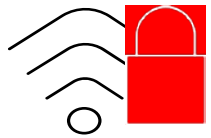


Figure 3: VoLTE Access control on the device side.

VoWifi Security



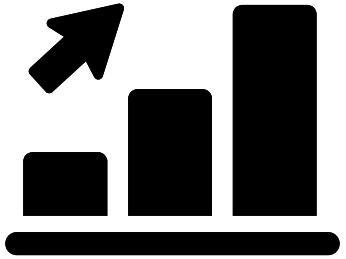
Signaling Security

Broad Market Trends

Devices & Connections

Smartphones, Applications, Internet of Things

- *Scale and performance*
- *IPv4→IPv6 transitions*
- *DDoS mitigation*



Exponential Growth

Of Data and Signaling Traffic

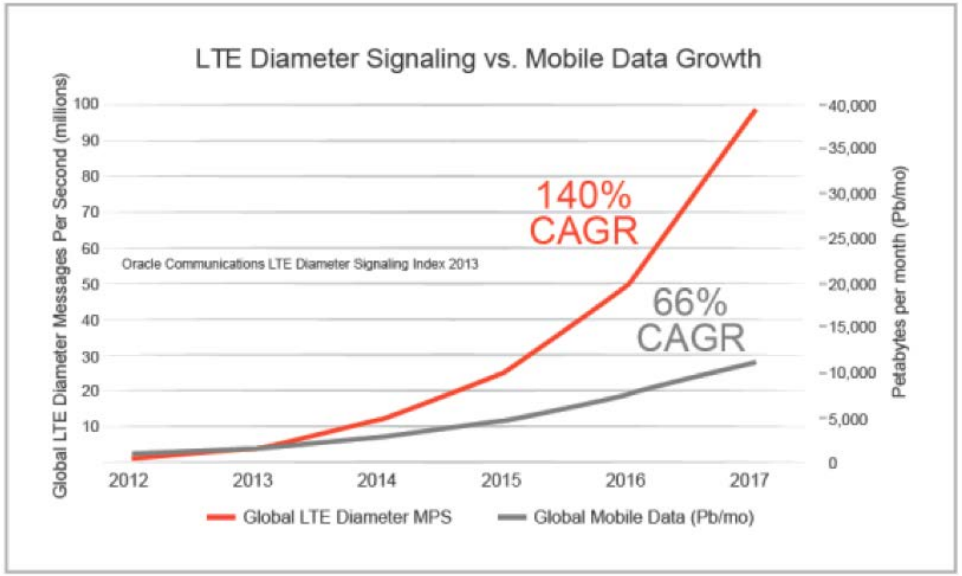
- *Scale and performance*
- *Control plane and data plane*
- *Signaling overload protection*

Increasing Security

Evolving and Increasing Threats and Attacks

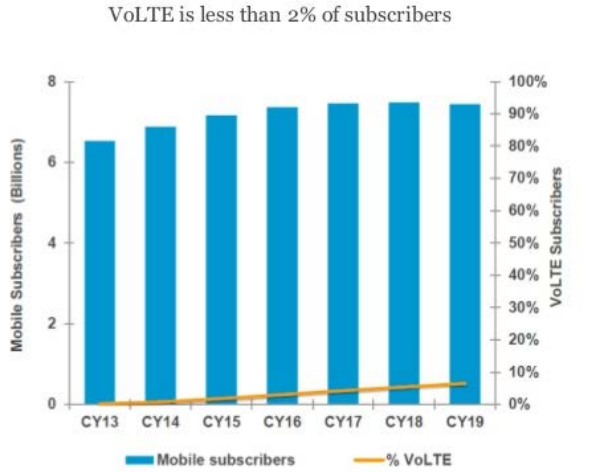
- *Scale and performance*
- *L4-L7 security*
- *Programmability and flexibility*

Signaling trends



VoLTE: Very Early Days

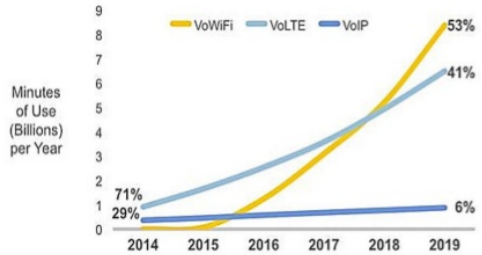
- 25 operators have launched commercially in some capacity across 16 countries
- VoLTE by itself is purely a technology migration
- 200+ VoLTE capable devices announced



Saghaeian [at] gmail.com

VoWi-Fi Market Scenario and Forecast

VoWi-Fi is going to surpass VoLTE by 2018 in terms of minutes of use

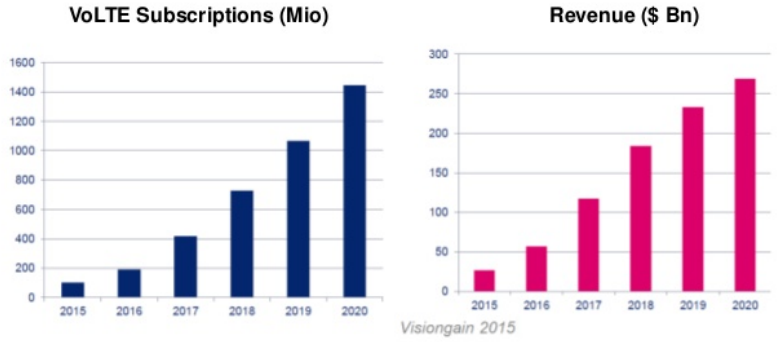


VoWi-Fi extends the coverage of MNOs offering an **cost-effective**, **scalable**, **high-quality** approach whereas cellular coverage might be sketchy

But VoWiFi also can help to win the battle against the erosion of revenue from over-the-top providers' (OTTPs') VoIP offers

Saghaeian [at] gmail.com

VoLTE Forecast 2015 - 2020



In 2020:

- VoLTE subscription more than 1.4 Bn
- VoLTE revenue going beyond $260 Bn

Saghaeian [at] gmail.com

Challenges Ahead For Service Providers

SCALING the Networks … End to End SECURITY … PROFITABLE New Services

- **SCALING** networks
- End-to-End **SECURITY**
- **PROFITABLE** new services

Connected Cars

Connected Homes

Connected Cities

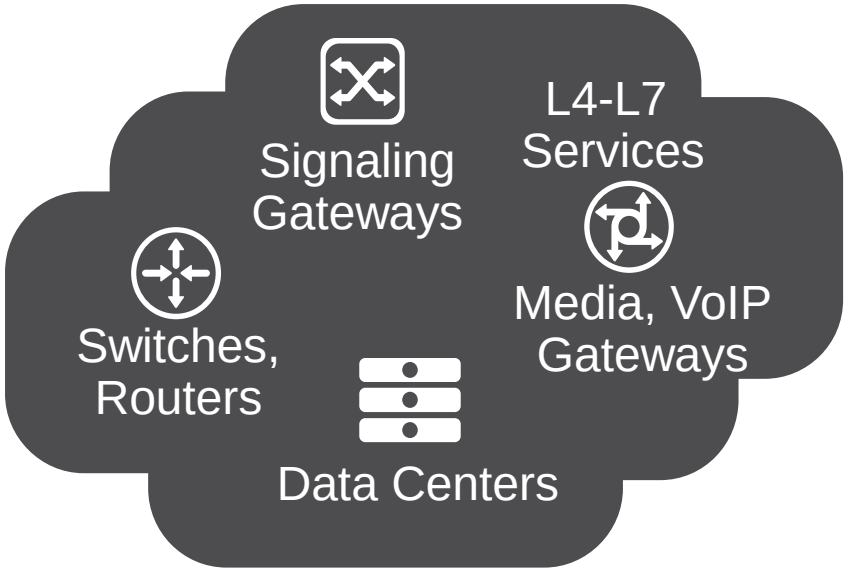
Wearables and Utilities

Surge in SP Network Access

Spikes in Application Usage

Increasing Connection Rates

50B Connected Devices Worldwide by 2020



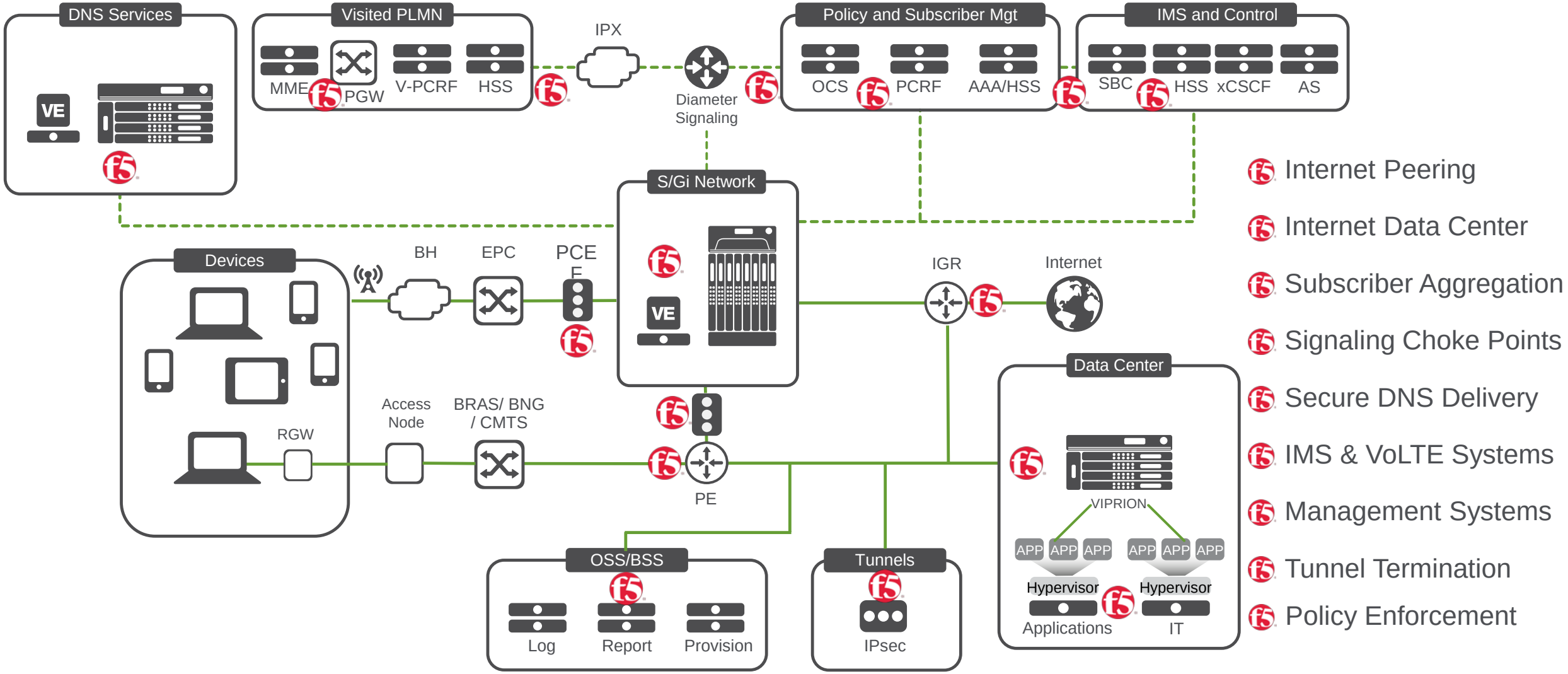
Service Provider Core Networks

Service Provider Challenges

- Network Signaling Spikes
- Diameter Signaling Storms
- Surge in DNS Queries
- IPv6 Addressing Requirements
- New DDoS Attack Vectors
- DNS Security Vulnerabilities
- Squeeze in Profit Margins
- New Service Delivery Models

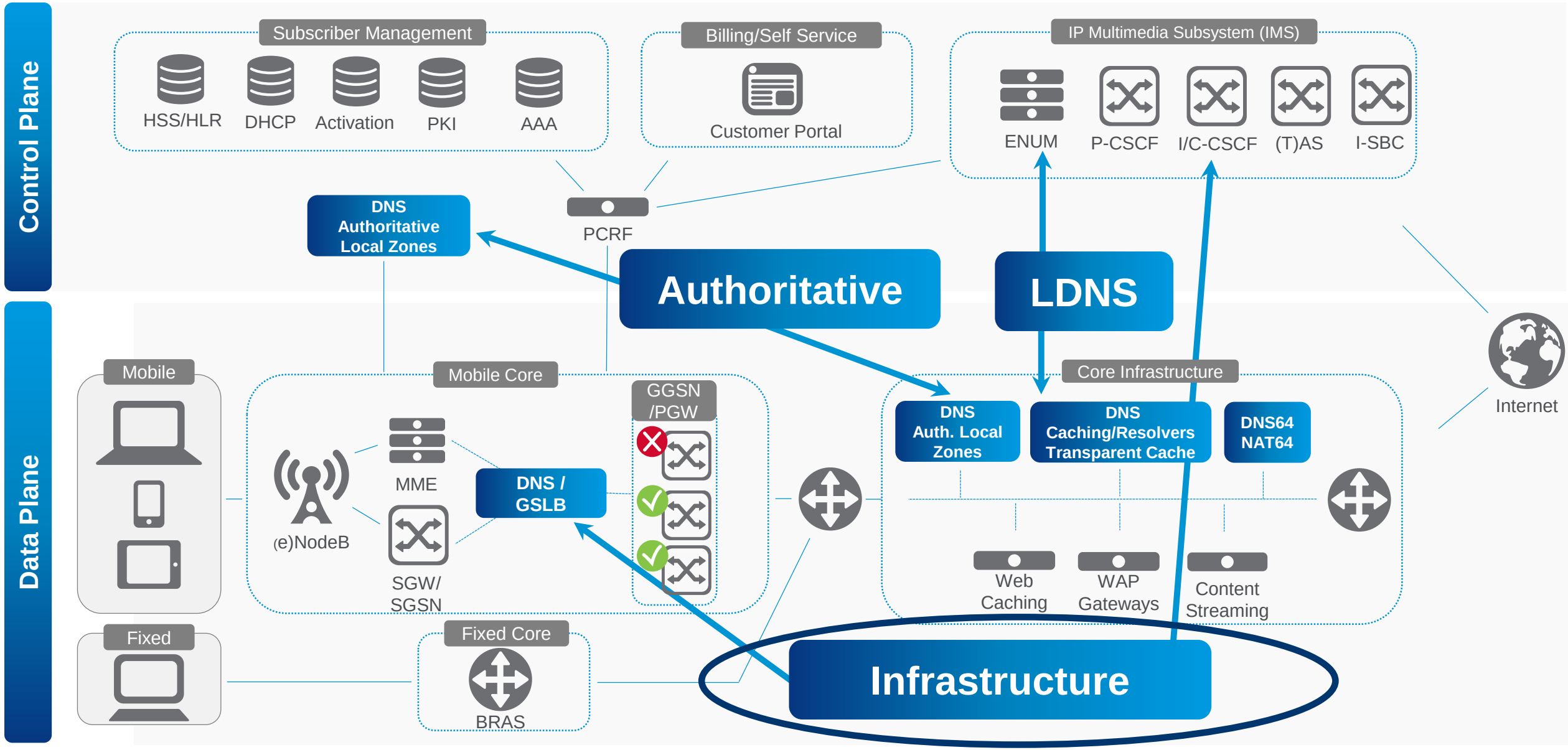
Solutions Can Help

F5 Deployment Footprints



DNS

Simplified and Consolidated DNS



DNS and DNS security extensively addressed in other session, here focus on Infrastructure

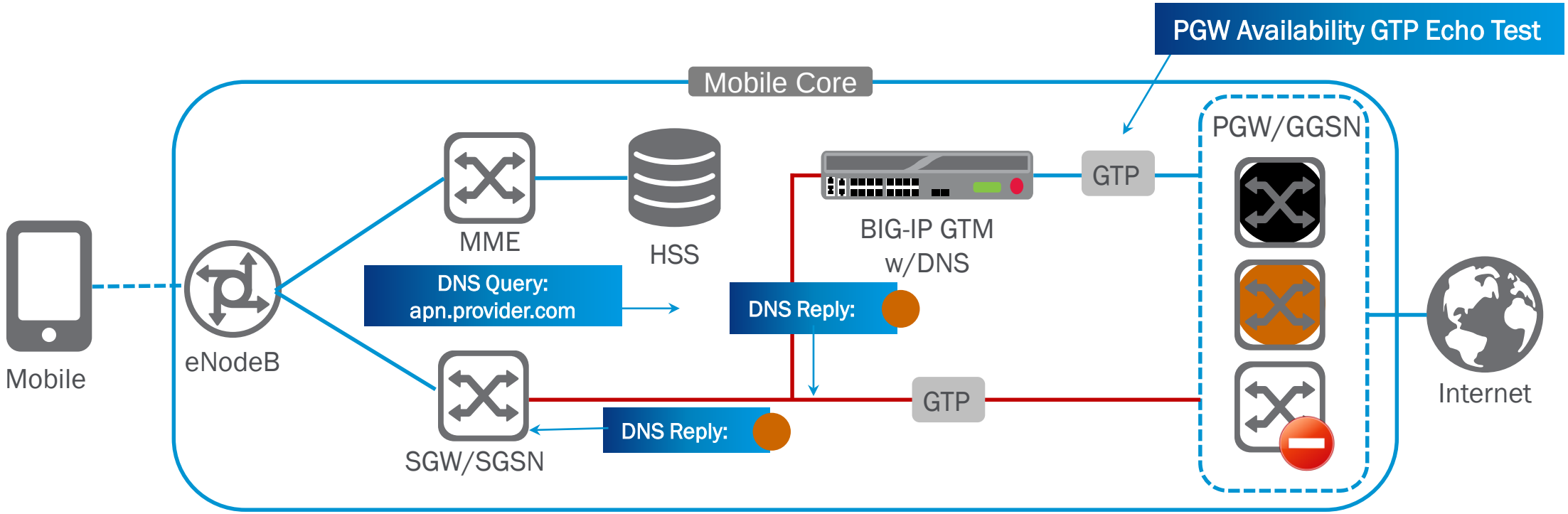
Infrastructure: Automatically Monitor Packet Gateways For Availability

Problem: Manually Remove Packet Gateways

- Many SPs don't monitor the PGW/GGSN from DNS
- SGSN/MME selects an APN by DNS lookup (apn.provider.com)
- DNS responds with the available PGW/GGSN
- Manually remove PGW from record list given to mobile unit

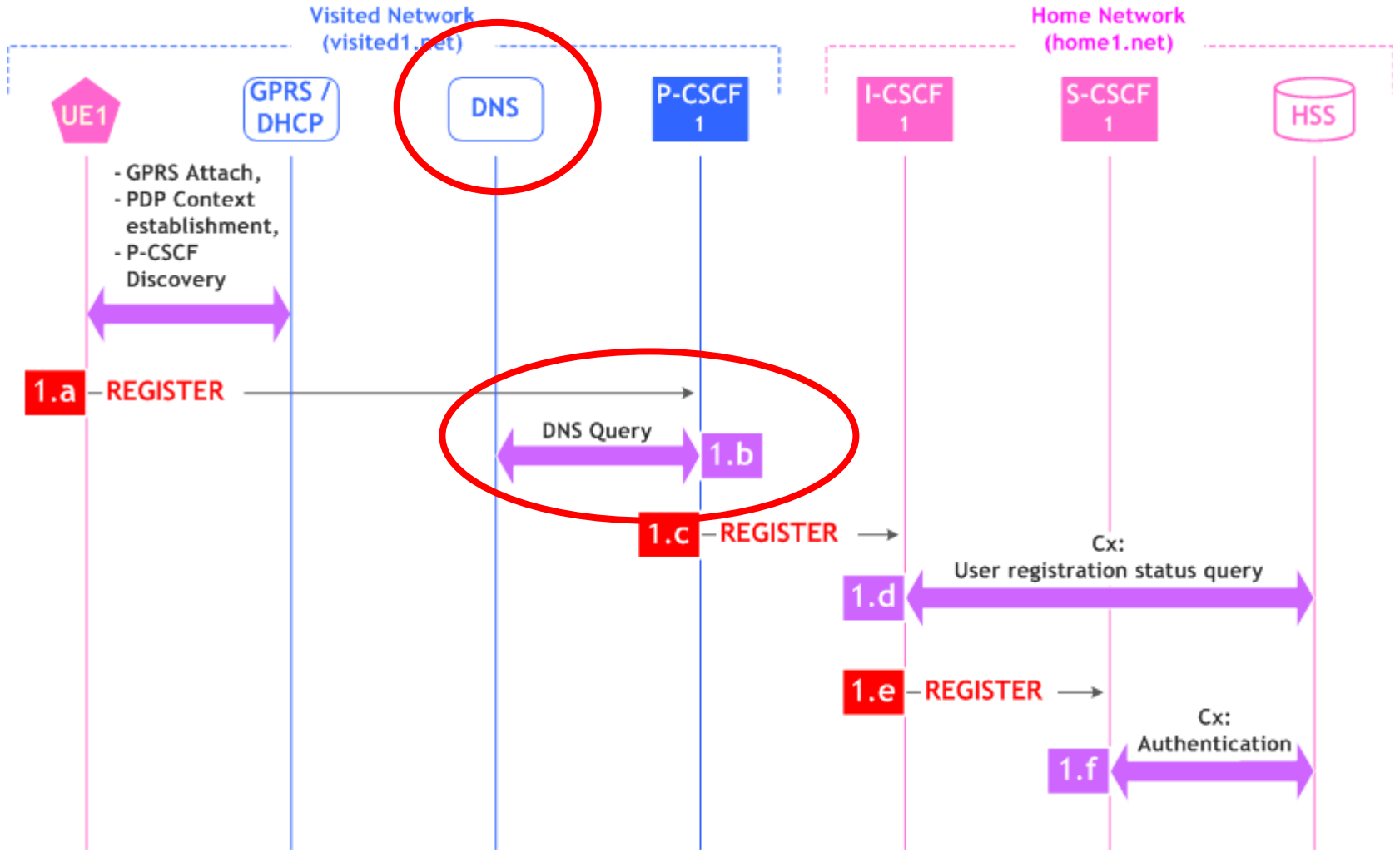
Solution: Automatically Monitor, Remove and Reload

- Higher availability of services
- Closer mapping of network capacity to required load
- Reduced overhead through overprovisioning
- Allows for capacity to be added or removed automatically



Note: BIG-IP supports A records (common for 3G) but also SRV and NAPTR (common for 4G and IMS)

IMS: REGISTER request uses DNS

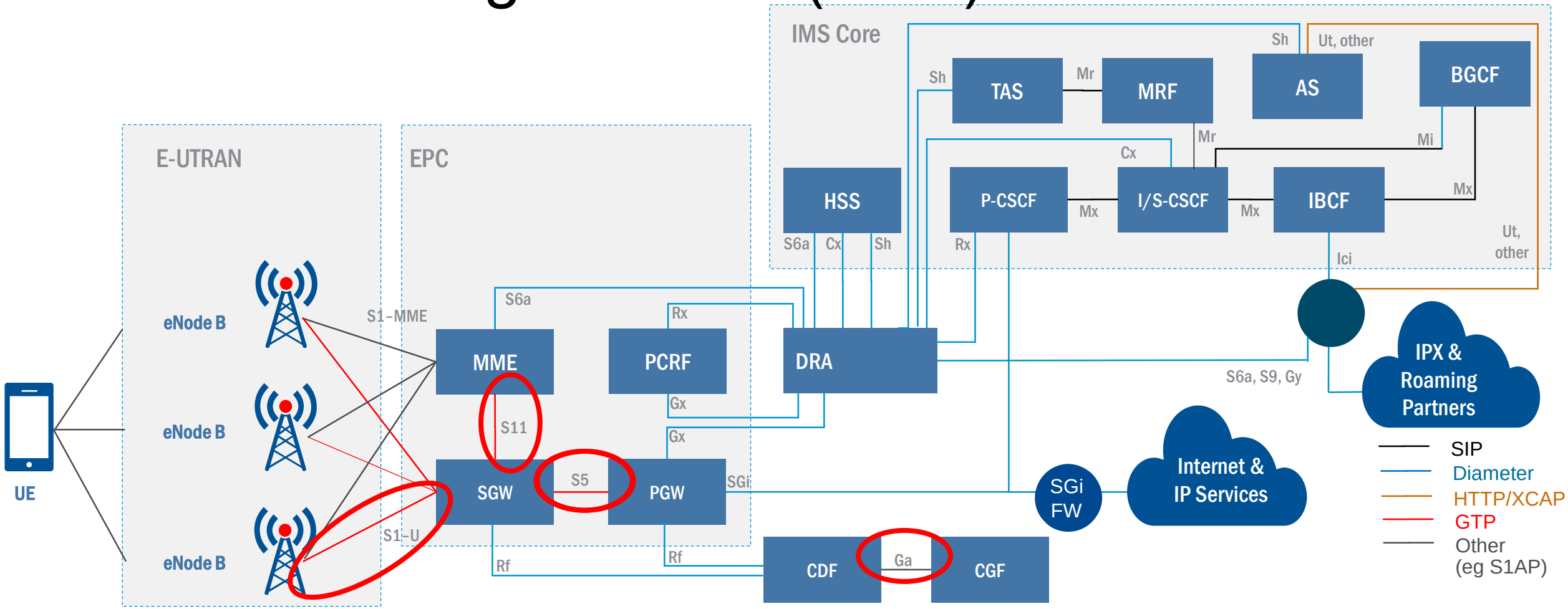


UE1 is located in a visited network, and determines the P-CSCF via the CSCF discovery procedure

IMS = IP Multimedia System

GTP Traffic Management & Security

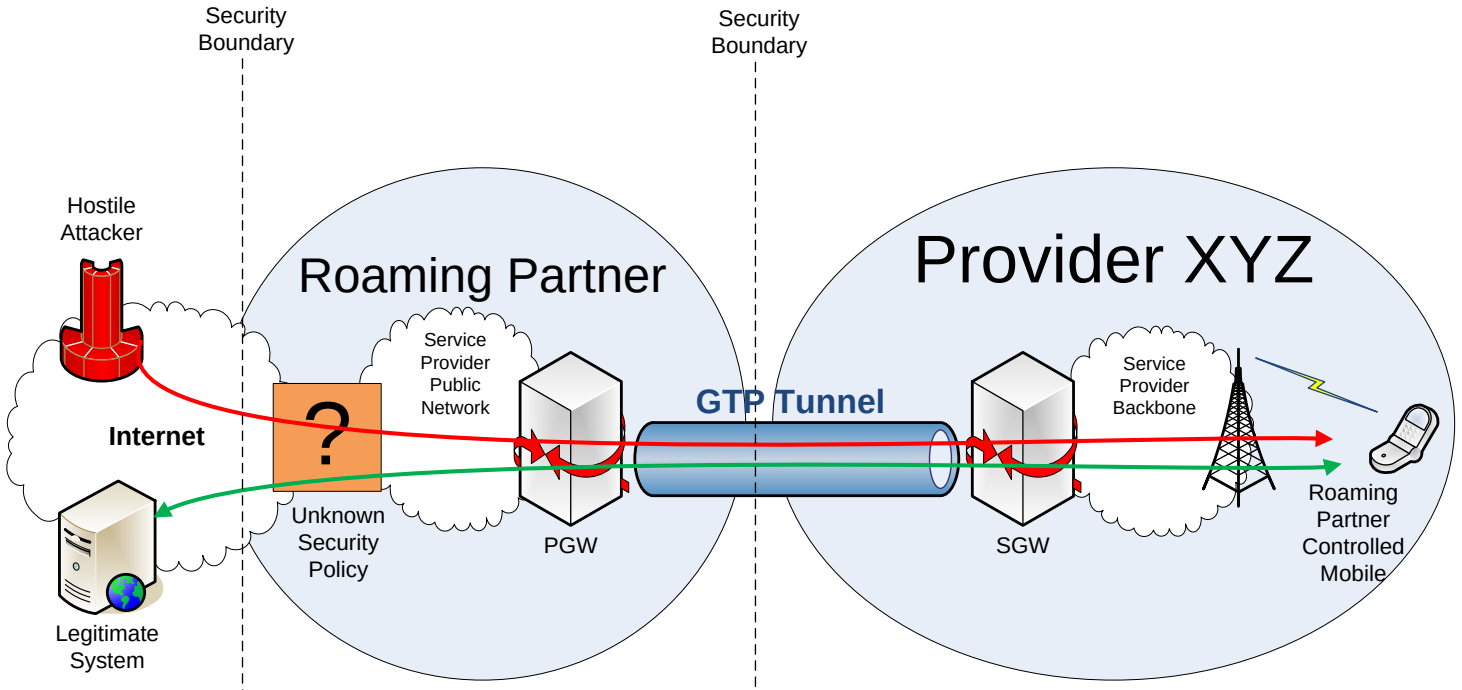
GPRS Tunneling Protocol (GTP)

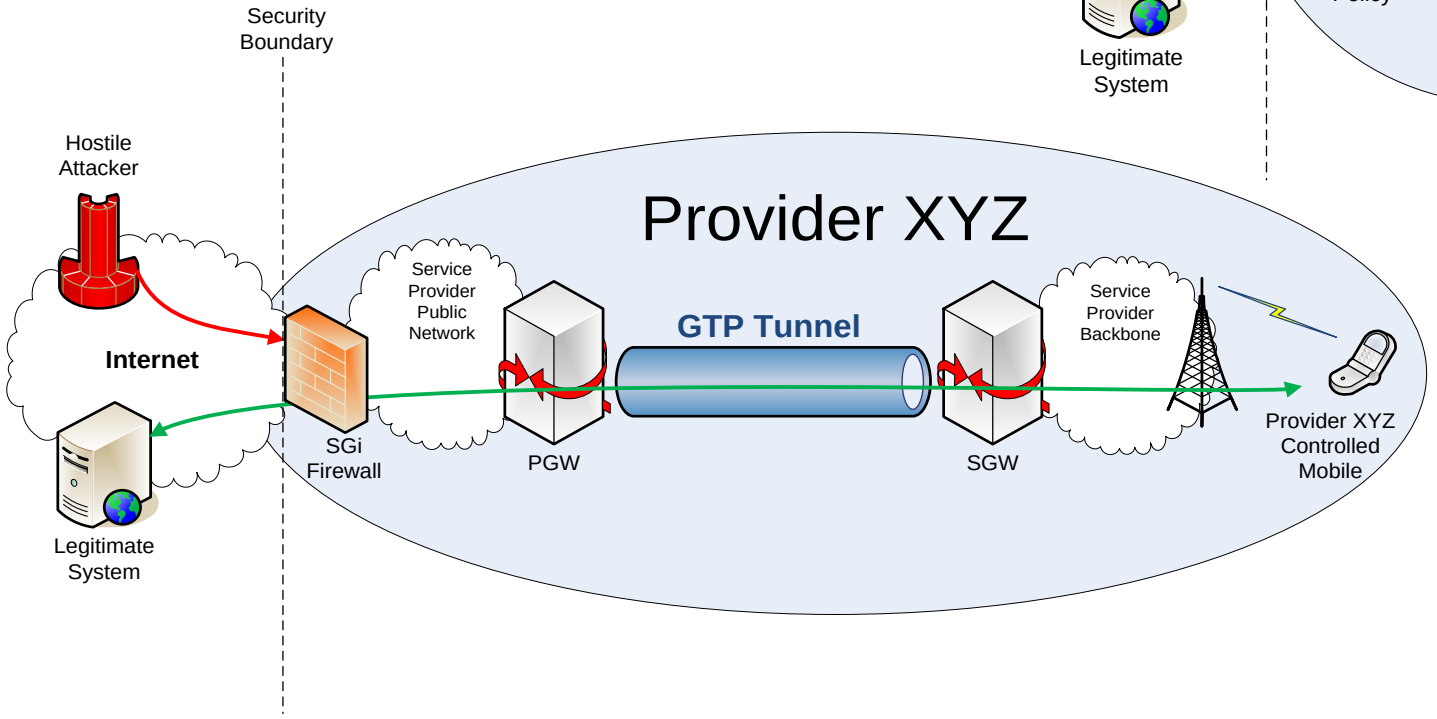


Protocol	Transport	LTE Interfaces	Notes
GTPv2-C (Control)	2123/UDP	S11: MME-SGW, S5: SGW-PGW	Signaling to create/maintain/delete tunnels
GTP-U (User Data)	2152/UDP	S1-U: eNodeB-SGW, S5: SGW-PGW	Tunneling for customer data packets
GTP' (Prime)	3386/(TCP||UDP)	Ga: CDF-CGF (Optional)	Transport CDRs from Charging Data Function (CDF) to Charging Gateway Function (CGF)

Roaming Security

Without Roaming, the Provider controls 100% of the network architecture, security controls, performance & customer experience.





With Roaming, the Provider loses control of security and sees just tunneled data. Traffic to/from roaming devices can impact network performance.

GTP Firewall: Limit APNs, Block Ports & IP Blacklisting

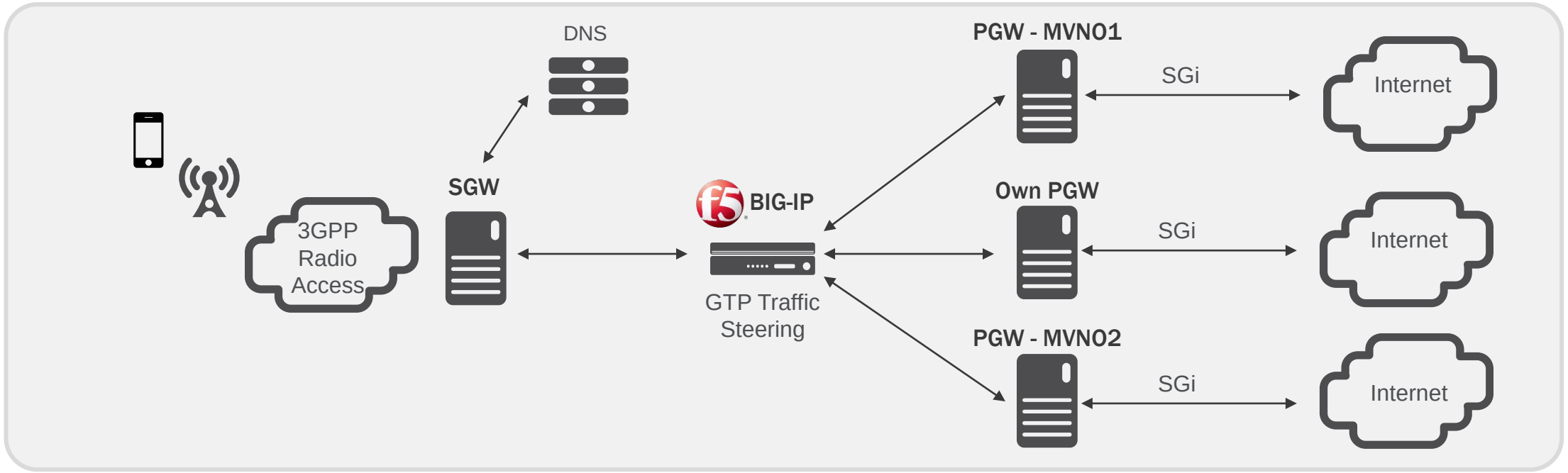
Search

				Source			Destination					
Rule List	Description	State	Schedule	Address/Region	Port	VLAN / Tunnel	Address/Region	Port	Protocol	iRule	Action	Logging
Roaming_Partner_1		Enabled										
Inbound_GTPv2-C		Enabled		Roaming_Partner_1_SGWs	Any	IPX	Provider_PGWs	GTPv2-C_2123	17 (UDP)	Roaming_Partner_1_APNs	Accept Decisively	Enabled
Inbound_GTP-U		Enabled		Roaming_Partner_1_SGWs	Any	IPX	Provider_PGWs	GTP-U_2152	17 (UDP)	Roaming_Blocked_Ports	Accept Decisively	Enabled
Inbound_ICMP		Enabled		Roaming_Partner_1_SGWs	Any	IPX	Provider_PGWs	Any	1 (ICMP)		Accept Decisively	Enabled
Outbound_ICMP		Enabled		Provider_PGWs	Any	Core	Roaming_Partner_1_SGWs	Any	1 (ICMP)		Accept Decisively	Enabled
Roaming_Partner_2		Enabled										
Inbound_GTPv2-C		Enabled		Roaming_Partner_2_SGWs	Any	IPX	Provider_PGWs	GTPv2-C_2123	17 (UDP)	Roaming_Partner_2_APNs	Accept Decisively	Enabled
Inbound_GTP-U		Enabled		Roaming_Partner_2_SGWs	Any	IPX	Provider_PGWs	GTP-U_2152	17 (UDP)	Roaming_IP_Blacklist	Accept Decisively	Enabled
Inbound_ICMP		Enabled		Roaming_Partner_2_SGWs	Any	IPX	Provider_PGWs	Any	1 (ICMP)		Accept Decisively	Enabled
Outbound_ICMP		Enabled		Provider_PGWs	Any	Core	Roaming_Partner_2_SGWs	Any	1 (ICMP)		Accept Decisively	Enabled
Roaming_Partner_3		Enabled										
Inbound_GTPv2-C		Enabled		Roaming_Partner_3_SGWs	Any	IPX	Provider_PGWs	GTPv2-C_2123	17 (UDP)	Roaming_Partner_3_APNs	Accept Decisively	Enabled
Inbound_GTP-U		Enabled		Roaming_Partner_3_SGWs	Any	IPX	Provider_PGWs	GTP-U_2152	17 (UDP)	Roaming_IP_Blacklist	Accept Decisively	Enabled
Inbound_ICMP		Enabled		Roaming_Partner_3_SGWs	Any	IPX	Provider_PGWs	Any	1 (ICMP)		Accept Decisively	Enabled
Outbound_ICMP		Enabled		Provider_PGWs	Any	Core	Roaming_Partner_3_SGWs	Any	1 (ICMP)		Accept Decisively	Enabled
		Enabled		Any	Any	Any	Any	Any	Any		Drop	Enabled

- APN Limiting for Create Session Requests
- Throttling per user or per roaming partner
- IP Blacklisting of Tunneled Packets
- Port Blocking of Tunneled Packets

- We can also screen on messages valid for a specifc interface, like okay for S5 but not for S8 (as per list from GSMA)
- If APN does not provide enough info look into GTP traffic for MSISDN and select the right PGW for per MVNO traffic steering

GTP Traffic Management – Case Study

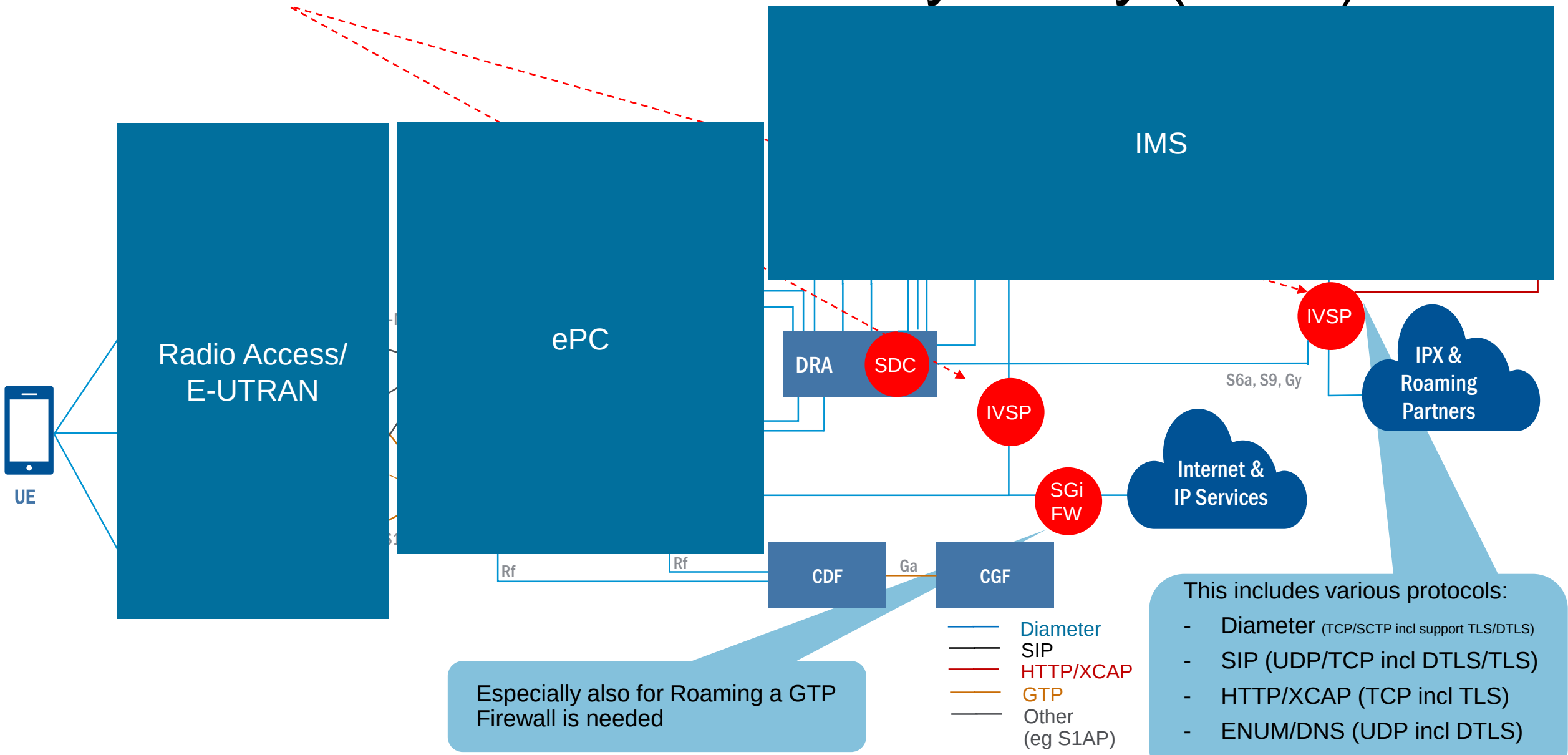


- Problem Statement
  - Same APN id used for home network and MVNOs
  - But want to use dedicated PGW per MVNO
  - Result: DNS-based APN resolution procedure to find the proper PGW will not work
- Solution
  - APN-based DNS resolution points to F5 BIG-IP
  - F5 BIG-IP is provisioned with a table mapping MS-ISDN ranges to the corresponding MVNO PGW
  - F5 BIG-IP steers incoming GTP-C messages to the right PGW based on MS-ISDN ranges (by inspecting GTP-C IE attributes)

IMS-VoLTE Security

like SIP, XCAP & RTP

Our vision: IMS/VoLTE Security Proxy (IVSP)

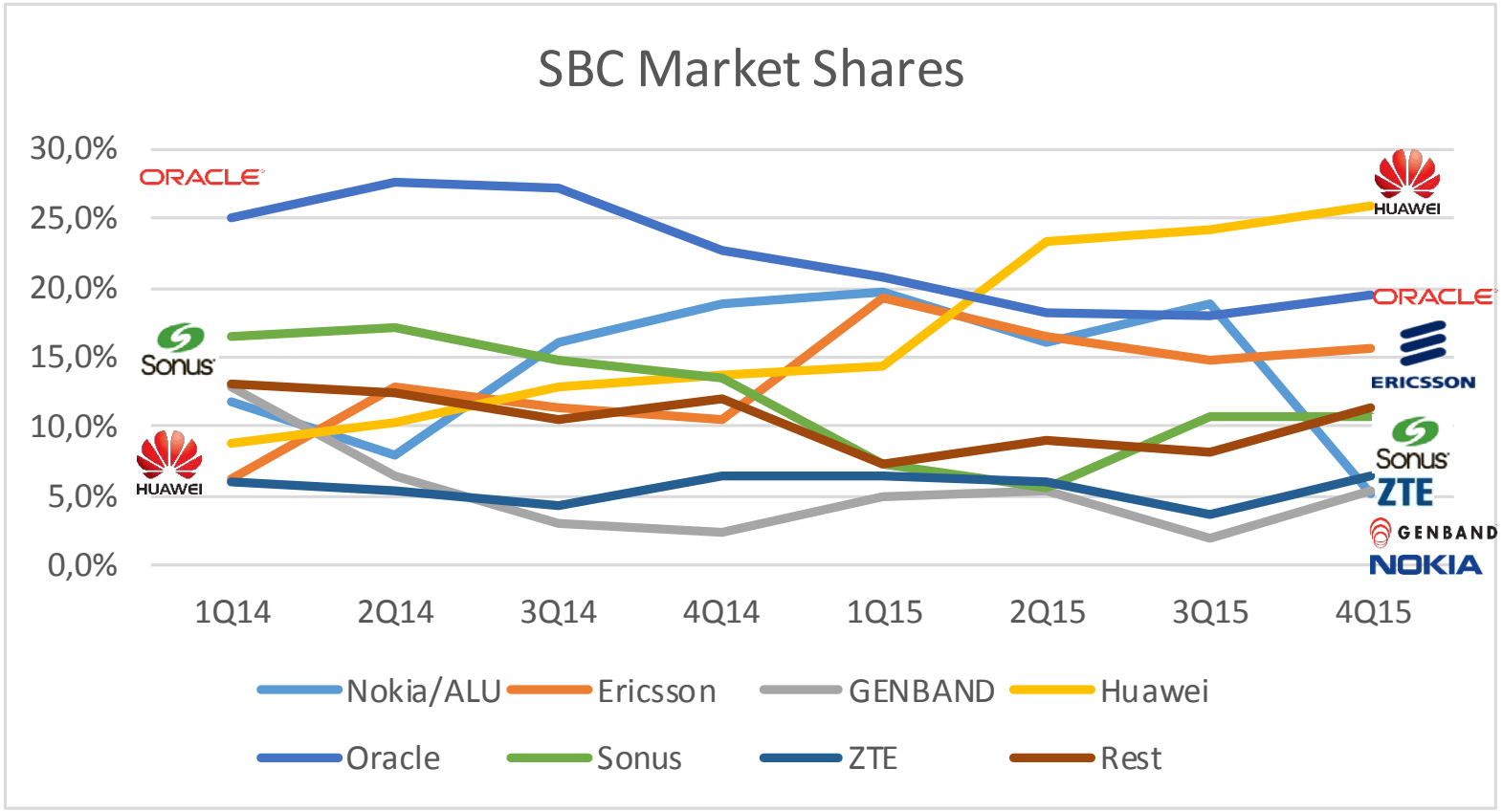


SBC Market Shares .... many ongoing changes

2014 Market leaders down
- Oracle, Sonus, Genband

2015/16 Leaders: NEPs
- Huawei, Ericsson, Nokia
- Very volatile (see Nokia)

SBCs need:
- Load Balancing / scaling
- SIP normalization
- Security
- More..



Source: Infonetics (paid service)

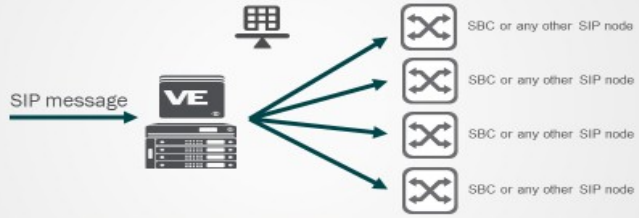
SIP signaling and F5

Our strength

What can we do TODAY with BIGIP in the SIP area...

© F5 Networks, Inc CONFIDENTIAL 20

SIP Load Balancing & SIP Routing

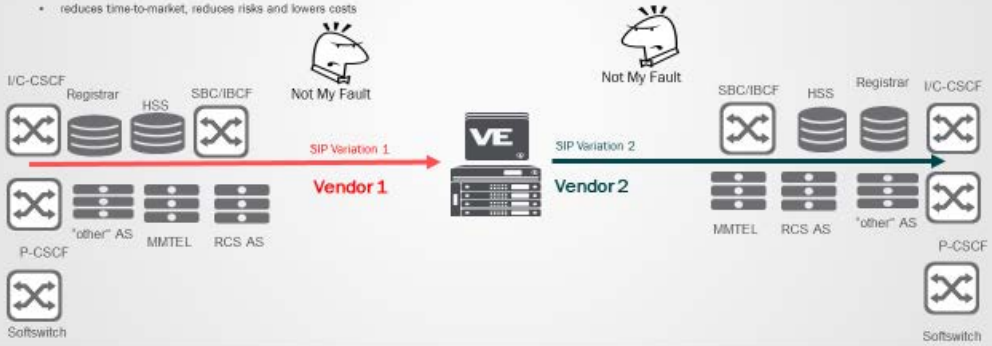


- Many LB algorithms can be applied
- SIP Routing functionalities

© F5 Networks, Inc. 15

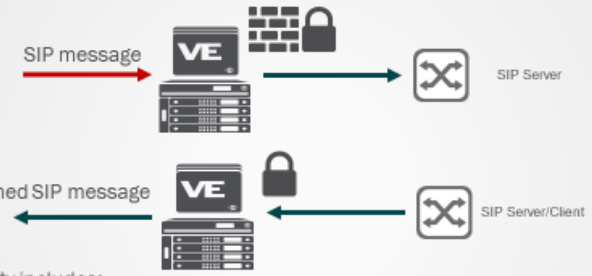
Use Case: SIP Normalization

- Problem: many different flavors of the same SIP interfaces, especially for new nodes like for IMS there will be many initial issues to connect various vendors
- Solution: Use BIGIP and F5's long experience on SIP mediation
  - Use F5's flexibility and experience
  - It is not "just" a flexible engine to modify SIP messages it also how to use it
  - reduces time-to-market, reduces risks and lowers costs



© F5 Networks, Inc. 22

SIP Security



SIP security includes:

- Screening, policing
- Access Control, WL/BL based on any content
- DDoS prevention
- Topology hiding
- more

© F5 Networks, Inc. 23

VoLTE: What are the Actual Vulnerabilities?

Attackers can…

- Gain **free data access** (VoLTE control plan not billed)
- **Shut down** existing access
- **Subdue** an ongoing call

Problems on both device & network

- Device: OS fails to limit access to VoLTE data plane
- Network: Infrastructure lacks proper controls (F5 can help here)

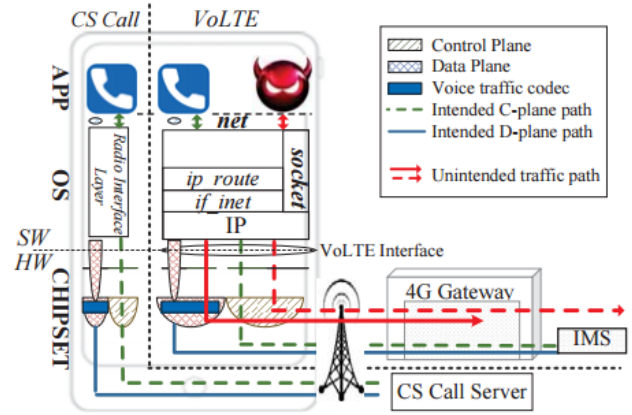


Figure 3: VoLTE Access control on the device side.

Sources: http://web.cs.ucla.edu/~ghtu/ccs15.pdf

http://www.kb.cert.org/vuls/id/943167

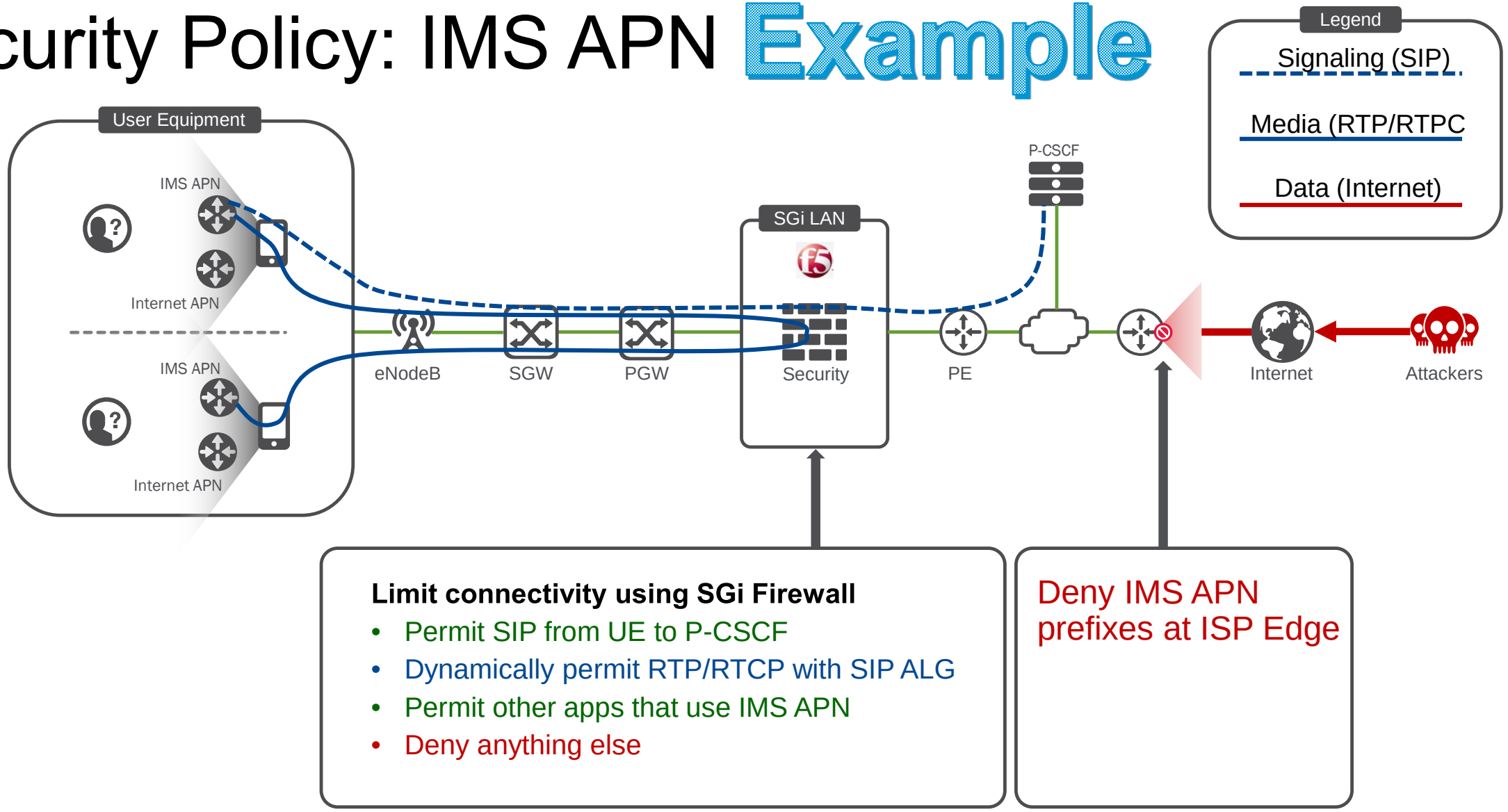
Category	Attack	Victim	Description and Threat	Vulnerability
Data (§3)	Free data	Operator	Adversary device gains free data access to the Internet or another mobile device.	V1: Lack of the control-plane access control (§3.1) V2: Imprudent forwarding in the network (§3.1) V3: Abusing no billing of VoLTE signaling traffic (§3.2)
	Overbilling	Individual	Adversary injects spams to impose excessive data bill on the victim.	
	Preemptive data	Operator, Individual	Adversary device gains undeserved higher-priority data access.	V1: Lack of the control-plane access control (§3.1) V4: Abusing highest-priority allocated to VoLTE control plane (§3.3)
	Data DoS	Individual	Adversary shuts down the ongoing data access on the victim phone.	
Voice (§4)	Muted voice (DoS)	Individual	Adversary mutes an ongoing VoLTE call on the victim.	V5: Insufficient data-plane access control (§4.1) V6: Side-channel leakage of data-plane information (§4.1)
	Enhanced muted voice	Individual	Adversary mutes the voice faster.	V5: Insufficient data-plane access control (§4.1) V7: Leakage from improper both-plane coordination (§4.2)

Table 1: Summary of our main findings on VoLTE vulnerabilities and proof-of-concept attacks.

SIP ALG

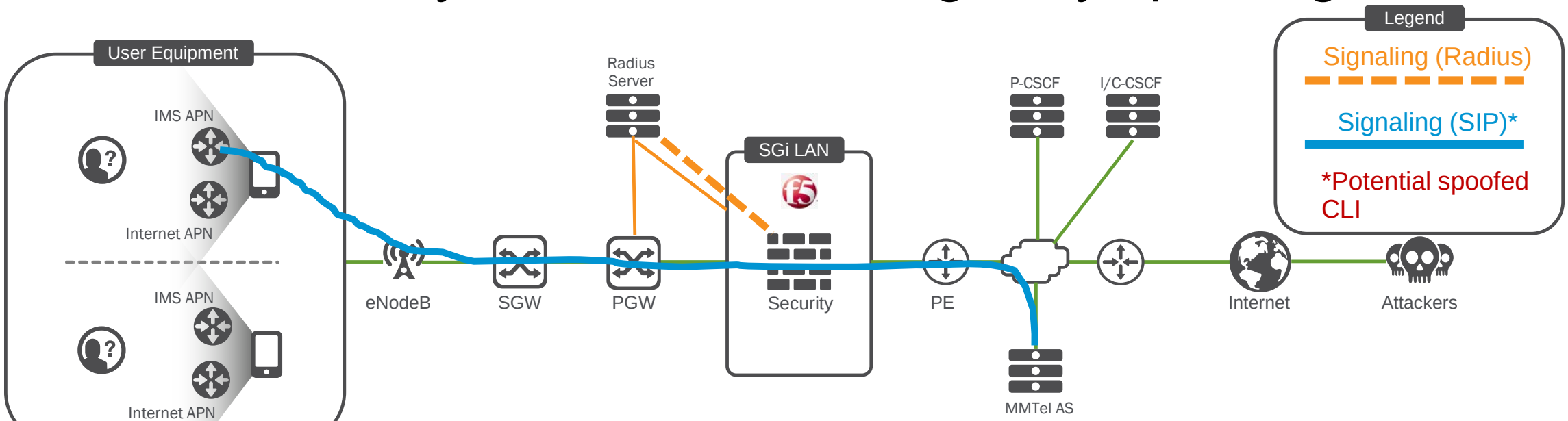
iRules…

Security Policy: IMS APN Example



Example

IMS & VoLTE Security Threat: SIP CallingParty spoofing



Same for XCAP

Symptom = UE inserts spoofed CallingPartyNumber in SIP invite

note that LTE Signaling bearer is validated based on MSISDN and IMSI

but if CLI in SIP invite ≠ validated MSISDN the issue arises

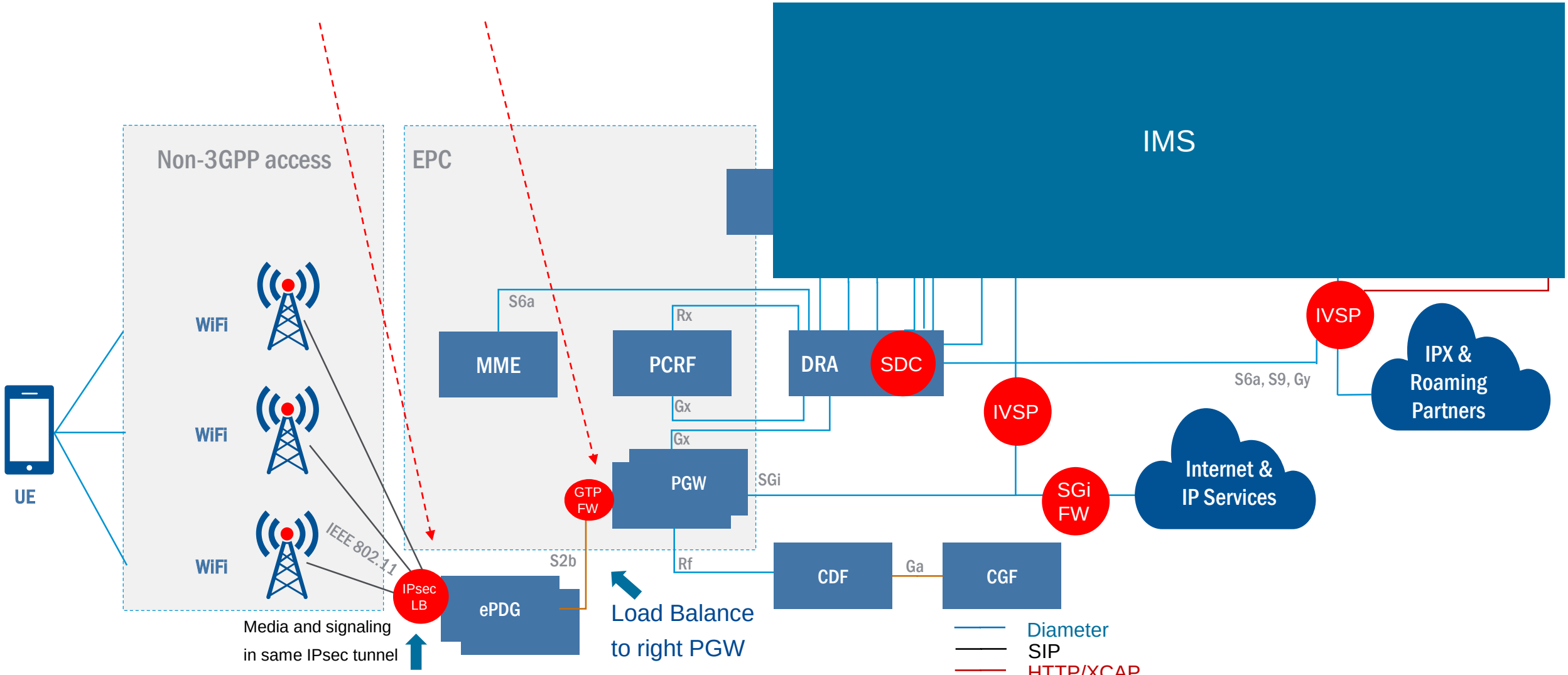
Impact = Free calling, occur costs for authenticated user

Cause = no cross check between LTE bearer and used CLI in SIP

Remedy = multi-layer check* by comparing SIP with Radius for CLI

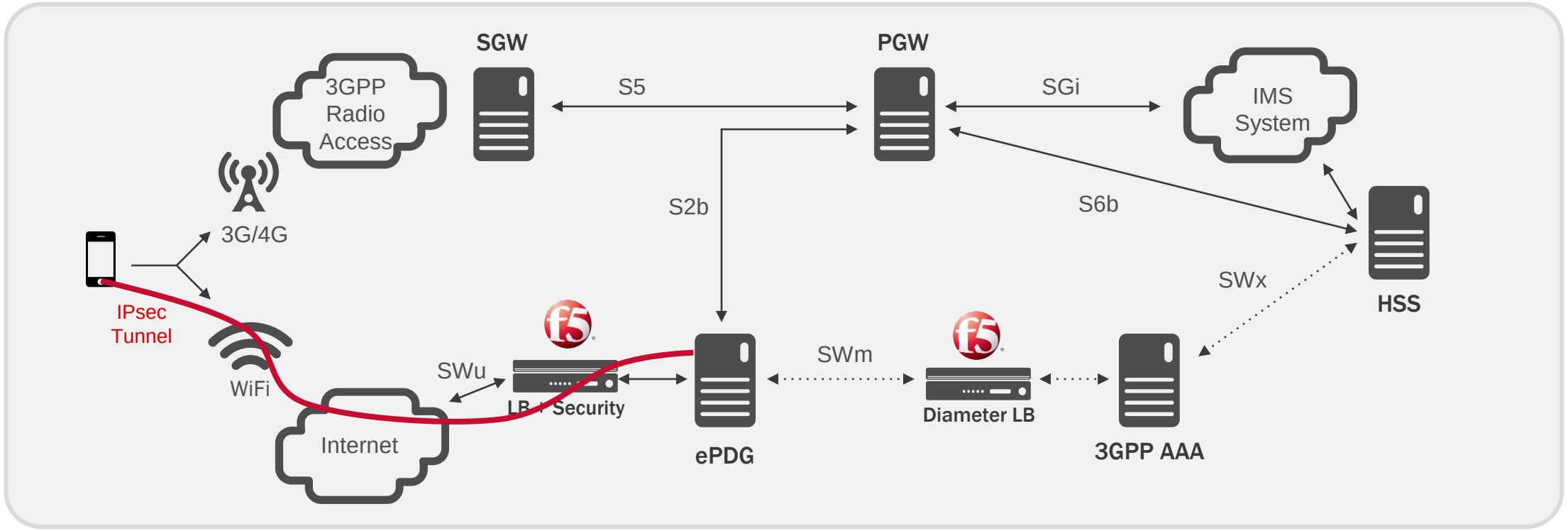
Secured (Vo)Wifi-access

Secure WiFi access



- IPsec LB
- Check IP source address to authorize access or not
- DNS based LB to ePDG
- IP reputation (avoid proxy, B/W addresses, etc.)

Voice over Wifi (VoWifi) – Load Balancing + Security



- Load Balancing ePDG
  - Geo-redundancy : GTM (DNS)
  - Local LB : LTM
- Securing ePDG
  - Geo-location DB + whitelist
    - Generate extra revenues
  - Only allow IPsec
  - IP intelligence (bots, proxies)
  - DDOS mitigation
- Load Balancing 3GPP AAA
  - Diameter/SCTP
- Securing Diameter SWm
  - Check on ‘bad behavior’

(Vo)Wifi security, what value can F5 add?

IPsec LB (note that we don't terminate the IPsec tunnel)
- Persistence key is source IP

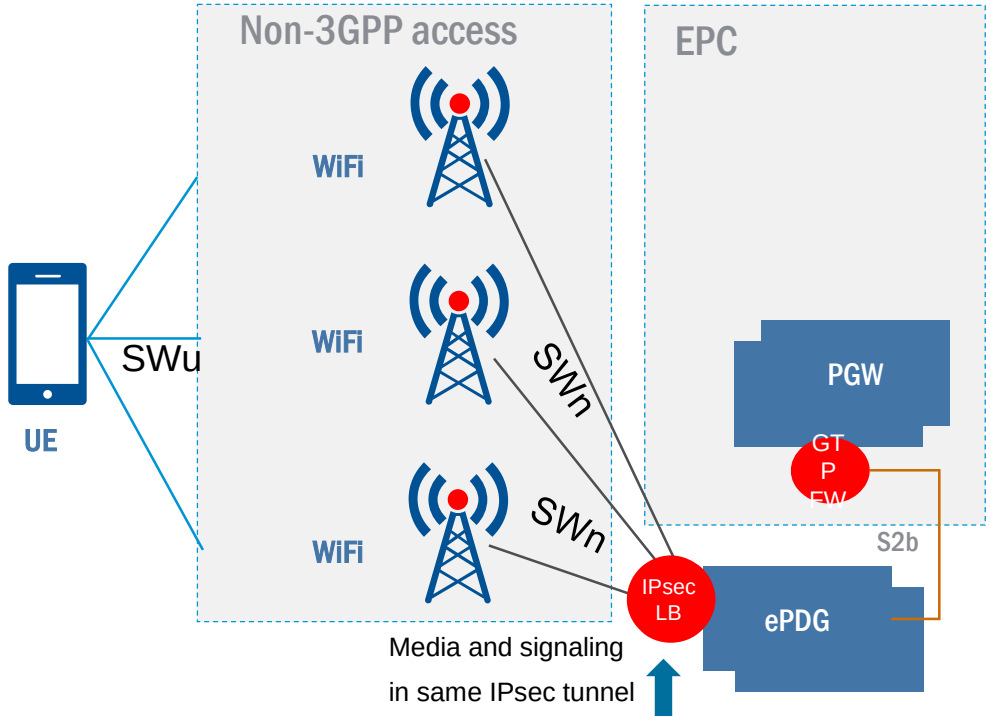
DNS based LB to ePDG
- Use GTP monitor to check loading of ePDG
- Also DNS based LB to PGW

Check IP source address to authorize access or not
- Like is IP from same country
- Is IP from valid 3rd party (McDonalds, Hotel, etc.)
  extra business benefit to include contracted companies IPs
- Optional: maximize #simultaneous calls for one UE/IP

IP-Intelligence, like
- avoid proxy while roaming (eg to pretend to be in country)
- Black/White Listing IPs

Avoid ePDG gets overloaded by unauthorized access attempts, eg roaming customers trying to access ePDG

Note that we can also load balance the Diameter SWm signaling towards the HSS/AAA and apply extra security



ePDG=evolved Packet Data Gateway (PGW)

Summary

Signaling security

Key mobile core signaling protocols

- Diameter security, increasing need for Firewalls
  - IPsec, (D)TLS, topology hiding, ACLs, DDoS prevention, etc.
  - Roaming and interconnect, MVNOs, OTTs
- SIP security, like for VoLTE Interconnect
- SS7 Security*, first FWs being implemented
- DNS security
- GTP, need for GTP firewall
- HTTP, Rest API for OTT access
- Secured VoWifi access

F5 combines all the above and utilizes years of signaling experience, scaling IP and application awareness

* With partner

SOLUTIONS FOR AN APPLICATION WORLD