Securing the backhaul

Huawei Network Conference,
Beijing, 26th May 2014

Andrew Davies, IP Architect
Telefónica UK
CCIE 4962

BE MORE_

Learning to love the LTE Security Gateway

My background

- Data (IP) Networking
- Telefónica UK; Mobile Operator, Fixed Broadband and Corporate Services
- I was lead for LTE IP Architecture and Design culminating in successful LTE launch August 2013.
- I had been learning to love the LTE Security Gateway for about eighteen months

About O2

- O2 is the commercial brand of Telefónica UK Limited and is a leading digital communications company with the highest customer satisfaction for any mobile provider according to Ofcom.

- With over 23 million customers, O2 runs 2G, 3G and 4G networks across the UK as well as operating O2 Wifi and owning half of Tesco Mobile.

- O2 has over 450 retail stores and sponsors The O2, O2 Academy venues and the England rugby team. Read more about O2 at www.o2.co.uk/news.

CONTENTS

01 The Requirement

02 The solution, PKI and IPSec, Firewalling

03 MTU

04 Auto-Integration

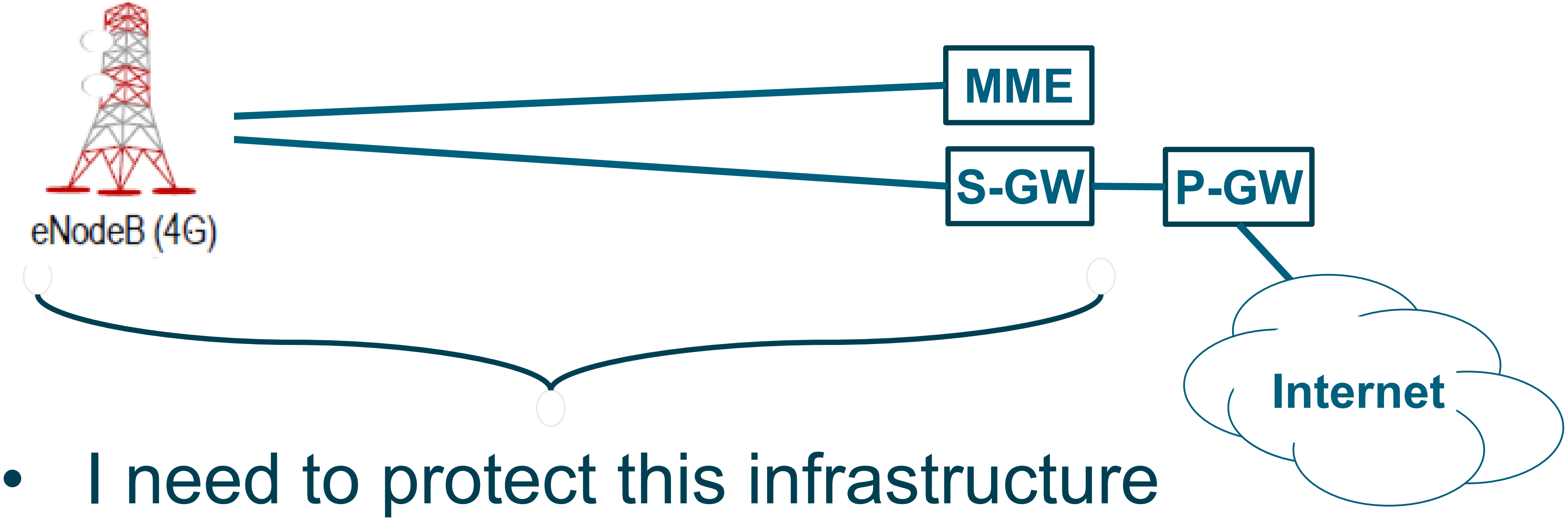
05 Geo-Resilience

06 LTE - Advanced

01

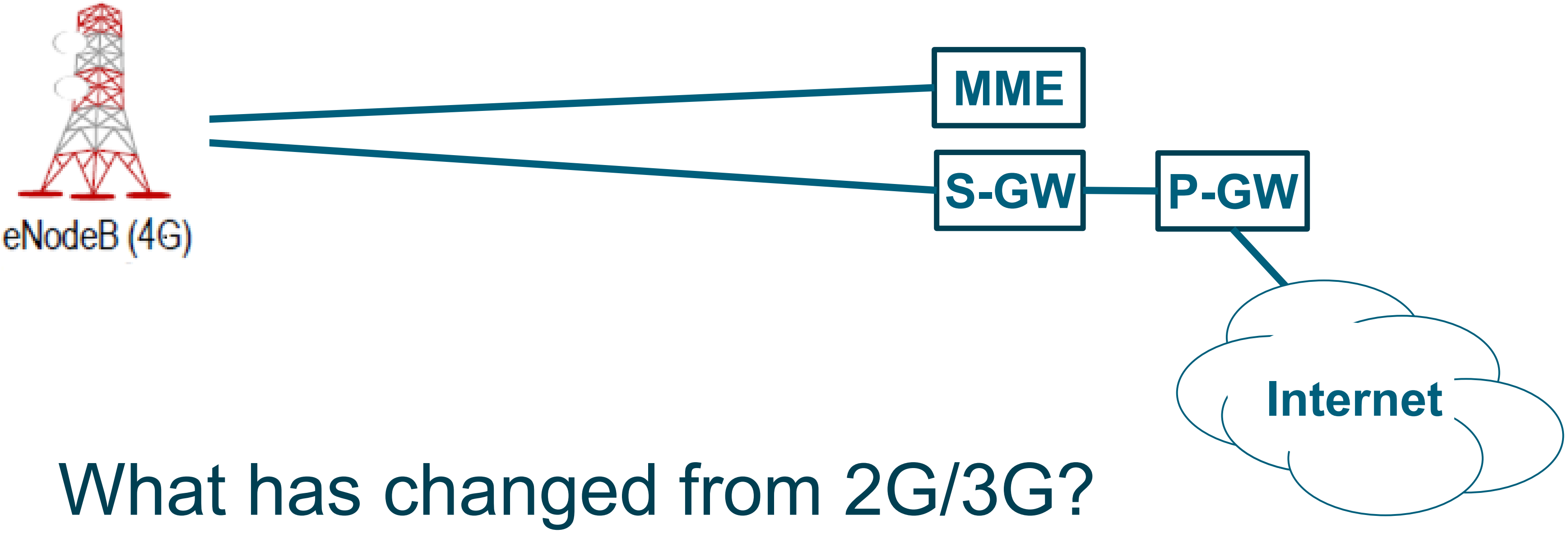
The Requirement?

The requirement – securing the backhaul



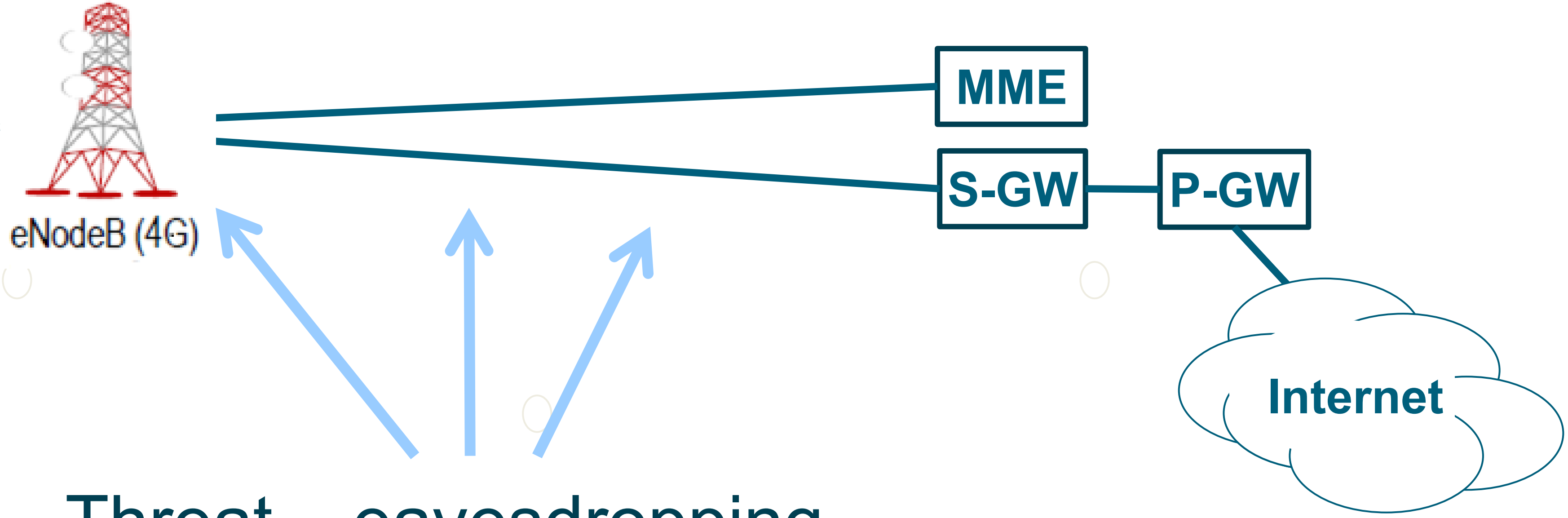
- I need to protect this infrastructure
- Customer confidentiality
- Service protection/Infrastructure integrity

The requirement – securing the backhaul



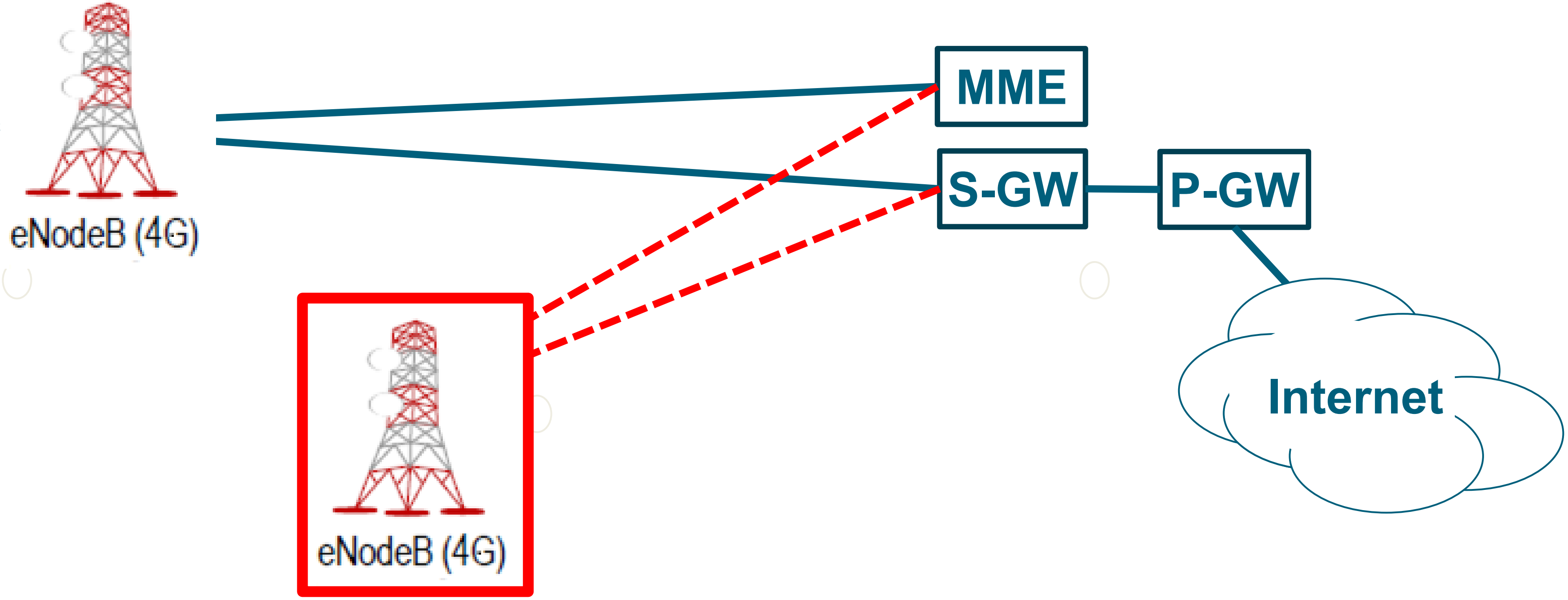
- What has changed from 2G/3G?
- All IP + Ethernet = RJ45, threat is similar but TDM kit not so widely available and as well understood as IP/Ethernet and free capture programs.
- 2G/3G core segregated from MBH by BSC/RNC

The requirement – securing the backhaul



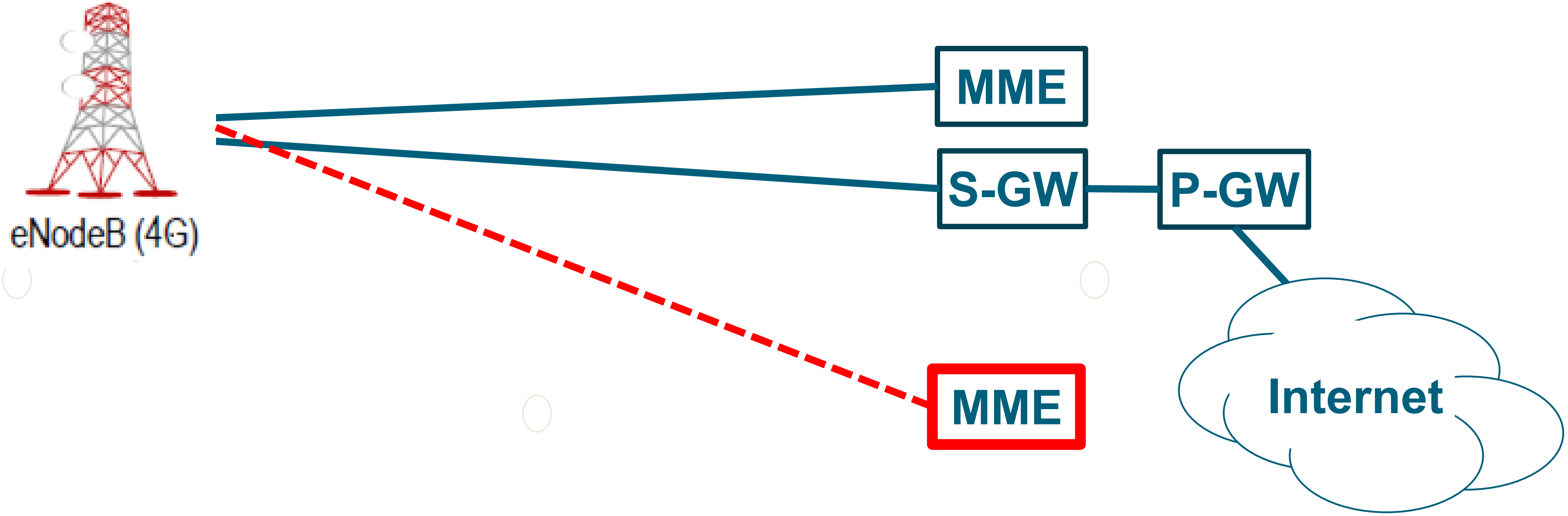
- Threat – eavesdropping
  - eNodeB locations may be insecure
  - First mile termination could be located in third party premises
  - Aggregation infrastructure could be located in third party premises

The requirement – securing the backhaul



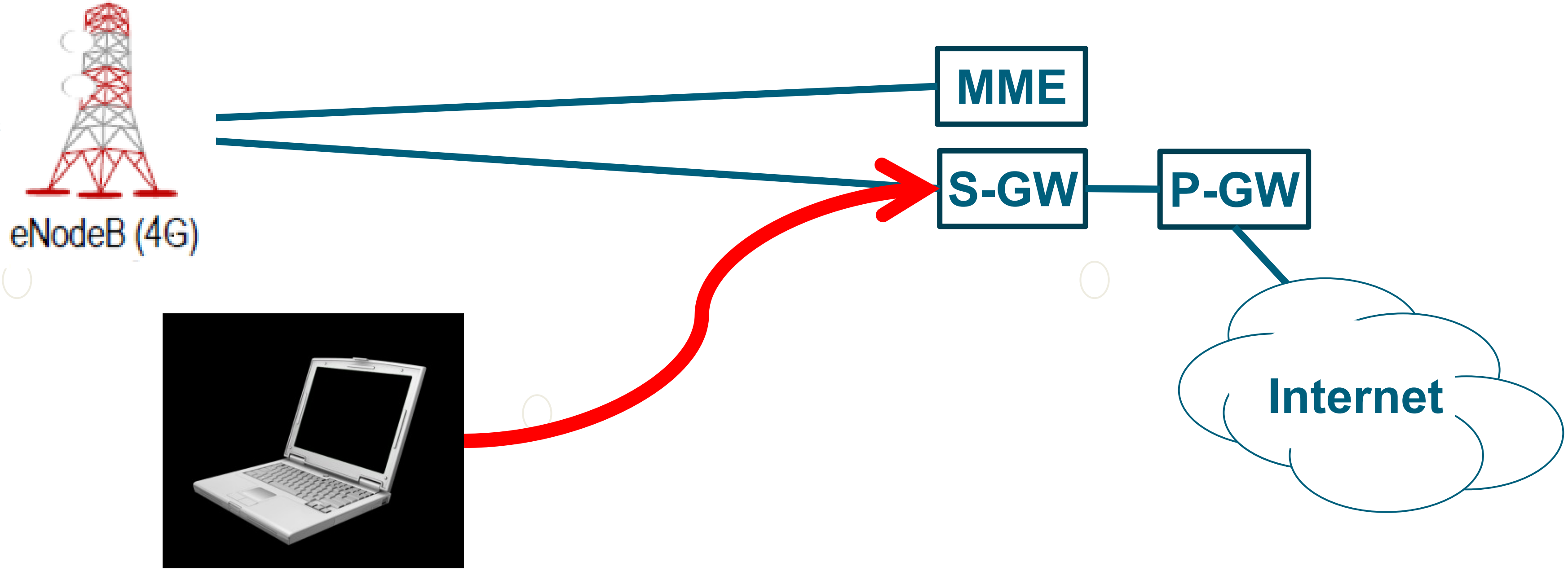
- Threat – Alien eNodeB
  - How do you prevent someone attaching an eNodeB to your infrastructure?

The requirement – securing the backhaul



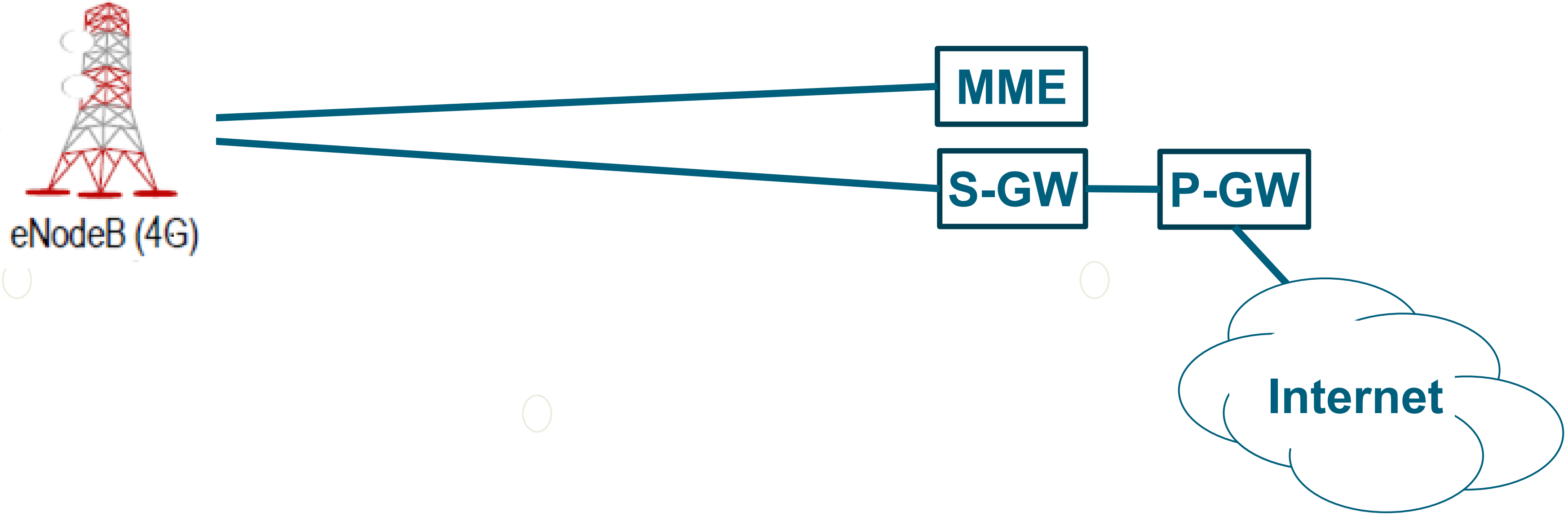
- Threat – Alien MME
  - How do you prevent someone attaching an MME to your infrastructure?

The requirement – securing the backhaul



- Threat – Denial of Service
  - How do you prevent someone flooding your IP infrastructure or attached systems?

The requirement – securing the backhaul

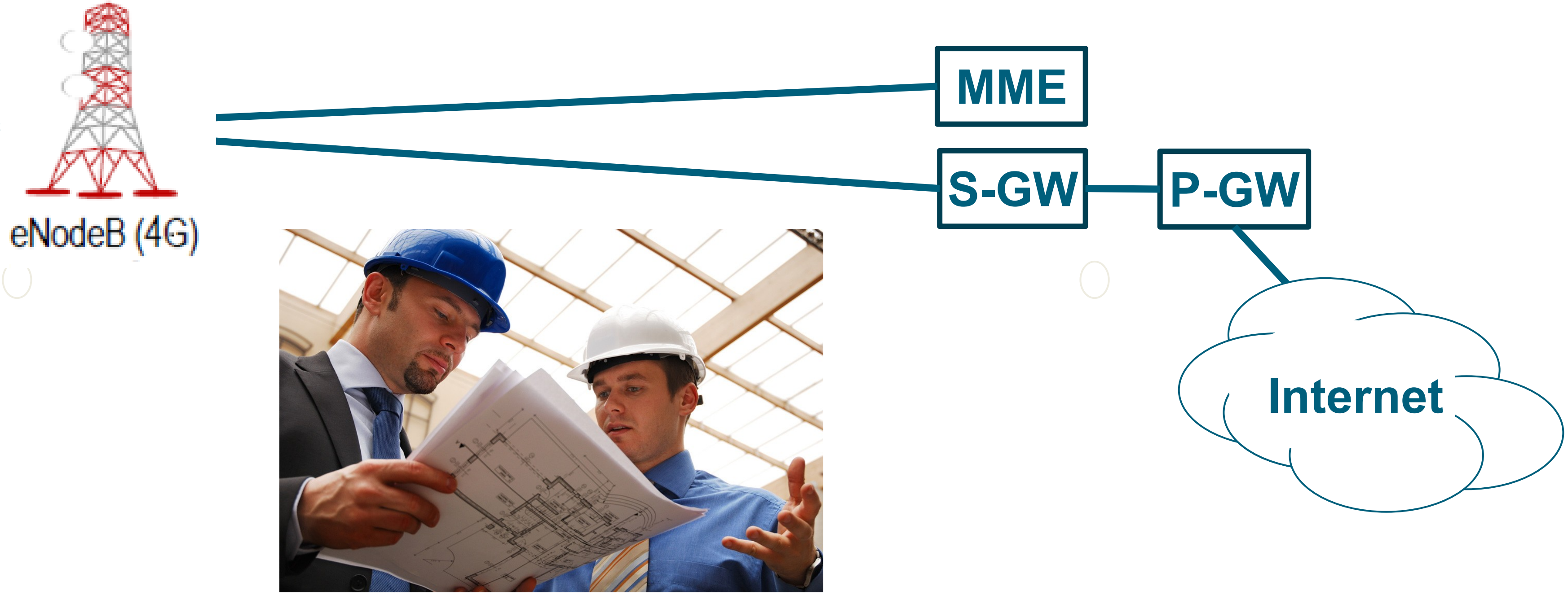


The requirement – securing the backhaul

- Caption competition…..

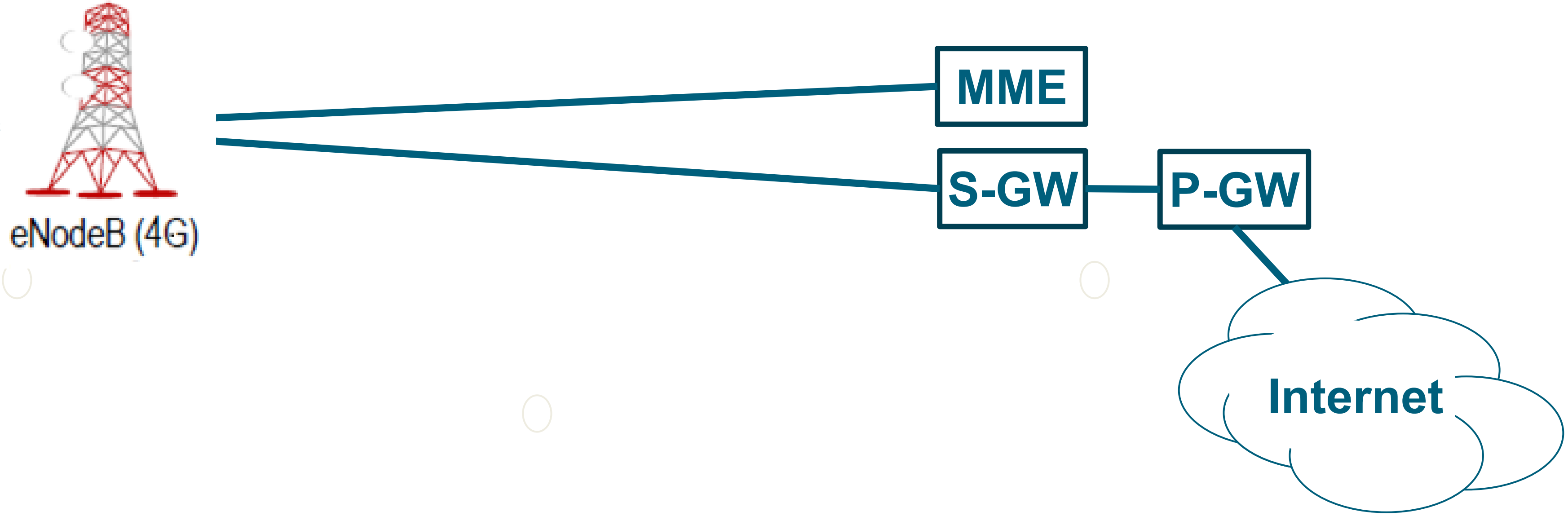
I don't know how it works either

The requirement – securing the backhaul



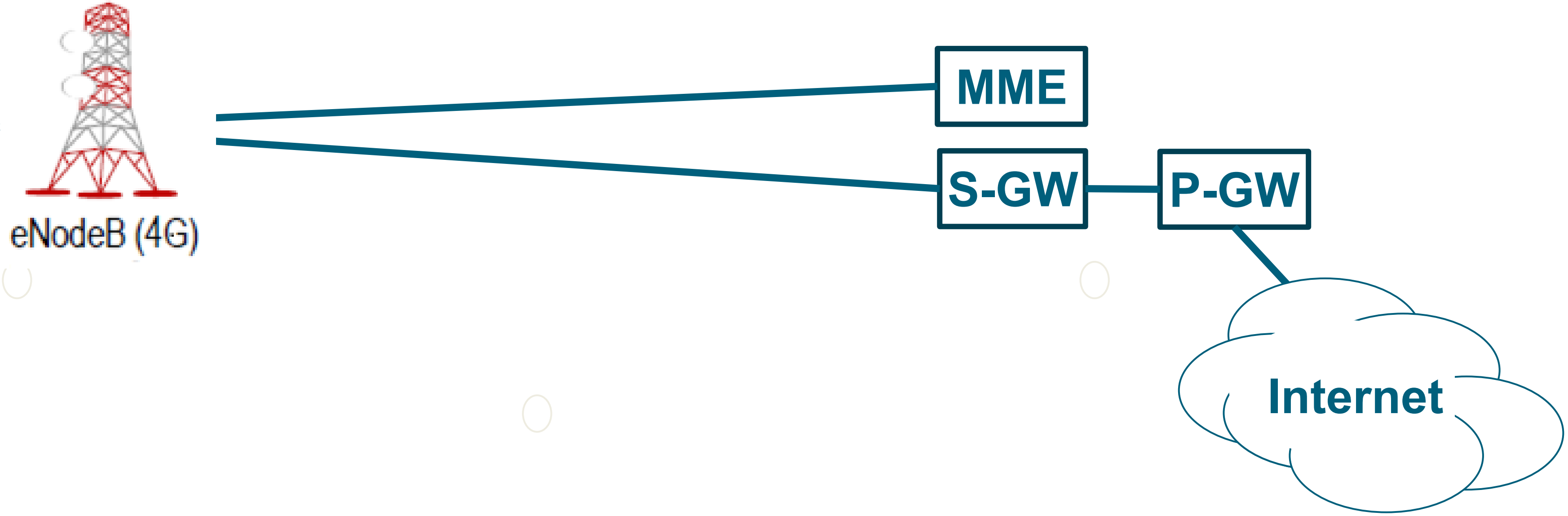
- Threat – Complexity
  - Difficult to maintain infrastructure is insecure

The requirement – securing the backhaul



- 3GPP
  - Encryption of IP traffic from eNodeB to EPC is not mandated.

The requirement – securing the backhaul

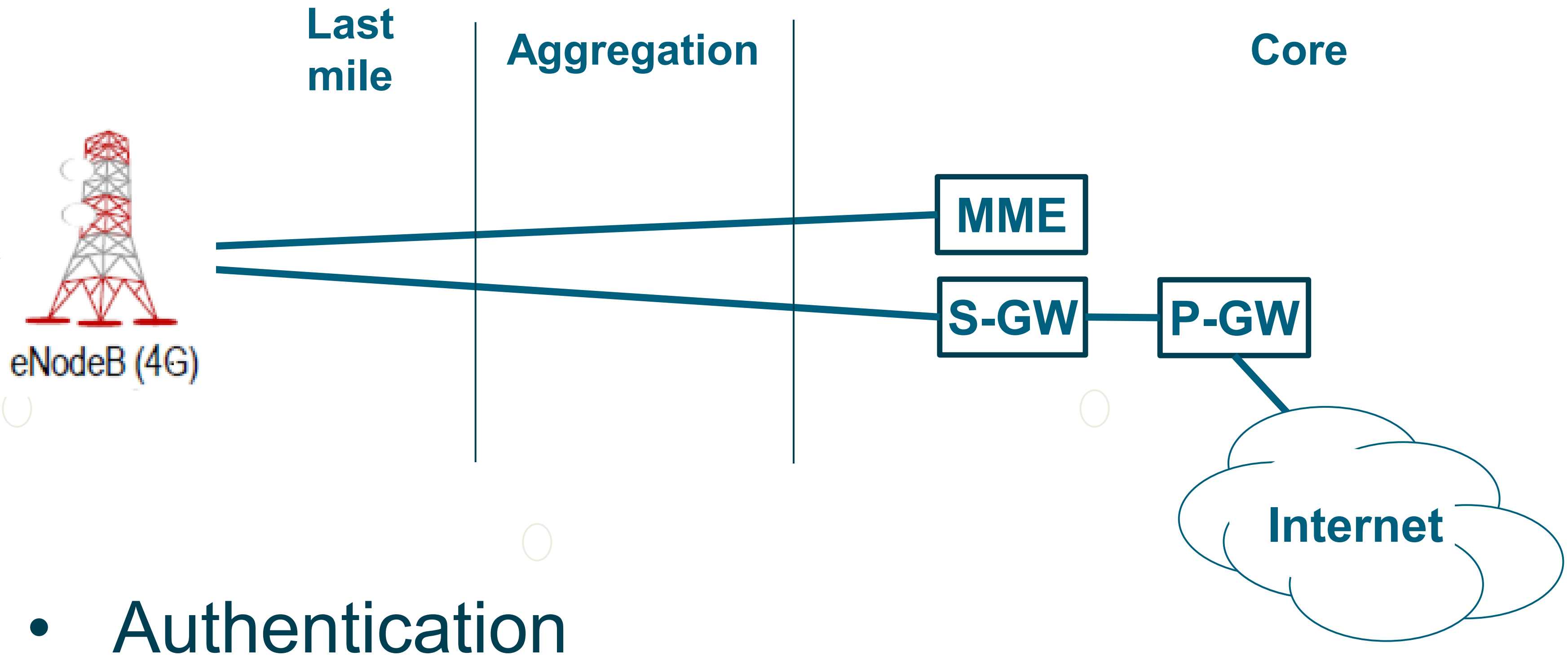


- What is everyone else doing?
  - Time for some market research

02

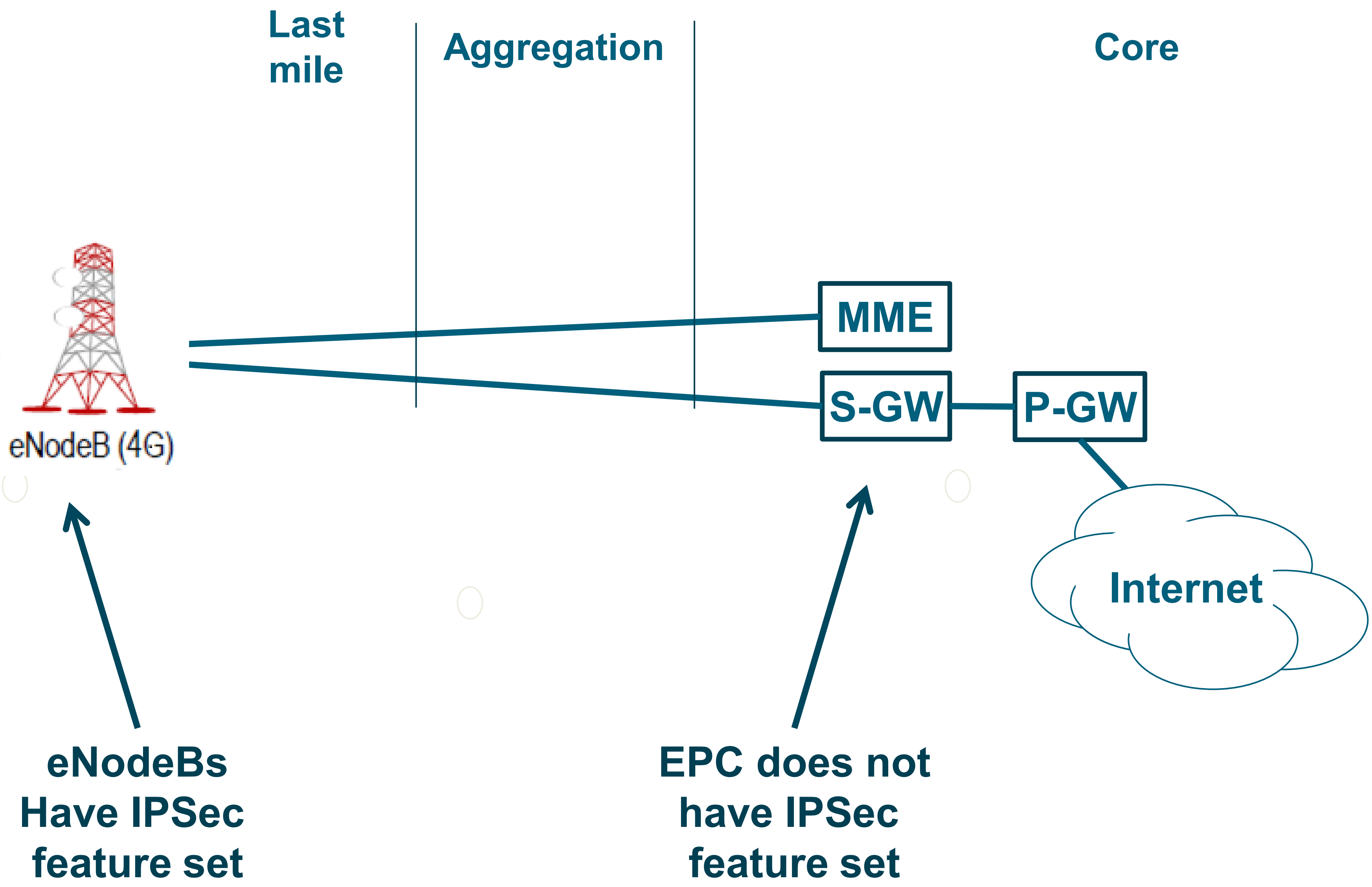
Securing the backhaul

- PKI
- IPSec



- Authentication
  - PKI = Public Key Infrastructure

- Encryption
  - IPSec = IETF defined IP Security protocol



Last mile

Aggregation

Core

eNodeB (4G)

MME

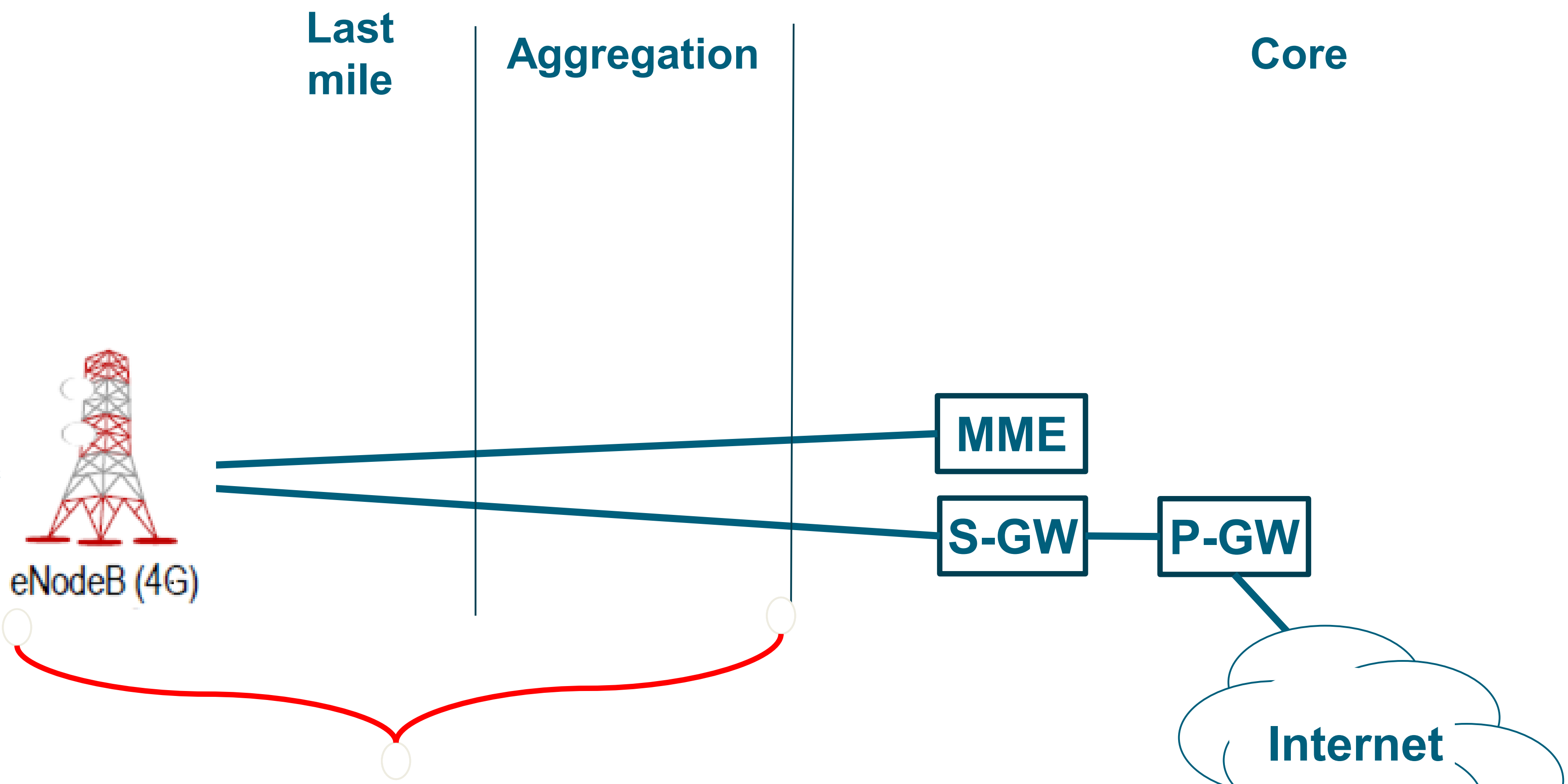
S-GW

P-GW

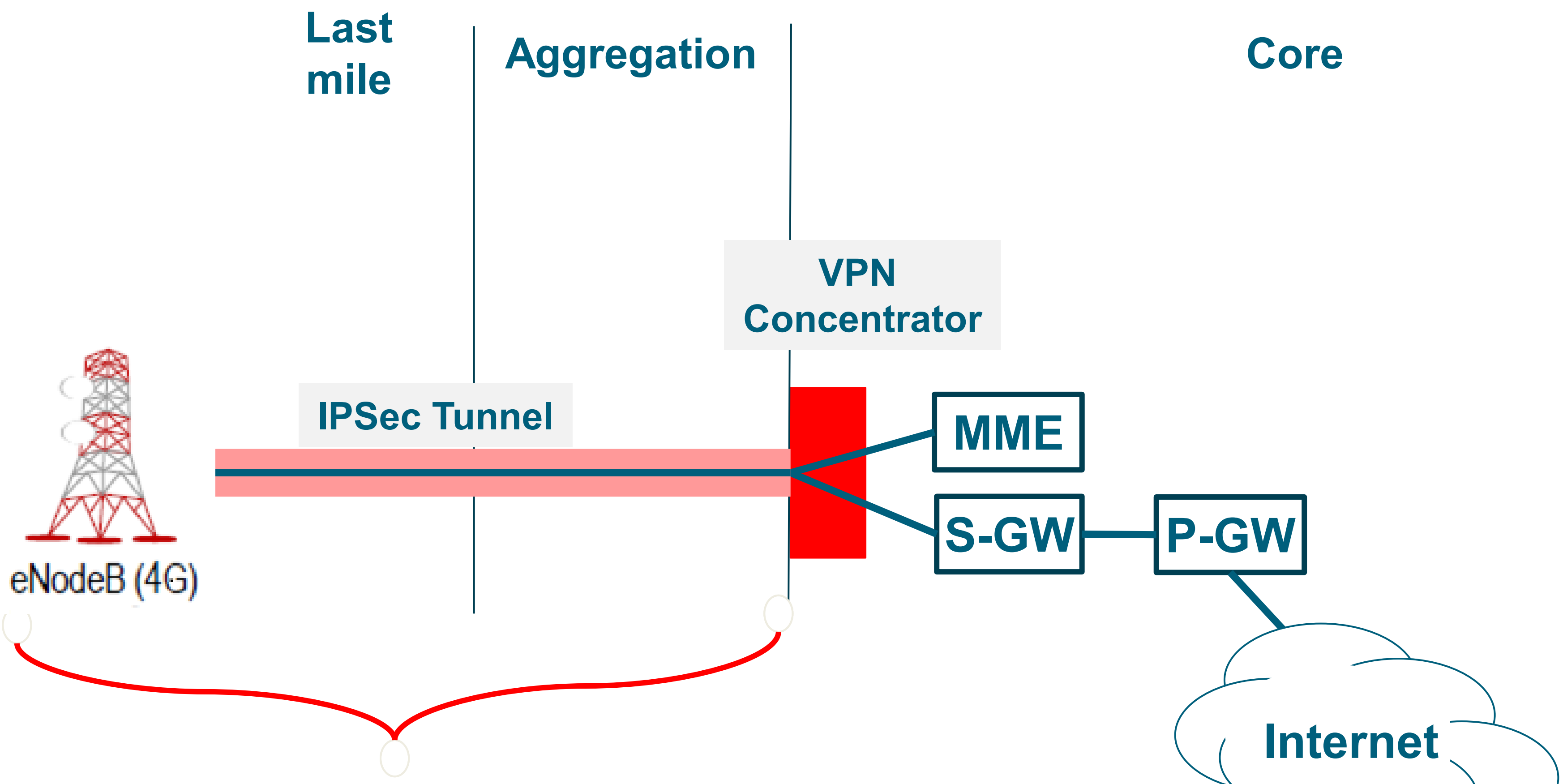
Internet

eNodeBs
Have IPSec
feature set

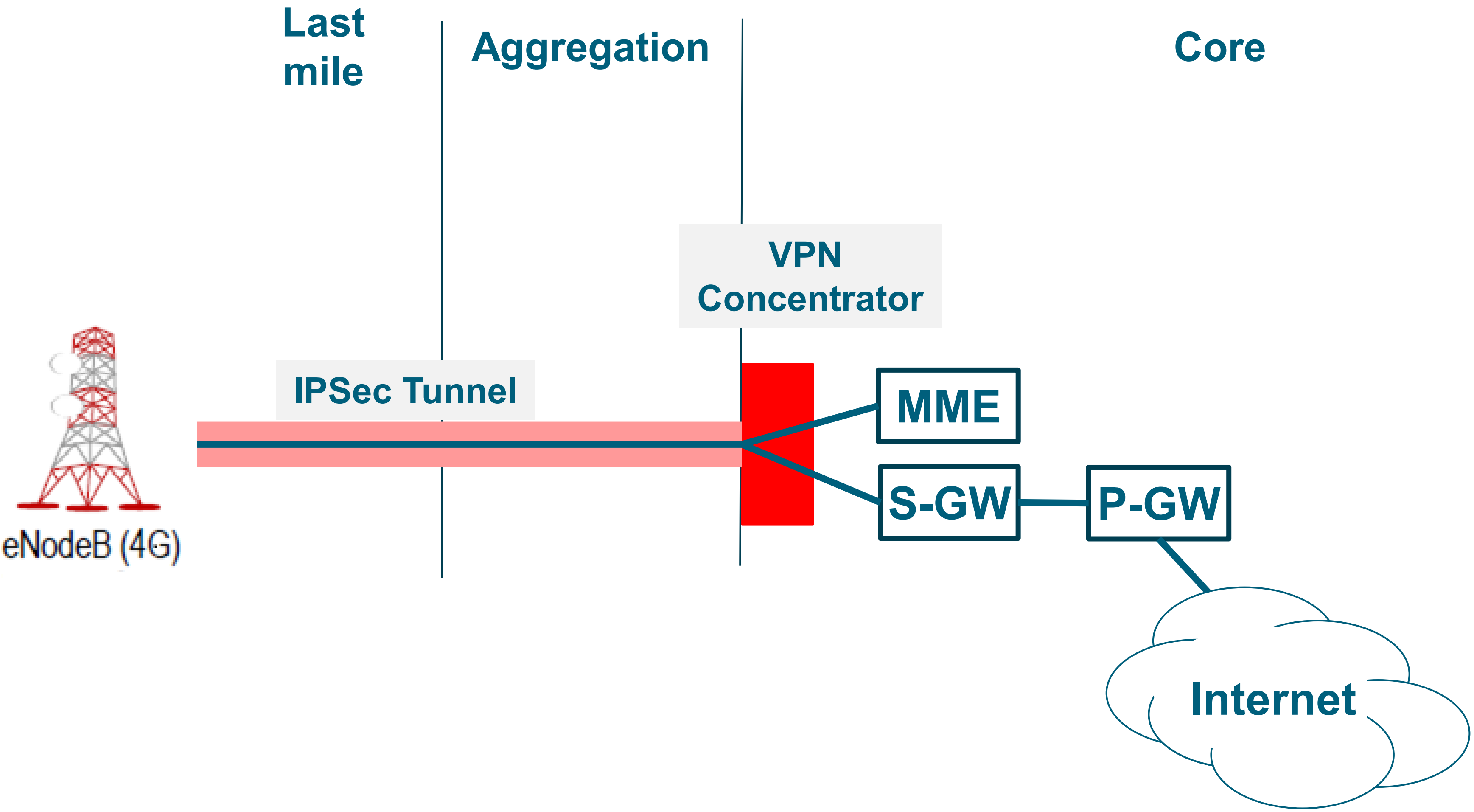
EPC does not
have IPSec
feature set

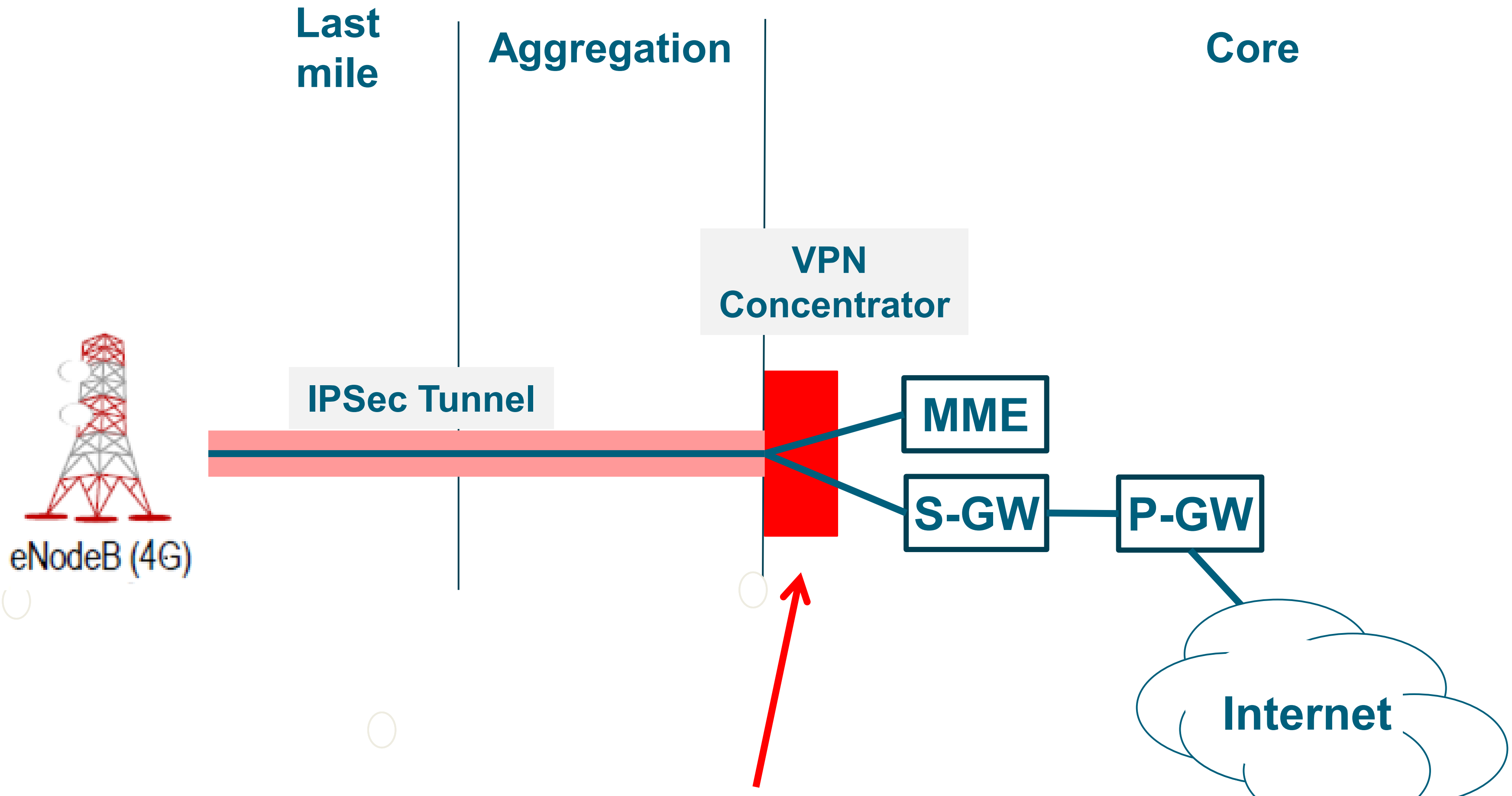


These could be Insecure Third Party locations

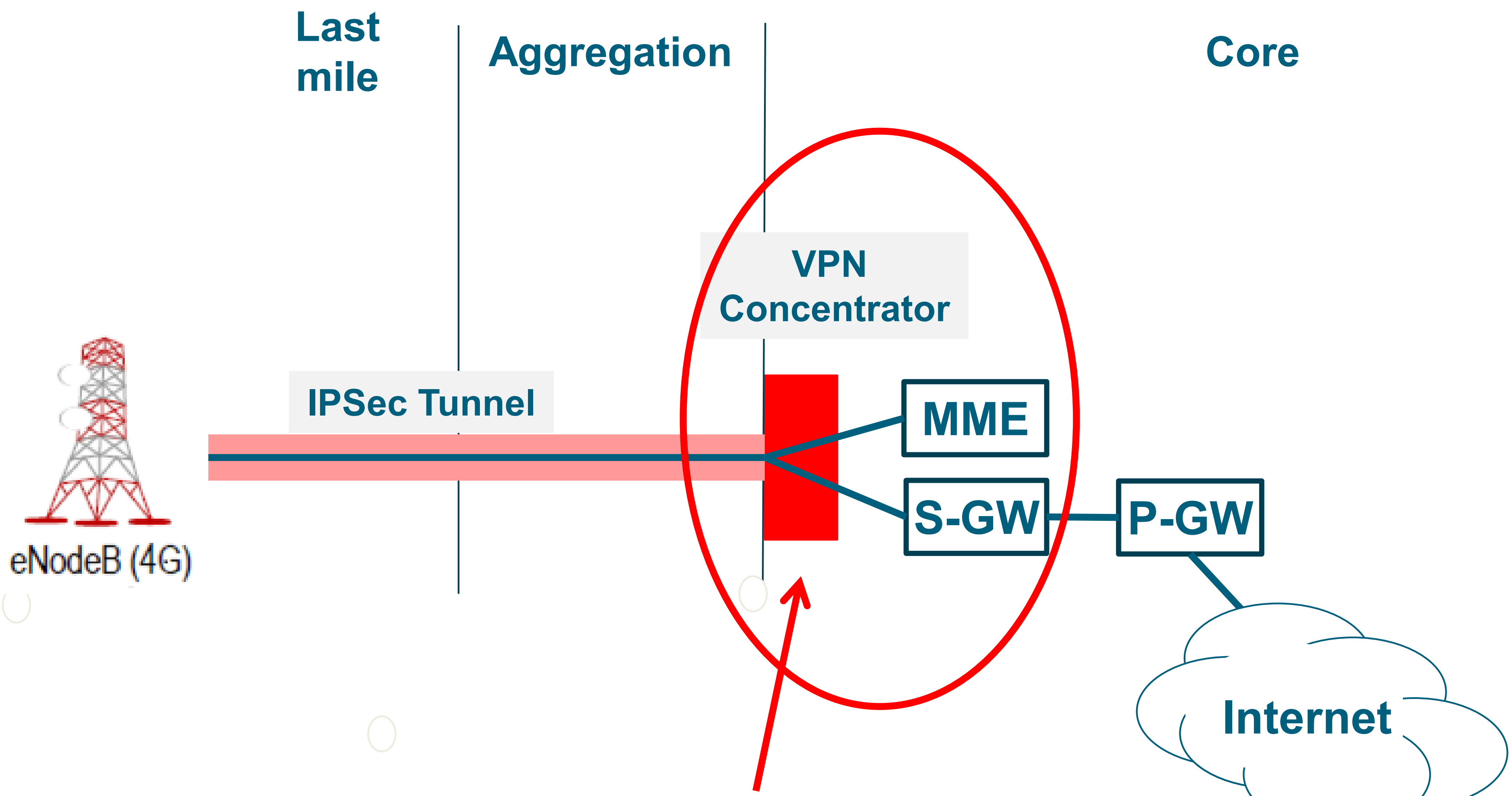


These could be Insecure Third Party locations


Last mile
Aggregation
Core
VPN Concentrator
IPSec Tunnel
MME
S-GW
P-GW
eNodeB (4G)
Internet



Only VPN Concentrator Between MBH and Core



Last mile

Aggregation

Core

VPN Concentrator

IPSec Tunnel

MME

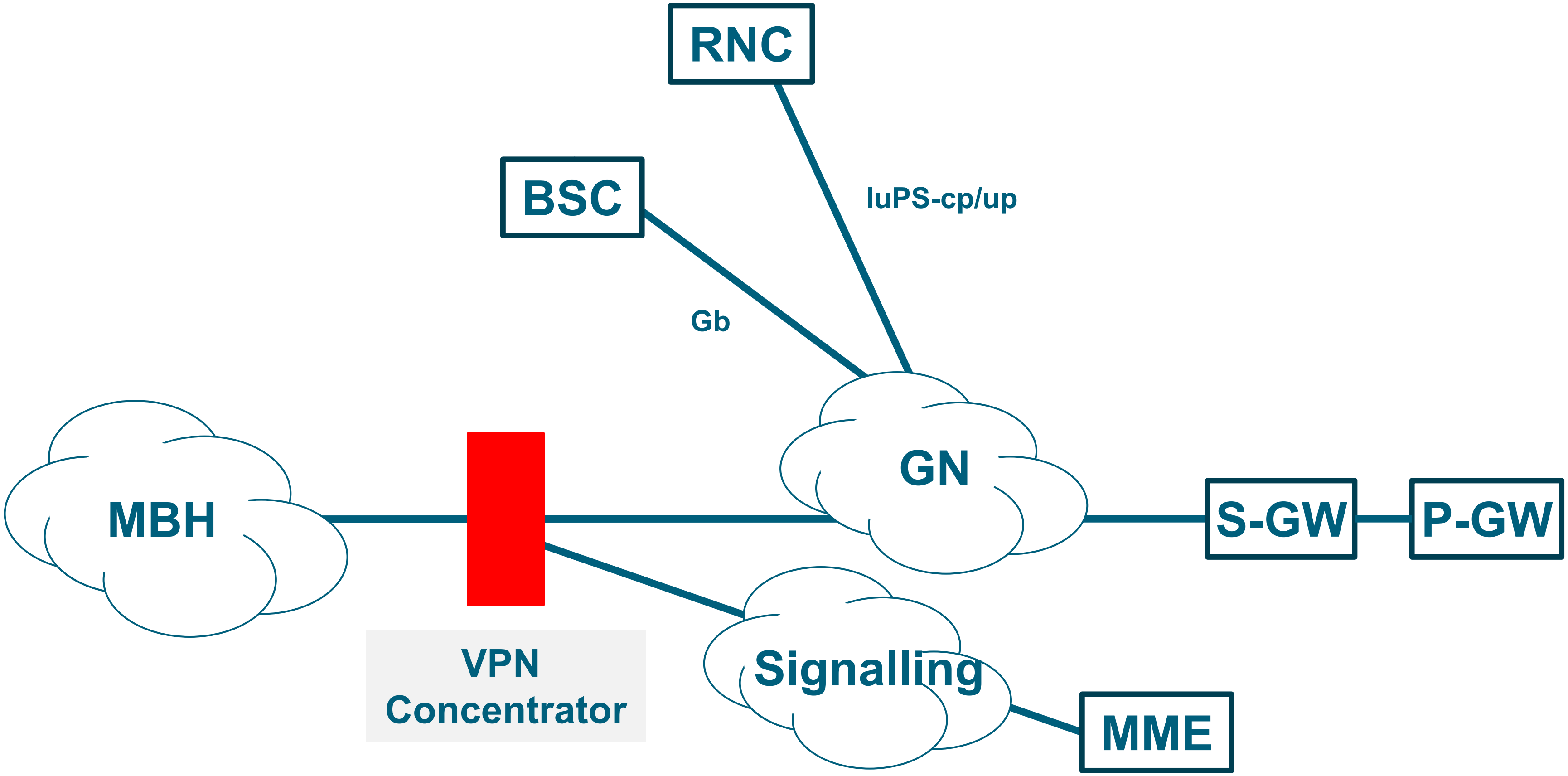
S-GW

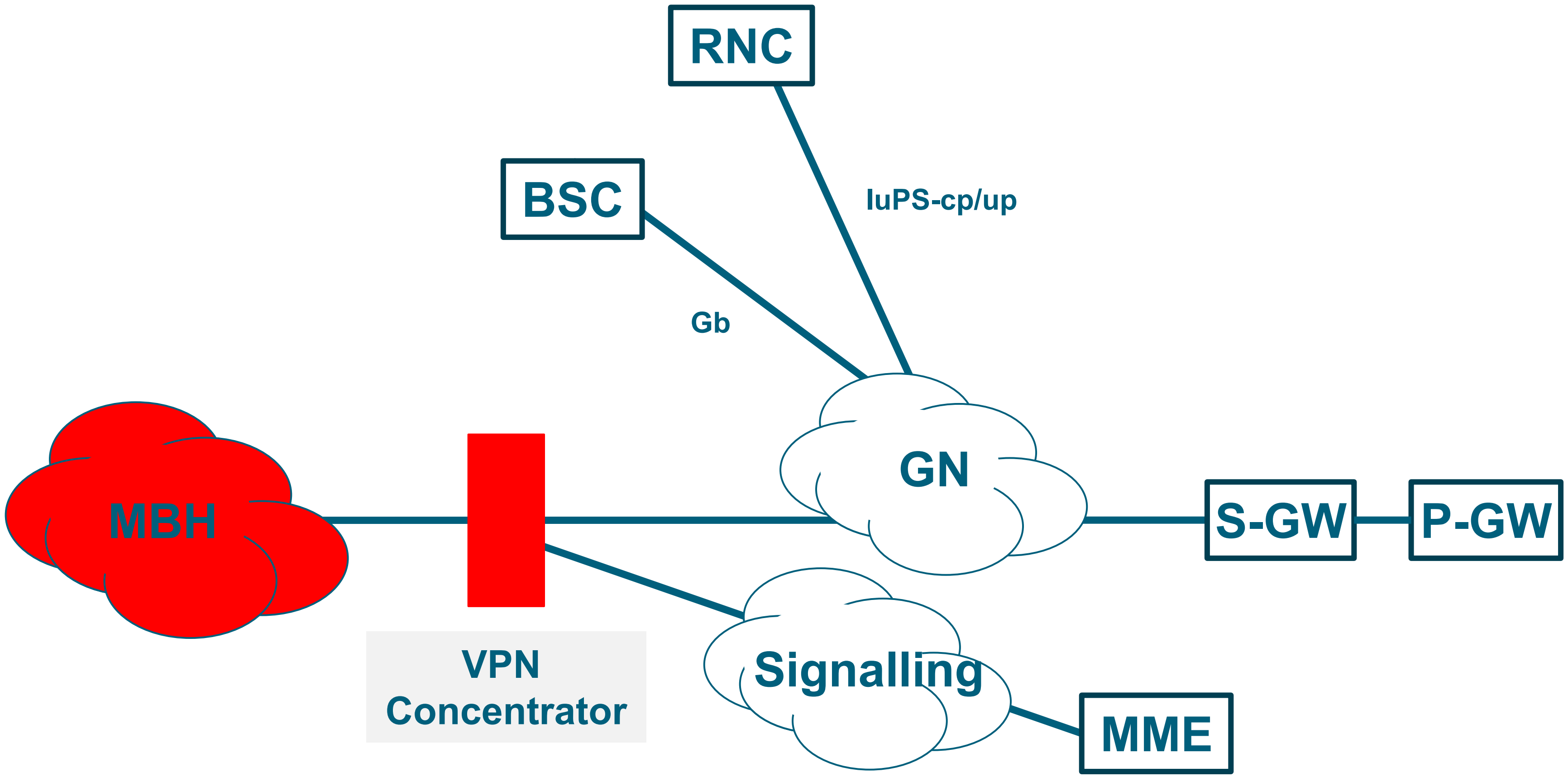
P-GW

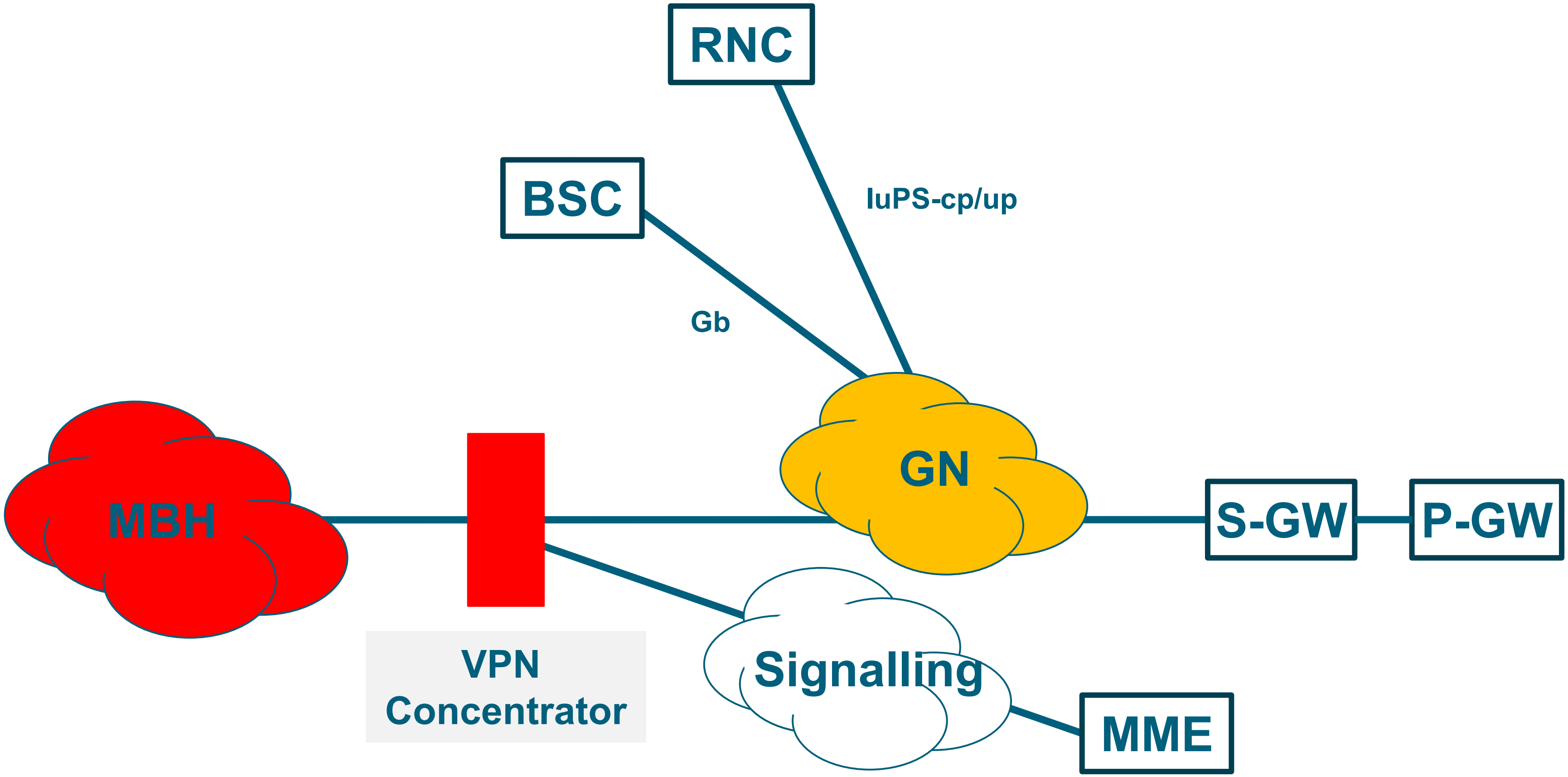
eNodeB (4G)

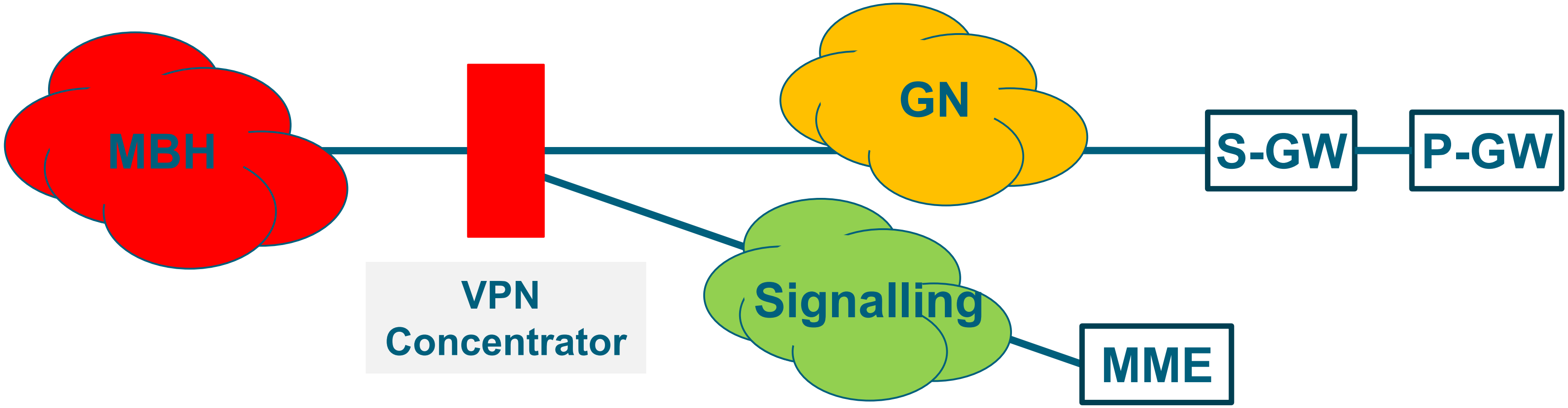
Internet

Only VPN Concentrator Between MBH and Core

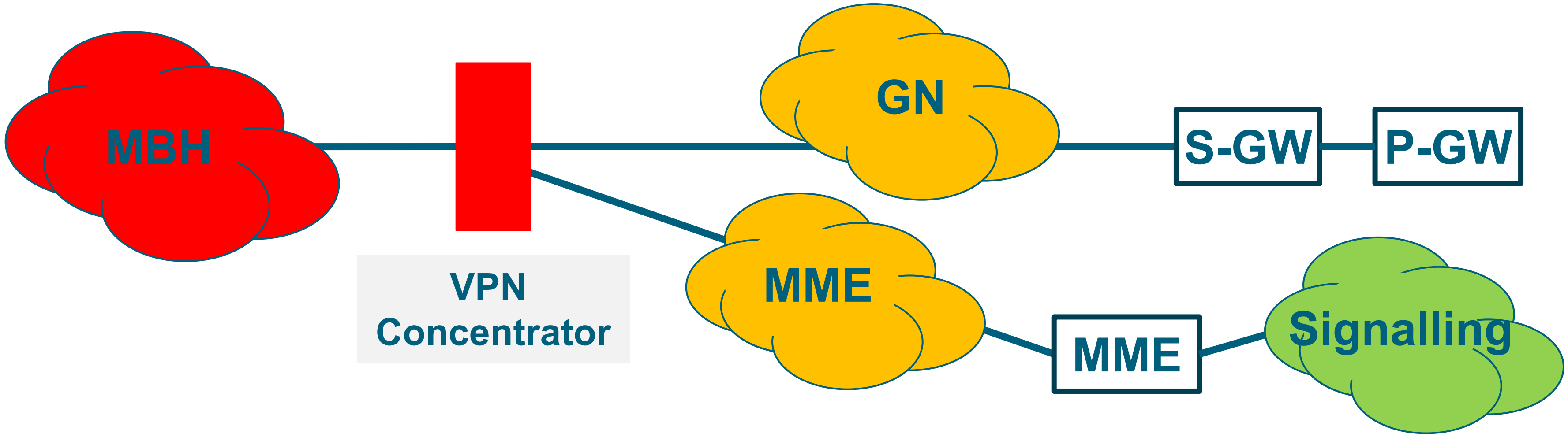

RNC
BSC
IuPS-cp/up
Gb
GN
MBH
S-GW
P-GW
Signalling
MME
VPN Concentrator


RNC
BSC
IuPS-cp/up
Gb
GN
MBH
S-GW
P-GW
VPN Concentrator
Signalling
MME


RNC
BSC
IuPS-cp/up
Gb
MBH
GN
S-GW
P-GW
VPN Concentrator
Signalling
MME

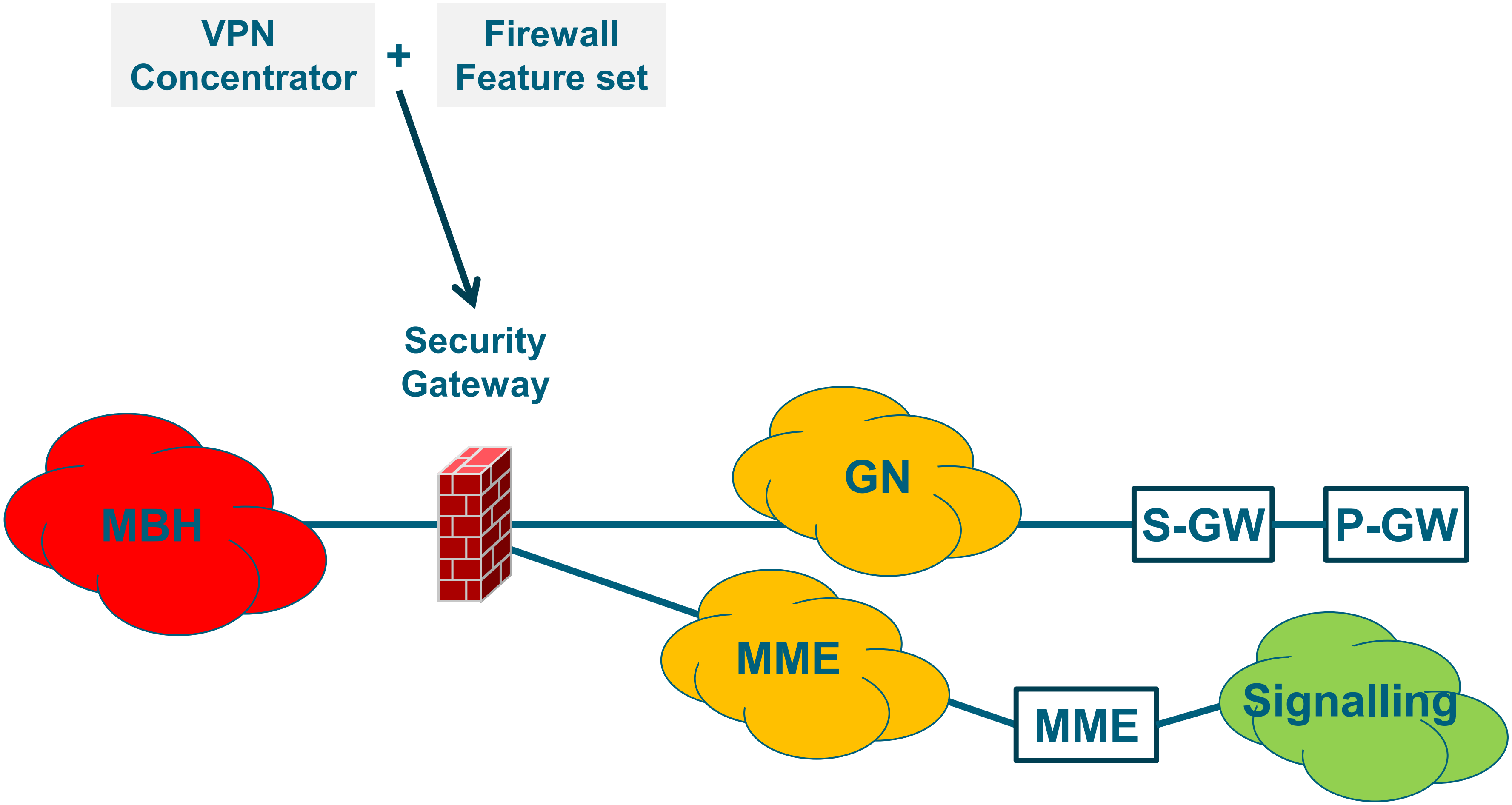


- **Do I want to connect my precious signalling infrastructure to MBH via VPN concentrator?**



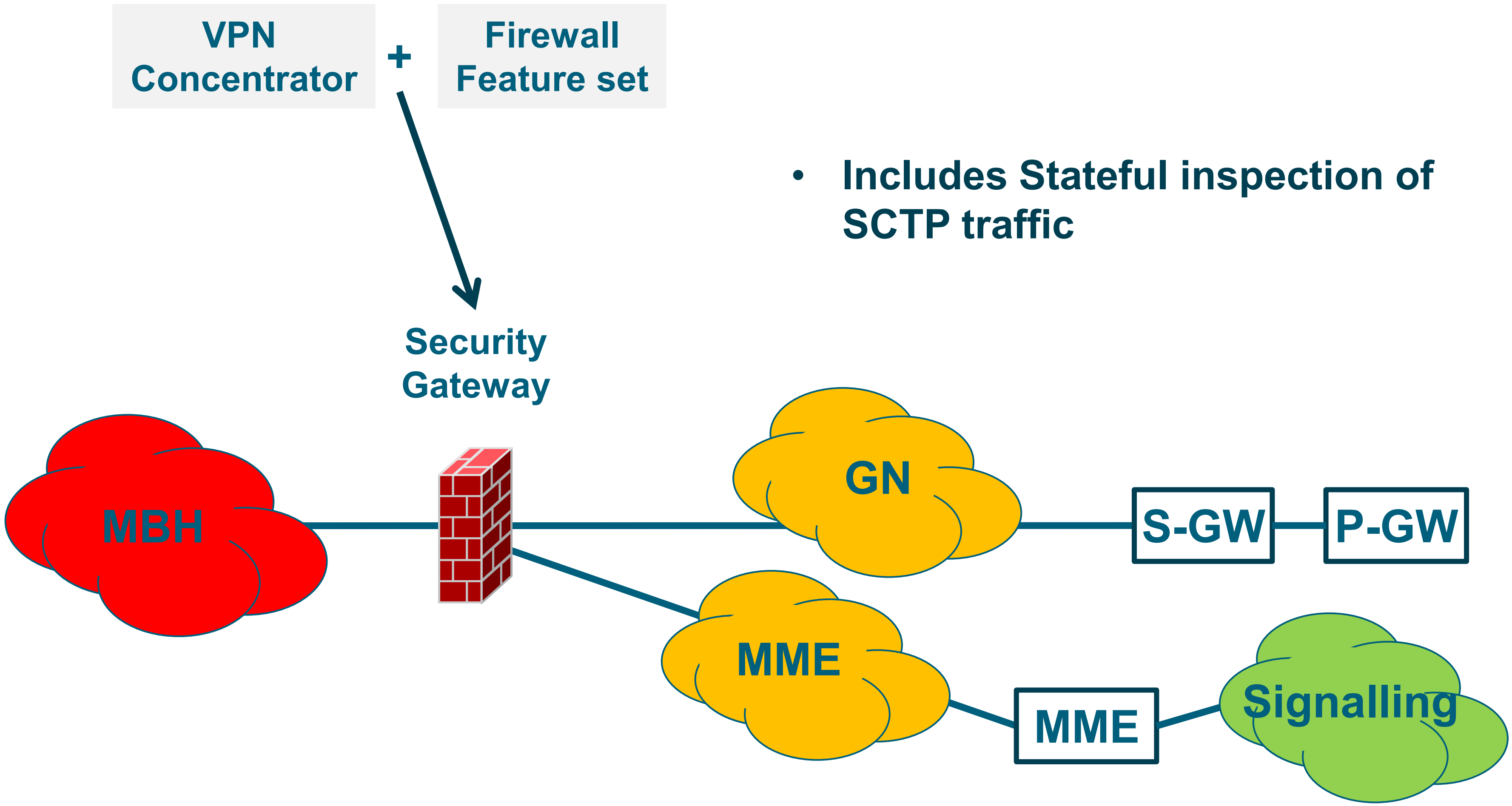
- **Dedicated Security domain for S1-MME interface on MME**

- Firewall feature set on LTE Security Gateway



- Dedicated Security domain for S1-MME interface on MME

- **Firewall feature set on LTE Security Gateway**



- **Includes Stateful inspection of SCTP traffic**

- **Dedicated Security domain for S1-MME interface on MME**

- **Telefónica UK deployed:-**

- **Huawei Eudemon 8000E-X3**
- **2 x 10Gbps ports**

- **Securing 2G and 3G alongside LTE**

		Secure when all IP?	Solution
LTE	OAM	No	IPSec
	UP	No	IPSec
	CP	No	IPSec
3G	OAM		
	UP		
	CP		
2G	OAM		
	UP		
	CP		

- **Securing 2G and 3G alongside LTE**

		Secure when all IP?	Solution
LTE	OAM	No	IPSec
	UP	No	IPSec
	CP	No	IPSec
3G	OAM	No	
	UP	Yes	
	CP	No	
2G	OAM		
	UP		
	CP		

- **Securing 2G and 3G alongside LTE**

		Secure when all IP?	Solution
LTE	OAM	No	IPSec
	UP	No	IPSec
	CP	No	IPSec
3G	OAM	No	IPSec
	UP	Yes	n/a
	CP	No	IPSec
2G	OAM		
	UP		
	CP		

- **Securing 2G and 3G alongside LTE**

		Secure when all IP?	Solution
LTE	OAM	No	IPSec
	UP	No	IPSec
	CP	No	IPSec
3G	OAM	No	IPSec
	UP	Yes	n/a
	CP	No	IPSec
2G	OAM	No	
	UP	No	
	CP	No	

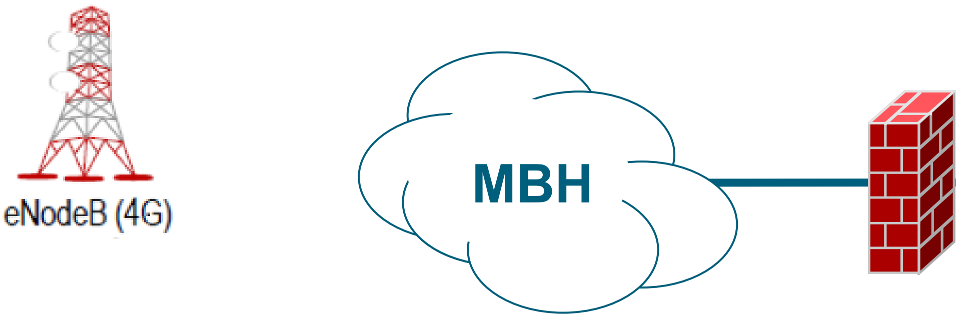
- **Securing 2G and 3G alongside LTE**

		Secure when all IP?	Solution
LTE	OAM	No	IPSec
	UP	No	IPSec
	CP	No	IPSec
3G	OAM	No	IPSec
	UP	Yes	n/a
	CP	No	IPSec
2G	OAM	No	IPSec
	UP	No	IPSec
	CP	No	IPSec

Securing 2G/3G

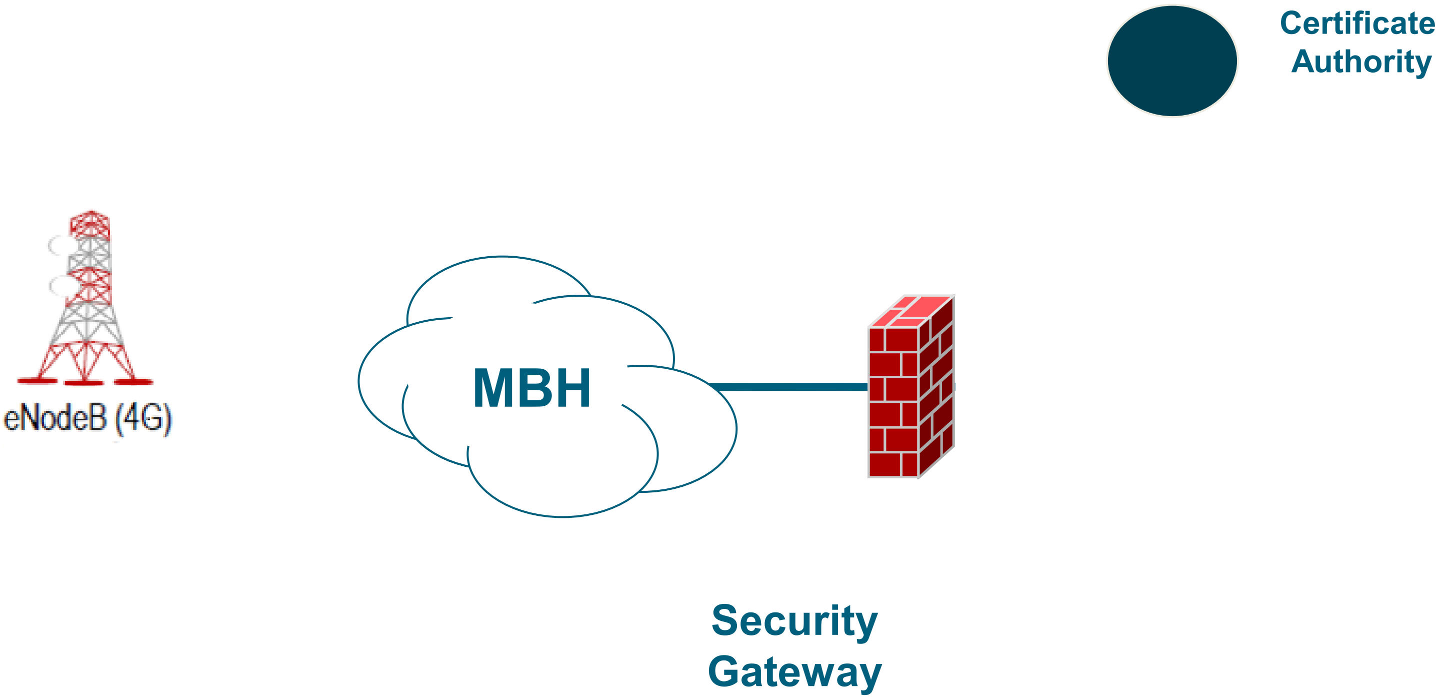
- Vendor support for IPSec on 2G/3G is coming………
- Do you want to put all your eggs in one basket?

- **Certificates**



Security Gateway

- **Certificates**



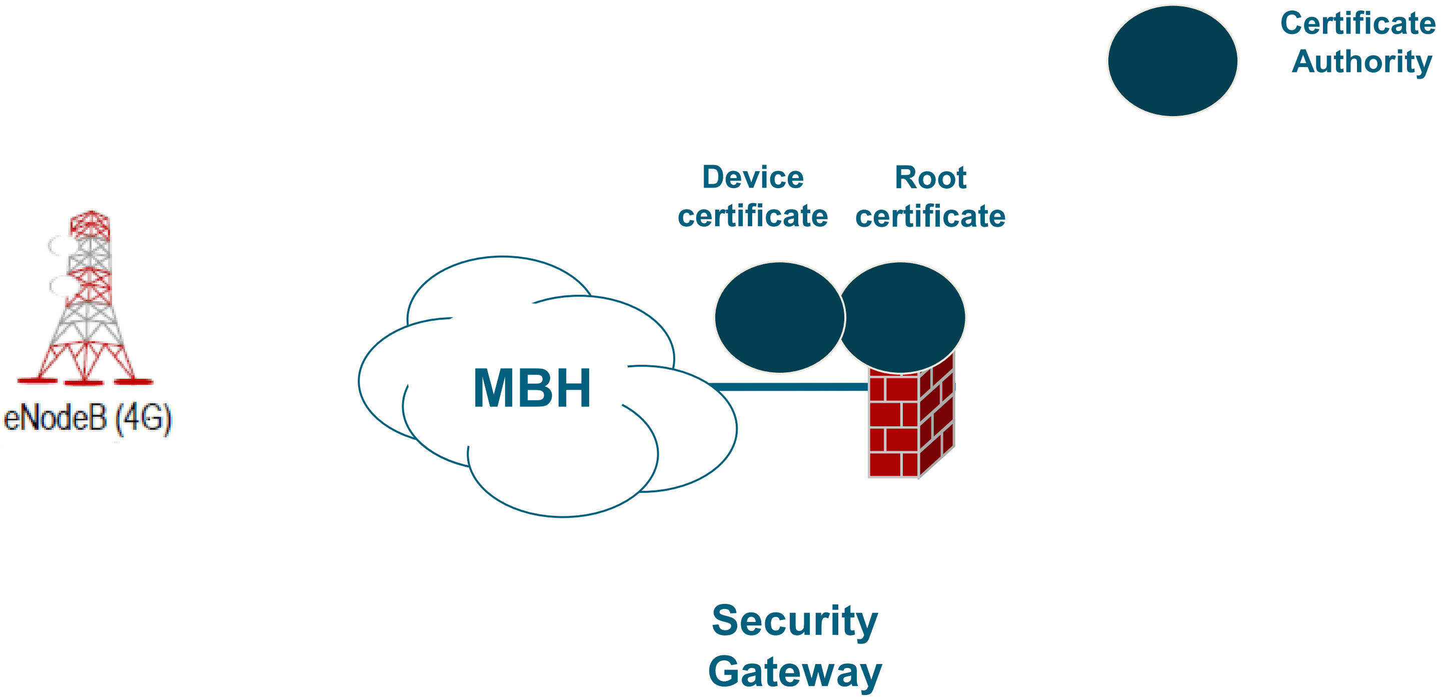
Certificate Authority

eNodeB (4G)

MBH

Security Gateway

- **Certificates**



Certificate Authority

Device certificate

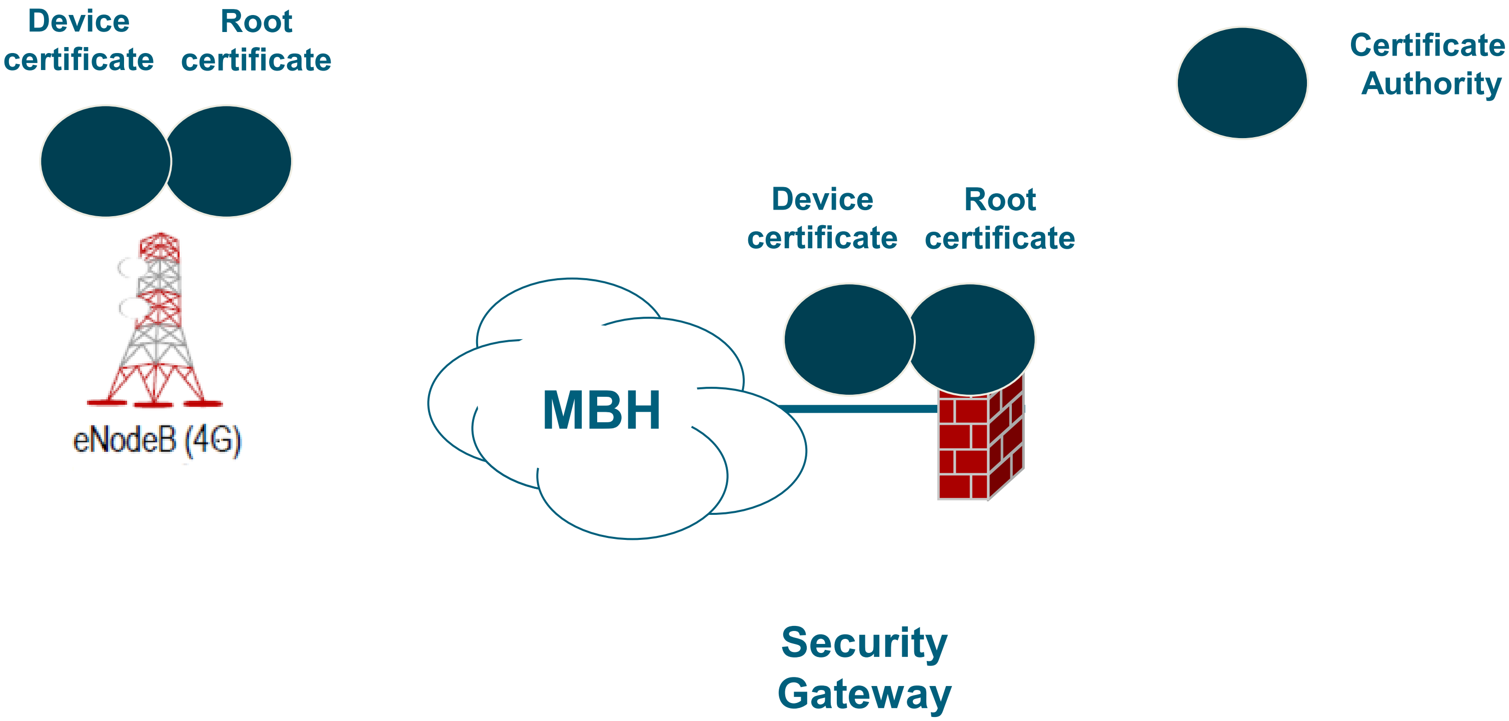
Root certificate

eNodeB (4G)

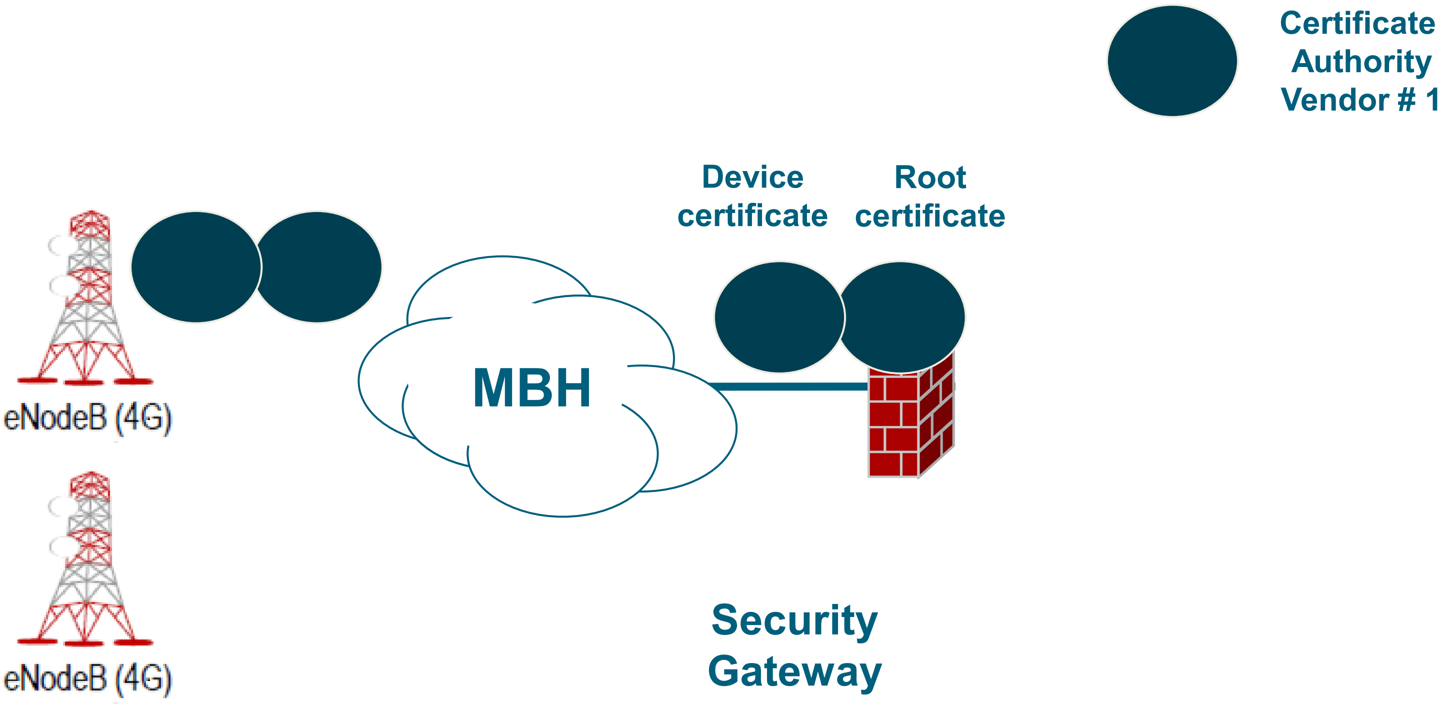
MBH

Security Gateway

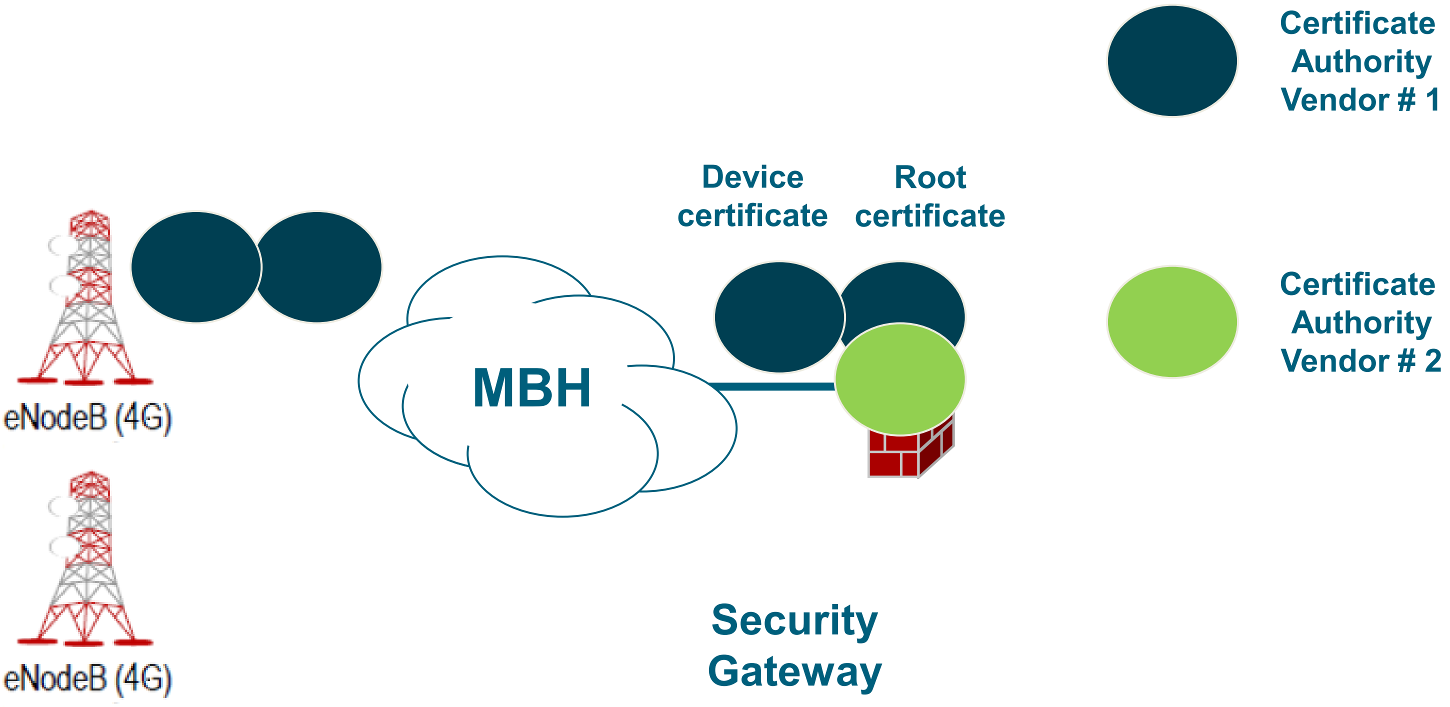
- **Certificates**



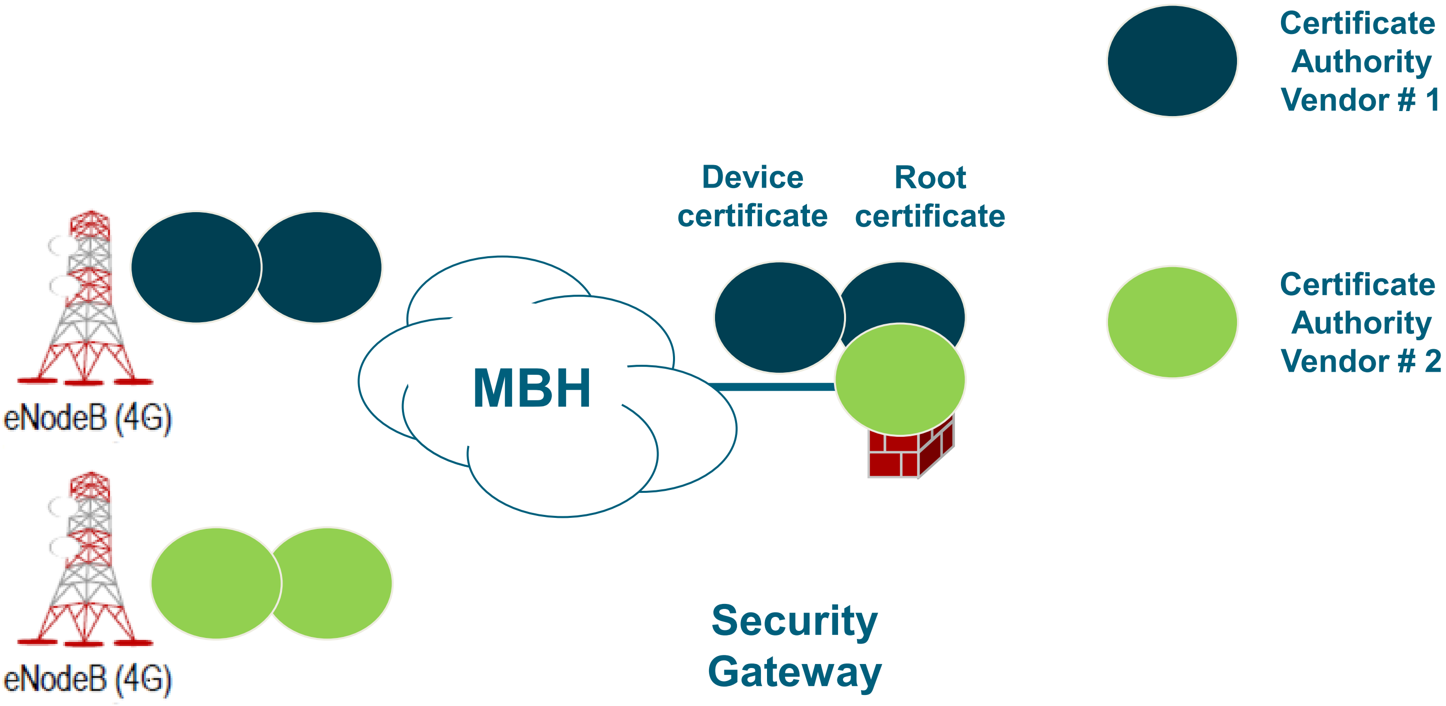
- **Certificates**



- **Certificates**



- **Certificates**



Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

Device certificate

Root certificate

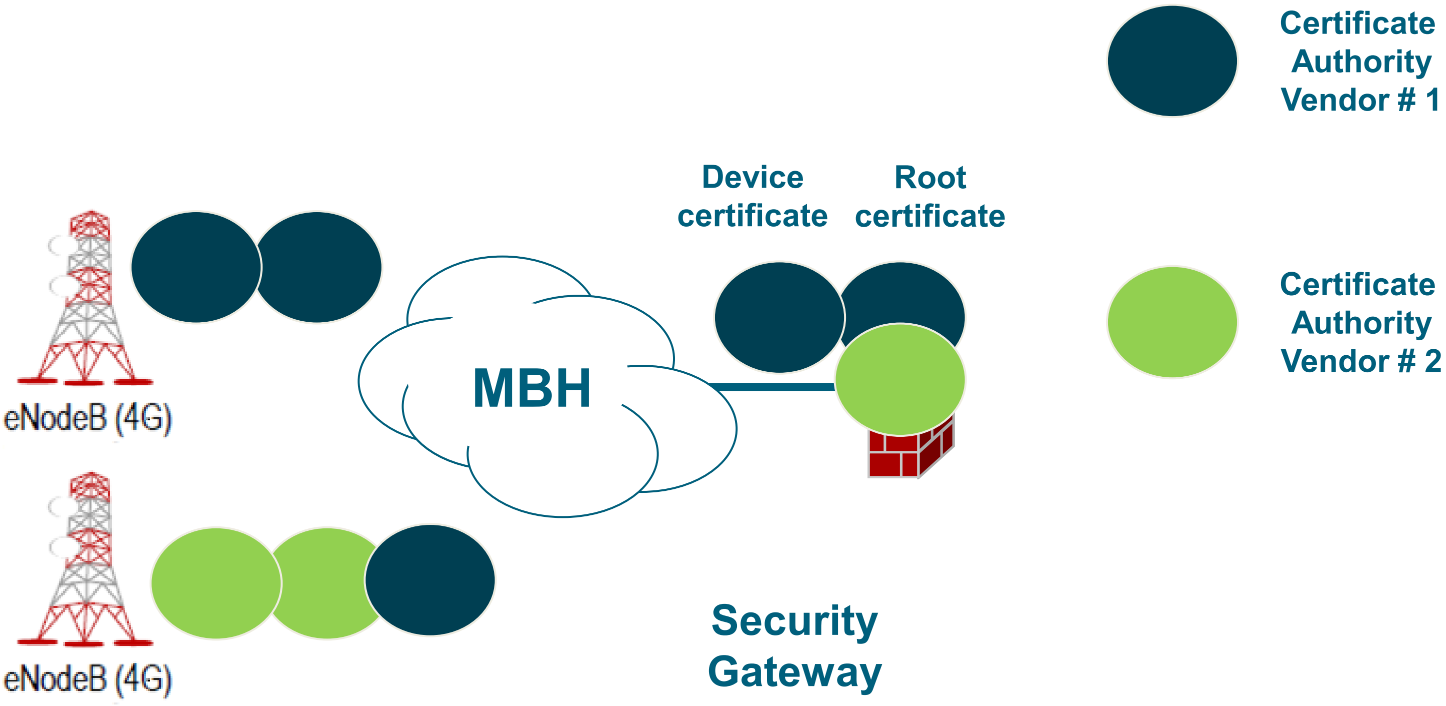
MBH

eNodeB (4G)

eNodeB (4G)

Security Gateway

- **Certificates**



Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

Device certificate

Root certificate

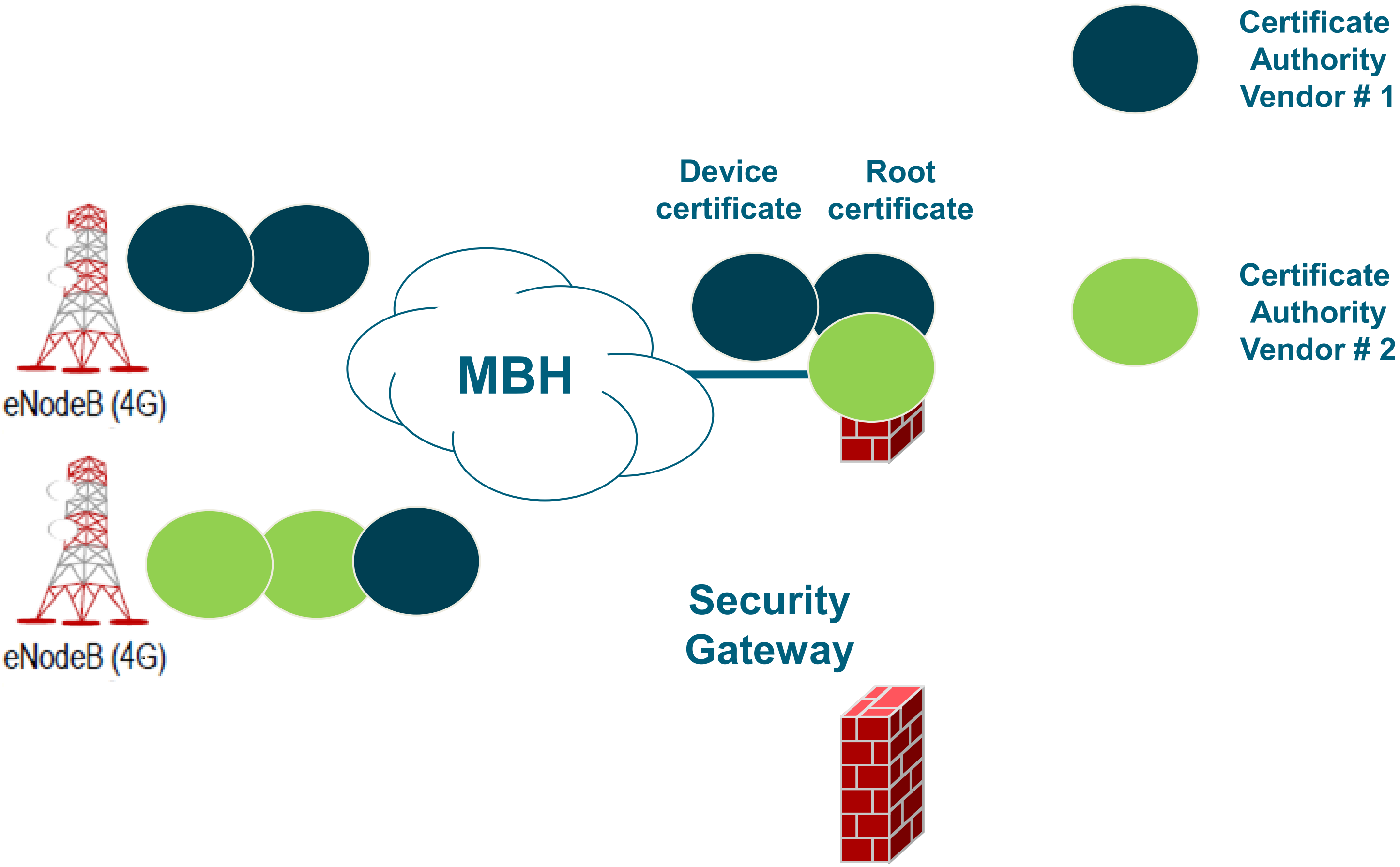
MBH

eNodeB (4G)

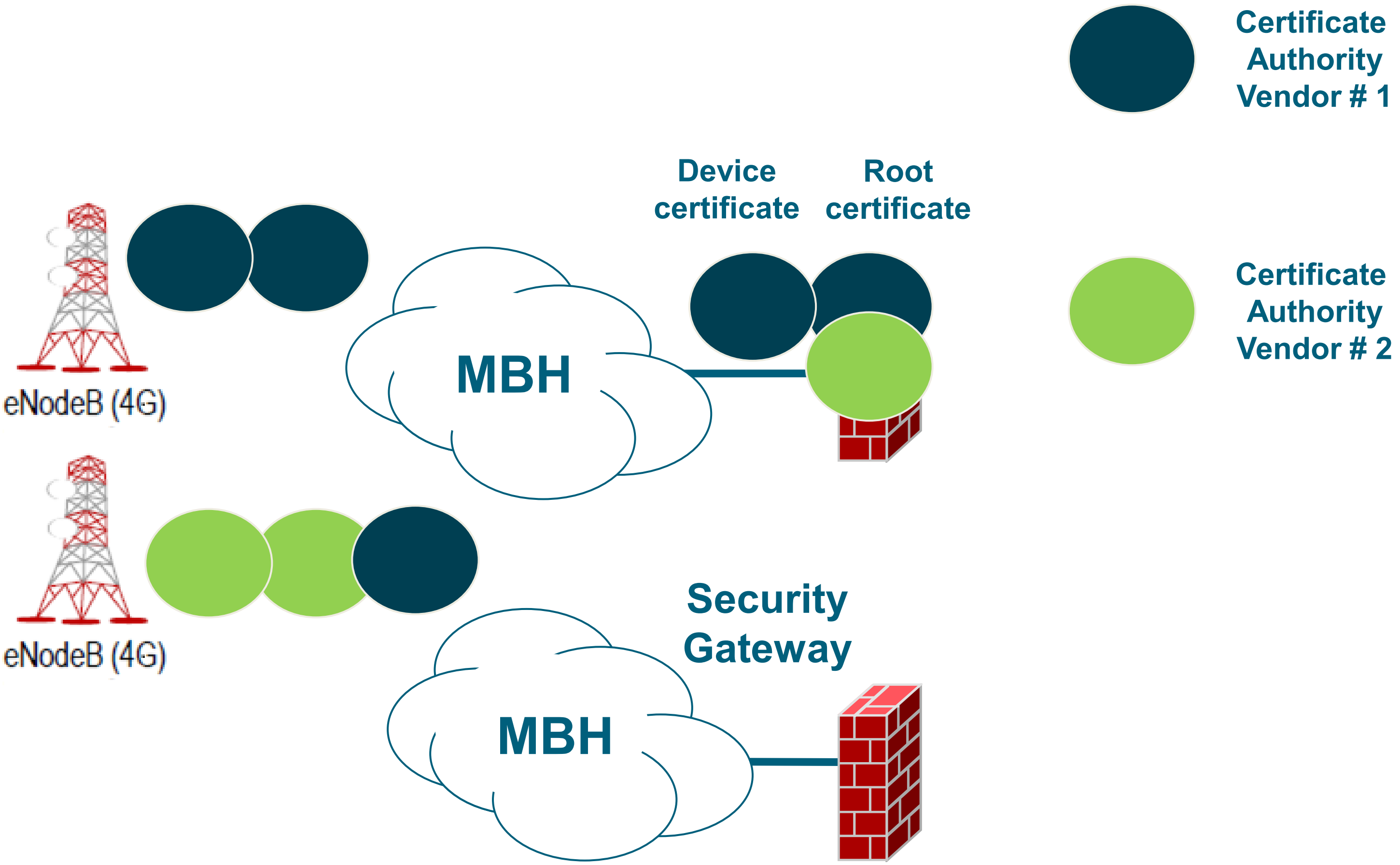
eNodeB (4G)

Security Gateway

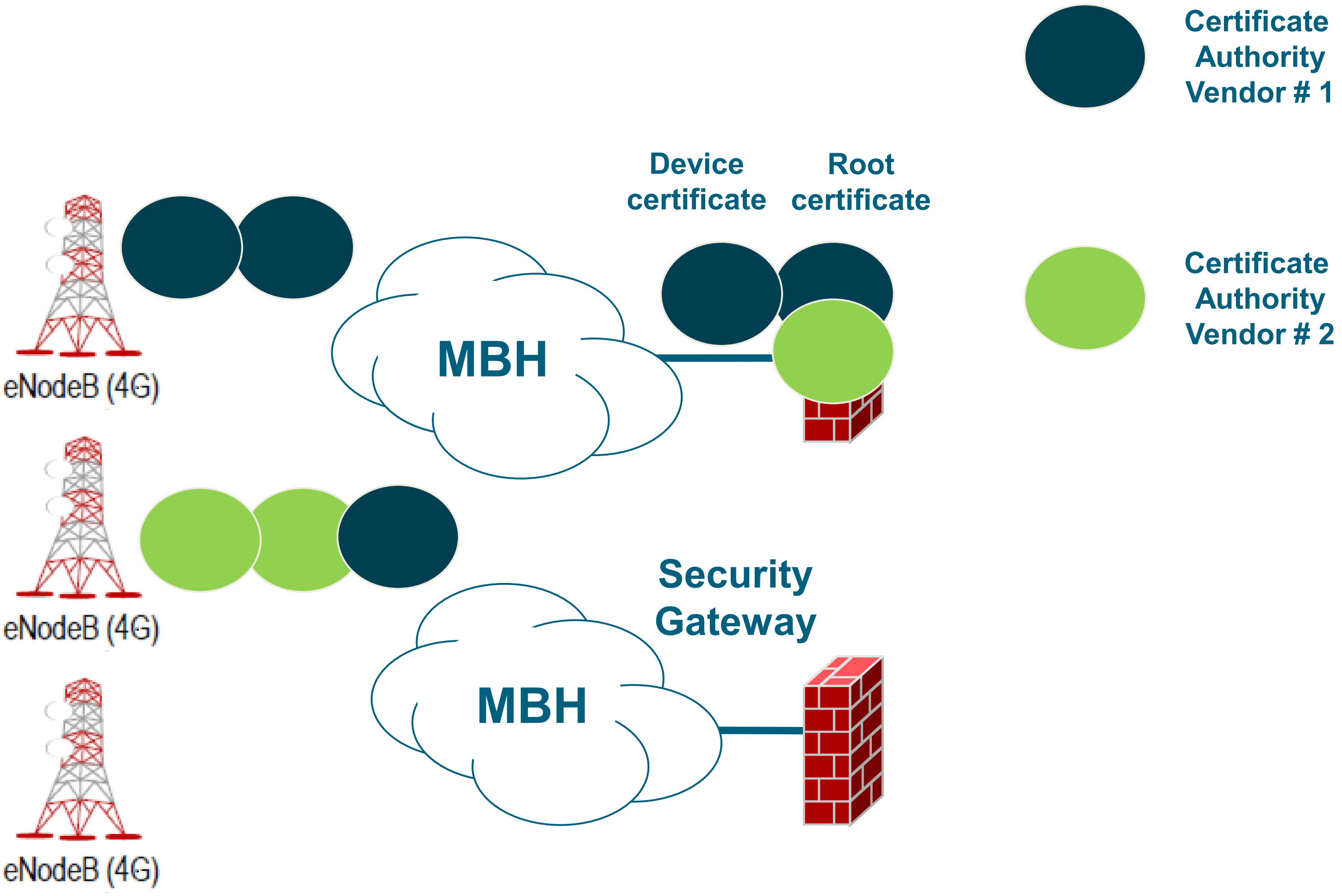
- **Certificates**



- **Certificates**



- **Certificates**



Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

Device certificate

Root certificate

MBH

MBH

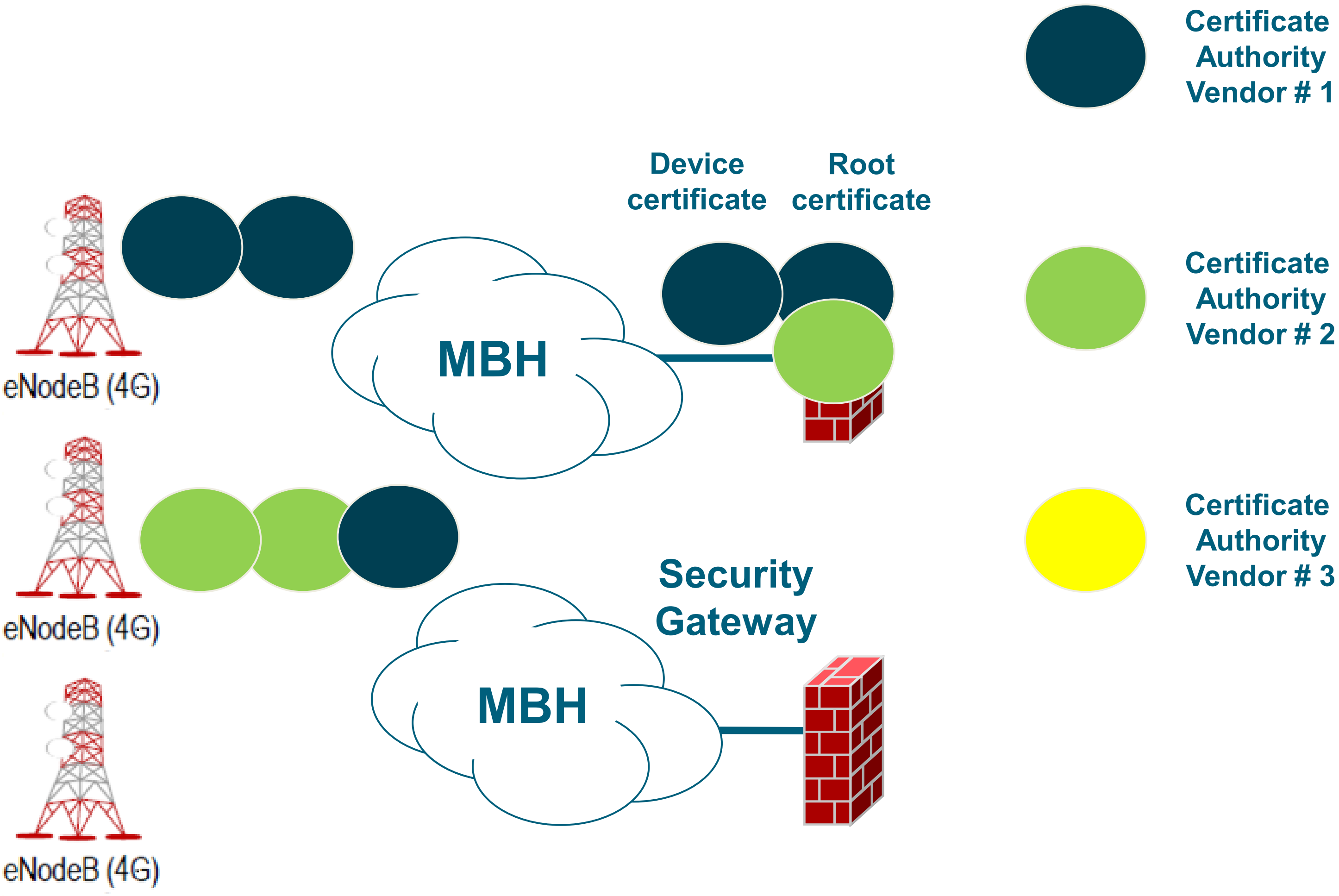
Security Gateway

eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

- **Certificates**



Device certificate

Root certificate

MBH

MBH

Security Gateway

eNodeB (4G)

eNodeB (4G)

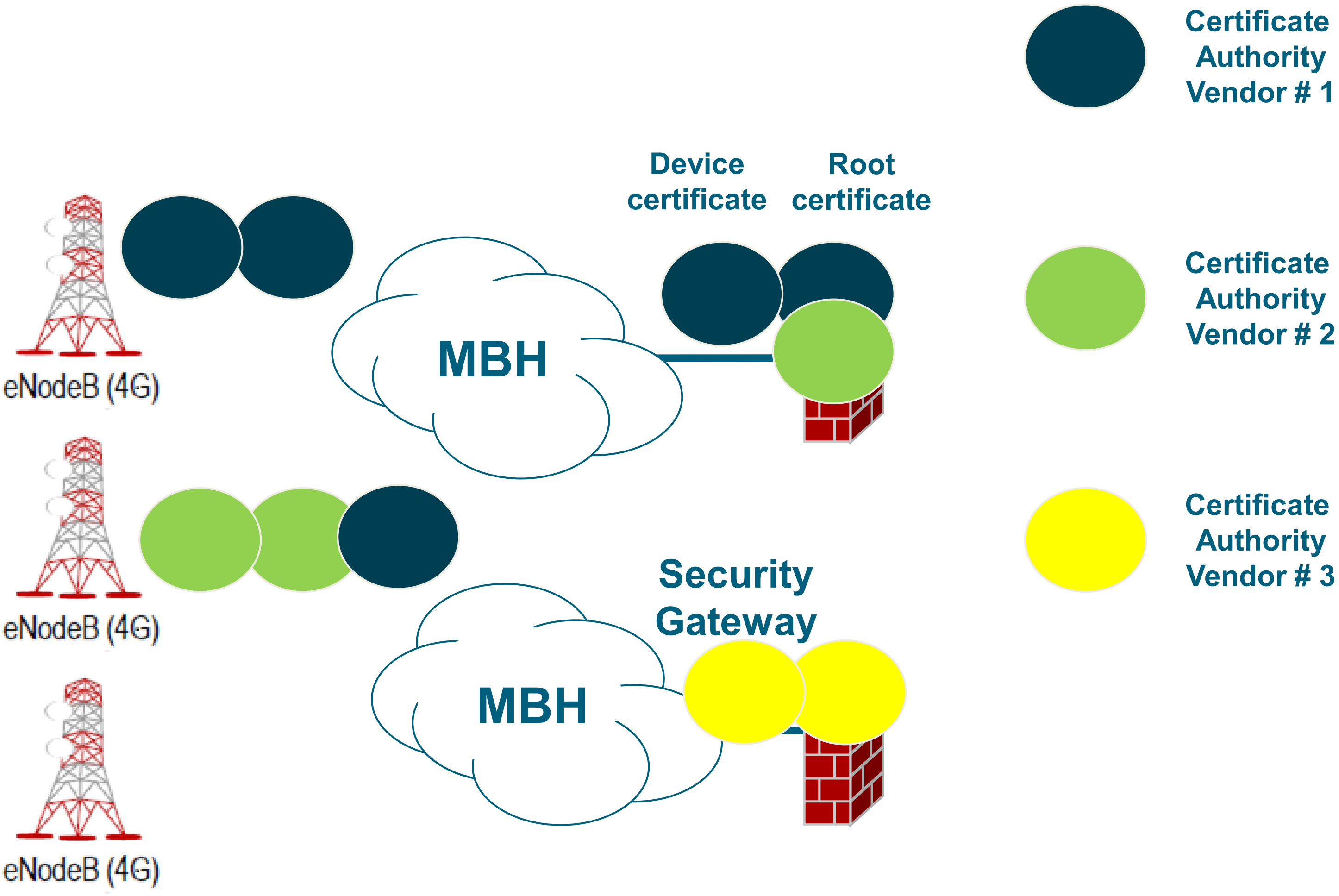
eNodeB (4G)

Certificate Authority Vendor # 1

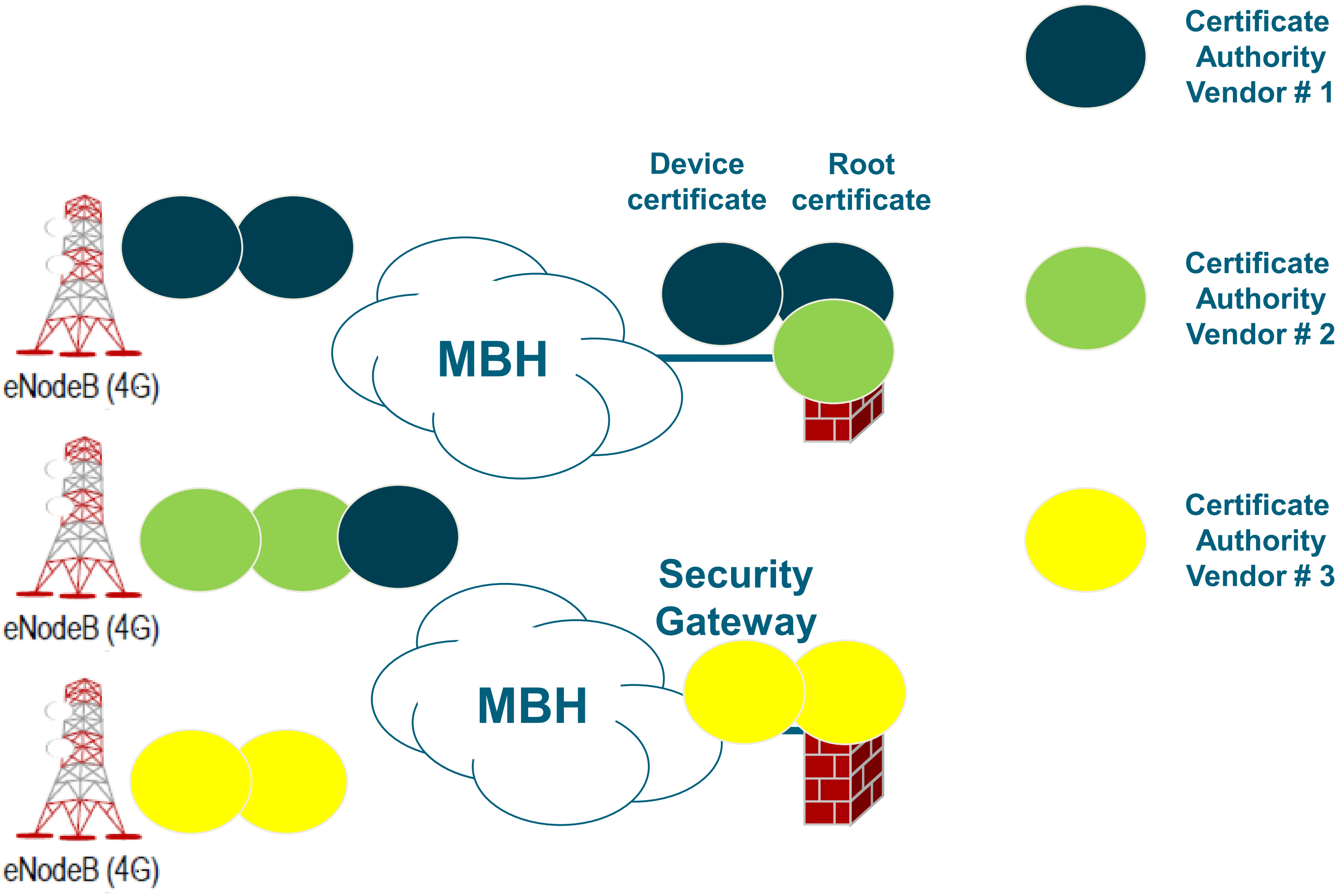
Certificate Authority Vendor # 2

Certificate Authority Vendor # 3

- **Certificates**


Certificate Authority Vendor # 1
Device certificate
Root certificate
Certificate Authority Vendor # 2
Certificate Authority Vendor # 3
eNodeB (4G)
MBH
eNodeB (4G)
Security Gateway
MBH
eNodeB (4G)

Certificates



Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

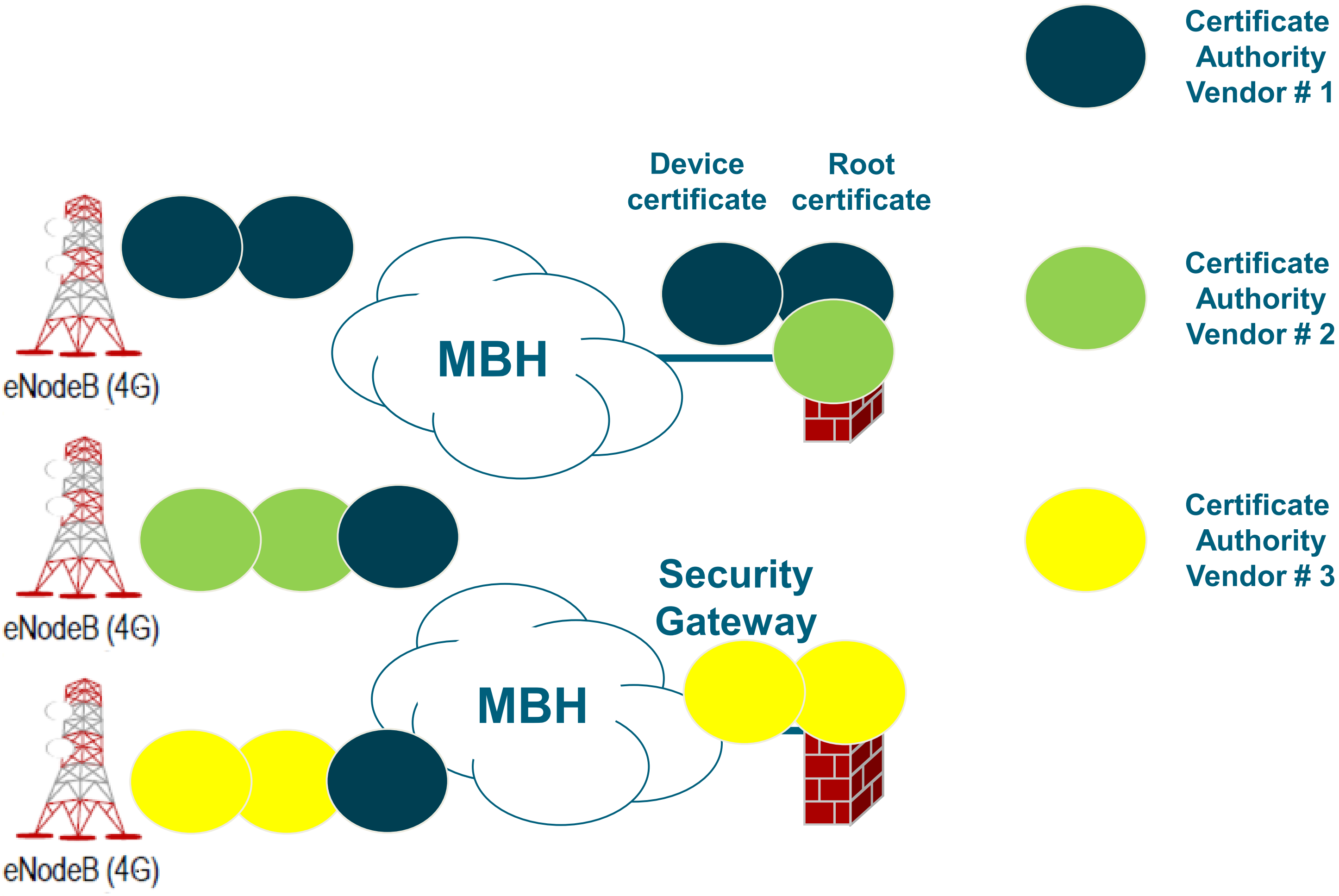
Certificate Authority Vendor # 3

Device certificate

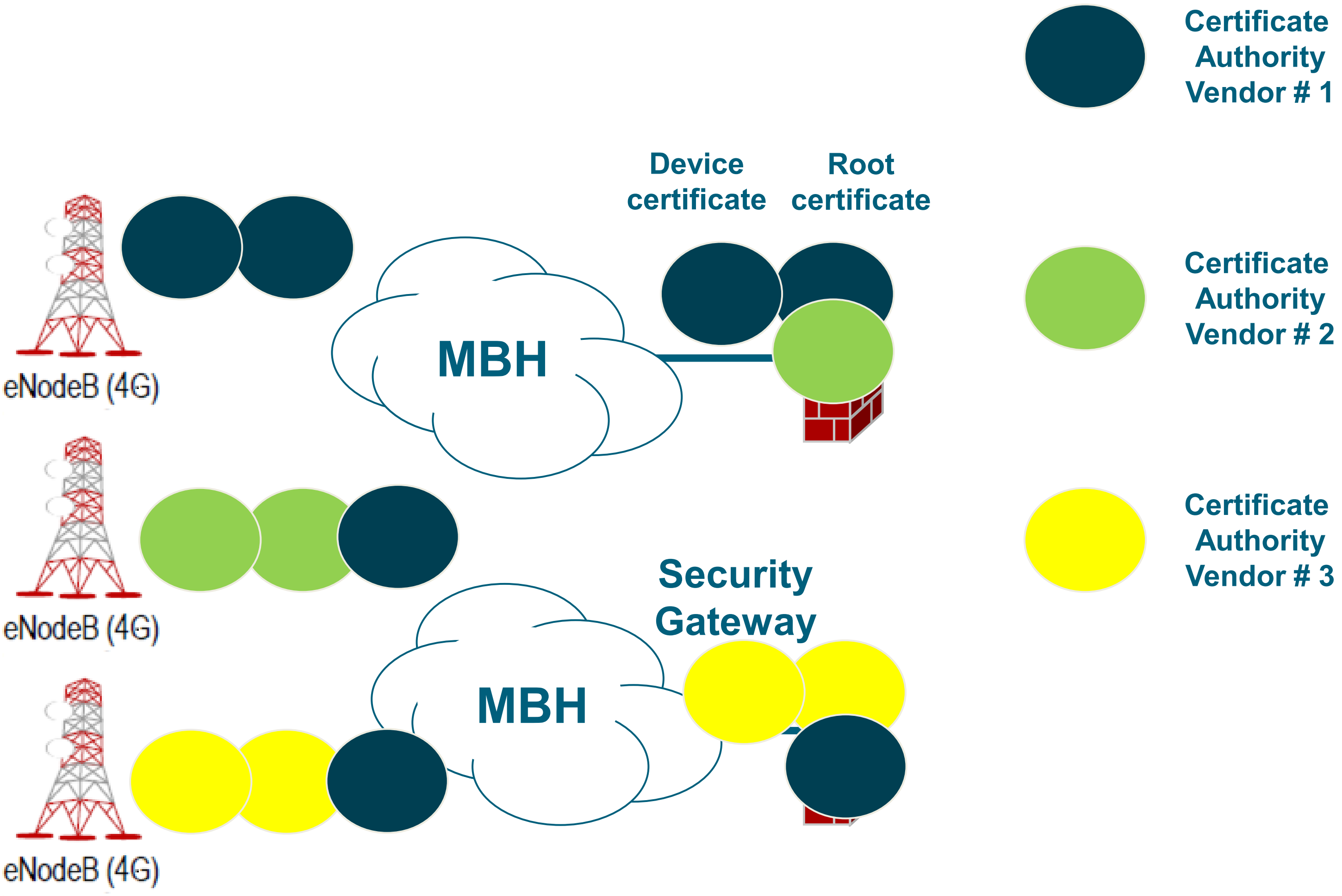
Root certificate

Security Gateway

- **Certificates**


Certificate Authority Vendor # 1
Certificate Authority Vendor # 2
Certificate Authority Vendor # 3
Device certificate
Root certificate
MBH
MBH
Security Gateway
eNodeB (4G)
eNodeB (4G)
eNodeB (4G)

- **Certificates**



Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

Certificate Authority Vendor # 3

Device certificate

Root certificate

MBH

MBH

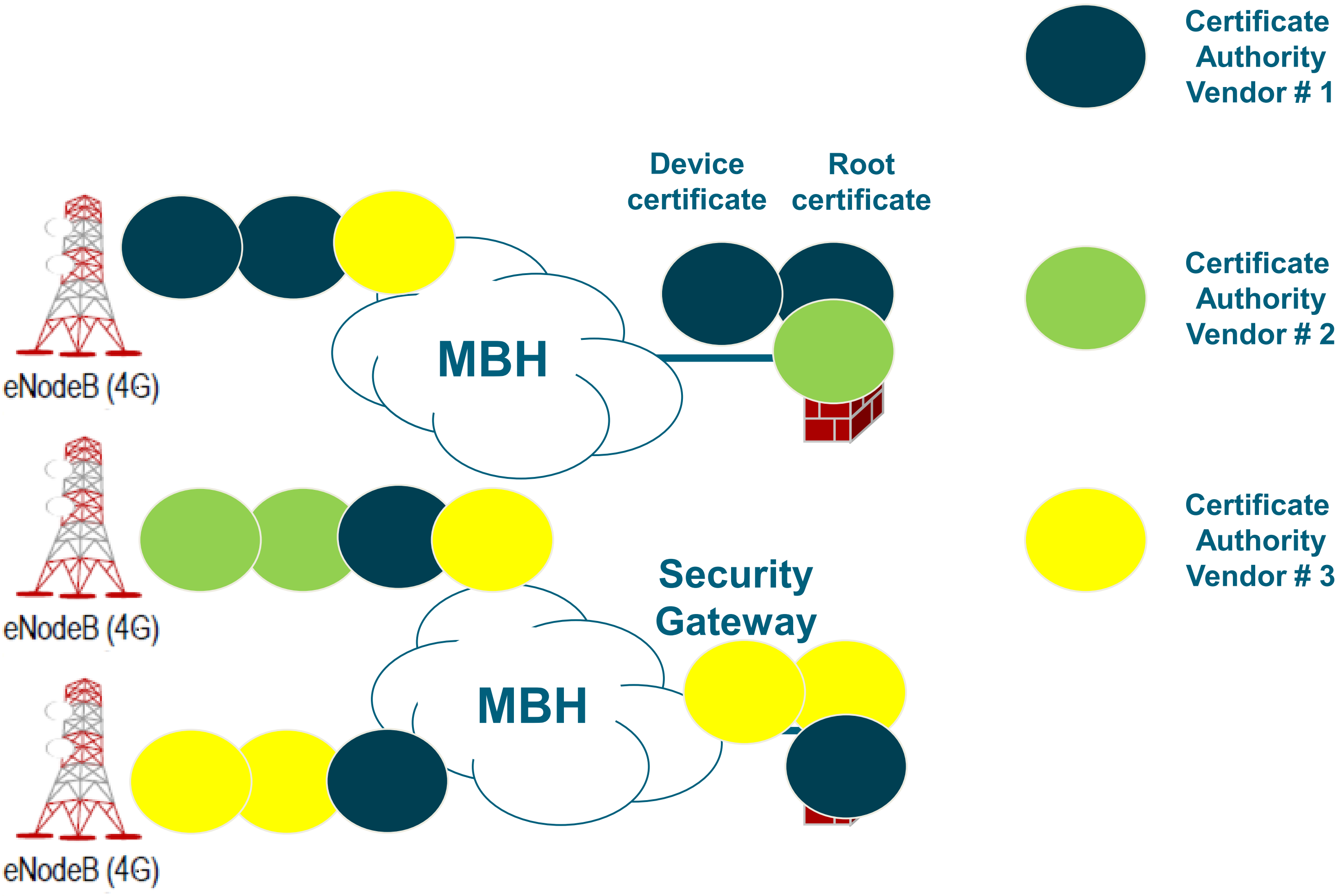
Security Gateway

eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

- **Certificates**



● Certificate Authority Vendor # 1

● Certificate Authority Vendor # 2

● Certificate Authority Vendor # 3

Device certificate

Root certificate

Security Gateway

MBH

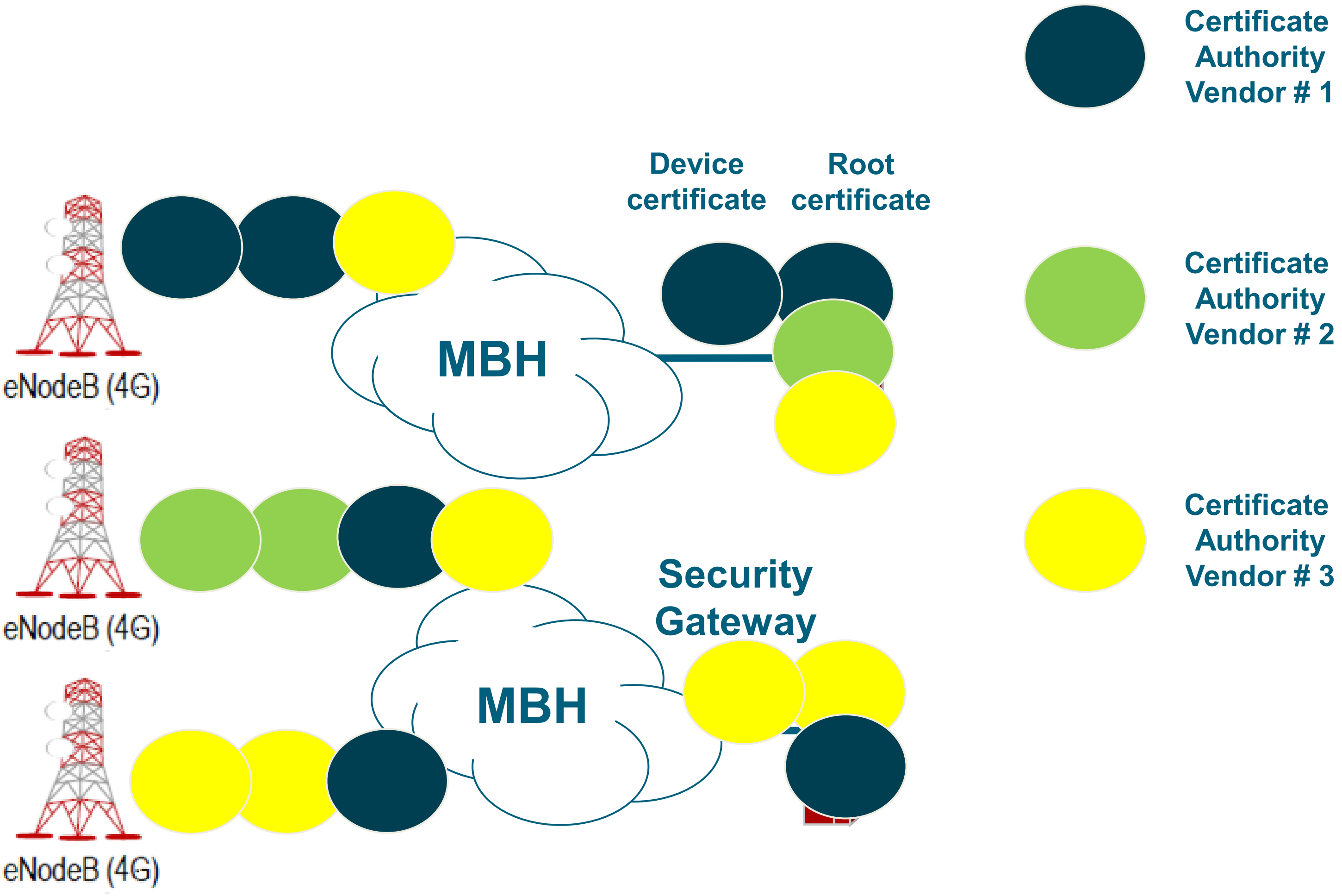
MBH

eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

- **Certificates**



Device certificate

Root certificate

MBH

MBH

Security Gateway

eNodeB (4G)

eNodeB (4G)

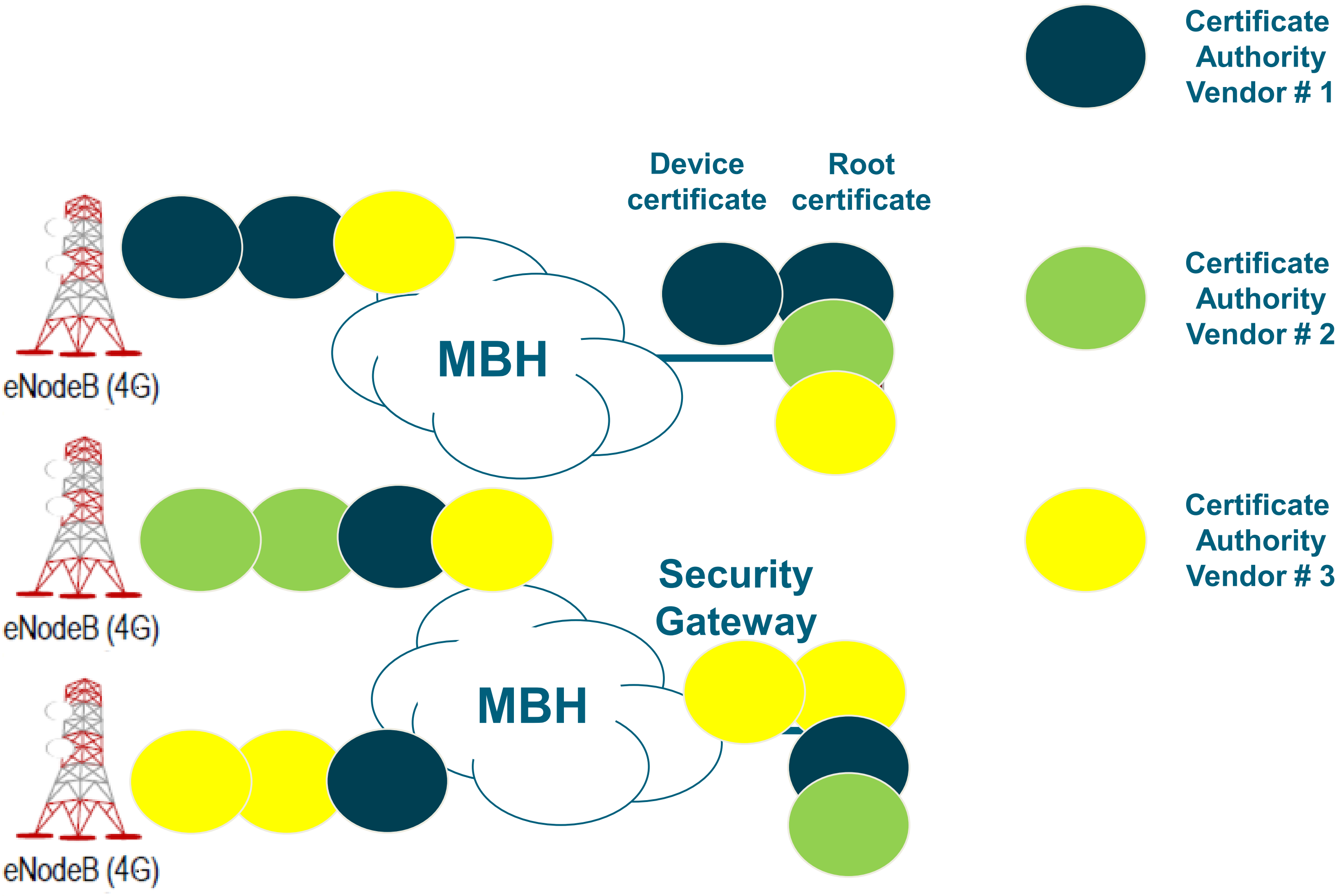
eNodeB (4G)

Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

Certificate Authority Vendor # 3

- **Certificates**



Device certificate

Root certificate

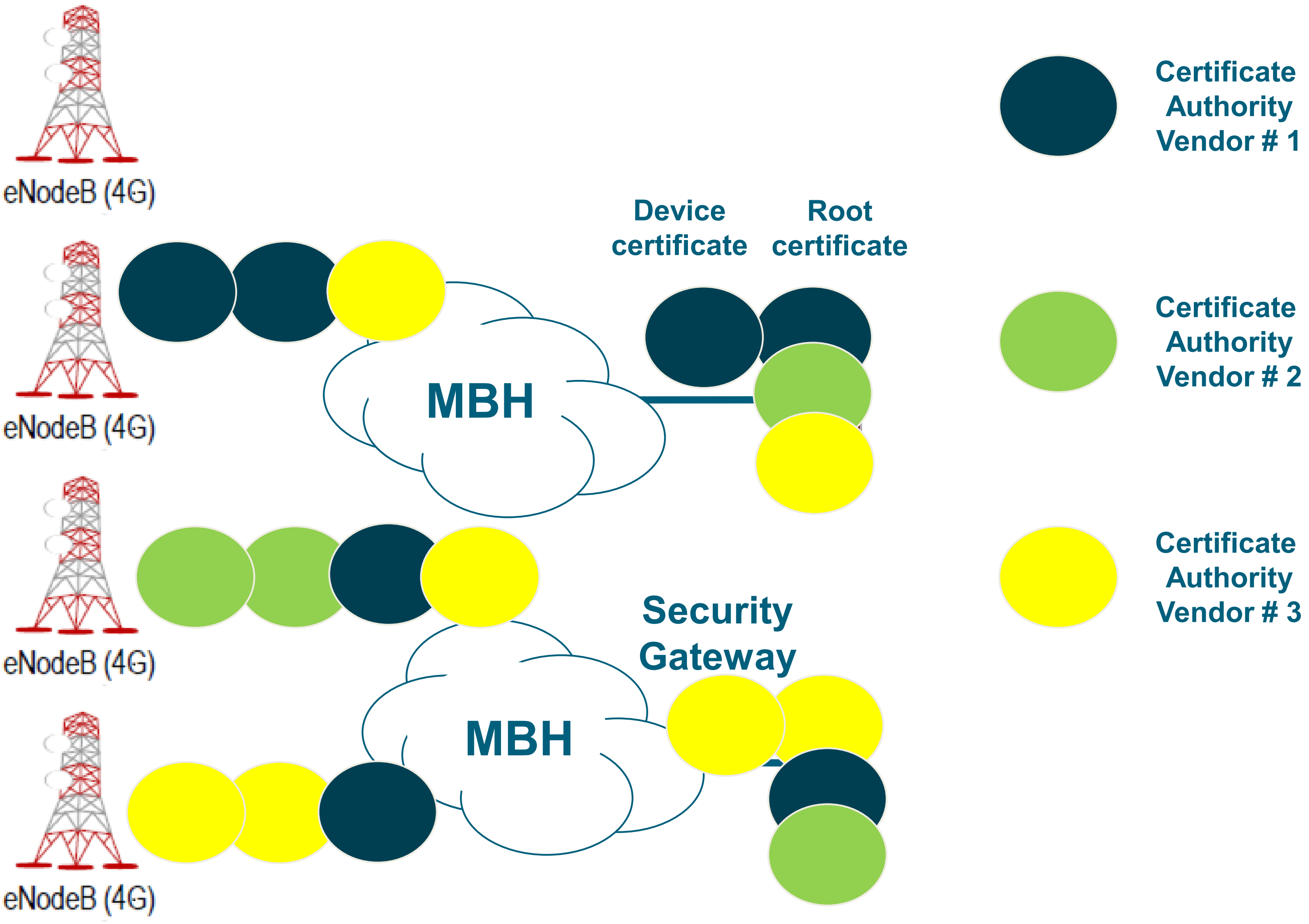
Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

Certificate Authority Vendor # 3

Security Gateway

- **Certificates**



eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

MBH

MBH

Device certificate

Root certificate

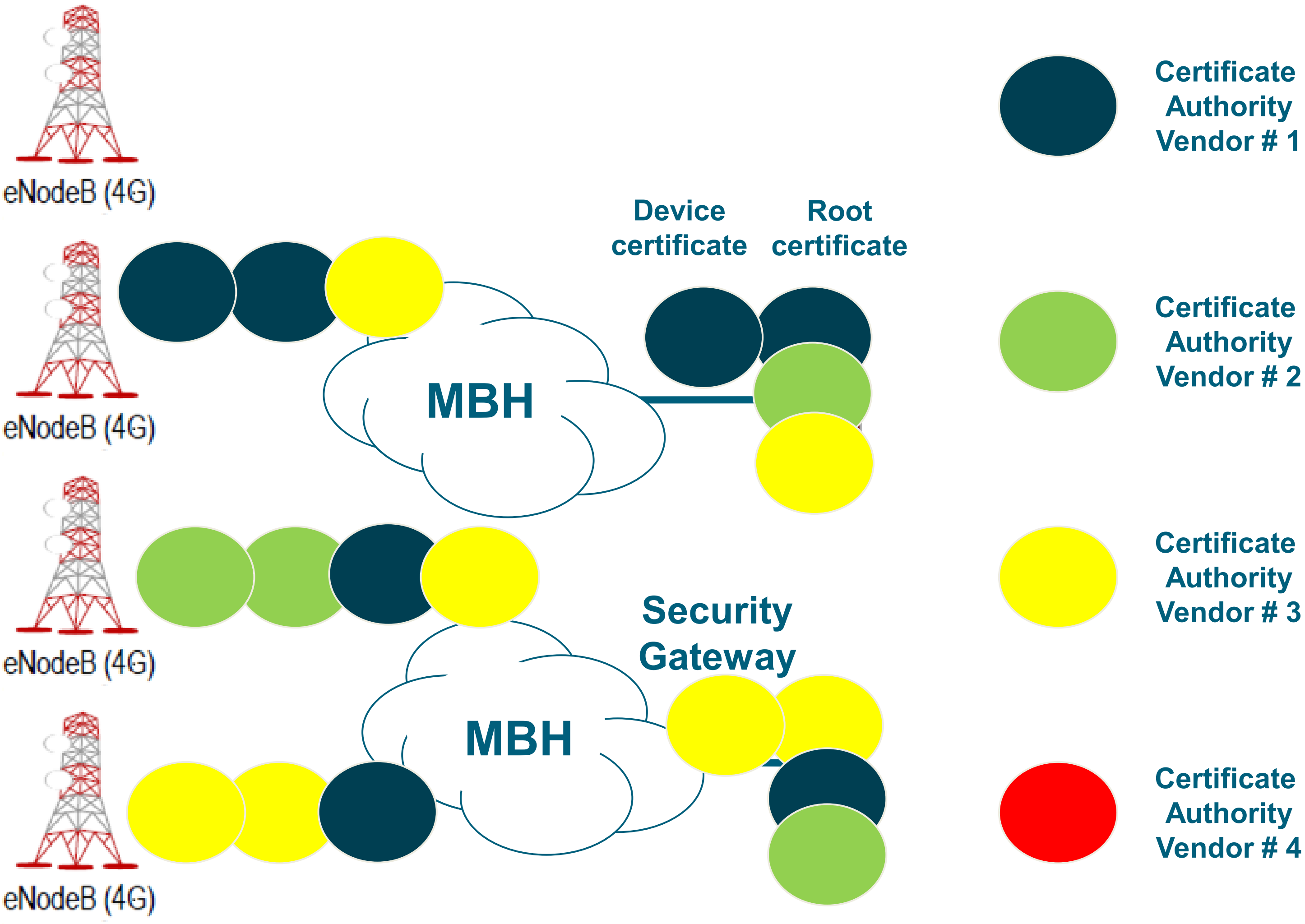
Security Gateway

Certificate Authority Vendor # 1

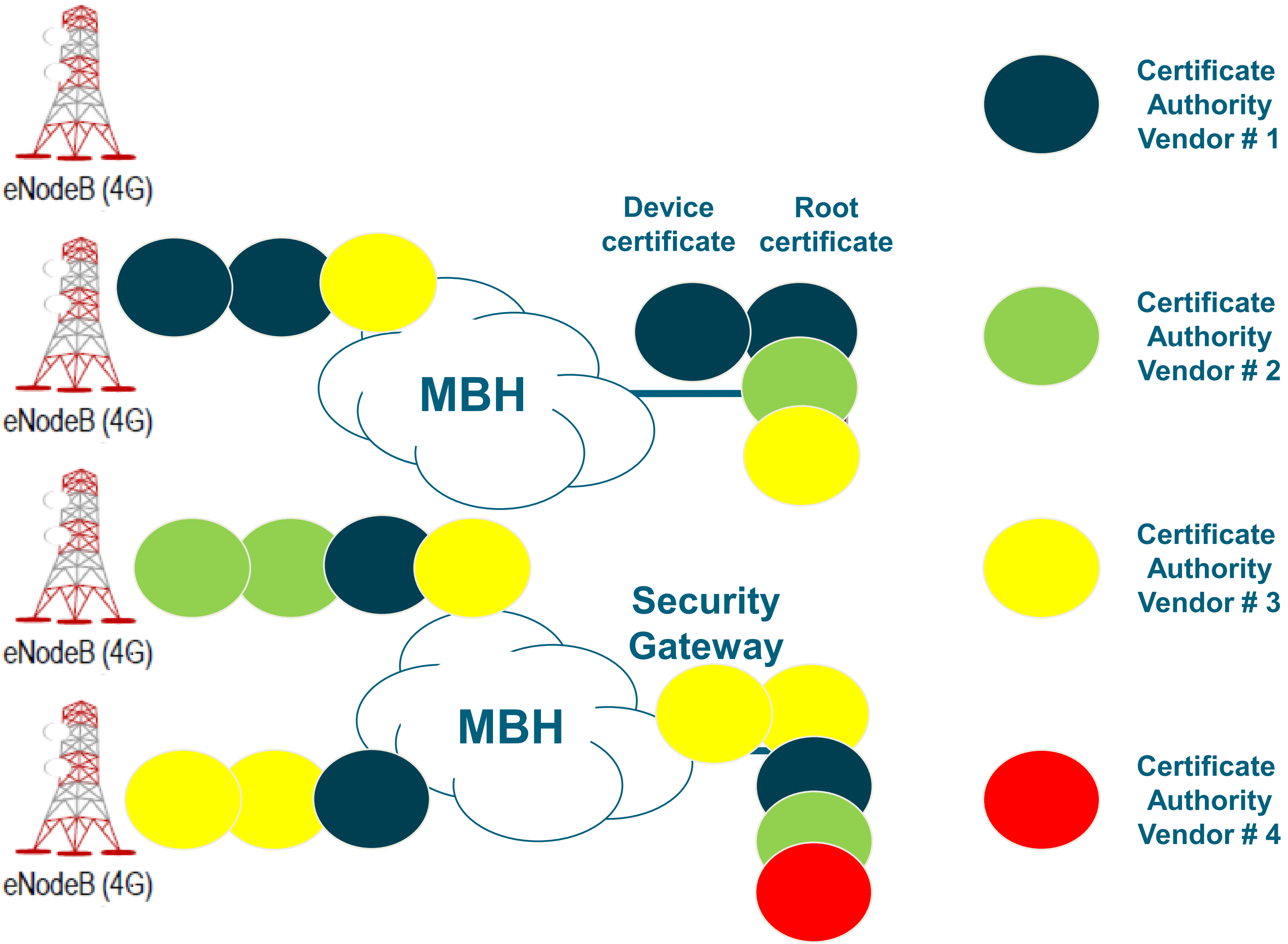
Certificate Authority Vendor # 2

Certificate Authority Vendor # 3

- **Certificates**


eNodeB (4G)
eNodeB (4G)
eNodeB (4G)
eNodeB (4G)
MBH
MBH
Device certificate
Root certificate
Security Gateway
Certificate Authority Vendor # 1
Certificate Authority Vendor # 2
Certificate Authority Vendor # 3
Certificate Authority Vendor # 4

- **Certificates**



eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

MBH

MBH

Device certificate

Root certificate

Security Gateway

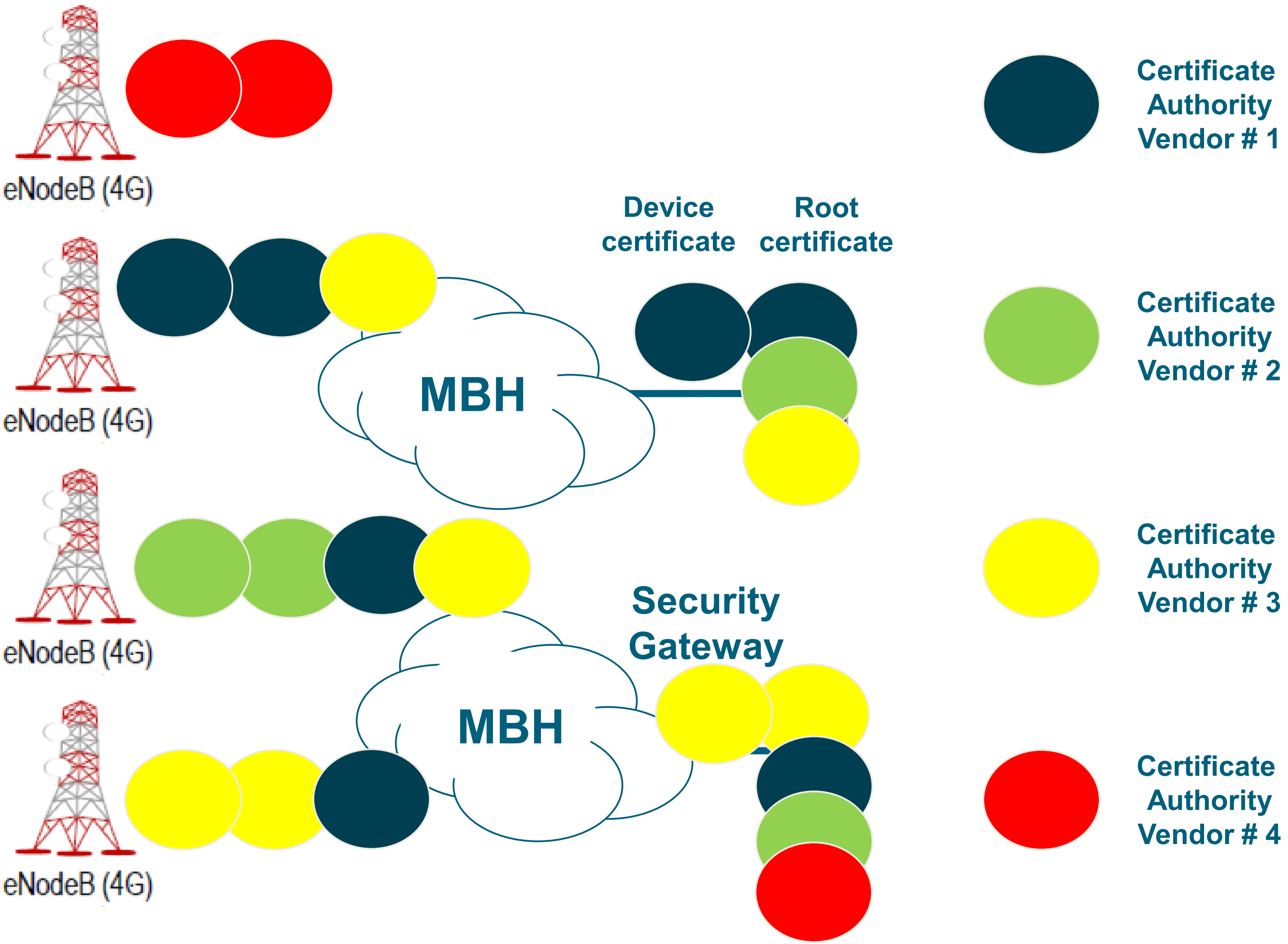
Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

Certificate Authority Vendor # 3

Certificate Authority Vendor # 4

- **Certificates**



eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

MBH

MBH

Device certificate

Root certificate

Security Gateway

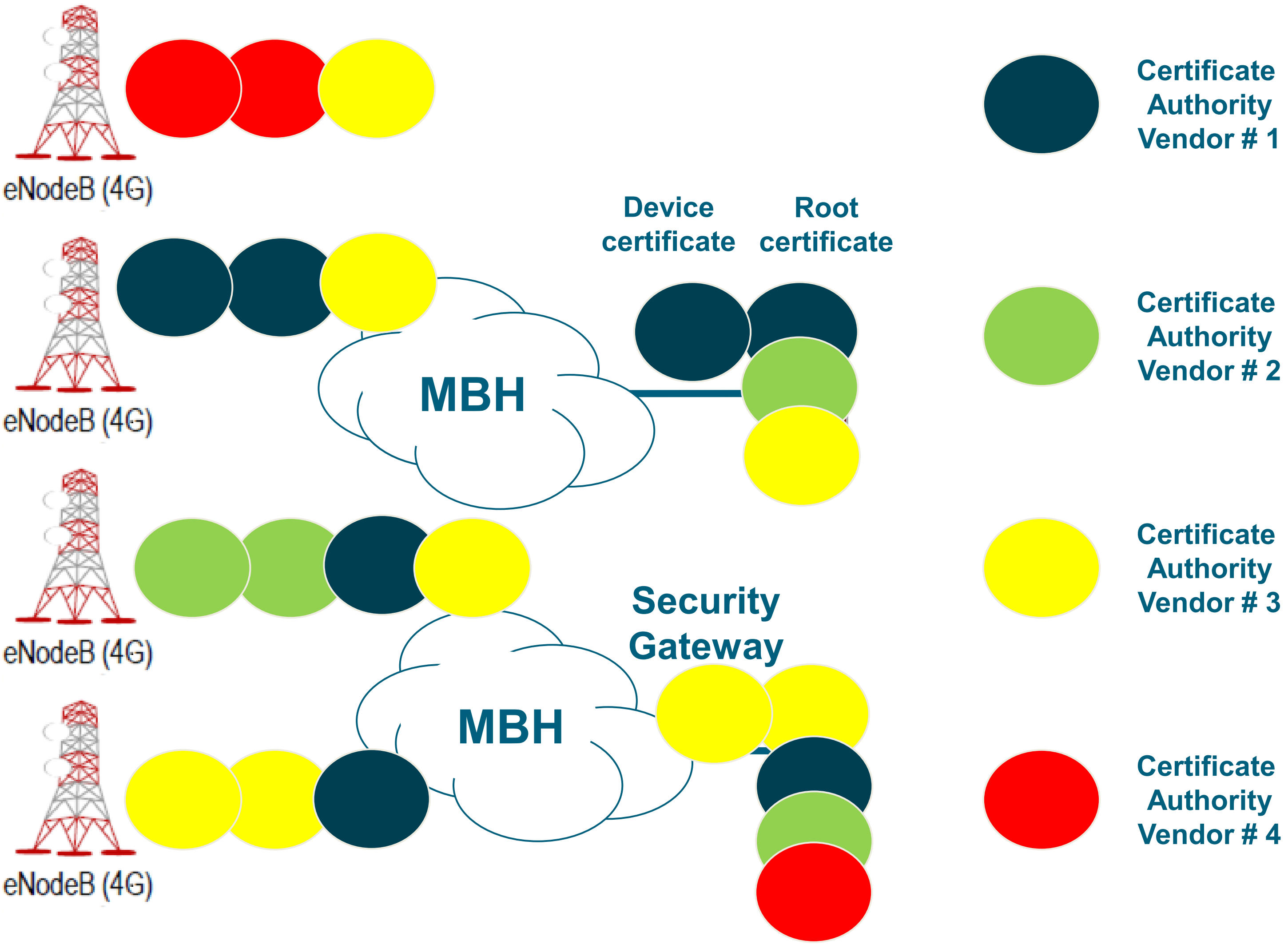
Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

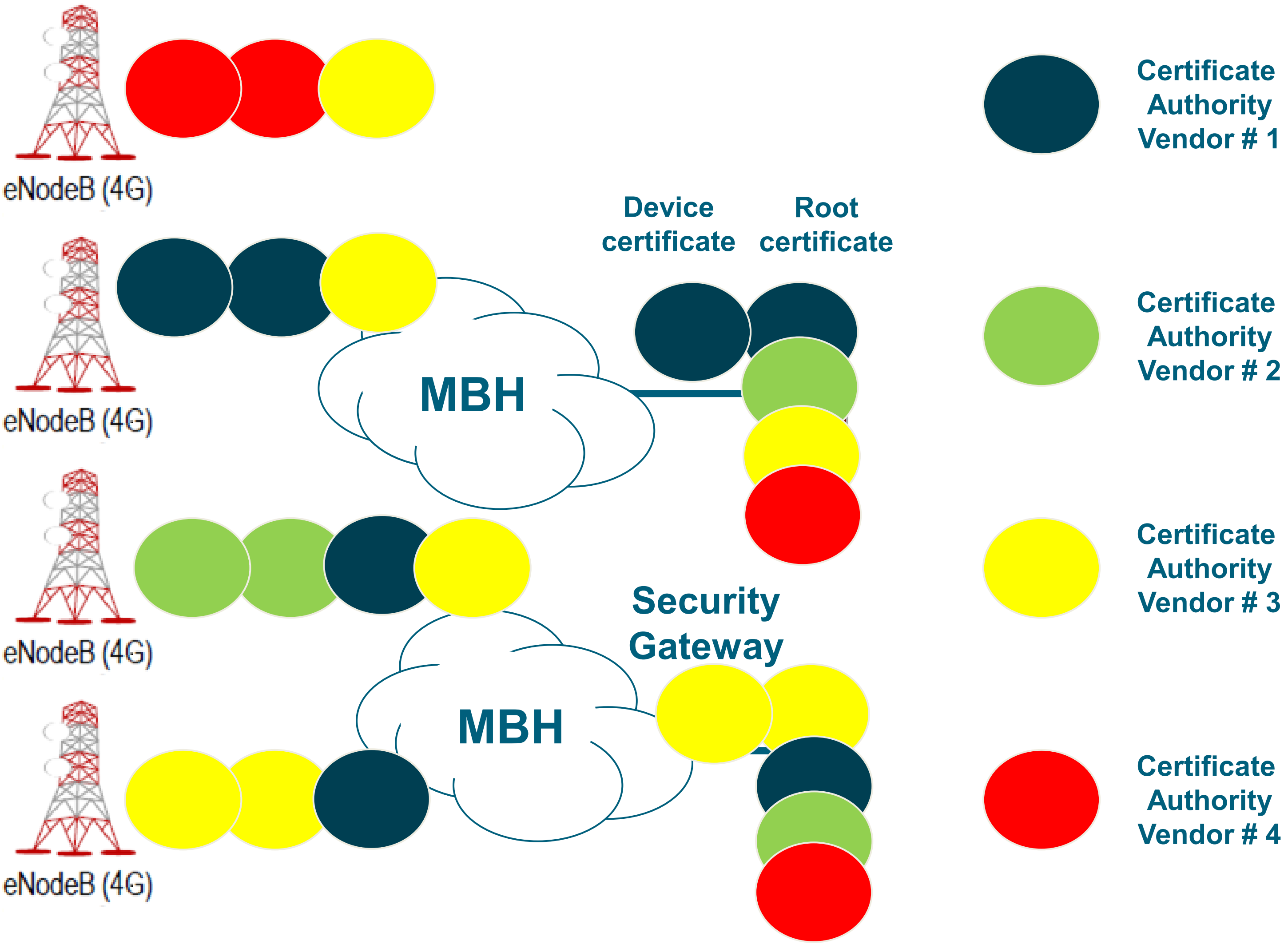
Certificate Authority Vendor # 3

Certificate Authority Vendor # 4

- **Certificates**


eNodeB (4G)
eNodeB (4G)
eNodeB (4G)
eNodeB (4G)
MBH
MBH
Device certificate
Root certificate
Security Gateway
Certificate Authority Vendor # 1
Certificate Authority Vendor # 2
Certificate Authority Vendor # 3
Certificate Authority Vendor # 4

- **Certificates**



eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

MBH

MBH

Device certificate

Root certificate

Security Gateway

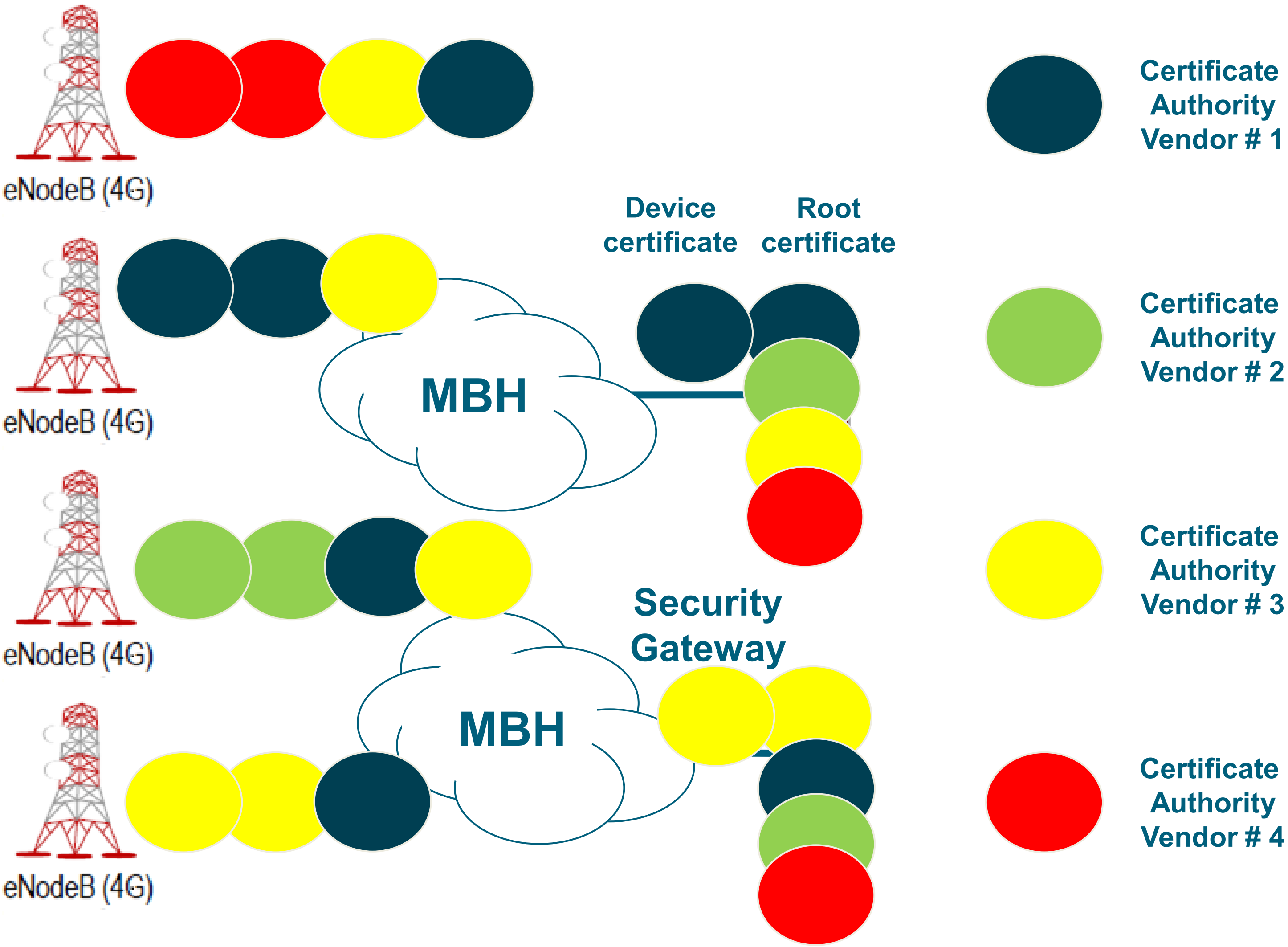
Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

Certificate Authority Vendor # 3

Certificate Authority Vendor # 4

- **Certificates**



eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

eNodeB (4G)

MBH

MBH

Device certificate

Root certificate

Security Gateway

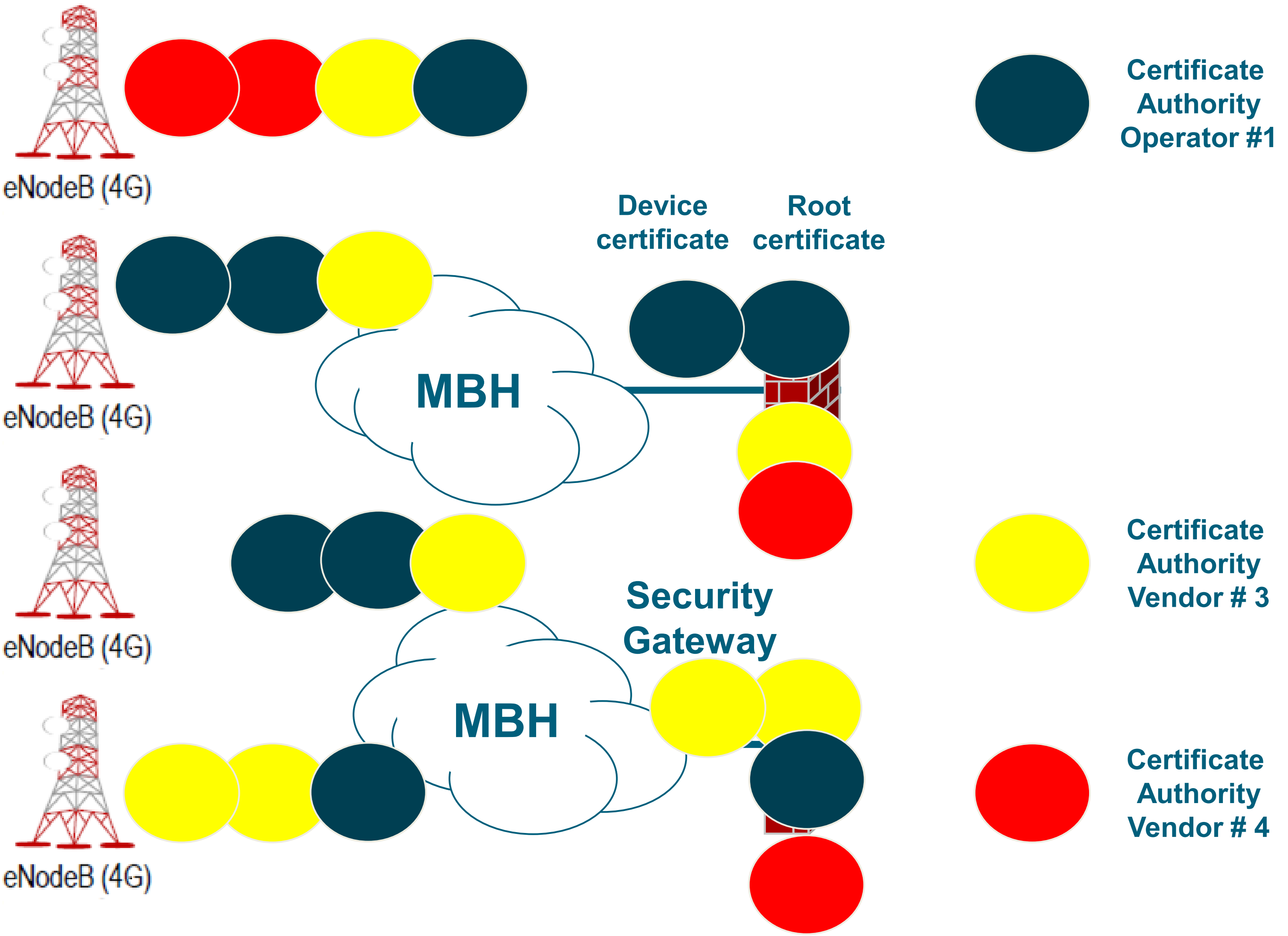
Certificate Authority Vendor # 1

Certificate Authority Vendor # 2

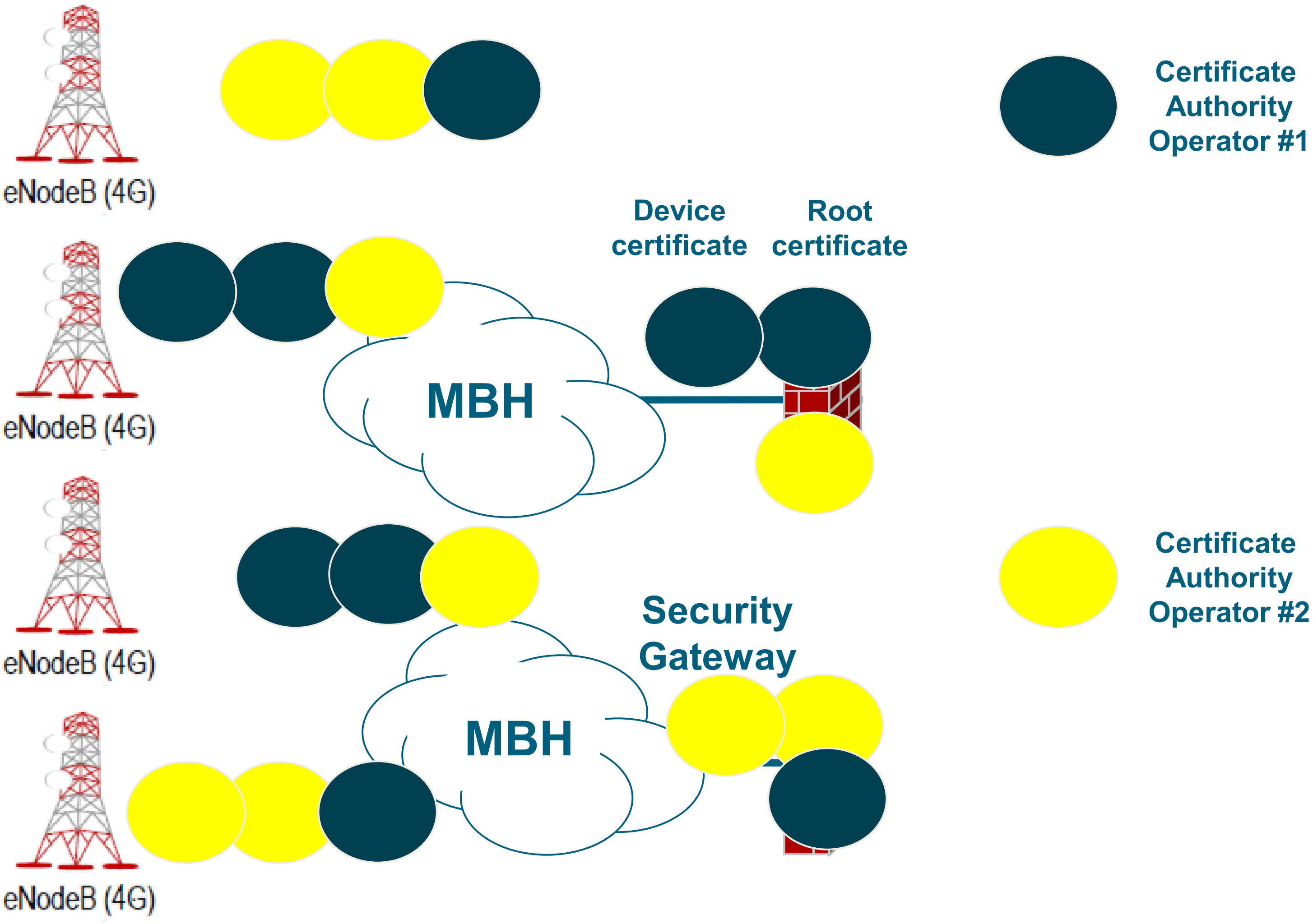
Certificate Authority Vendor # 3

Certificate Authority Vendor # 4

- **Certificates**



- **Certificates**

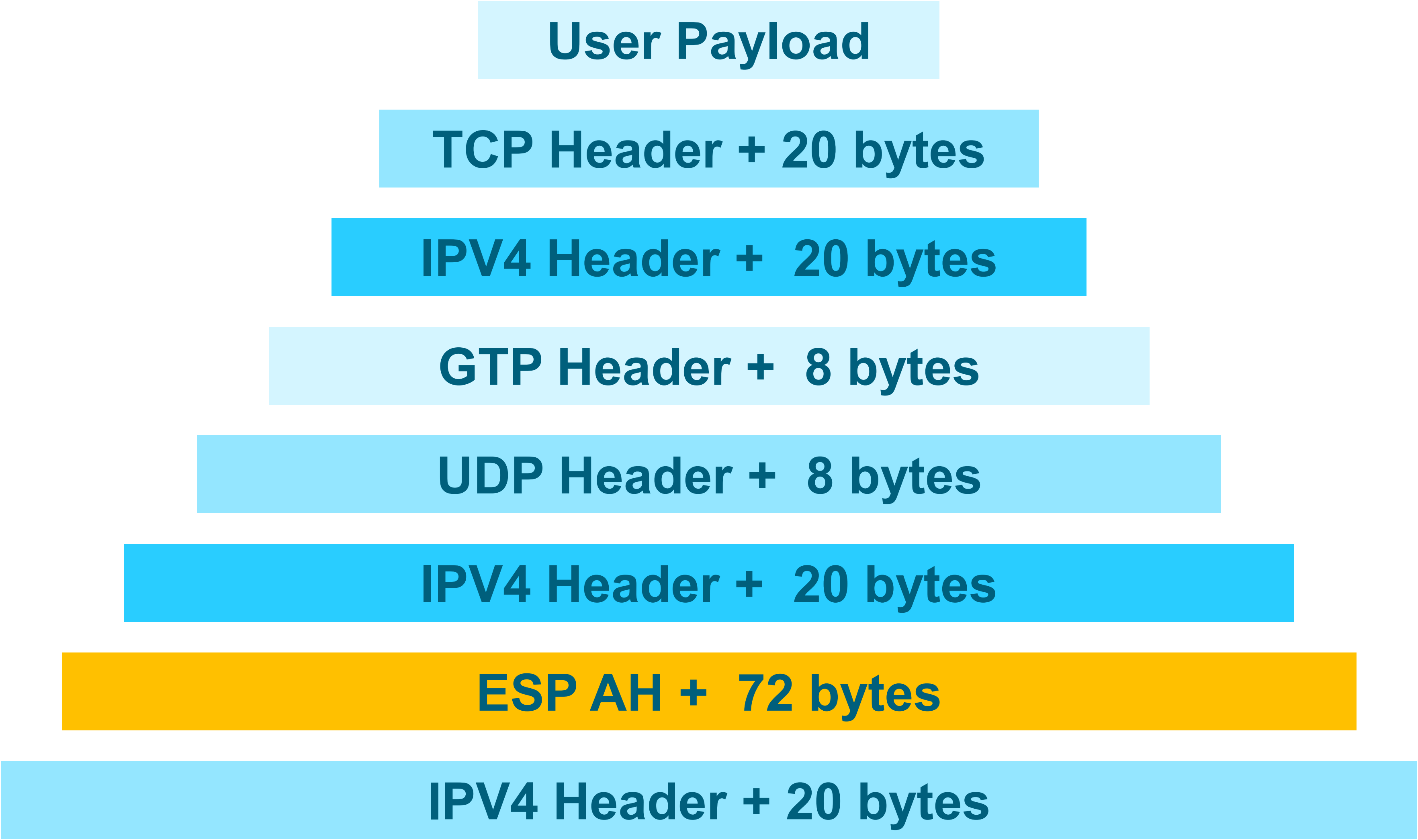


03

MTU Size

MTU Size

- Ethernet MTU is 1500bytes
- IPSec overhead can be as large as 72bytes
- If your Carrier Ethernet solution can support Jumbo frames or Baby Jumbo’s (1700) then you are OK



User Payload

TCP Header + 20 bytes

IPV4 Header + 20 bytes

GTP Header + 8 bytes

UDP Header + 8 bytes

IPV4 Header + 20 bytes

ESP AH + 72 bytes

IPV4 Header + 20 bytes

MTU Size

- Ethernet MTU is 1500
- Outer IP Header = 20 bytes (1500-20 = 1480)
- ESP Overhead Total = 72 bytes (1480-72 = 1408)
- Inner IP Header = 20 bytes (1408-20 = 1388)
- Fragmentation requirement 1388 (modulus 8) = 1384)
- Padding so IP packet modulus 16 = 1384 + 20 (modulus16) = 12

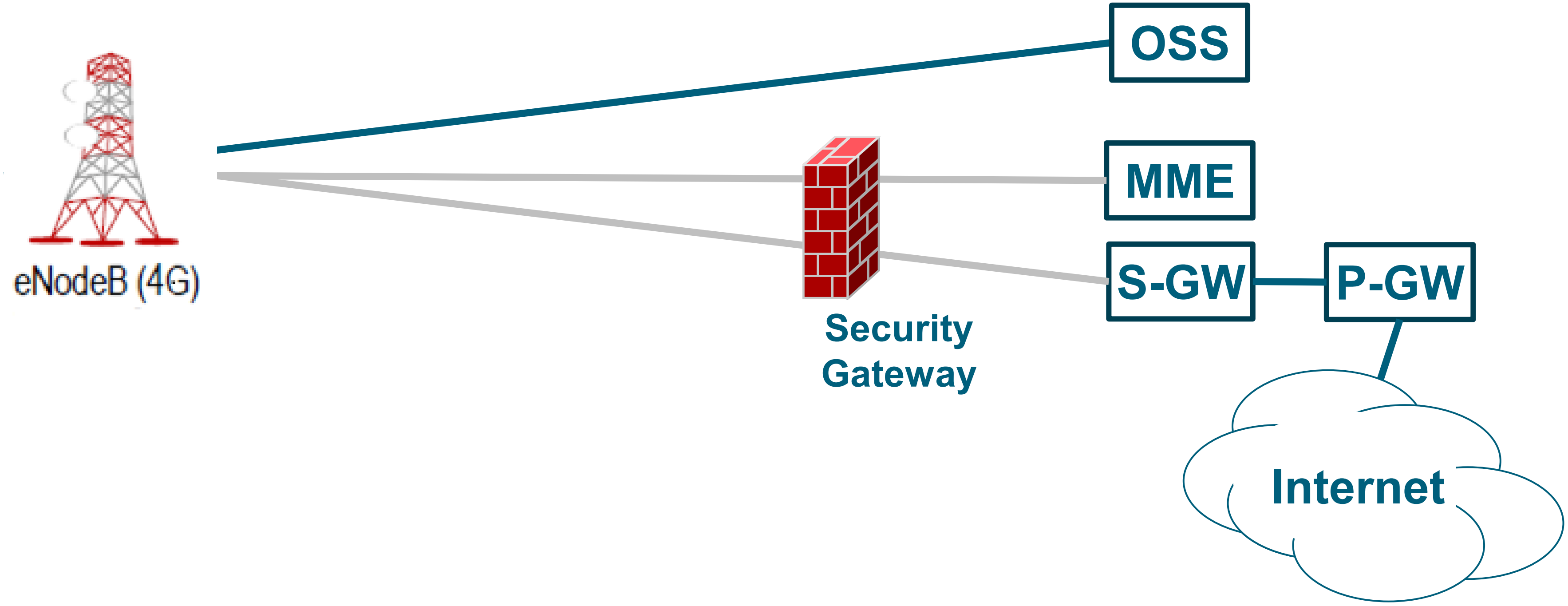
  16-12 = 4, 1384+20+4=1408
- UDP Header = 8 bytes (1384-8 = 1376)
- GTP-U Header = 8 bytes (1376-8 = 1368)
- User IP Header = 20 bytes (1368-20 = 1348)
- Padding so IP packet modulus 16 = 1348 + 20 (modulus16) = 8

  16-8 = 8, 1348-8 = 1340
- TCP Header = 20 bytes (1340-20 = 1320)

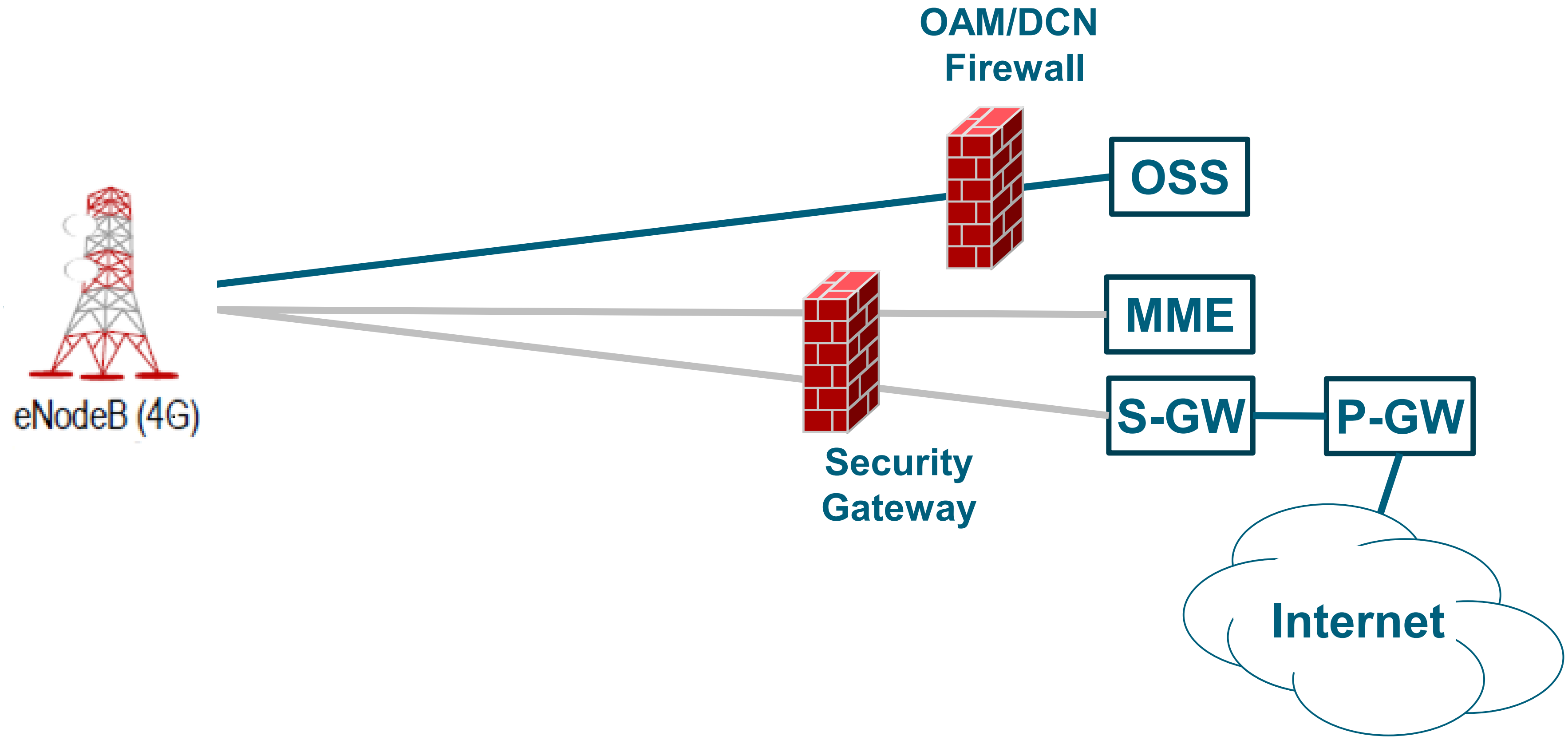
- **MTU Size**
  - Pre-fragmentation of IP packets ahead of IPSec encryption is a good idea where eNodeB does not support re-assembly of encrypted packets

04

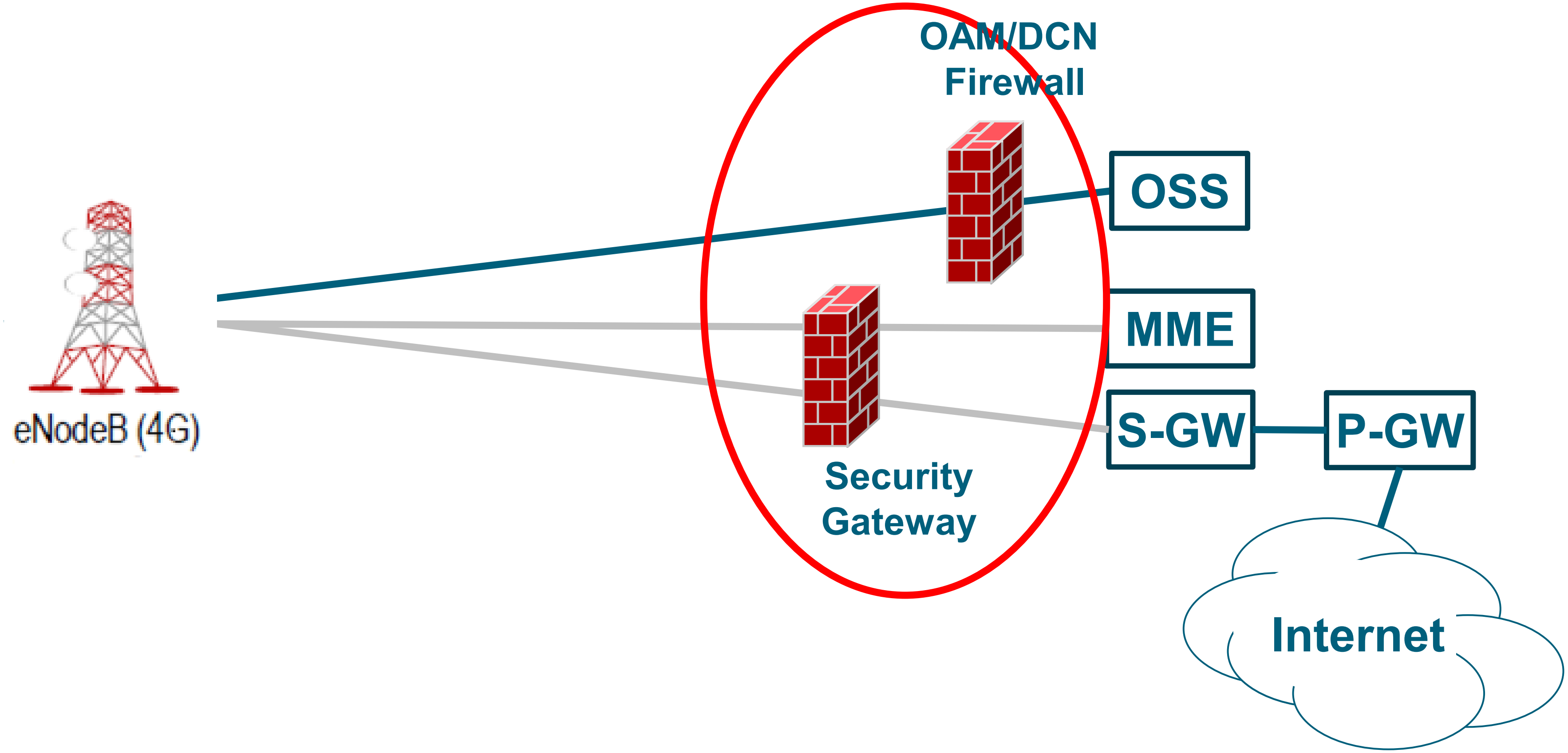
Auto-Integration



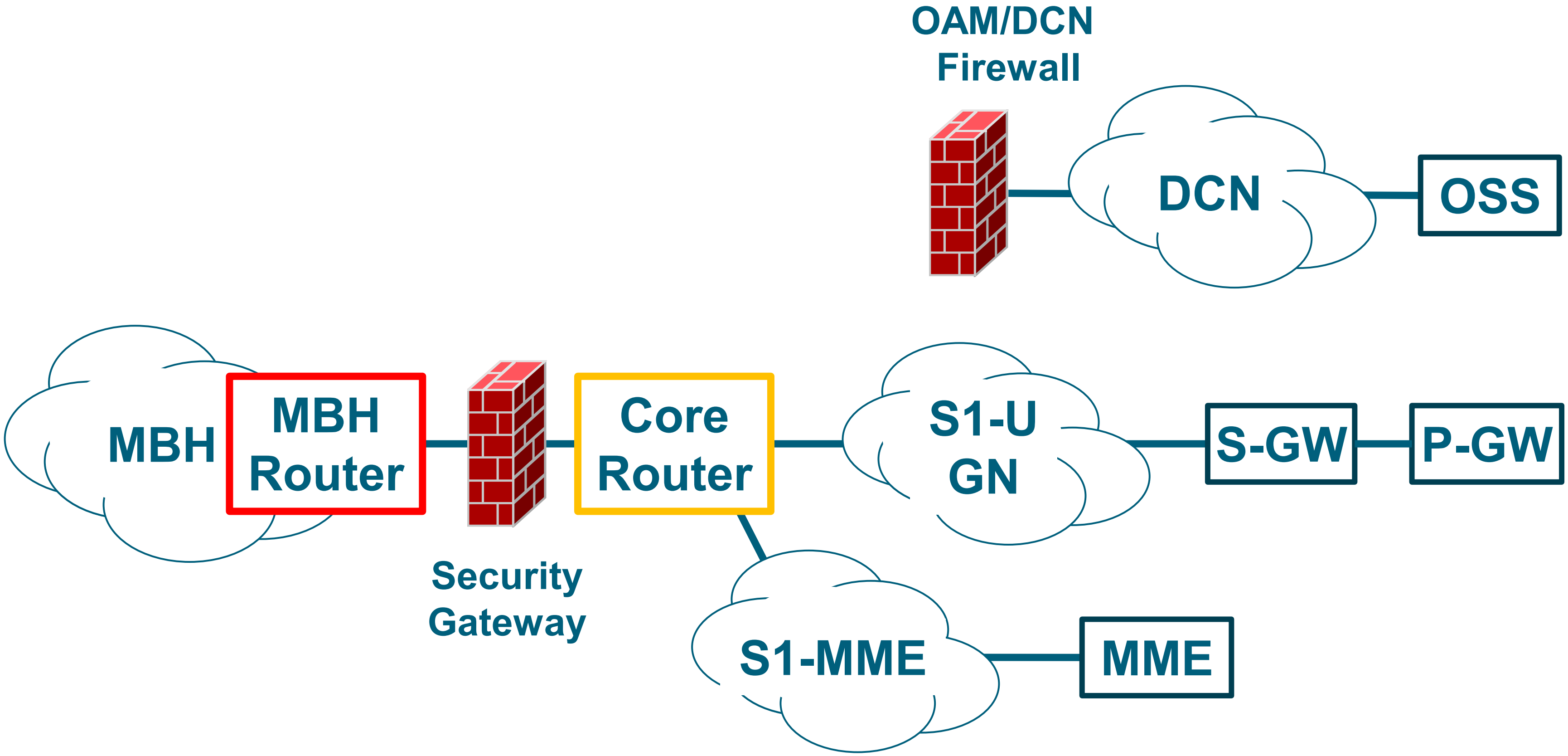
- How are you going to commission eNodeBs on industrial scale?



- **How are you going to commission eNodeBs on industrial scale?**

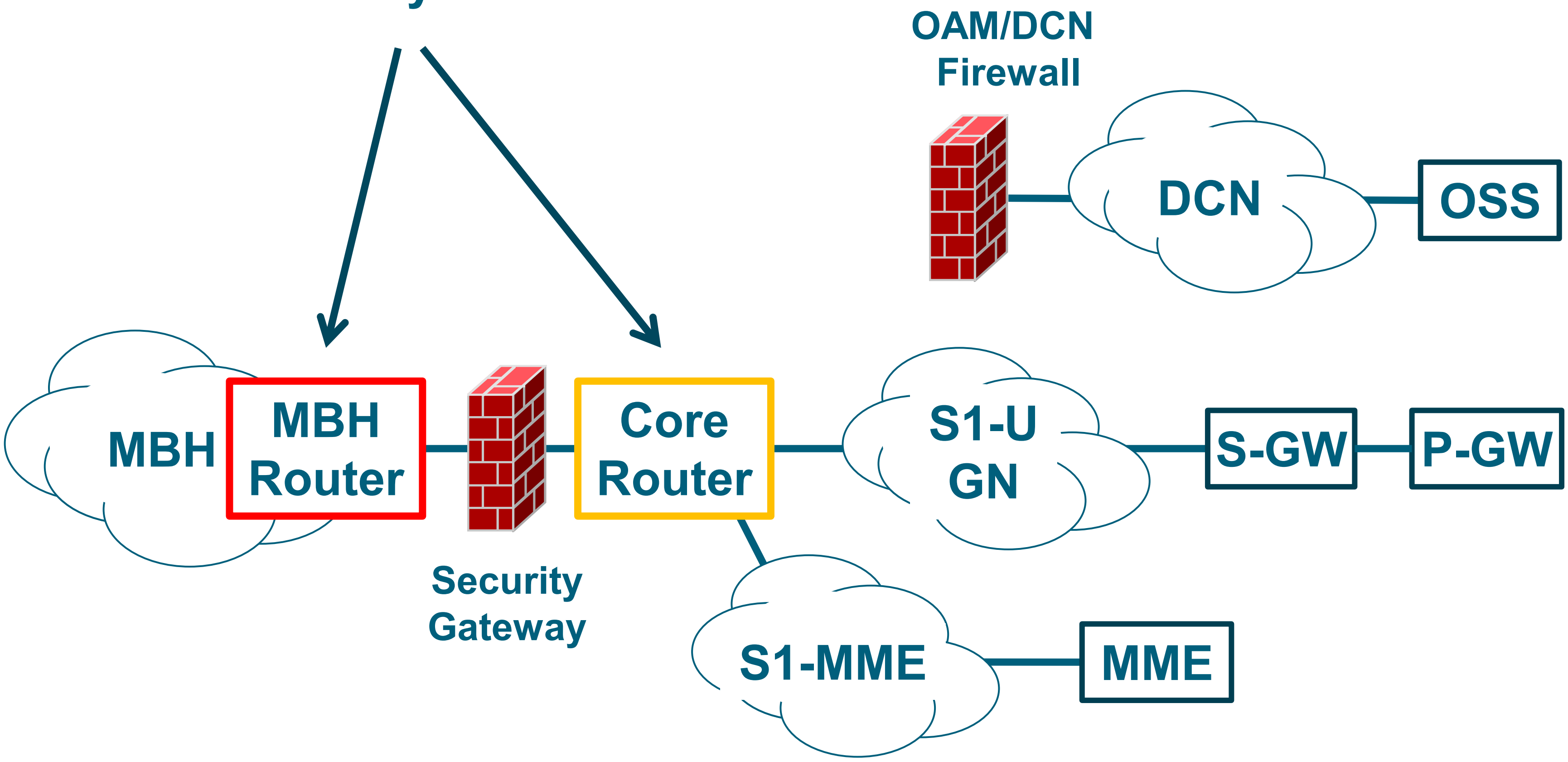


- How are you going to commission eNodeBs on industrial scale?

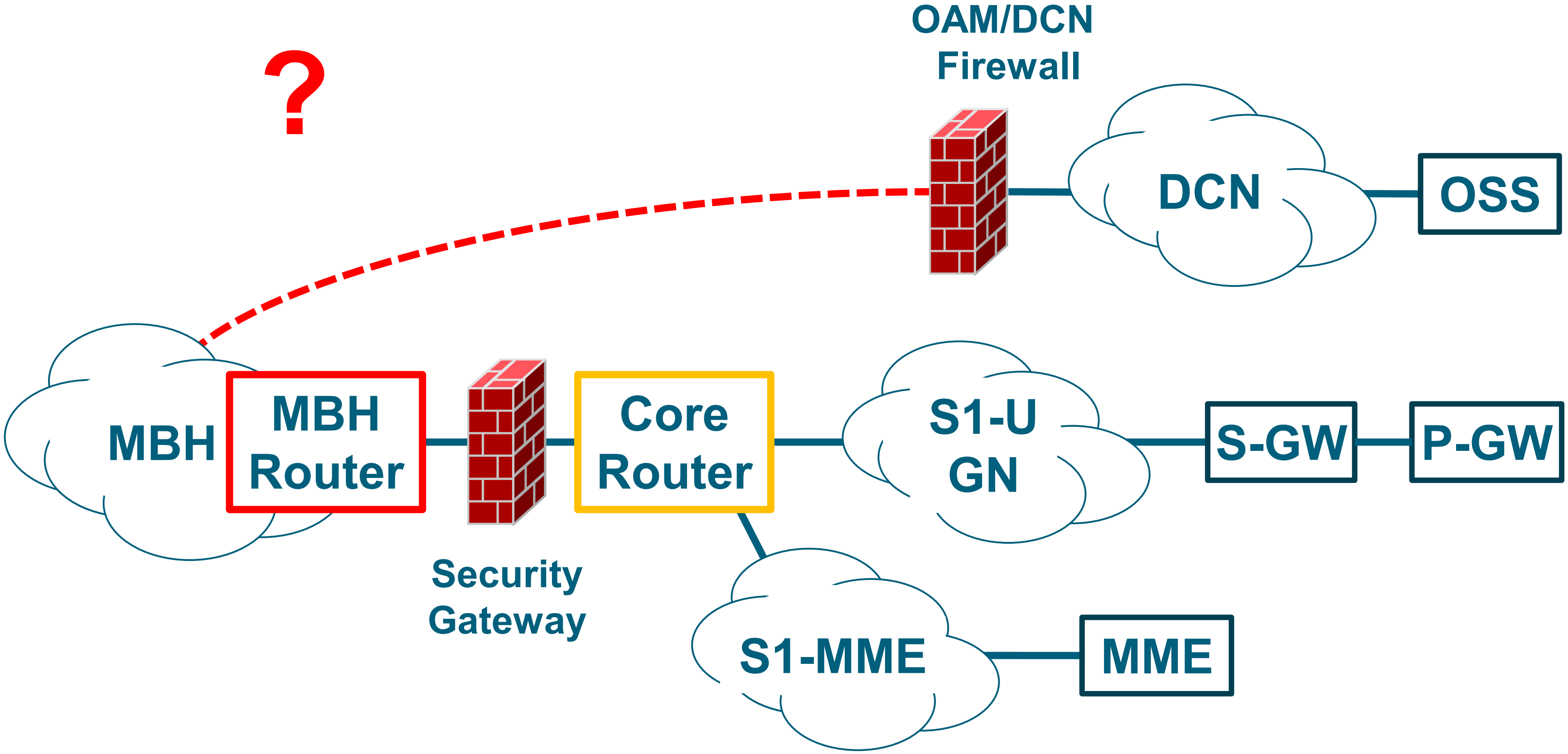


- How are you going to create a clean and secure Architecture?

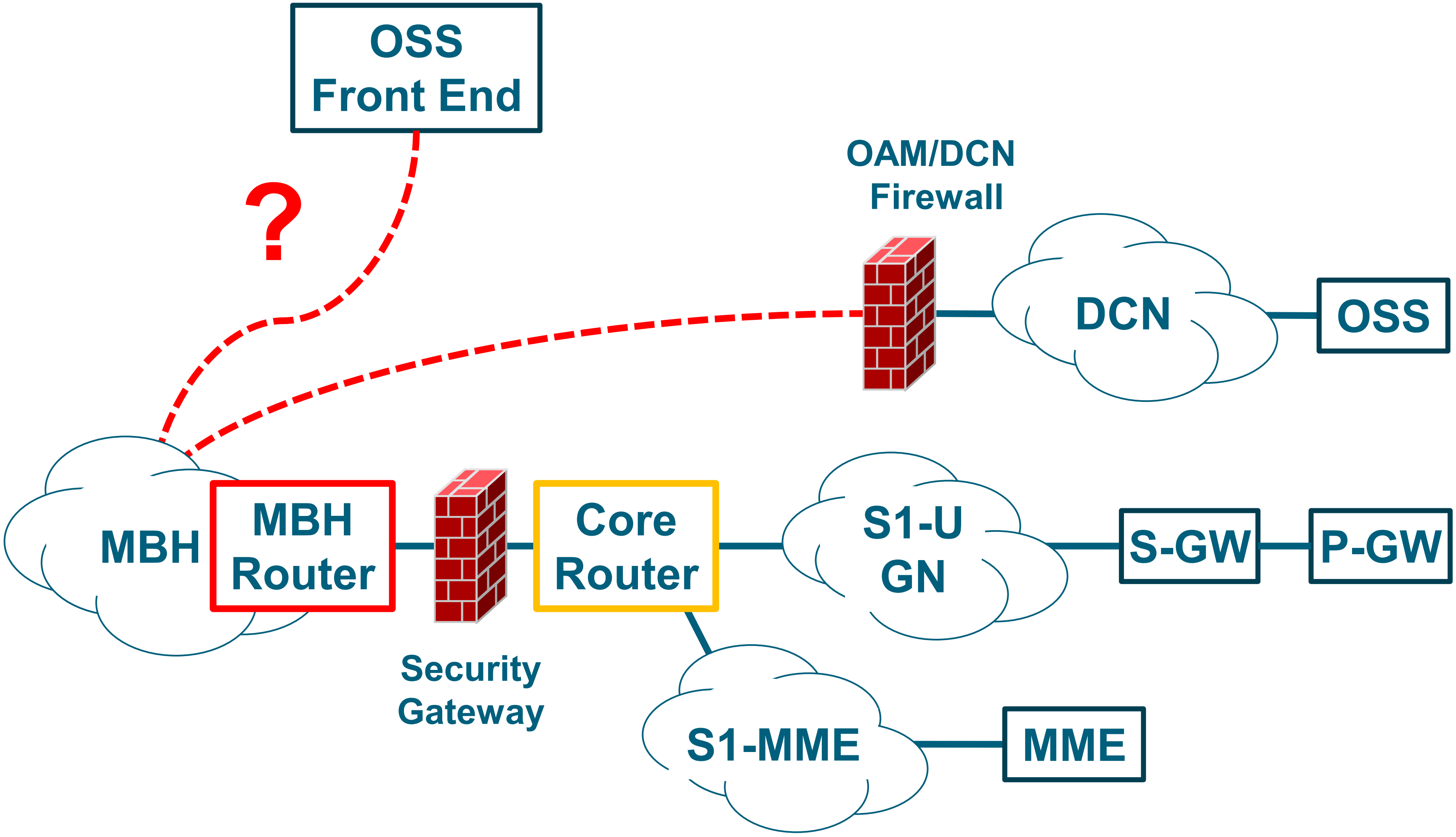
Good basic principle if these are physically different systems



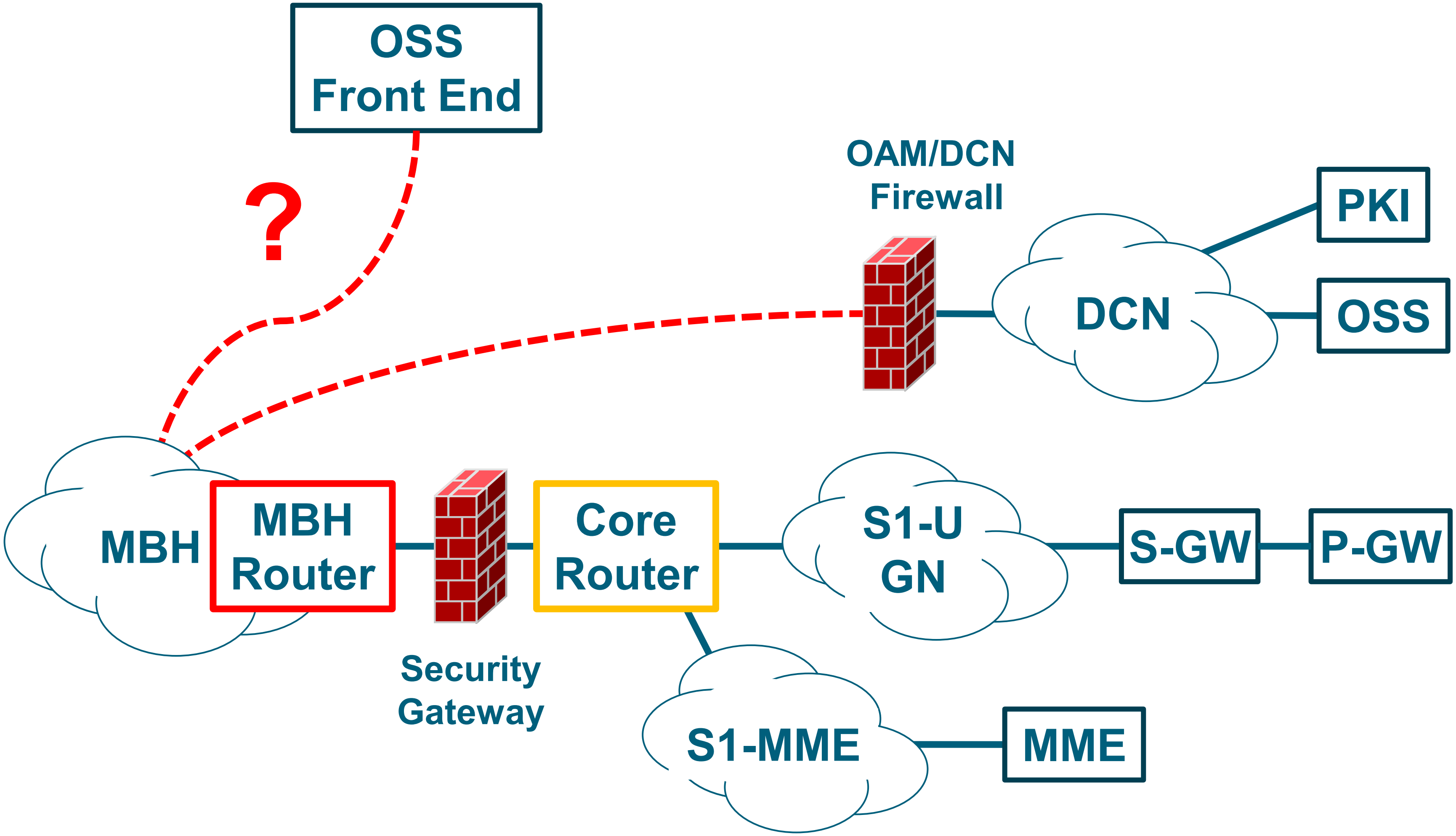
- How are you going to create a clean and secure Architecture?



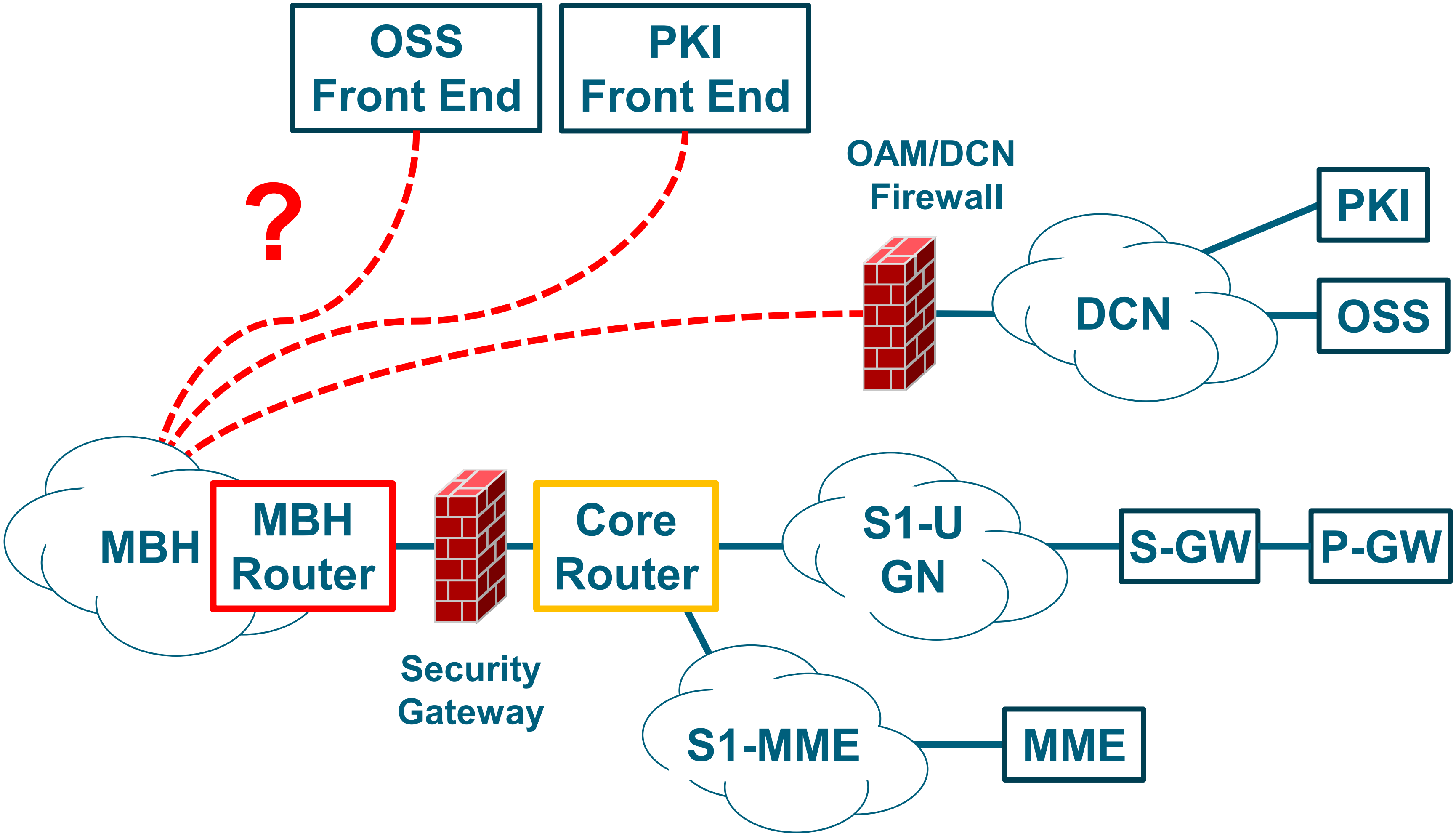
- How are you going to create a clean and secure Architecture?



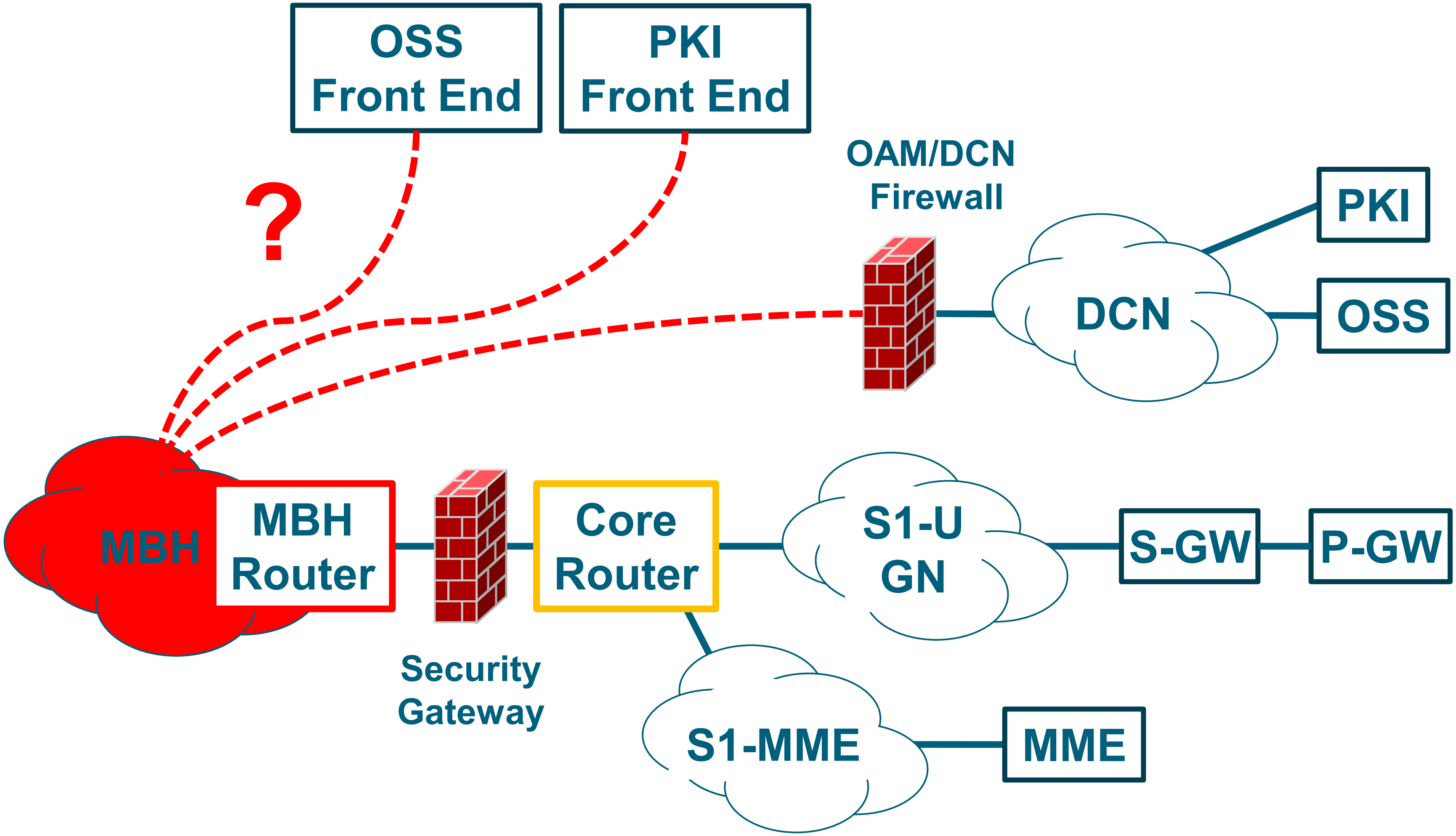
- How are you going to create a clean and secure Architecture?



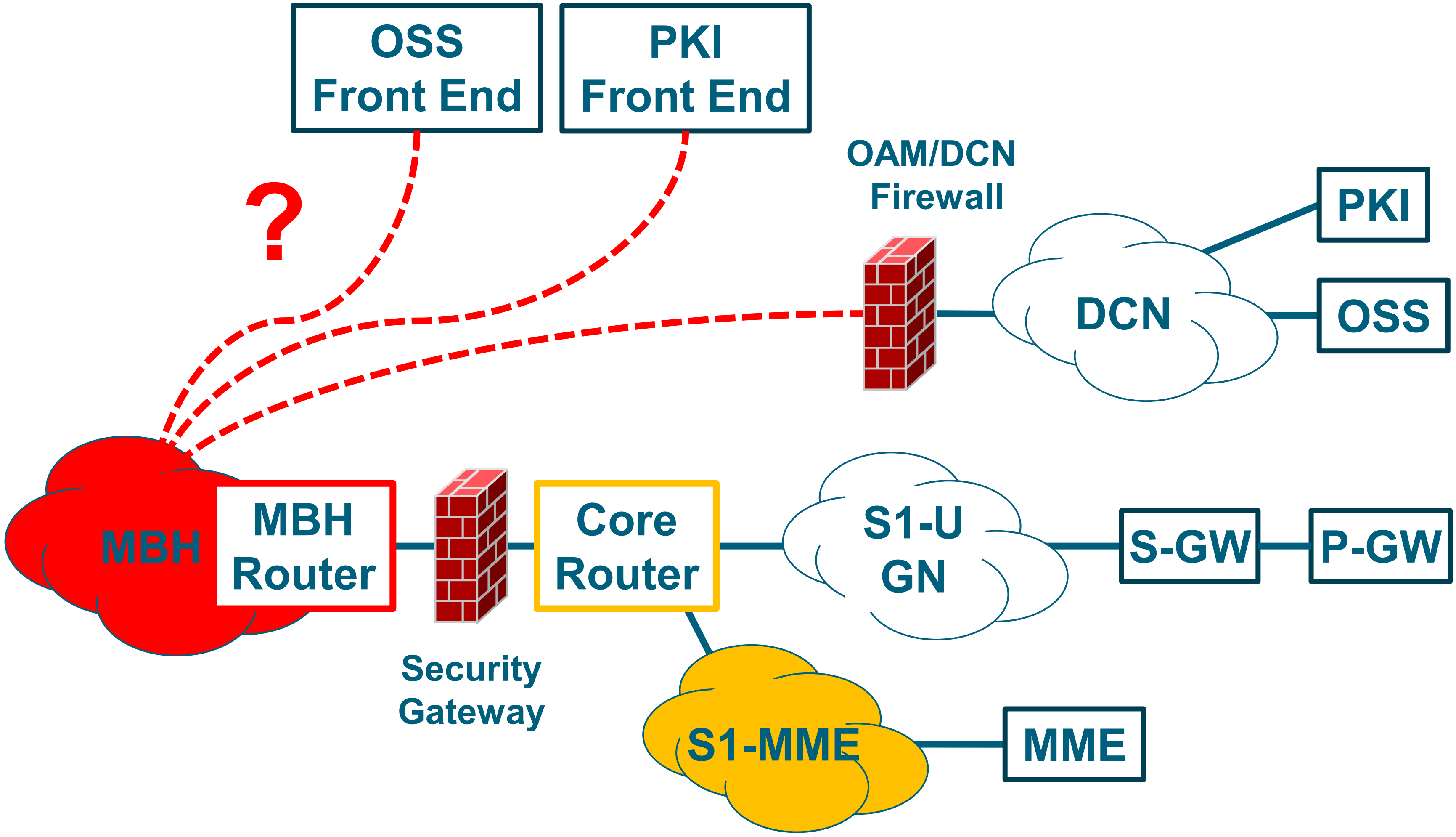
- How are you going to create a clean and secure Architecture?



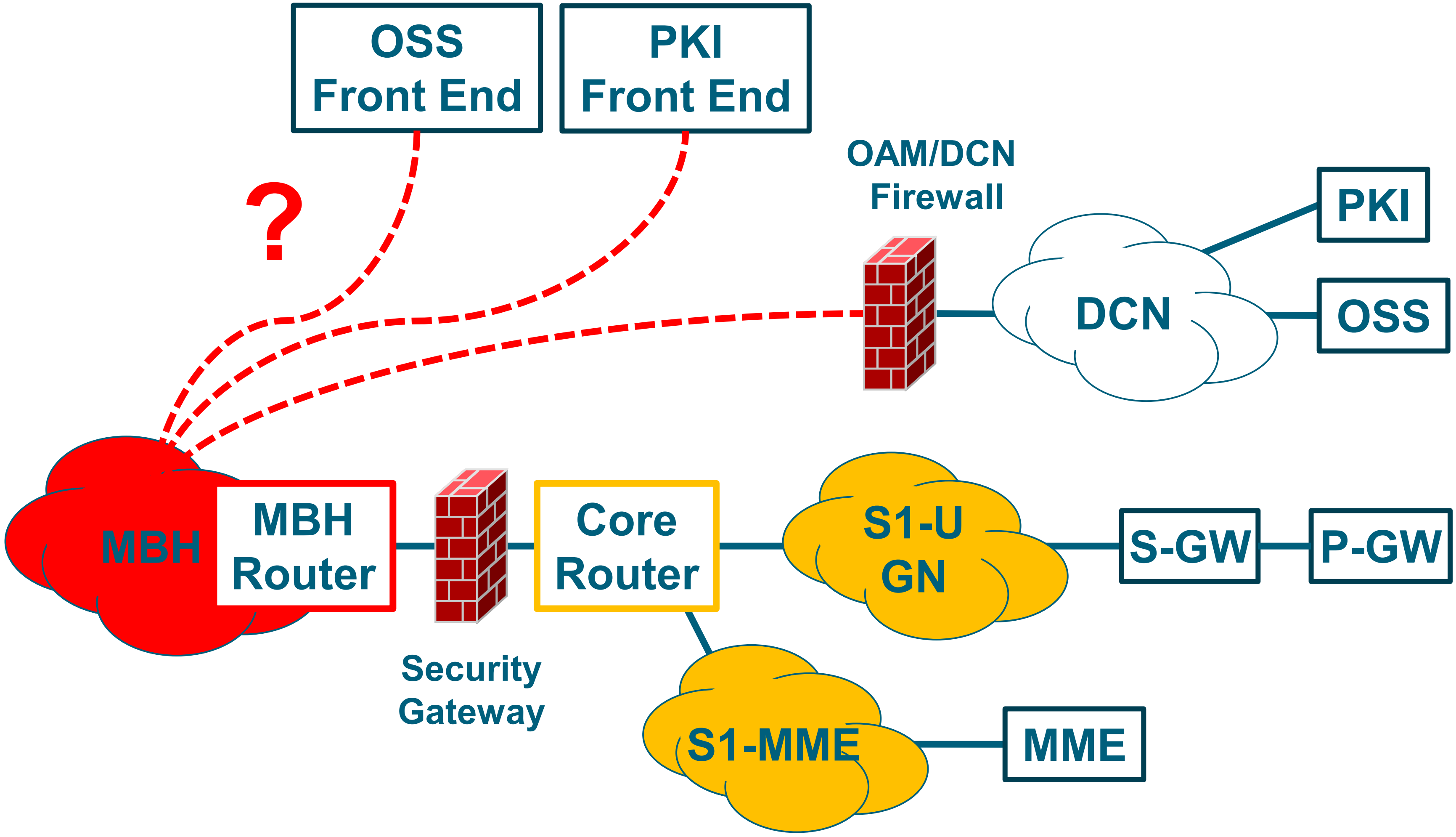
- How are you going to create a clean and secure Architecture?



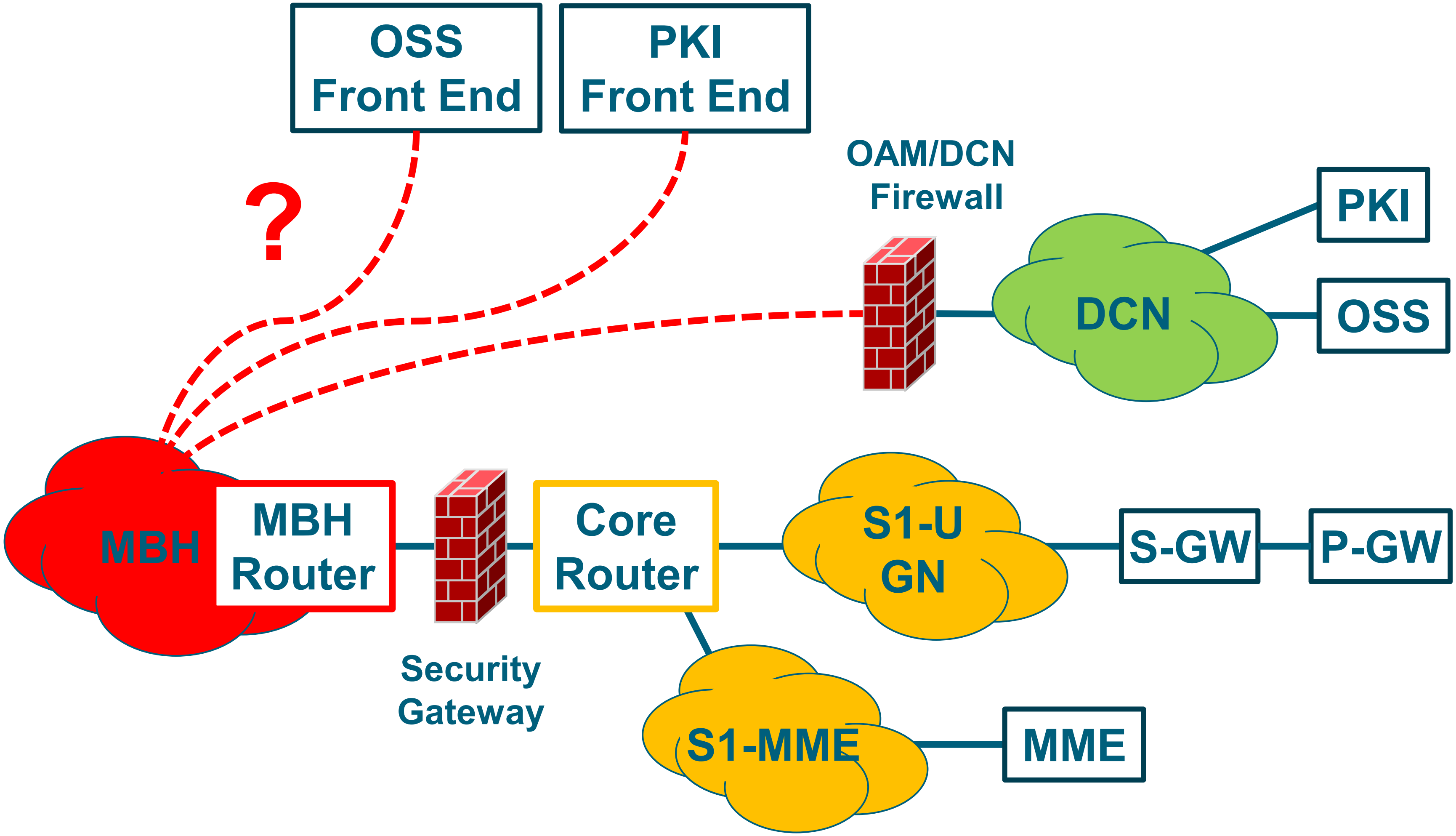
- How are you going to create a clean and secure Architecture?



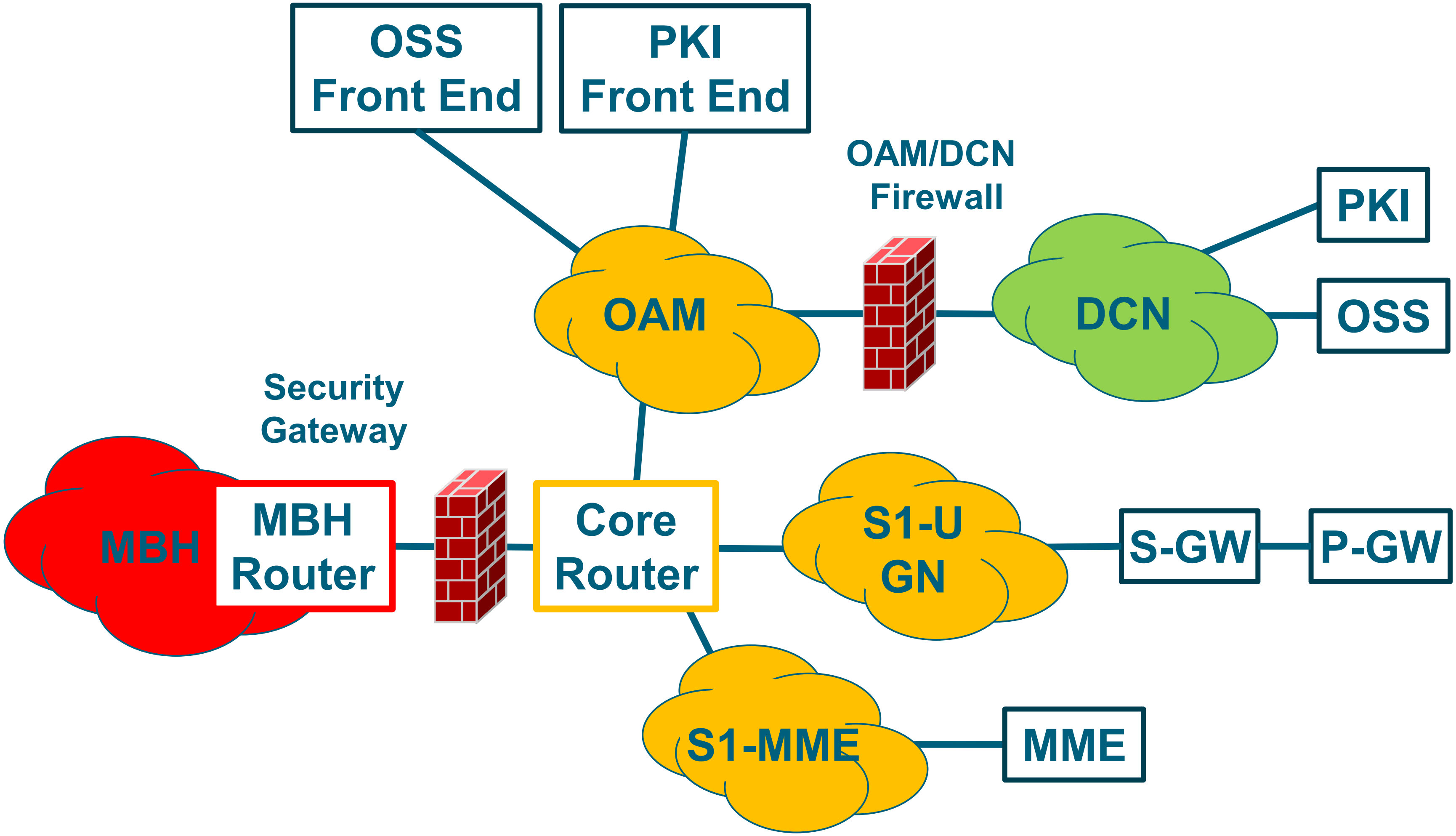
- How are you going to create a clean and secure Architecture?



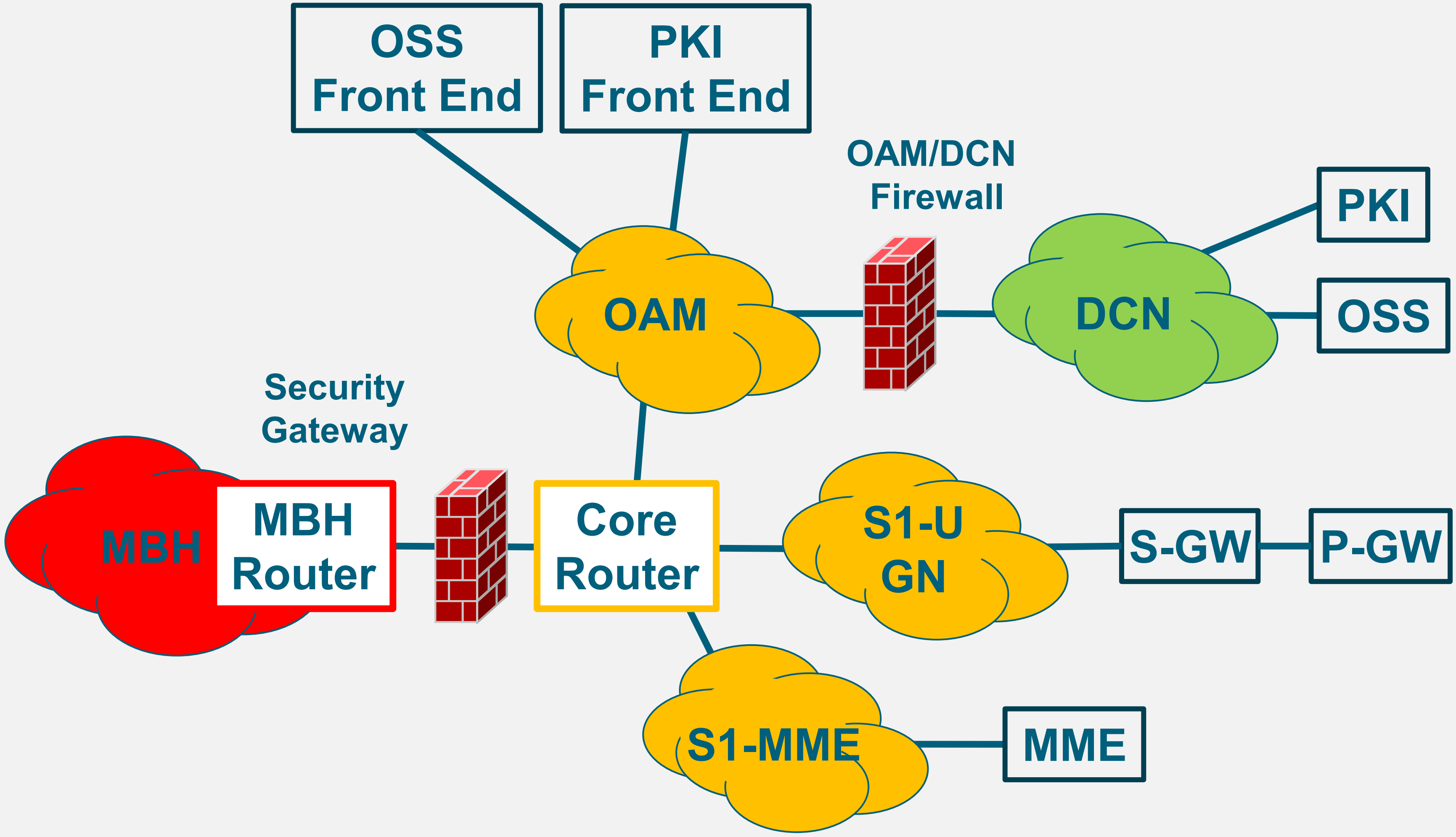
- How are you going to create a clean and secure Architecture?



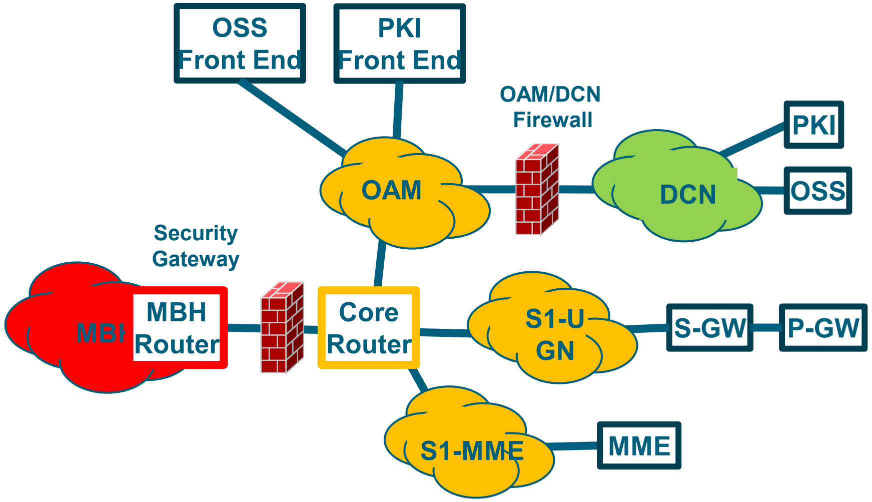
- How are you going to create a clean and secure Architecture?



- How are you going to create a clean and secure Architecture?



- How are you going to create a clean and secure Architecture?

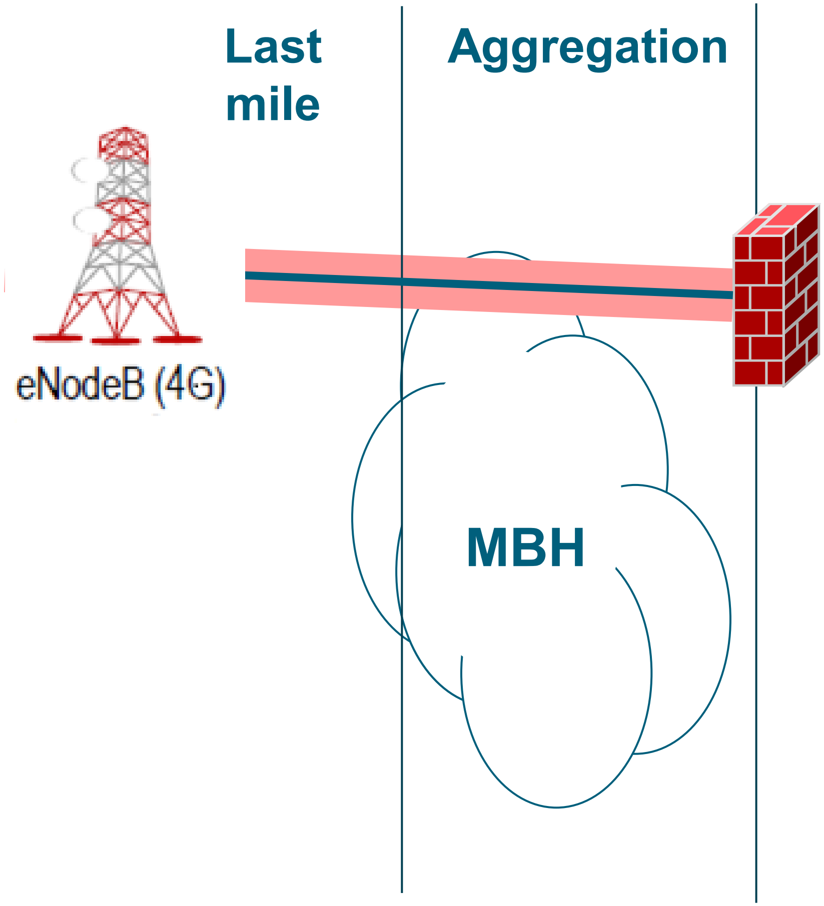


- How are you going to create a clean and secure Architecture?

- **Auto integration means an un-encrypted un-authenticated path from your eNodeB to the OSS platforms**

05
Geo-resilience

- Geo-resilience
  - Building the infrastructure to provide resilience against the loss of a significant location/installation.



Last mile

Aggregation

Core

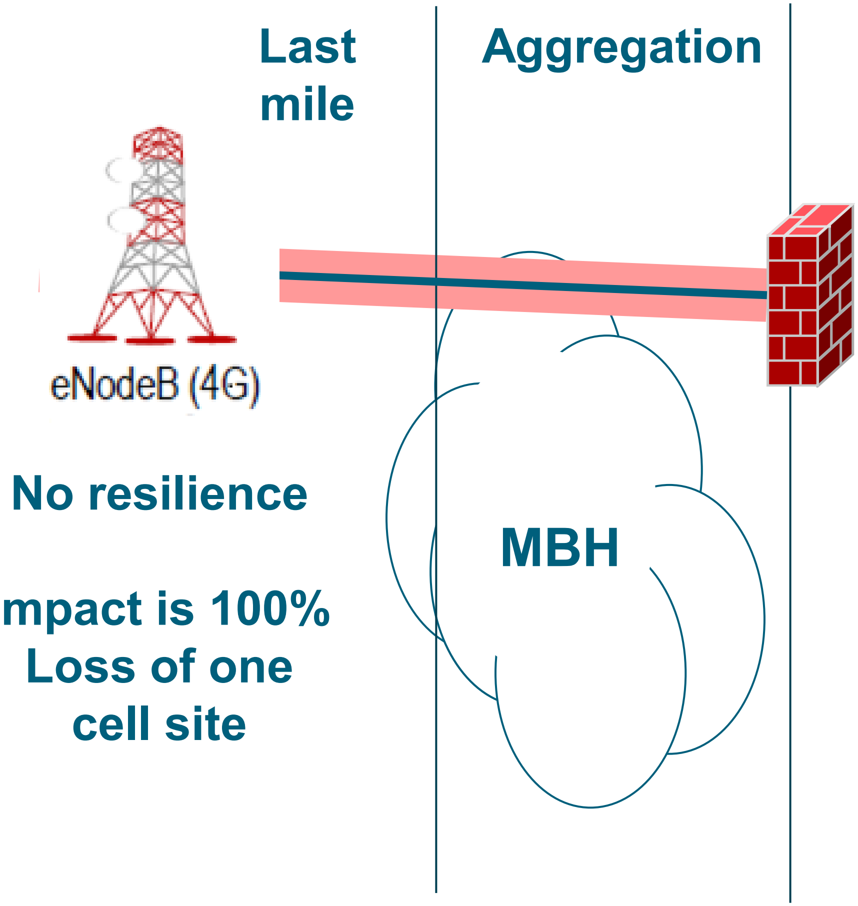
eNodeB (4G)

MBH

Last mile

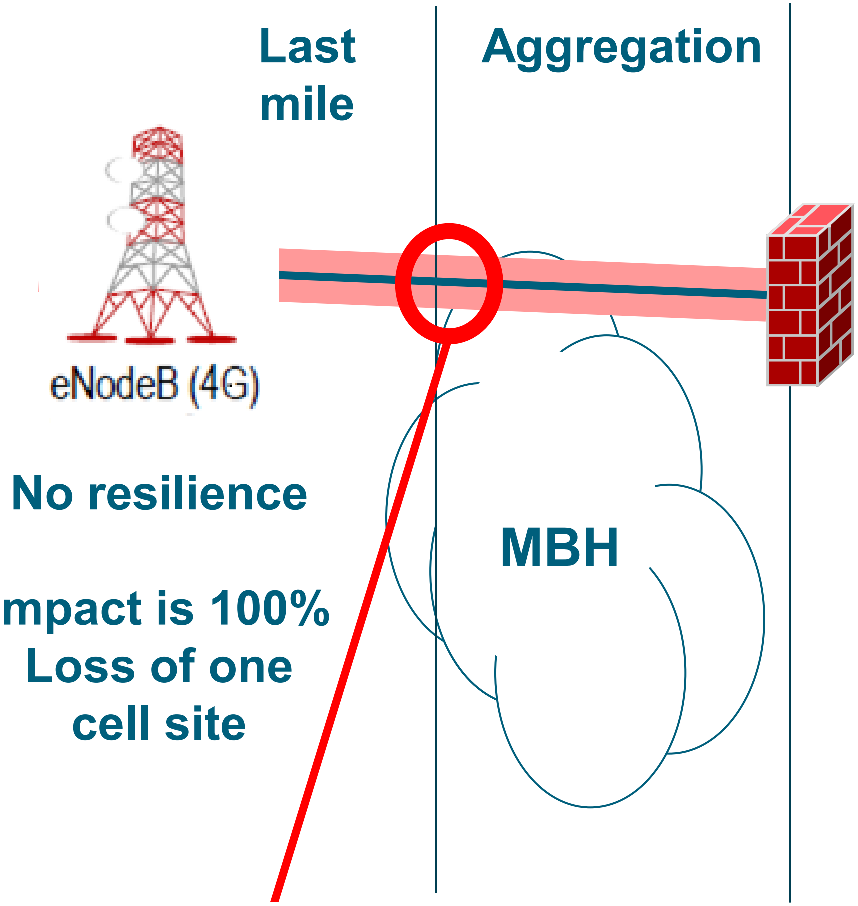
Aggregation

Core



No resilience

**Impact is 100%
Loss of one
cell site**



Last mile

Aggregation

Core

eNodeB (4G)

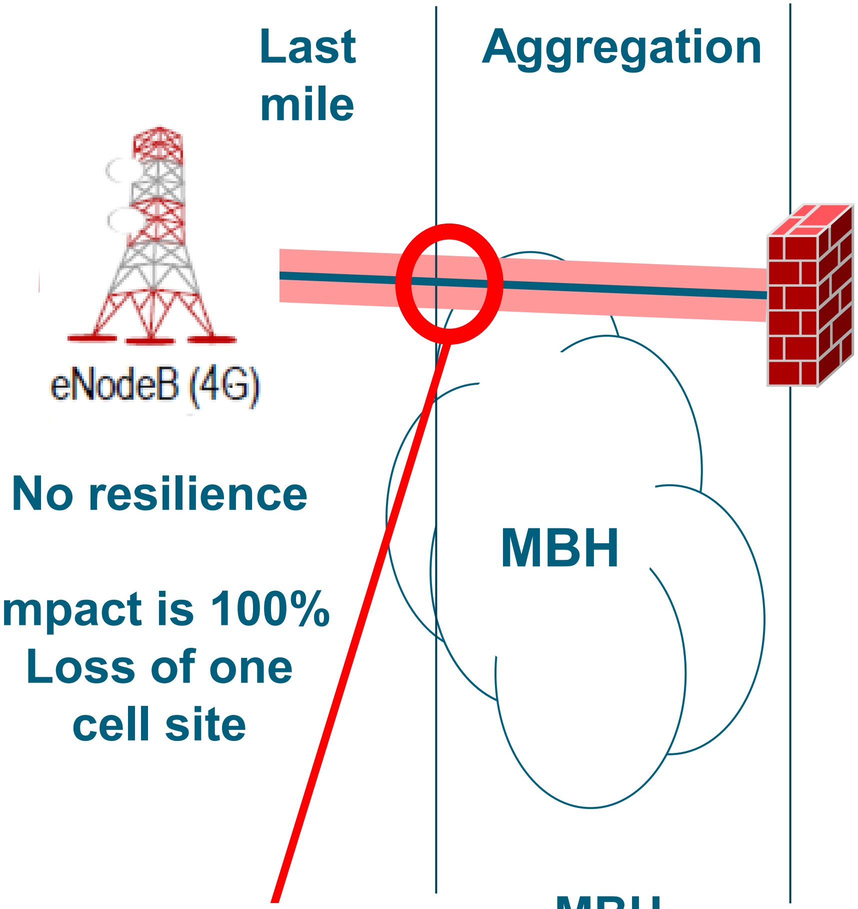
MBH

No resilience

Impact is 100%
Loss of one
cell site

Access edge

Impact is 100%
loss of N cell
sites



Last mile

Aggregation

Core

eNodeB (4G)

MBH

No resilience

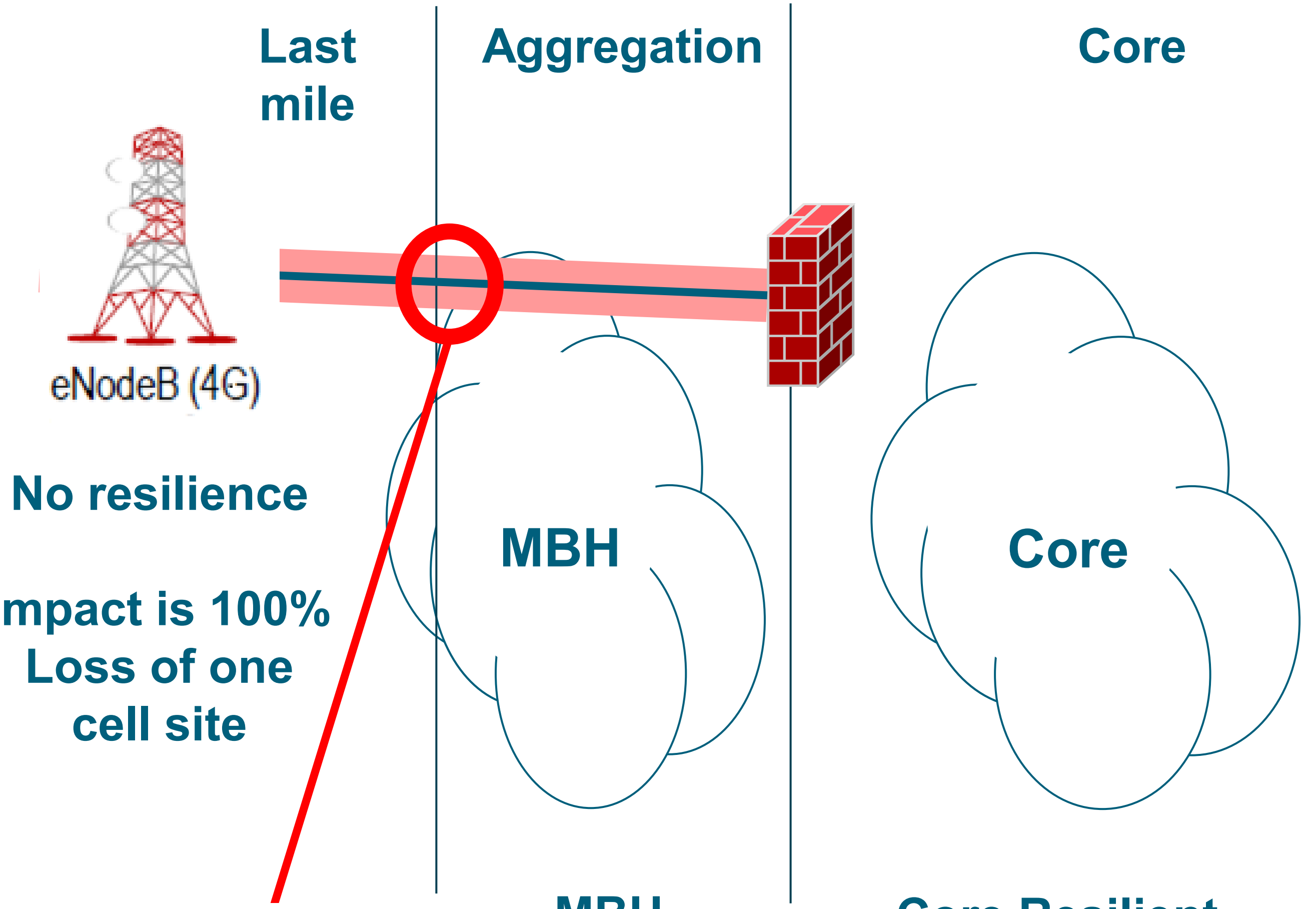
Impact is 100%
Loss of one
cell site

Access edge

Impact is 100%
loss of N cell
sites

MBH
Resilient

No SPOF



Last mile

Aggregation

Core

eNodeB (4G)

MBH

Core

No resilience

Impact is 100%
Loss of one
cell site

Access edge

Impact is 100%
loss of N cell
sites

MBH
Resilient

No SPOF

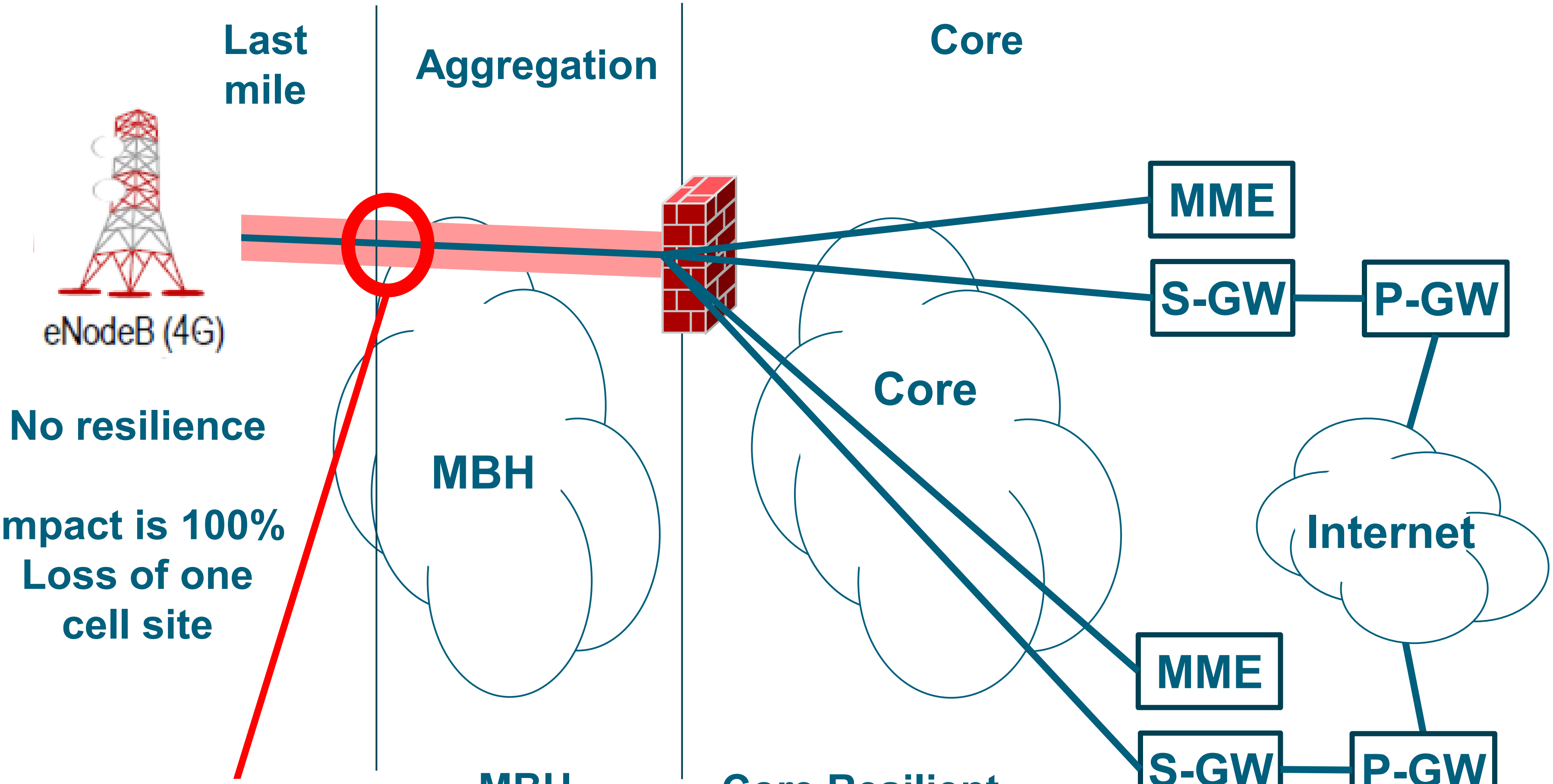
Core Resilient

No SPOF

Last mile

Aggregation

Core



No resilience

Impact is 100%
Loss of one
cell site

Access edge

Impact is 100%
loss of N cell
sites

MBH
Resilient

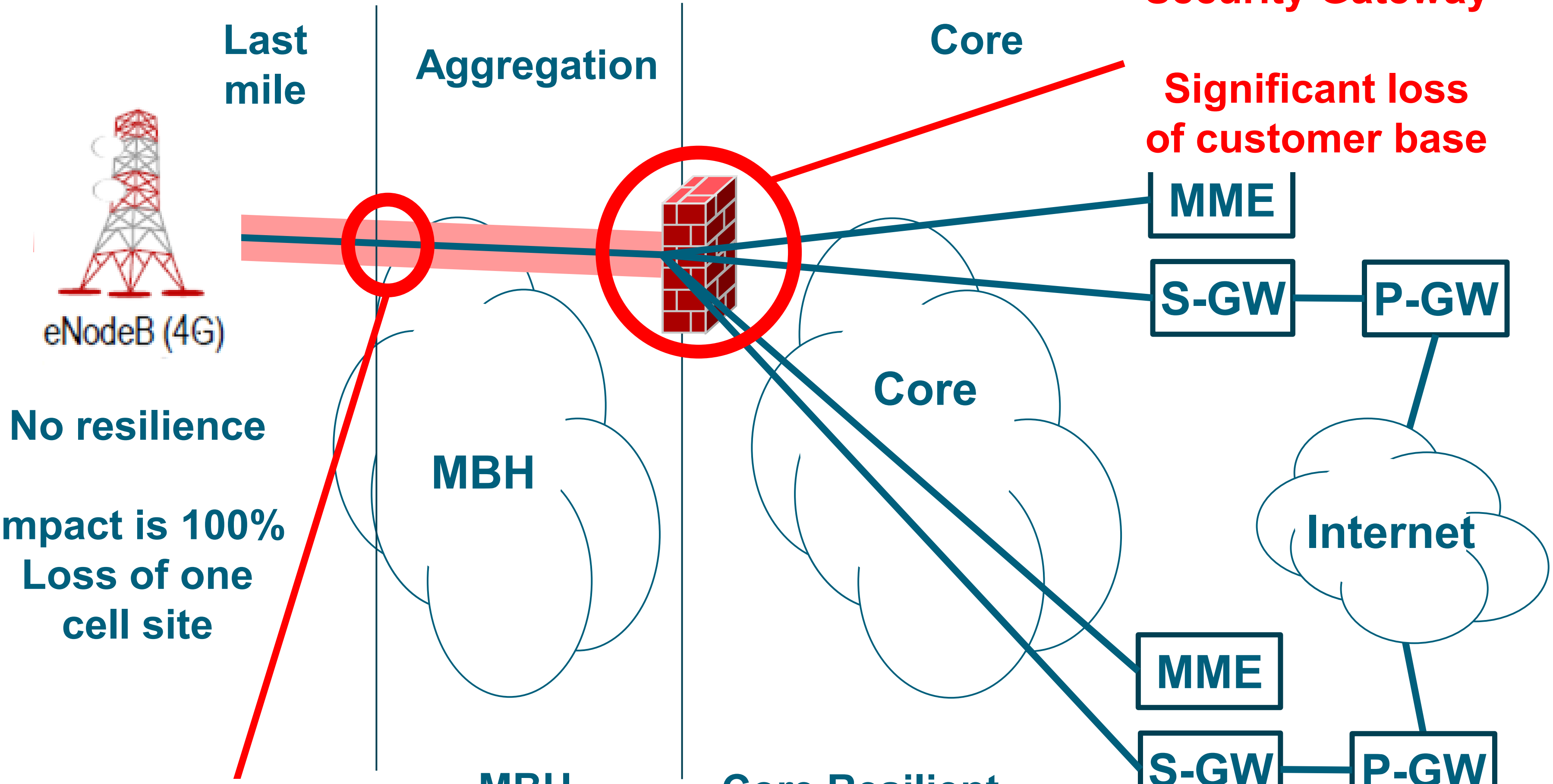
No SPOF

Core Resilient

No SPOF

EPC Resilient

No SPOF



Security Gateway

Significant loss of customer base

No resilience

Impact is 100%
Loss of one cell site

Access edge

Impact is 100%
loss of N cell sites

MBH Resilient

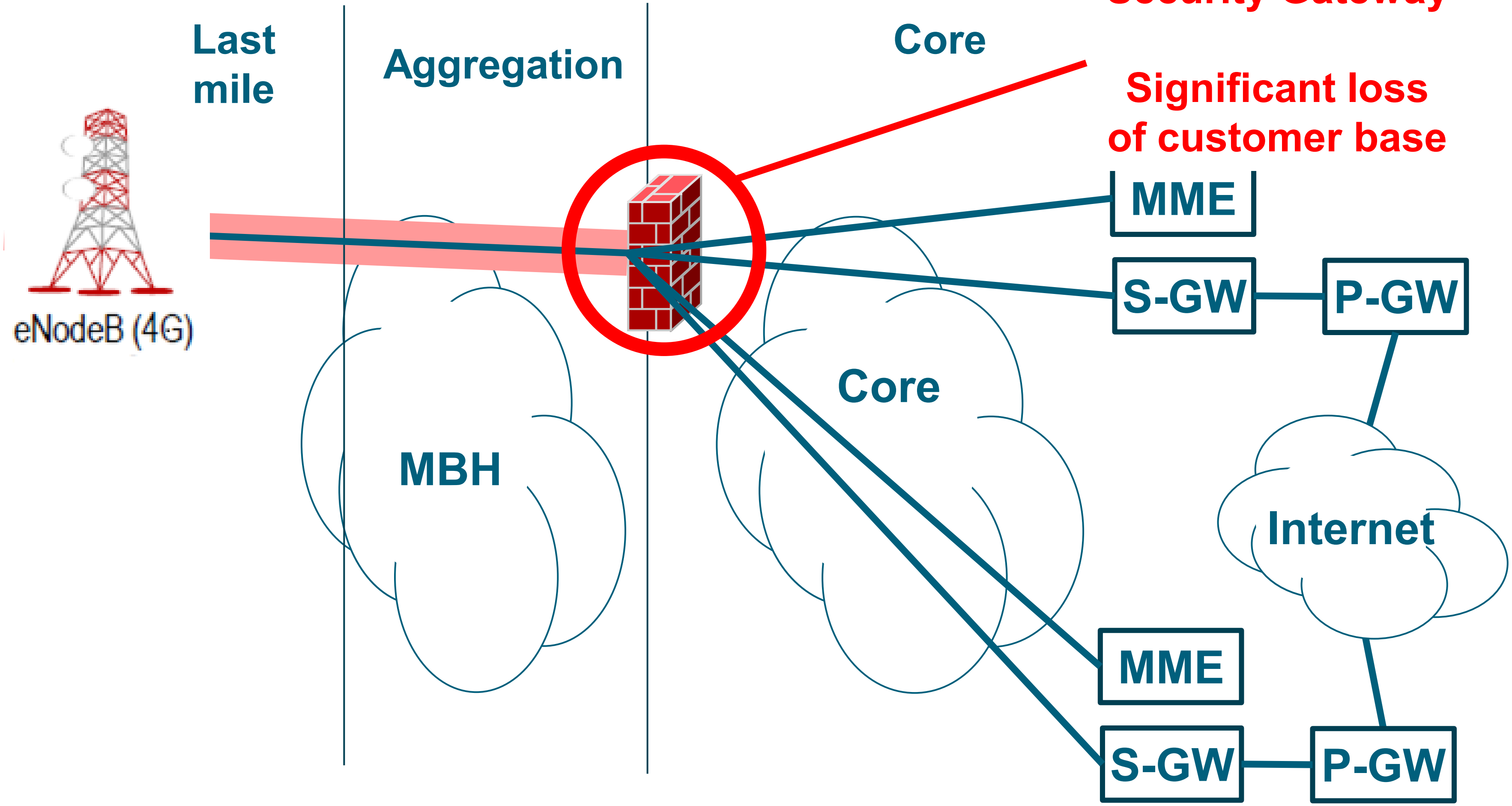
No SPOF

Core Resilient

No SPOF

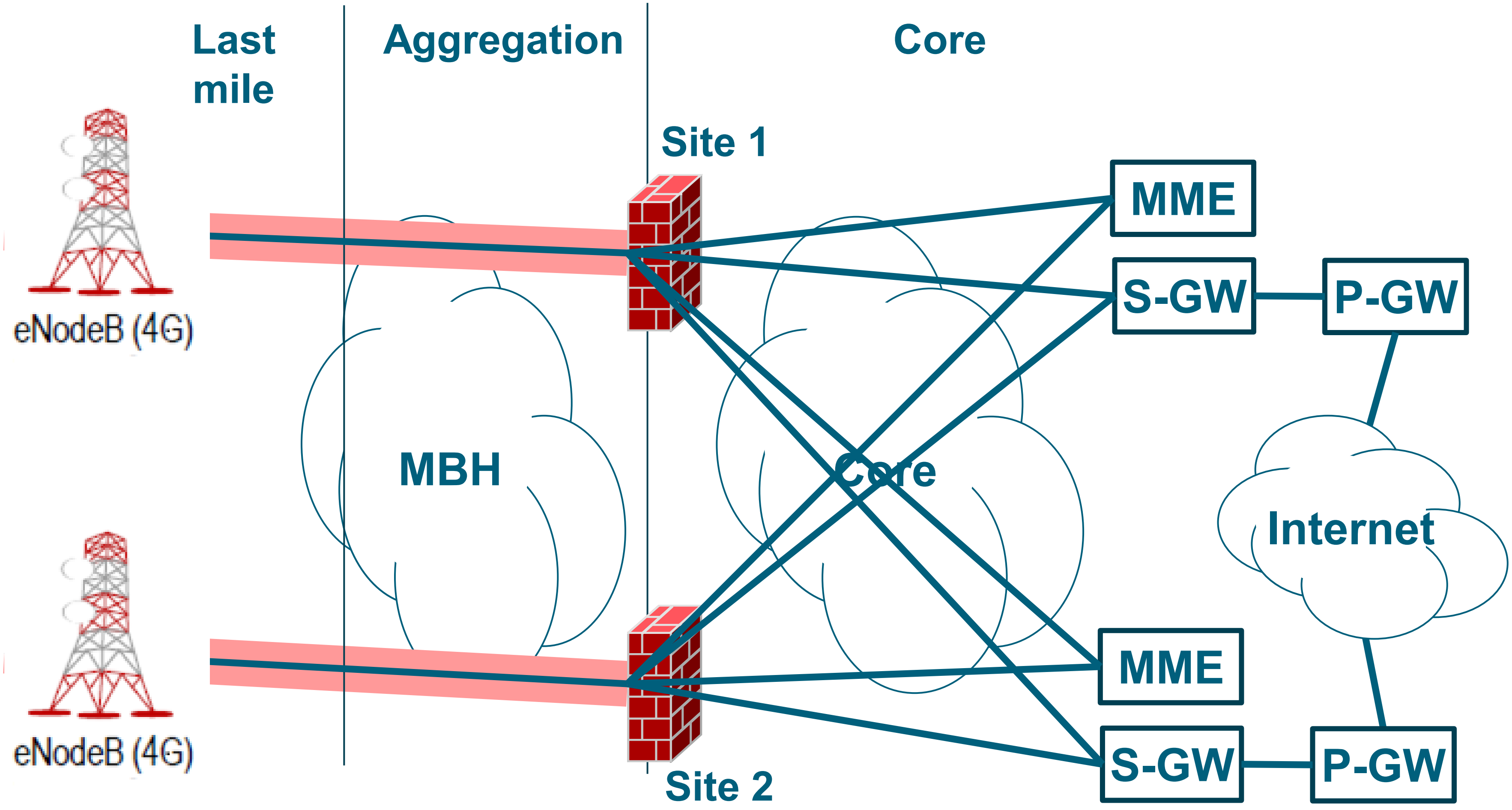
EPC Resilient

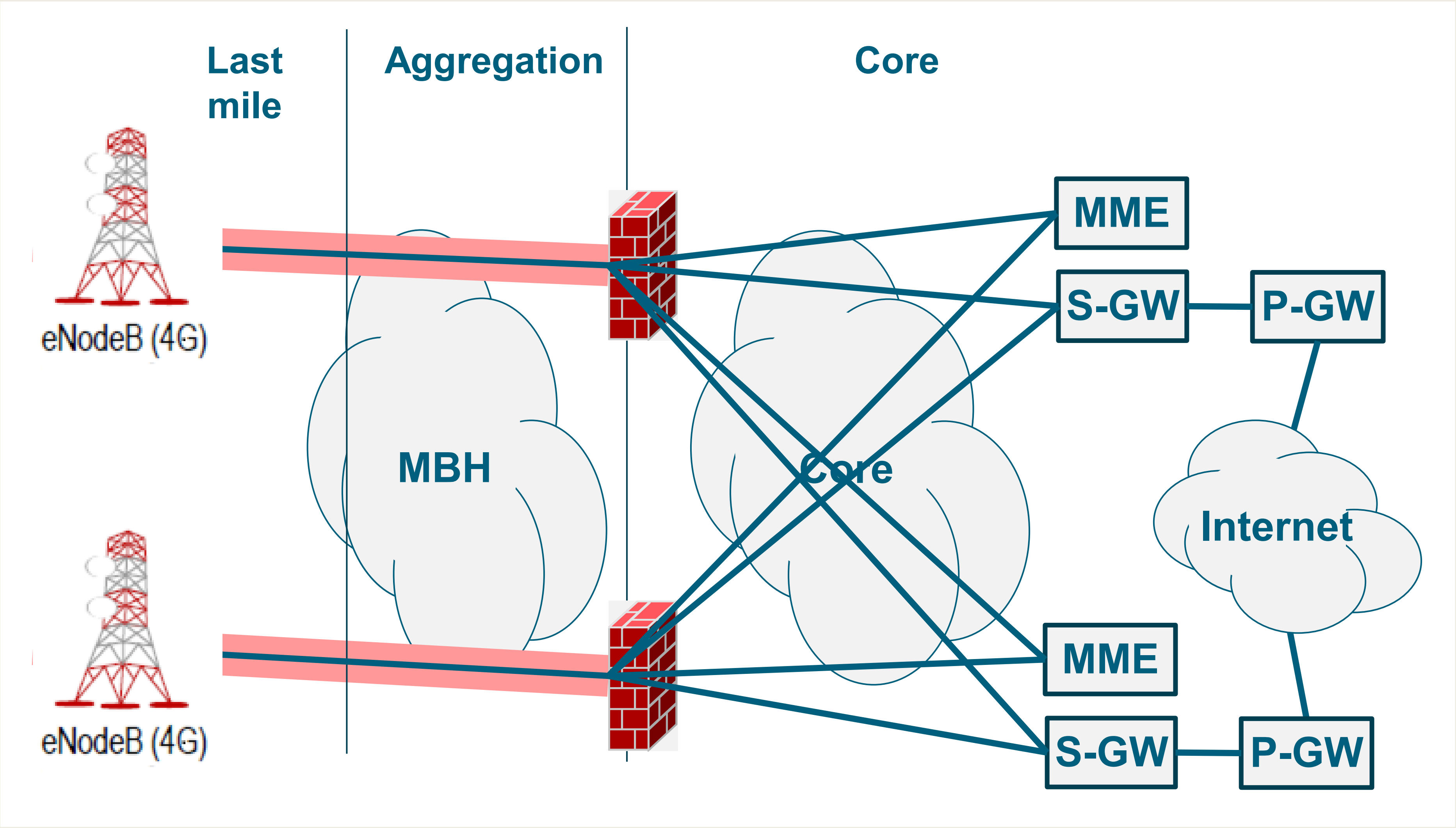
No SPOF

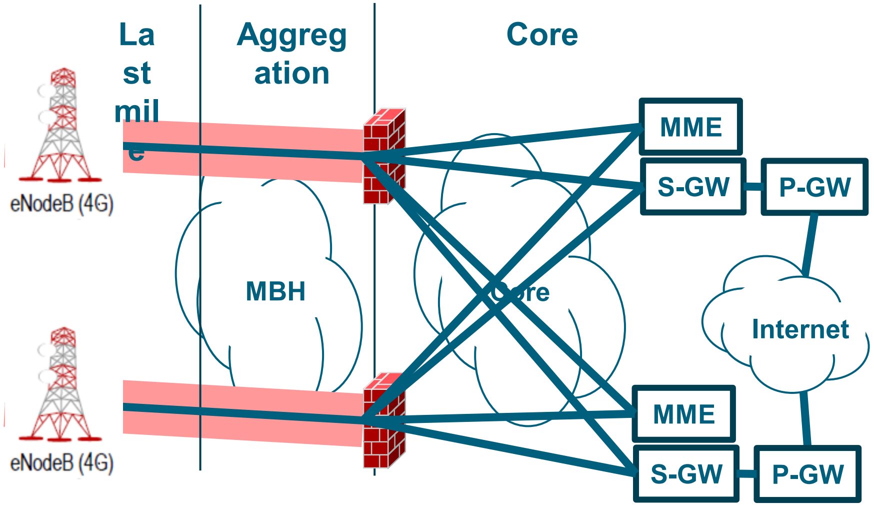


Security Gateway

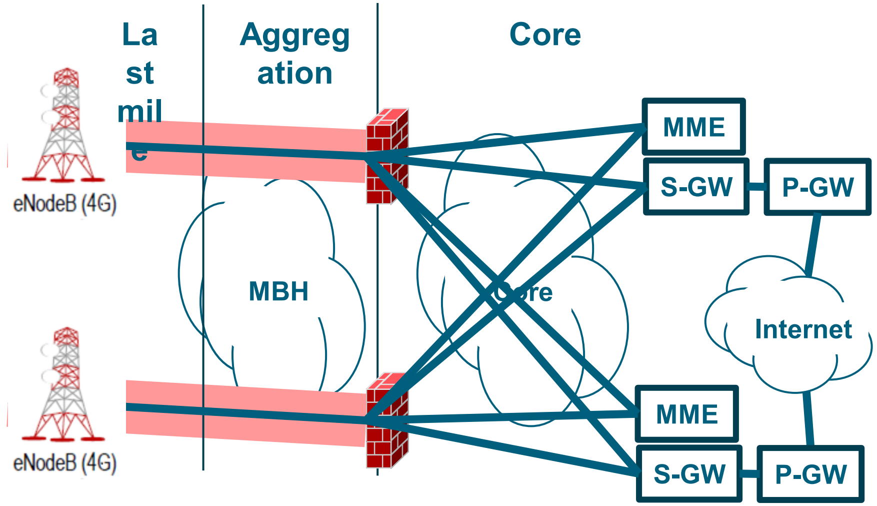
Significant loss of customer base


Last mile
Aggregation
Core
Site 1
eNodeB (4G)
MBH
Core
MME
S-GW
P-GW
Internet
eNodeB (4G)
MME
S-GW
P-GW
Site 2

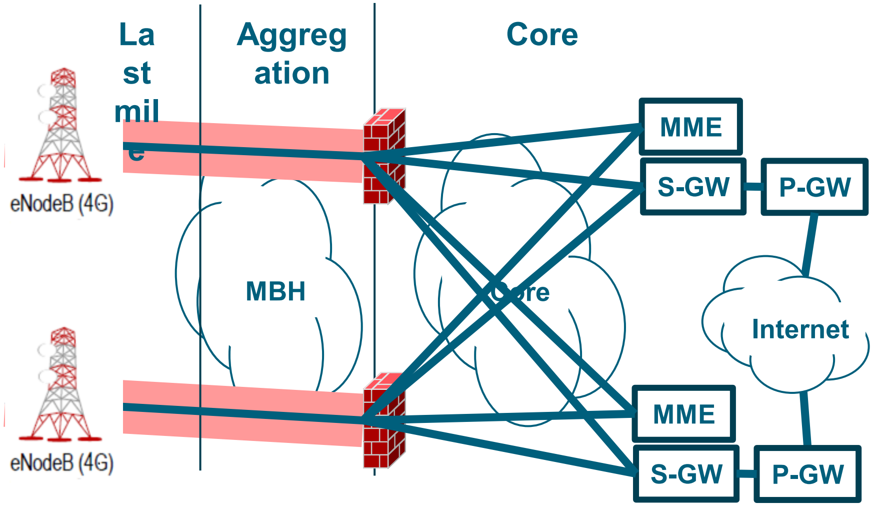

Last mile
Aggregation
Core
eNodeB (4G)
eNodeB (4G)
MBH
Core
MME
S-GW
P-GW
Internet
MME
S-GW
P-GW



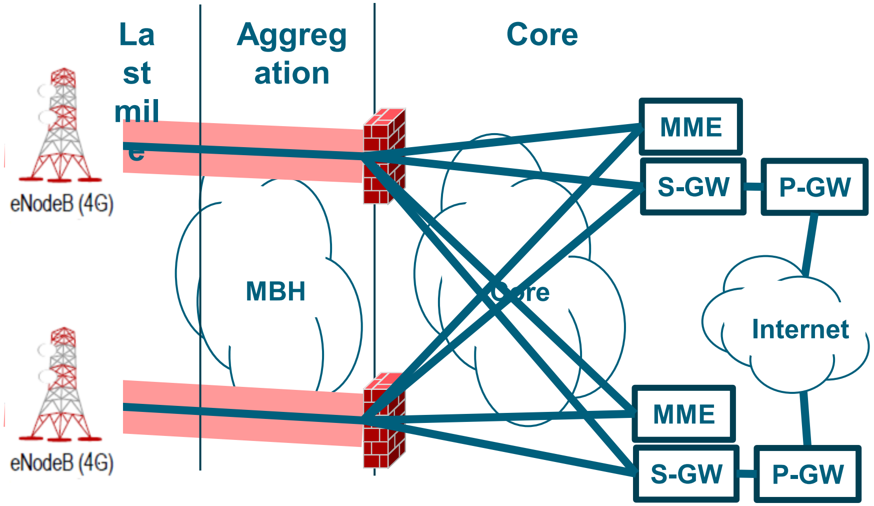
- **Options for Geo-resilience?**



- Options for Geo-resilience?
  - Backup IPSec tunnels

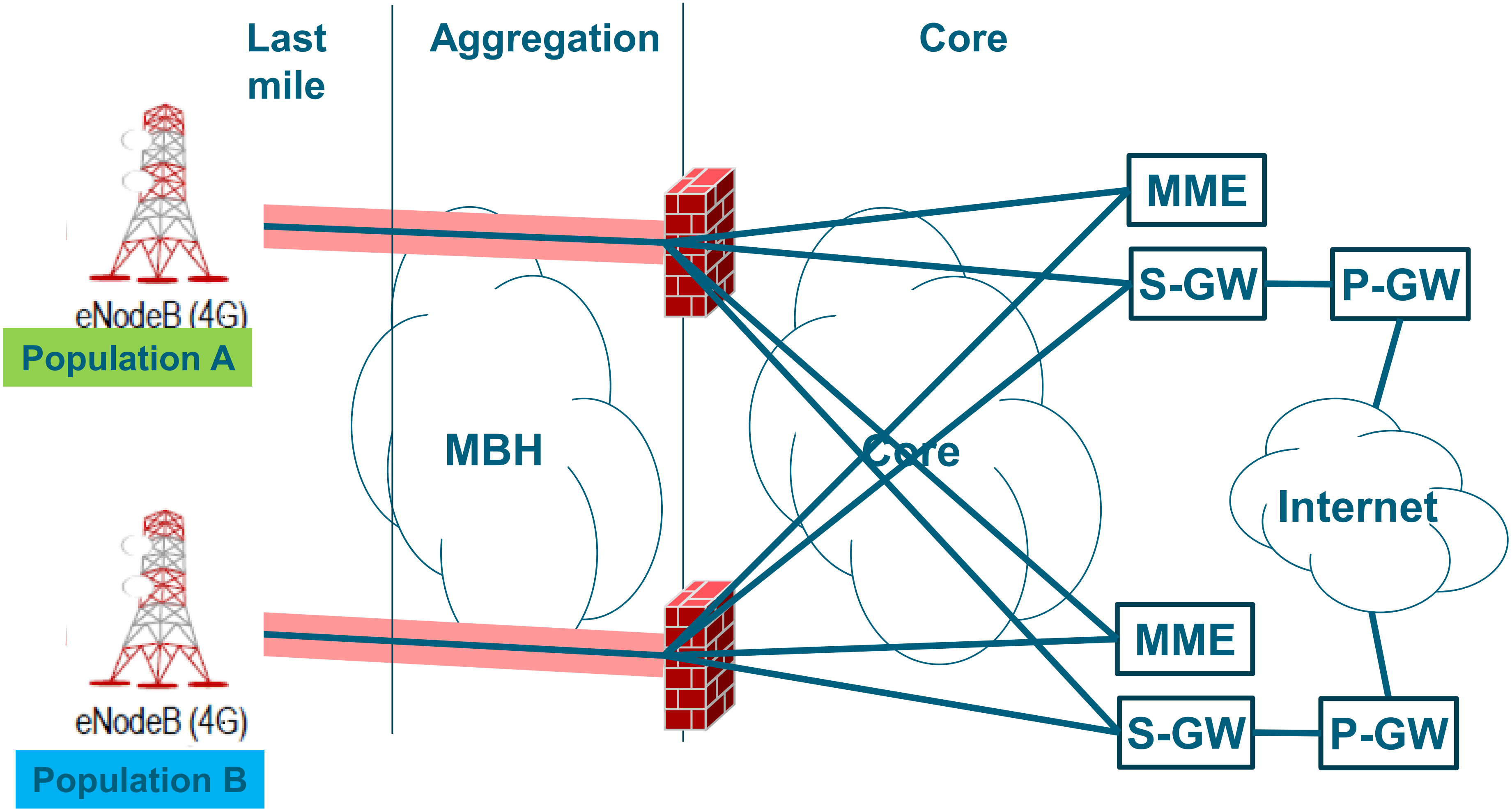


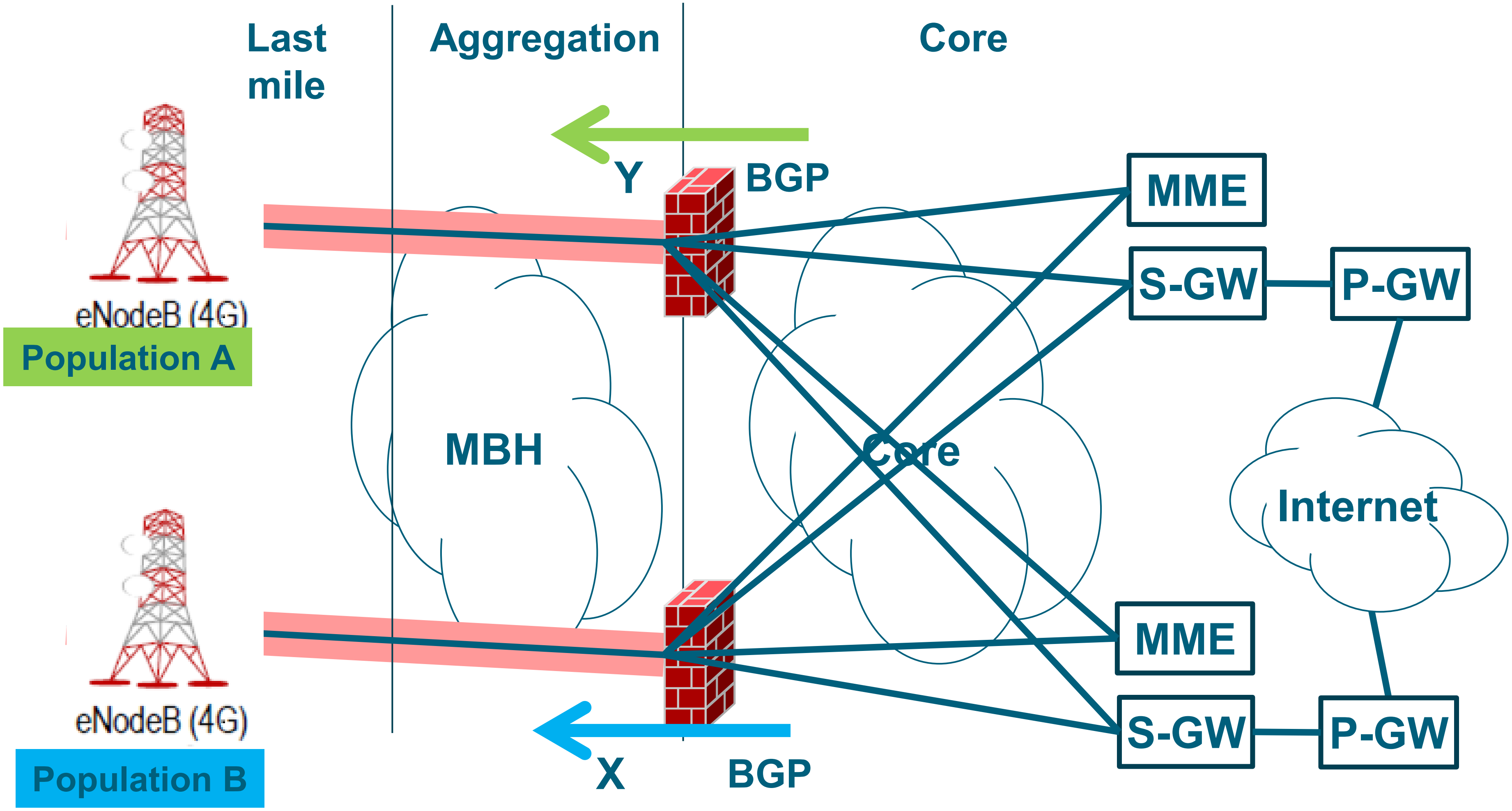
- Options for Geo-resilience?
  - Backup IPSec tunnels
  - Dynamic IP Routing



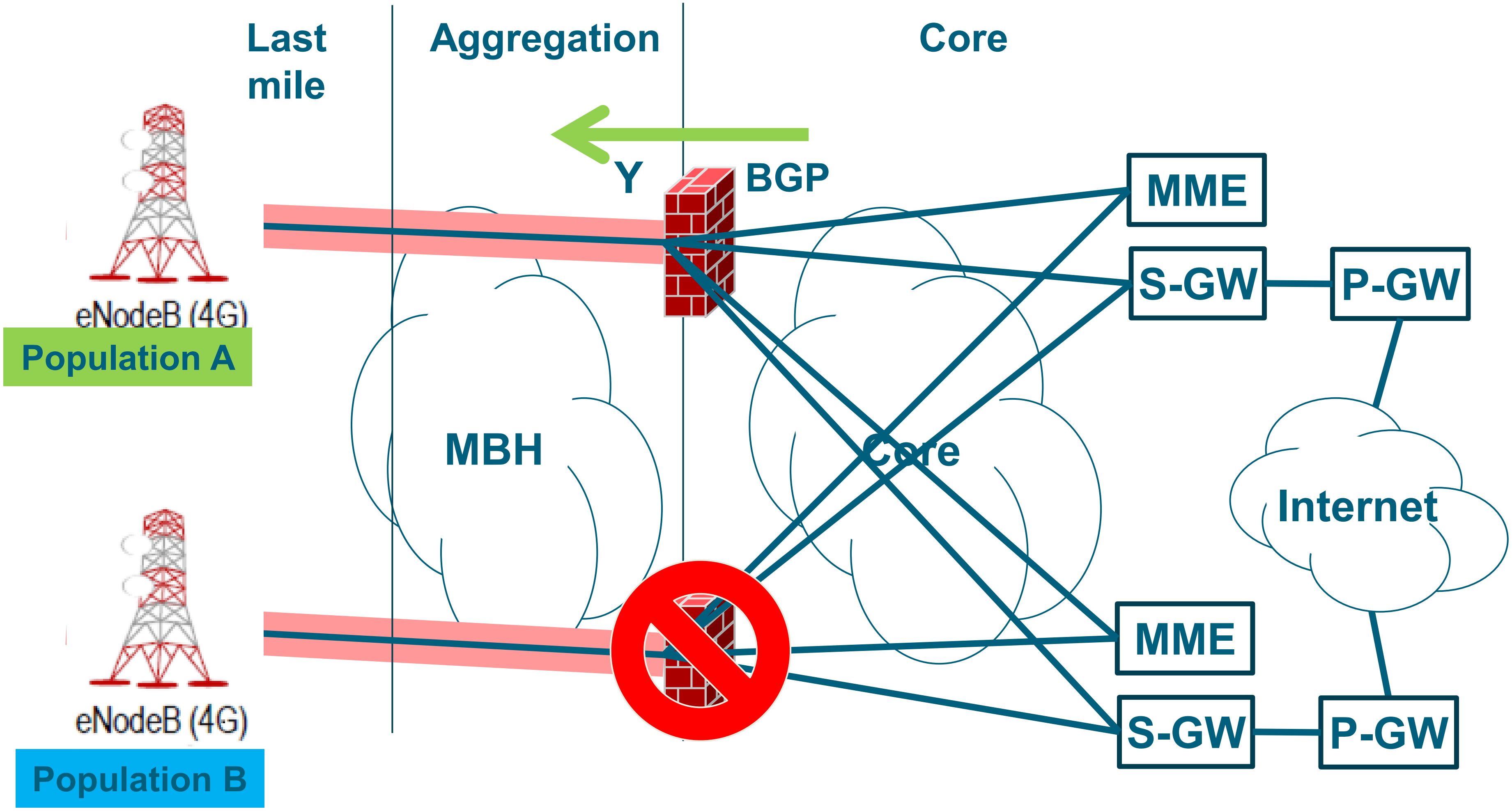
- Options for Geo-resilience?
  - Backup IPSec tunnels
  - Dynamic IP Routing

- Our evaluation of backup IPSec tunnels was that the technology was not completely ready.

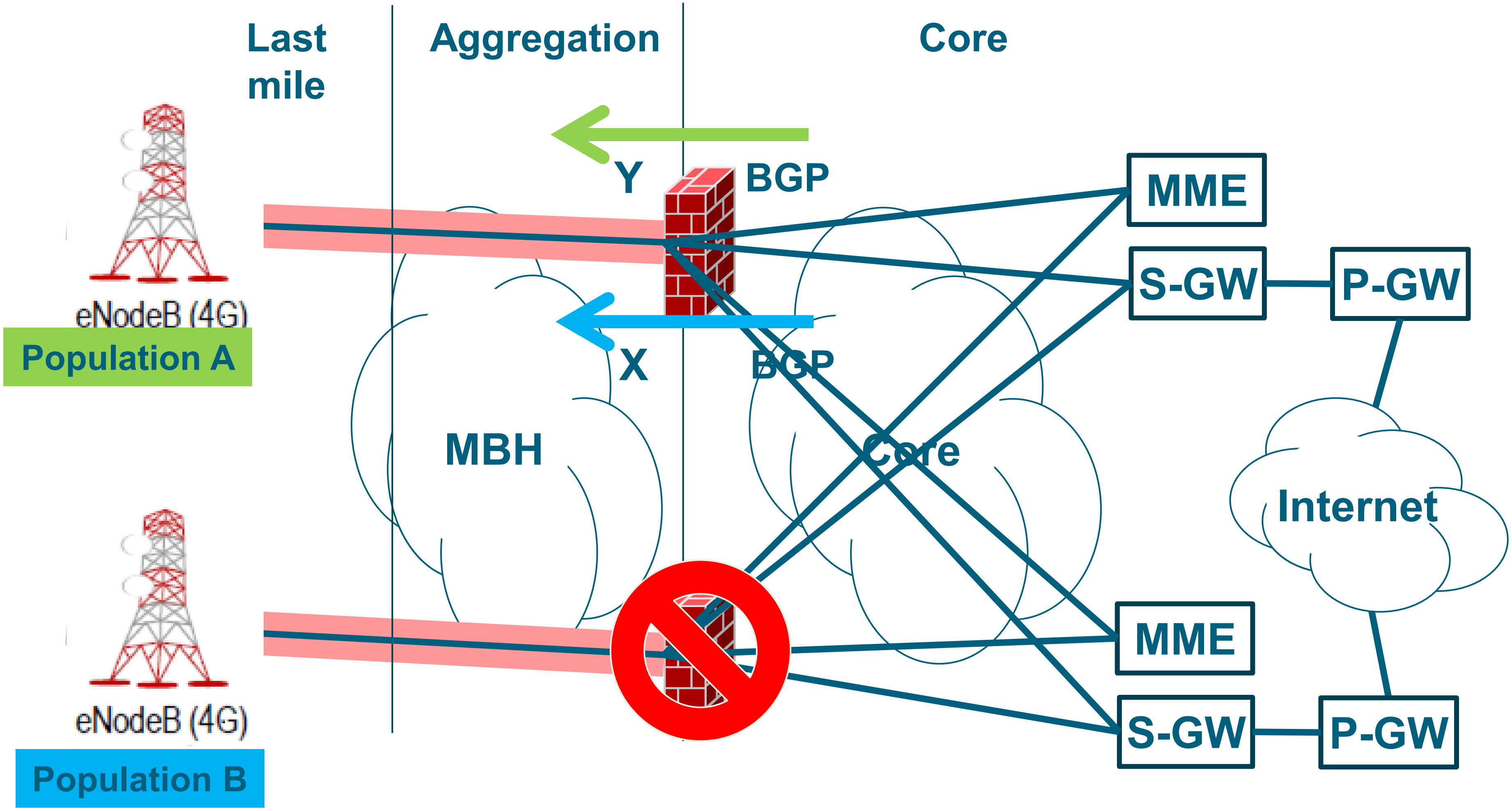

Last mile
Aggregation
Core
MME
S-GW
P-GW
eNodeB (4G)
Population A
MBH
Core
Internet
eNodeB (4G)
MME
S-GW
P-GW
Population B



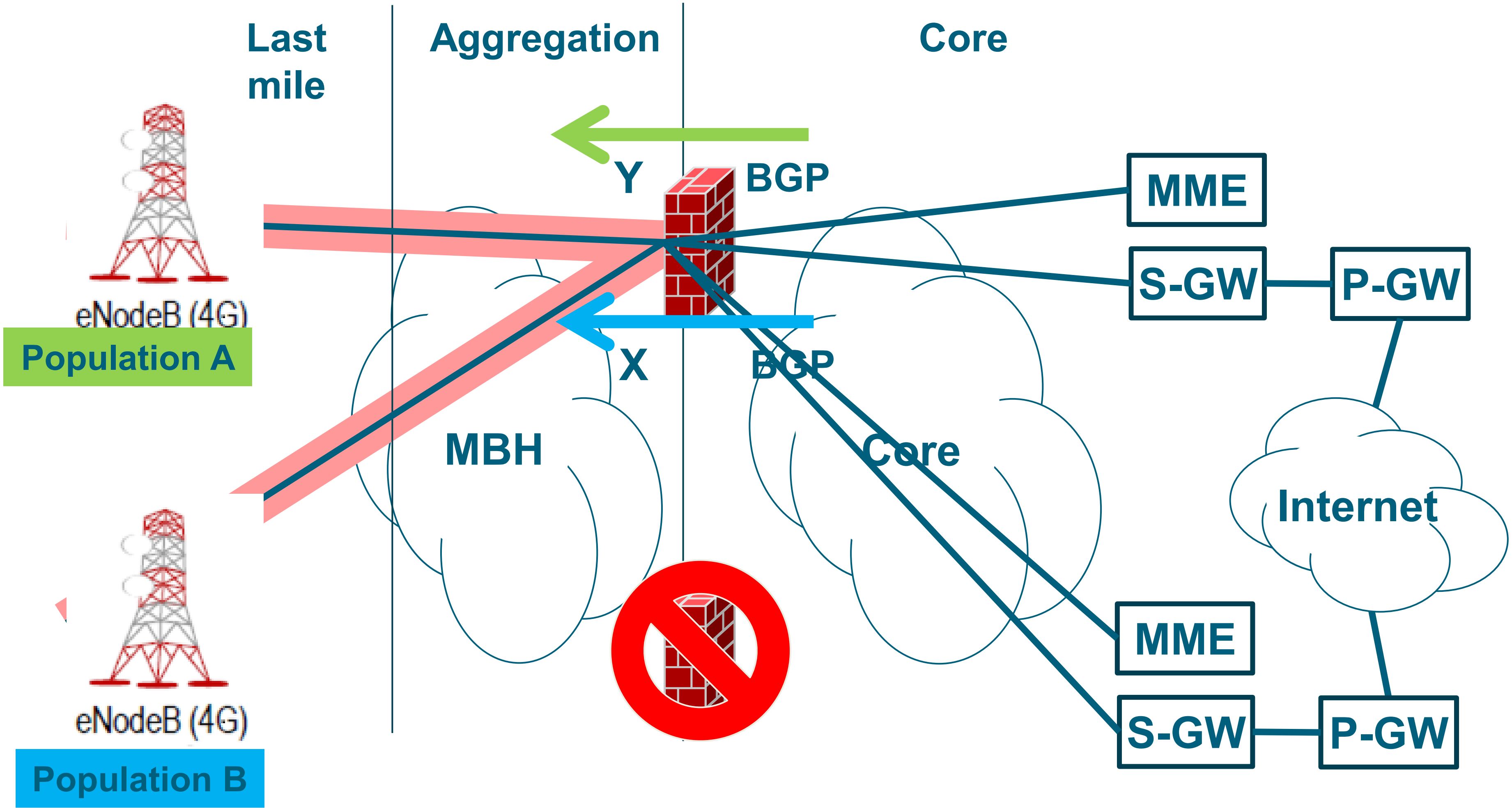
- Advertise the IPSec end point address using BGP



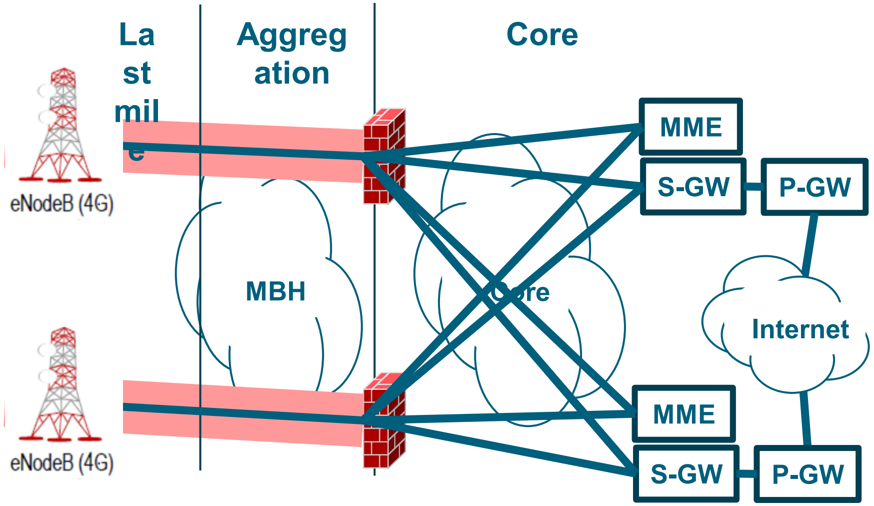
- **Advertise the IPSec end point address using BGP**



- **Advertise the IPSec end point address using BGP**

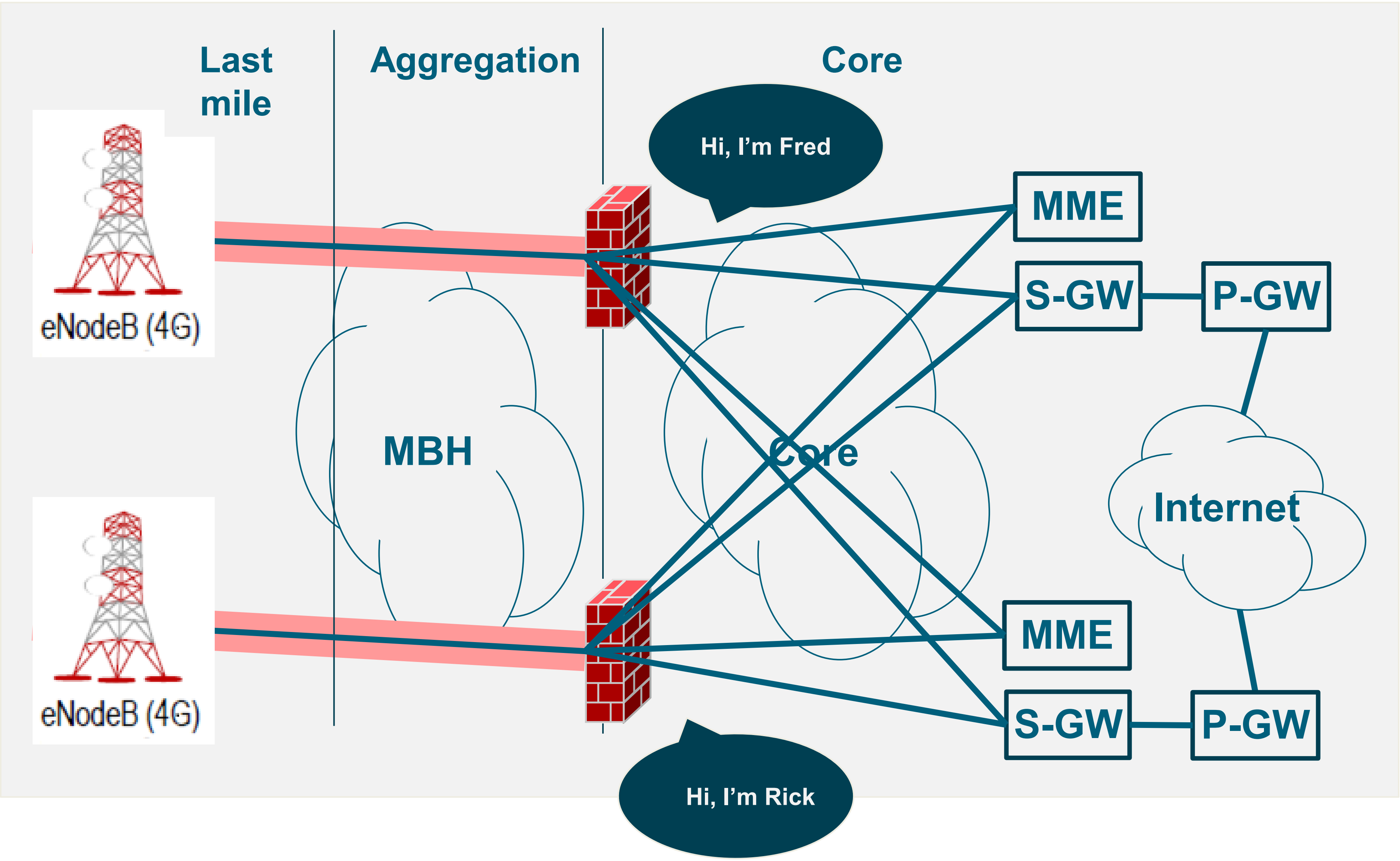


- **Advertise the IPSec end point address using BGP**

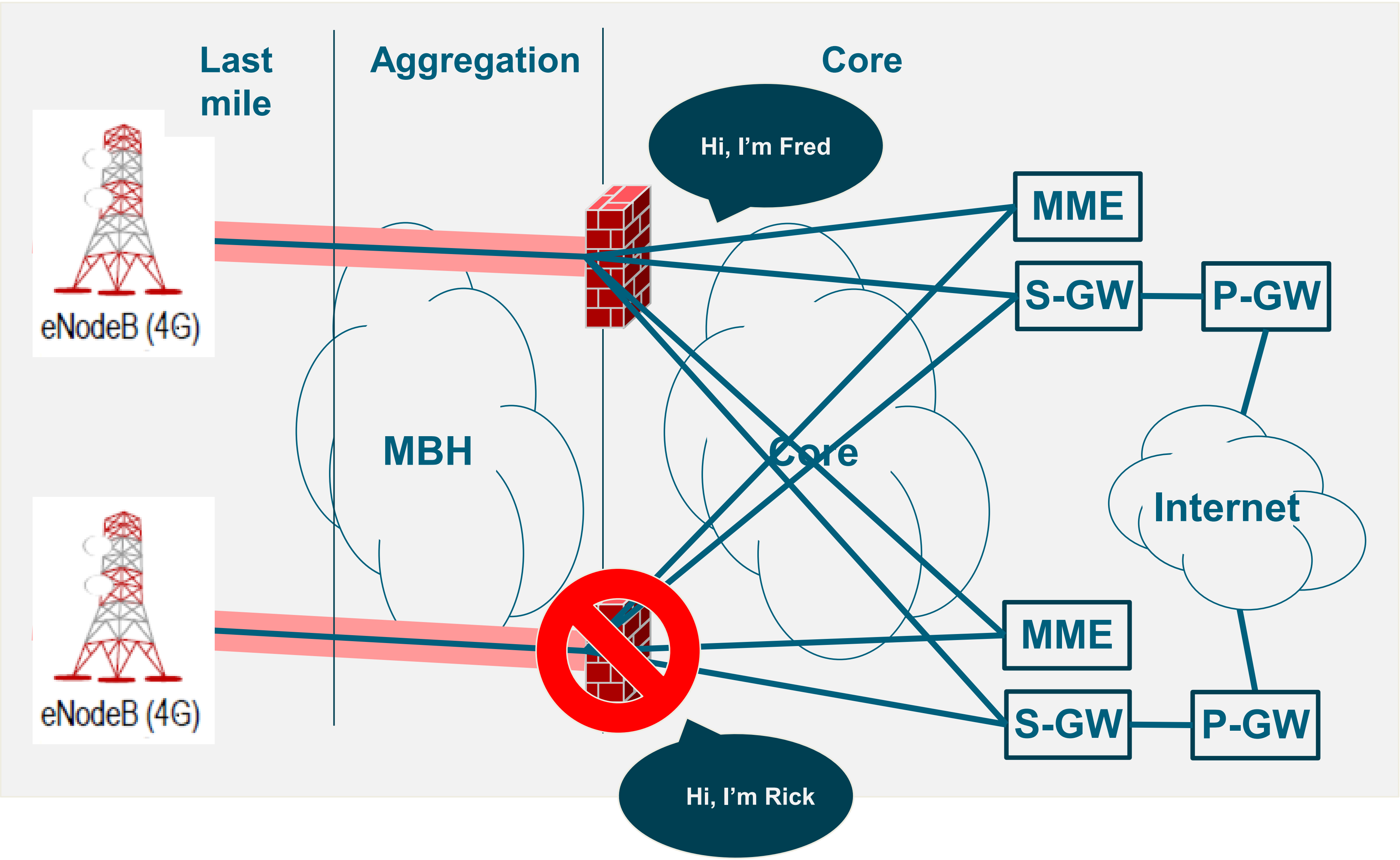


- Options for Geo-resilience?
  - Backup IPSec tunnels
  - Dynamic IP Routing

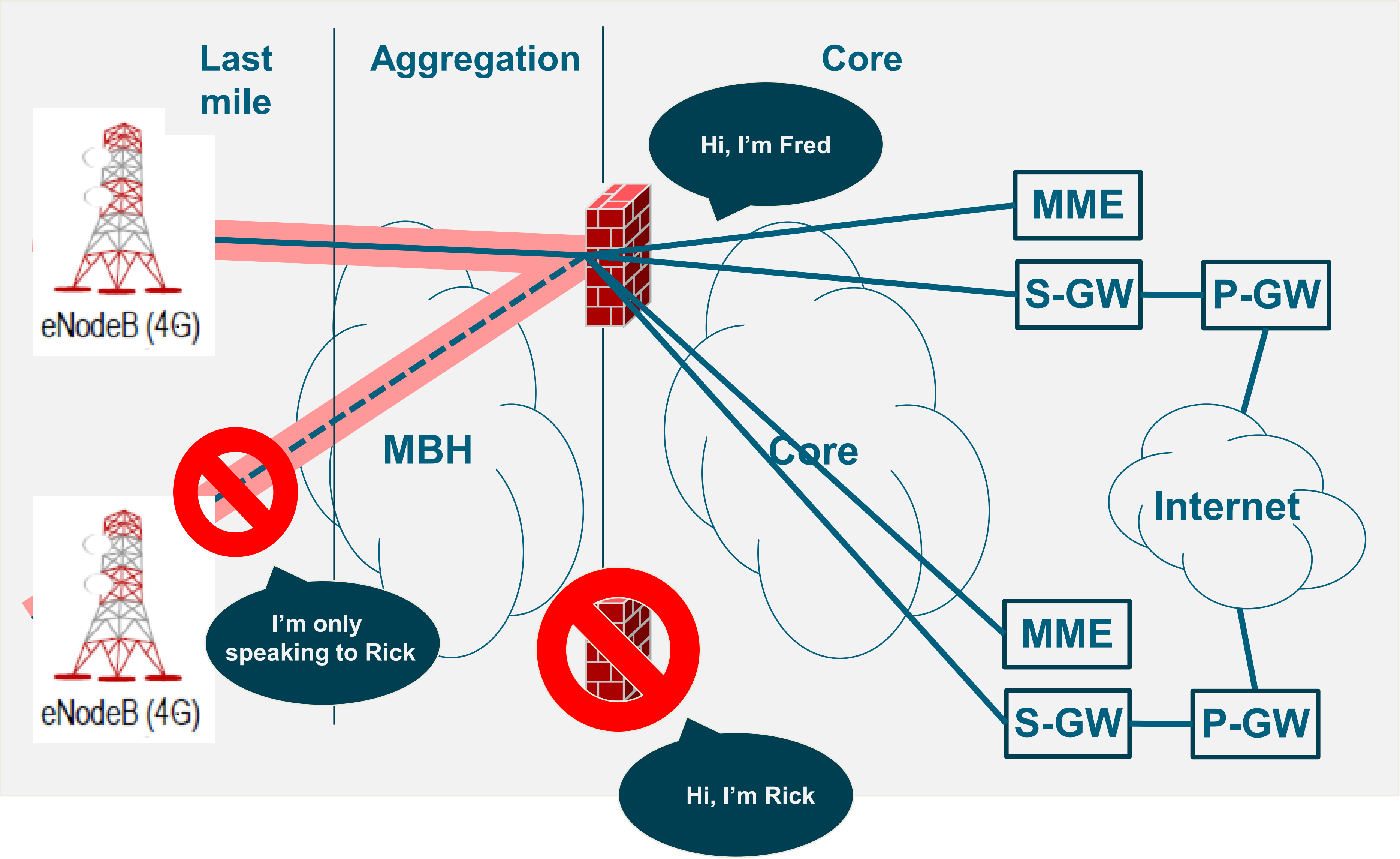
- Challenges with Geo-resilience?
  - IP Routing



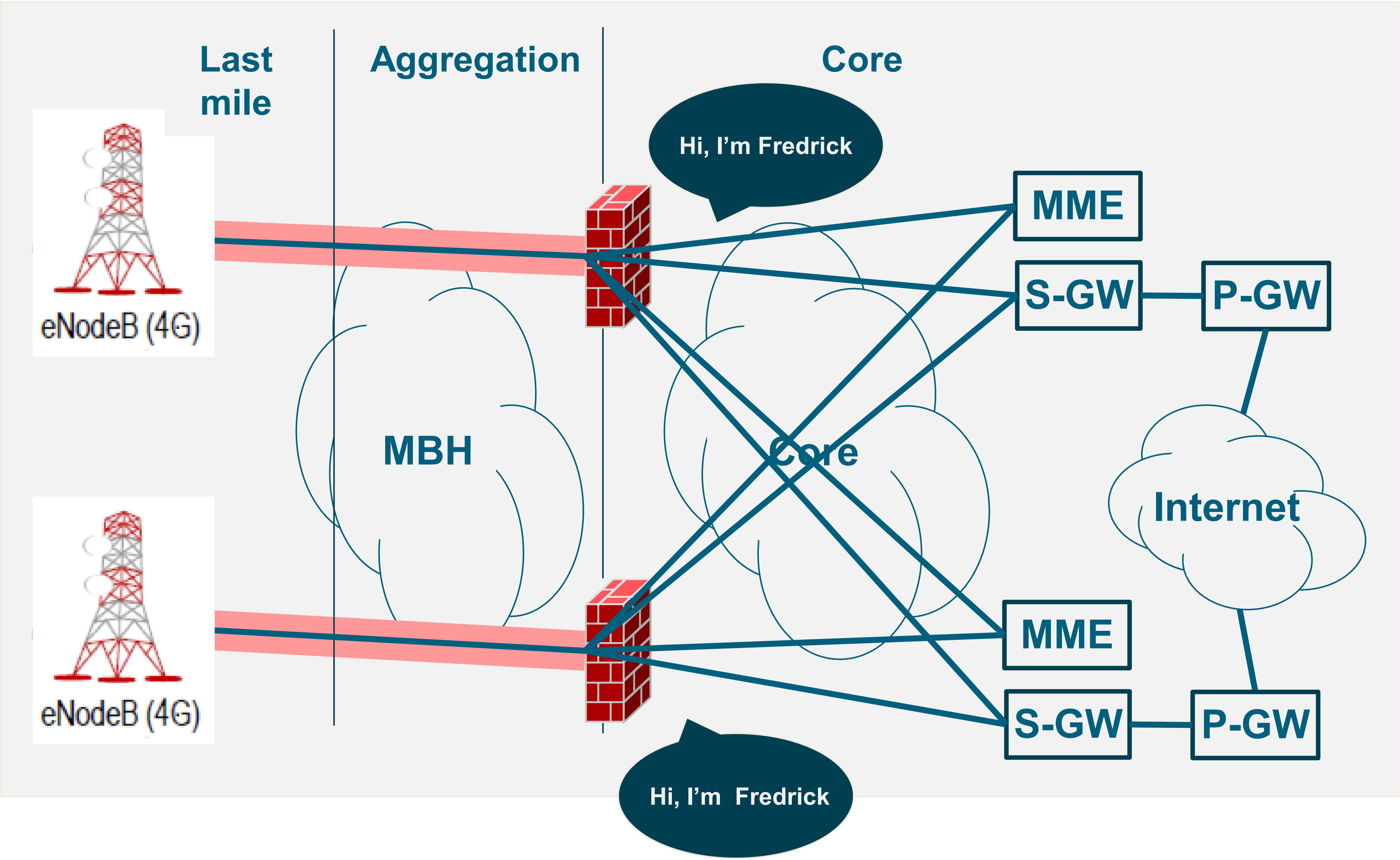
SubjectAltname field



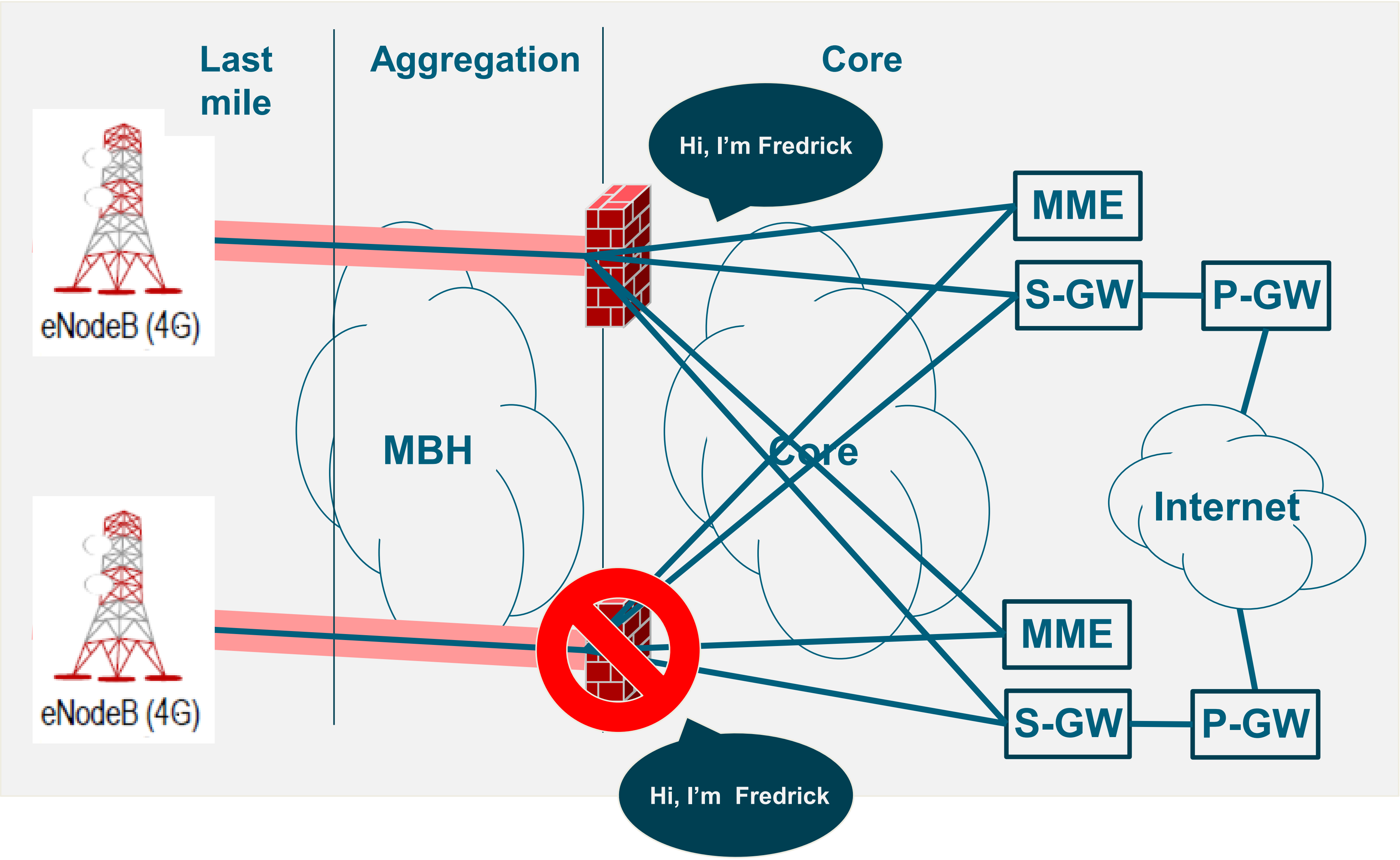
SubjectAltname field



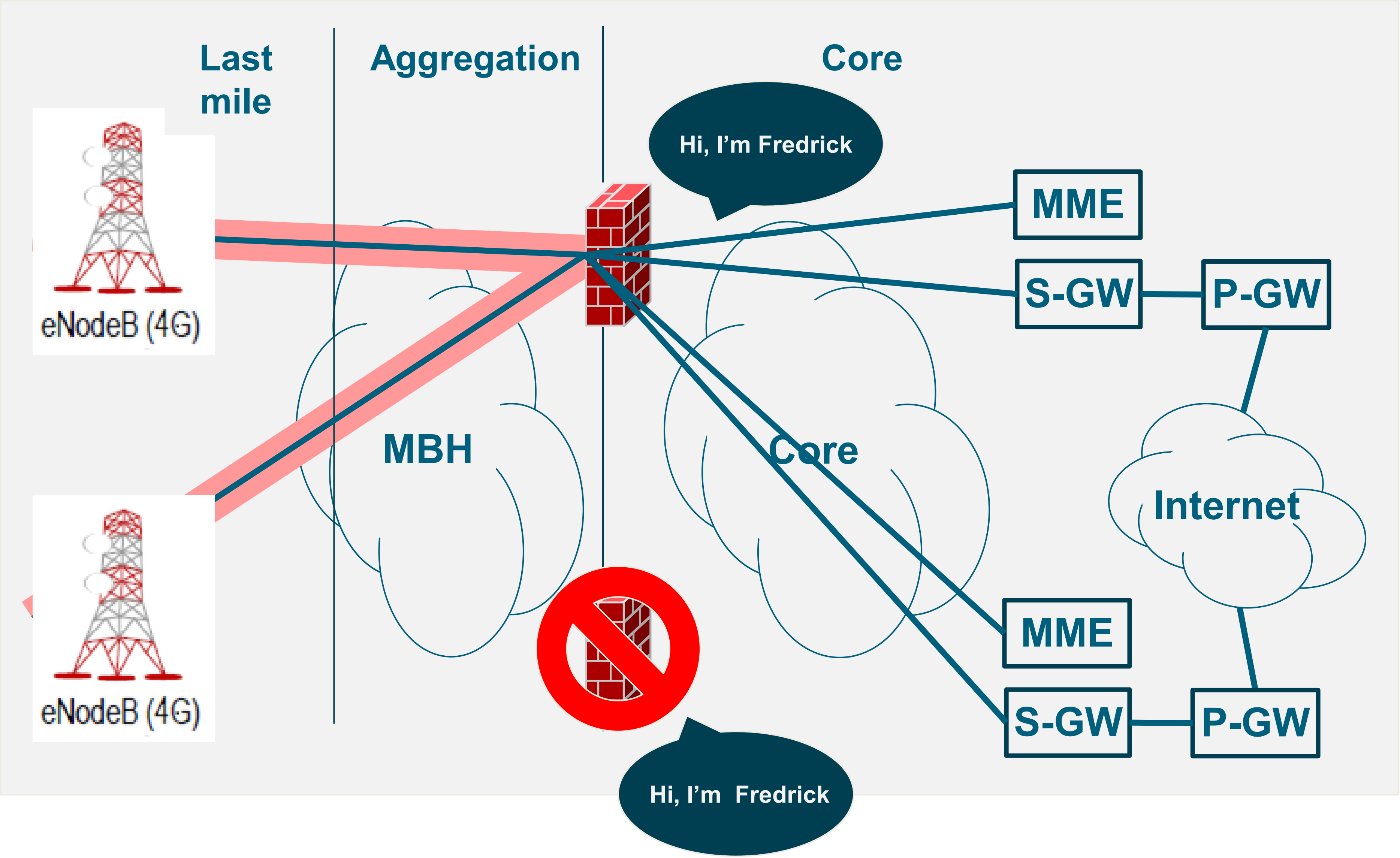
SubjectAltname field



SubjectAltname field



SubjectAltname field



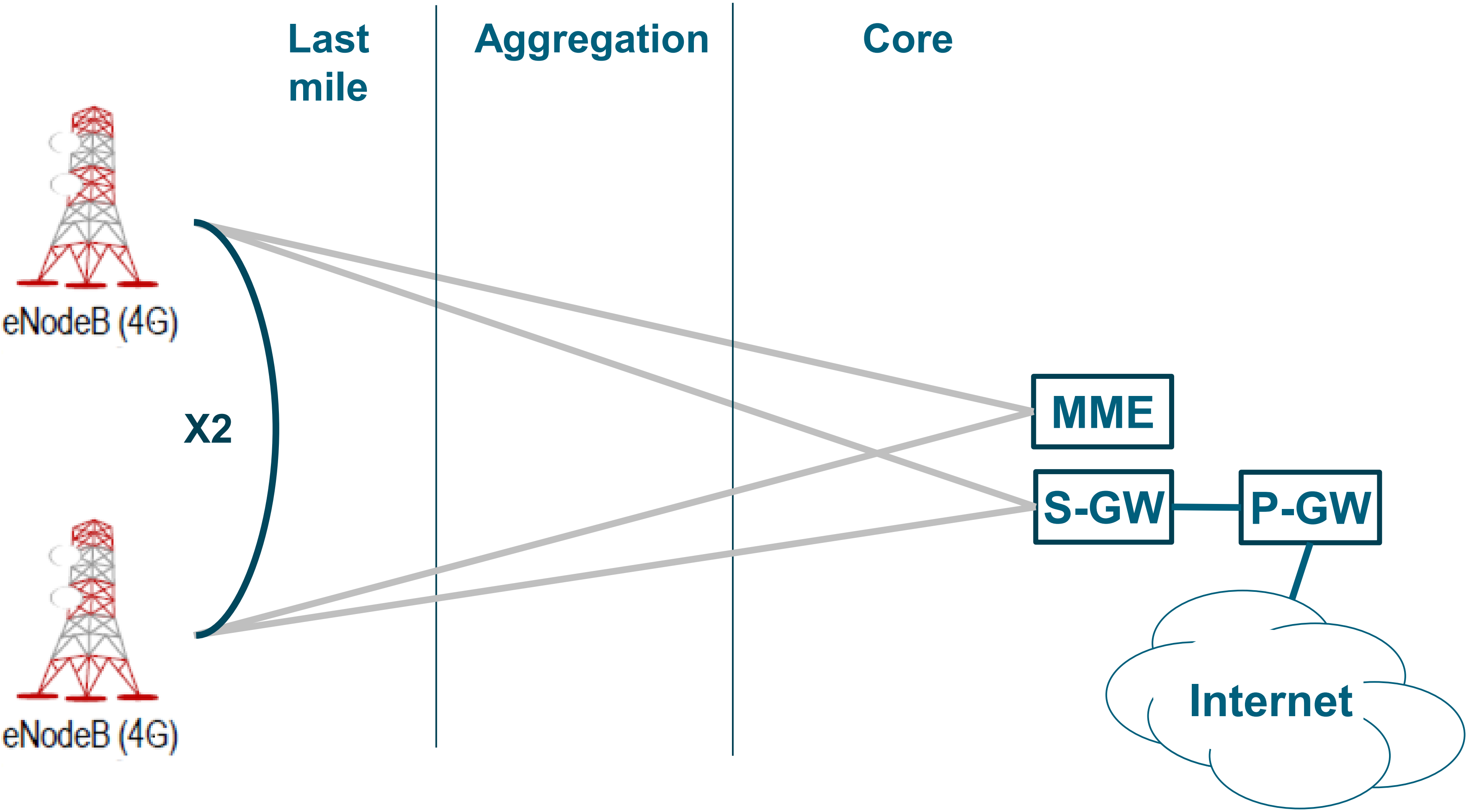
SubjectAltname field

06

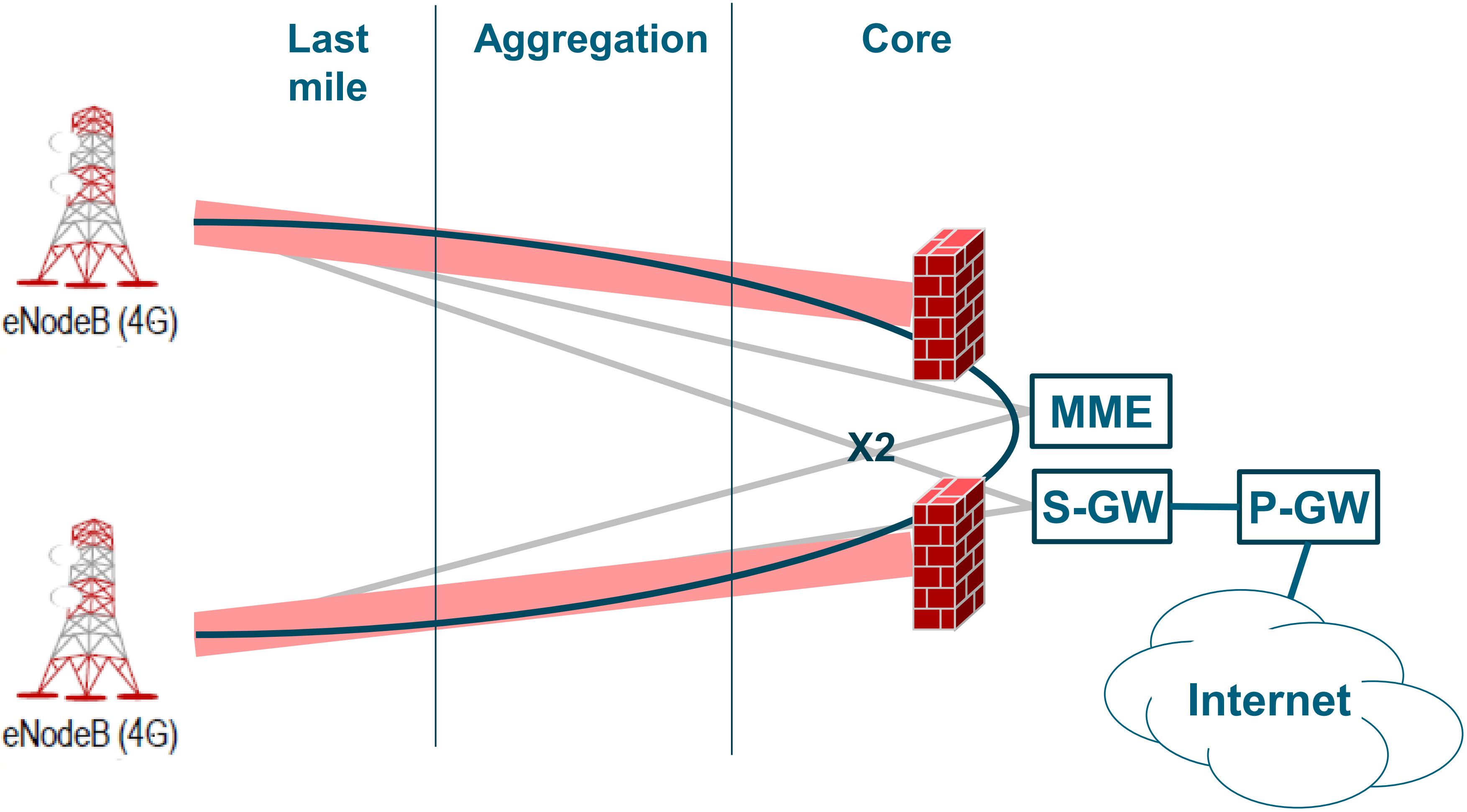
LTE - Advanced

LTE-Advanced

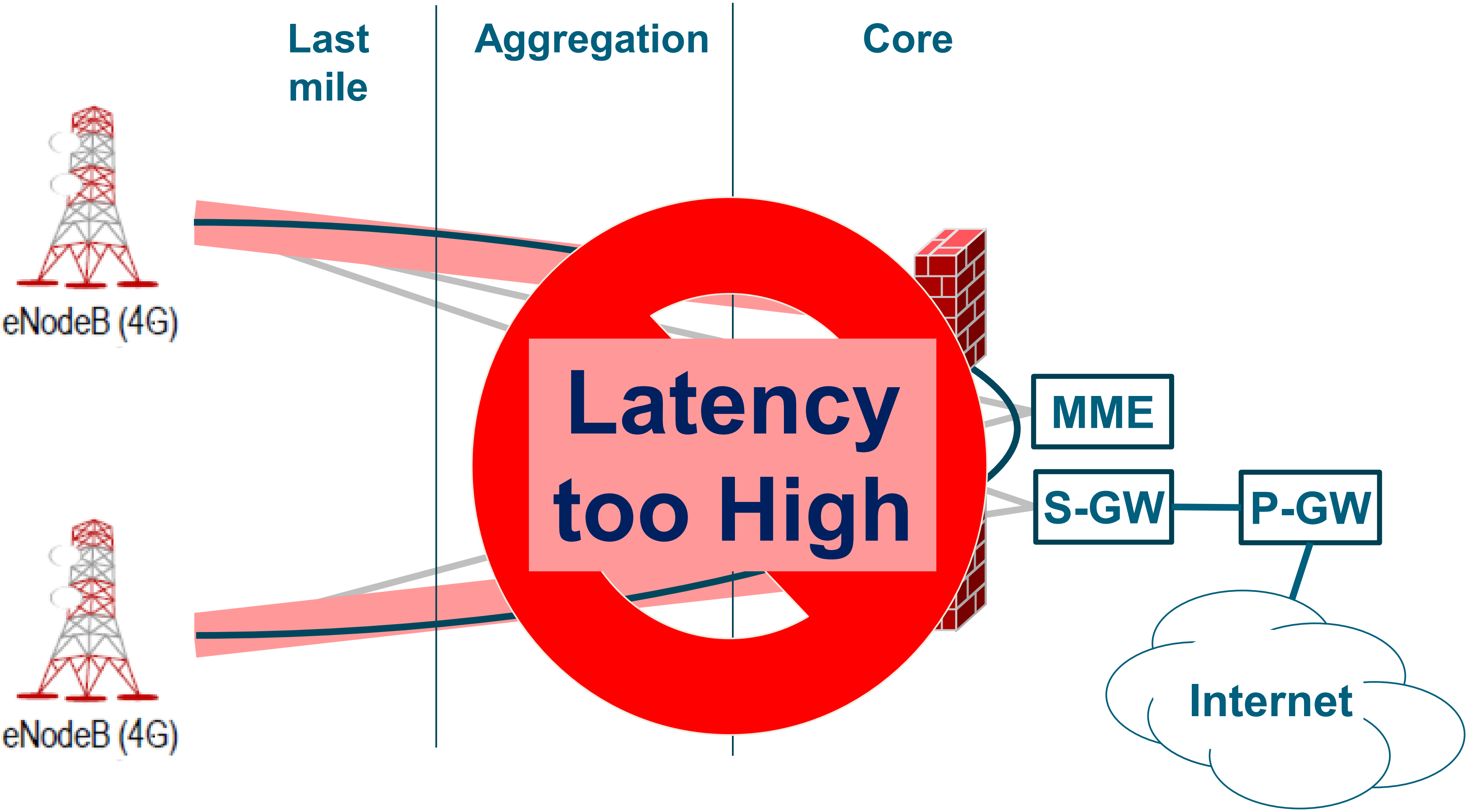
- How will we secure X2 traffic with the very stringent demands of LTE-A? Target latency above which a performance decrement is seen is 1ms.



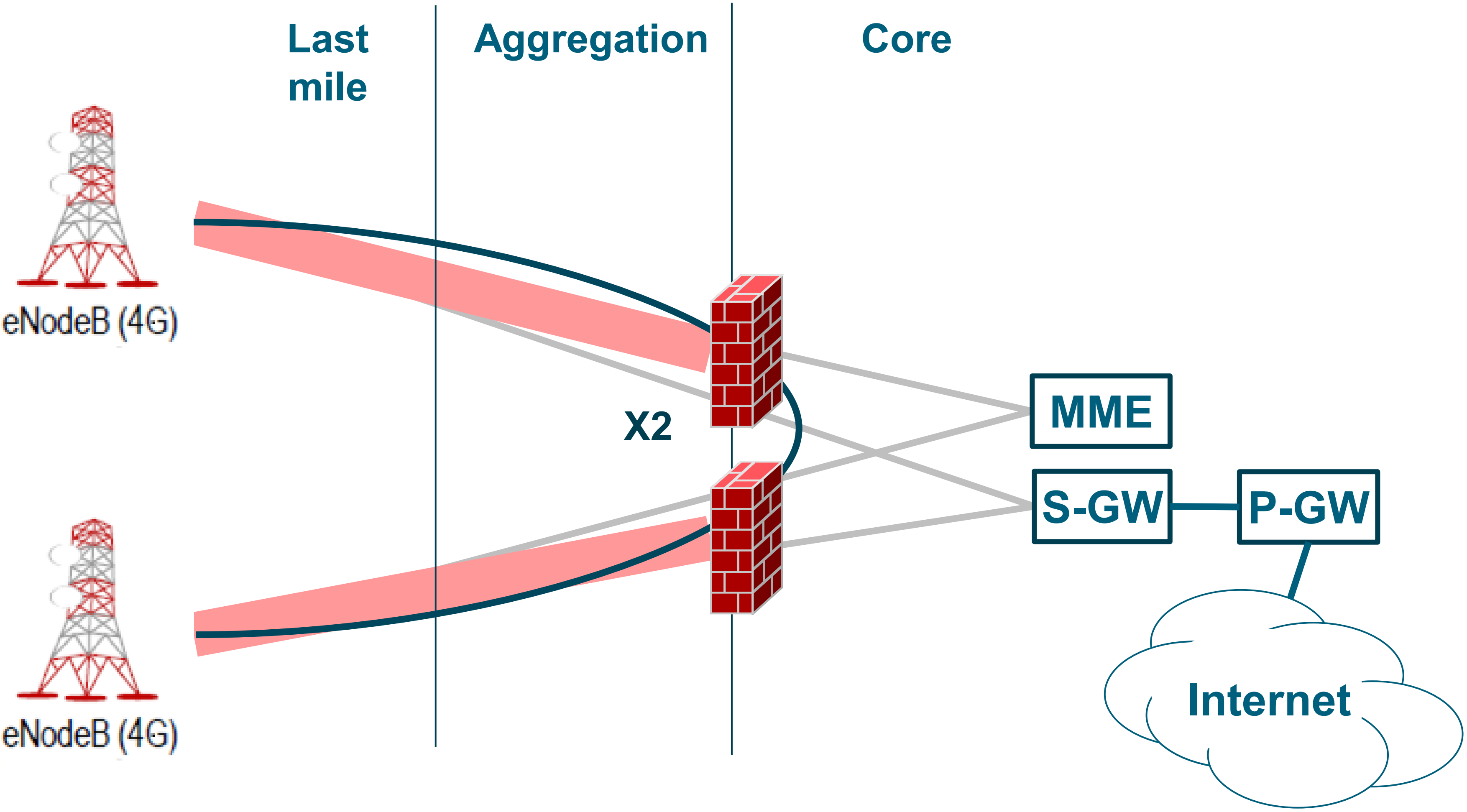
- **Where are you going to deploy the VPN concentrator for X2 handover?**



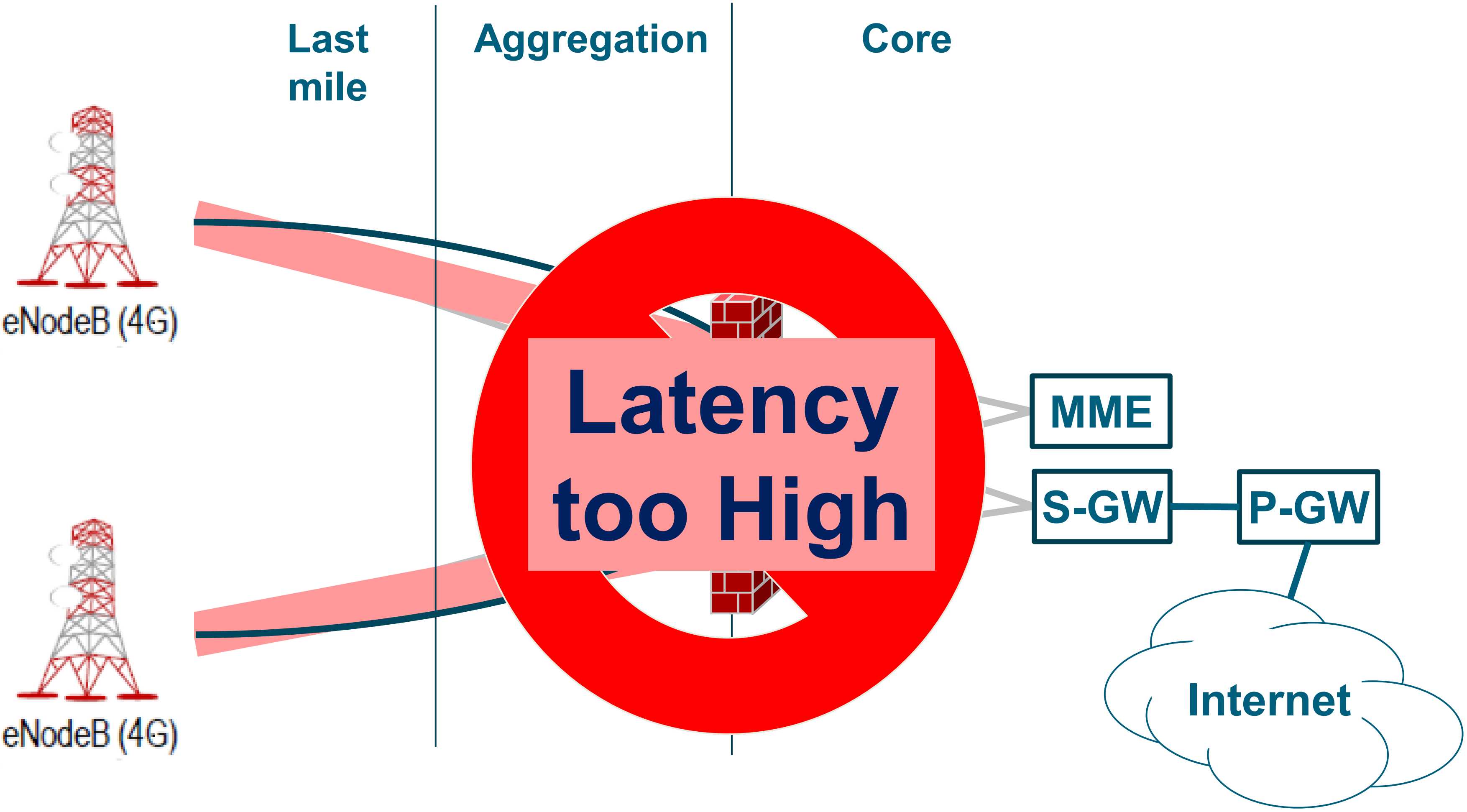
- **Option 1 – Centralised SecGW?**



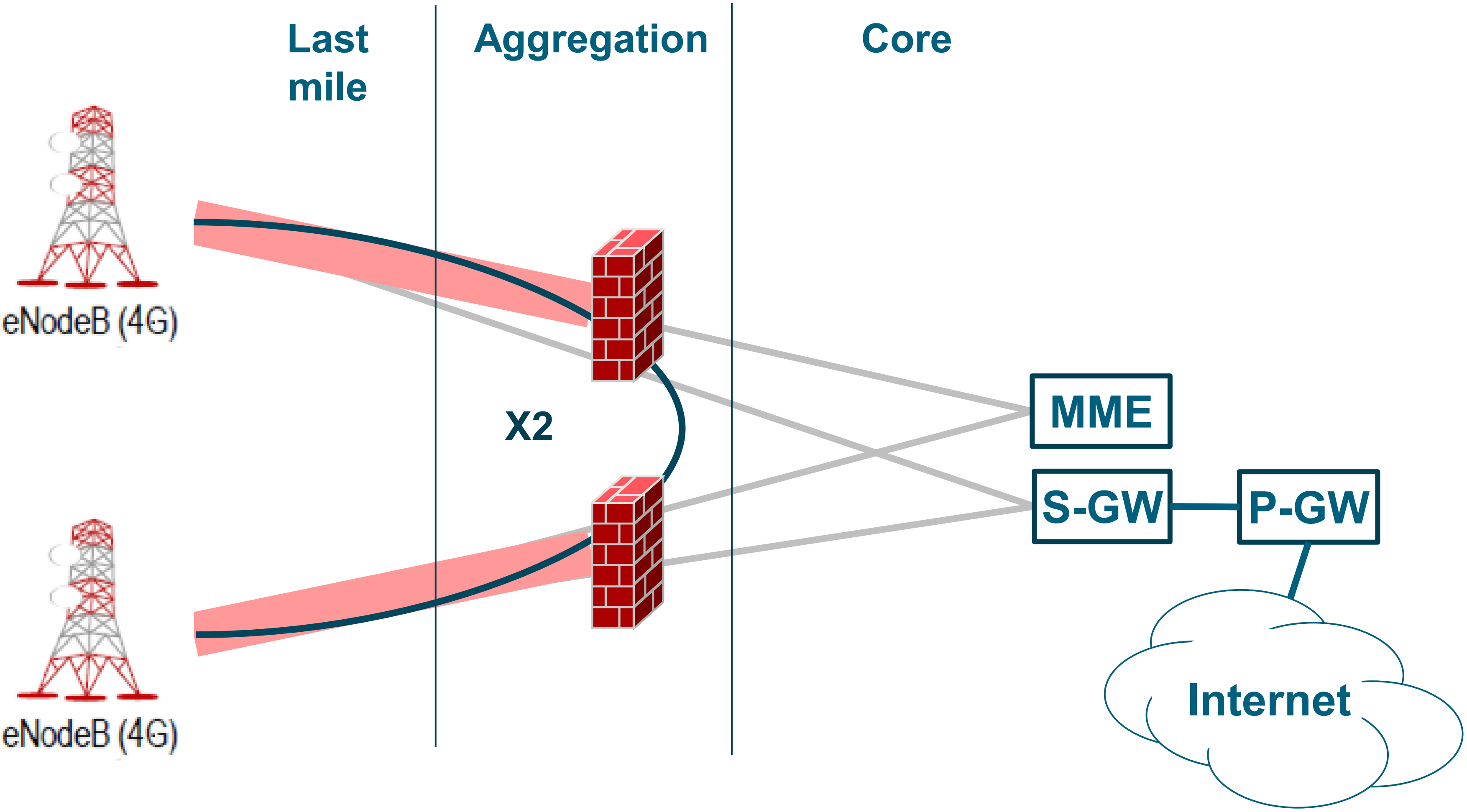
- Option 1 – Centralised SecGW?



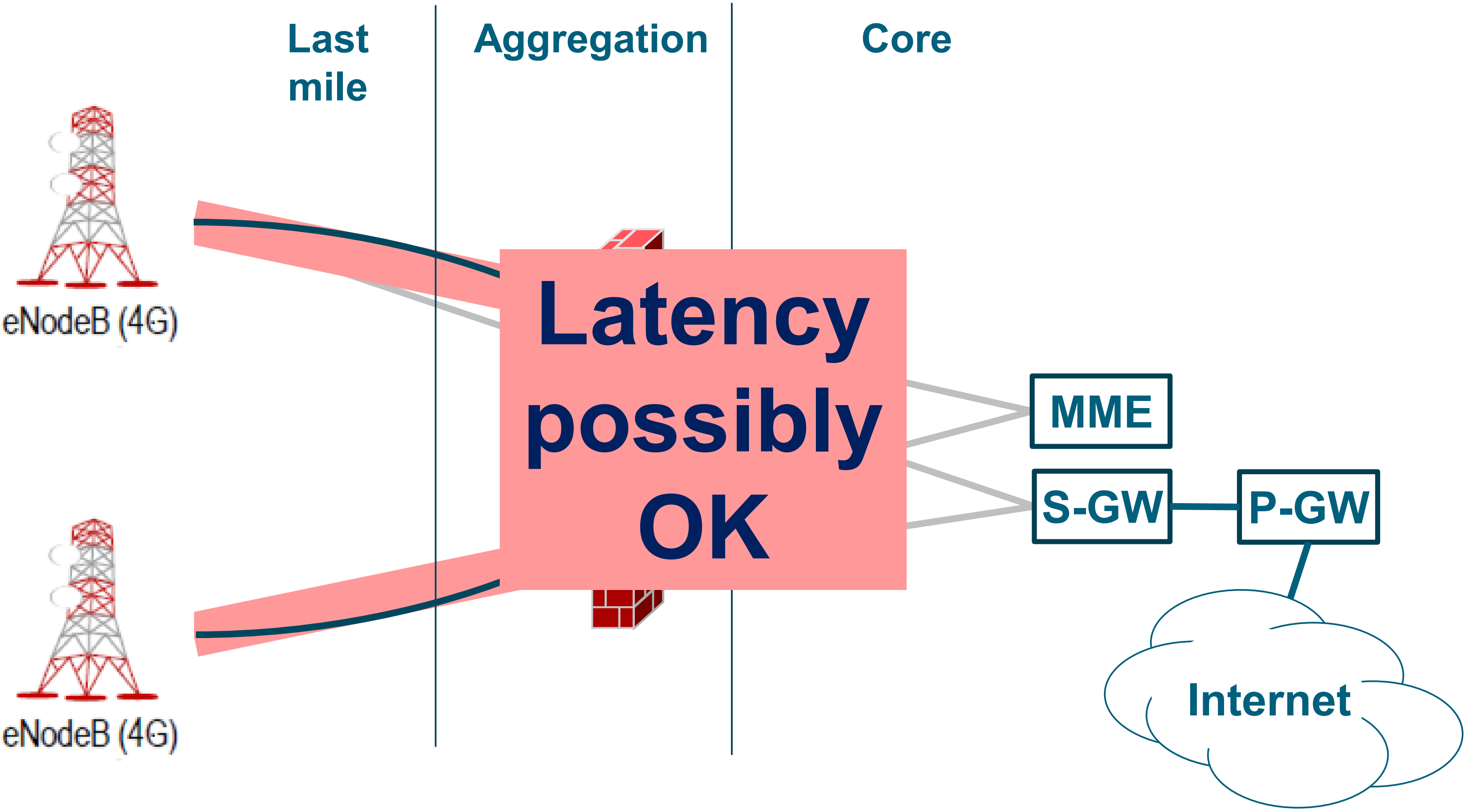
- **Option 2 – SecGW at Core Edge?**



- Option 2 – SecGW at Core Edge?

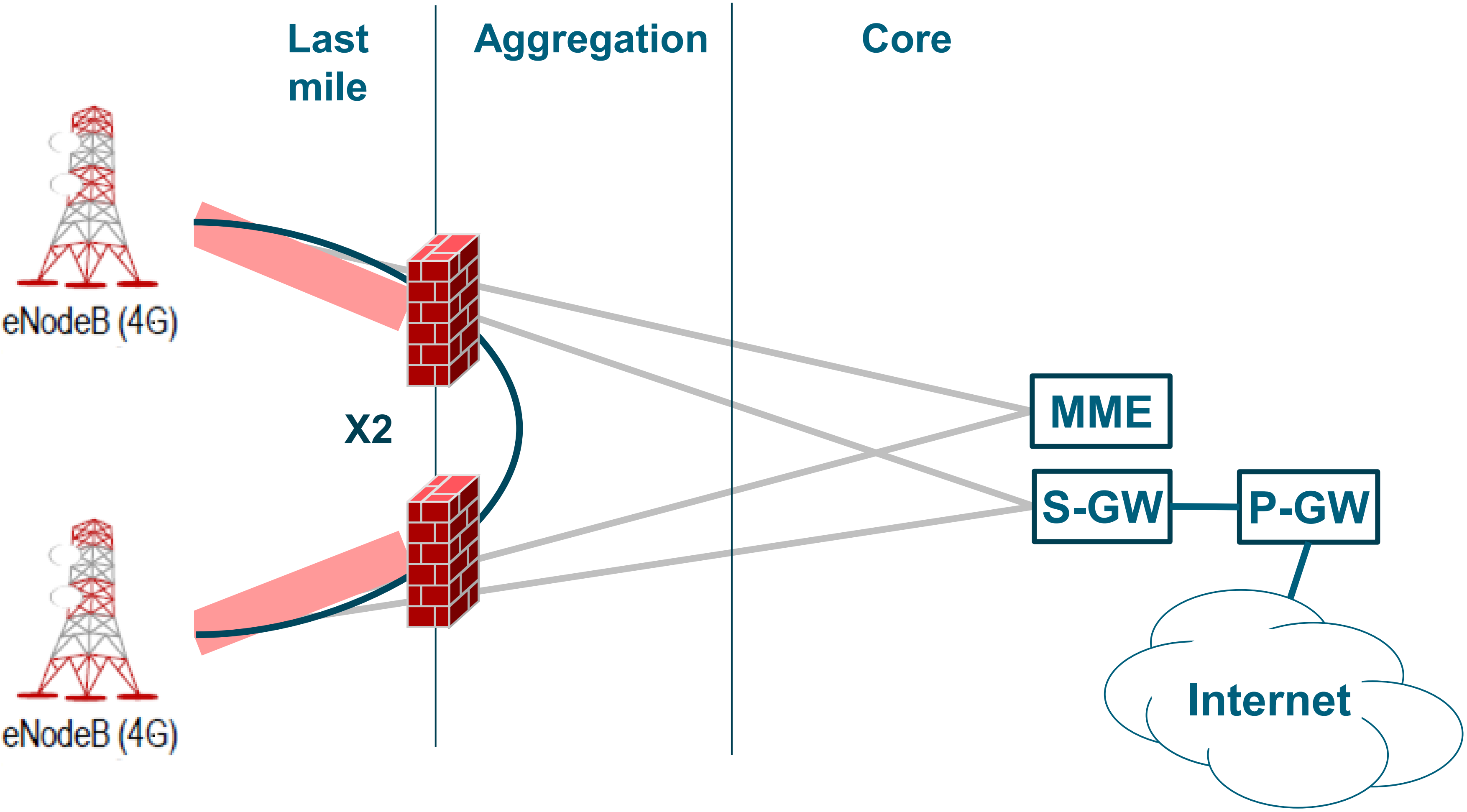


- Option 3 – Tens of SecGW distributed in Aggregation?

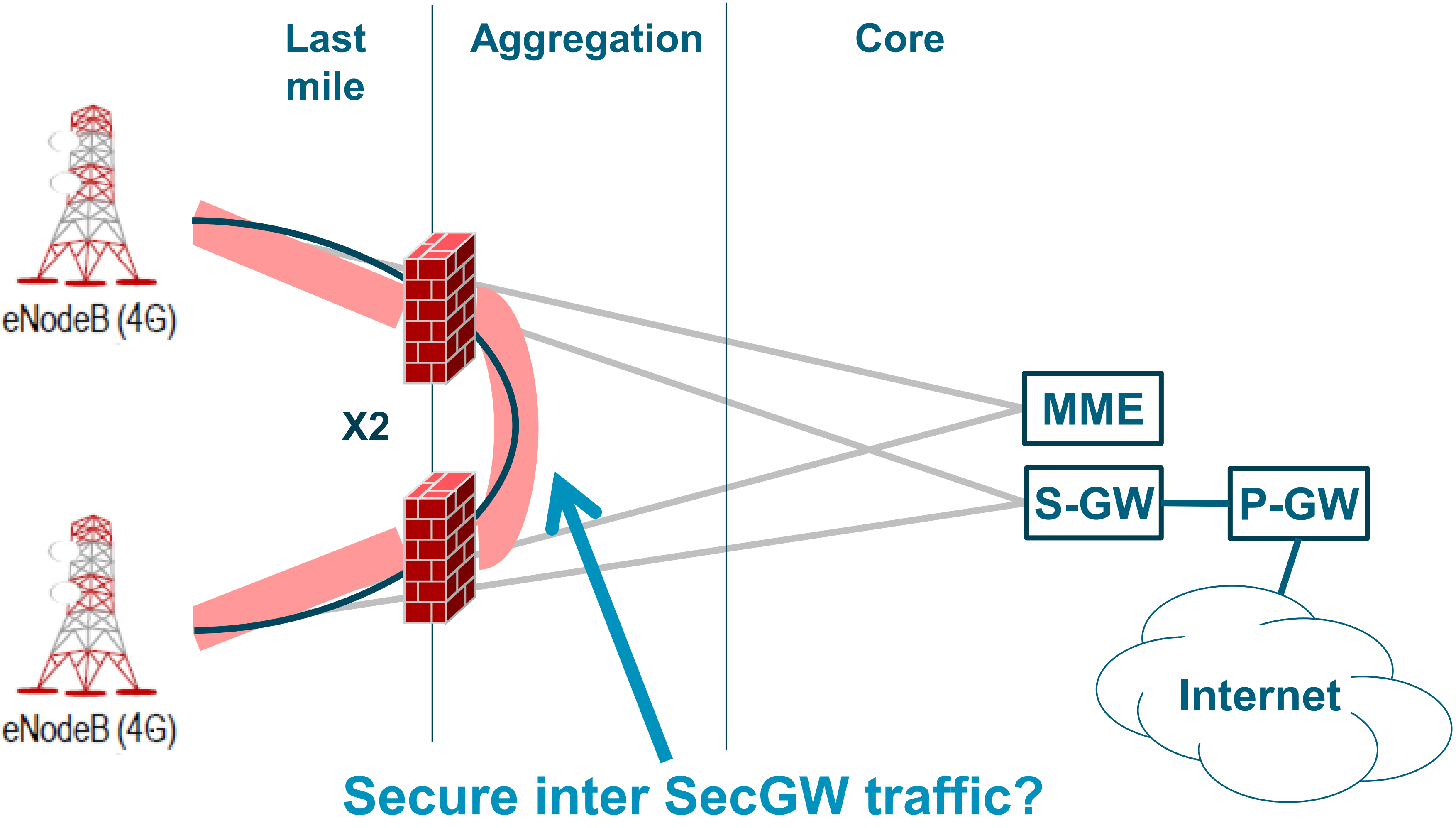


Latency possibly OK

- **Option 3 – Tens of SecGW distributed in Aggregation?**

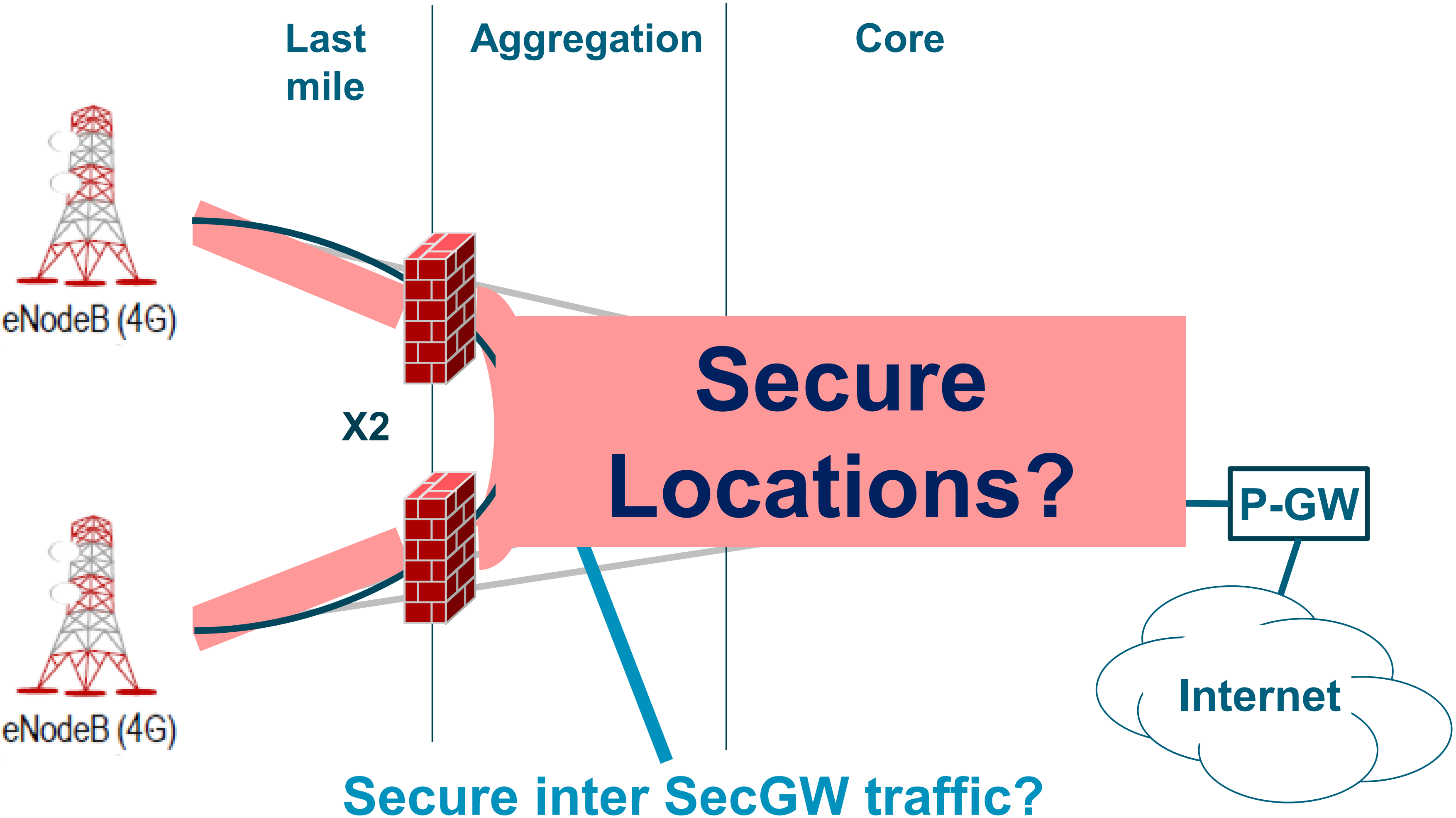


- **Option 4 – Hundreds of SecGW at local exchanges?**



Secure inter SecGW traffic?

- Option 4 – Hundreds of SecGW at local exchanges?



Last mile

Aggregation

Core

eNodeB (4G)

X2

eNodeB (4G)

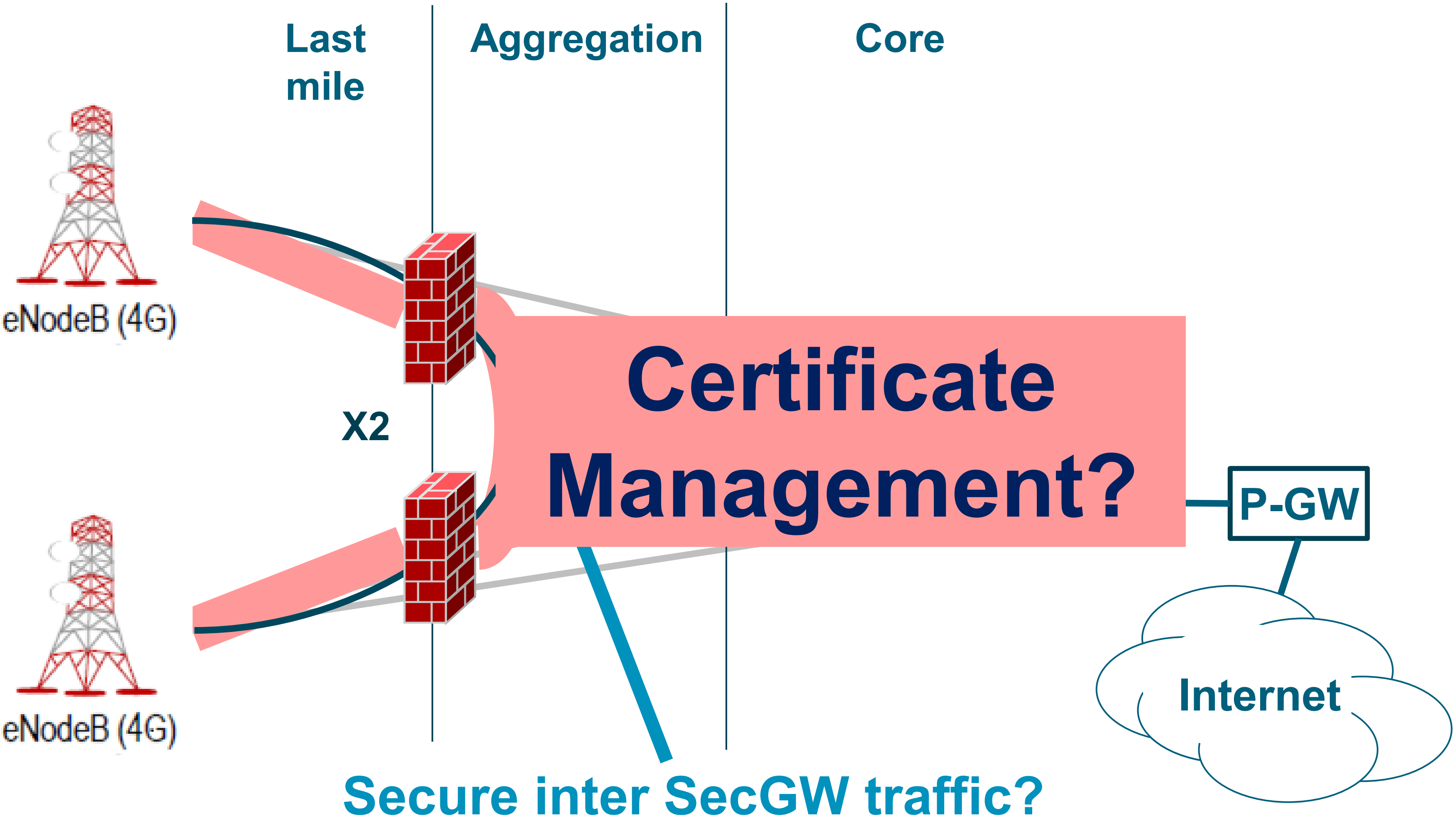
Secure Locations?

P-GW

Internet

Secure inter SecGW traffic?

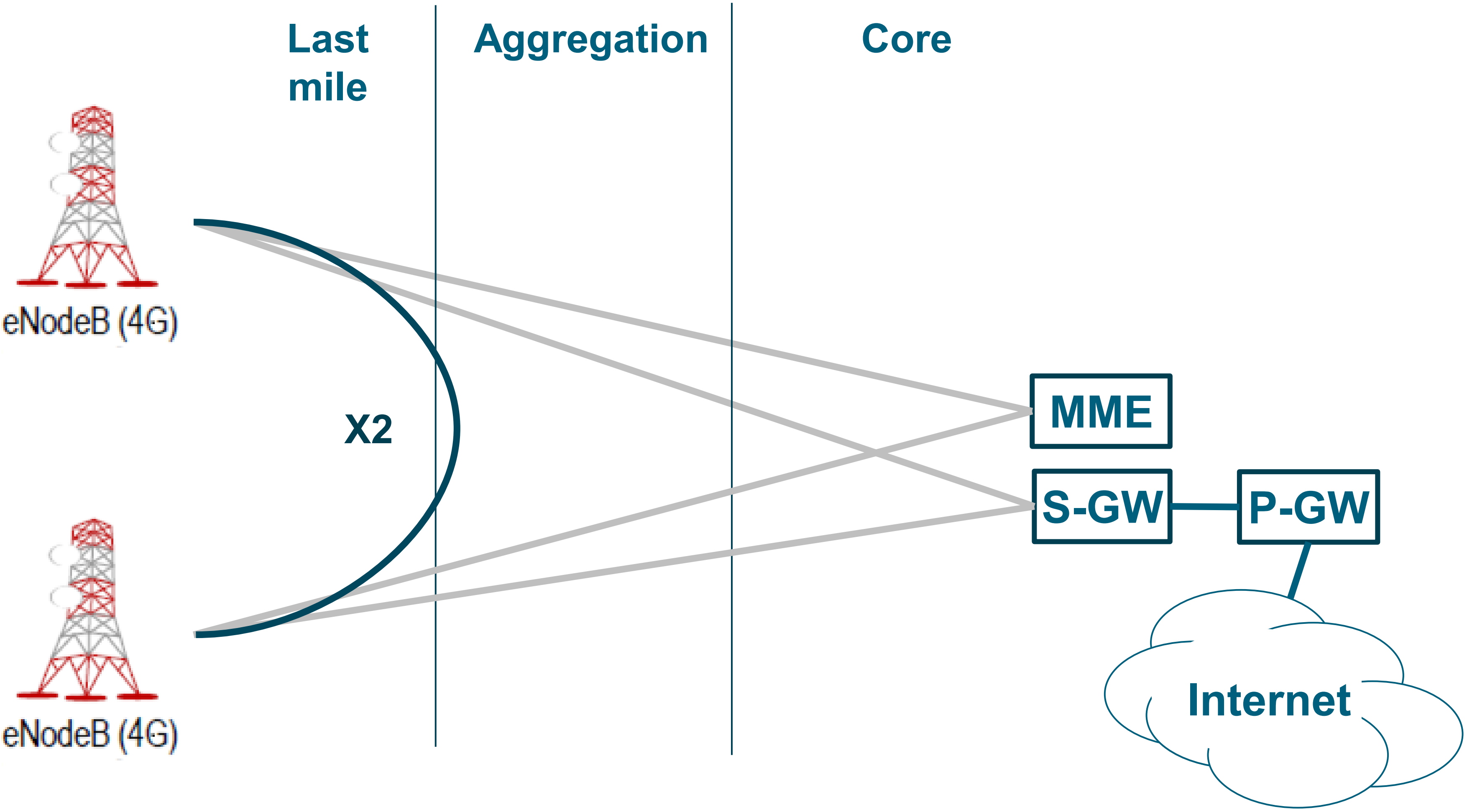
- Option 4 – Hundreds of SecGW at local exchanges?



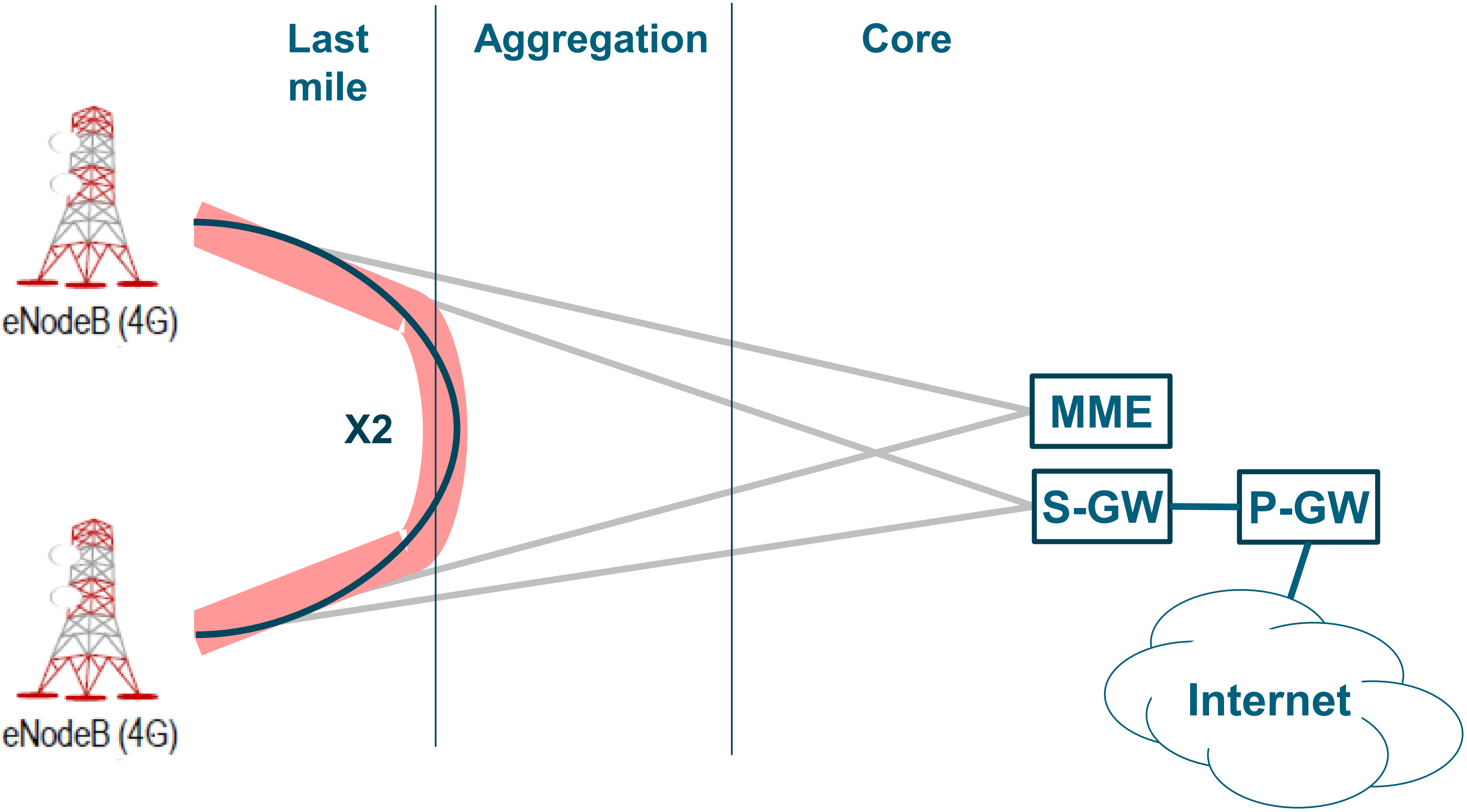
Certificate Management?

Secure inter SecGW traffic?

- Option 4 – Hundreds of SecGW at local exchanges?



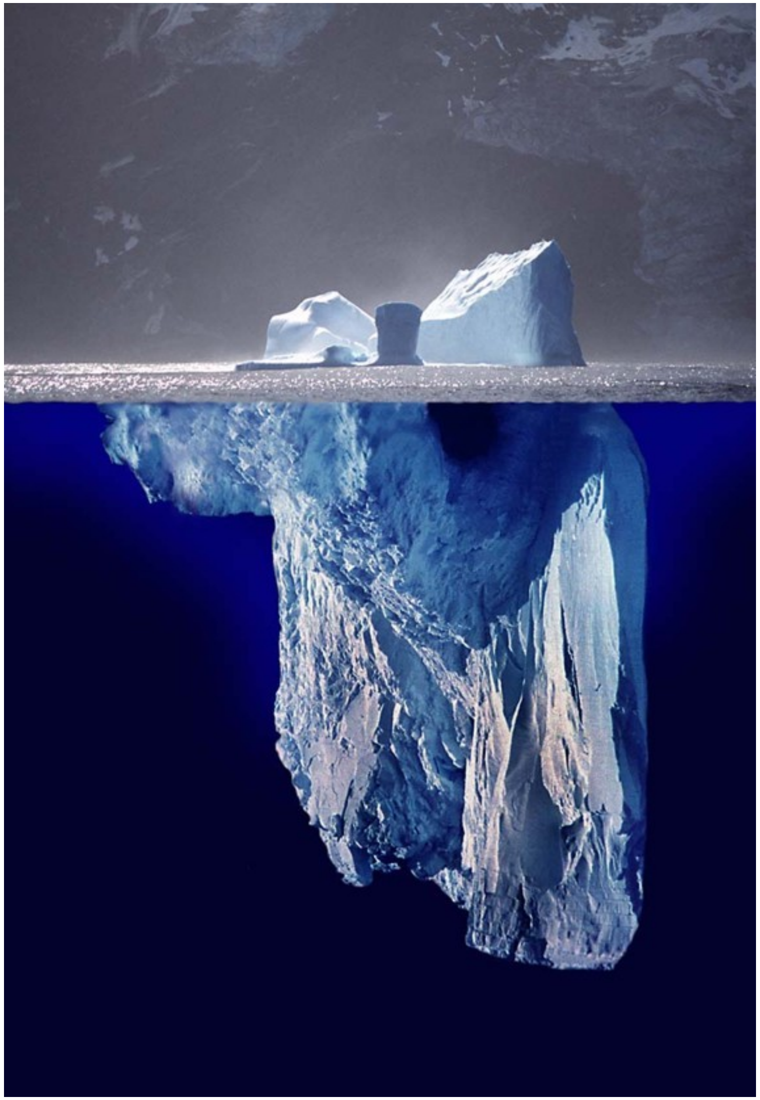
- **Option 5 – Don’t encrypt?**



- **Option 6 – No VPN concentrator ?**

- Summary
  - Simple – Just deploy LTE Security Gateway and encrypt with IPSec.
  - There's a few gotcha's to watch out for.
  - Keeping a multi operator and multi vendor deployed environment simple is not easy.

- Questions?



Thank You

Telefónica