BACKHAUL SECURITY CONSIDERATIONS AND IMPLEMENTATION OPTIONS

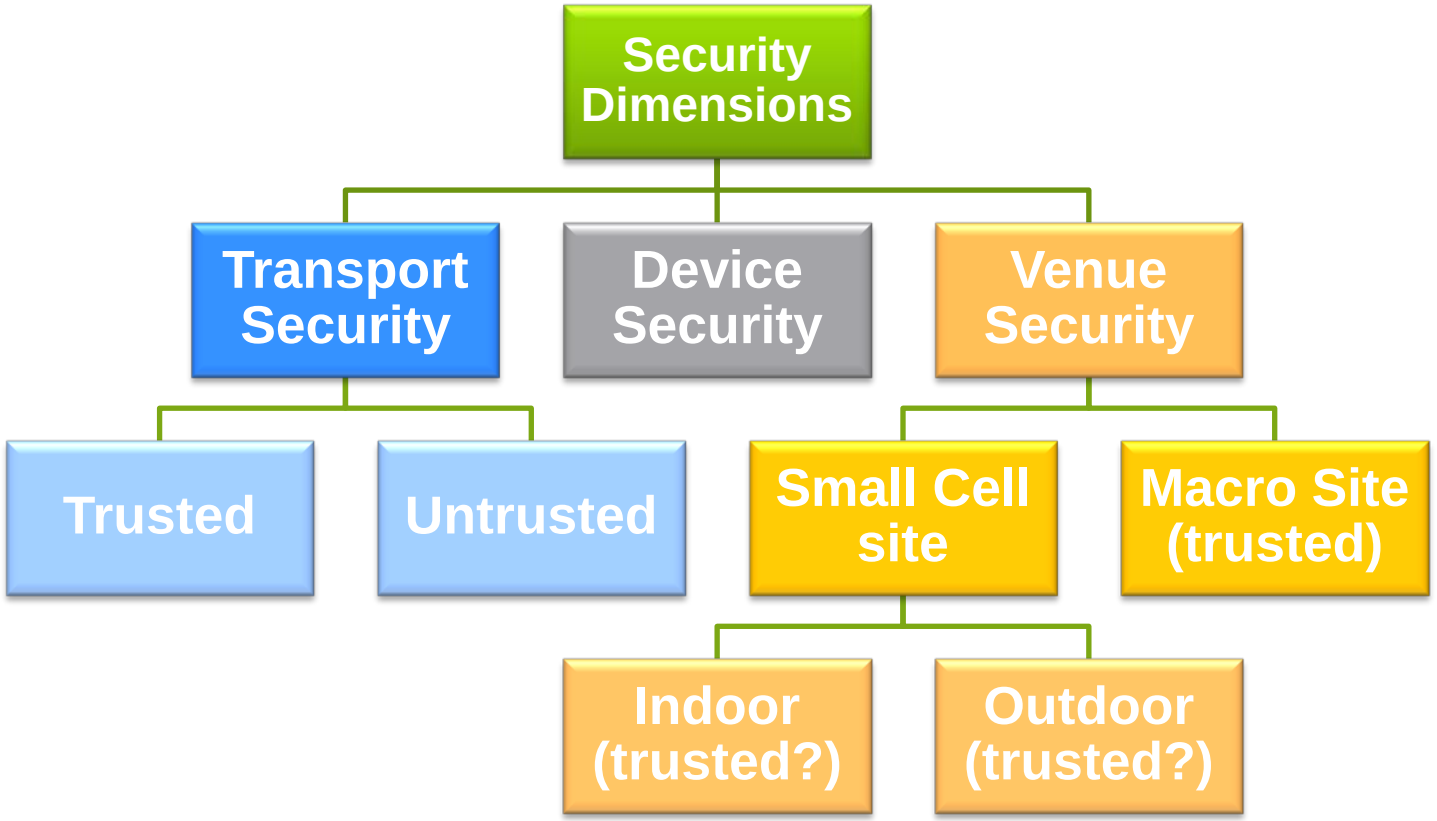
IEEE CQR Workshop
Tucson, AZ
May 12-15, 2014

Peter Staxen, MScEE, MBA
Mobile Backhaul Solution Manager
Ericsson Inc.
peter.staxen@ericsson.com

SCOPE

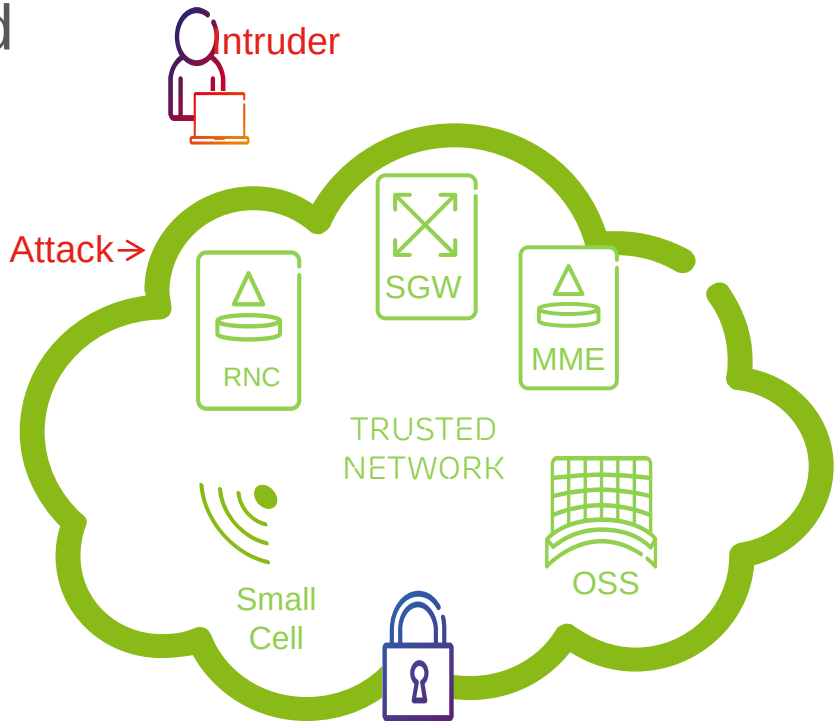
- Backhaul security driving forces
- Backhaul Security Architecture Options
- Security Architecture Impact on
  - Implementation complexity
  - Network performance
- Backhaul security in SDN/NFV era
- Conclusions

SECURITY DIMENSIONS



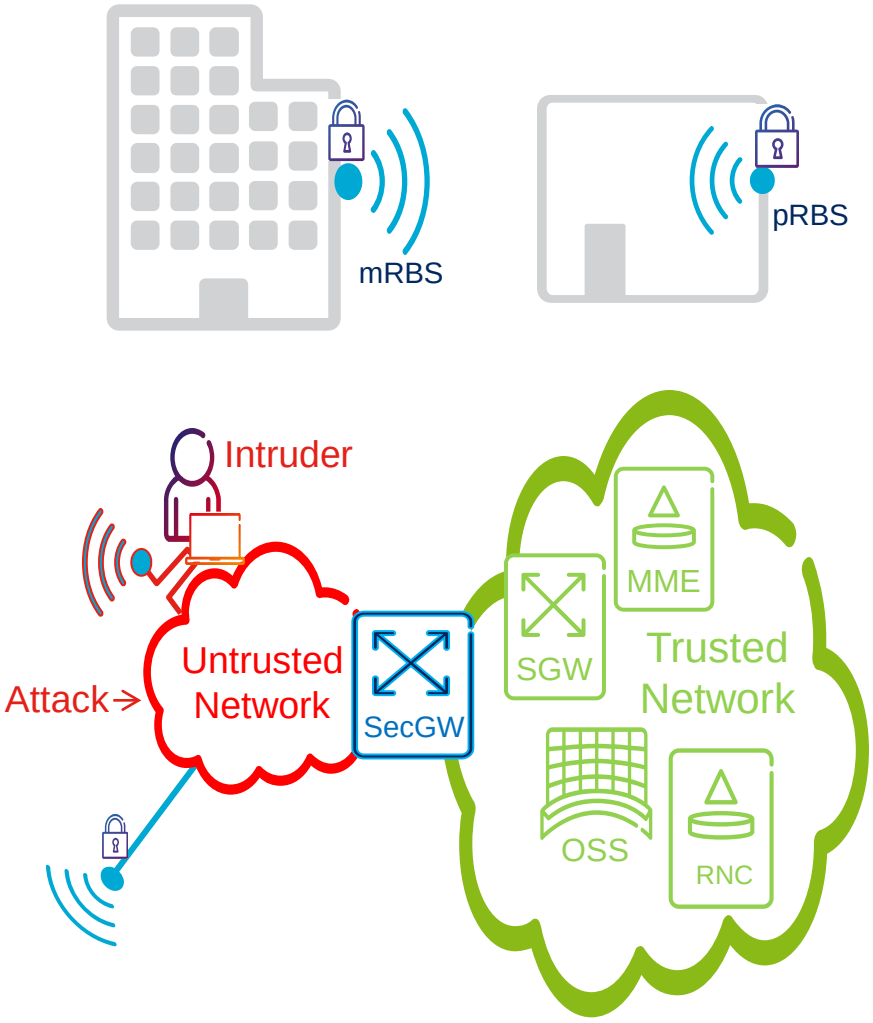
A TRUSTED ENVIRONMENT

- An environment where:
  - the operator has control over both network infrastructure and configurations
  - the transport network is considered secured against attack
    - Generally, the same TN on which the macro network is deployed
  - the location is physically secured
    - Secure enclosure and/or a locked room



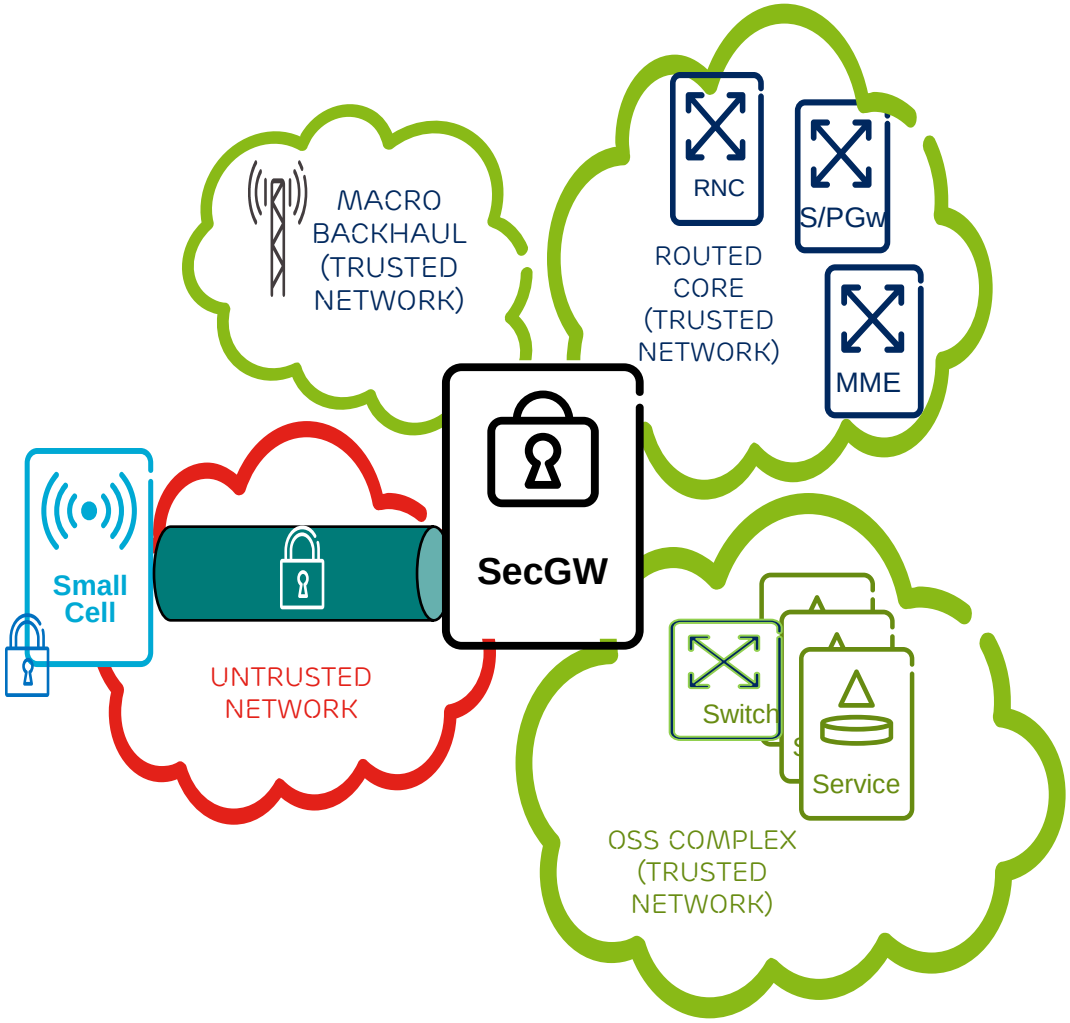
AN UNTRUSTED ENVIRONMENT

- An environment where:
  - ‘Public’ networks are used as backhaul
  - The operator has little or no control over the transport network infrastructure and configurations
  - Locations of the small cell is physically exposed

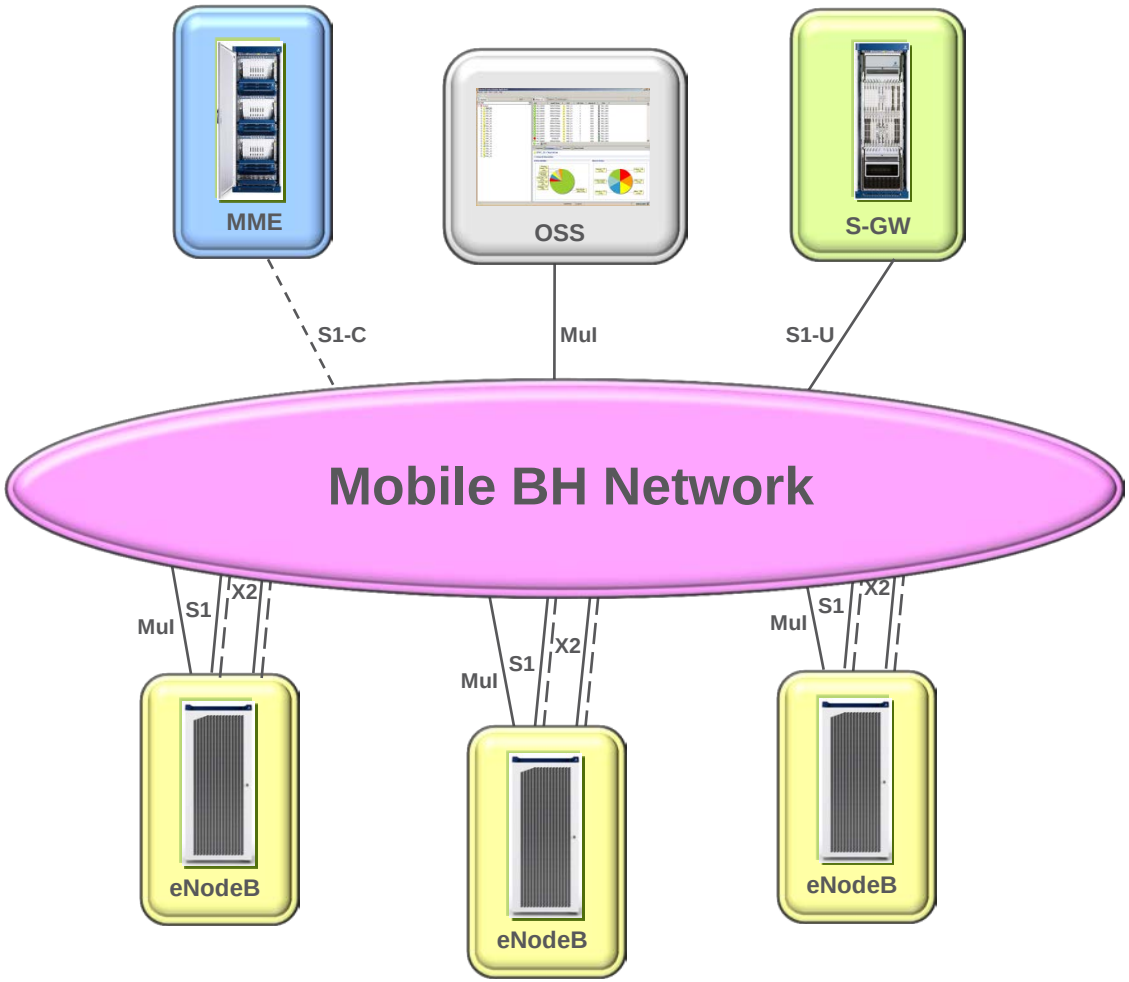


IMPACT OF UNTRUSTED BACKHAUL

- Need IPSec
  - To prevent traffic being intercepted between small Cells and Secure Core/OSS Complex
  - To 'hide' the infrastructure behind the SecGW
- Need Authentication
  - Nodes shall be able to identify themselves both as
    a) An Vendor node
    b) An Operator node
- IPSec/Auth supported as an integrated part of the Auto-integration small cells

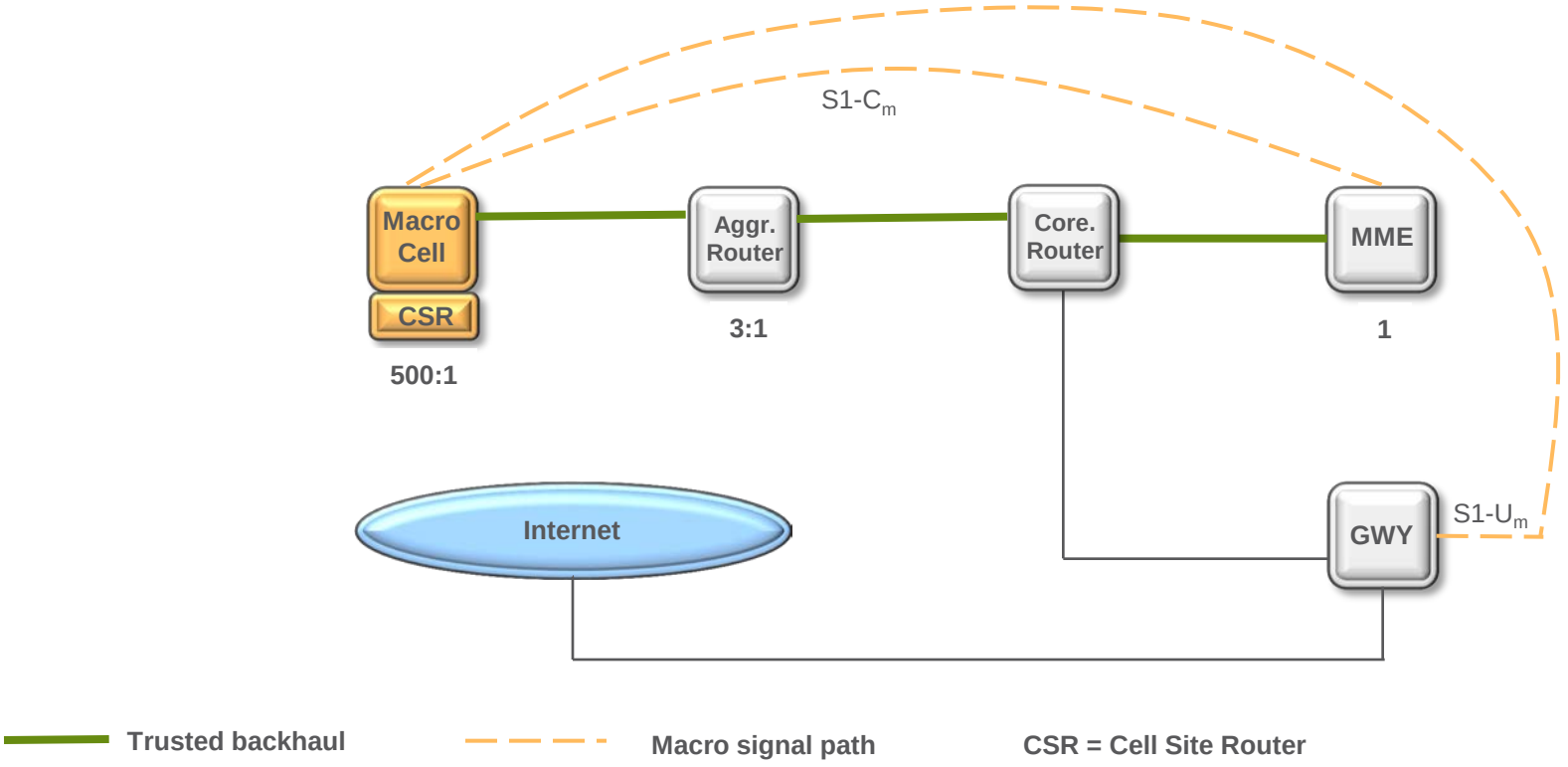


LTE FROM BH PERSPECTIVE

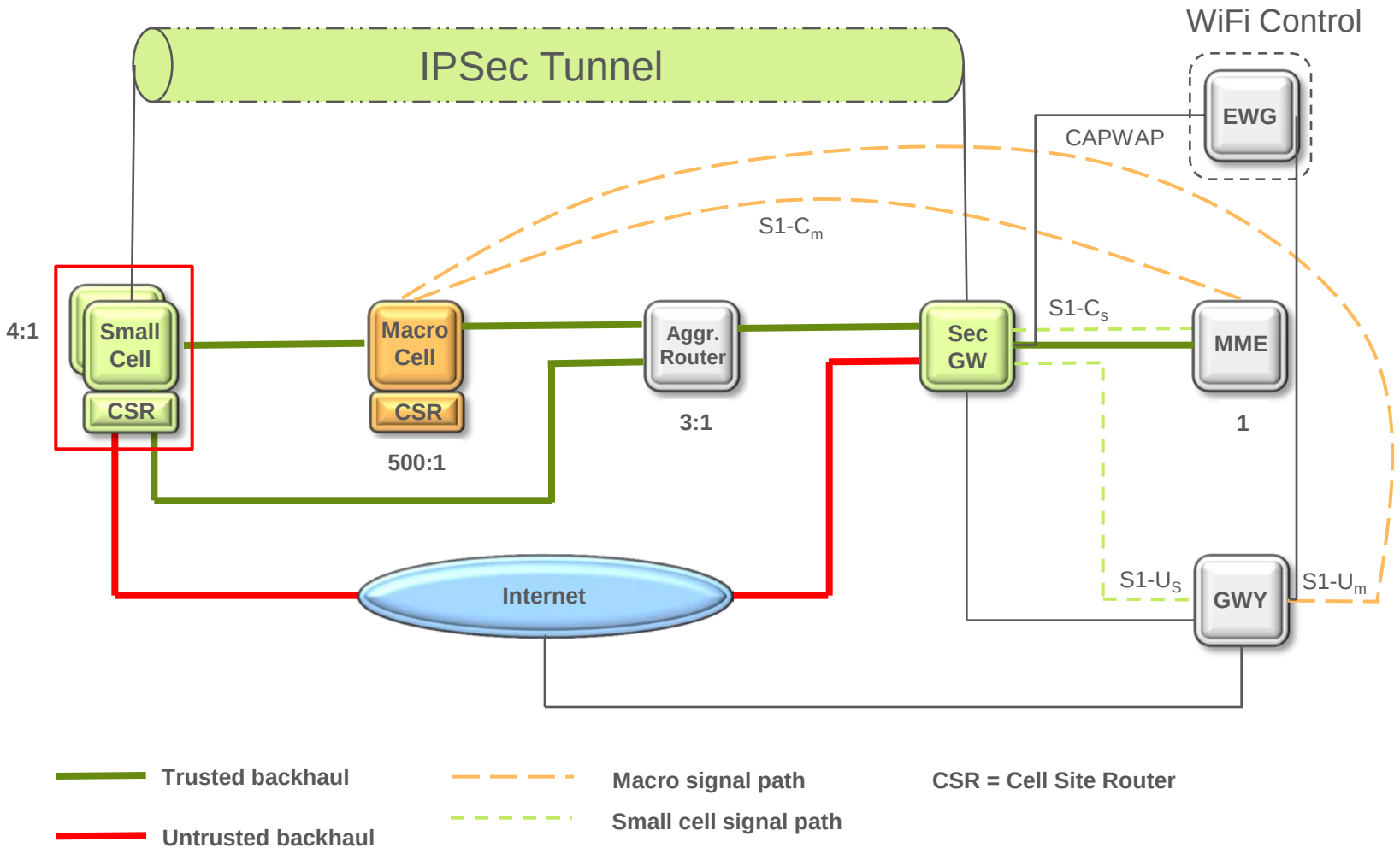


MACRO BACKHAUL SECURITY
PRINCIPAL ARCHITECTURE

- VLAN separation of bearer and O&M traffic
- IP Subnet separation of bearer and O&M traffic
- Separate routing contexts for bearer and O&M traffic

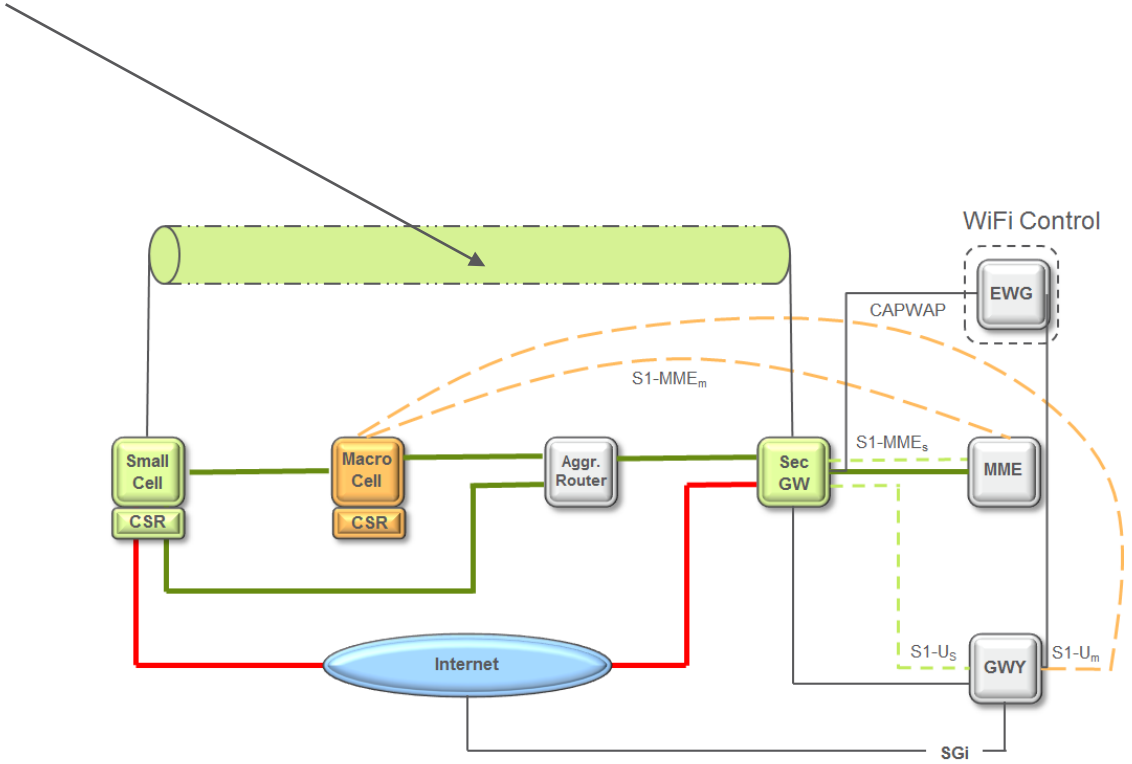


HETNET BACKHAUL SECURITY
PRINCIPAL ARCHITECTURE

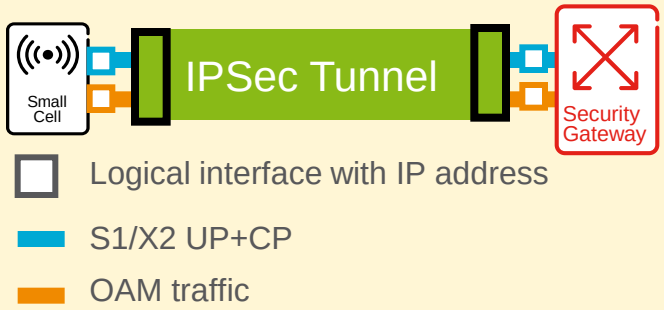


IPSEC CHOICES

- What goes into the IP tunnel?
- How many IP tunnels?
- Where do we terminate the tunnel?

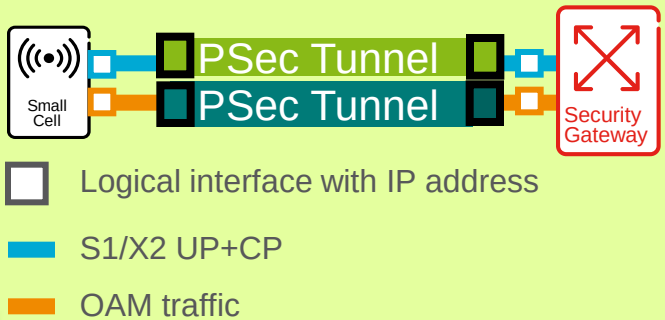


IPSEC SCENARIOS



Single IPsec Tunnel

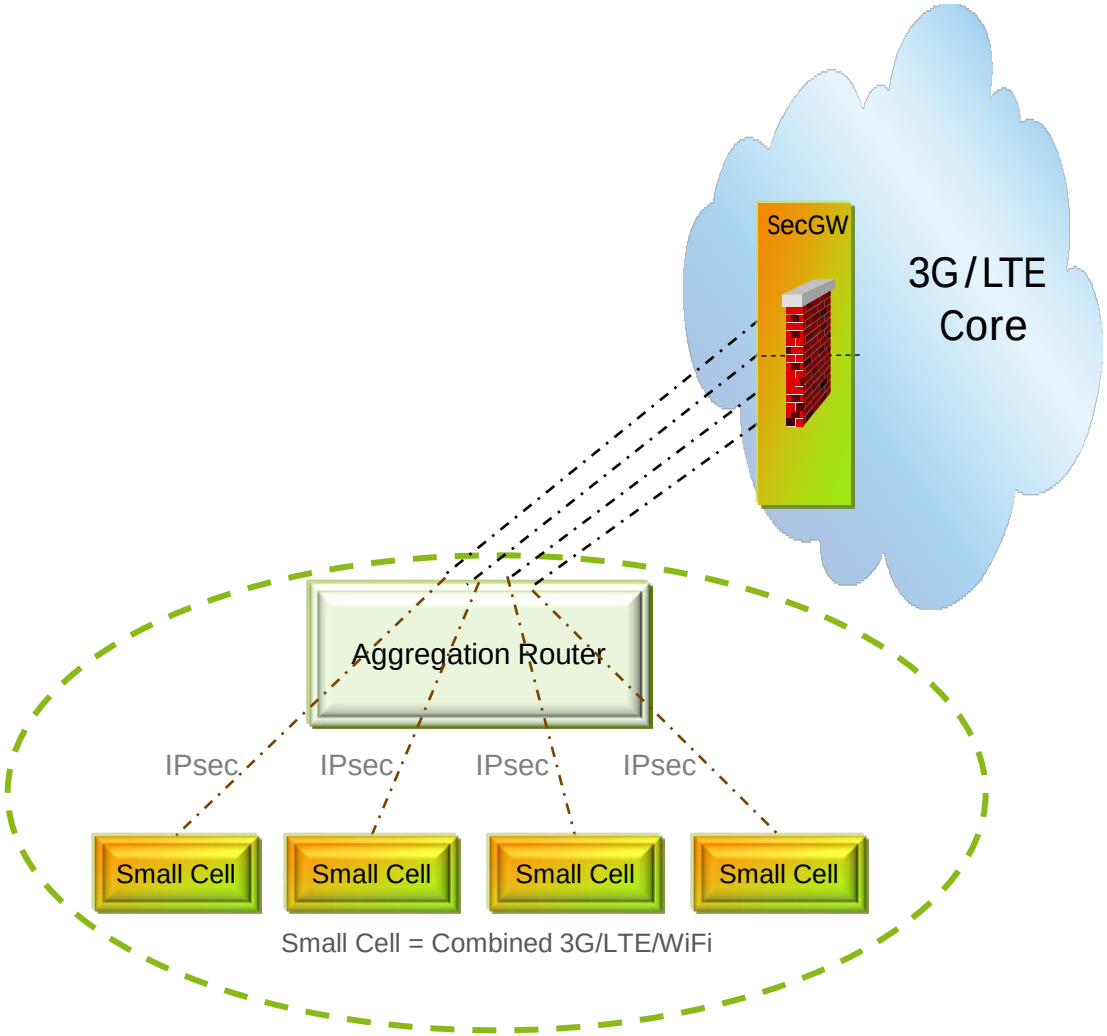
- Traffic and OAM through a single IPsec tunnel;
- 1 VLAN for traffic (S1/X2) and OAM;
- Same security gateway termination point.



OAM IPsec Tunnel, UP+CP IPsec Tunnel

- Traffic and OAM on separate IPsec tunnels
- 1 VLAN for traffic (S1/X2) and 1 VLAN for OAM;
- May use same or different security gateway termination points.

IPSEC NETWORKING
CASE 1 – E2E INDIVIDUAL TUNNELS



Aggregation Router: Simple Aggregation

Pros:

- **Simplicity**
- **Minimum Management**
- **Minimum Configuration/Provisioning**
- **End-to-End Security**

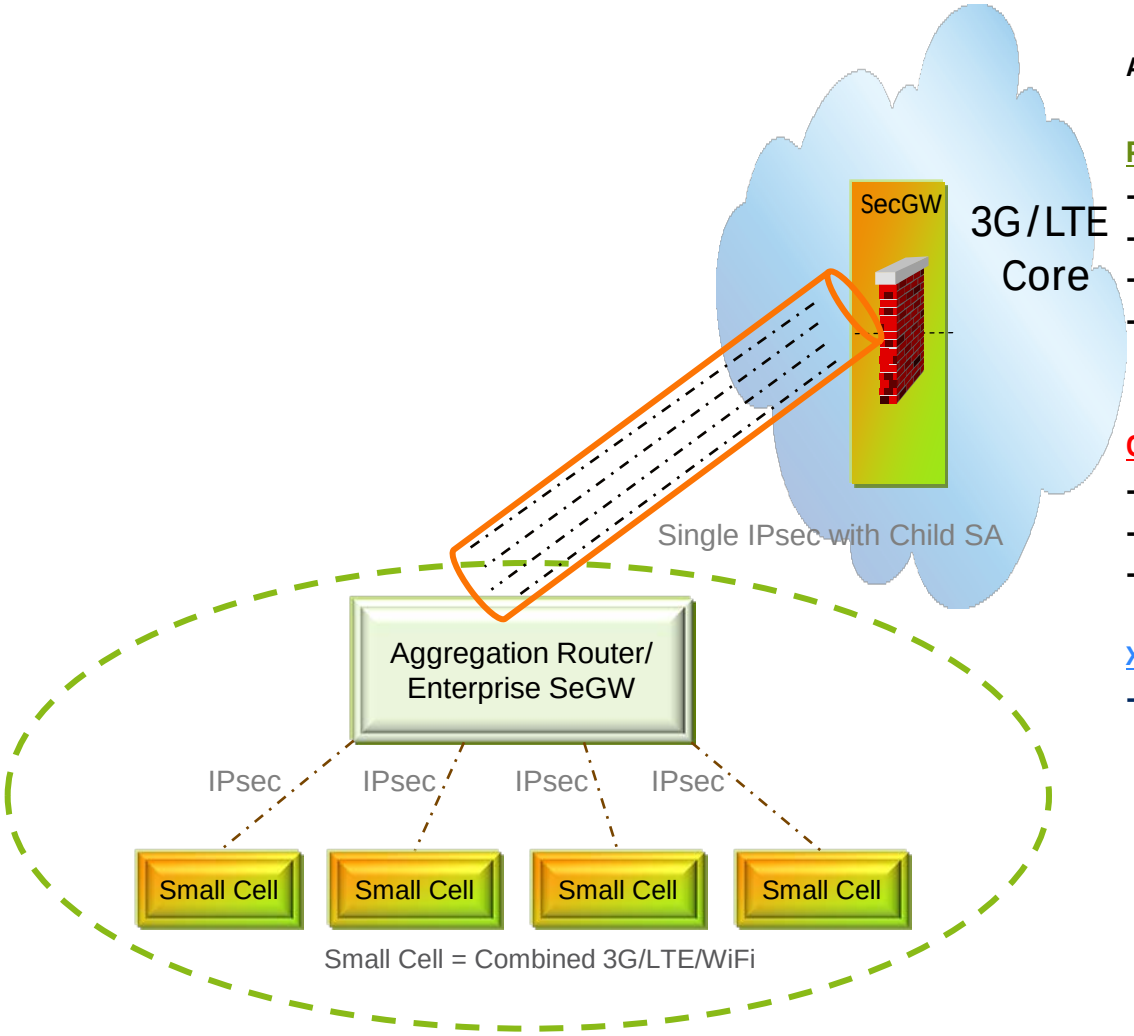
Cons:

- **High load on IP SeGW**
- **Maintenance of Certificates**
- **Local breakout within the Small Cell**
- **Local breakout security??**

X2:

- **X2 outside IPsec – Security of X2?**
- **X2 inside IPSec - X2 performance impact (latency)**

IPSEC NETWORKING
CASE 2 – LOCAL SECURITY GATEWAY



Aggregation Router: Enterprise SeGW and IPsec Aggregation

Pros:

- **Single IPsec and Single entity to the core**
- **End-to-end Security via segmented IPsec**
- **Local Breakout through via Enterprise GW**
- **Local intelligent functions**

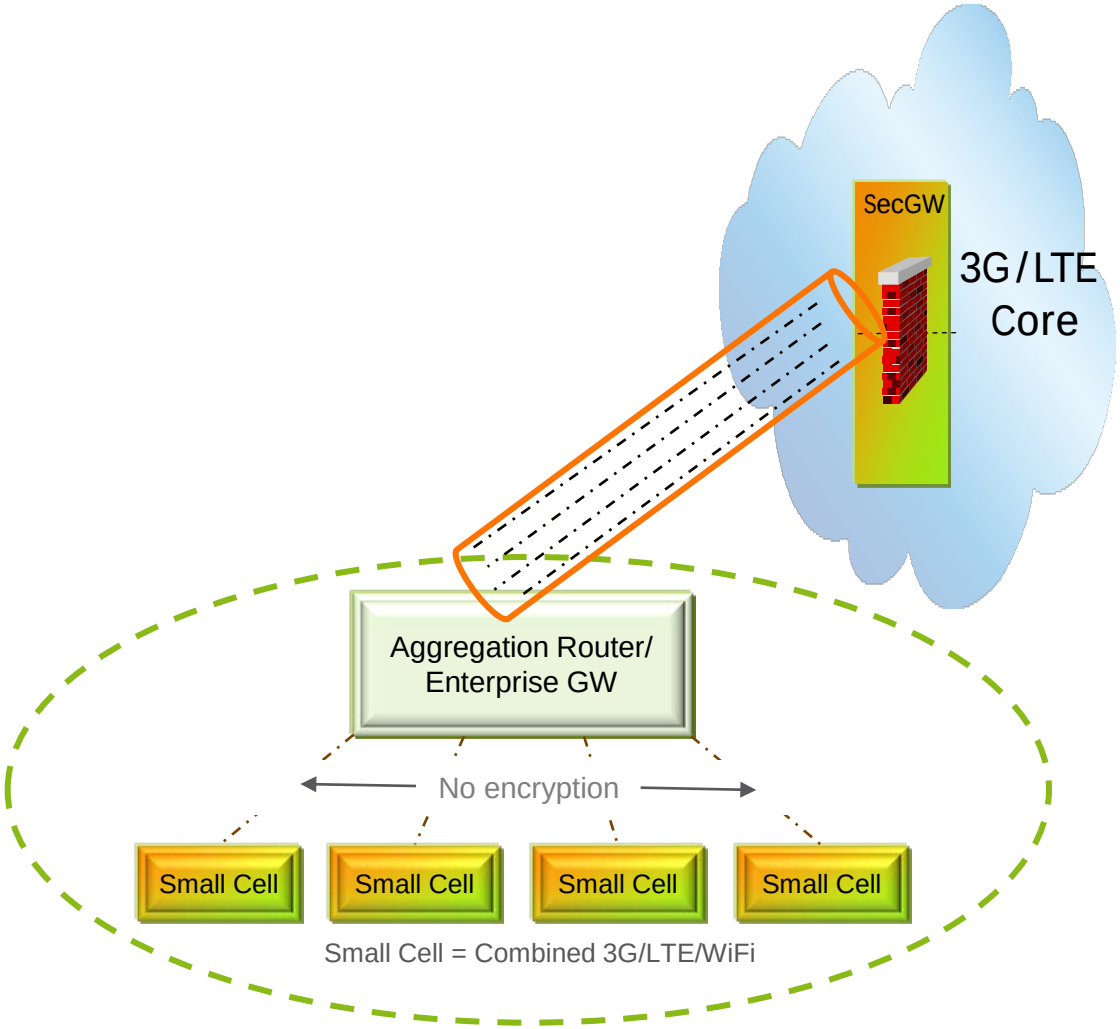
Cons:

- **Cost and performance of Ent SeGW**
- **Cost of Core SeGW feature development and new IP design**
- **Remote SeGW management**

X2:

- **Can be routed inter-Enterprise by the local SeGW**

IPSEC NETWORKING
CASE 3 – ONLY UPLINK TUNNEL



Aggregation Router: Enterprise GW w/o Enterprise IPsec

Pros:

- **Simplicity on Enterprise GW**
- **Inter-Enterprise X2 routing**
- **Local Breakout through via Enterprise GW or Small Cell**
- **Local intelligent functions**

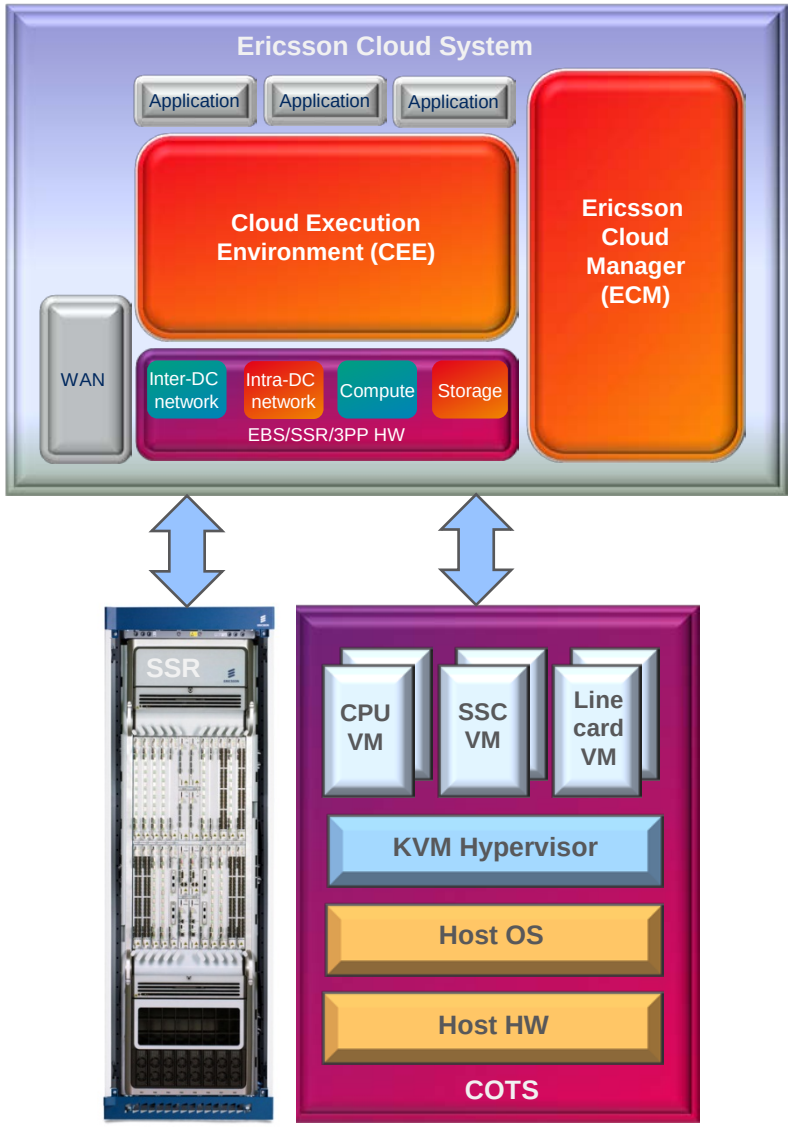
Cons:

- **Outdoor / Indoor Application Security**
- **Dependency on Enterprise LAN security**
- **No end-to-end security**

X2:

- **Can be routed inter-Enterprise by the local GW**

SECURITY GW VIRTUALIZATION
VIRTUAL IP SERVICES PLATFORM



CONCLUSIONS

- Introduction of heterogeneous networks creates an untrusted network environment for service providers.
- There are multiple implementation options for securing the network environment each with its pros and cons.
- Virtualization of IP Services provides the opportunity to deploy functions such as the Security Gateway in a flexible and cost efficient manner.

ERICSSON