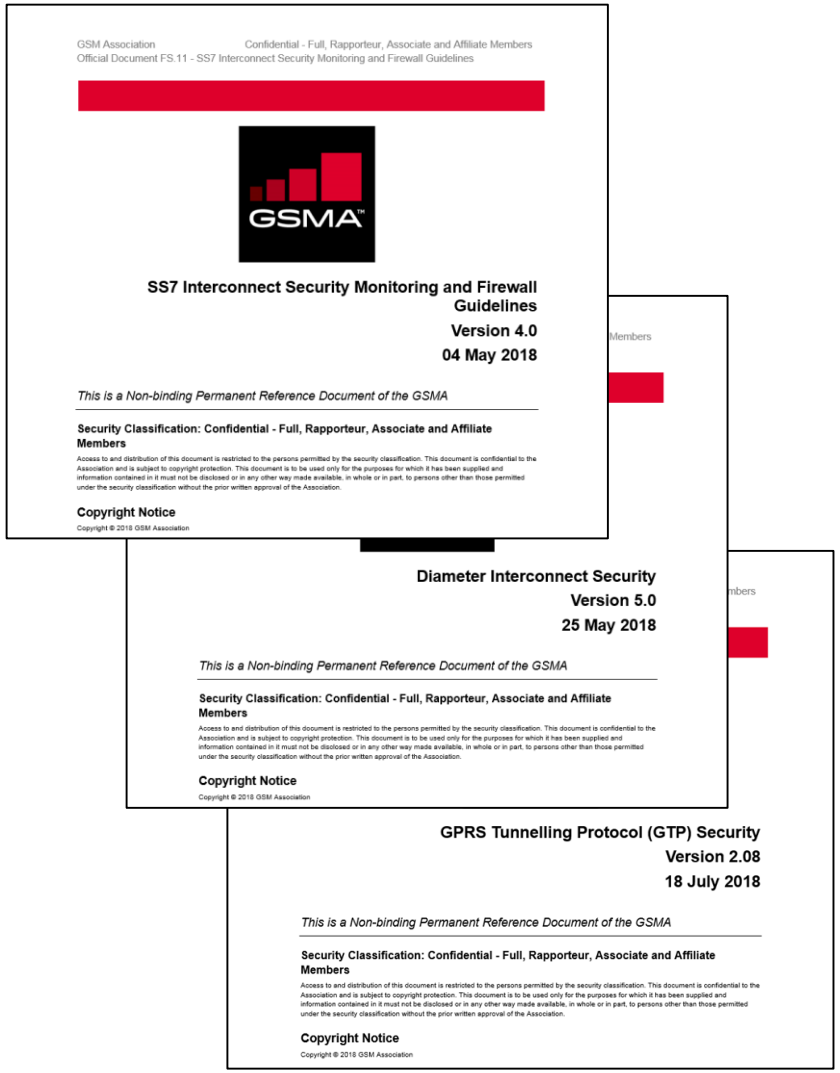
Vulnerabilities, Potential Risks and Recommendations

Vulnerablities and Risks

- Your customers' locations can be accurately pin-pointed
- Personal phone calls and messages can be monitored
- Network & subscriber data can be modified
- User privacy and revenues from key services are under threat
- Data billing avoidance by subscriber impersonation
- Unauthorized access to APN and credentials abuse (e.g. corporate VPN)

Recommendations

- Firewall SMS: Home Routing, Greyroute, A2P control, Simbox mitigation
- Firewall SS7 interconnect: Categories 1/2/3 (GSMA FS.11)
- Firewall Diameter interconnect: Categories 1/2/3/LowLayer (GSMA FS.19)
- Firewall GTP-C interconnect : Categories 1/2/3/LowLayer (GSMA FS.20)
- Protocol Correlation (GSMA FS.21)
- 5G Roaming

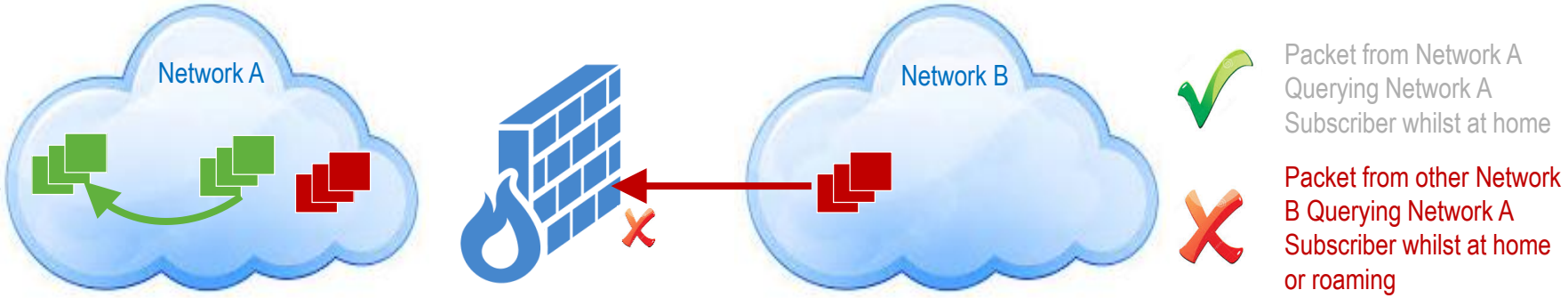


SS7 Threat Categories– Allowed/Disallowed Packets

Category 1

Prohibited Interconnect Packets

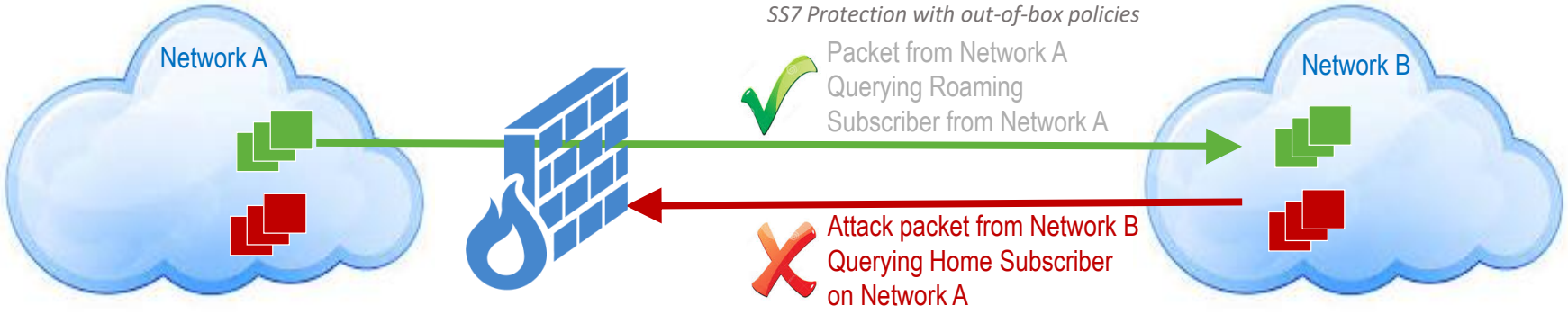
Messages that should only normally be received from within the same network or networks with bilateral agreements



Category 2

Unauthorised Packets

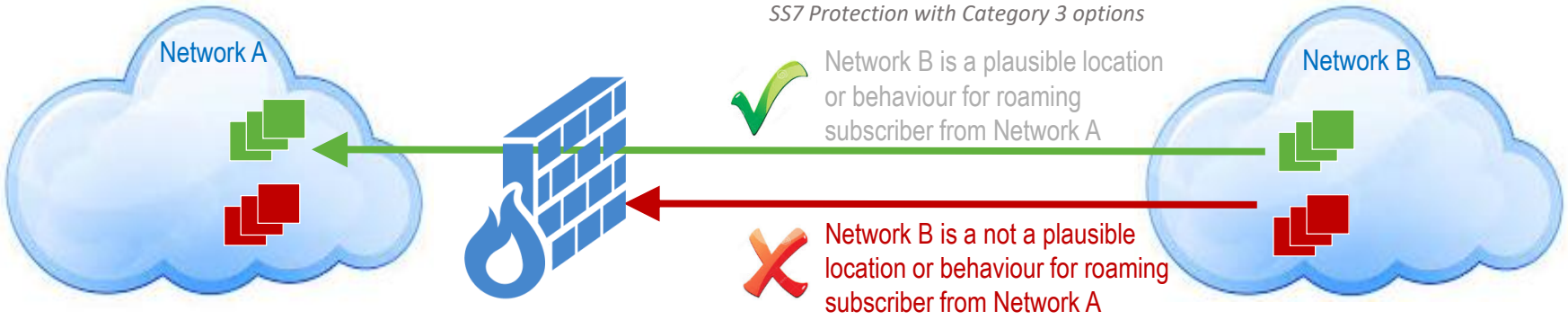
Messages that should only be sent about a visiting subscriber from that subscriber's home network



Category 3

Suspicious Location Packets

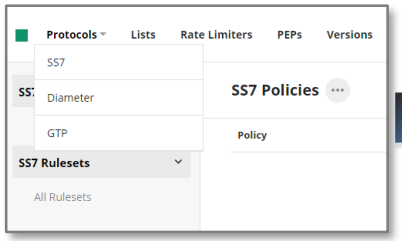
Messages that should only be sent about a visiting subscriber from that subscriber's current visited network

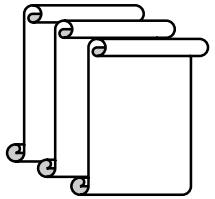


Backup reference

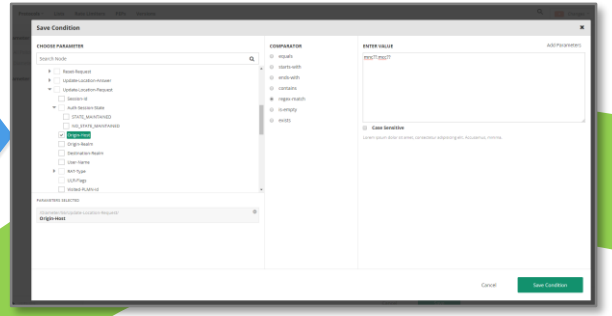
Securing the Network

Baseline
Out-of-the-box
GSMA rules





Adapt
Address unique threats



Collaborate
Global Intelligence (ML/AI)

Insight
Observe and Learn

Classic Category 3.2: Trajectory plausibility