:: Positive Technologies

Cheaper by the dozen:

Simultaneous attacks on SS7 and Diameter

Sergey Puzankov

About the team

Sergey Mashukov
sergey.mashukov@positive-tech.com

The main point of interest is security of the Diameter protocol. Sergey performs Diameter security audits for international MNOs and conducts research on the protocol weaknesses. Sergey is also the general developer of the Telecom Vulnerability Scanner tool and member of the Telecom Attack Discovery development team.

Alexandr Onegov
alexandr.onegov@positive-tech.com

Alexander researched both SS7 and Diameter signaling protocols from security point of view and developed algorithms for an intrusion detection system. He also performs security assessments for mobile operators and conducts research on the network vulnerabilities.

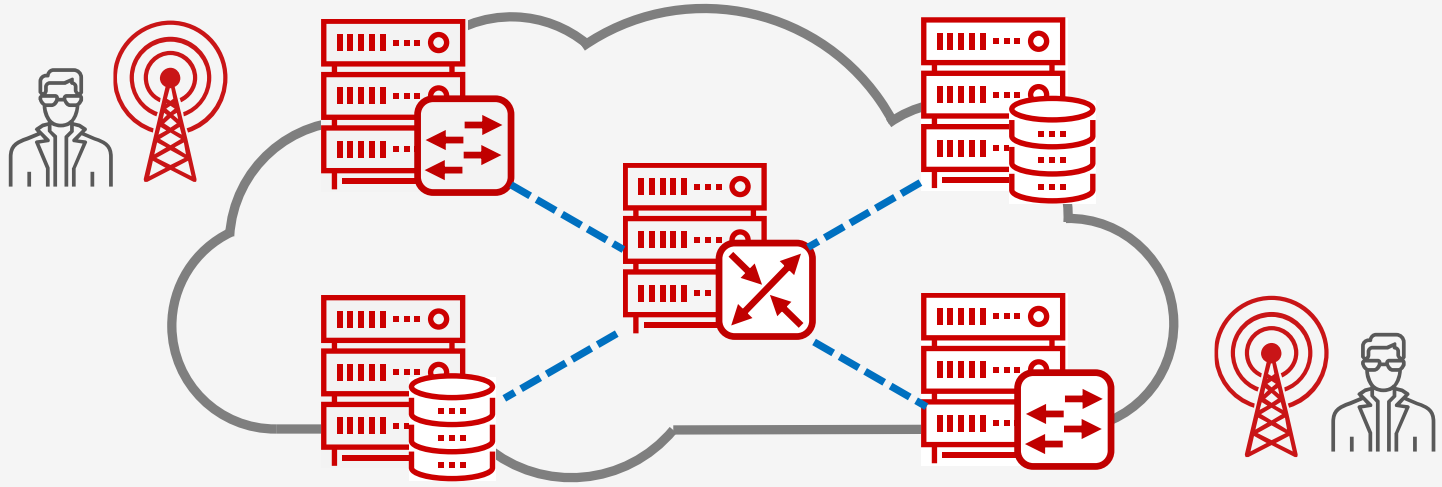
Sergey Puzankov
sergey.puzankov@positive-tech.com

Sergey conducted research of by-design vulnerabilities in SS7 networks, discovered a number of critical vulnerabilities in mobile network equipment, and showed how an intruder is able to bypass mobile operators' protection means.

Signaling basics

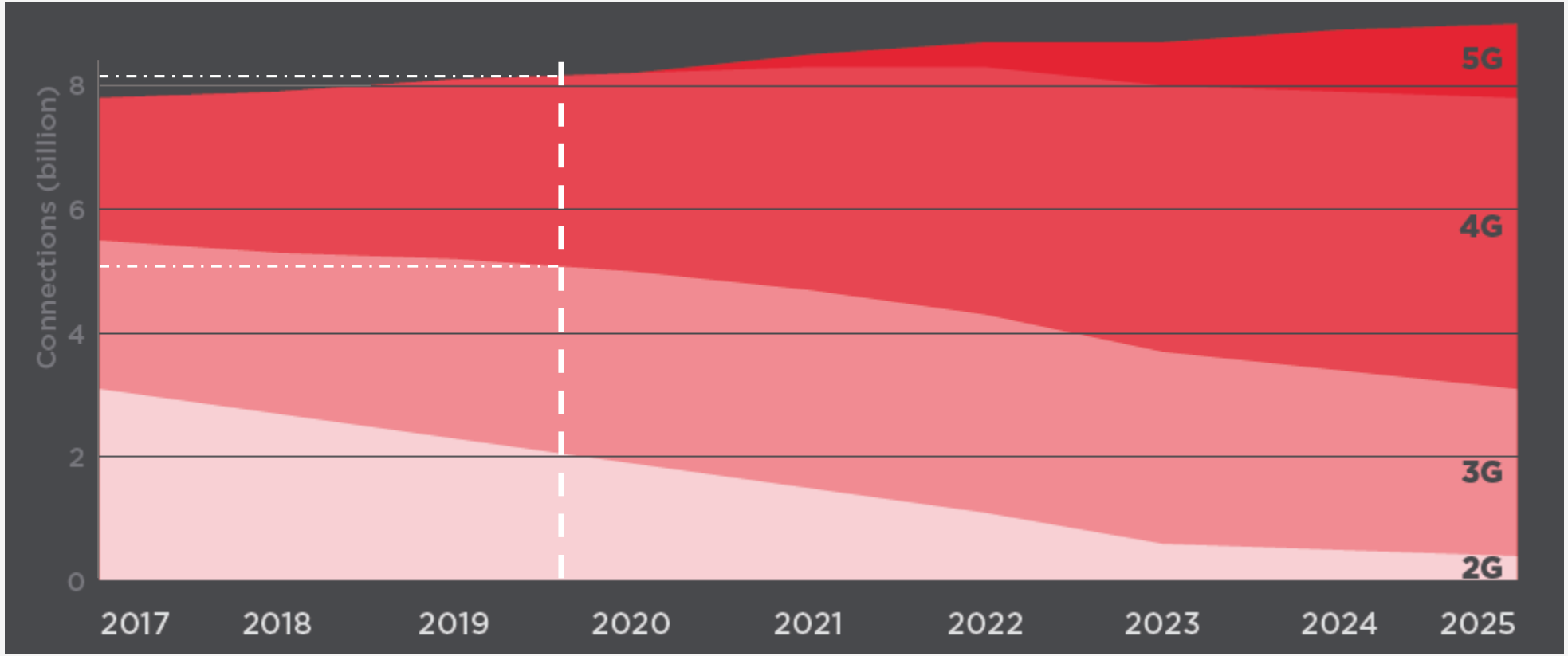
SS7 (Signaling System No. 7) is a **set of telephony protocols** used to set up and tear down telephone calls, send and receive SMS messages, provide subscriber mobility, and more.

Diameter is an authentication, authorization, and accounting protocol for computer networks. **RFC 5516** defines a set of IANA Diameter Command Codes to be used in new vendor-specific Diameter applications defined for the **3GPP Evolved Packet System** (EPS).



The basic unit in signaling is a **message**.

Who are potential targets?



© GSMA Intelligence 2018, Mobile connections by technology
https://www.gsmaintelligence.com/research/2018/02/infographic-mobile-connections-by-technology/656/

Now what can a hacker do?

Intercept **private data, calls, and SMS** messages

Easily

Track **location** of **VIPs** and **public figures**

From anywhere

Perform **massive denial of service** attacks

Take control of your **digital identity**

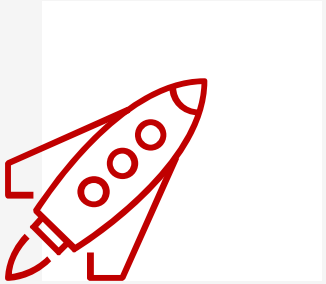
Any mobile operator

Get access to your **email and social media**

No special skills needed

Steal **money**

History of signaling security

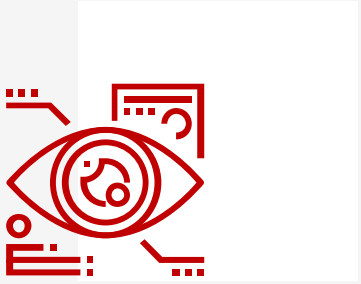


SS7 development

Trusted environment. No security mechanisms in the protocol stack. SIGTRAN (SS7 over IP) introduced. Security is still missing

Scope grows

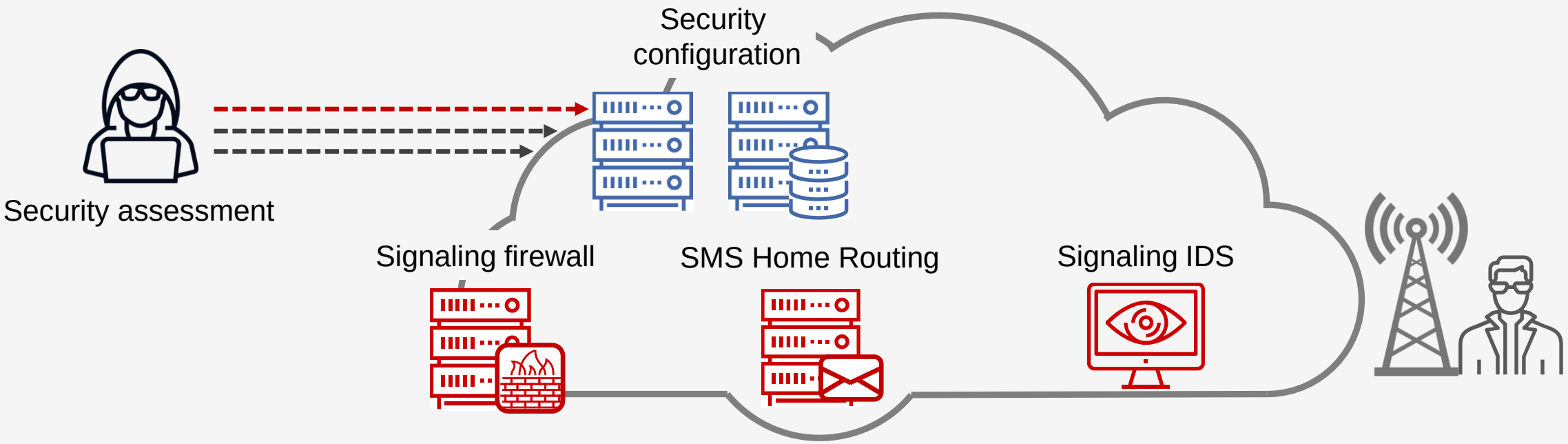
Growing number of SS7 connections, increasing amount of SS7 traffic. No security policies or restrictions



Not trusted anymore

Huge number of MNOs, MVNOs, and VAS providers. SS7 widely used, Diameter added and spreading. Still not enough security

Mobile operators and signaling security

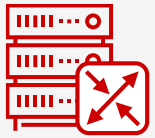


Nodes and identifiers in GSM/UMTS

MSISDN — Mobile Subscriber Integrated Services Digital Number

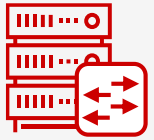
GT — Global Title, address of a core node element

IMSI — International Mobile Subscriber Identity

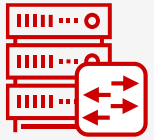


STP — Signaling Transfer Point

HLR — Home Location Register



MSC/VLR — Mobile Switching Center and Visited Location Register



SGSN — Serving GPRS Support Node

SMS-C — SMS Centre

Nodes and identifiers in LTE

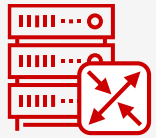
EPC — Evolved Packet Core

Realm — standardized network identity

`epc.mnc070.mcc466.3gppnetwork.org`

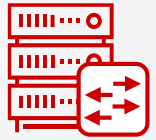
HostID — name of a node within the network

`mme01.epc.mnc070.mcc466.3gppnetwork.org`

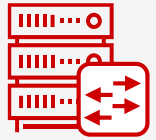


DEA — Diameter Edge Agent

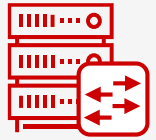
HSS — Home Subscriber Server



MME — Mobile Management Entity

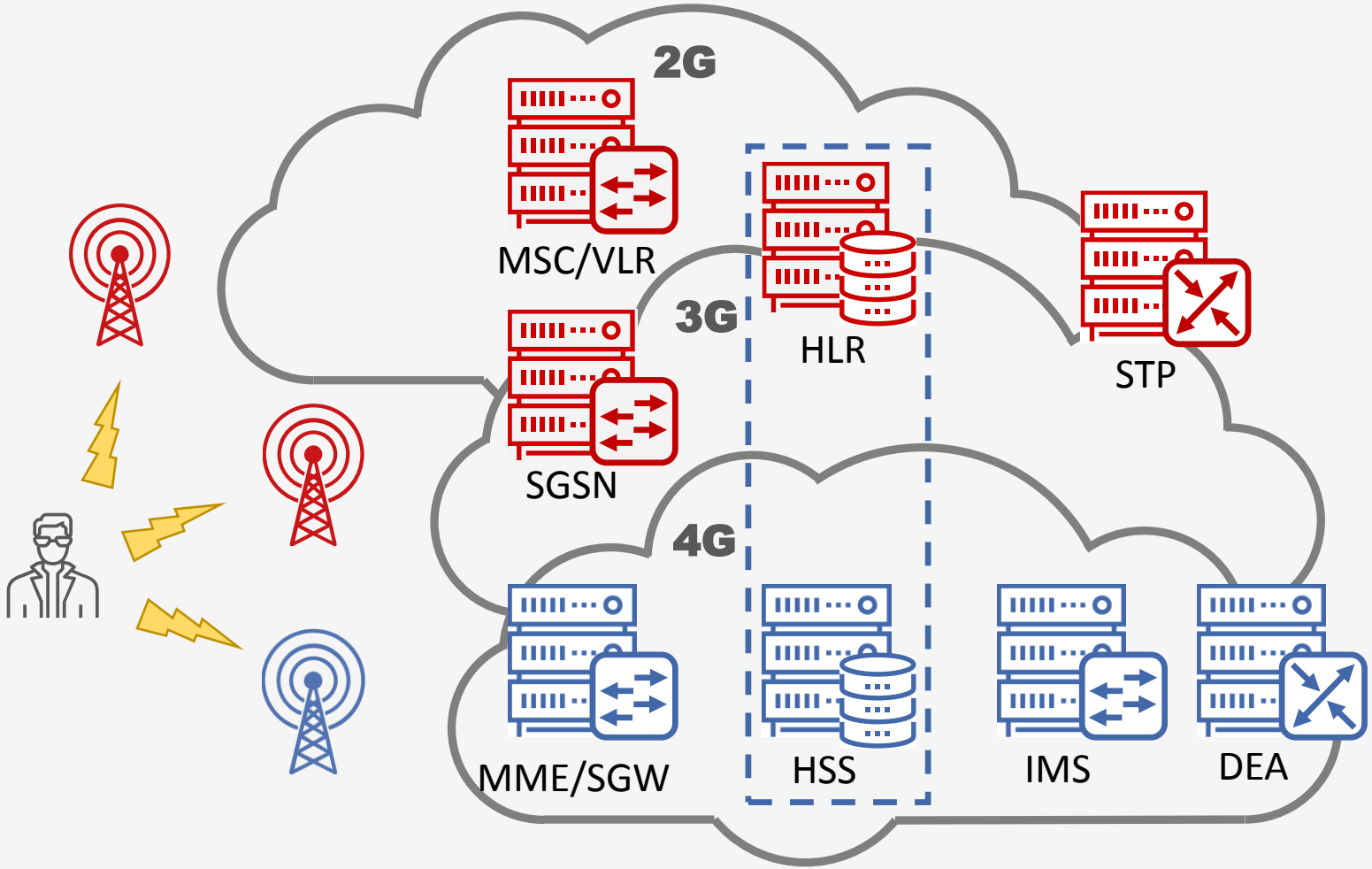


SGW — Serving Gateway



IMS — IP Multimedia System

Mobile networks evolution



SS7 protocol stack

MAP

Mobile Application Part

is payload that contains an **operation code** and appropriate **parameters** such as **IMSI**, profile information, and location data.

TCAP

Transaction Capabilities Application Part

is responsible for **transactions** and **dialogues** processing.

SCCP

Signaling Connection Control Part

is responsible for the **routing** of a signaling message by **Global Titles**.

Diameter protocol stack

Diameter

Diameter
is payload that contains a **command code**, **application ID**, and appropriate **parameters** within Attribute-Value Pairs (**AVP**) blocks.

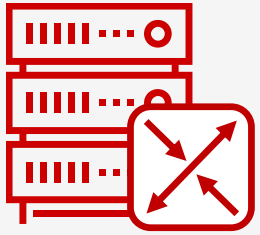
SCTP

Stream Control Transmission Protocol
is a **transport** protocol that provides some of the features of both UDP and TCP.

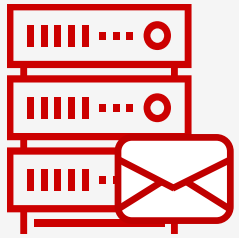
IP

Internet Protocol
is responsible for the node internetworking at the internet layer.

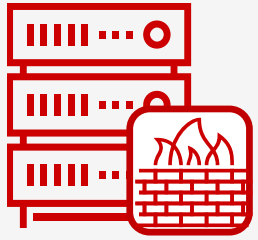
Signaling security means



STP/DEA
makes simple screening of signaling messages.

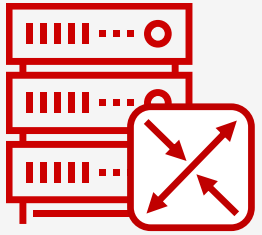


SMS Home Routing
is intended to prevent SMS fraud and hide IMSI identities.



SS7/Diameter firewall
is the most sophisticated signaling security tool that protects the network against a wide range of threats such as IMSI disclosure, location tracking, and traffic interception.

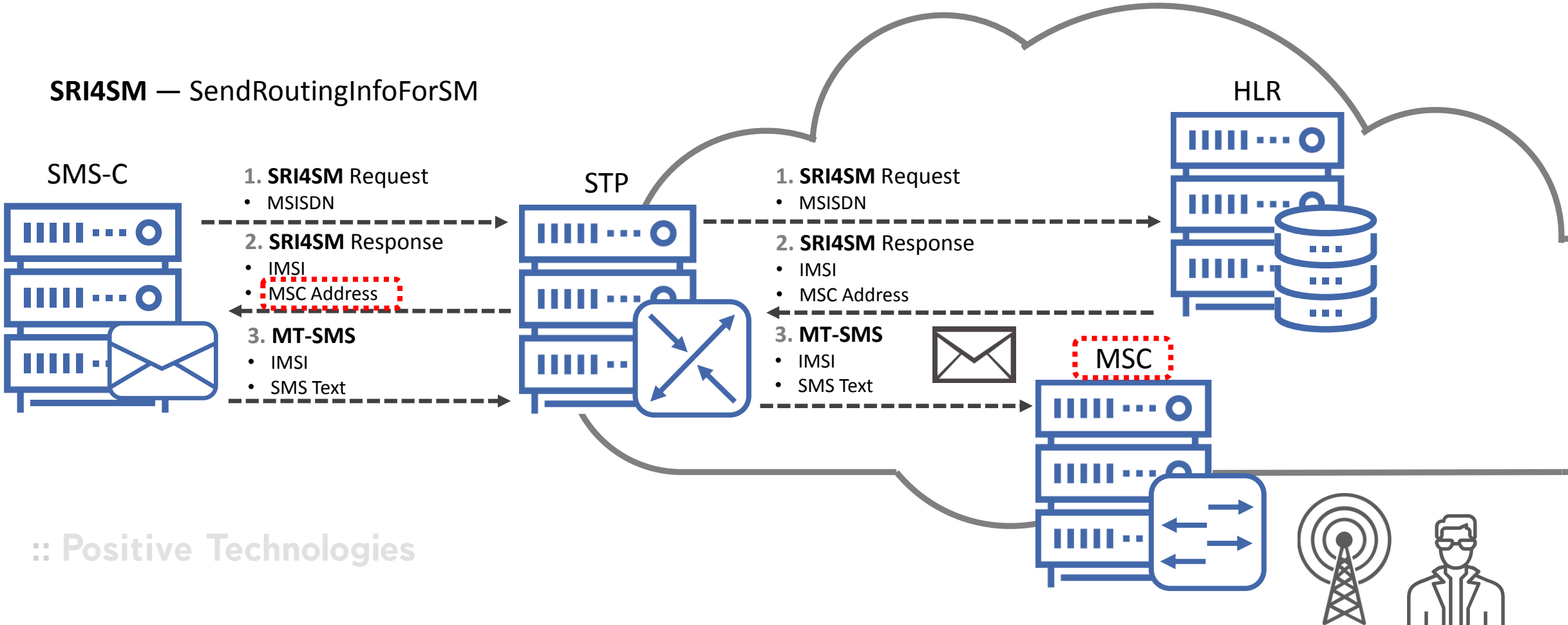
STP and DEA



- **Signaling Transfer Point** and **Diameter Edge Agent** are routers that relays signaling messages between signaling points.
- Usually the **STP** and **DEA** are **border points** in a signaling network.
- It is possible to use the **STP** and **DEA** for the **screening of the ineligible** signaling traffic.
- **Screening rules** of the most STPs and DEAs are **simple**, for instance, blocking a signaling message by a source address or redirecting a signaling message by an operation code.

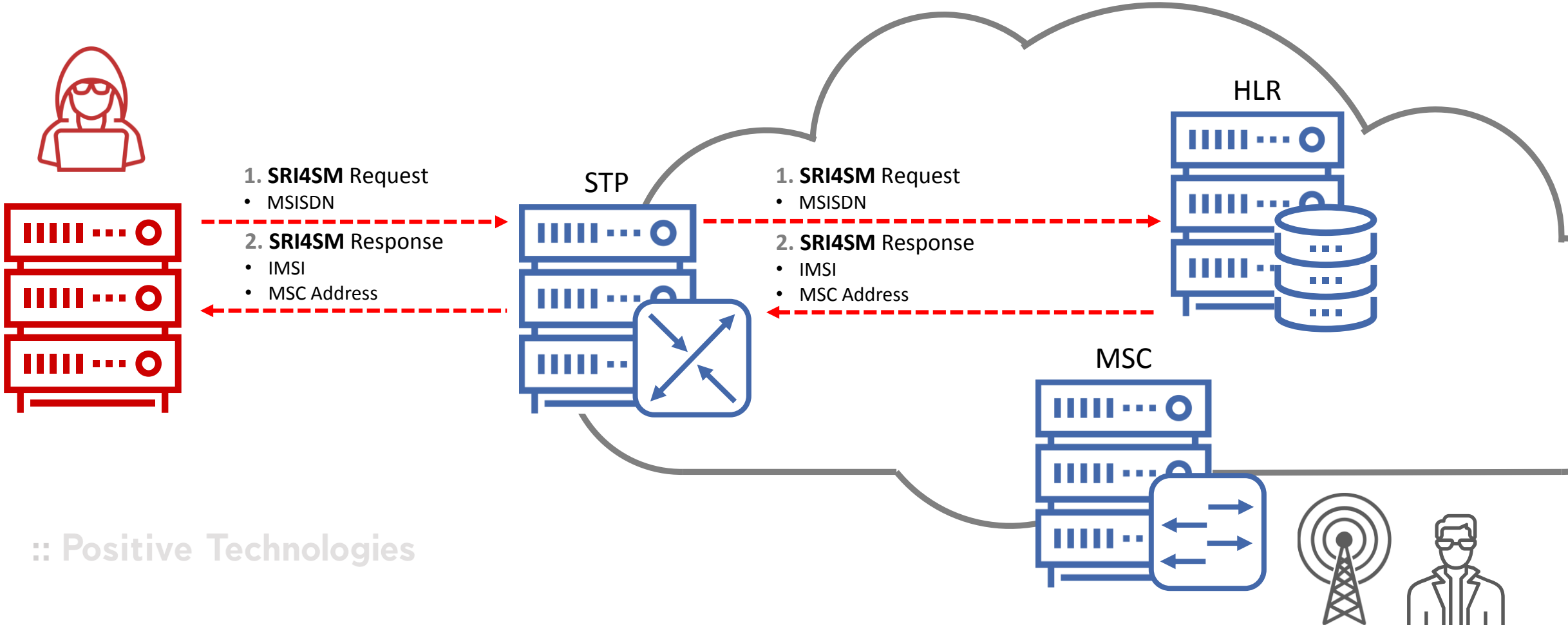
SMS Home Routing

SMS delivery process

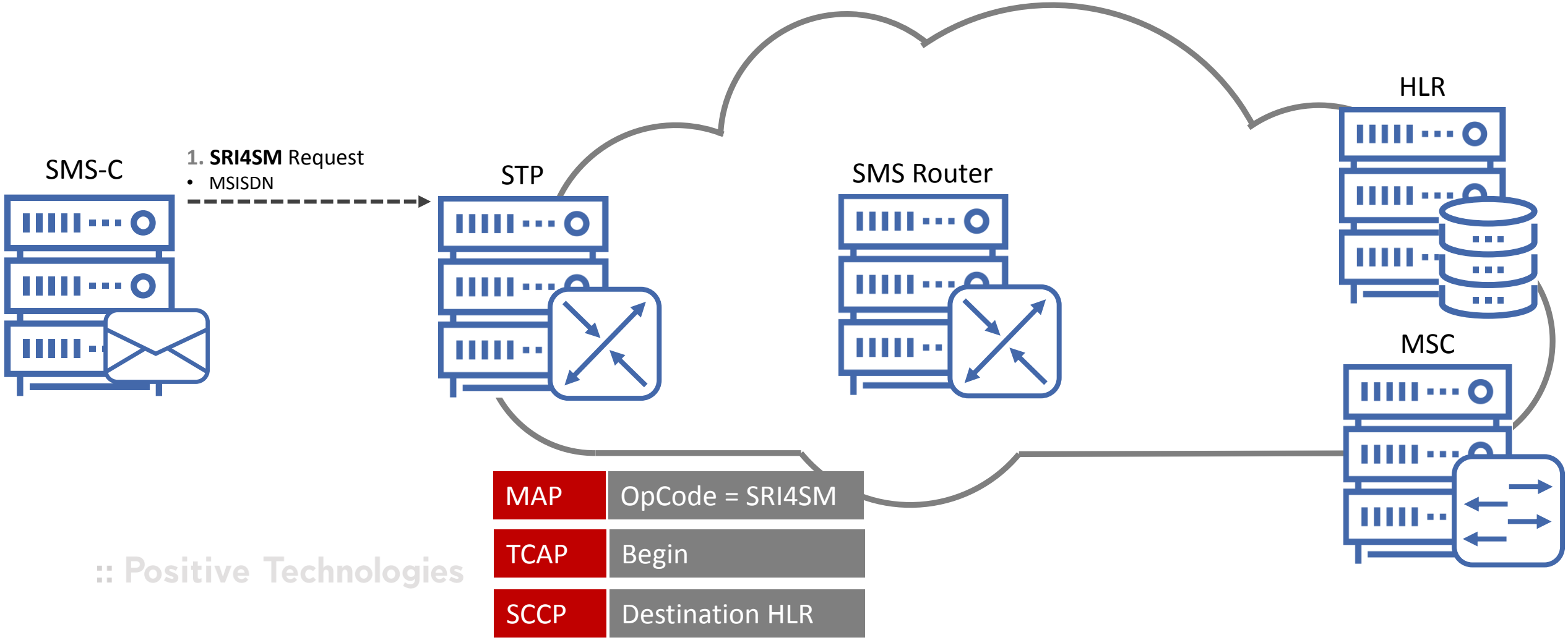


SMS Home Routing

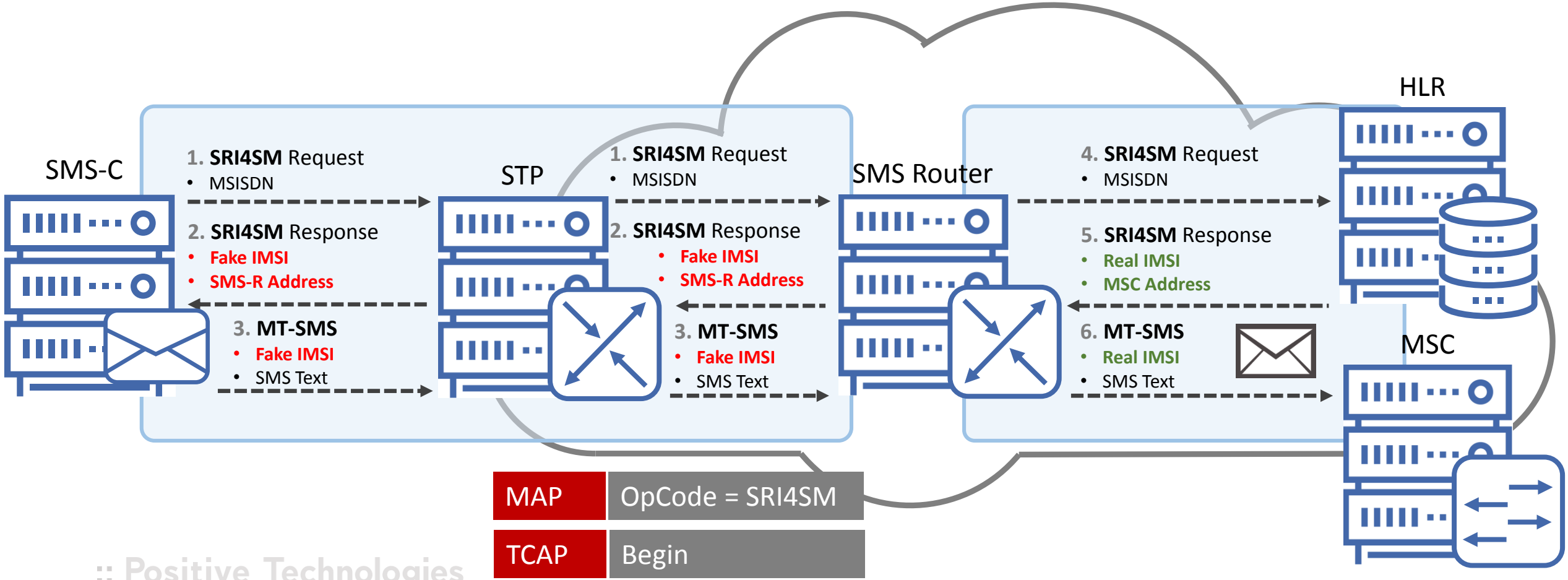
SRI4SM abuse by a malefactor



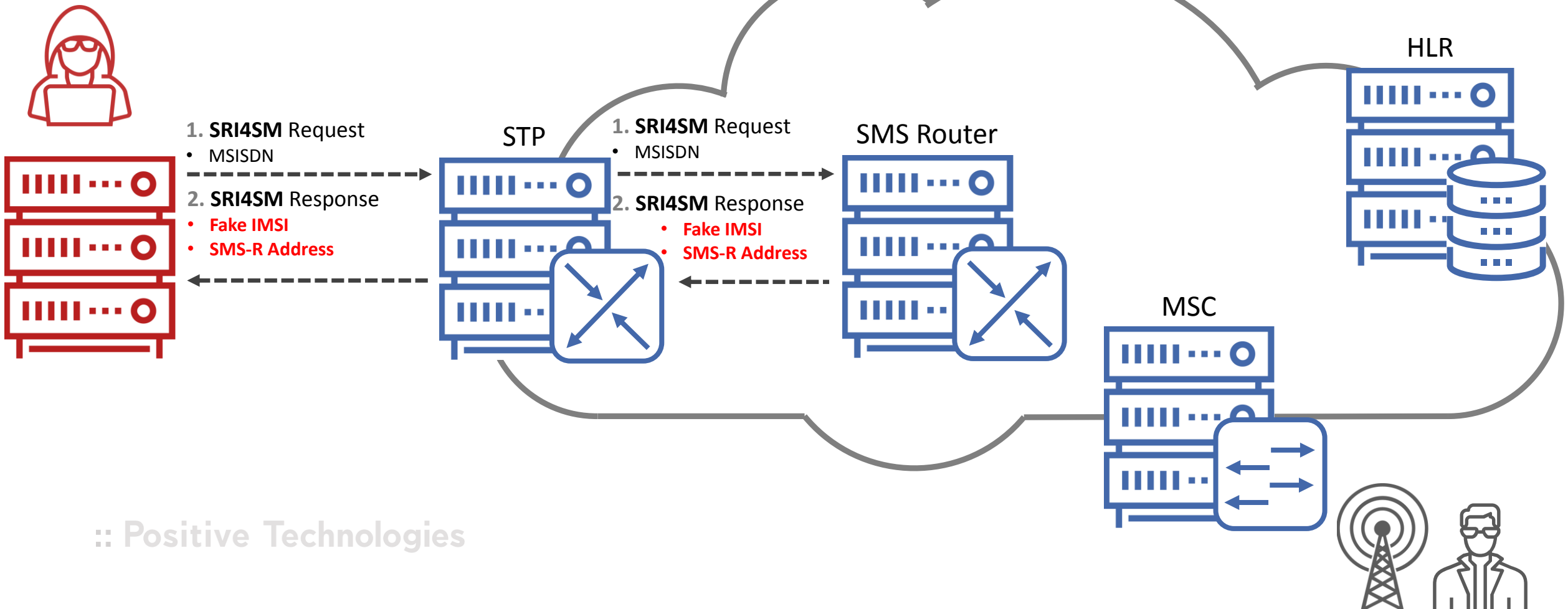
SMS Home Routing



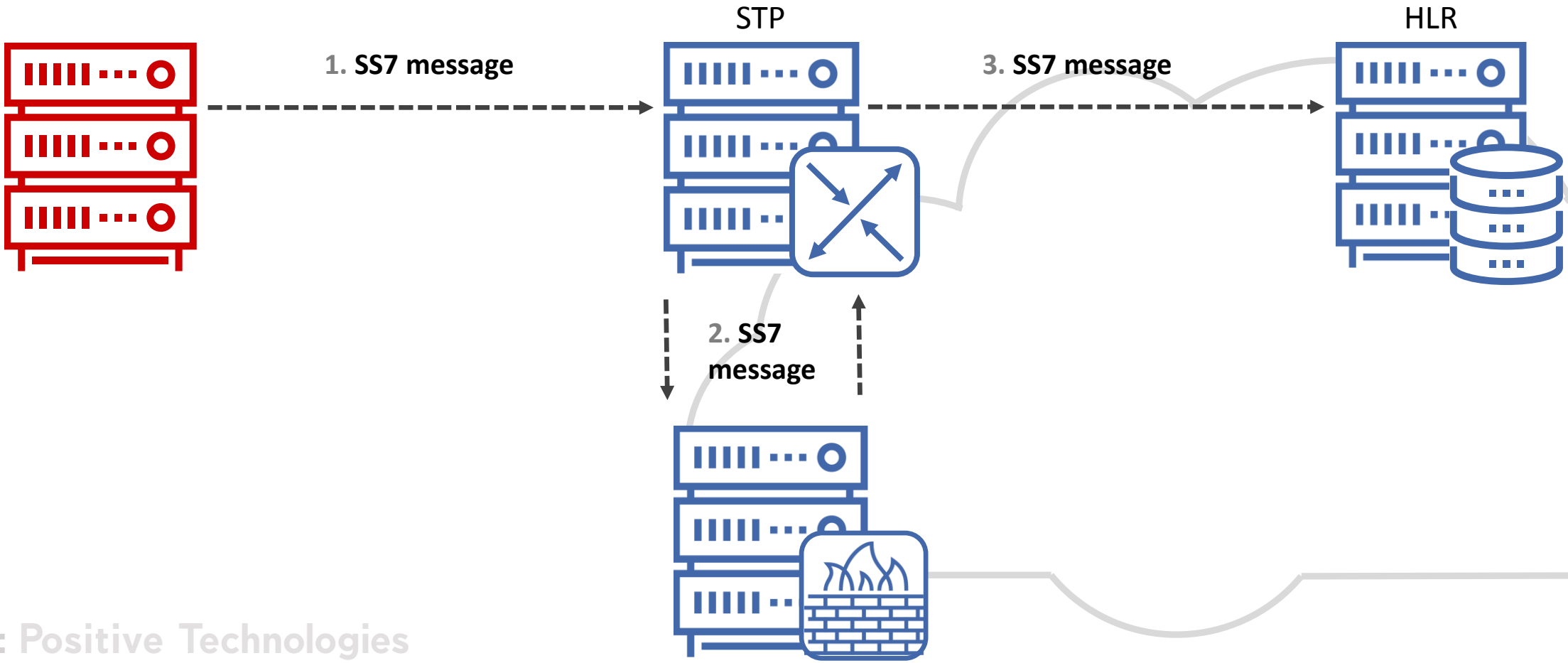
SMS Home Routing



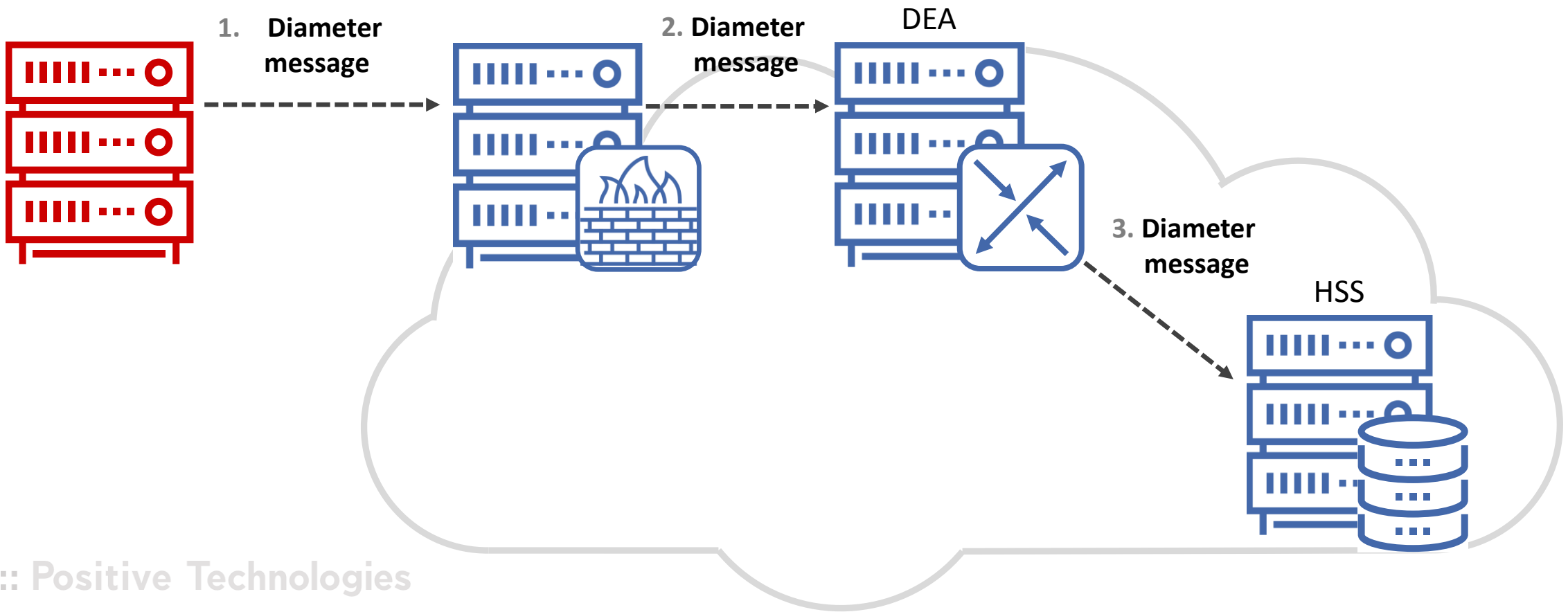
SMS Home Routing against malefactors



SS7 firewall: typical deployment scheme



Diameter firewall: typical deployment scheme

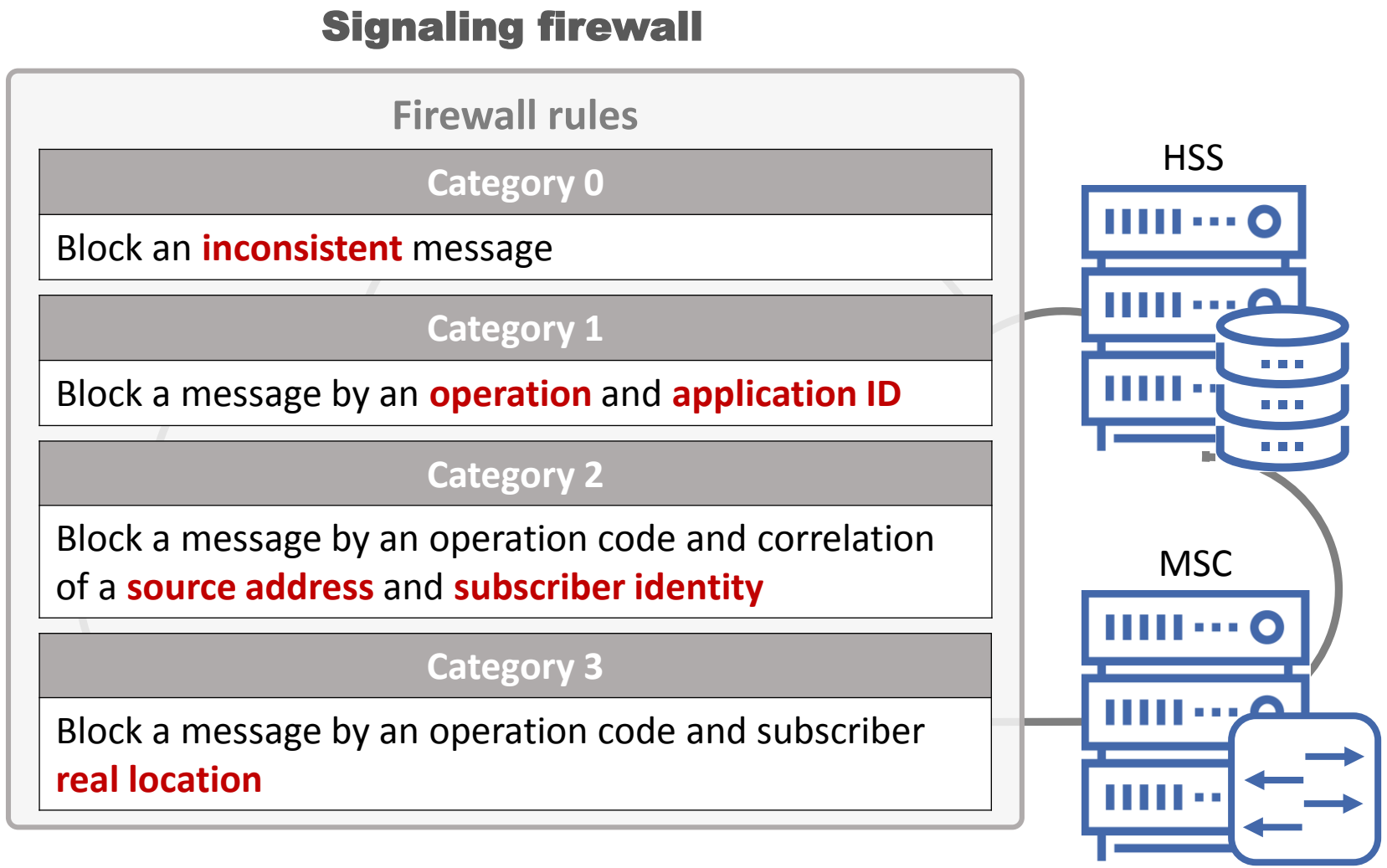


Signaling firewall: blocking rules

Signaling Message

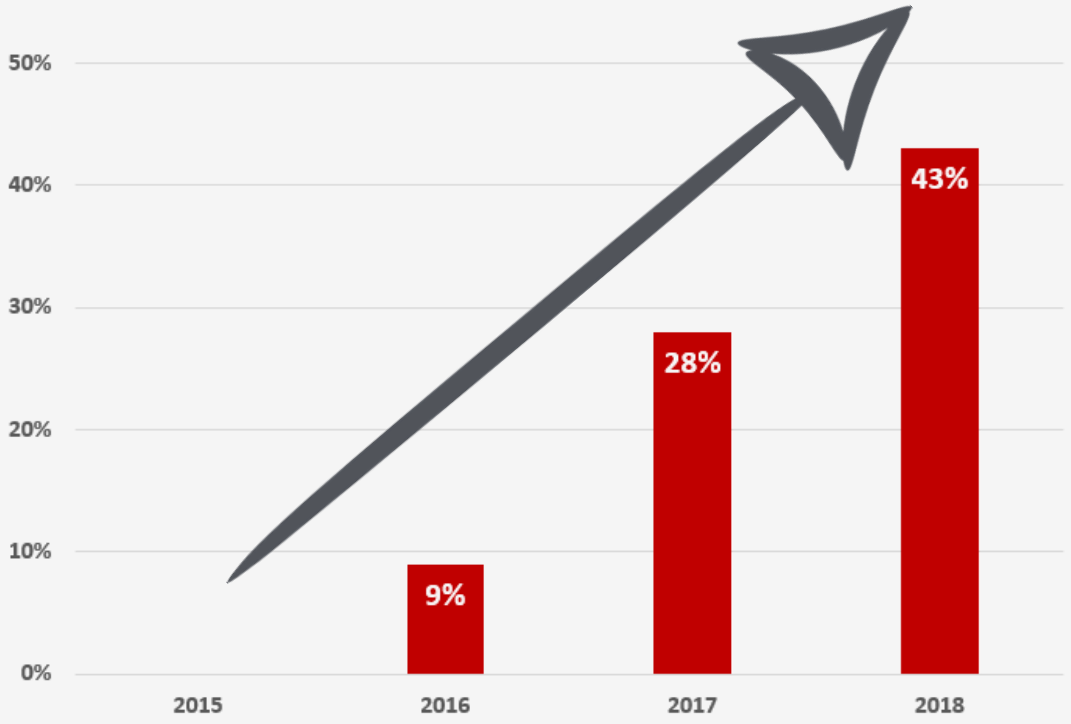
MAP	OpCode, IMSI…
TCAP	Application Context
SCCP	Source / Dest GT

Diameter	Cmd Code, AppID…
SCTP	Ports
IP	Source / Dest IP

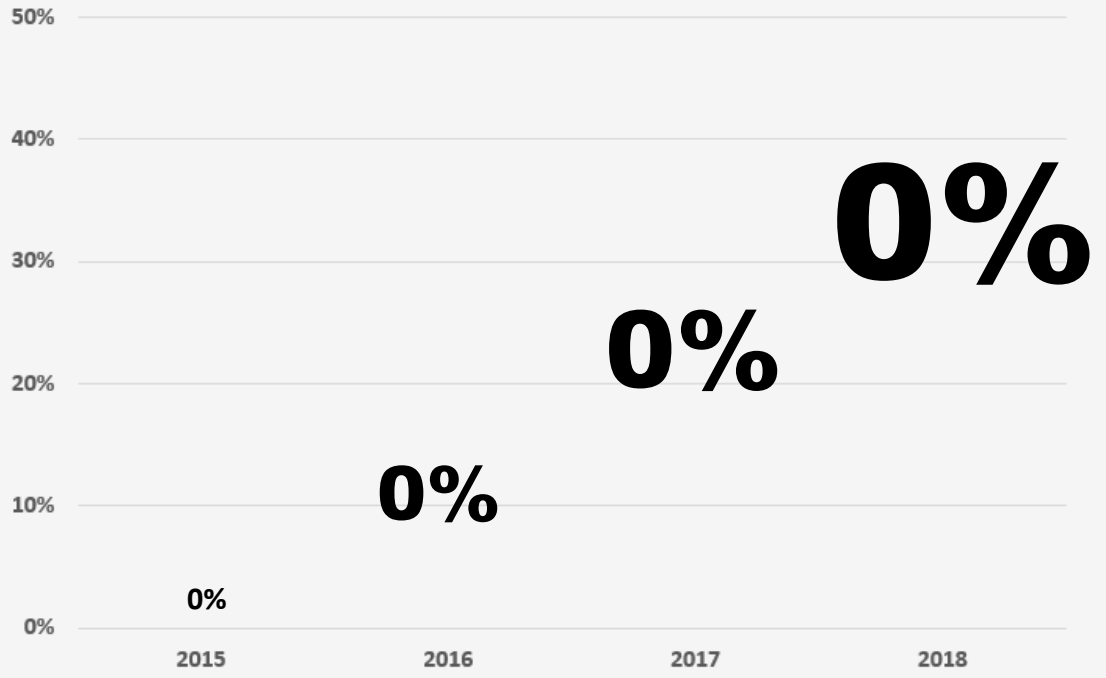


SS7 and Diameter firewall penetration

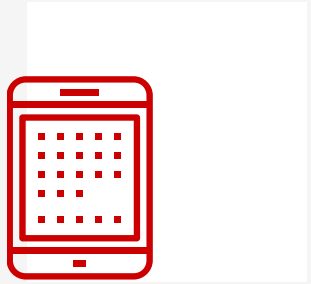
SS7 firewall penetration growth



Diameter firewall penetration



Attack cases on signaling networks

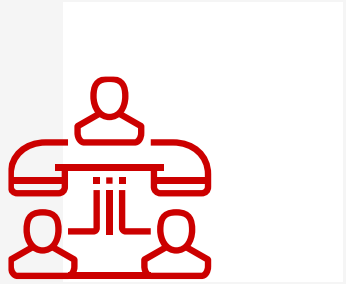


IMSI disclosure

Attack on SS7 network with SMS Home Routing bypassing

Location tracking

Attack on Diameter network



Voice call interception (MITM)

Attack via VoLTE suppression and SS7 firewall bypassing

IMSI disclosure

Attack on SS7 network with SMS Home Routing bypassing

IMSI

An **IMSI** identifier, by itself, is not valuable to an intruder.

But intruders can carry out many malicious actions against subscribers when they know the **IMSI**, such as:

- Location tracking
- Service disturbance
- SMS interception
- Voice call eavesdropping

The **IMSI** is considered personal data as per GDPR.

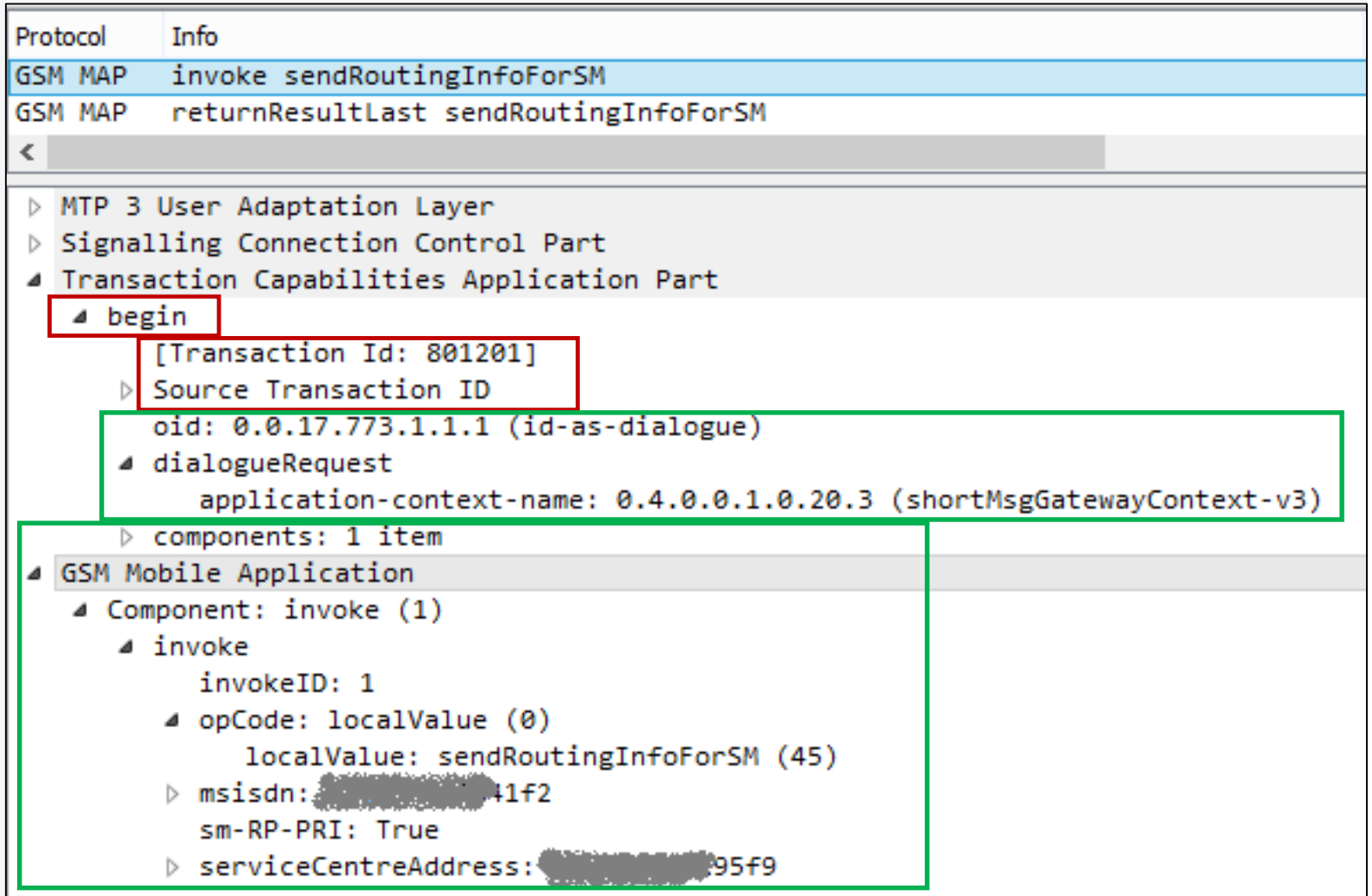
TCAP protocol

TCAP Message Type — mandatory

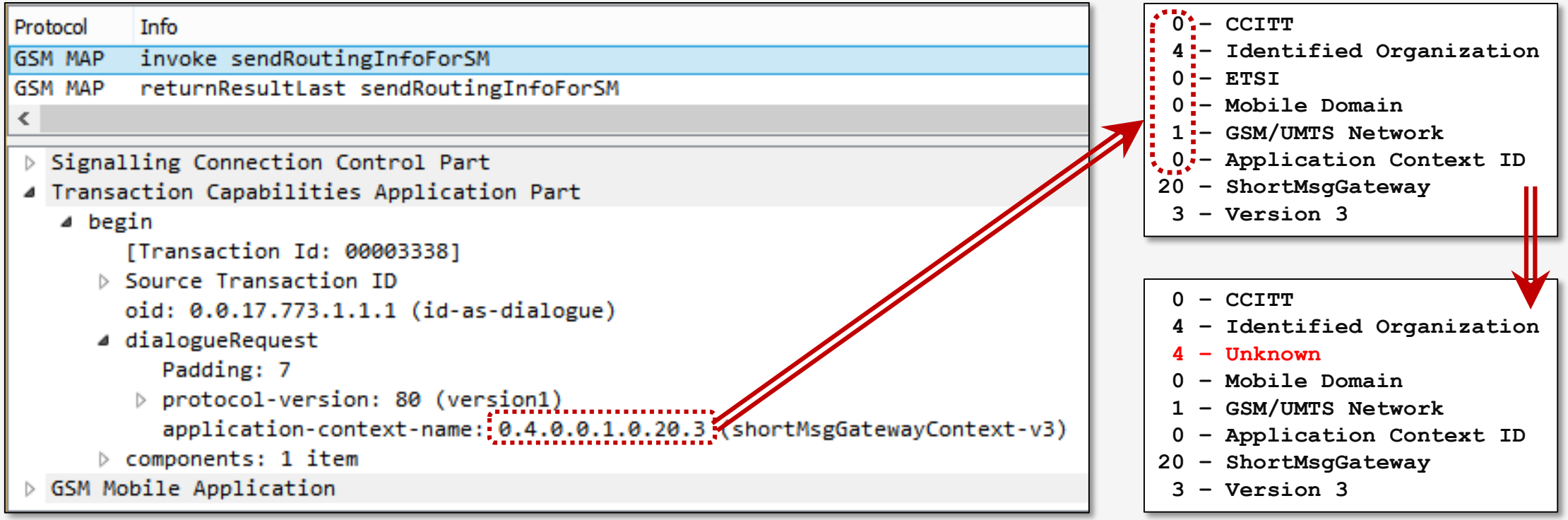
Transaction IDs — mandatory

Dialogue Portion — optional

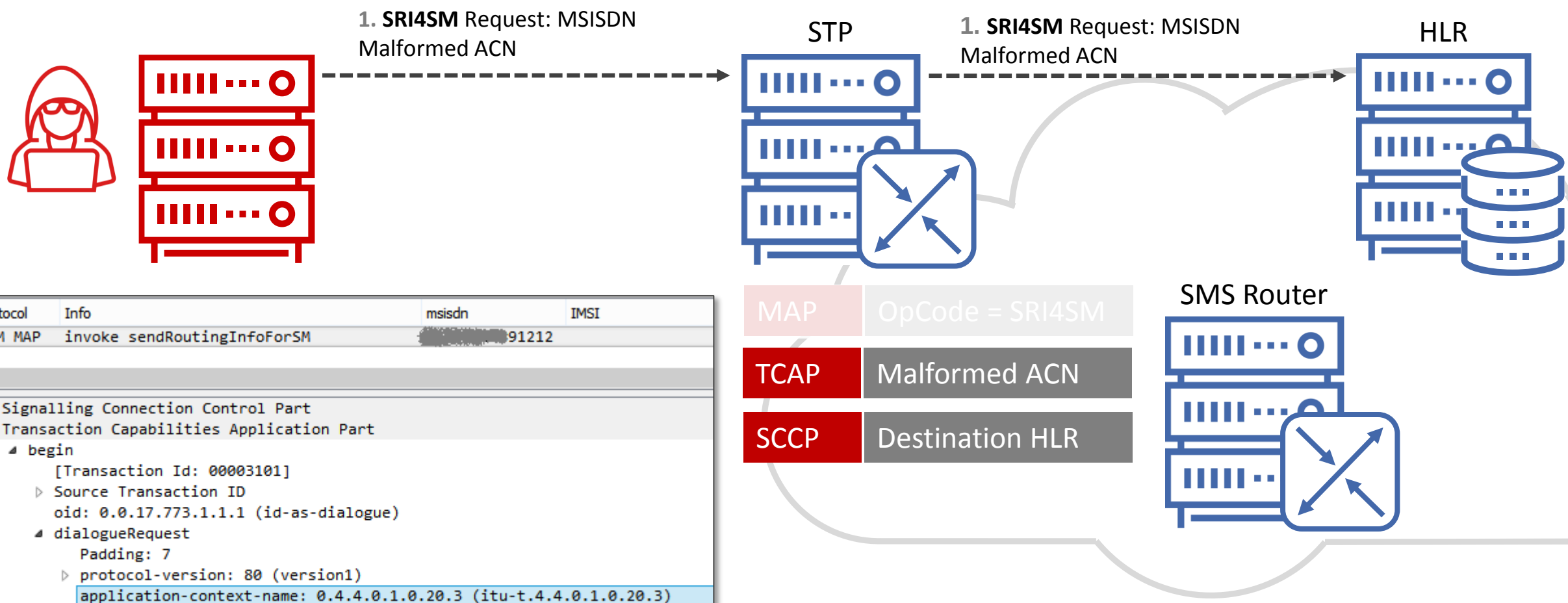
Component Portion — optional



Changing ACN

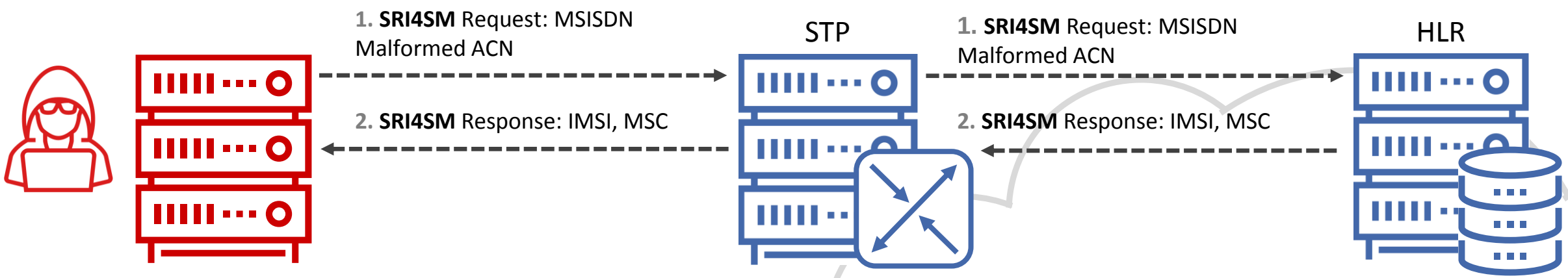


::IMSI disclosure via malformed ACN



Malformed ACN

IMSI disclosure via malformed ACN



Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfoForSM		[redacted]00111

```
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: returnResultLast (2)
    returnResultLast
      invokeID: 1
      resultretres
        opCode: localValue (0)
        IMSI:[redacted]00111
        locationInfoWithLMSI
```

SMS Router bypassed

Location tracking

Attack on
Diameter network

Cell Global Identity

Mobile Country Code (MCC)
- **466** – Taiwan

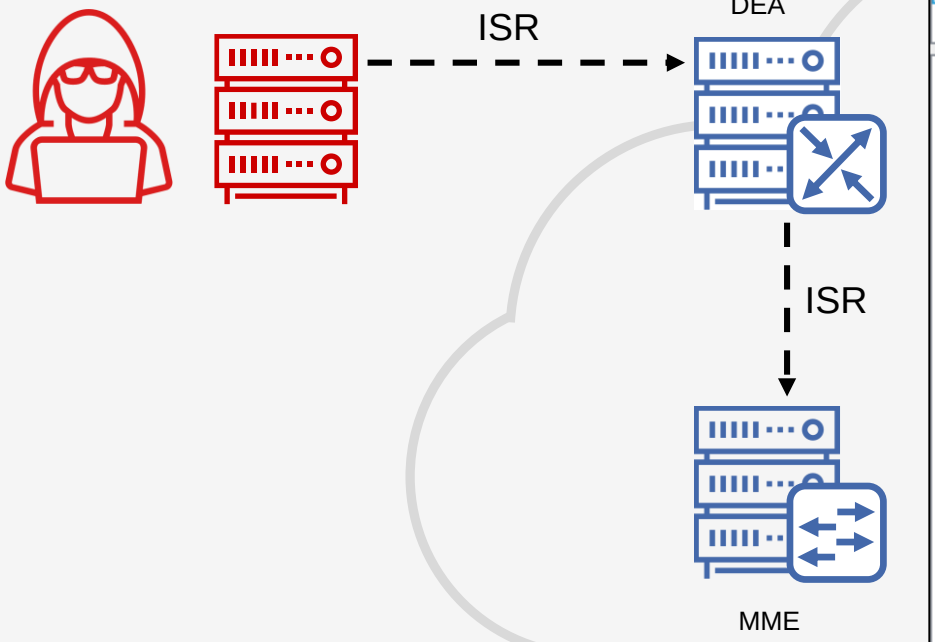
Mobile Network Code (MNC)
- **70** – Operator ID

Location Area Code (LAC)
- **00001**

Cell Identity (CID)
- **00001**

Location tracking on Diameter

ISR – Insert-Subscriber-Data Request

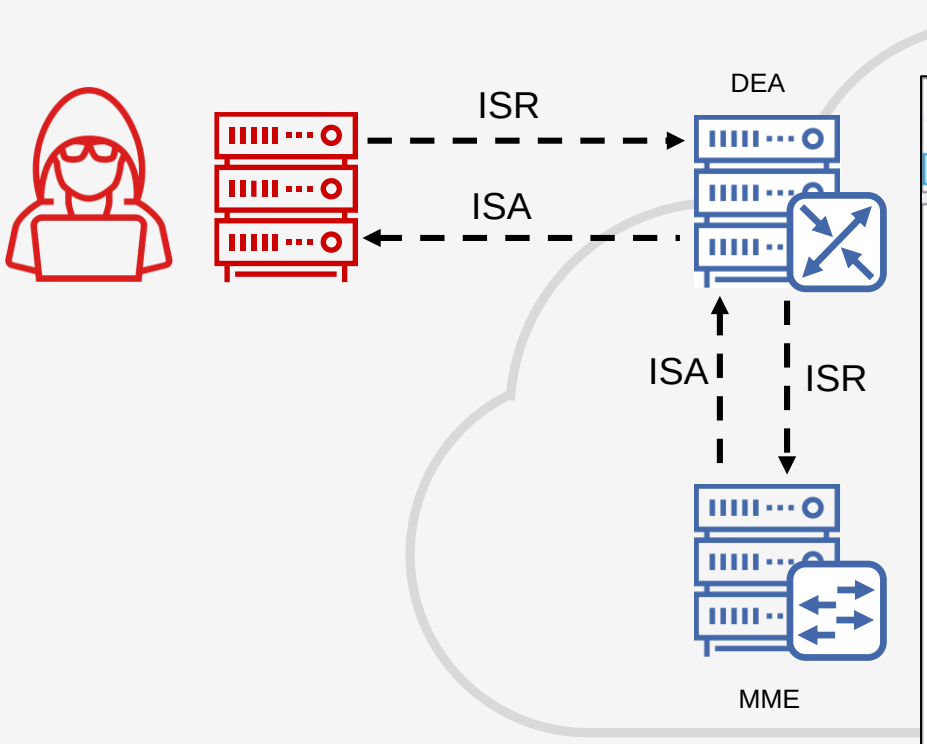



```
Protocol  Info
DIAMETER  cmd=3GPP-Insert-Subscriber-Data Request(319) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h

    ▷ AVP: User-Name(1) l=23 f=-M- val=[redacted]0932
    ▷ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
    ▷ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
    ▷ AVP: Supported-Features(628) l=56 f=VM- vnd=TGPP
    ▷ AVP: Supported-Features(628) l=56 f=VM- vnd=TGPP
    ◢ AVP: IDR-Flags(1490) l=16 f=VM- vnd=TGPP val=30
        AVP Code: 1490 IDR-Flags
      ▷ AVP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set
        AVP Length: 16
        AVP Vendor Id: 3GPP
        IDR-Flags: 30
      ◢ IDR Flags: 0x0000001e
          0000 0000 0000 0000 0000 000. .... .... = Spare: 0x000000
          .... .... .... .... .... ...0 .... .... = P-CSCF Restoration Request: Not set
          .... .... .... .... .... .... 0... .... = RAT-Type Requested: Not set
          .... .... .... .... .... .... .0.. .... = Remove SMS Registration: Not set
          .... .... .... .... .... .... ..0. .... = Local Time Zone Request: Not set
          .... .... .... .... .... .... ...1 .... = Current Location Request: Set
          .... .... .... .... .... .... .... 1... = EPS Location Information Request: Set
          .... .... .... .... .... .... .... .1.. = EPS User State Request: Set
          .... .... .... .... .... .... .... ..1. = T-ADS Data Request: Set
          .... .... .... .... .... .... .... ...0 = UE Reachability Request: Not set
```

Location tracking on Diameter

ISA – Insert-Subscriber-Data Answer




```
Protocol  Info
DIAMETER  cmd=3GPP-Insert-Subscriber-Data Request(319) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=
DIAMETER  cmd=3GPP-Insert-Subscriber-Data Answer(319) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=

    AVP: EPS-Location-Information(1496) l=80 f=VM- vnd=TGPP
        AVP Code: 1496 EPS-Location-Information
      ▷ AVP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set
        AVP Length: 80
        AVP Vendor Id: 3GPP (10415)
      ◢ EPS-Location-Information: 0000064080000044000028af0000064280000013000028af…
        ◢ AVP: MME-Location-Information(1600) l=68 f=V-- vnd=TGPP
            AVP Code: 1600 MME-Location-Information
          ▷ AVP Flags: 0x80, Vendor-Specific: Set
            AVP Length: 68
            AVP Vendor Id: 3GPP (10415)
          ◢ MME-Location-Information: 0000064280000013000028af[redacted]04400000000643…
            ◢ AVP: E-UTRAN-Cell-Global-Identity(1602) l=19 f=V-- vnd=TGPP val=[redacted]0440
                AVP Code: 1602 E-UTRAN-Cell-Global-Identity
              ▷ AVP Flags: 0x80, Vendor-Specific: Set
                AVP Length: 19
                AVP Vendor Id: 3GPP
                E-UTRAN-Cell-Global-Identity: [redacted]0440
                Padding: 00
            ▷ AVP: Tracking-Area-Identity(1603) l=17 f=V-- vnd=TGPP val=[redacted]00000
            ▷ AVP: Age-Of-Location-Information(1611) l=16 f=V-- vnd=TGPP val=0
```

Location tracking on SS7

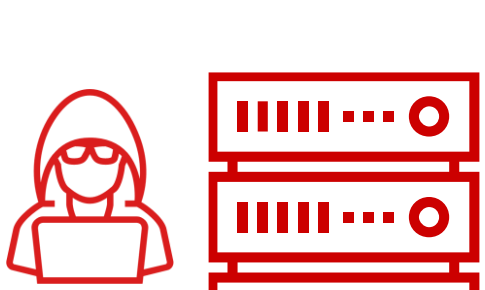
Signaling messages used for the location tracking

- ProvideSubscriberInfo
- ProvideSubscriberLocation
- AnyTimeInterrogation
- SendRoutingInfo
- InsertSubscriberData
- AnyTimeModification

Voice call interception (MITM)

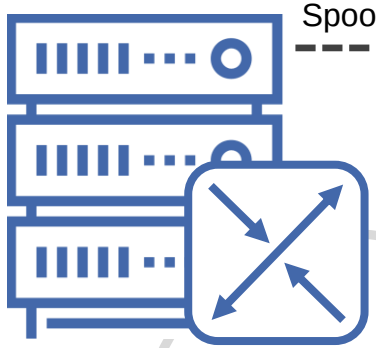
Attack via VoLTE suppression and SS7 firewall bypassing

:: Voice call interception (MITM)



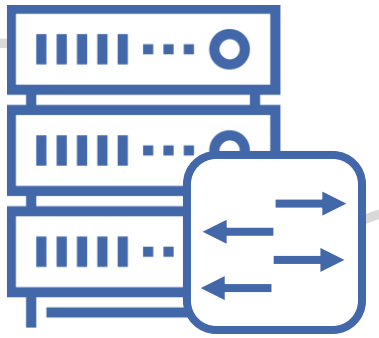
1. **InsertSubscriberData** Request: IMSI
Spoofed billing platform address

STP



1. **InsertSubscriberData** Request: IMSI
Spoofed billing platform address

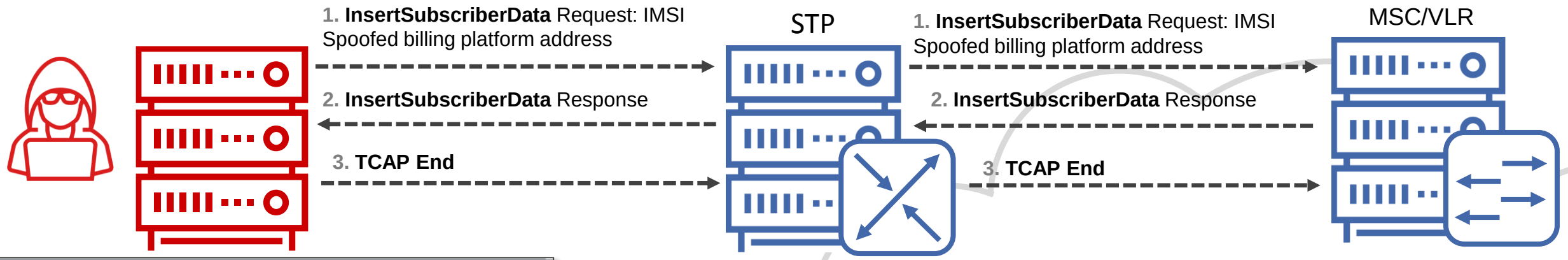
MSC/VLR



No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ▷ opCode: localValue (0)
      ▷ IMSI: [redacted]74534
      ▷ vlrCamelSubscriptionInfo
```

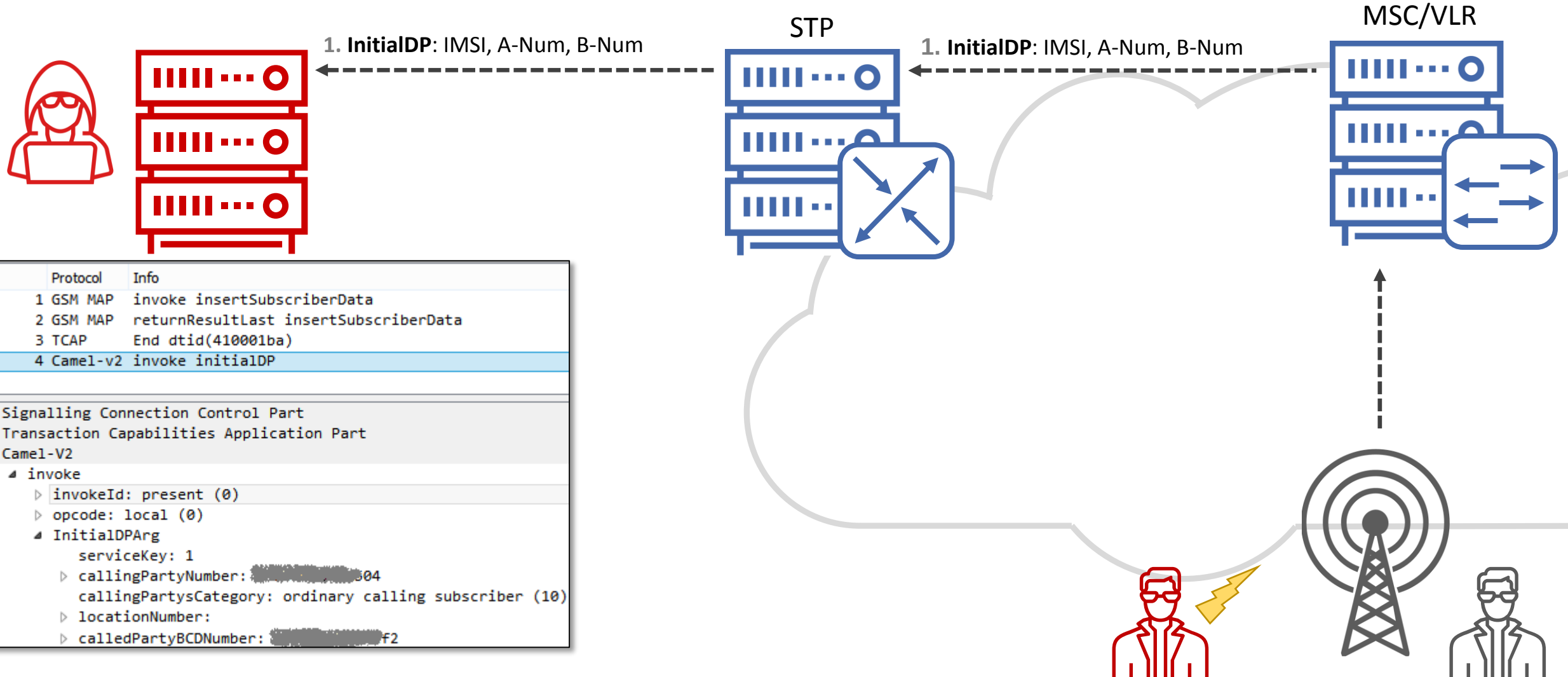
Voice call interception (MITM)



No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData
2	GSM MAP	returnResultLast insertSubscriberData
3	TCAP	End dtid(410001ba)

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: returnResultLast (2)
    ◢ returnResultLast
        invokeID: 1
      ◢ resultretres
        ▷ opCode: localValue (0)
          Padding: 4
        ▷ supportedCamelPhases: c0 (phase1, phase2)
```

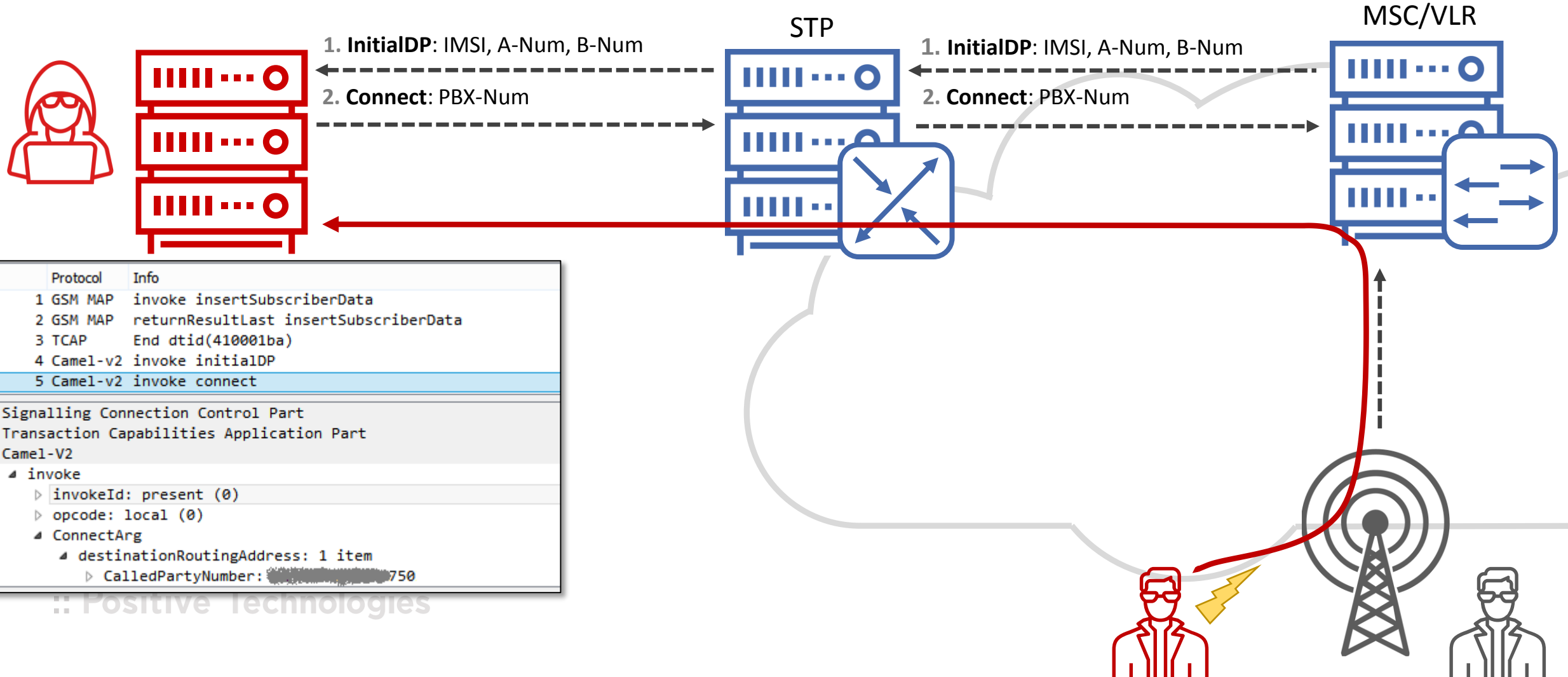
Voice call interception (MITM)



No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData
2	GSM MAP	returnResultLast insertSubscriberData
3	TCAP	End dtid(410001ba)
4	Camel-v2	invoke initialDP

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ Camel-V2
  ◢ invoke
    ▷ invokeId: present (0)
    ▷ opcode: local (0)
    ◢ InitialDPArg
        serviceKey: 1
      ▷ callingPartyNumber: [redacted]504
        callingPartysCategory: ordinary calling subscriber (10)
      ▷ locationNumber:
      ▷ calledPartyBCDNumber: [redacted]f2
```

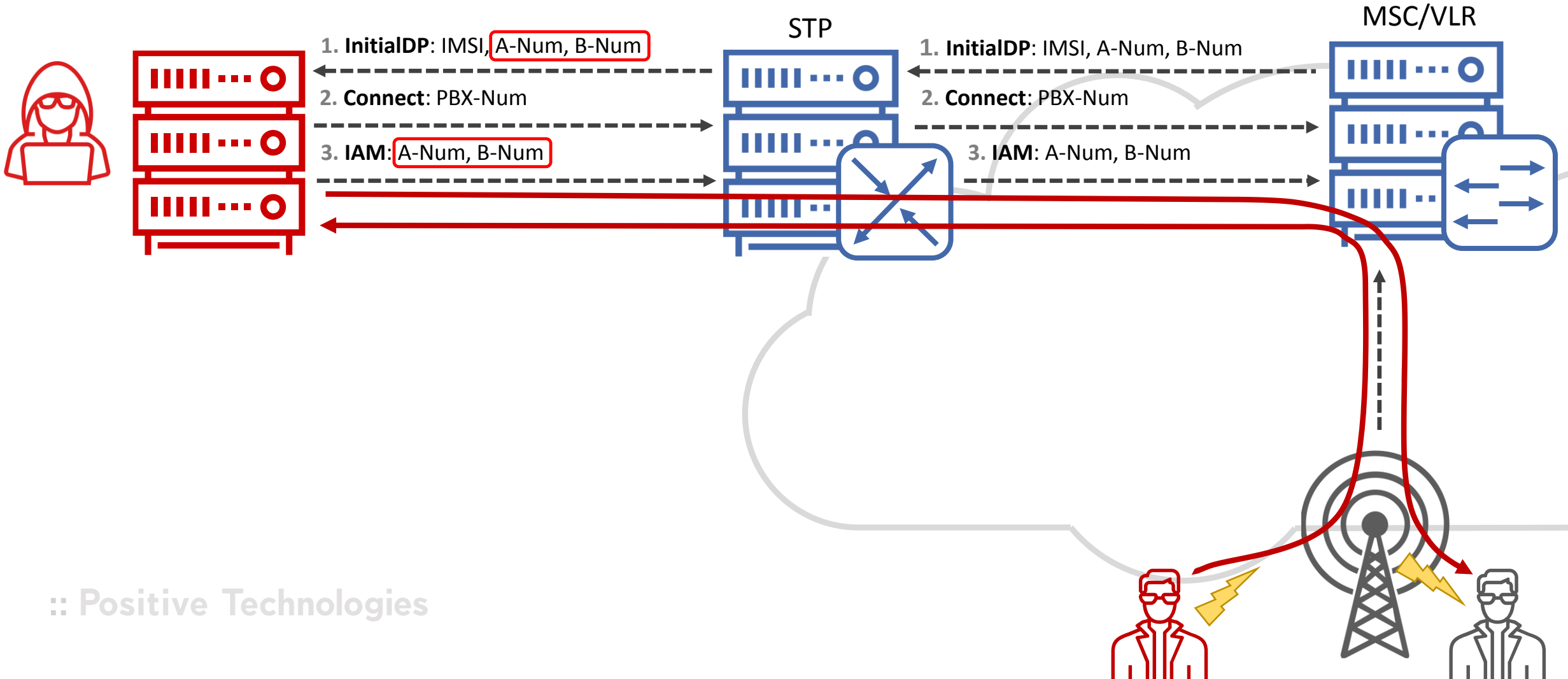
Voice call interception (MITM)



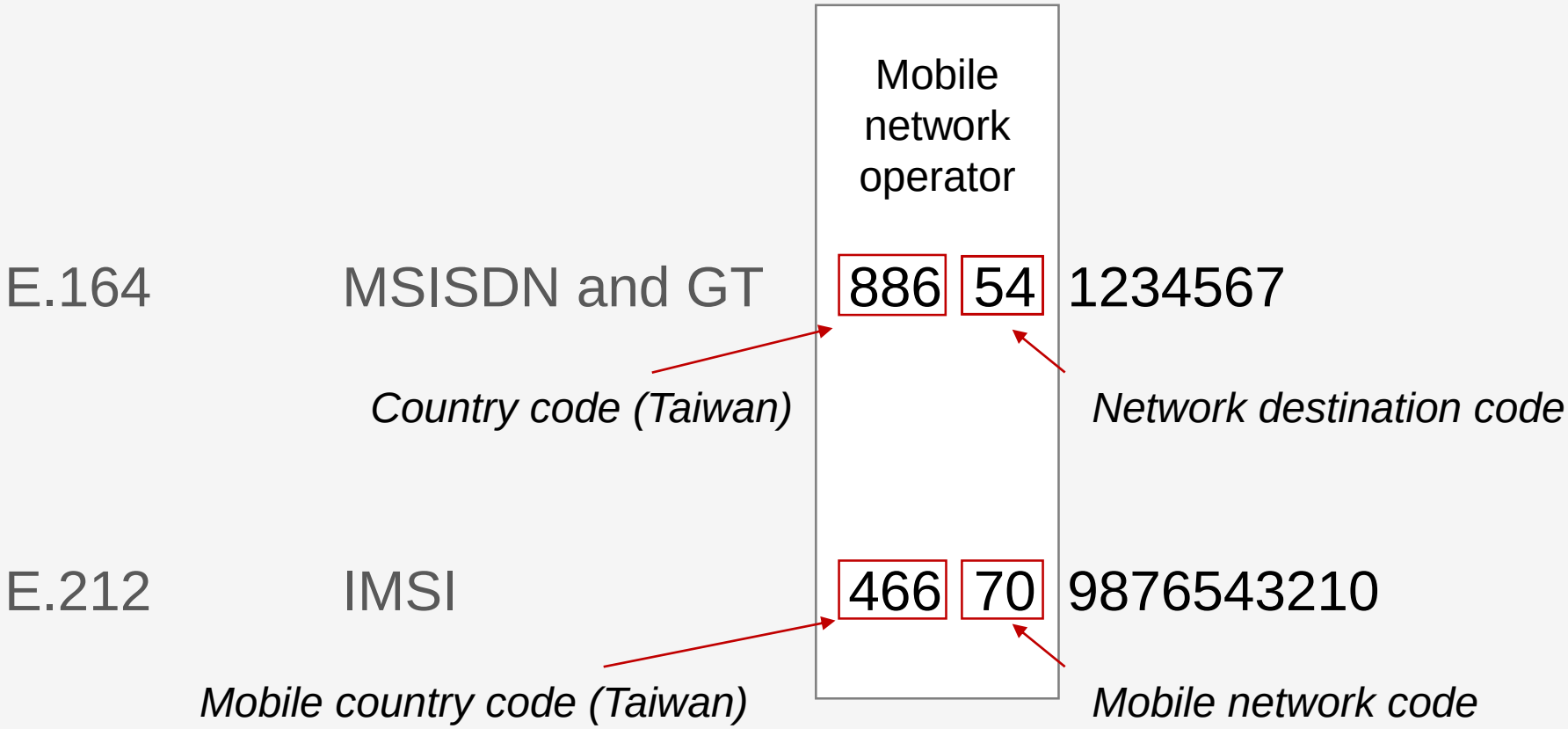
No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData
2	GSM MAP	returnResultLast insertSubscriberData
3	TCAP	End dtid(410001ba)
4	Camel-v2	invoke initialDP
5	Camel-v2	invoke connect

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ Camel-V2
  ◢ invoke
    ▷ invokeId: present (0)
    ▷ opcode: local (0)
    ◢ ConnectArg
      ◢ destinationRoutingAddress: 1 item
        ▷ CalledPartyNumber: [redacted]750
```

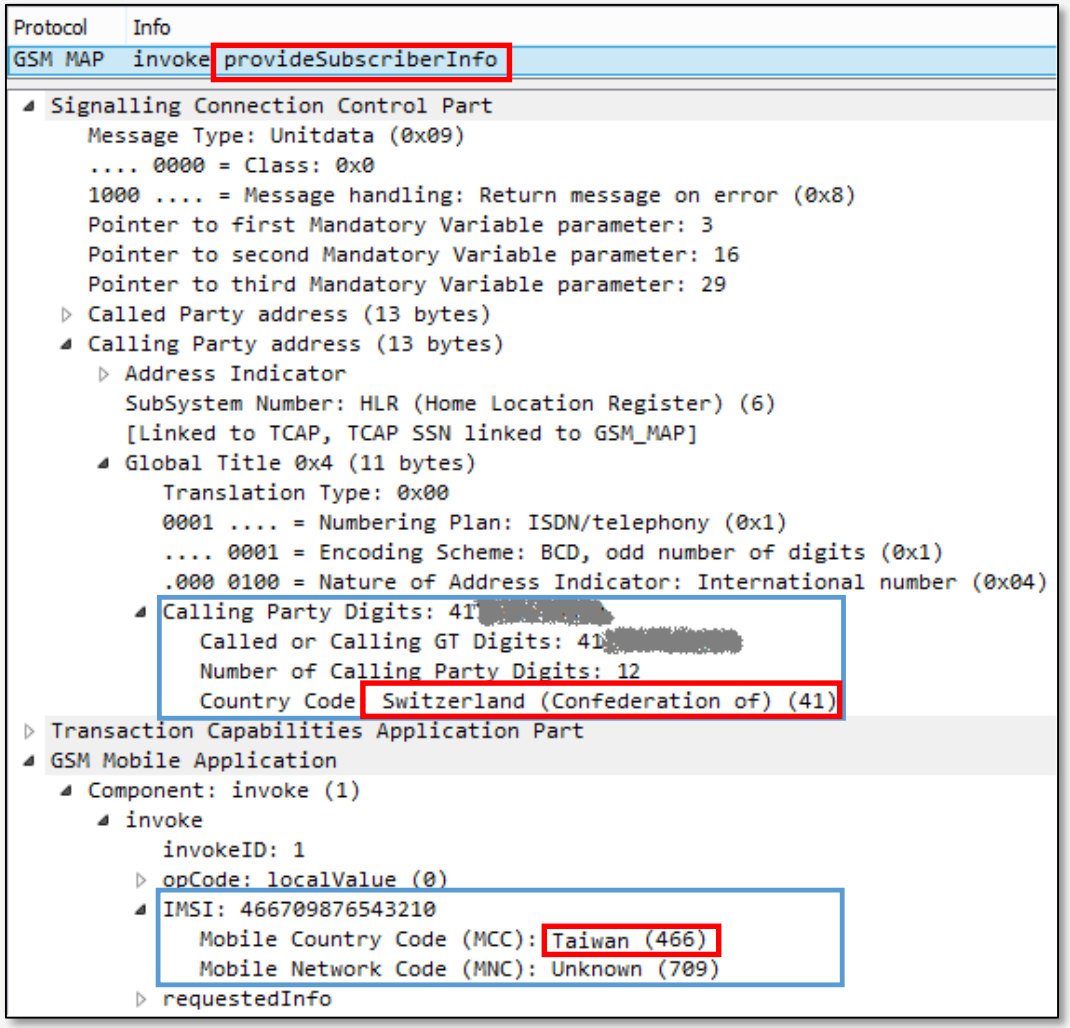
:: Voice call interception (MITM)



Numbering plans



Blocking rule: Category 2



Operation code

Category 2

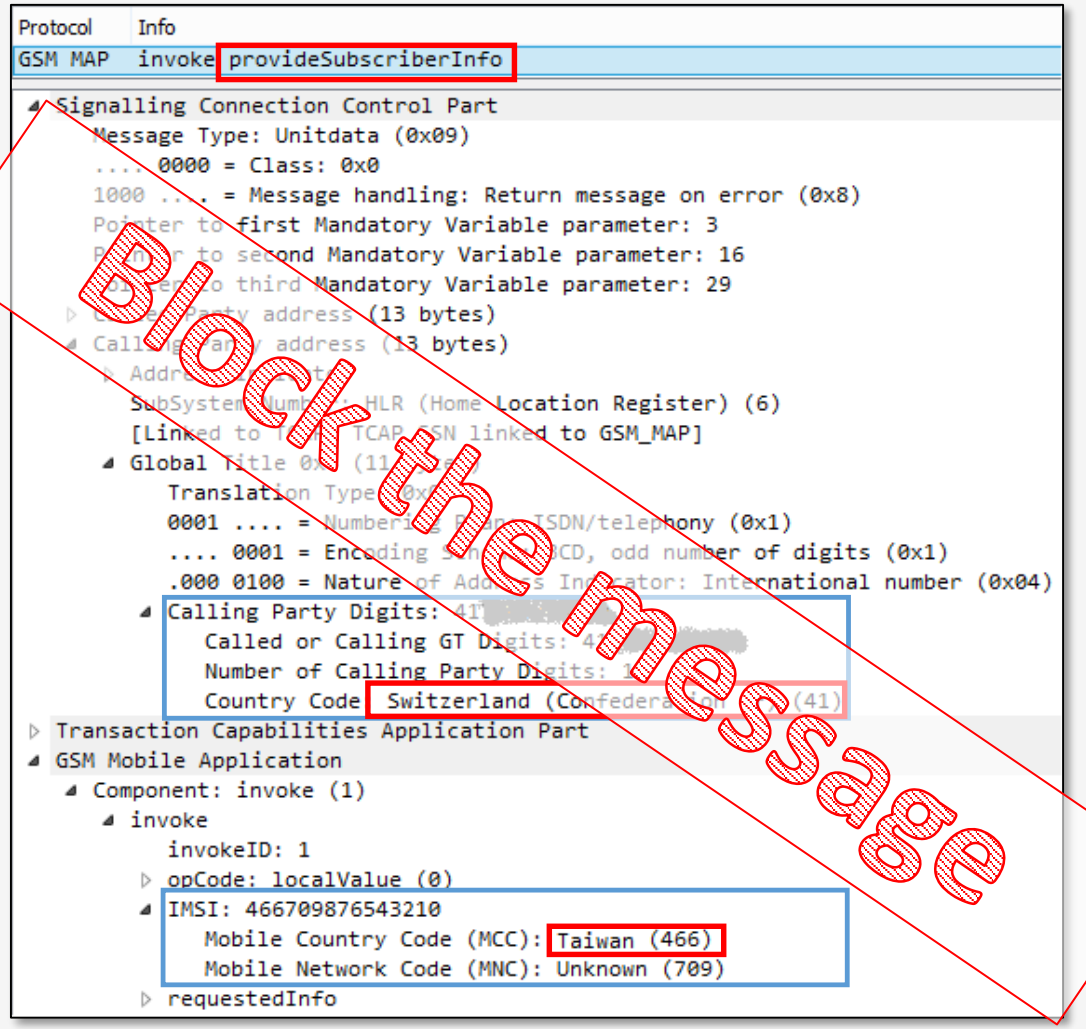
Block a message by an operation code and correlation of a **source address** and **subscriber identity**

Source address

Subscriber identity

Switzerland ≠ Taiwan

Blocking rule: Category 2



Operation code

Category 2

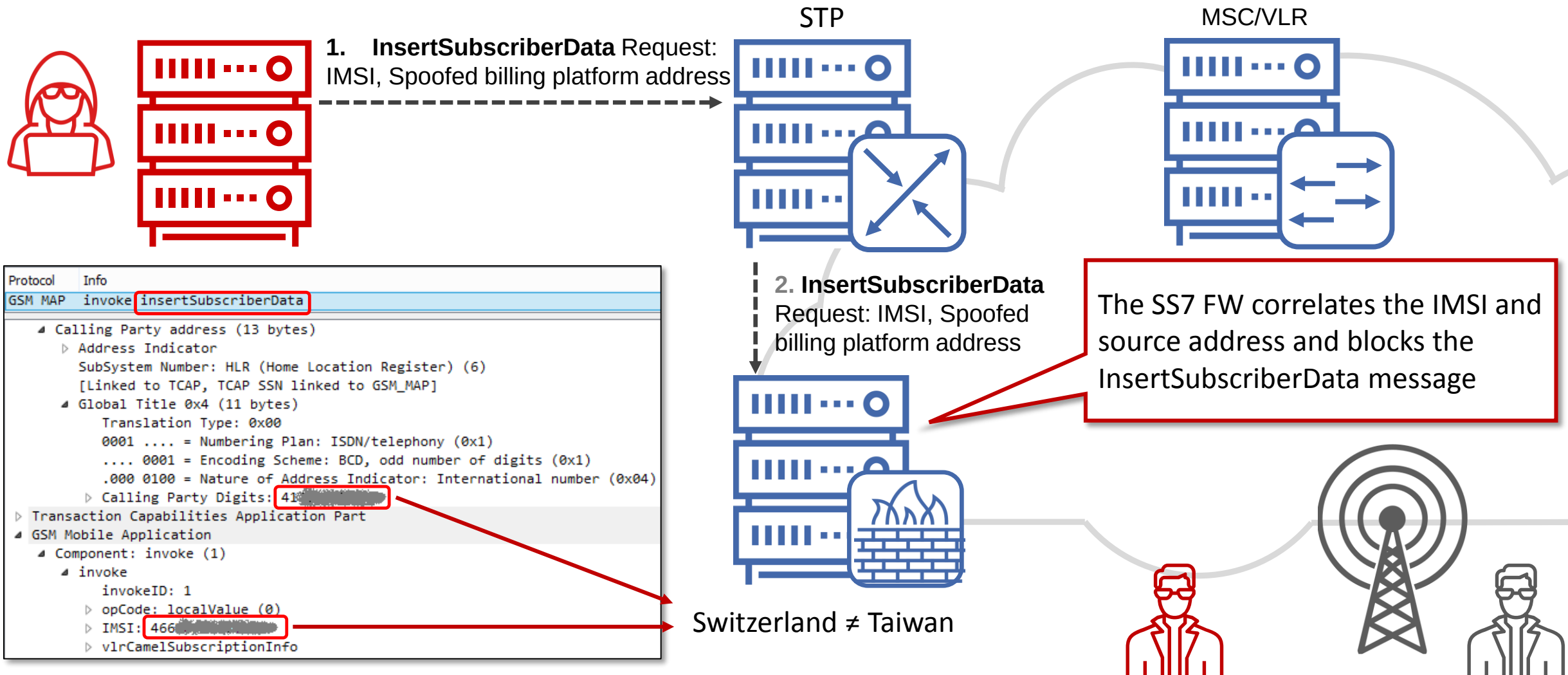
Block a message by an operation code and correlation of a **source address** and **subscriber identity**

Source address

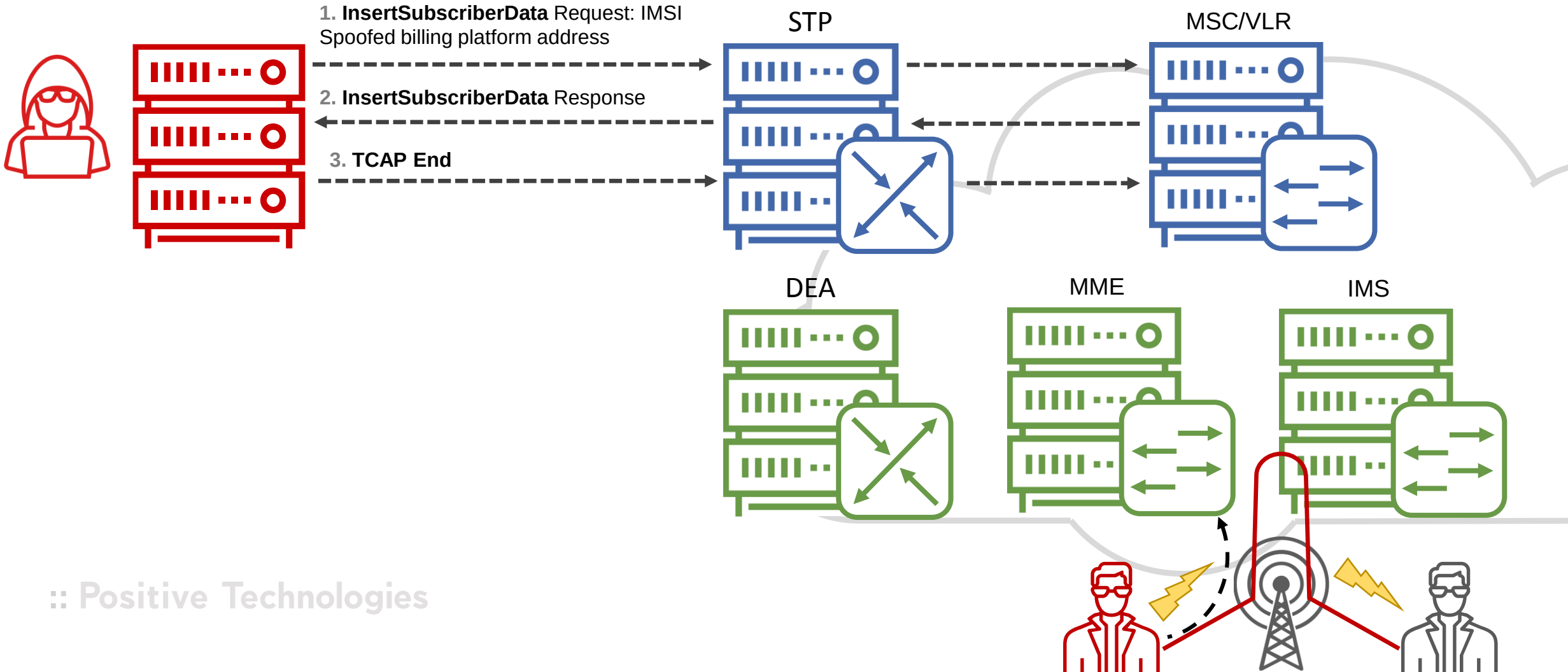
Switzerland ≠ Taiwan

Subscriber identity

SS7 FW against MITM attack

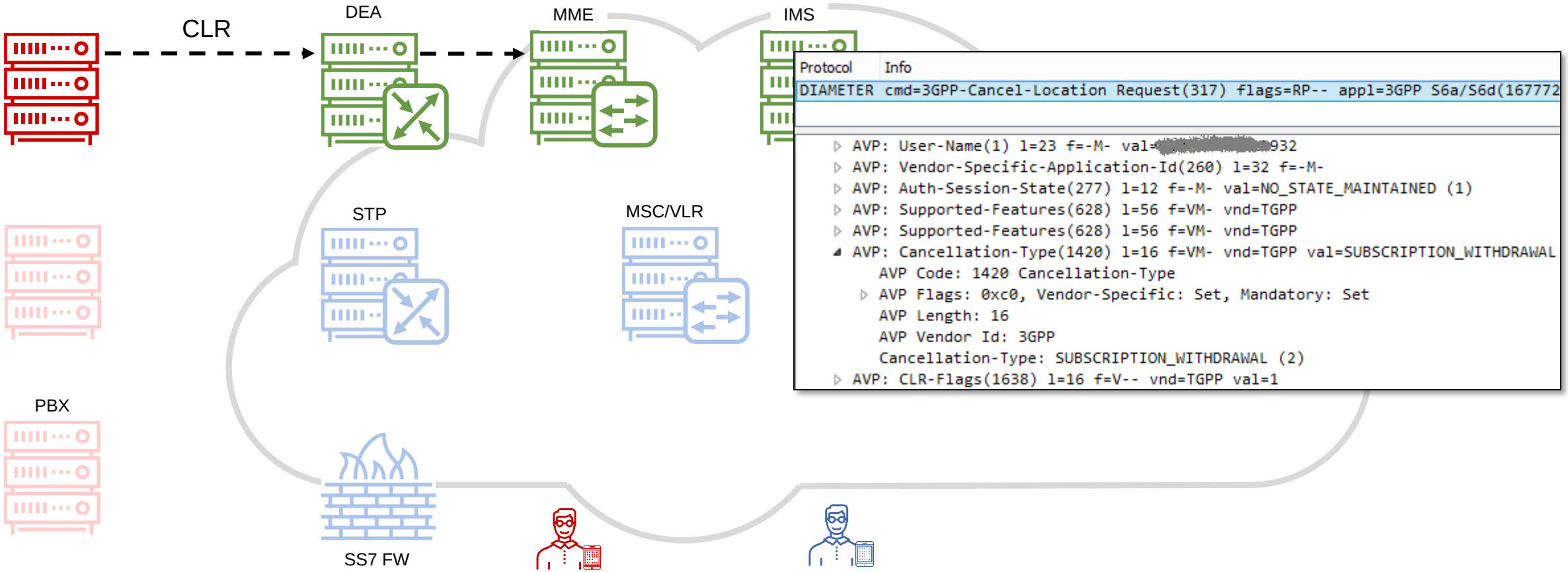


VoLTE against MITM attack



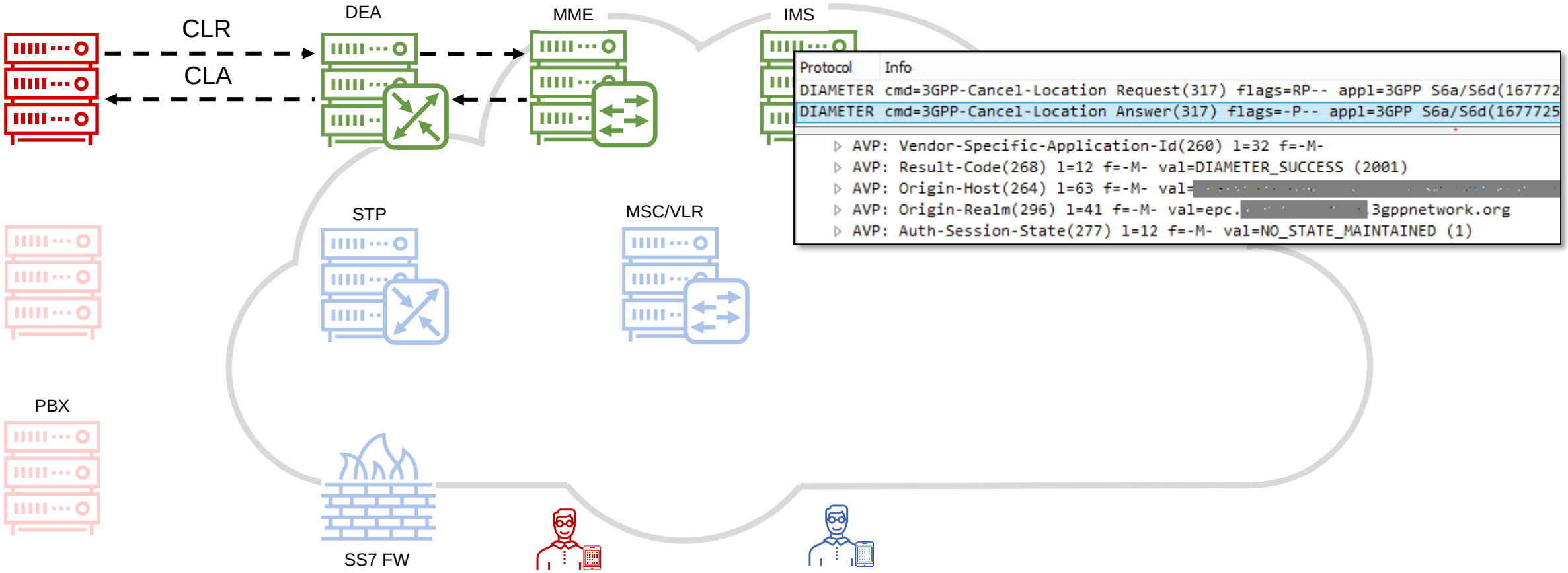
VoLTE service suppression

CLR – Cancel-Location Request



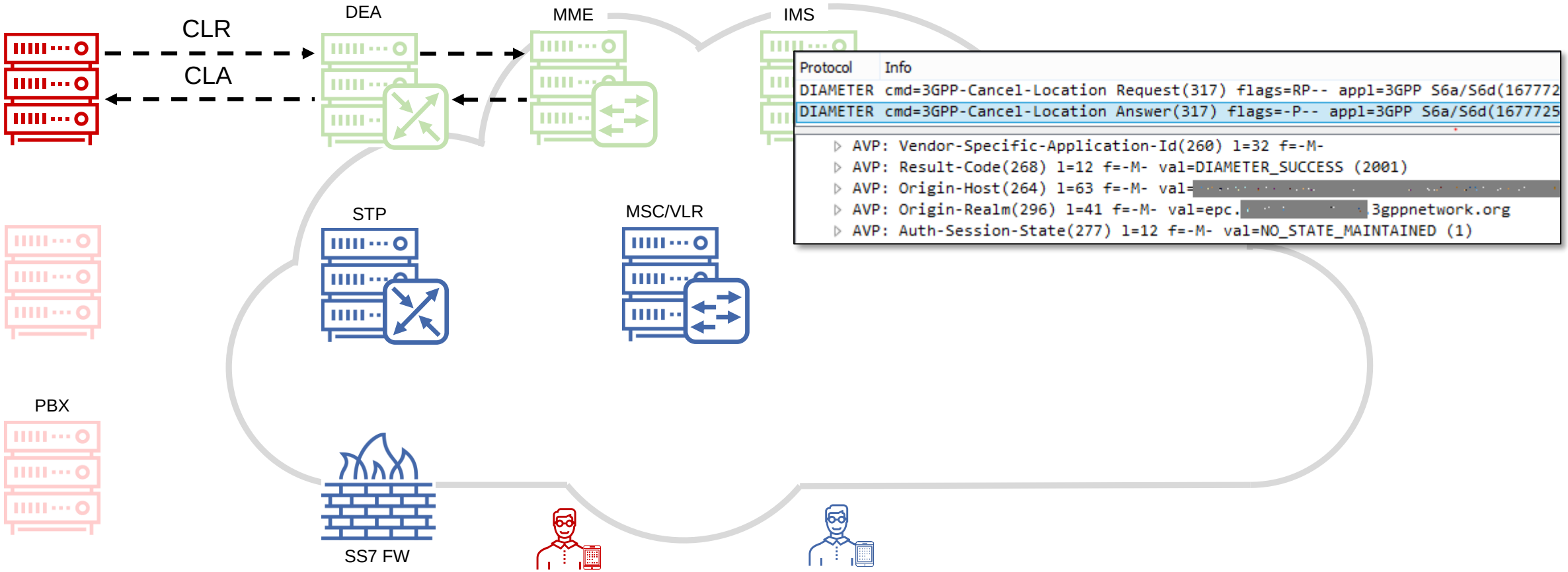
VoLTE service suppression

CLR – Cancel-Location Answer



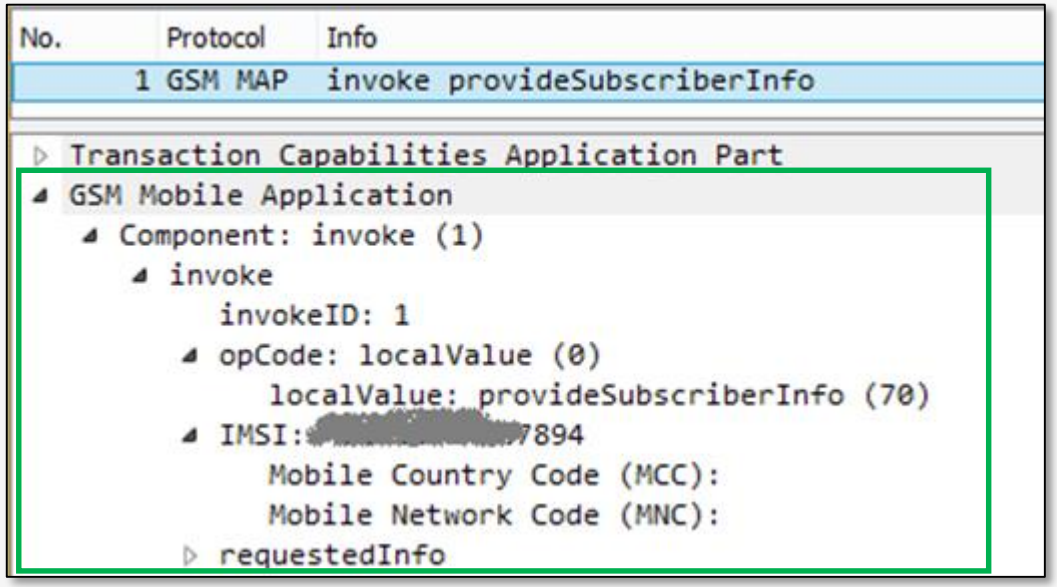
VoLTE service suppression

CLR – Cancel-Location Answer



TCAP protocol

- TCAP Message Type — mandatory
- Transaction IDs — mandatory
- Dialogue Portion — optional
- Component Portion — optional



Double MAP component

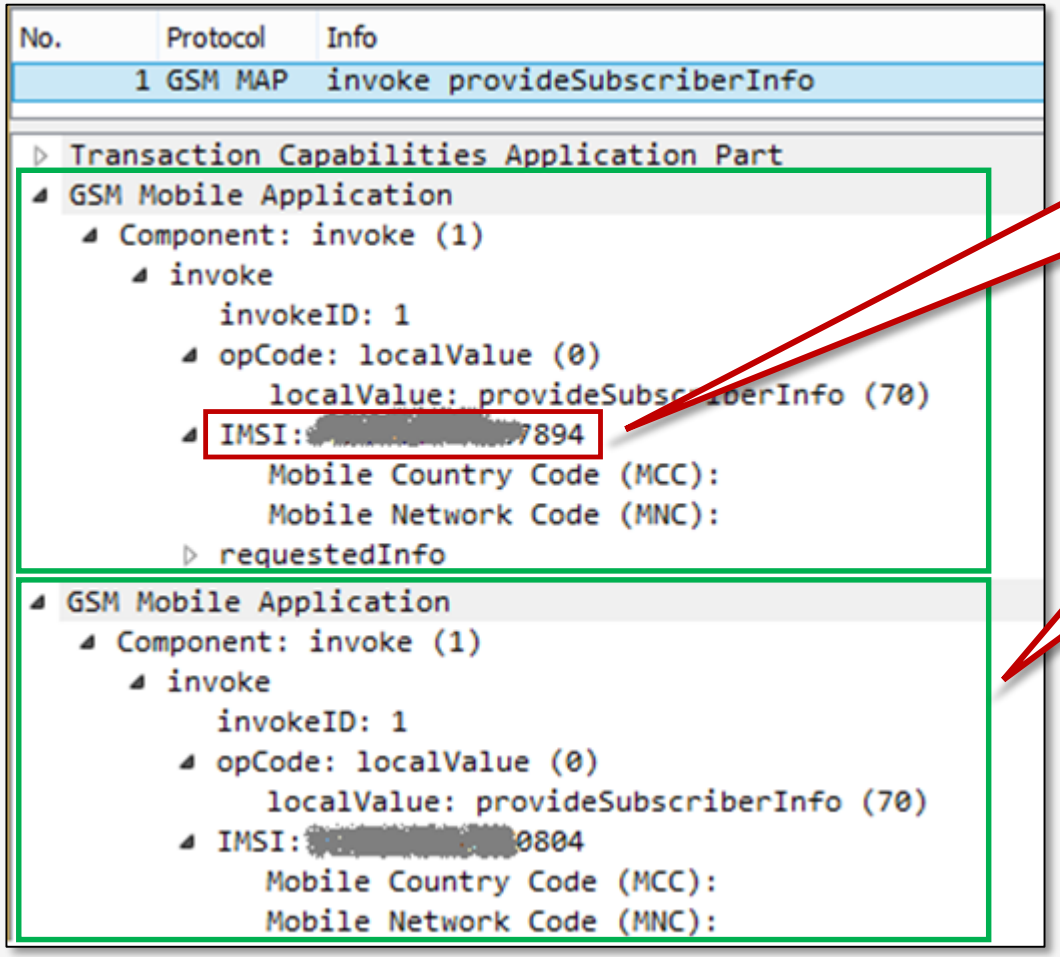
TCAP Message Type — mandatory

Transaction IDs — mandatory

Dialogue Portion — optional

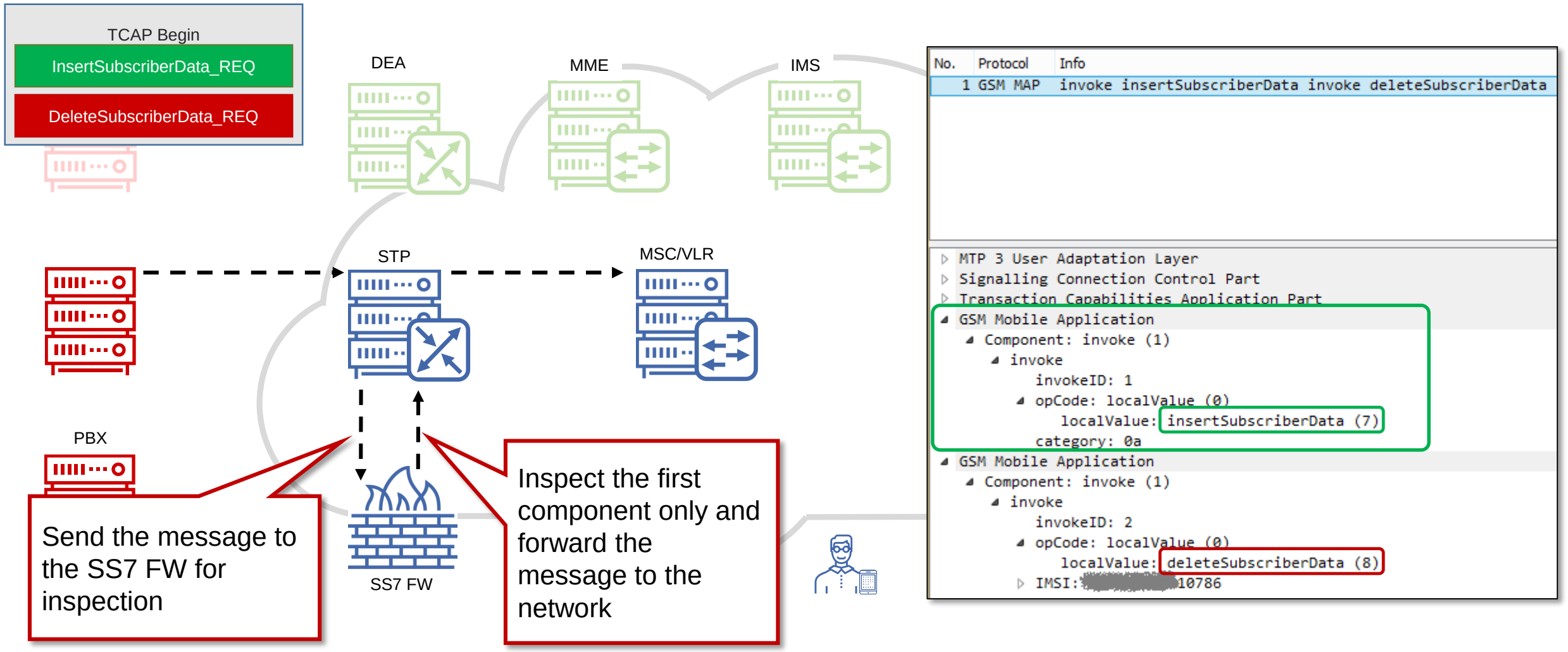
Component Portion — optional

- Component 1
- Component 2

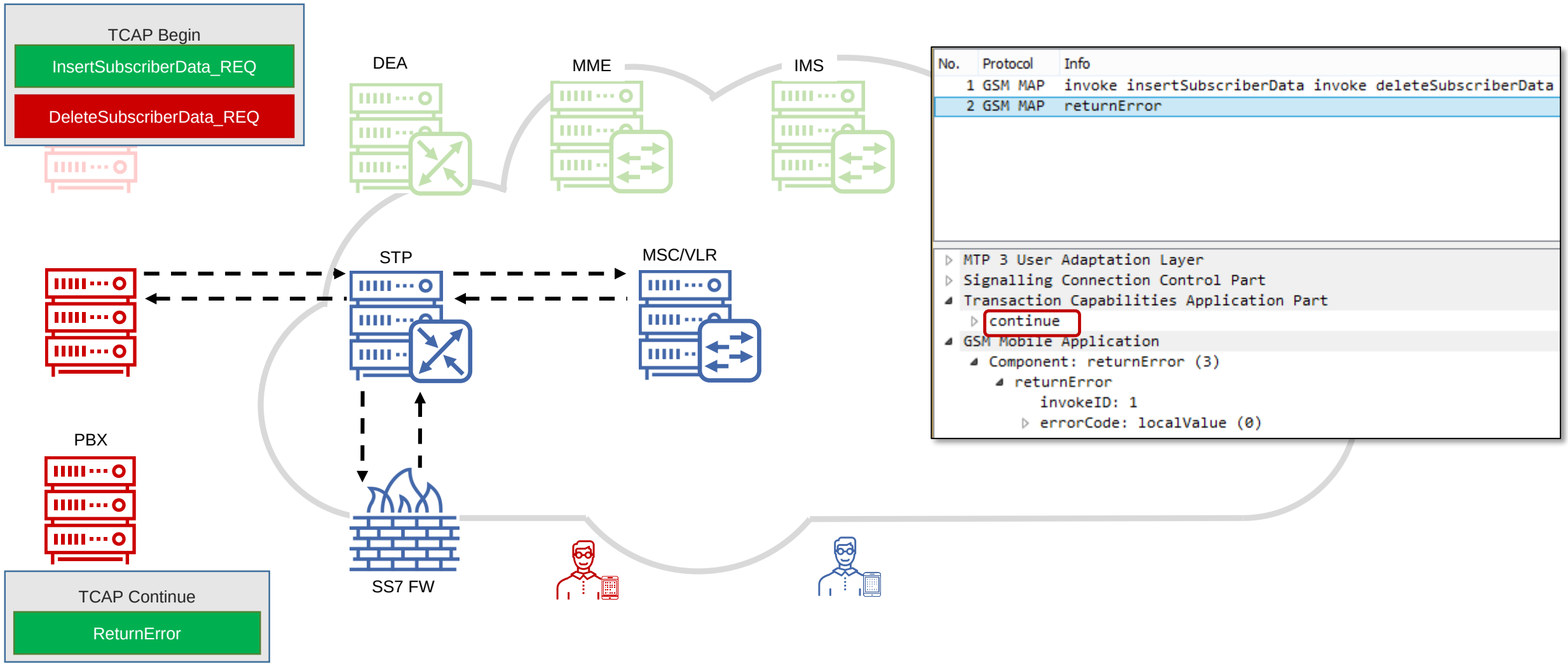


The SS7 FW checks a subscriber's ID in the first component considering the other data as a long payload not meant to be inspected

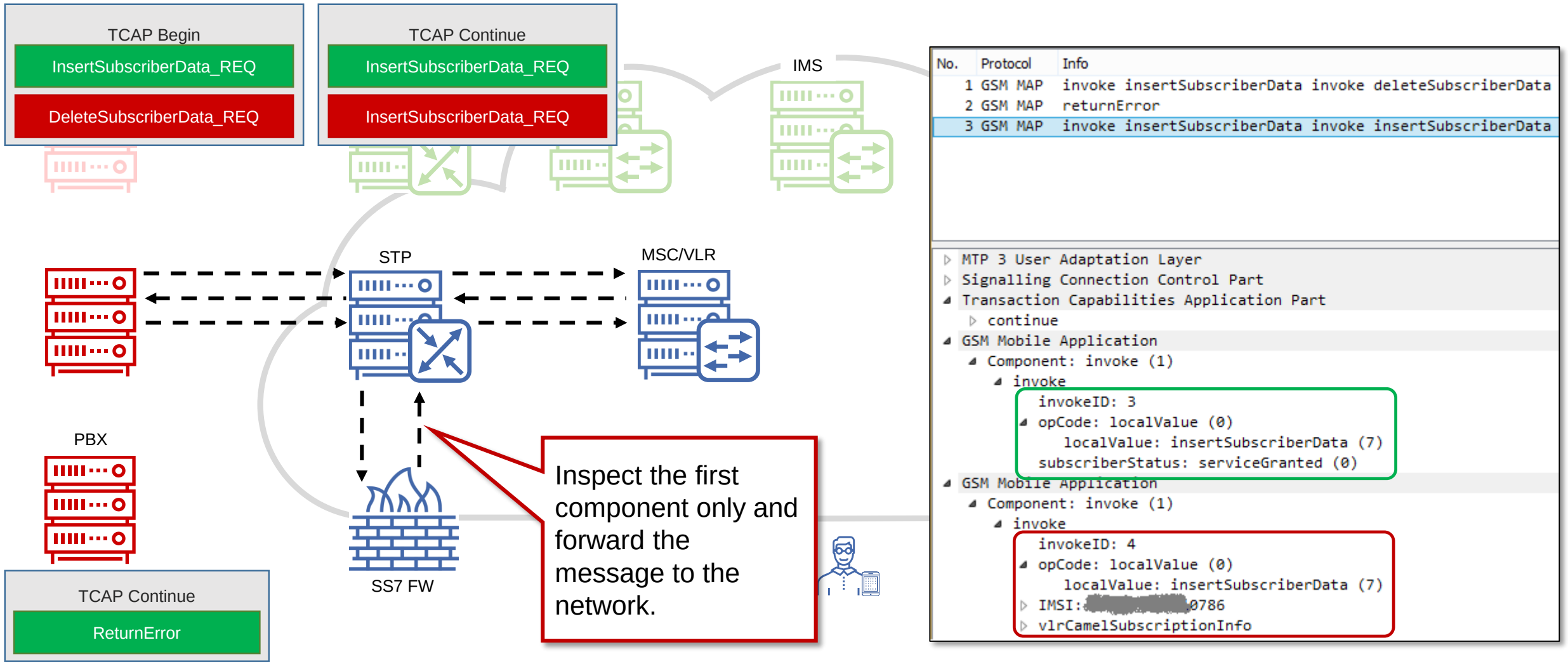
Double MAP in MITM attack



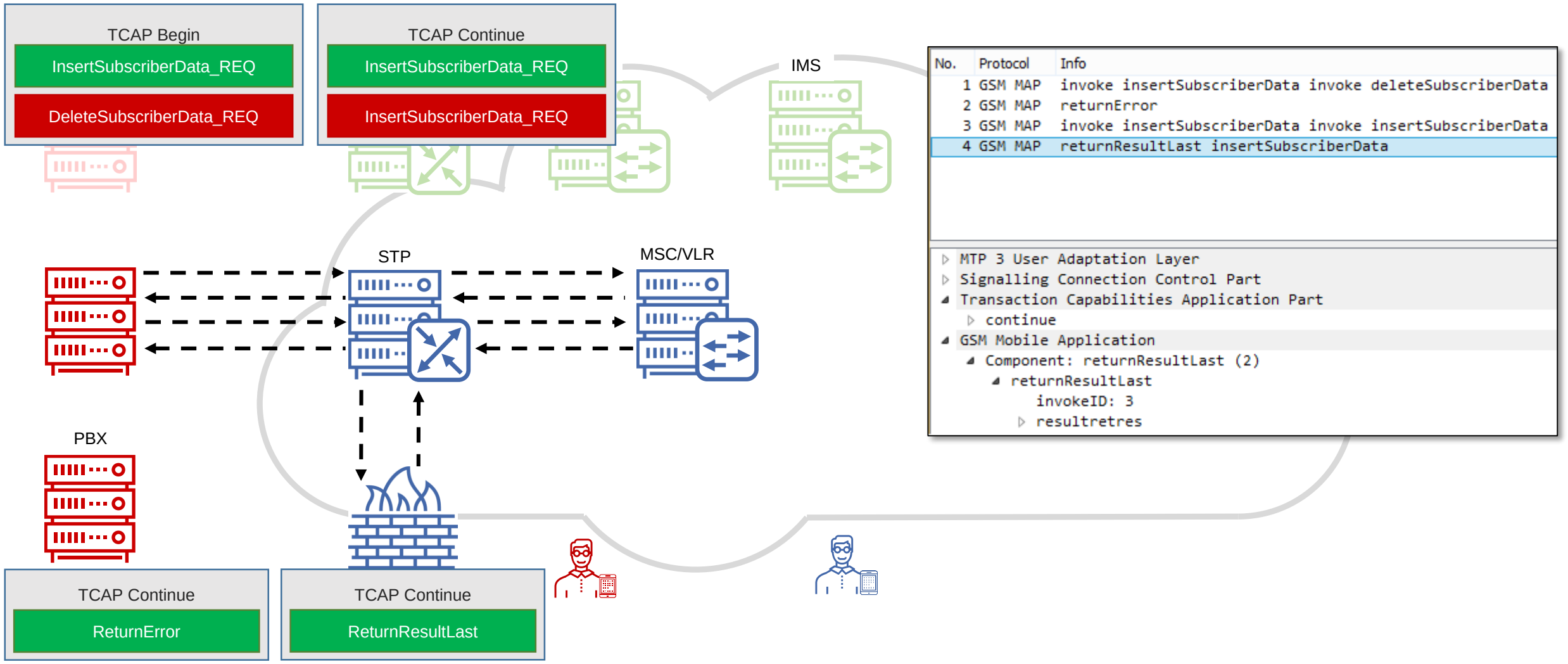
Double MAP in MITM attack



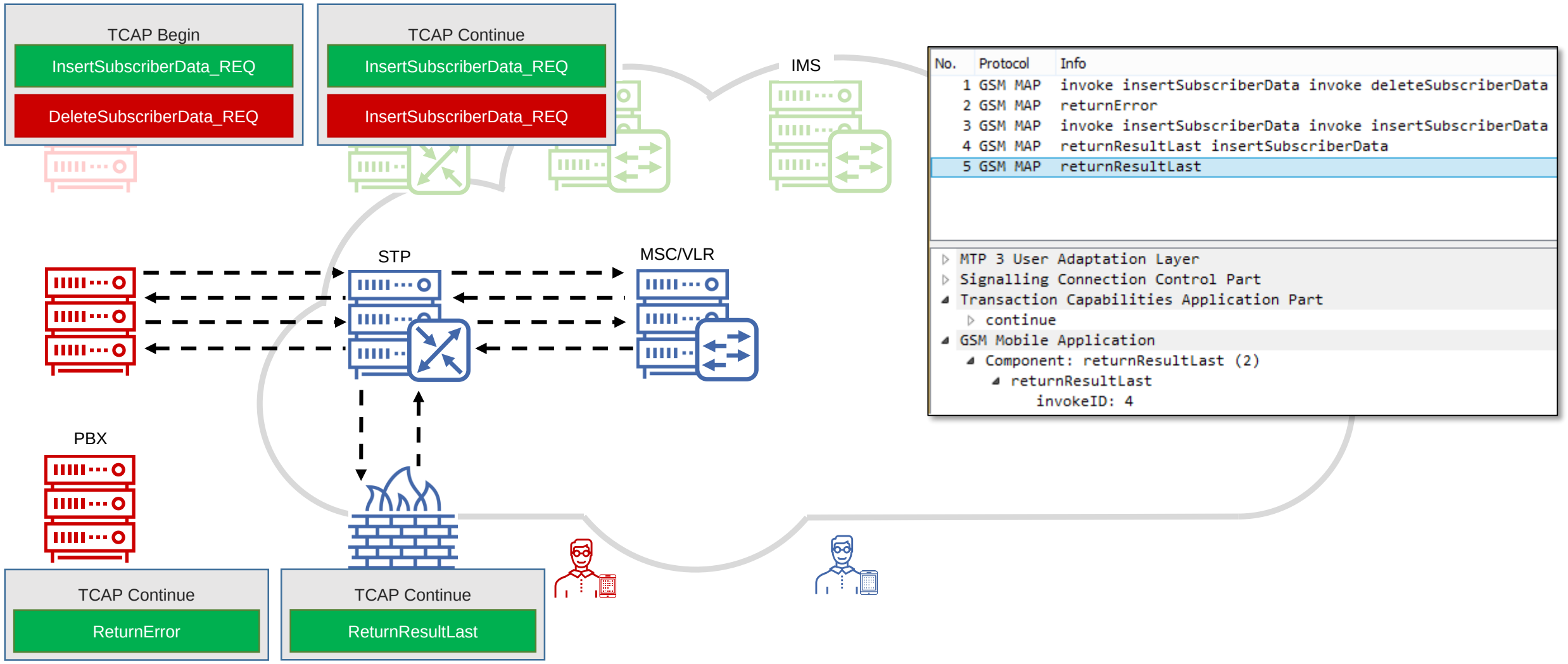
Double MAP in MITM attack



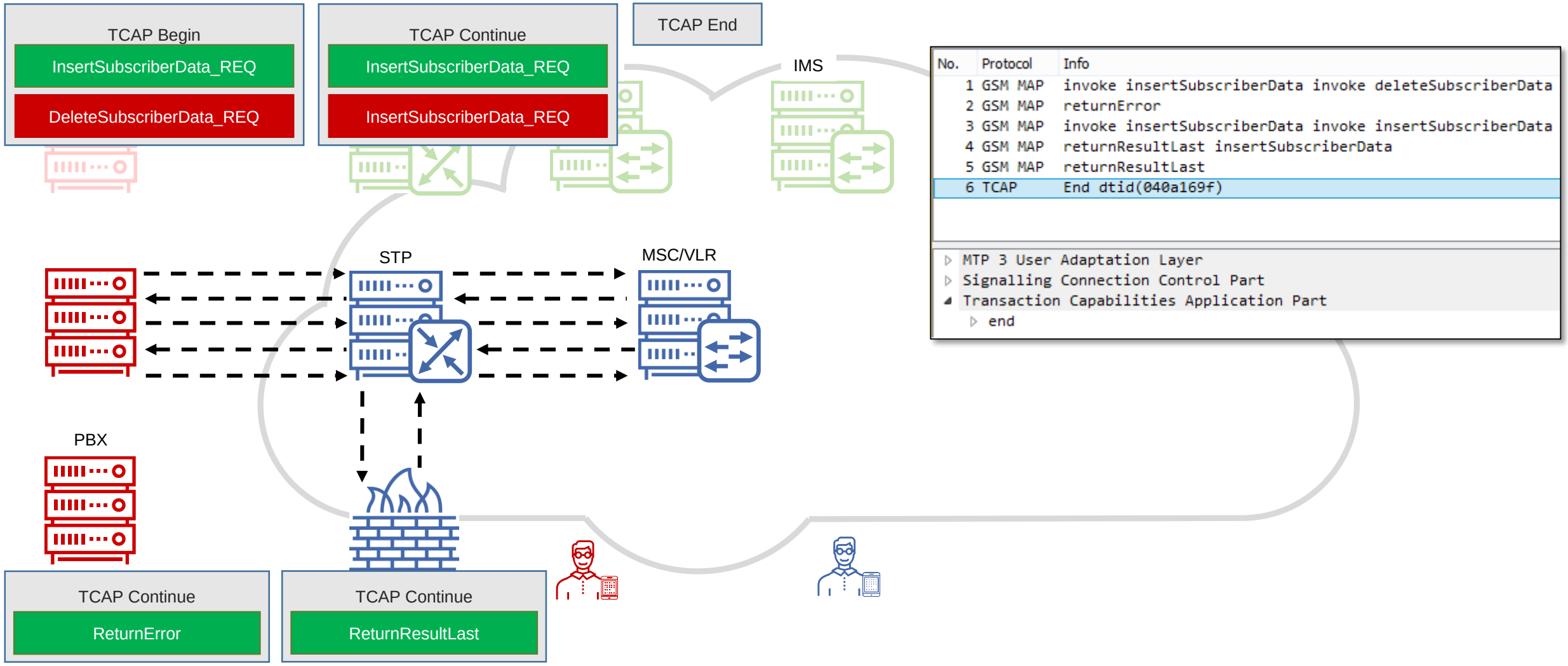
Double MAP in MITM attack



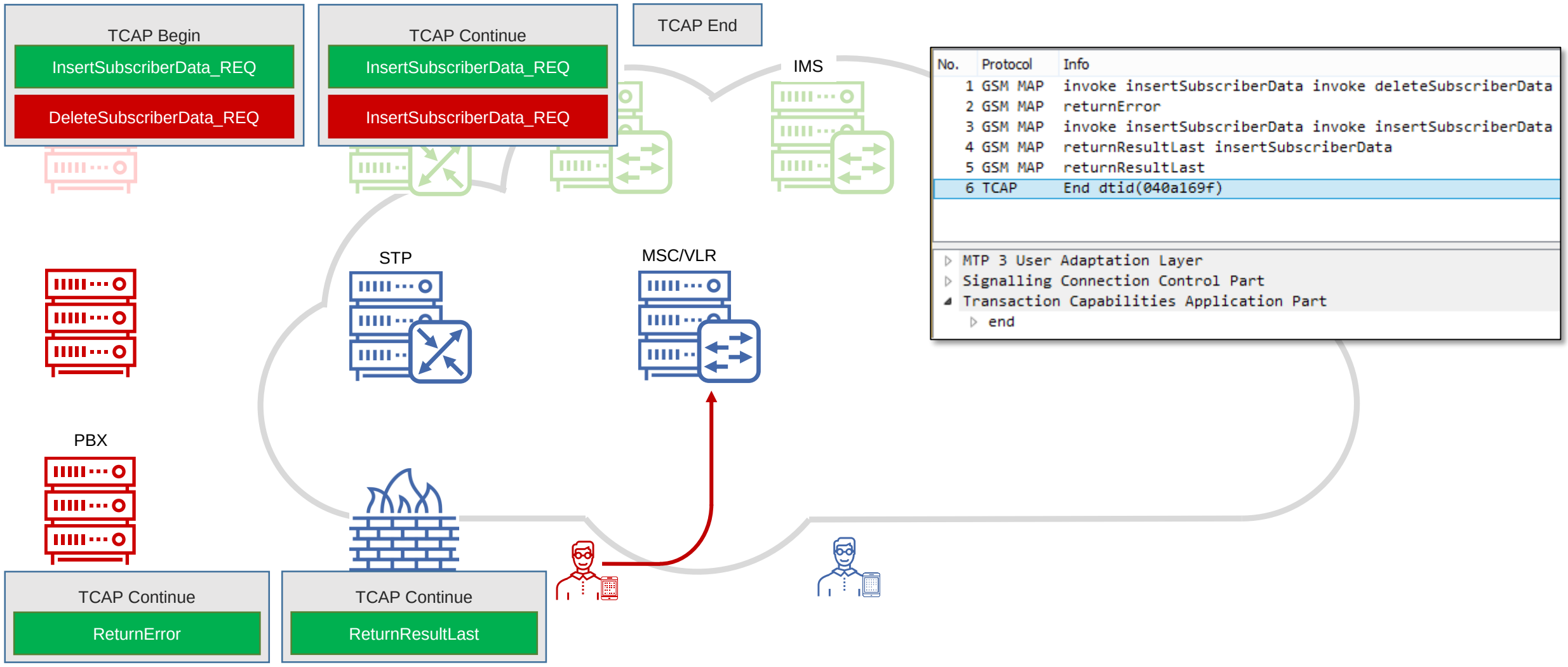
Double MAP in MITM attack



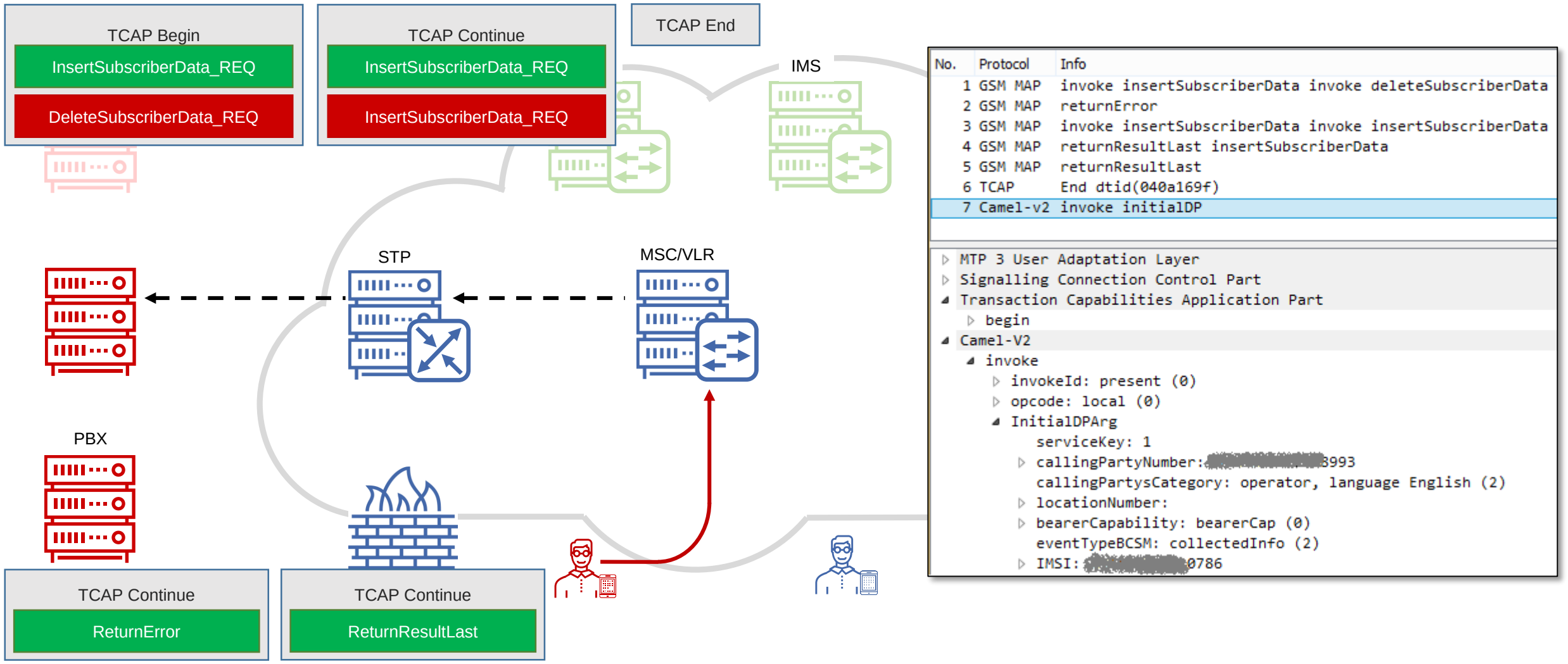
Double MAP in MITM attack



Double MAP in MITM attack



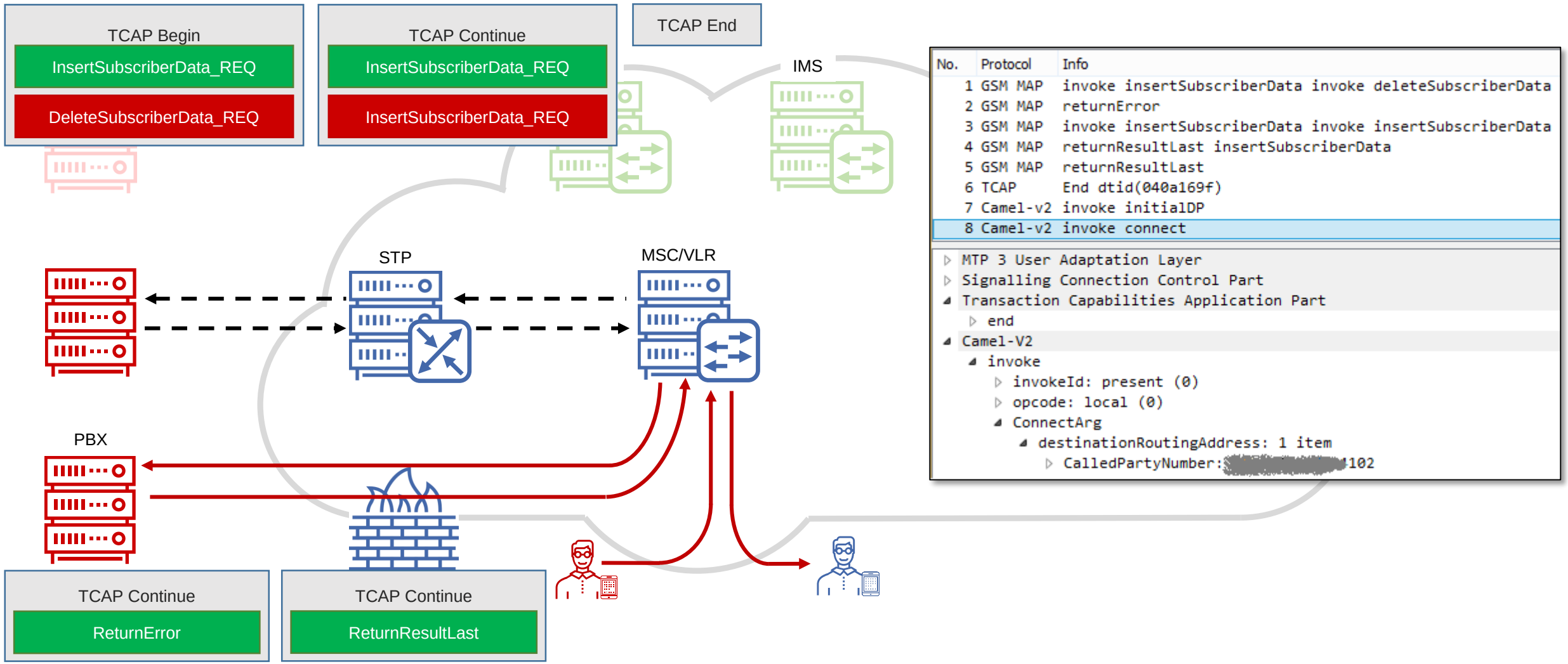
Double MAP in MITM attack



No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData invoke deleteSubscriberData
2	GSM MAP	returnError
3	GSM MAP	invoke insertSubscriberData invoke insertSubscriberData
4	GSM MAP	returnResultLast insertSubscriberData
5	GSM MAP	returnResultLast
6	TCAP	End dtid(040a169f)
7	Camel-v2	invoke initialDP

```
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ begin
◢ Camel-V2
  ◢ invoke
    ▷ invokeId: present (0)
    ▷ opcode: local (0)
    ◢ InitialDPArg
        serviceKey: 1
      ▷ callingPartyNumber: [redacted]8993
        callingPartysCategory: operator, language English (2)
      ▷ locationNumber:
      ▷ bearerCapability: bearerCap (0)
        eventTypeBCSM: collectedInfo (2)
      ▷ IMSI: [redacted]0786
```

Double MAP in MITM attack



No.	Protocol	Info
1	GSM MAP	invoke insertSubscriberData invoke deleteSubscriberData
2	GSM MAP	returnError
3	GSM MAP	invoke insertSubscriberData invoke insertSubscriberData
4	GSM MAP	returnResultLast insertSubscriberData
5	GSM MAP	returnResultLast
6	TCAP	End dtid(040a169f)
7	Camel-v2	invoke initialDP
8	Camel-v2	invoke connect

```
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ end
◢ Camel-V2
  ◢ invoke
    ▷ invokeId: present (0)
    ▷ opcode: local (0)
    ◢ ConnectArg
      ◢ destinationRoutingAddress: 1 item
        ▷ CalledPartyNumber: [redacted]102
```

Contribution to GSMA

- Information about discovered vulnerabilities has been reported to the **GSMA Coordinated Vulnerability Programme** in December 2018.
- Vulnerability ID – **CVD-2018-0015**.
- Information about the vulnerabilities appeared in a new version of the **"SS7 Interconnect Security Monitoring and Firewall Guidelines"** document that is effective from May 2019.

Main issues in signaling security

- Architecture flaws
- Configuration mistakes
- Software bugs

Protection measures

1. Check if your security tools are effective against new vulnerabilities.

2. Use an intrusion detection solution along with an **SS7** and **Diameter** firewalls in order to detect threats promptly and block a hostile source.

3. Configure your STP, DEA, and signaling firewall carefully. Do not forget about reported vulnerabilities such as malformed Application Context Name and double MAP encapsulation.

Continual real time monitoring is essential to measure network security efficiency and provide rapid detection and mitigation.

Completely secure your network by addressing both generic vulnerabilities (GSMA) and the threats that actually effect you as an ongoing process.

Auditing provides the essential visibility to fully understand your ever changing network risks.

:: Positive Technologies

谢谢您

Sergey Puzankov
sergey.puzankov@positive-tech.com