**3GPP SA WG2 Meeting #161 S2-2402352**

**Athens, Greece, February 26 – March 1, 2024**

**Source: Ericsson**

**Title: TR 23.700-63, KI#2: Getting public IP address and port after NAT**

**Document for: Approval**

**Agenda Item: 19.11**

**Work Item / Release: FS\_UPEAS Ph2 / Rel-19**

*Abstract of the contribution: The contribution proposes a solution to KI#2*

# 1. Introduction/Discussion

Solution proposal for KI#1

Although there are ways to handle NAT when NWDAF request data collection for a UE from AF, as been proposed in Rel-18. Still some more solutions may be used depending on scenarios.

# 2. Text Proposal

It is proposed to introduce the following changes vs. TR 23.700-63.

\* \* \* \* First change \* \* \* \*

## 6.X 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |
| --- | --- | --- | --- |
|  | Key Issues | | |
| Solutions | <Key Issue #1> | <Key Issue #2> |  |
| #1 |  |  |  |
| #2 |  |  |  |
| #x |  | X |  |

\* \* \* \* Next change (all new) \* \* \* \*

## 6.X Solution #X: Translating SUPI/GPSI to NATed IP address

### 6.X.1 Description

#### 6.x.1.1 Background and problem description

While in R18 UPEAS item, the NAT related issues are introduced and solved. If NAT deployed in network, there exists the mapping table between internal private UE IP address (used in 5GC internally) and public UE IP address used in application server.

If NAT is supported in network, there exists the problem that in eNA UE data collection procedure listed below:

- As indicated in step 3a and 3b in section 6.2.8.2.3 of TS 23.288[x], the NWDAF subscribes to the AF in trusted/untrusted domain for UE data collection. In the request from NWDAF, the SUPI or to GPSI is included to identify the target UE for data collection. And also indicated in the section 6.2.8.2.4.1 of TS 23.288[x], the UE IP address is used to identify the user plane connection established between the UE application and the AF for data collection. The AF is required to correlate the UE IP address to the SUPI or to GPSI. Or, as indicated in section 6.2.8.2.4.4, the NWDAF should correlate the UE IP address to the SUPI or to GPSI.

- And as described in section 6.2.8.2.4.2, 6.2.8.2.4.3 and 6.2.8.2.4.4, the AF or NWDAF uses the SUPI/GPSI to obtain the serving SMF id(s) and the corresponding PDU Session id(s) from UDM, and request the SMF to obtain the allocated IPv4 address or IPv6 prefix for the UE. After these procedures, the AF or NWDAF gets the UE IP address.

However, the allocated IPv4 address here that AF or NWDAF gets from SMF is a private IP address, not the public UE IP address. The SMF or DHCP can only allocate the private UE IP address. And in the internal 5GC, between the interaction of each 5GC elements, only the private UE IP address is used.

Even if the AF receives the private UE IP address, the AF cannot identify the target UE for data collection, because the AF can only identify the public UE IP address, if the NAT function is deployed in UPF.

So, as the description above, after introducing the NAT functionality, there is a lack of a process to provide public UE IP address to AF to identify the target UE for data collection.

#### 6.x.1.2 High level description

NWDAF can subscribe to the AF in order for the AF to collect data from UE which can be used by NWDAF for analytics to the UE. In the subscription, the NWDAF can provide the SUPI/GPSI to the AF, and the AF then needs to be able to correlate the IP flow between itself and the UE with the received SUPI/GPSI. The NWDAF can also by itself provide the IP address to the AF, i.e. NWDAF translates SUPI to UE IP address.

One solution to this correlation is for the AF/NEF to query UPF for this mapping e.g. via SMF. Since a UE can have many PDU sessions for a DNN and S-NSSAI each with its own NAT address, and the UE can also have many ongoing IP flows on a PDU sessoin where only one of these is towards the AF, there must be a way to distinguish the flow between the UE and the AF from all other flows. This solution proposes that the AF provides a list of its IP addresses that the AF uses for its communication with the UEs, or if AF uses NEF, the NEF is configured with the list of IP address the AF uses for its communication with UEs, or the UPF provides the full NAT mapping table for a UE address.

### 6.X.2 Procedures

#### 6.X.2.1 Procedure

SMF

NF/AF

UPF

1. Nsmf\_GetPublicIPaddressAndPort req.

2. Nupf\_GetPublicIPaddressAndPort req.

3. Nupf\_GetPublicIPaddressAndPort resp.

2. Nsmf\_GetPublicIPaddressAndPort req.

Figure 6.X.2-1: Getting NATed IP address and port

0. PDU session(s) has been established. If GPSI is known, NF(e.g. NEF or NWDAF)/AF has translated GPSI to SUPI. NF has discovered SMF(s) handling ~~a~~ the PDU session(s) for the combination of SUPI and DNN and S-NSSAI. The NF needs to know the endpoint addresses of the remote end (that is, all possible destination IP addresses of the UE IP flows e.g. the AF endpoints) if it is the NF and not AF that is to execute the procedure.

1. NF/AF sends 1. Nsmf\_GetPublicIPaddressAndPort request (SUPI, DNN, S-NSSAI, optionally: list of public IP addresses for the remote endpoint, e.g. the AF endpoints) to SMF. The NF/AF consumes Nudm\_UECM\_Get to obtain the address of SMFs that serving this UE.

NOTE 1: If the UE has several PDU sessions for the DNN and S-NSSAI, and these are served by different SMFs, the NF/AF sends a request to each of those SMFs.

2. SMF translate the SUPI, DNN and S-NSSAI to UE private IP address(es), and sends Nupf\_GetPublicIPaddressAndPort request (UE private IP address and,DNN, S-NSSAI, and if received, list of public IP addresses for the remote end) to UPF.

NOTE 2: If the UE has more than one PDU session for the DNN and S-NSSAI, then if the SMF uses IP address in the request to UPF, the SMF sends several requests to UPF.

3. UPF finds all related NAT mappings for the received UE private IP address (or SUPI) and if a list of public addresses was received in step 2., UPF selects the NAT mapping of the UE flows with destination IP address within the received list of public IP addresses for the remote end, andUPF responds with Nupf\_GetPublicIPaddressAndPort response (UE's NATed Public IP address, TCP/UDP Port). If UPF did not receive a list of public IP addresses for the remote end, UPF responds with all NAT mappings related to UE IP address in Nupf\_GetPublicIPaddressAndPort response.

4. SMF forwards the received info in step 3 to NF/AF.

If AF requested the public IP address via NEF, and if NEF receives the full mapping NAT mapping table (i.e., UPF did not receive a list of public IP addresses for the remote end), NEF only provides the public IP address and port that is relevant for the AF.

NOTE 3: providing full mapping table to an untrusted AF might have some privacy issues.

Editor's note: The main use case is data collection, it is FFS if the IP connection used between AF and UE in TS 23.651 is short lived or if it is long lived.

#### 6.X.2.2 Service definition

##### 6.X.2.2.1 Nupf\_GetPublicIPaddressAndPort

**Service operation name:** Nupf\_GetPublicIPaddressAndPort\_Get

**Description:** NF service consumer gets the NATed UE public IP address and Port, for the IP flow between the UE and a remote end, e.g. an AF.

**Inputs, Required:** private UE address (UE IPv4 address assigned by 5GC for the PDU session).

**Inputs, Optional:** DNN, S-NSSAI, IP domain, list of public IP addresses of the remote end.

**Outputs, Required:** if list of public IP addresses was in Inputs: a public IP address and source TCP/UDP port (or non, if no NAT mapping was found). If no list of public IP addressees was in Inputs: the full NAT mapping table for the UE IP address.

**Outputs, Optional:** None

### 6.X.3 Impacts on services, entities and interfaces

NWDAF: New service operation, need to know the end point addresses of the remote end, e.g. via configuration.

NEF: New service operation, need to know the end point addresses of the remote end, e.g. via configuration, or via signalling from AF.

AF: New service operation, can provide the end point addresses of the remote end to NEF. A trusted AF provides these endpoint addresses.

SMF: new service.

UPF: new service, providing NAT mapping.

## \* \* \* \* End of changes \* \* \* \*