Troubleshoot "Blank Natted IP" Issue in Event Data Record

Contents

[Introduction](#)
[Problem](#)
[Troubleshoot](#)
[Scenario 1](#)
[Scenario 2](#)
[Scenario 3](#)
[Scenario 4](#)

Introduction

This document describes how to troubleshoot the "blank natted IP" issue in the Event Data Record (EDR).

Problem

EDR can be seen with natted IP field as blank:

```
06/06/2022 14:53:03:056,01/01/1970 05:30:00:000,a.b.c.d,123,,,e.f.g.h,443,6,0 06/06/2022
14:53:03:098,01/01/1970 05:30:00:000,a1.b1.c1.d1,456,,,e1.f1.g1.h1,443,6,0 06/06/2022
14:53:03:109,01/01/1970 05:30:00:000,a2.b2.c2.d2,789,,,e2.f2.g2.h2,8888,6,0
```

Troubleshoot

Scenario 1

First, check to which **Firewall-and-Nat Policy** International Mobile Subscriber Identification (IMSI) is mapped and if the configuration is accurate.

For example, in **show subscribers full imsi <>** ,you can see Network Address Translation (NAT) Policy NAT44: Not-required which must be in “Required state” and also you do not see any mapped IP pool here:

```
Firewall-and-Nat Policy: xyz Firewall Policy IPv4: Required Firewall Policy IPv6: Not-required
NAT Policy NAT44: Not-required NAT Policy NAT64: Not-required CF Policy ID: n/a Congestion Mgmt
Policy: n/a active input plcy grp: n/a active output plcy grp: n/a S6b Auth Status: N/A
```

When you further check the configuration for **Firewall-and-Nat Policy: xyz**, there is no natted IP Pool mapped.

```
fw-and-nat policy fw-policy access-rule priority 3 access-ruledef acc_P3_Server1 permit access-
rule priority 4 access-ruledef acc_P3_Server2 permit access-rule priority 5 access-ruledef
```

```
acc_P3_Server3 permit access-rule priority 6 access-ruledef acc_P3_Server4 permit access-rule
priority 7 access-ruledef acc_P3_Server5 permit access-rule priority 8 access-ruledef
acc_P3_Server6 permit access-rule priority 9 access-ruledef acc_P3_Server7 permit access-rule
priority 10 access-ruledef acc_P3_Server8 permit access-rule priority 11 access-ruledef
acc_P3_ipv6_Server1 permit access-rule priority 16 access-ruledef ACC_ICMP_DENY_ALL deny
```

If you compare the same with the non-problematic scenario, you can see **Firewall-and-Nat Policy: abc ,** NAT Policy NAT44: Required and Nat Realm: www_nat.

```
Firewall-and-Nat Policy: abc Firewall Policy IPv4: Required Firewall Policy IPv6: Required NAT
Policy NAT44: Required NAT Policy NAT64: Required Nat Realm: www_nat Nat ip address: a.b.c.d
(on-demand) (publicpool1) Nexthop ip address: n/a
```

If you check the configuration for “abc”, you can observe that **nat-realm www_nat** is configured and nat-realm has IP-Pool configured:

```
fw-and-nat policy abc access-rule priority 12 access-ruledef DNSipv41 permit bypass-nat access-
rule priority 13 access-ruledef DNSipv42 permit bypass-nat access-rule priority 20 access-
ruledef DNSipv61 permit bypass-nat access-rule priority 21 access-ruledef DNSipv62 permit
bypass-nat access-rule priority 36 access-ruledef ACC_ICMP_DENY_ALL deny access-rule priority 59
access-ruledef NAT64-prefix permit nat-realm www_nat access-rule priority 60 access-ruledef
ipv4_any permit nat-realm www_nat access-rule priority 2000 access-ruledef ar-all-ipv6 permit
bypass-nat ip pool public_www8 a.b.c.d 255.255.255.0 napt-users-per-ip-address 1100 group-name
public_internet max-chunks-per-user 10 port-chunk-size 32 ip pool publicpool1 a1.b1.c1.d1
255.255.252.0 napt-users-per-ip-address 1024 group-name www_nat alert-threshold pool-used 80
clear 70 on-demand max-chunks-per-user 8 port-chunk-size 64 ip pool publicpool2 a2.b2.c2.d2
255.255.252.0 napt-users-per-ip-address 1024 group-name www_nat alert-threshold pool-used 80
clear 70 on-demand max-chunks-per-user 8 port-chunk-size 64 ip pool test a3.b3.c3.d3
255.255.255.248 private 0 group-name Test
```

Scenario 2

Check if the subscriber has a valid subscription. If for any user **Credit-Control is off**, the subscriber does not get a public natted IP.

Scenario 3

In some scenarios, natted IP cannot be seen and for those EDRs, you see incorrect end time.

```
06/29/2022 04:35:57:754,01/01/1970 05:30:00:000,a.b.c.d,51564,,,w.x.y.z,443,6,0 06/29/2022
04:35:57:752,01/01/1970 05:30:00:000,a1.b1.c1.d1,46060,,,w1.x1.y1.z1,443,6,0 06/29/2022
04:35:57:755,01/01/1970 05:30:00:000,a2.b2.c2.d2,60670,,,w1.x1.y1.z1,443,6,0
```

As per the logs, EDR has a flow end time with the date 01/01/1970.

When there is a NAT failure or some failure on the first packet, and the flow has only the first packet time set, then the last packet's time is in the initialized state. When such type of flow timeout and EDR gets generated, then the last packet time is not set and hence in the EDR, you see the epoch time.

Scenario 4

Internet Control Message Protocol (ICMP) EDRs with no public IP: For a NAT-enabled subscriber, if there is a flow initiated from the server side, NAT translation is not done for such a flow, which means such downlink flows can not be natted. This is expected behavior and as per design.

Also, for an uplink packet, if the server is unreachable (as an example), an ICMP error is returned (in the downlink direction). This ICMP flow cannot be NAT-translated. Therefore, EDR generated for this ICMP flow can not have the public IP/port.

Sample snippet:

In this EDR, it can be seen that the ICMP flow follows a UDP flow just a fraction of a second later for the same server with blank natted IP.

START TIME	END TIME	UE_PRIVATE_IP	PORT_Num	UE_PUBLIC_IP	PORT_Num	Destination_IP	PROTOCOL			MSISDN	UE_Location
07/27/2022 10:41:08:054	07/27/2022 10:48:40:154	x.x.x.x	37232	y.y.y.y	17033	a.b.c.d	443	17	0	12345	abc_def
07/27/2022 10:48:40:376	07/27/2022 10:48:40:376	x.x.x.x	0			a.b.c.d	0	1	0	12345	abc_def