

# Risoluzione dei problemi relativi a "Blank Nated IP" Issue in Event Data Record

## Sommario

---

[Introduzione](#)

[Problema](#)

[Risoluzione dei problemi](#)

[Scenario 1](#)

[Scenario 2](#)

[Scenario 3](#)

[Scenario 4](#)

---

## Introduzione

In questo documento viene descritto come risolvere il problema degli indirizzi IP vuoti nel record dei dati relativi agli eventi (EDR, Event Data Record).

## Problema

L'EDR può essere visualizzato con il campo IP nativo vuoto:

```
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
```

## Risoluzione dei problemi

### Scenario 1

Innanzitutto, selezionare a quale **Firewall-and-Nat Policy** Viene eseguito il mapping dell'International Mobile Subscriber Identification (IMSI) e se la configurazione è accurata.

Ad esempio, in `show subscribers full imsi <>`, è possibile visualizzare Network Address Translation (NAT) Policy NAT44: Not-required, che deve essere in "Required state" e inoltre non viene visualizzato alcun pool IP mappato:

```
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
```

Quando si controlla ulteriormente la configurazione per **Firewall-and-Nat Policy: xyz**, non è stato mappato alcun pool IP nated.

```
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
```

Se si confronta lo stesso scenario con quello senza problemi, è possibile visualizzare **Firewall-and-Nat Policy: abc** , NAT Policy NAT44: richiesto e 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)
                                     Nextthop ip address: n/a
```

Se si controlla la configurazione per "abc", si può notare che **nat-realm www\_nat** è configurato e per **nat-realm** è configurato IP-Pool:

```
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
```

```

ip pool publicpool1 a1.b1.c1.d1 255.255.252.0 napt-users-per-ip-address 1024 group-name www_nat ale
ip pool publicpool2 a2.b2.c2.d2 255.255.252.0 napt-users-per-ip-address 1024 group-name www_nat ale
ip pool test a3.b3.c3.d3 255.255.255.248 private 0 group-name Test

```

## Scenario 2

Verificare se il sottoscrittore dispone di una sottoscrizione valida. Se per qualsiasi utente **Credit-Control is off**, il sottoscrittore non ottiene un IP pubblico.

## Scenario 3

In alcuni scenari, non è possibile visualizzare l'IP nativo e per questi EDR l'ora di fine risulta errata.

```

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

```

In base ai registri, EDR ha un'ora di fine flusso con data 01/01/1970.

Quando si verifica un errore NAT o un errore sul primo pacchetto e per il flusso è impostata solo l'ora del primo pacchetto, l'ora dell'ultimo pacchetto è in stato inizializzato. Quando si genera un timeout di flusso di questo tipo e l'EDR, l'ora dell'ultimo pacchetto non è impostata e quindi nell'EDR, viene visualizzata l'ora dell'ora.

## Scenario 4

EDR Internet Control Message Protocol (ICMP) senza IP pubblico: per un sottoscrittore abilitato NAT, se esiste un flusso avviato dal lato server, la conversione NAT non viene eseguita per tale flusso, il che significa che tali flussi di download non possono essere annotati. Questo è il comportamento previsto e secondo la progettazione.

Inoltre, se il server non è raggiungibile (ad esempio, per un pacchetto uplink), viene restituito un errore ICMP (nella direzione di download). Questo flusso ICMP non può essere tradotto NAT. Pertanto, l'EDR generato per questo flusso ICMP non può avere l'IP/la porta pubblica.

Frammento di esempio:

In questo EDR, si può notare che il flusso ICMP segue un flusso UDP di appena una frazione di secondo per lo stesso server con IP vuoto.

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

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).