

Probleemoplossing "blanco natte IP" probleem in gebeurtenisgegevensrecord

Inhoud

[Inleiding](#)

[Probleem](#)

[Problemen oplossen](#)

[Scenario 1](#)

[Scenario 2](#)

[Scenario 3](#)

[Scenario 4](#)

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij het probleem van "lege genateerde IP" in de Event Data Record (EDR).

Probleem

EDR kan met natted IP-veld als leeg worden weergegeven:

```
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
```

Problemen oplossen

Scenario 1

Controleer eerst op welke **Firewall-and-Nat Policy** International Mobile Subscriber Identification (IMSI) wordt toegewezen en als de configuratie nauwkeurig is.

Bijvoorbeeld, in **show subscribers full imsi <>**, u kunt zien Network Address Translation (NAT) Policy NAT44: Niet-vereist die in "Vereiste staat" moet zijn en ook ziet u hier geen in kaart gebrachte IP-pool:

```
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
```

Wanneer u de configuratie verder controleert op **Firewall-and-Nat Policy: xyz**, is er geen genummerde IP-pool in kaart gebracht.

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

```
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
```

Als je hetzelfde vergelijkt met het niet-problematische scenario, kun je zien **Firewall-and-Nat Policy: abc**, **NAT-beleid NAT44: vereist** en **Nat-domein: 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
```

Als u de configuratie op "abc" controleert, ziet u dat **nat-realm www_nat** is geconfigureerd en **NAT-domein** heeft **IP-pool** geconfigureerd:

```
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

Controleer of de abonnee een geldig abonnement heeft. Indien voor een gebruiker **Credit-Control** is **off** De abonnee ontvangt echter geen openbare natte IP.

Scenario 3

In sommige scenario's is geen genummerde IP te zien en voor die EDR's zie je een onjuiste eindtijd.

```
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
```

Zoals in de logboeken, heeft EDR een flow-end tijd met de datum 01/01/1970.

Wanneer er een NAT-fout of een fout in het eerste pakket optreedt en de stroom alleen de eerste pakkettijdset heeft, dan bevindt de tijd van het laatste pakket zich in de geïnitieerde status. Wanneer een dergelijk type flow timeout en EDR gegenereerd worden, dan wordt de laatste pakkettijd niet ingesteld en dus in de EDR, ziet u de tijdstijd.

Scenario 4

Internet Control Message Protocol (ICMP) EDR's zonder openbare IP: voor een NAT-enabled abonnee, als er een stroom wordt gestart vanaf de serverkant, wordt NAT-vertaling niet uitgevoerd voor een dergelijke stroom, wat betekent dat dergelijke downlink-stromen niet kunnen worden

genatteerd. Dit is het verwachte gedrag en het ontwerp.

Ook, voor een uplinkpakket, als de server (als voorbeeld) onbereikbaar is, wordt een ICMP-fout teruggegeven (in de downlink-richting). Deze ICMP-stroom kan niet NAT-vertaald zijn. Daarom kan EDR die voor deze ICMP stroom wordt geproduceerd niet de openbare IP/poort hebben.

Monsterfragment:

In deze EDR kan worden gezien dat de ICMP-stroom een UDP-stroom volgt, slechts een fractie van een seconde later, voor dezelfde server met lege natte 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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.