Solucionar problemas de "problema de IP" nato en blanco en registro de datos de eventos

Contenido

Introducción

Este documento describe cómo resolver el problema de "IP natted en blanco" en el Registro de datos de eventos (EDR).

Problema

EDR se puede ver con el campo IP natted en blanco:

```
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

Escenario 1

En primer lugar, compruebe a qué **Firewall-and-Nat Policy** La identificación de suscriptor móvil internacional (IMSI) está asignada y si la configuración es precisa.

Por ejemplo, en **show subscribers full imsi <>** ,puede ver la política NAT44 de traducción de direcciones de red (NAT): No obligatoria, que debe estar en "Estado obligatorio" y tampoco ve ningún conjunto de IP asignado aquí:

```
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
```

Cuando vuelva a comprobar la configuración de **Firewall-and-Nat Policy: xyz**, no hay ningún conjunto de IP con nat asignado.

```
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
```

Si compara lo mismo con el escenario no problemático, puede ver **Firewall-and-Nat Policy: abc** , NAT Policy NAT44: Required y 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
```

Si verifica la configuración para "abc", puede observar que **nat-realm www_nat** está configurado y nat-realm tiene IP-Pool configurado:

```
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
```

Escenario 2

Compruebe si el suscriptor tiene una suscripción válida. Si es para cualquier usuario **Credit-Control is off**, el suscriptor no obtiene una IP de red pública.

Escenario 3

En algunos escenarios, no se puede ver la IP natted y para esos EDR, se ve una hora de finalización incorrecta.

```
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
```

Según los registros, EDR tiene un tiempo de fin de flujo con la fecha 01/01/1970.

Cuando hay una falla de NAT o alguna falla en el primer paquete, y el flujo tiene solamente el tiempo del primer paquete configurado, entonces el tiempo del último paquete está en el estado inicializado. Cuando se genera este tipo de tiempo de espera de flujo y EDR, el tiempo del último paquete no se establece y, por lo tanto, en EDR, se ve el tiempo de época.

Situación 4

EDR de protocolo de mensajes de control de Internet (ICMP) sin IP pública: para un suscriptor con NAT habilitada, si hay un flujo iniciado desde el lado del servidor, la traducción NAT no se realiza para dicho flujo, lo que significa que no se pueden obtener los flujos de enlace

descendente. Este es el comportamiento esperado y según el diseño.

Además, para un paquete de enlace ascendente, si el servidor es inalcanzable (como ejemplo), se devuelve un error ICMP (en la dirección de enlace descendente). Este flujo ICMP no se puede traducir con NAT. Por lo tanto, el EDR generado para este flujo ICMP no puede tener el puerto/IP público.

Fragmento de ejemplo:

En este EDR, se puede ver que el flujo ICMP sigue un flujo UDP apenas una fracción de segundo después para el mismo servidor con IP natted en blanco.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).