對事件資料記錄中的"；空虛的IP"；問題進行故障排除

目錄

簡介

本文說明如何解決事件資料記錄(EDR)中的「空白IP」問題。

問題

使用空的IP欄位可以看到EDR:

```
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
```

疑難排解

案例 1

首先，檢視哪個 **Firewall-and-Nat Policy** 對映國際移動使用者標識(IMSI)，以及配置是否準確。

例如，在 **show subscribers full imsi <>** ,您可以看到網路地址轉換(NAT)策略NAT44：不需要（必須處於「必需」狀態），而且您在這裡沒有看到任何對映的IP池：

```
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
```

當您進一步檢查 **Firewall-and-Nat Policy: xyz**，沒有對映的nat IP池。

```
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
```

如果將相同方案與無問題的方案進行比較，您會看到 **Firewall-and-Nat Policy: abc** ,NAT策略NAT44：必需和Nat領域：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
```

如果檢查「abc」的配置，可以觀察到 **nat-realm www_nat** 配置了nat-realm且配置了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 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
```

案例 2

檢查訂閱者是否有有效的訂閱。如果適用於任何使用者 **Credit-Control is off**，則訂閱者無法獲得公共指定的IP。

案例 3

在某些情況下，無法看到靜態IP，並且對於這些EDR，您會看到不正確的結束時間。

```
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
```

根據日誌，EDR的流結束時間是01/01/1970。

如果第一個資料包出現NAT故障或某些故障，並且流只設定了第一個資料包時間，則最後一個資料包的時間處於初始化狀態。當生成此類型別的流超時和EDR時，則未設定最後一個資料包時間，因此，在EDR中，您將看到紀元時間。

案例 4

沒有公用IP的網際網路控制訊息通訊協定(ICMP)EDR：對於啟用NAT的訂戶，如果有從伺服器端啟動的流，則不會對這種流執行NAT轉譯，這表示無法捨棄此類下行鏈路流。這是預期行為，根據設計。

此外，對於上行鏈路資料包，如果伺服器無法訪問（例如），將返回ICMP錯誤（在下行鏈路方向）。此ICMP流無法進行NAT轉換。因此，為此ICMP流生成的EDR不能具有公共IP/埠。

示例片段：

在此EDR中，可以看到ICMP流在經過幾分之一秒之後，對於具有空白本徵IP的同一伺服器，

ICMP流遵循一個UDP流。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。