对事件数据记录中的"；空白自动处理IP"；问题进行故障排除

目录

[简介](#)
[问题](#)
[故障排除](#)
[场景 1](#)
[场景 2](#)
[场景 3](#)
[场景 4](#)

简介

本文档介绍如何解决事件数据记录(EDR)中的“空白IP”问题。

问题

EDR可以看到，其中的IP字段为空：

```
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
```

故障排除

场景 1

首先，检查哪个 **Firewall-and-Nat Policy** 映射国际移动用户标识(IMSI)，并且配置是否准确。

例如，在 **show subscribers full imsi <>** ,您可以看到“网络地址转换(NAT)策略NAT44：非必需”，它必须处于“必需”状态，而且您在此处不会看到任何映射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
```

当您进一步检查 **Firewall-and-Nat Policy: xyz**，没有映射的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
```

如果将其与非问题场景进行比较，您会看到 **Firewall-and-Nat Policy: abc** ,NAT策略NAT44：必需和Nat领域：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
```

如果检查“abc”的配置，您可以观察到 **nat-realm www_nat** 已配置，并且nat-realm已配置IP池：

```
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
```

场景 2

检查订阅者是否有有效的订阅。如果适用于任何用户 **Credit-Control is off**，则用户不会获得公有的IP。

场景 3

在某些情况下，无法看到已nat的IP，并且对于这些EDR，您会看到不正确的结束时间。

```
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
```

根据日志，EDR的流结束时间是01/01/1970。

如果第一个数据包上出现NAT故障或某些故障，并且流只设置了第一个数据包时间，则最后一个数据包的时间处于初始化状态。当生成此类类型的流超时和EDR时，则未设置最后一个数据包时间，因此，在EDR中，您将看到纪元时间。

场景 4

没有公有IP的互联网控制消息协议(ICMP)EDR：对于启用NAT的用户，如果存在从服务器端启动的流，则不会对此流执行NAT转换，这意味着无法转换此类下行链路流。这是预期行为，根据设计。

此外，对于上行链路数据包，如果服务器无法访问（例如），则会返回ICMP错误（在下行链路方向）。此ICMP流不能进行NAT转换。因此，为此ICMP流生成的EDR不能具有公共IP/端口。

示例代码段：

在此EDR中，可以看到ICMP流遵循的UDP流只是稍后的几分之一秒，适用于具有空本征IP的同一服务器。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。