이벤트 데이터 레코드에서 발생한 빈 네이티브 IP" 문제 해결(&Quot;)

목차

소개

이 문서에서는 EDR(Event Data Record)에서 "빈 네이티브 IP" 문제를 해결하는 방법에 대해 설명합니다.

문제

EDR은 아래 IP 필드가 비어 있는 것으로 표시됩니다.

```
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
```

문제 해결

시나리오 1

먼저, 어느 쪽에 **Firewall-and-Nat Policy** IMSI(International Mobile Subscriber Identification)가 매핑되며 컨피그레이션이 정확한 경우

예를 들어, **show subscribers full imsi <>** ,"필수 상태"여야 하는 NAT(Network Address Translation) 정책 NAT44: Not-required를 볼 수 있으며 매핑된 IP 풀이 없습니다.

```
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
```

다음에 대한 컨피그레이션을 추가로 확인할 때 **Firewall-and-Nat Policy: xyz**매핑된 네이티브 IP 풀이 없습니다.

```
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
```

동일한 시나리오를 문제가 없는 시나리오와 비교할 경우 **Firewall-and-Nat Policy: abc** , NAT 정책 NAT44: 필수 및 NAT 영역: 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
```

"abc"에 대한 컨피그레이션을 확인하는 경우 **nat-realm www_nat** 가 구성되고 nat-realm에 IP-Pool이 구성되었습니다.

```
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
```

시나리오 2

가입자에 유효한 가입이 있는지 확인합니다. 모든 사용자의 경우 **Credit-Control is off**, 가입자는 공용 네이티브 IP를 받지 않습니다.

시나리오 3

일부 시나리오에서는 네이티브 IP를 볼 수 없으며 해당 EDR의 경우 잘못된 종료 시간이 표시됩니다.

```
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
```

로그에 따르면 EDR의 흐름 종료 시간은 1970년 1월 1일입니다.

첫 번째 패킷에서 NAT 실패 또는 일부 실패가 발생하고 흐름에 첫 번째 패킷 시간만 설정된 경우 마지막 패킷의 시간은 초기화된 상태입니다. 이러한 유형의 흐름 시간 초과와 EDR이 생성되면 마지막 패킷 시간이 설정되지 않으므로 EDR에서 에포크 시간을 볼 수 있습니다.

시나리오 4

공용 IP가 없는 ICMP(Internet Control Message Protocol) EDR: NAT가 활성화된 가입자의 경우 서버 측에서 시작된 플로우가 있는 경우 해당 플로우에 대해 NAT 변환이 수행되지 않으므로 이러한 다운링크 플로우를 연결할 수 없습니다. 이는 설계에 따른 예상 동작입니다.

또한 업링크 패킷의 경우 서버에 연결할 수 없는 경우(예: 다운링크 방향) ICMP 오류가 반환됩니다.

이 ICMP 흐름은 NAT 변환할 수 없습니다. 따라서 이 ICMP 흐름에 대해 생성된 EDR은 공용 IP/포트를 가질 수 없습니다.

샘플 스니펫:

이 EDR에서는 ICMP 흐름이 빈 네이티브 IP가 있는 동일한 서버에 대해 나중에 몇 초 정도의 UDP 흐름을 따른다는 것을 알 수 있습니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.