Fehlerbehebung bei "IP"-Problemen mit leeren Angaben im Ereignisdatensatz

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für das "blank natted IP"-Problem im Event Data Record (EDR) beschrieben.

Problem

EDR ist sichtbar, wenn das IP-Feld leer ist:

```
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
```

Fehlerbehebung

Szenario 1

Überprüfen Sie zunächst, **Firewall-and-Nat Policy** International Mobile Subscriber Identification (IMSI) wird zugeordnet, und es wird geprüft, ob die Konfiguration korrekt ist.

Beispiel: in **show subscribers full imsi <>** ,wird die NAT-Richtlinie (Network Address Translation) NAT44: Not-required (Nicht erforderlich) angezeigt, die sich im Status "Required" (Erforderlich) befinden muss. Außerdem wird hier kein zugeordneter IP-Pool angezeigt:

```
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
```

Wenn Sie die Konfiguration für **Firewall-and-Nat Policy: xyz**ist kein übergeordneter IP-Pool zugeordnet.

```
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
```

Wenn Sie das Gleiche mit dem unproblematischen Szenario vergleichen, sehen Sie **Firewall-and-Nat Policy: abc** , NAT-Richtlinie NAT44: Erforderlich und NAT-Bereich: 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
```

Wenn Sie die Konfiguration für "abc" markieren, können Sie feststellen, dass **nat-realm www_nat** ist konfiguriert, und für nat-realm ist der IP-Pool konfiguriert:

```
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
```

Szenario 2

Überprüfen Sie, ob der Abonnent über ein gültiges Abonnement verfügt. Wenn für einen beliebigen Benutzer **Credit-Control is off**, erhält der Teilnehmer keine öffentliche natted IP.

Szenario 3

In einigen Szenarien ist natted IP nicht sichtbar, und für diese EDRs wird eine falsche Endzeit angezeigt.

```
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
```

Den Protokollen zufolge hat EDR eine Endzeit des Datenflusses mit dem Datum 01.01.1970.

Wenn beim ersten Paket ein NAT-Fehler oder ein Fehler auftritt und für den Flow nur die erste Paketzeit festgelegt wurde, befindet sich die Zeit des letzten Pakets im initialisierten Zustand. Wenn eine solche Art von Flow Timeout und EDR generiert wird, wird die letzte Paketzeit nicht festgelegt, und daher wird im EDR die Epochenzeit angezeigt.

Szenario 4

Internet Control Message Protocol (ICMP)-EDRs ohne öffentliche IP: Für einen NAT-fähigen Teilnehmer wird bei einem von der Serverseite initiierten Datenfluss für einen solchen Datenfluss keine NAT-Übersetzung durchgeführt, d. h. solche Downlink-Datenflüsse können nicht verarbeitet werden. Dies ist erwartetes Verhalten und entspricht dem Design.

Wenn der Server beispielsweise nicht erreichbar ist, wird bei einem Uplink-Paket ein ICMP-Fehler zurückgegeben (in Abwärtsrichtung). Dieser ICMP-Fluss kann nicht in die NAT übersetzt werden. Aus diesem Grund darf der für diesen ICMP-Fluss generierte EDR nicht über die öffentliche IP/den öffentlichen Port verfügen.

Beispielausschnitt:

In diesem EDR ist zu sehen, dass der ICMP-Datenstrom einem UDP-Datenstrom nur Bruchteile einer Sekunde später für denselben Server mit leerer natted IP folgt.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.