أستكشاف الأخطاء وإصلاحها &t؛IP" فارغ متصل بالأحرف؛ إصدار سجل بيانات الحدث

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء إصدار "IP طبيعي فارغ" وإصلاحها في سجل بيانات الحدث (EDR).

المشكلة

يمكن مالحظة EDR مع حقل IP الحالي على أنه فارغ:

```
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
```

أستكشاف الأخطاء وإصلاحها

السيناريو 1

أوال، تحقق من أي **Firewall-and-Nat Policy** يتم تعيين المعرف الدولي لمشترك الهاتف المحمول (IMSI) وإذا كان التكوين دقيقا.

على سبيل المثال، في **show subscribers full imsi <>**, أنت يستطيع رأيت شبكة عنوان ترجمة (nat) سياسة NAT44: غير مطلوب أي يكون في "حالة مطلوبة" وأيضا ال يرى أنت أي يخطط ip برتقالة هنا:

```
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
```

عند التحقق من التكوين لـ **Firewall-and-Nat Policy: xyz**، لم يتم تعيين أي تجمع IP تابع.

```
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
```

اذإ تمق ةنراقمب سفن ويرانيسلا عم ءيشلا يذلا ال ببسي لكاشم، كنكمي نأ ىرت **Firewall-and-Nat Policy: abc** ، ةسايس NAT NAT44: بولطم و 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
```

اذإ تمق بالتحقق نم نيوكت "abc"، كنكمي ةظحالم نأ **nat-realm www_nat** مت اهنيوكت مويقو NAT-realm نيوكتب 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
```

السيناريو 2

تحقق امم إذا ناك المشترك هيدل كارتشا حلاص. إذا ناك يأل مدختسم **Credit-Control is off**، المشترك ال يحصل ىلع IP ماع.

السيناريو 3

يف ضعب السيناريوهات، ال نكمي ةدهاشم IP المجوود ايلاح ةبسنلابو ىلإ تادحو EDR هذه، كنكمي ةدهاشم تقو ءاهتنا ريغ حيحص.

```
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
```

اقفو للسجلات، يوتحي EDR ىلع تقو ءاهتنا التدفق خيراتلاب 01/01/1970.

امدنع نوكي كانه لشف NAT وأ ضعب الفشل ىلع الحزمة الأولى، والتدفق يقلتي طقف لوأ ةعومجم تقو الحزمة، دعب كلذ رخآ طبر تقو يف الحالة ةيأم. امدنع متي إنشاء اذه النوع نم EDR، ال متي نييعت رخآ تقو للحزمة والبالتالي يف EDR، ىرتس الوقت و التدفق ةلهم المستغرق.

السيناريو 4

تادحو EDR الخاصة ةصاخ لوكوتوربب لئاسر التحكم يف الإنترنت (ICMP) نودب ناونع IP ماع: متي ال، مداخلا بناج نم أدب قفدت كانه ناك اذإ ،NAT نيكمت مت يذلا كرتشملل ةبسنلاب تاطابترالا تاقفدت ريرمت نكمي ال هنأ ينعي امم ،قفدتلا اذه لثمل NAT ةمجرت ءارجإ الخلفية هذه. اذه وه السلوك المتوقع وفقا للتصميم.

بالنسبة لحزمة الوصلات أيضا، إذا كان الخادم لا يمكن الوصول إليه (على سبيل المثال)، يتم إرجاع خطأ ICMP (في إتجاه الارتباط البعيد). لا يمكن ترجمة تدفق ICMP هذا بواسطة NAT. لذلك، لا يمكن أن يحتوي EDR الذي تم إنشاؤه لتدفق ICMP هذا على IP/المنفذ العام.

نموذج التعليمة البرمجية:

في هذا EDR، يمكن ملاحظة أن تدفق ICMP يتبع تدفق UDP بعد جزء من الثانية فقط لنفس الخادم مع IP ثابت فارغ.

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).