تكوين الكشف المبكر عن الحزم ل AppID في الدفاع ضد تهديد جدار الحماية الآمن 7.4

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين الكشف المبكر عن حزم AppID في جدار الحماية الآمن من Cisco 7.4.

الخلفية - مشكلة (متطلبات العميل)

- يمكن أن يستغرق اكتشاف التطبيق من خلال الفحص العميق لحزم البيانات أكثر من حزمة واحدة لتحديد حركة المرور.
- في بعض الأحيان، حيث يكون IP و/أو المنفذ معروفا لخادم تطبيق، يمكنك تجنب فحص الحزم الإضافية.

ام الجديد

- تم إنشاء واجهة برمجة تطبيقات Lua AppID جديدة تستند إلى Snort مما يتيح لنا تعيين عنوان IP ومنفذ وبروتوكول إلى المنفذ ذي الصلة:
  - بروتوكول التطبيق (معرف تطبيق الخدمة)،
  - تطبيق العميل (معرف التطبيق العميل) و
  - تطبيق ويب (APPID الخاص بالحمولة).
- يمكن إنشاء "مكتشفات التطبيقات المخصصة" على FMC باستخدام واجهة برمجة التطبيقات هذه لاكتشاف التطبيقات.
- بمجرد تنشيط مكتشف البيانات هذا، ستسمح لنا واجهة برمجة التطبيقات الجديدة هذه بتحديد التطبيقات على الحزمة الأولى في جلسة عمل.

نظرة عامة على الميزة

- يتم تعريف واجهة برمجة التطبيقات على النحو التالي:
  - **addHostFirstPktApp** (protocol_appId، client_appId، payload_appId، عنوان IP، منفذ، بروتوكول، respect)

- يتم إنشاء إدخال ذاكرة تخزين مؤقت لكل تعيين تم إنشاؤه في مكتشف التطبيق المخصص.

- يتم فحص الحزمة الأولى من كل الجلسات الواردة لمعرفة ما إذا تم العثور على تطابق في ذاكرة التخزين المؤقت.

- بمجرد العثور على تطابق، نقوم بتعيين المسارات المقابلة لجلسة العمل وتوقف عملية اكتشاف التطبيقات.

- يتوفر للمستخدمين خيار إعادة تذكر حركة المرور حتى بعد العثور على تطابق من قبل واجهة برمجة التطبيقات (API).

- وسيطة RecoverView هي قيمة منطقية تشير إلى ما إذا كانت هناك حاجة إلى إعادة مراعاة التطبيقات الموجودة في الحزمة الأولى أم لا.

- عندما تكون عملية إعادة الفحص صحيحة، يستمر اكتشاف التطبيقات حتى إذا وجدت واجهة برمجة التطبيقات (API) تطابق.

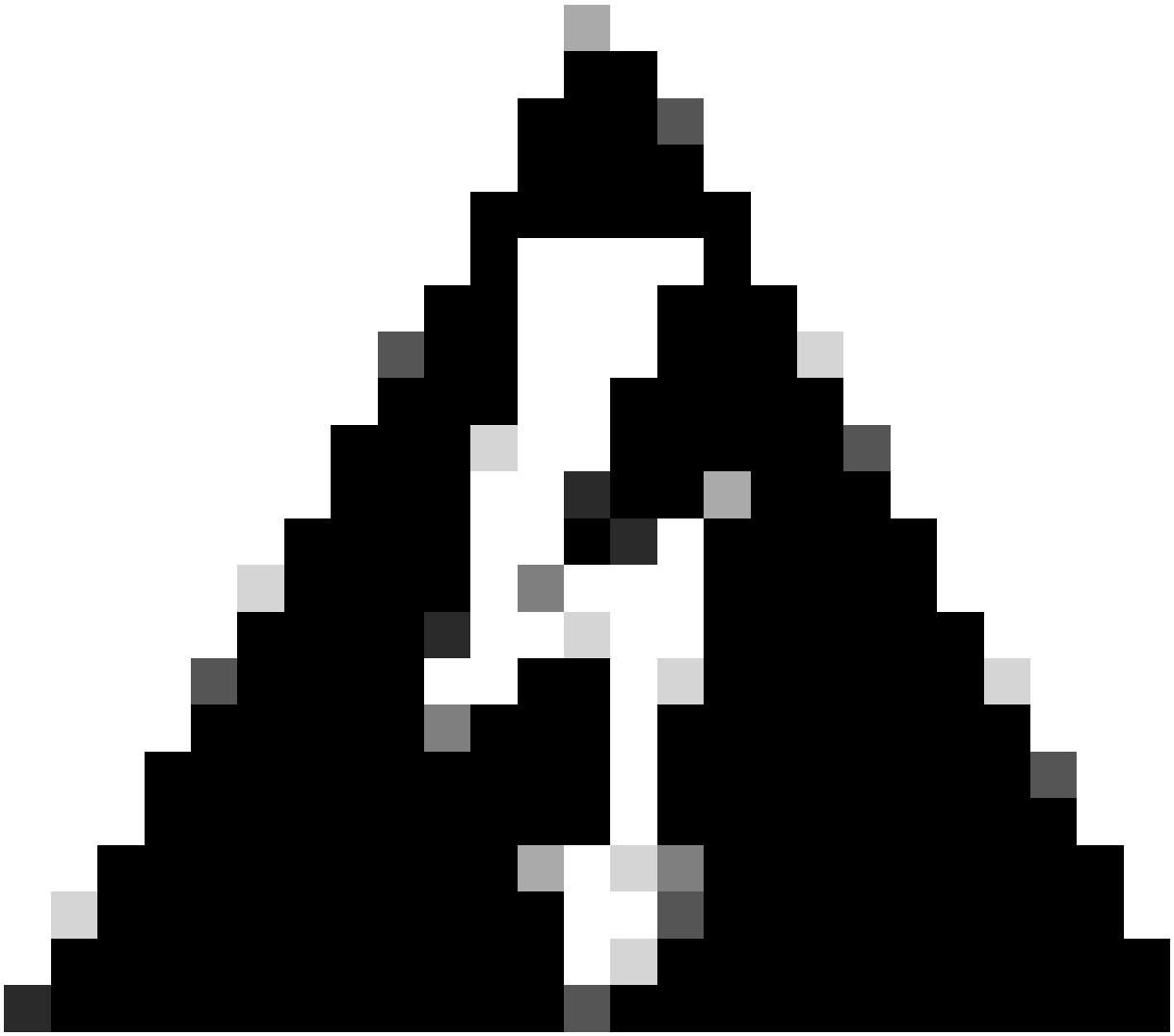
- في هذه الحالة، يمكن أن تتغير المسارات المعينة على الحزمة الأولى.

المتطلبات الأساسية والأنظمة الأساسية المدعومة والتراخيص

الحد الأدنى للبرامج والأجهزة الأساسية

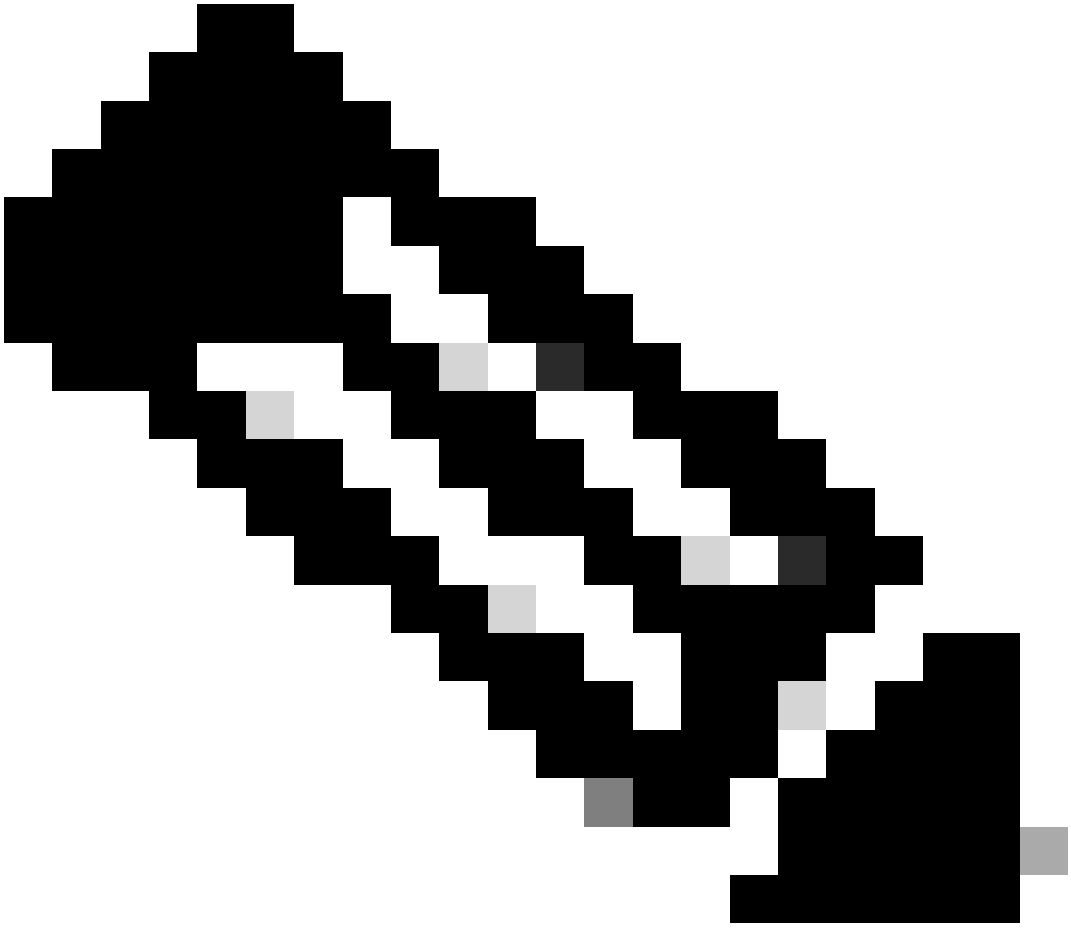
التطبيق والحد الأدنى للإصدار	النظام (الأنظمة) الأساسية المدارة والإصدار المدعوم	المدير (المدارة)	ملاحظات

Secure Firewall، الإصدار 7.4 إستخدام snort3	جميع الأنظمة الأساسية التي تدعم برنامج FTD 7.4	FMC على PREM + FTD	هذه ميزة جانب جهاز، ويجب أن يكون FTD على 7.4



تحذير: لا يدعم Snort 2 واجهة برمجة التطبيقات هذه.

دعم نظام التشغيل Snort 3 و Multi-Instance و HA/Cluster



ةظحالم: يتطلب أن يكون Snort 3 هو محرك الكشف.

نظام Firepower Threat Defense (FTD)	
هل تم دعم عدة مثيلات؟	نعم
مدعومة بأجهزة HA	نعم

هل يتم دعمه بأجهزة مجمعة؟	نعم

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:
· برنامج الدفاع ضد تهديد FirePOWER من Cisco الإصدار 7.4 وأ إصدار أعلى.

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تفاصيل الميزة

وصف الميزة الوظيفية

الإصدار الذي قبل هذا الإصدار

جدار الحماية الآمن الجديد 7.4	في جدار الحماية الآمن 7.3 أو أقل
· يتم تقييم واجهة برمجة تطبيقات كاشف LUA الجديد قبل أي آلية أخرى للكشف عن التطبيقات، · وبالتالي، في 7.4، ندعم الكشف على الحزمة الأولى في جلسة.	· لم يكن اكتشاف التطبيقات لمجموعة IP/Port/Protocol معروفة متاحا إلا خيار إحتياطي بعد استنفاد جميع آليات اكتشاف التطبيقات الأخرى. · بشكل أساسي، لم يتم دعم الكشف على الحزمة الأولى في جلسة عمل.

كيف يعمل

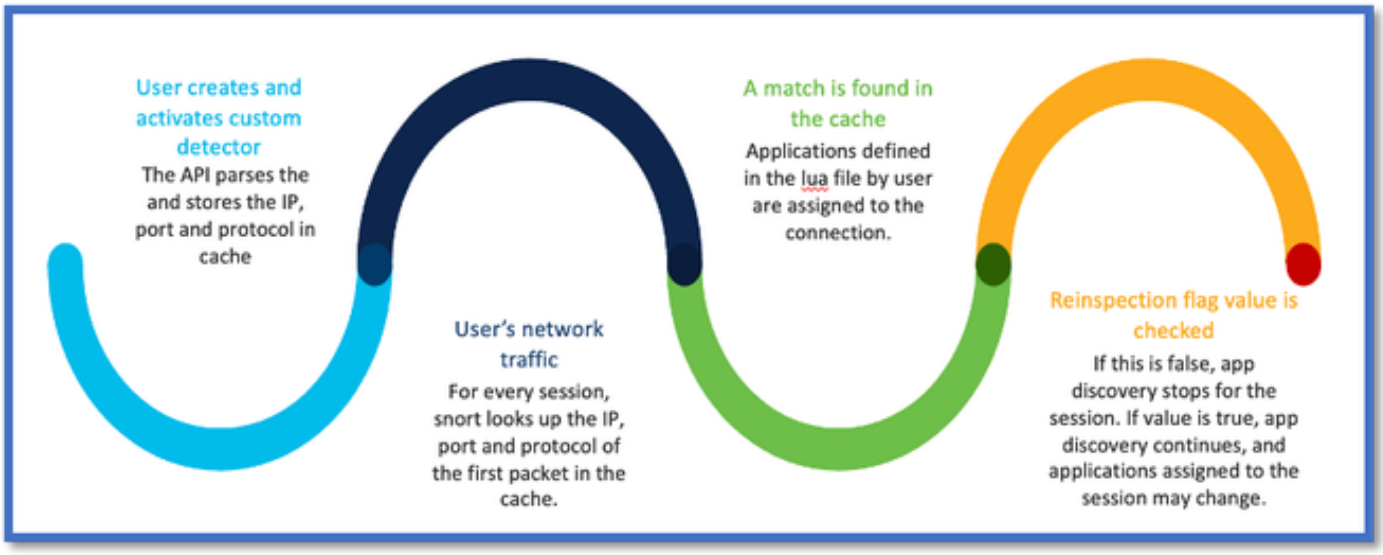
- إنشاء ملف LUA: تأكد من وجود الملف في قالب LUA (بدون أخطاء في بناء الجملة). تحقق أيضا من صحة الوسيطات المعاطاة ل API في الملف.

- قم بإنشاء مكتشف مخصص جديد: قم بإنشاء مكتشف مخصص جديد على FMC وقم بتحميل ملف LUA الخاص بك فيه. قم بتنشيط جهاز الكشف.

- تشغيل حركة المرور: إرسال حركة مرور البيانات التي تطابق مجموعة IP/port/protocol المحددة في مكتشف التطبيقات المخصص إلى الجهاز.

- تحقق من أحداث الاتصال: على FMC، تحقق من أحداث الاتصال التي تمت تصفيتها بواسطة IP والمنفذ. سيتم تحديد التطبيقات المعرفة من قبل المستخدم.

سير عمل واجهة برمجة التطبيقات للكشف المبكر عن الحزم لـ AppID



وصف حقول API من مثال الكشف المخصص

gDetector:addHostFirstPktApp

(gAppIdProto، gAppIdClient، gAppId، 0, "192.0.2.1", 443, DC.ipproto.tcp):

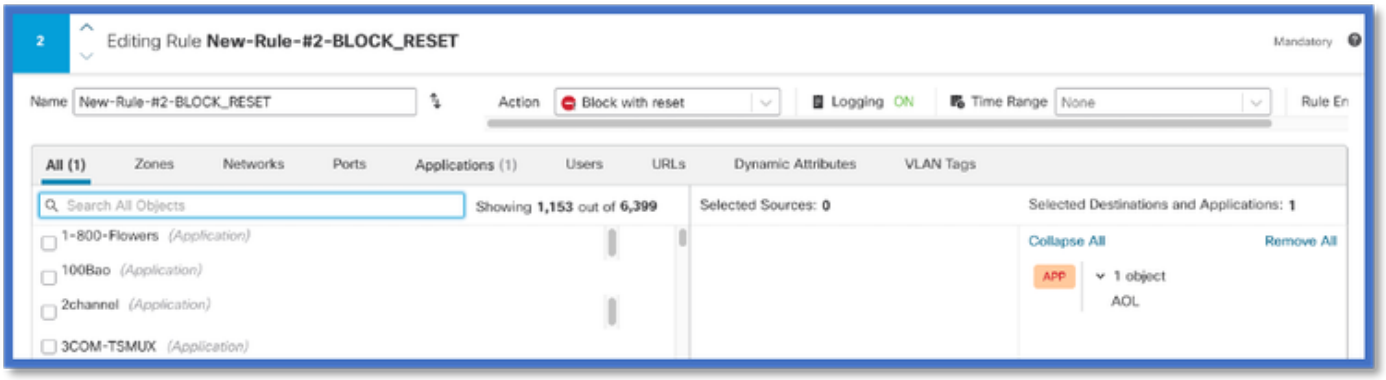
- الوسيطات المبرزة هي القيم المعرفة من قبل المستخدم لعلامة Respect وعنوان IP والمنفذ والبروتوكول.
- يشير 0 إلى حرف بدل.

الوسيطات	الشرح	القيم المتوقعة
علم ريسبيكت	إذا كان المستخدم يفضل فحص حركة المرور بدلا من إتخاذ إجراء جدار الحماية استنادا إلى IP/Port/Protocol، فيمكنه تمكين قيمة علامة REMiewSIGHT إلى 1.	0 = تعطيل إعادة التوجيه أو 1 = تمكين إعادة البث
عنوان IP	عنوان IP الهدف (واحد أو نطاق من عناوين IP في شبكة فرعية) الخاص	192.168.4.198 أو 192.168.4.198/24 أو

	باالخادم. غاية ip من ال 1st ربط في جلسة.	2a03:2880:f103:83:face:b00c:0:25de وأ 2a03:2880:f103:83:face:b00c:0:25de/32
المنفذ	غاية ميناء من ال 1st ربط في جلسة.	من 0 إلى 65535
البروتوكول	بروتوكول الشبكة	TCP/UDP/ICMP

حالة االستخدام: كيفية حظر حركة المرور بشكل أسرع

- عرض النهج: قاعدة الحظر للتطبيق "AOL".



- إختبار حركة المرور باستخدام االرتباط مع: curl https://www.example.com v/s curl https://192.0.2.1/ (أحد عناوين IP الخاصة ب TEST)

<#root>

> curl https://www.example.com/

curl: (35) OpenSSL SSL_connect: SSL_ERROR_SYSCALL in connection to www.example.com:443

```
> curl https://192.0.2.1/
```

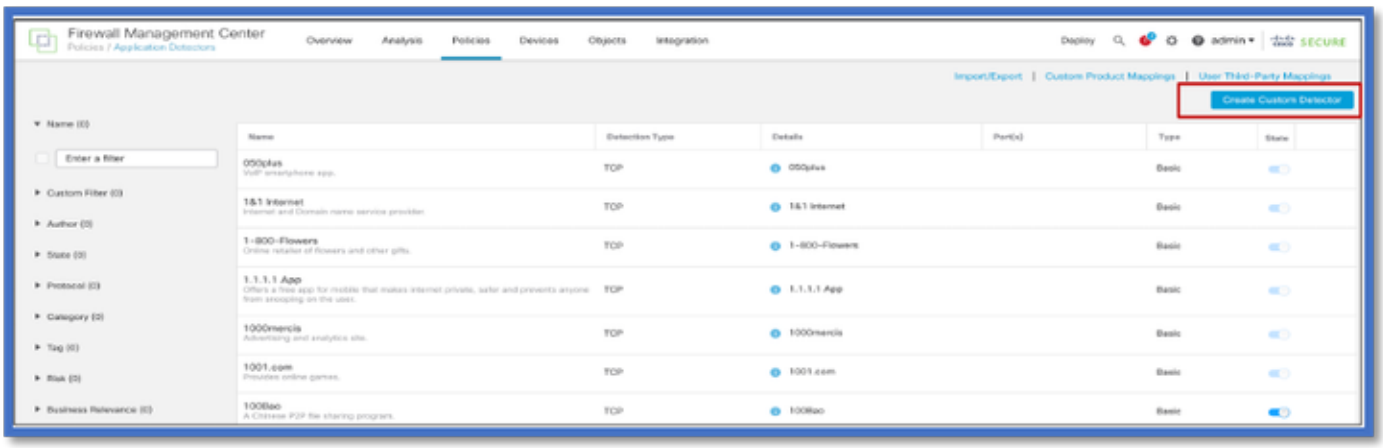
```
curl: (7) Failed to connect to 192.0.2.1 port 443: Connection refused
```

مركز إدارة جدران الحماية Walkthrough

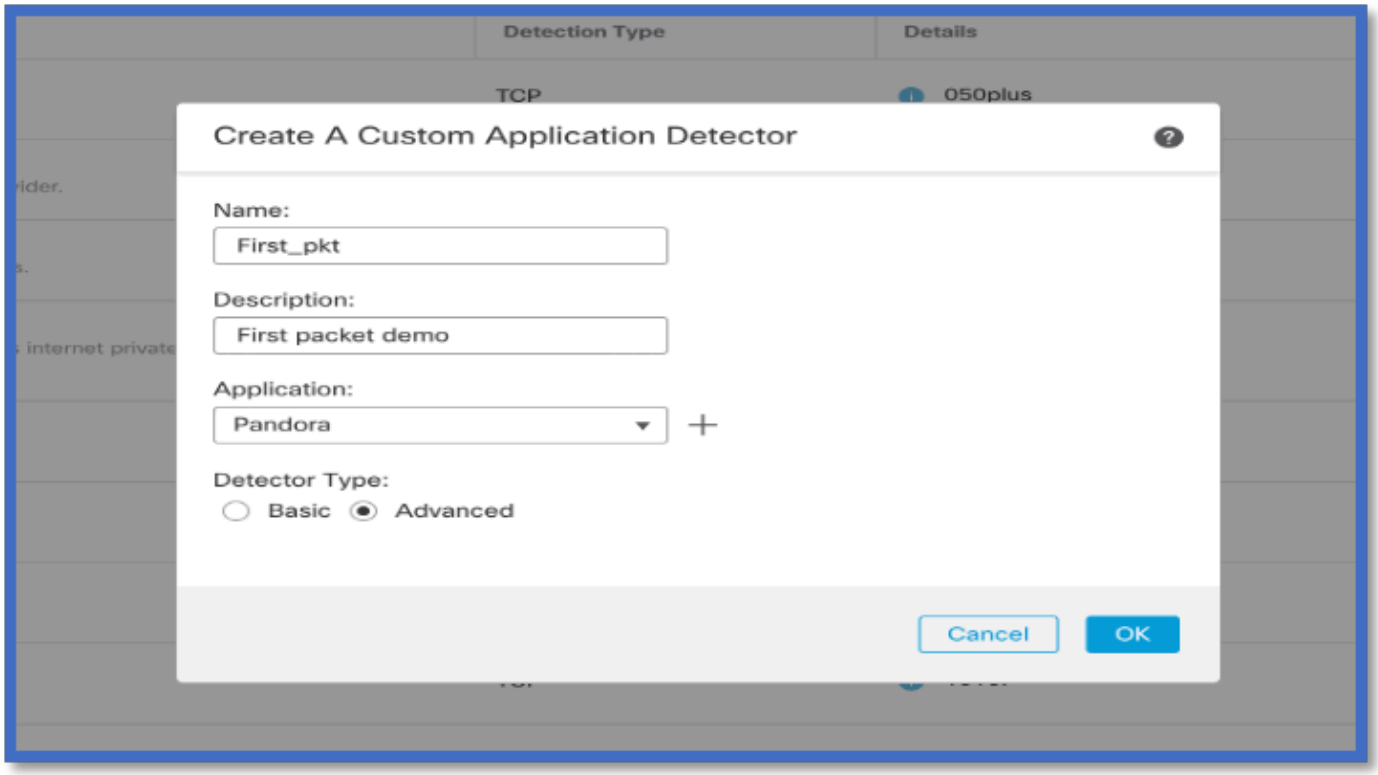
خطوات إنشاء مكتشف مخصص باستخدام واجهة برمجة التطبيقات (API)

قم بإنشاء مكتشف مخصص جديد على FMC من:

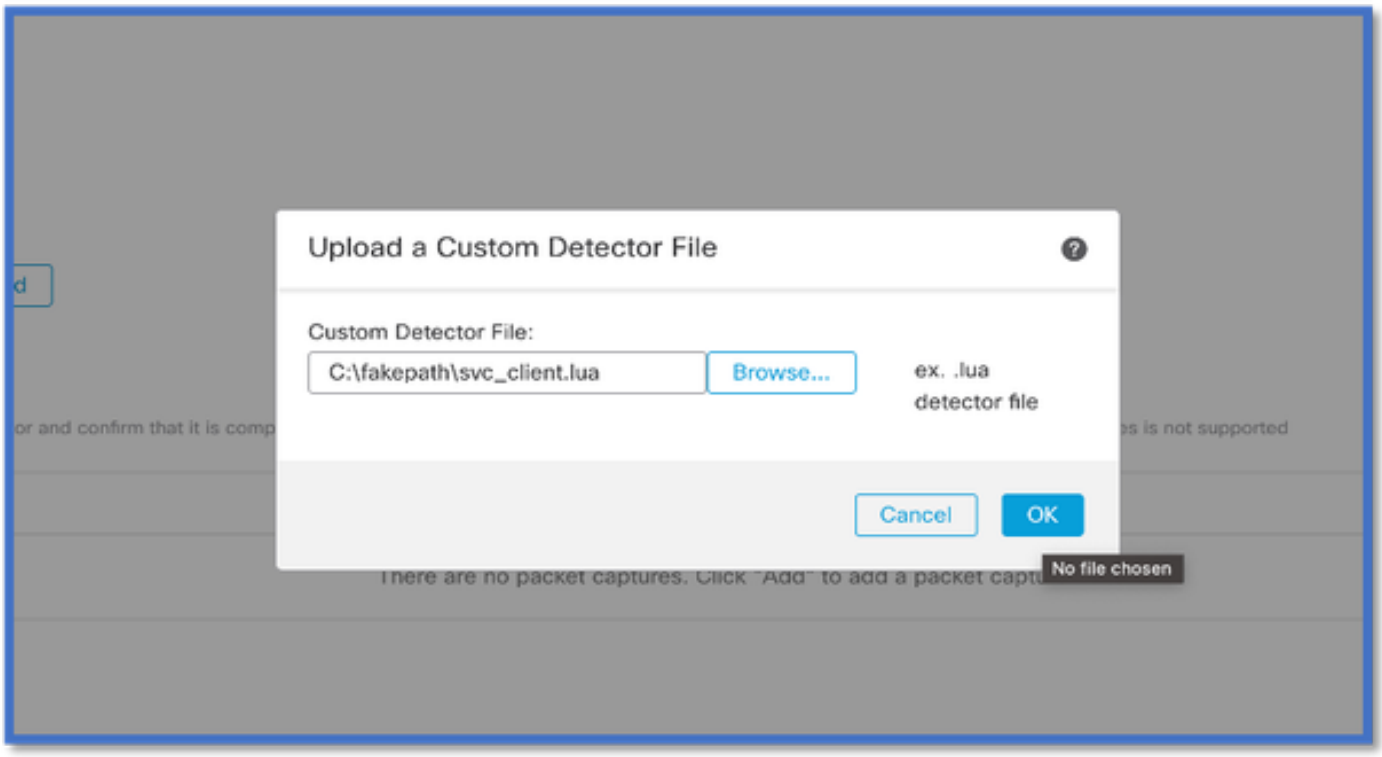
- Policies > Application Detectors > Create Custom Detector .



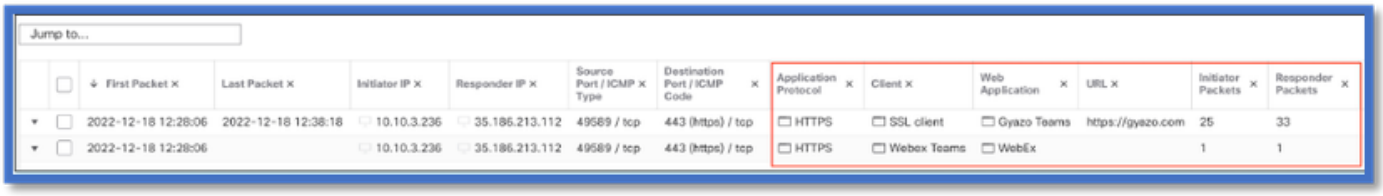
- قم بتحديد الاسم والوصف.
  - أختر التطبيق من القائمة المنسدلة.
  - حدد نوع المكتشف المتقدم.



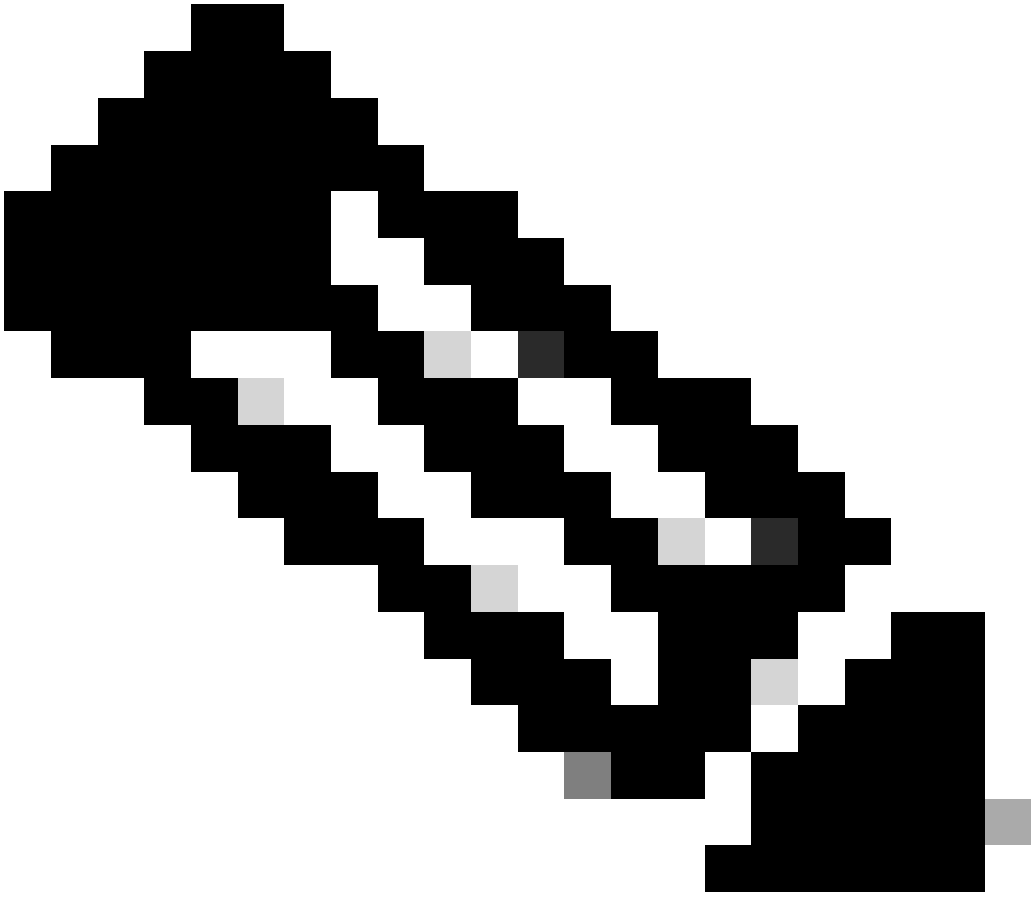
- قم بتحميل ملف LUA تحت معايير الكشف. قم بحفظ جهاز الكشف وتنشيطه.



تم تعطيل RecEnabled v/s



- يظهر الحدثان بداية الاتصال v/s نهاية الاتصال عند تمكين إعادة الفحص.



ملاحظة: أشياء يمكن ملاحظتها:

1. يتم تعريف "فرق HTTPS و Webex و Webex" بواسطة واجهة برمجة التطبيقات (API) في بداية الاتصال. أما أن عملية إعادة الفحص صحيحة، يستمر اكتشاف التطبيقات ويتم تحديث AppIds إلى 'HTTPS وعميل SSL و Gyazo Teams'.

2. لاحظ عدد حزم البادئ والمستجيب. تتطلب أساليب اكتشاف التطبيقات العادية حزم أكثر بكثير من واجهة برمجة التطبيقات.

أستكشاف الأخطاء وإصلاحها/التشخيص

نظرة عامة على التشخيص

- تتم إضافة سجلات جديدة في تصحيح أخطاء تعريف تطبيق معرف النظام للإشارة إلى ما إذا تم العثور على أي تطبيقات بواسطة واجهة برمجة تطبيقات اكتشاف الحزم الأولى.
- تظهر السجلات أيضا إذا اختار المستخدم إعادة فحص حركة المرور.
- يمكن العثور على محتويات ملف مكتشف LUA الذي تم تحميله بواسطة المستخدم على FTD ضمن /var/sf/appid/custom/lua/<UUID> .
- أي أخطاء في ملف LUA يتم إلقاؤها على FTD في ملف /var/log/messages في وقت تنشيط الكاشف.

CLI: معرف النظام تطبيق-identification-debug

<#root>

192.0.2.1 443 -> 192.168.1.16 51251 6 AS=4 ID=0 New AppId session

192.0.2.1 443 -> 192.168.1.16 51251 6 AS=4 ID=0 Host cache match found on first packet, service: HTTPS(1

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 app event with client changed, service changed, payload

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 New firewall session
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 Starting with minimum 2, 'New-Rule-#1-MONITOR', and Src
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 match rule order 2, 'New-Rule-#1-MONITOR', action Audit
```

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 match rule order 3, 'New-Rule-#2-BLOCK_RESET', action Re

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 MidRecovery data sent for rule id: 268437504, rule_acti
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 Generating an SOF event with rule_id = 268437504 ruleAc
```

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 reset action

192.0.2.1 443 > 192.168.1.16 51251 6 AS-4 ID=0 New AppId session
192.0.2.1 443 > 192.168.1.16 51251 6 AS=4 ID=0 Host cache match found on first packet, service:
HTTPS (1122), client: AOL(1419), payload: AOL (1419), reinspect: False
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 app event with client changed, service changed, payload changed, referred no change, miss no change, Mad no change, fas host no change, bits 0x1D 192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 New firewall session
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 Starting with minimum 2, 'New-Rule-#1-MONITOR', and Saclone first with zones 1 →> 1, geo 0(xff0) →> 0, yan 0, sae, sgt; 0, sag sat, type: unknown, det sat: 0, det sat type: unknown, sve 1122, payload 1419, client 1419, mise 0, user 9999997, no Mad or host, no xff
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 match rule order 2, 'New-Rule-#1-MONITOR', action Audit
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 match rule order 3, 'New-Rule-#2-BLOCK_
_RESET', action
Reset
192.168.1.16 51251 > 192.0.2.1 443 6 AS-4 ID=0 MidRecovery, data sent for rule id: 268437504, rule_action:5, rev id:3558448739, Eule_match flag:0x1
192.168.1.16 51251 > 192.0.2.1 443 6 AS-4 ID-0 Generating an SOF event with zuleid - 268437504
ruleAction = 5 ruleReason = 0

موقع محتوى كاشفات AppID Lua

لتأكيد ما إذا كان مكتشف LUA مع واجهة برمجة تطبيقات جديدة موجودة على الجهاز/FTD، يمكنك البحث عن ما إذا كان التطبيق قيد الاستخدام في مجلدين الكتشاف التطبيقات AddHostFirstPktApp API:

1. كاشفات VDB AppID/var/sf/appid/odp/lua

2 - أجهزة الكشف المخصصة -/var/sf/appid/custom/lua

على سبيل المثال:grep addHostFirstPktApp * في كل مجلد.

مشاكل العينة:

- المشكلة: لم يتم تنشيط مكتشف LUA المخصص على FMC.

الموقع المطلوب التحقق منه: /var/sf/appid/custom/lua/

النتيجة المتوقعة: يجب وجود ملف واحد لكل مكتشف تطبيق مخصص منشط على FMC هنا. تحقق من مطابقة المحتويات لملف LUA الذي تم تحميله.

- المشكلة: يحتوي ملف مكتشف LUA الذي تم تحميله على أخطاء.

الملف المطلوب التحقق منه: /var/log/messages on FTD

سجل الأخطاء:

<#root>

Dec 18 14:17:49 intel-x86-64 SF-IMS[15741]:

Error - appid: can not set env of Lua detector /ngfw/var/sf/appid/custom/lua/6698fbd6-7ede-11ed-972c-d12

استكشاف الأخطاء وإصلاحها

المشكلة: التطبيقات التي لم يتم التعرف عليها بشكل صحيح لحركة المرور التي تنتقل إلى عنوان IP والمنفذ

المعرف من قبل المستخدم.

خطوات أستكشاف الأخطاء وإصلاحها:

- تحقق من تحديد مكتشف LUA وتنشيطه بشكل صحيح على FTD.
  - تحقق من محتويات ملف LUA على FTD وتحقق من عدم ظهور أخطاء على التنشيط.
- فحصت الغاية ip، ميناء وبروتوكول من أول رطب في الحركة مرور جلسة.
  - يمكن أن تطابق القيم المعرفة في مكتشف العدسة.
- تحقق من تصحيح أخطاء دعم النظام-application-identification-debug.
  - ابحث عن السطر Host cache match found on first packet. إذا كان هذا السطر مفقودا، فإنه يشير إلى عدم العثور على تطابق بواسطة واجهة برمجة التطبيقات (API).

تفاصيل القيود والمشاكل الشائعة والحلول البديلة

في 7.4، لا توجد واجهة مستخدم لادخال واجهة برمجة التطبيقات. ستتم إضافة دعم واجهة المستخدم في الإصدارات المستقبلية.

محفوظات المراجعة

التعليقات	تاريخ النشر	مراجعة
الإصدار الأولي	18 يوليو-2024	1.0

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).