تكوين PBR المستند إلى تطبيق FTD ل Umbrella SIG

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

نظرة عامة

الرسم

PBR المستند إلى التطبيق

التحقق

المقدمة

يوضح هذا المستند كيفية تكوين التوجيه المستند إلى السياسة (PBR) الخاص بتحديد جدار الحماية (FTD) ل Umbrella SIG.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الوصول إلى لوحة معلومات المظلة
- وصول المسؤول إلى FMC الذي يشغل الإصدار 7.1.0+ لنشر التكوين إلى الإصدار 7.1.0+ من FTD. يتم دعم PBR المستند إلى التطبيقات فقط على الإصدار 7.1.0 والإصدارات الأعلى
- (مفضل) معرفة بتكوين FMC/FTD و Umbrella SIG
- (إختياري ولكن موصى به بشدة): يتم تثبيت "شهادة جذر المظلة"، ويتم إستخدام هذه الشهادة من قبل SIG عندما تكون حركة المرور بروكسال أو محظورة. لمزيد من التفاصيل حول تثبيت الشهادة الجذر، أقرأ المزيد في وثائق Umbrella.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى عبارة الإنترنت الآمنة (SIG) من Cisco Umbrella.

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

نظرة عامة

تهدف المعلومات الواردة في هذا المستند إلى تغطية خطوات التكوين الخاصة بكيفية نشر PBR المستندة إلى التطبيق على FTD عند إنشاء نفق SIG IPsec VTI إلى Umbrella، حتى يمكنك إستباعاد حركة مرور البيانات على VPN استنادا إلى التطبيقات التي تستخدم PBR أو تضمينها.

يركز مثال التكوين الموضح في هذه المقالة على كيفية إستباعاد تطبيقات معينة من الشبكة الخاصة الظاهرية (VPN) ل IPsec أثناء إرسال كل شيء آخر عبر الشبكة الخاصة الظاهرية (VPN).

يمكن العثور على المعلومات الكاملة حول PBR على FMC في وثائق Cisco.

القيود

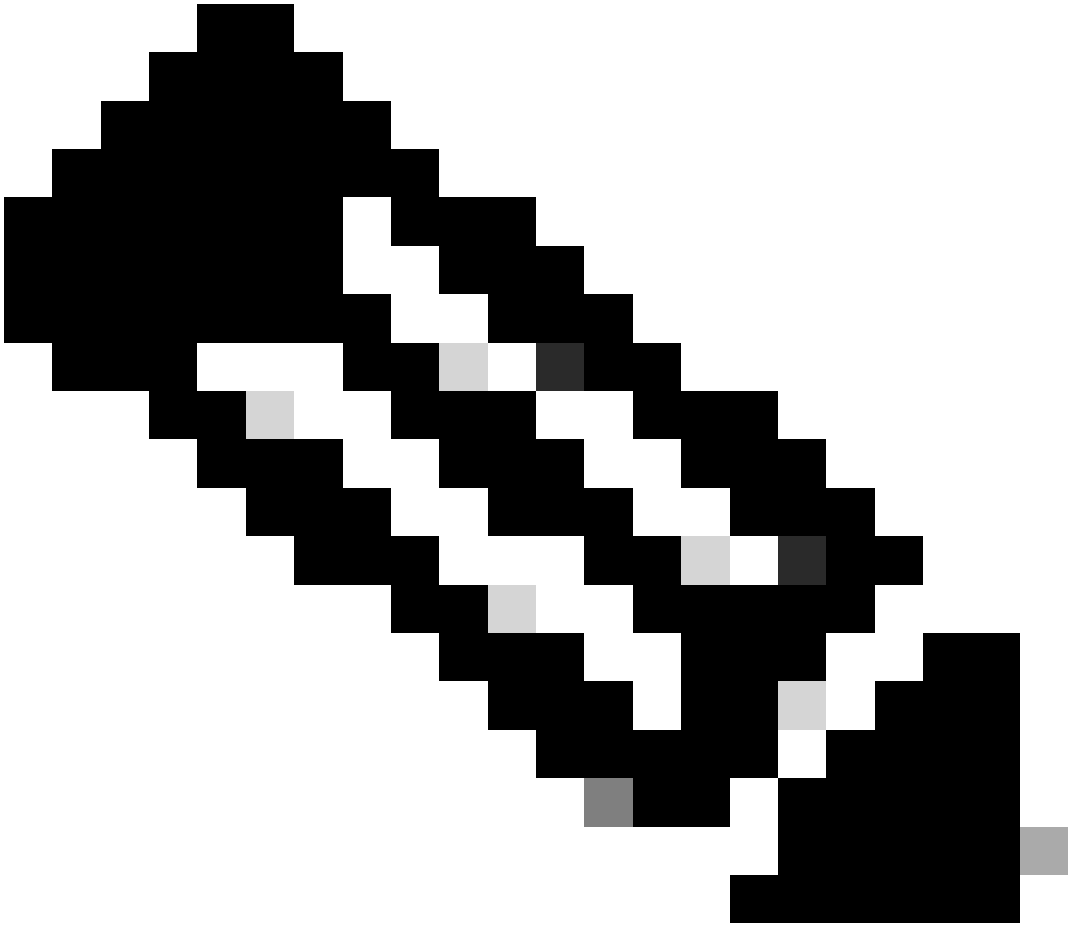
- لا يمكن تعريف كل من التطبيق وعنوان الوجهة في ACE.
- أثناء تحديد قائمة التحكم في الوصول (ACL) لمعايير مطابقة السياسة، يمكنك تحديد تطبيقات متعددة من قائمة التطبيقات المحددة مسبقا لتكوين إدخال التحكم في الوصول (ACE).
  حاليا، لا يمكنك الإضافة إلى قائمة التطبيقات المحددة مسبقا أو تعديلها.
- بالنسبة لتلك التطبيقات غير المدرجة في قائمة التطبيقات المحددة مسبقا على وحدة التحكم في إدارة للوحة الأساسية (FMC) أو أي سلوك غير متوقع مع تطبيق، يمكن إستخدام بروتوكولات الإنترنت (IPs) بدلا من التطبيقات الموجودة في وحدة التحكم في اللوحة الأساسية (PBR).
- للحصول على قائمة بالقيود الكاملة، يرجى الرجوع إلى وثائق PBR.

PBR المستند إلى التطبيق

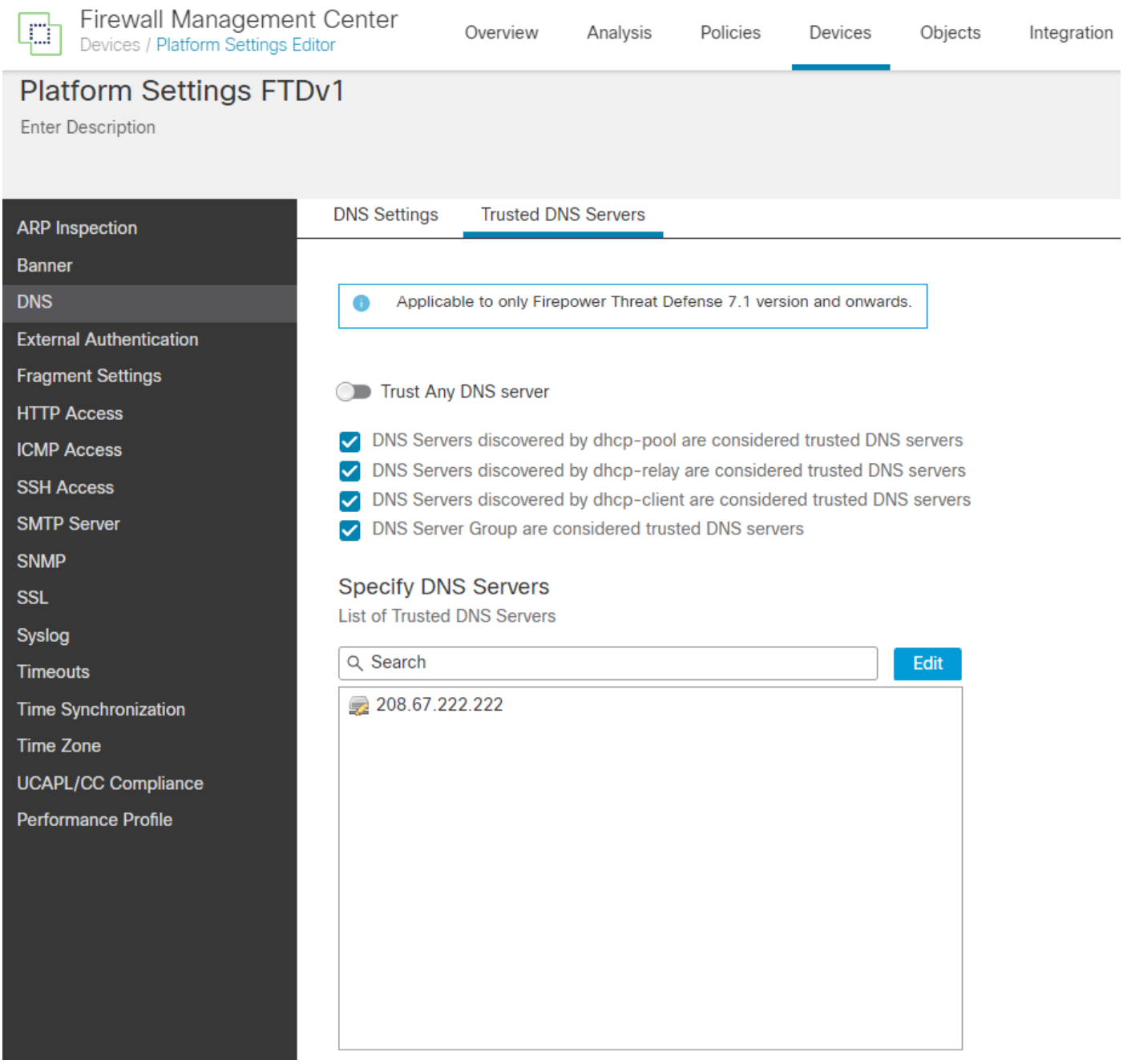
1. ابدأ بتكوين نفق IPsec على FMC وكذلك على لوحة معلومات Umbrella. يمكن العثور على إرشادات كيفية تنفيذ هذا التكوين في وثائق Umbrella.

2. تأكد من إدراج خادم DNS الذي يستخدمه جهاز المستخدم النهائي خلف FTD كخادم DNS موثوق به ضمن الأجهزة > إعدادات النظام الأساسي > DNS > خوادم DNS الموثوق بها.

إذا كانت الأجهزة تستخدم خادم DNS غير مدرج، يمكن أن يفشل التطفل على DNS، وبالتالي لا يمكن أن يعمل PBR المستند إلى التطبيقات. إختياريا (ولكن غير مستحسن لأسباب أمنية)، يمكنك التبديل بين الثقة في أي خادم DNS بحيث تكون إضافة خادم (خوادم) DNS مطلوبة.



ملاحظة: إذا تم إستخدام VAs كمحولات DNS داخلية، فيجب إضافتها كخوادم DNS موثوقة.



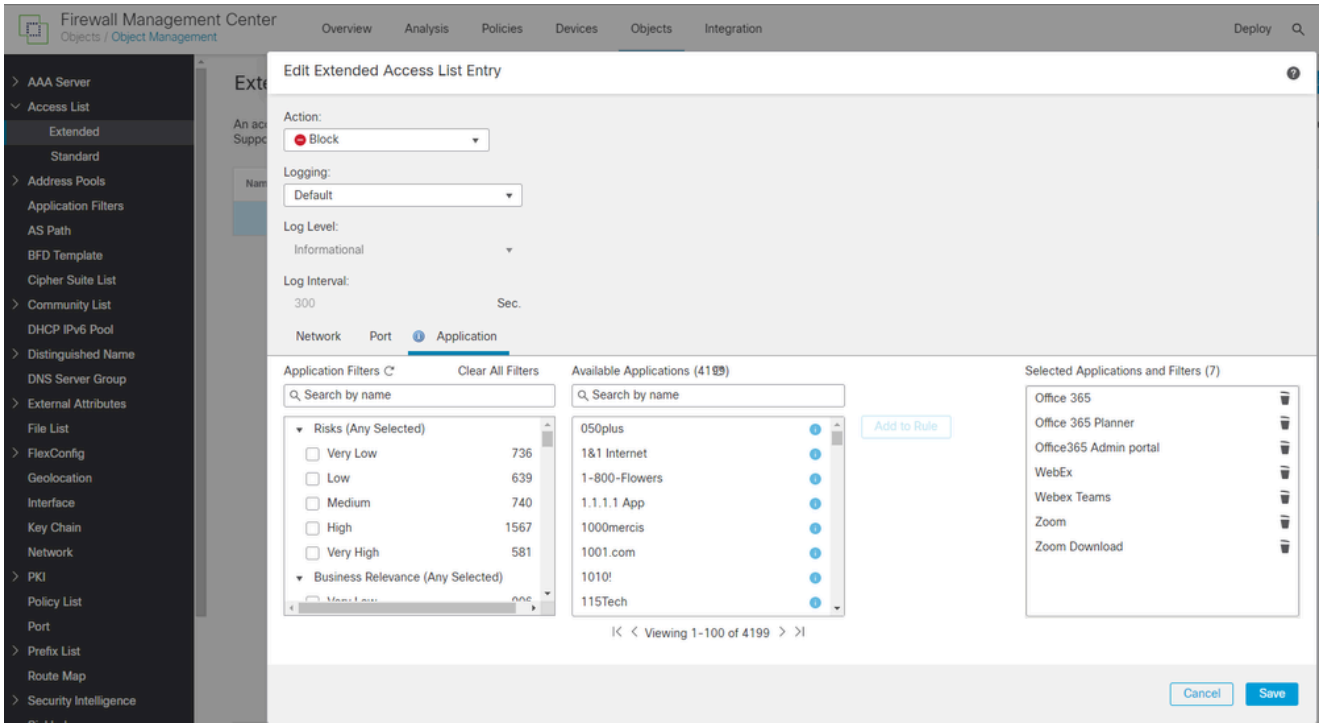
15669097907860

3. قم بإنشاء قائمة تحكم في الوصول (ACL) موسعة يمكن إستخدامها من قبل FTD لعملية PBR لتحديد ما إذا كانت حركة المرور يتم إرسالها إلى Umbrella لـ SIG أو إذا كان مستبعدا من IPsec والتي يتم إرسالها إلى Umbrella على الإطلاق.

- يعني رفض ACE على قائمة التحكم في الوصول إستبعاد حركة المرور من SIG.
- يعني إدخال التحكم في الوصول (ACE) المسموح به على قائمة التحكم في الوصول (ACE) يمكن تطبيق سياسة SIG (CDFW، SWG، وما إلى ذلك) إرسال حركة المرور عبر IPsec.

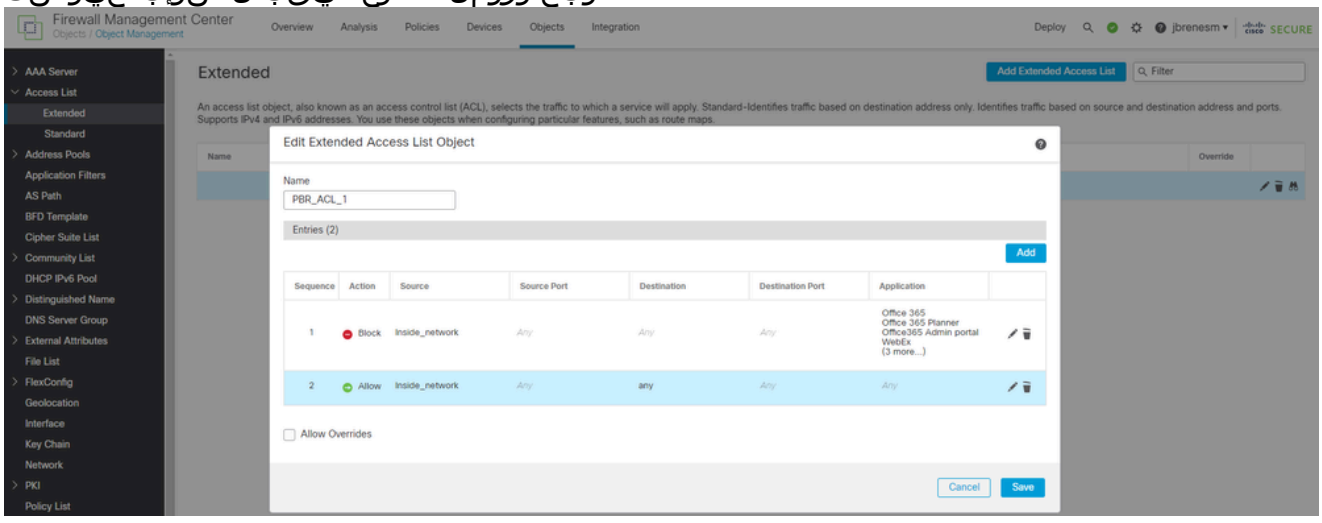
يستبعد هذا المثال التطبيقات "Office365" و"Zoom" و"Cisco Webex" التي تحتوي على رفض ACE. يتم إرسال باقي حركة المرور إلى Umbrella لمزيد من الفحص.

1. انتقل إلى الكائن > إدارة الكائن > قائمة الوصول > موسع.
2. قم بتحديد الشبكة المصدر والمنافذ كما تفعل عادة، ثم قم بإضافة التطبيقات للمشاركة على PBR.



15669947000852

يمكن ل ACE الأول "رفض" هذه التطبيقات المذكورة سابقا، بينما يمثل ACE الثاني تصريحا بإرسال بقية حركة المرور عبر IPsec.

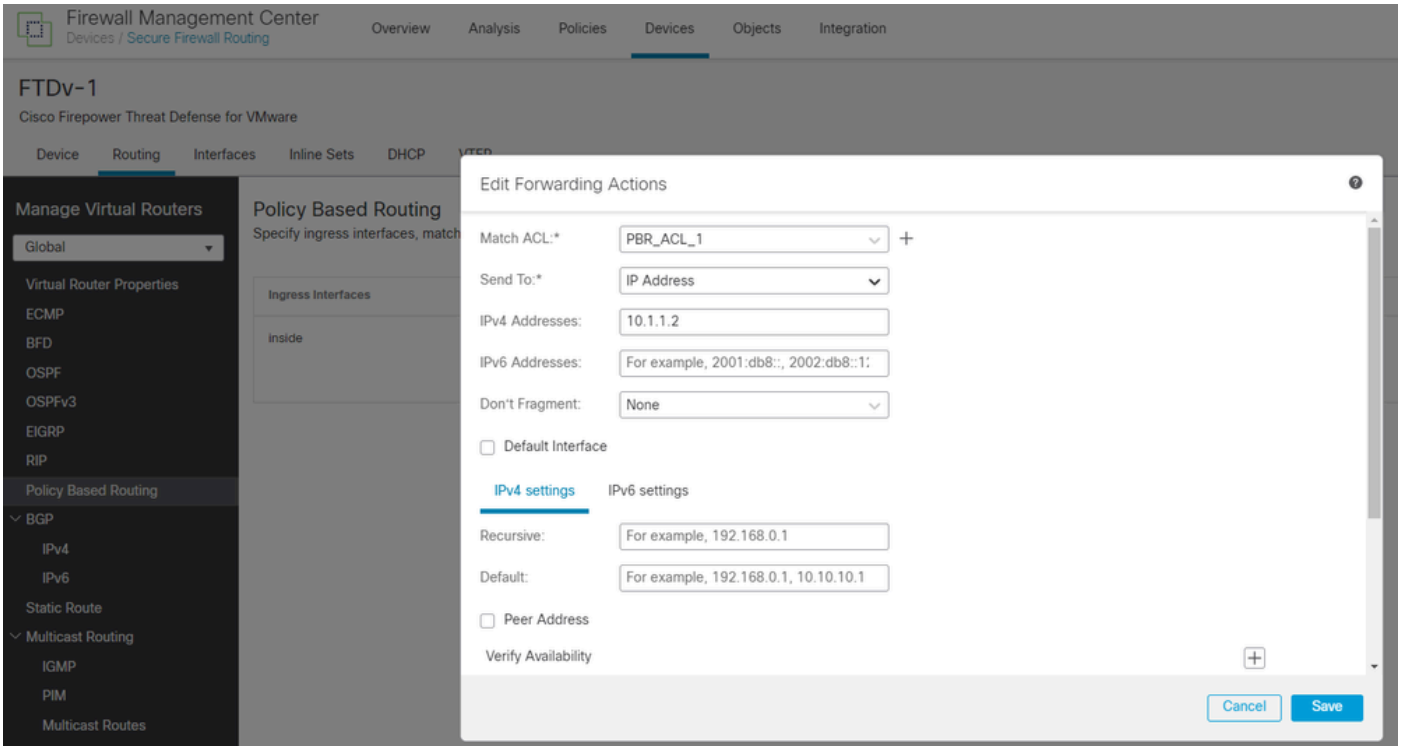


15670006987156

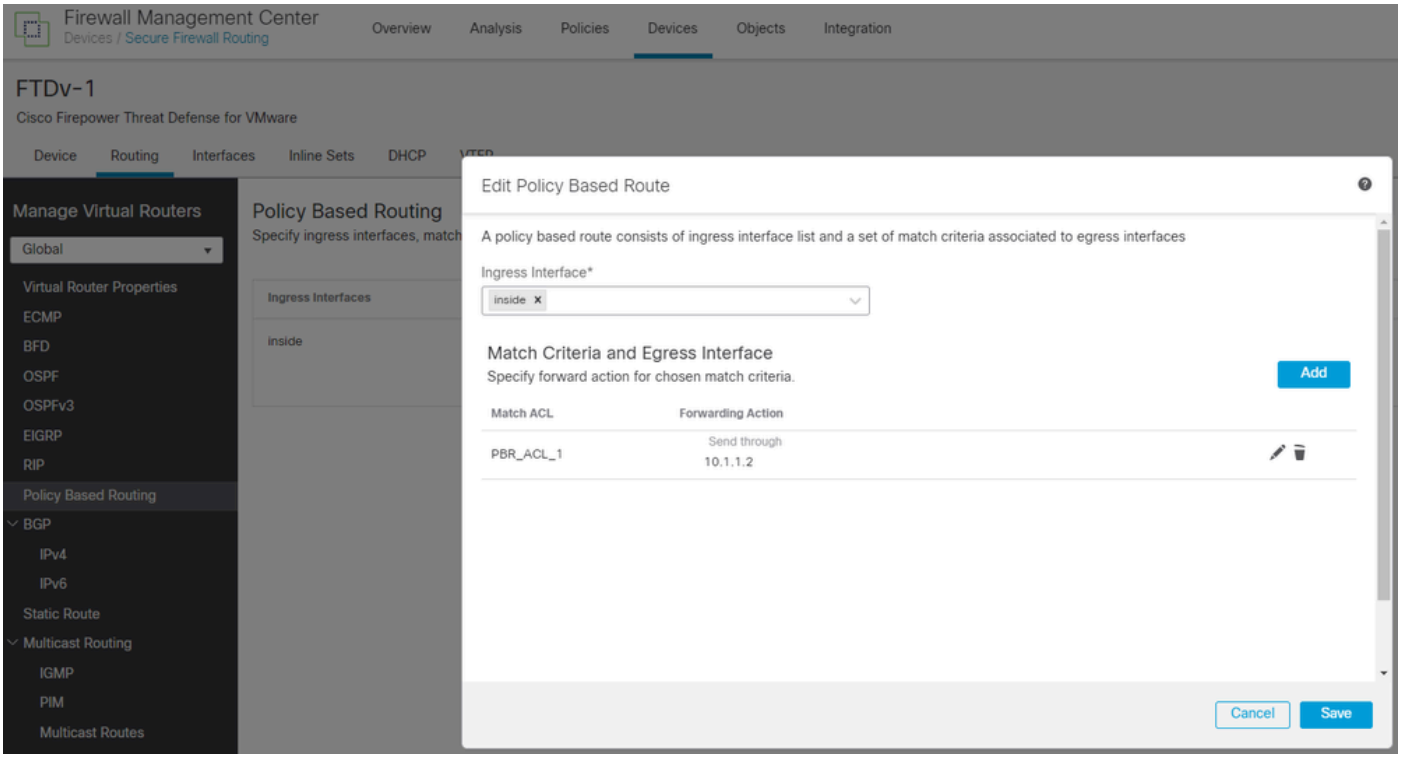
4. قم بإنشاء PBR تحت الأجهزة > إدارة الأجهزة > [حدد جهاز FTD] > التوجيه > التوجيه المستند إلى السياسة.

- واجهة الدخول: الواجهة التي تأتي منها حركة المرور المحلية.
- قائمة التحكم في الوصول (ACL) المطابقة: قائمة التحكم في الوصول (ACL) الموسعة التي تم إنشاؤها على الخطوة السابقة، قائمة التحكم في الوصول (ACL) "PBR_ACL_1".
- إرسال إلى: عنوان IP
- عنواني IPv4: الخطوة التالية عندما يجد PBR عبارة سماح، لذلك يتم توجيه حركة المرور

إلى IP الذي تضيفه هنا. في هذا المثال، هذا هو عنوان IPsec الخاص ب Umbrella. إذا كان عنوان IP الخاص بشبكة VPN الخاصة بك هو 10.1.1.1، فسيكون عنوان IPsec الخاص بالمظلة هو أي شيء داخل الشبكة نفسها (10.1.1.2 على سبيل المثال).



15670209158036



15670247521556

5. نشر التغييرات على FMC.

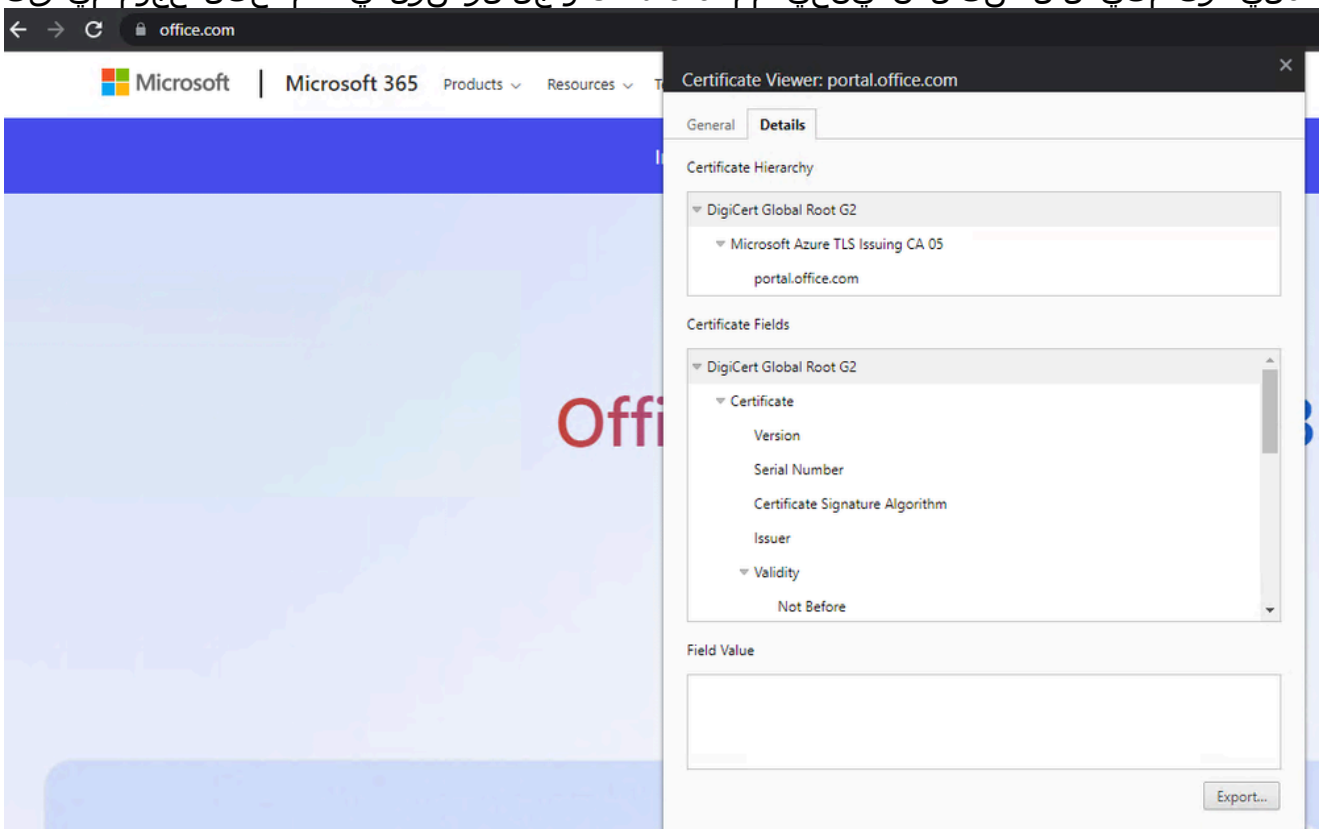
التحقق

في جهاز الكمبيوتر الذي تم إختباره والموجود خلف برنامج الإرسال فائق السرعة (FTD)، تحقق من:

- يتم بالفعل إرسال حركة مرور البيانات من الكمبيوتر عبر IPsec إلى Umbrella. انتقل إلى: https://policy-debug.checkumbrella.com/

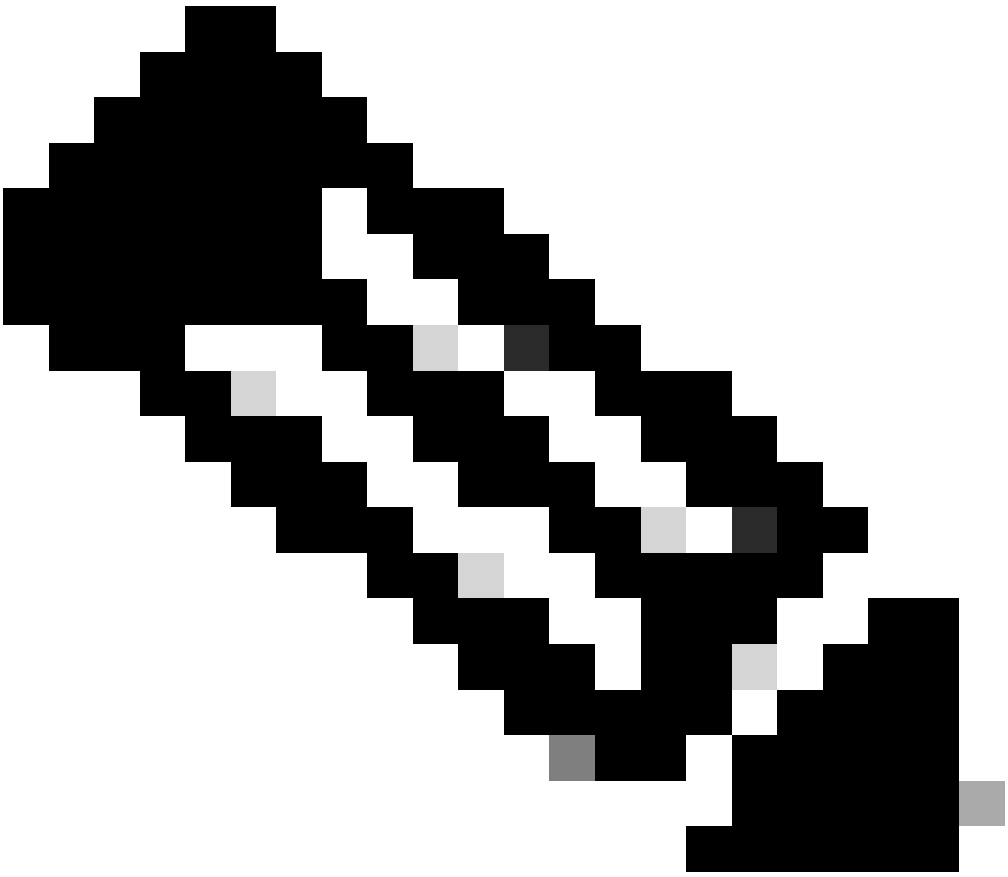
15670737148948

- حاول الانتقال إلى أي من المواقع المستبعدة على تكوين PBR/ACL وتأكد من عدم تقديم مرجع التحكم في الوصول لجذر Umbrella، مما يعني أن الاتصال لا يتم توكيله:

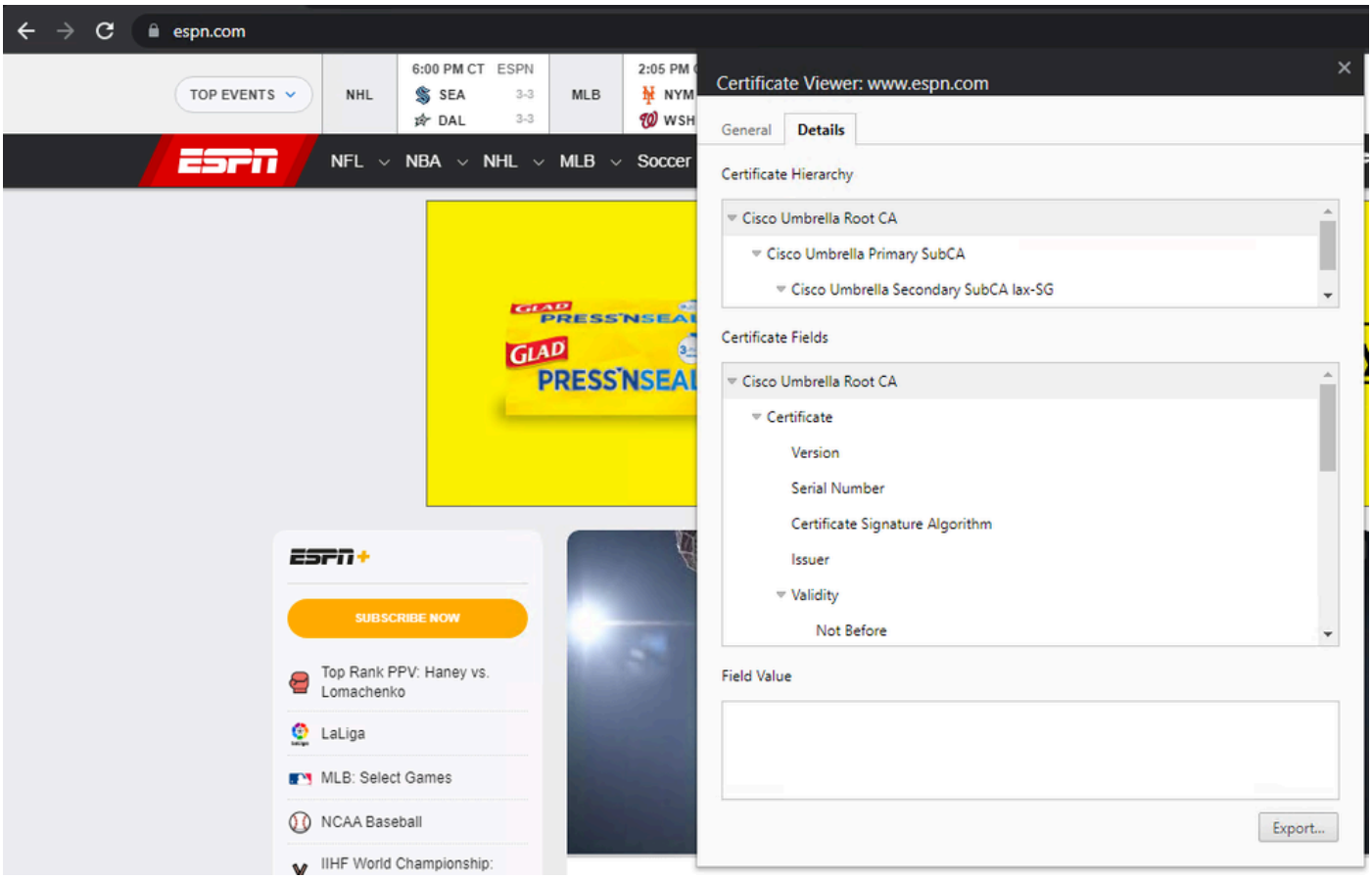


15670820980756

- حاول الانتقال إلى أي موقع آخر لا يعتمد على التطبيقات المستبعدة من PBR وتأكد من أن Umbrella تقوم بالفعل بتوكيل الاتصال:



ملاحظة: لتجنب حدوث مشاكل في صفحة تخيري غير موثوق بها، تأكد من تثبيت شهادة مرجع مصدق جذر Umbrella.



- على واجهة سطر أوامر (CLI) واجهة سطر الأوامر (CLI) الخاصة ب FTD، يمكنك تشغيل بعض الأوامر لتأكيد دفع التكوين والعمل بشكل صحيح:
  - `show run route-map` (يتحقق من تكوين PBR):

```
ftd# sh run route-map
!
route-map FMC_GENERATED_PBR_1682004086289 permit 5
 match ip address PBR_ACL_1
 set ip next-hop 10.1.1.2

!
ftd#
```

15670322054036

  - `show run interface gigabitEthernet 0/1` (يتحقق من تطبيق PBR على الواجهة المناسبة)

```
ftd# sh run interface gigabitEthernet 0/1
!
interface GigabitEthernet0/1
 nameif inside
 security-level 0
 ip address 172.16.72.1 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1682004086289
ftd#
```

15678344219540

- show run access-list pbr_acl_1، show object-group id FMC_NSG_179869596 (يؤكد المجالات التي تمت إضافتها إلى قائمة التحكم في الوصول للاستباعاد)

```
ftd# sh run access-list PBR_ACL_1
access-list PBR_ACL_1 extended deny ip object Inside_network object-group-network-service FMC_NSG_17179869596
access-list PBR_ACL_1 extended permit ip object Inside_network any
ftd# sh object-group id FMC_NSG_17179869596
object-group network-service FMC_NSG_17179869596 (id=f1000001)
 network-service-member "Office 365" dynamic
  description Traffic generated by MS Office 365 applications and web services.
  app-id 2812
  domain nexus.officeapps.live.com (bid=-1815422039) ip (hitcnt=0)
  domain officehome.msocdn.com (bid=-1815266895) ip (hitcnt=0)
  domain scuofficehome.msocdn.com (bid=-1815215737) ip (hitcnt=0)
  domain eusofficehome.msocdn.com (bid=-1814954697) ip (hitcnt=0)
  domain seaofficehome.msocdn.com (bid=-1814948459) ip (hitcnt=0)
  domain msauth.net (bid=-1814770899) ip (hitcnt=0)
  domain msauthimages.net (bid=-1814643885) ip (hitcnt=0)
  domain msftauth.net (bid=-1814478573) ip (hitcnt=0)
  domain msftauthimages.net (bid=-1814363583) ip (hitcnt=0)
  domain officecdn.microsoft.com.edgesuite.net (bid=-1814169495) ip (hitcnt=0)
  domain staffhub.ms (bid=-1814084129) ip (hitcnt=0)
  domain mem.gfx.ms (bid=-1813977425) ip (hitcnt=0)
  domain assets.onestore.ms (bid=-1813901907) ip (hitcnt=0)
  domain o365weve.com (bid=-1813725851) ip (hitcnt=0)
  domain msappproxy.net (bid=-1813517013) ip (hitcnt=0)
  domain officeppe.com (bid=-1813427701) ip (hitcnt=0)
  domain Portal.Office.com (bid=-1813355559) ip (hitcnt=0)
  domain Home.Office.com (bid=-1813195231) ip (hitcnt=0)
  domain office365.com (bid=-1813005001) ip (hitcnt=0)
  domain office.com (bid=-1812953305) ip (hitcnt=0)
  domain office.net (bid=-1812729659) ip (hitcnt=0)
  domain microsoftonline.com (bid=-1812611427) ip (hitcnt=0)
  domain onmicrosoft.com (bid=-1812561405) ip (hitcnt=0)
  domain glbdns.microsoft.com (bid=-1812432381) ip (hitcnt=0)
  domain login.windows.net (bid=-1812242319) ip (hitcnt=0)
  domain login.microsoftonline.com (bid=-1812155687) ip (hitcnt=0)
  domain office365servicehealthcommunications.cloudapp.net (bid=-1812019313) ip (hitcnt=0)
  domain prod.msocdn.com (bid=-1811890529) ip (hitcnt=0)
  domain office.microsoft.com (bid=-1811800355) ip (hitcnt=0)
```

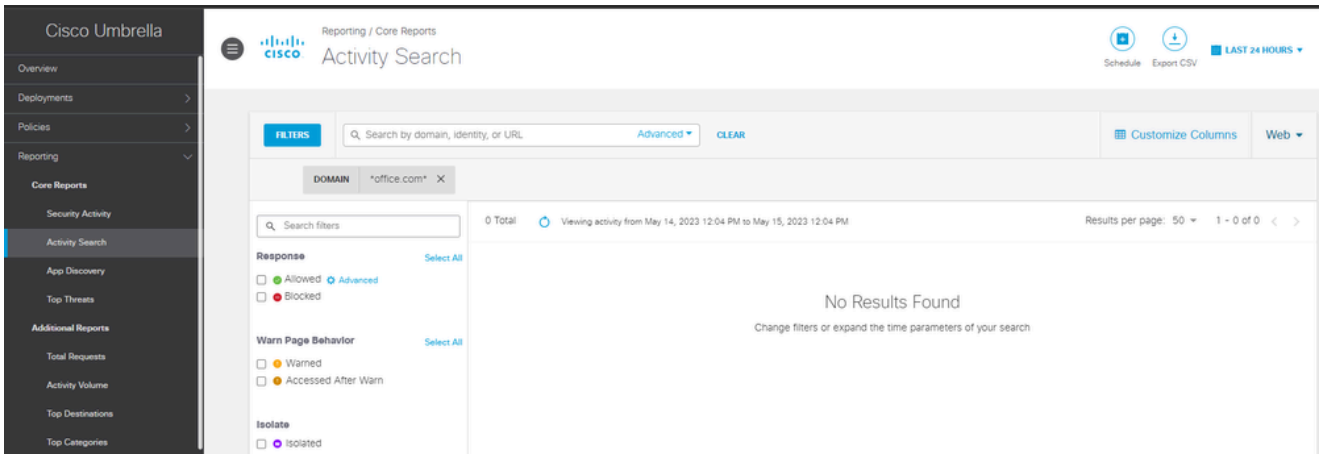
15670420887316

```
ftd# sh object-group id FMC_NSG_17179869596 | i office.com
  domain office.com (bid=-1812953305) ip (hitcnt=8)
  domain tasks.office.com (bid=-1674300035) ip (hitcnt=0)
  domain controls.office.com (bid=-1674092701) ip (hitcnt=0)
  domain clientlog.portal.office.com (bid=-1673794351) ip (hitcnt=0)
  domain portal.office.com (bid=88903411) ip (hitcnt=0)
ftd#
```

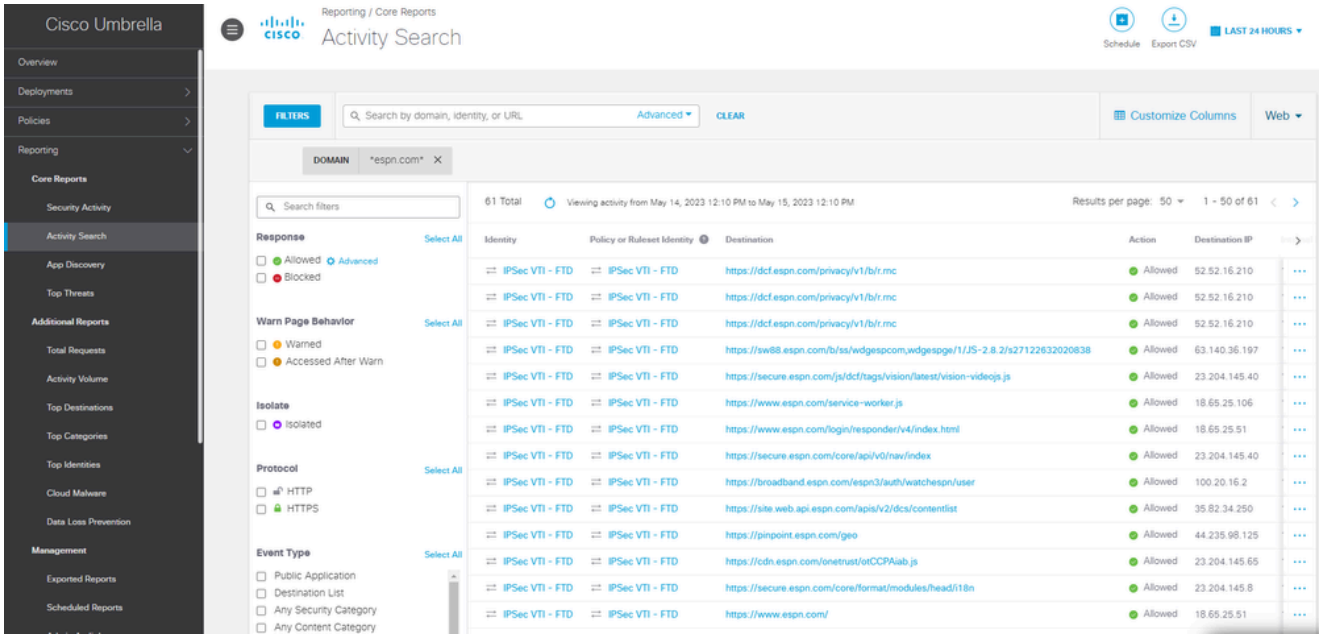
15670635784852

- مدخل Packet-tracer داخل TCP 172.16.72.10 1234 fqdn office.com 443 مفصل (يتحقق من إستخدام الواجهة الخارجية كإخراج وليس VTI واحد)

- في لوحة معلومات Umbrella، تحت البحث عن الأنشطة، يمكنك أن ترى أن حركة مرور الويب التي تنتقل إلى office.com لم يتم إرسالها إلى Umbrella مطلقا، بينما تم إرسال حركة المرور التي تنتقل إلى espn.com.



15671098042516



15671302832788

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).