Configurer le PBR basé sur l'application FTD pour Umbrella SIG

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Aperçu](#)

- [Limites](#)

[PBR basé sur les applications](#)

[Vérification](#)

Introduction

Ce document décrit comment configurer le routage basé sur les politiques d'application (PBR) Firewall Threat Defense (FTD) pour Umbrella SIG.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au tableau de bord Umbrella
- Accès administrateur au FMC exécutant 7.1.0+ pour déployer la configuration sur la version FTD 7.1.0+. PBR basé sur des applications est pris en charge uniquement sur la version 7.1.0 et ultérieure
- (Préféré) Connaissances sur la configuration FMC/FTD et Umbrella SIG
- (Facultatif mais fortement recommandé) : Certificat racine de parapluie installé, utilisé par SIG lorsque le trafic est mis en proxy ou bloqué. Pour plus de détails sur l'installation du certificat racine, lisez la documentation Umbrella.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella Secure Internet Gateway (SIG).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Les informations de ce document sont destinées à couvrir les étapes de configuration sur la façon de déployer le PBR basé sur les applications sur le FTD lors de l'établissement d'un tunnel VTI IPSec SIG vers Umbrella, afin que vous puissiez exclure ou inclure le trafic sur un VPN basé sur les applications utilisant le PBR.

L'exemple de configuration décrit dans cet article se concentre sur la façon d'exclure certaines applications du VPN IPsec tout en envoyant tout le reste sur le VPN.

Vous trouverez des informations complètes sur PBR sur FMC dans la documentation Cisco.

Limites

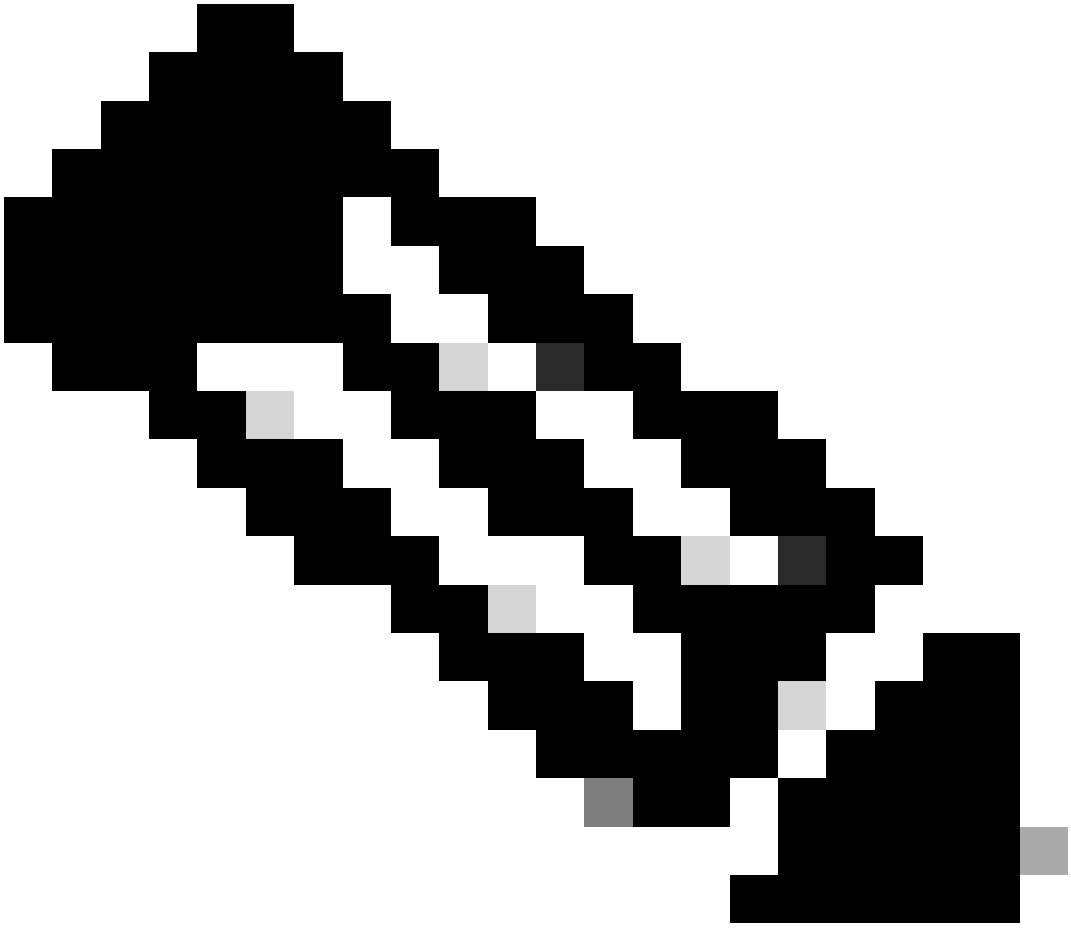
- Vous ne pouvez pas avoir d'adresse d'application et de destination définie dans une ACE.
- Lors de la définition de la liste de contrôle d'accès pour les critères de correspondance de stratégie, vous pouvez sélectionner plusieurs applications dans une liste d'applications prédéfinies pour former une entrée de contrôle d'accès (ACE).
  Actuellement, vous ne pouvez pas ajouter ou modifier la liste des applications prédéfinies.
- Pour les applications non répertoriées dans la liste des applications prédéfinies sur le FMC ou tout comportement inattendu avec une application, les adresses IP peuvent être utilisées à la place des applications dans le PBR.
- Pour une liste complète des limitations, veuillez vous reporter à la documentation du PBR.

PBR basé sur les applications

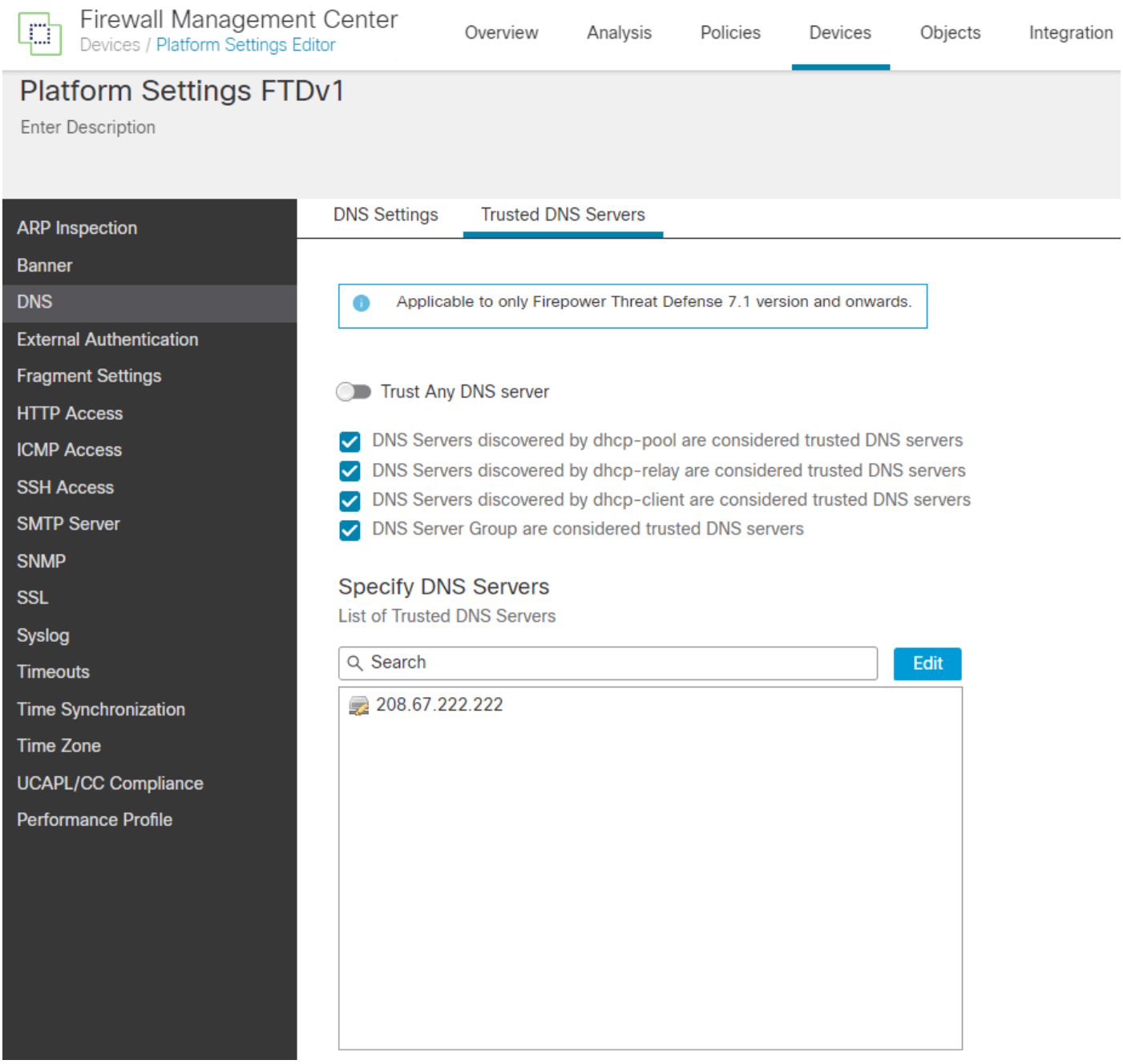
1. Commencez par configurer le tunnel IPsec sur le FMC ainsi que sur le tableau de bord Umbrella. Les instructions sur la façon d'effectuer cette configuration se trouvent dans la documentation d'Umbrella.

2. Assurez-vous que le serveur DNS utilisé par le périphérique de l'utilisateur final derrière le FTD est répertorié comme serveur DNS approuvé sous Périphériques > Paramètres de la plate-forme > DNS > Serveurs DNS approuvés.

Si les périphériques utilisent un serveur DNS qui n'est pas répertorié, la surveillance DNS peut échouer, et par conséquent le PBR basé sur les applications ne peut pas fonctionner. En option (mais non recommandé pour des raisons de sécurité), vous pouvez activer l'option Trust Any DNS server afin d'ajouter le ou les serveurs DNS.



Remarque : Si des VA sont utilisés comme résolveurs DNS internes, ils doivent être ajoutés en tant que serveurs DNS approuvés.



15669097907860

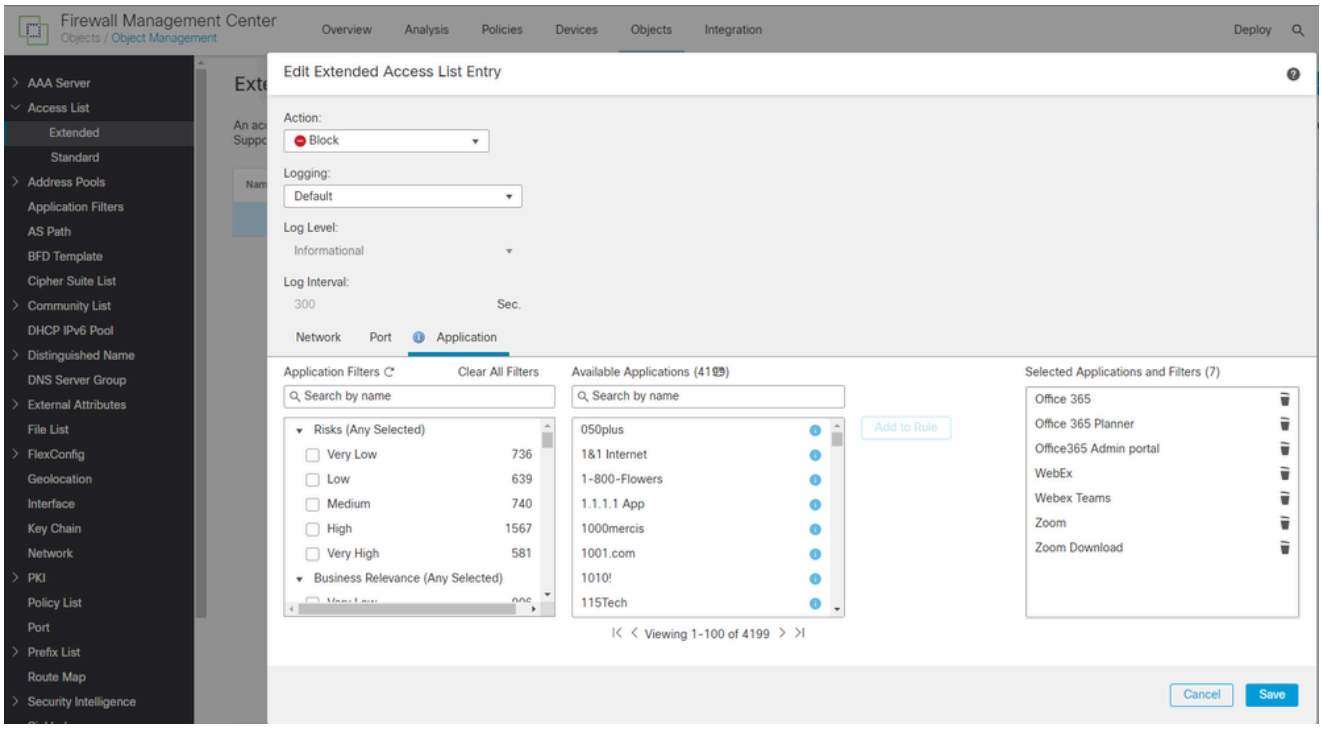
3. Créez une liste de contrôle d'accès étendue qui peut être utilisée par le FTD pour le processus PBR afin de décider si le trafic est envoyé à Umbrella pour SIG ou s'il est exclu de l'IPsec et n'est pas du tout envoyé à Umbrella.

- Une entrée de contrôle d'accès deny sur la liste de contrôle d'accès signifie que le trafic est exclu de SIG.
- Une ACE d'autorisation sur la liste de contrôle d'accès signifie que le trafic est envoyé sur IPsec et peut appliquer une stratégie SIG (CDFW, SWG, etc.).

Cet exemple exclut les applications « Office365 », « Zoom » et « Cisco Webex » avec un ACE deny. Le reste du trafic est envoyé à Umbrella pour une inspection plus approfondie.

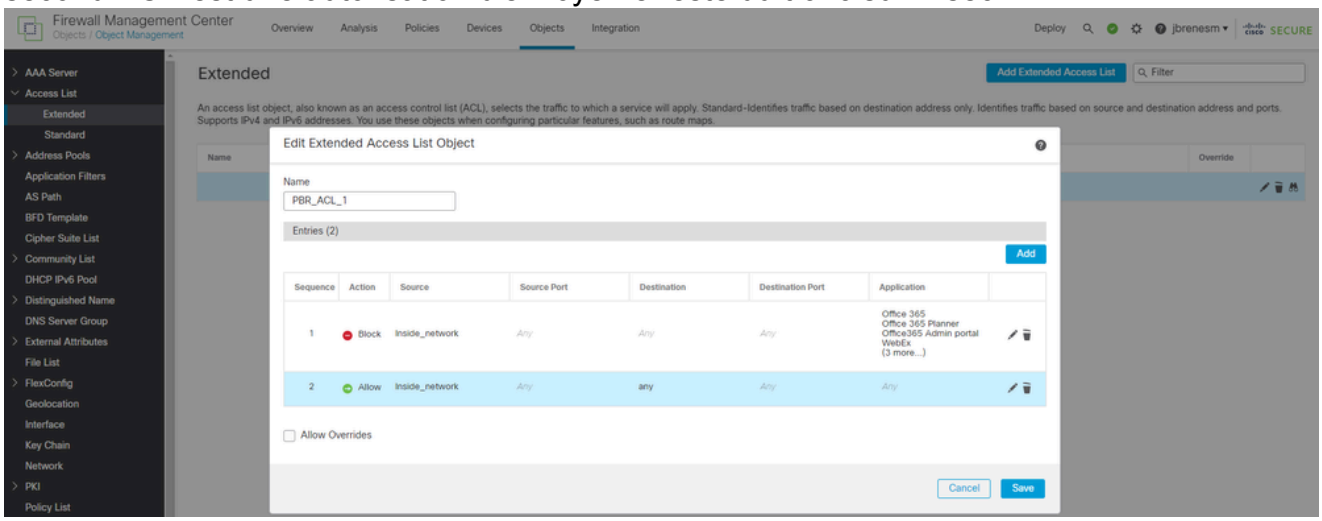
1. Accédez à Object > Object Management > Access List > Extended.
2. Définissez le réseau source et les ports comme vous le feriez normalement, puis ajoutez les

applications à participer sur le PBR.



15669947000852

Le premier ACE peut « refuser » pour les applications mentionnées précédemment, et le second ACE est une autorisation d'envoyer le reste du trafic sur IPsec.

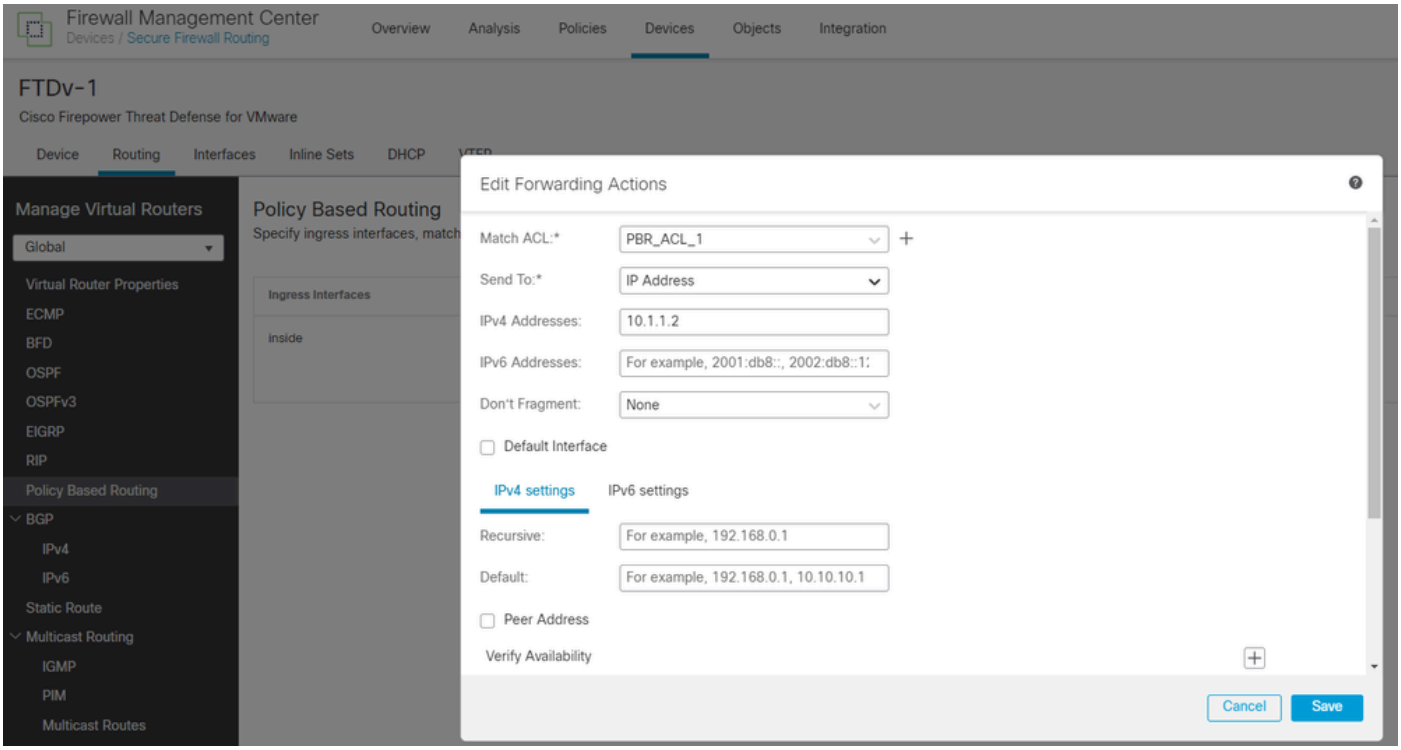


15670006987156

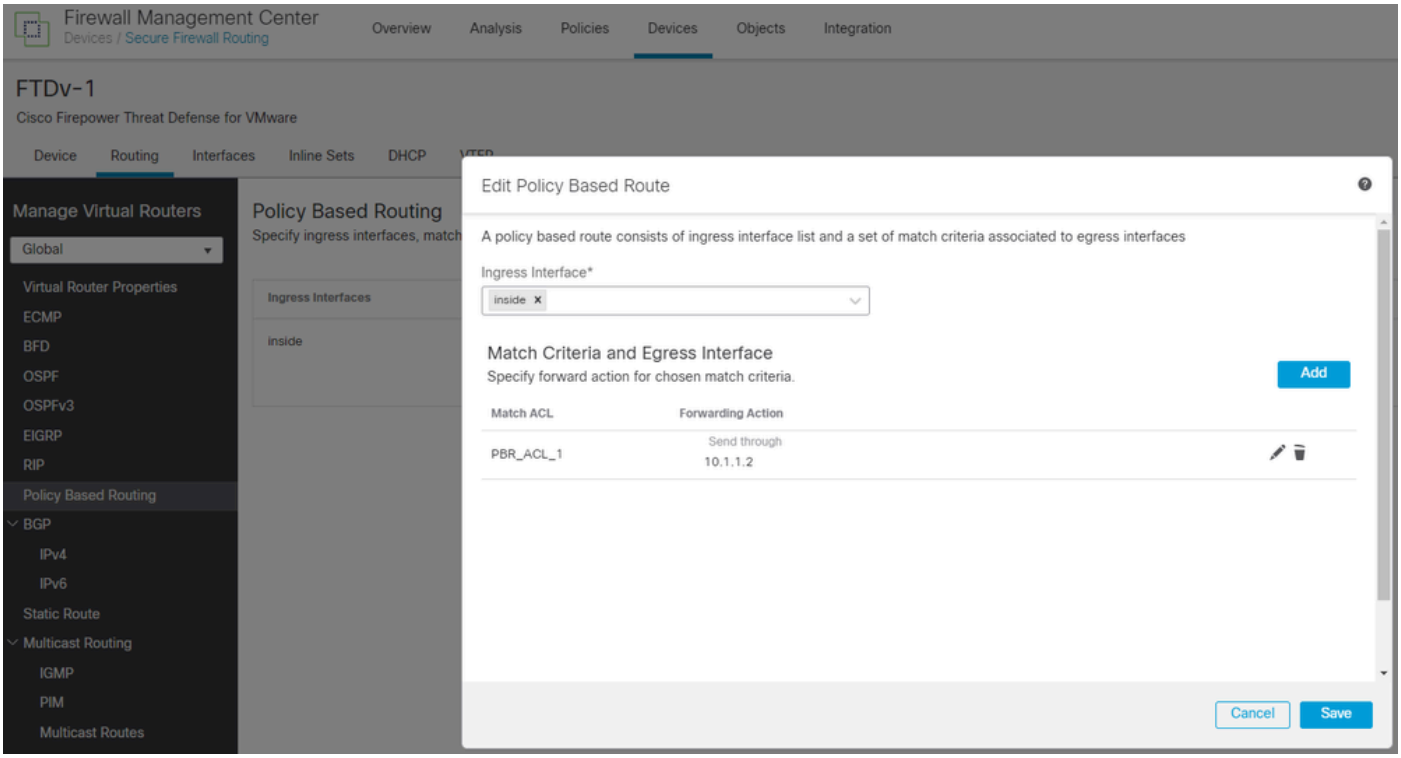
4. Créez le PBR sous Devices > Device Management > [sélectionnez le périphérique FTD] > Routing > Policy Based Routing.

- Interface d'entrée : Interface d'où provient le trafic local.
- ACL correspondante : Liste de contrôle d'accès étendue créée à l'étape précédente, ACL "PBR_ACL_1".
- Envoyer à : Adresse IP
- Adresses IPv4 : Tronçon suivant lorsque le PBR trouve une instruction d'autorisation, de

sorte que le trafic soit routé vers l'IP que vous ajoutez ici. Dans cet exemple, il s'agit de l'IPsec d'Umbrella. Si l'IP de votre VPN VTI est 10.1.1.1, alors l'IP IPsec d'Umbrella serait n'importe quoi à l'intérieur de ce même réseau (10.1.1.2 par exemple).



15670209158036



15670247521556

5. Déployez les modifications sur le FMC.

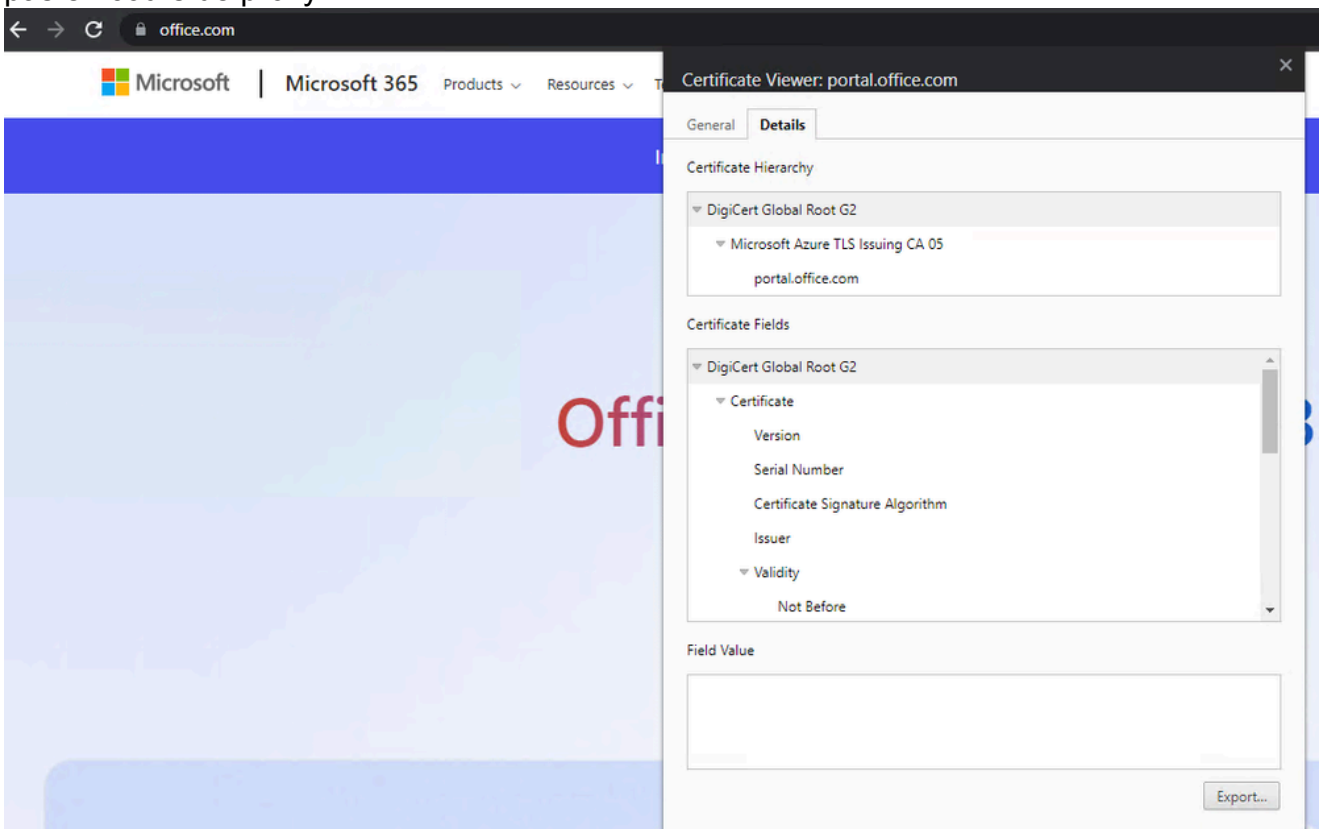
Vérification

Sur le PC de test situé derrière le FTD, vérifiez les points suivants :

- Le trafic en provenance du PC est en fait envoyé via IPsec à Umbrella.
  Accédez à : https://policy-debug.checkumbrella.com/

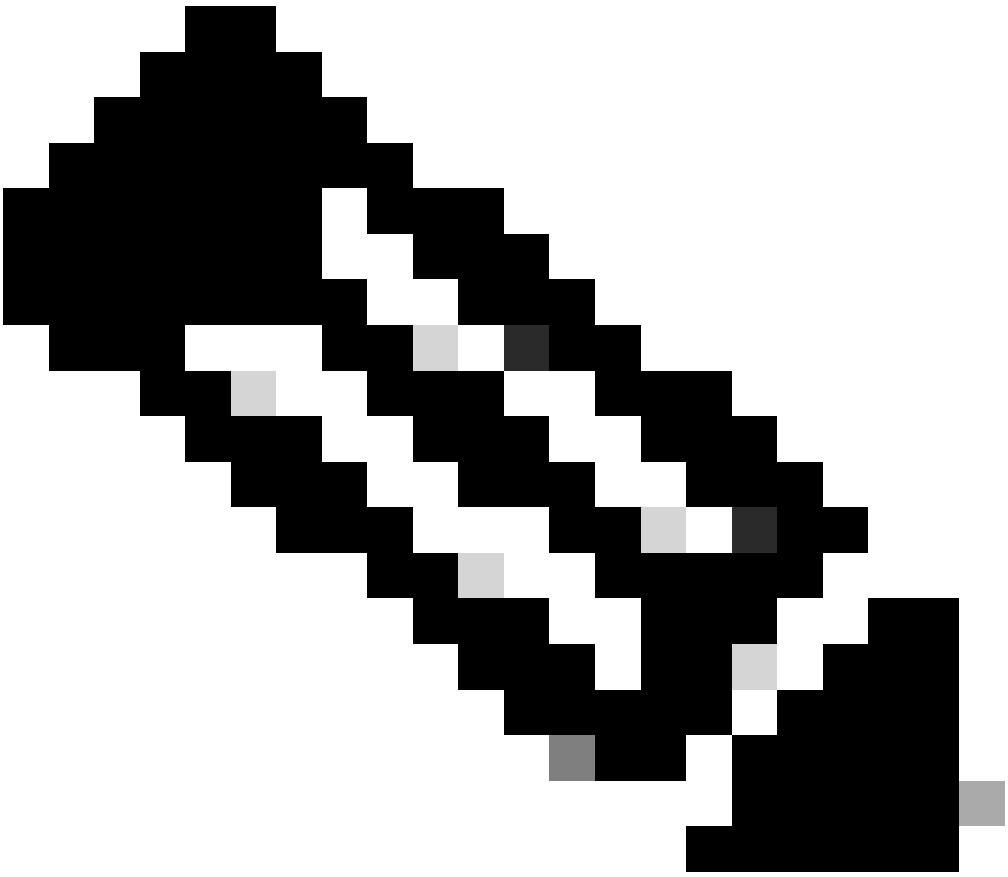
15670737148948

- Essayez d'accéder à l'un des sites qui sont exclus de la configuration PBR/ACL et assurez-vous que l'AC racine d'Umbrella n'est pas présentée, ce qui signifie que la connexion n'est pas en cours de proxy :

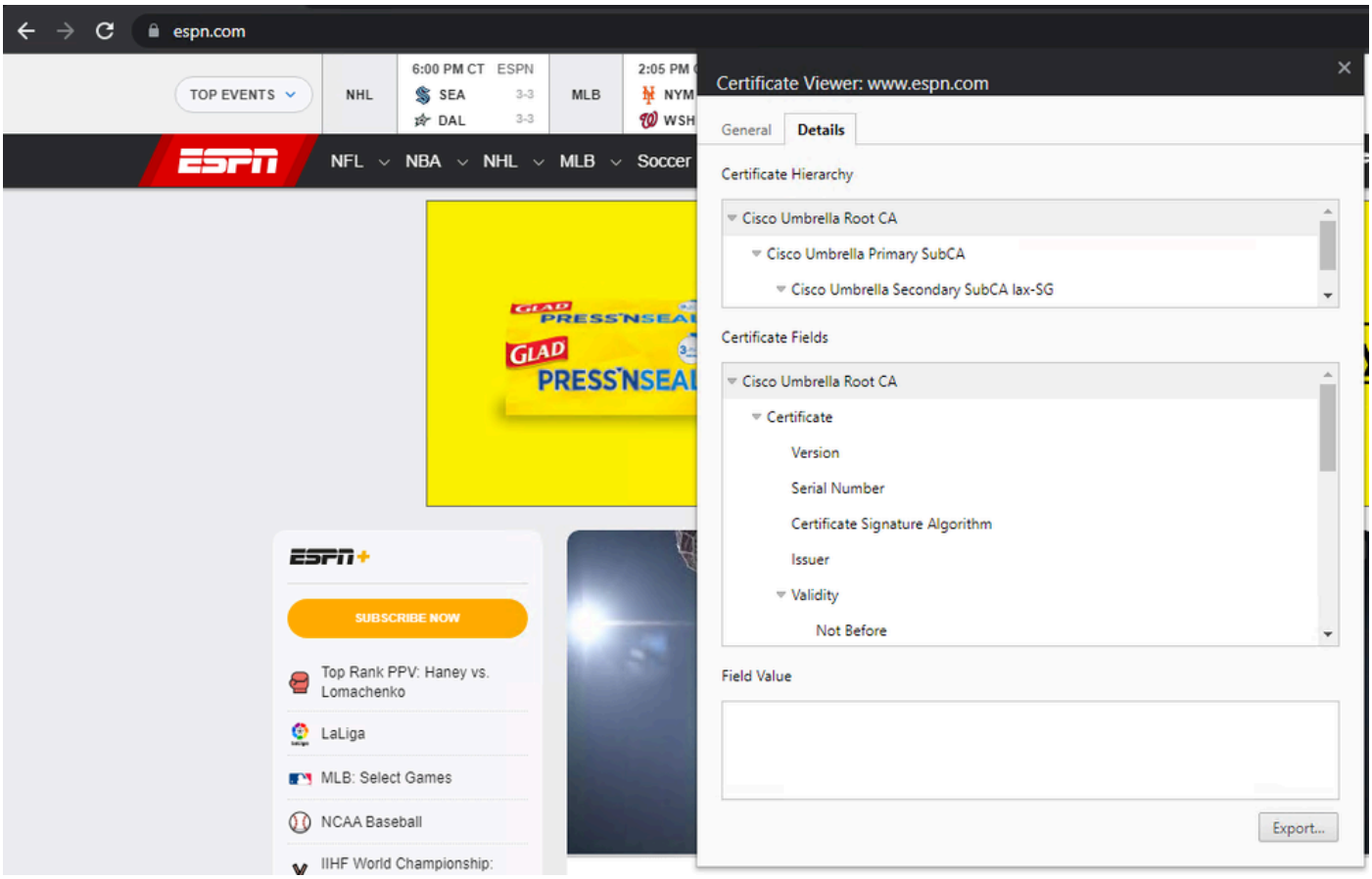


15670820980756

- Essayez d'accéder à tout autre site qui n'est pas basé sur les applications exclues du PBR et assurez-vous qu'Umbrella est bien un proxy de la connexion :



Remarque : Afin d'éviter des problèmes avec une page d'avertissement non approuvée, assurez-vous que le certificat CA racine Umbrella est installé.



- Sur l'interface de ligne de commande du FTD, vous pouvez exécuter quelques commandes pour confirmer que la configuration a été correctement poussée et qu'elle fonctionne :
  - `show run route-map` (vérifie la configuration 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#
```

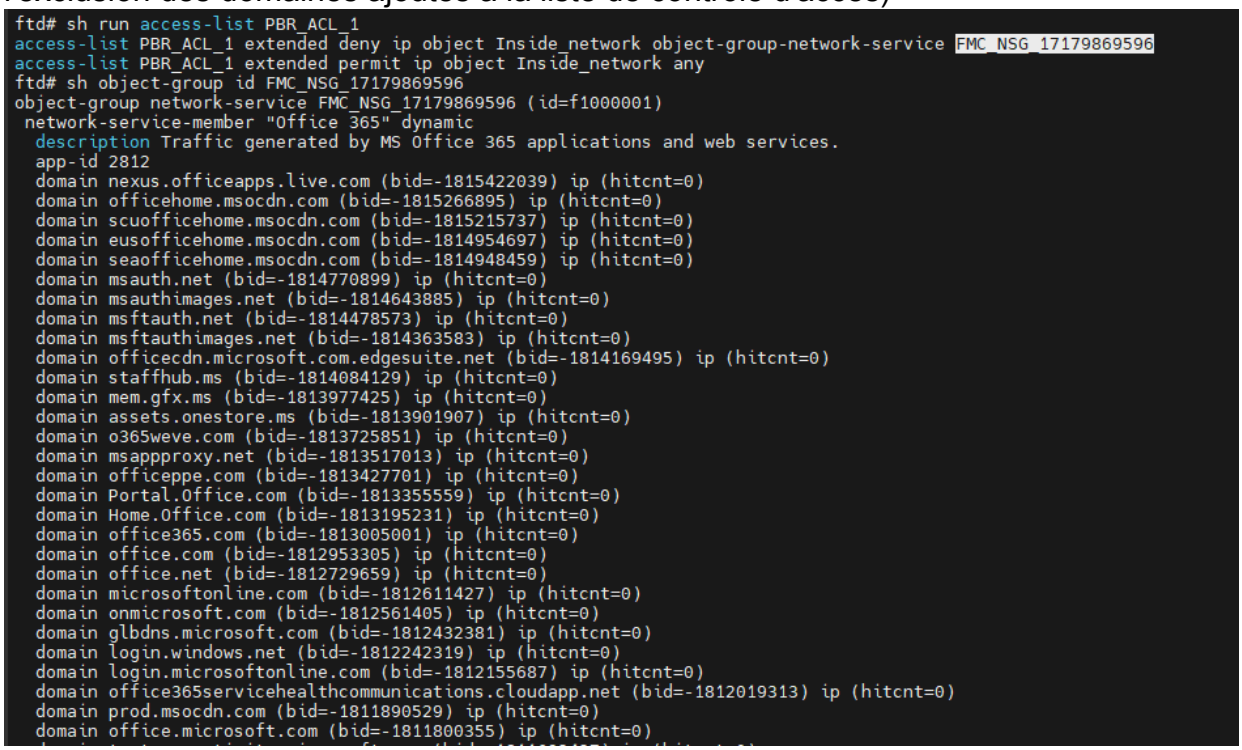
15670322054036

  - `show run interface gigabitEthernet 0/1` (vérifie que le PBR est appliqué à l'interface appropriée)

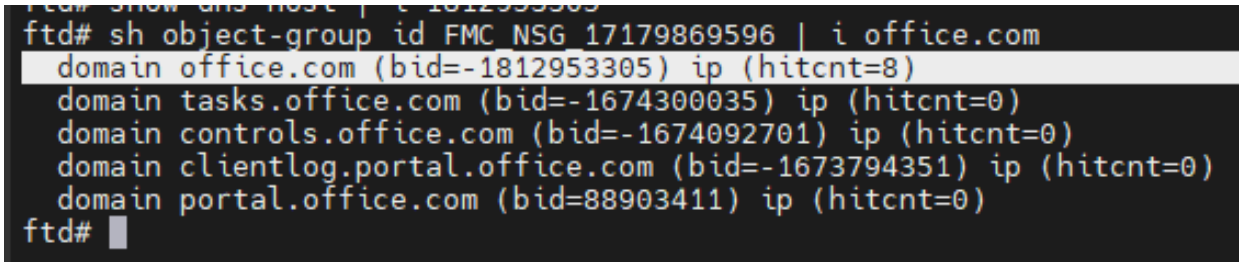
```
ftd# sh run interface gigabitEthernet 0/1
!
interface GigabitEthernet0/1
 nameif inside
 security-level 0
 ip address 172.16.72.1 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1682004086289
ftd#
```

15678344219540

- `show run access-list PBR_ACL_1, show object-group id FMC_NSG_17179869596` (confirme l'exclusion des domaines ajoutés à la liste de contrôle d'accès)



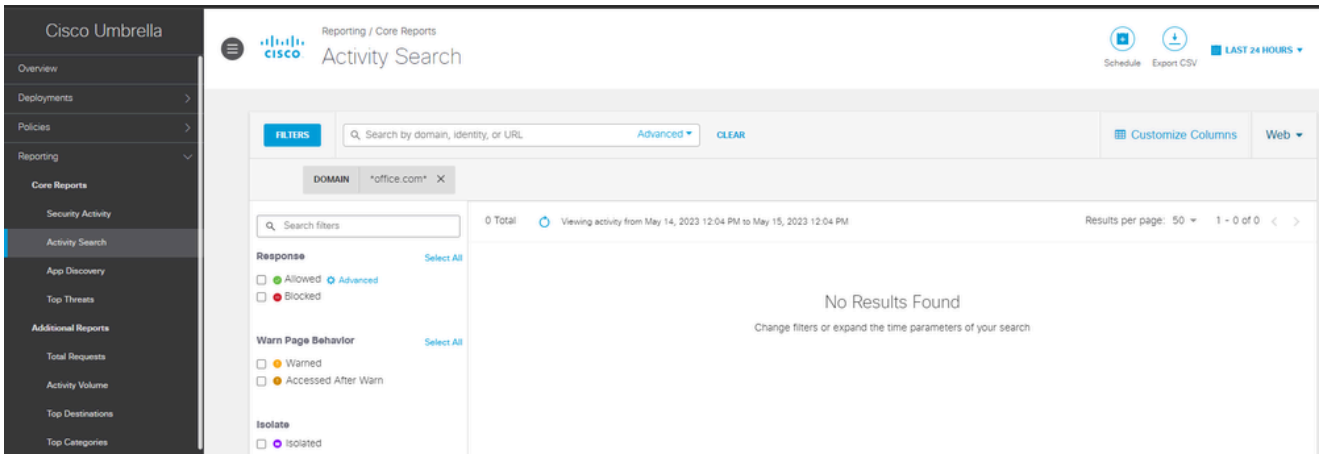
15670420887316



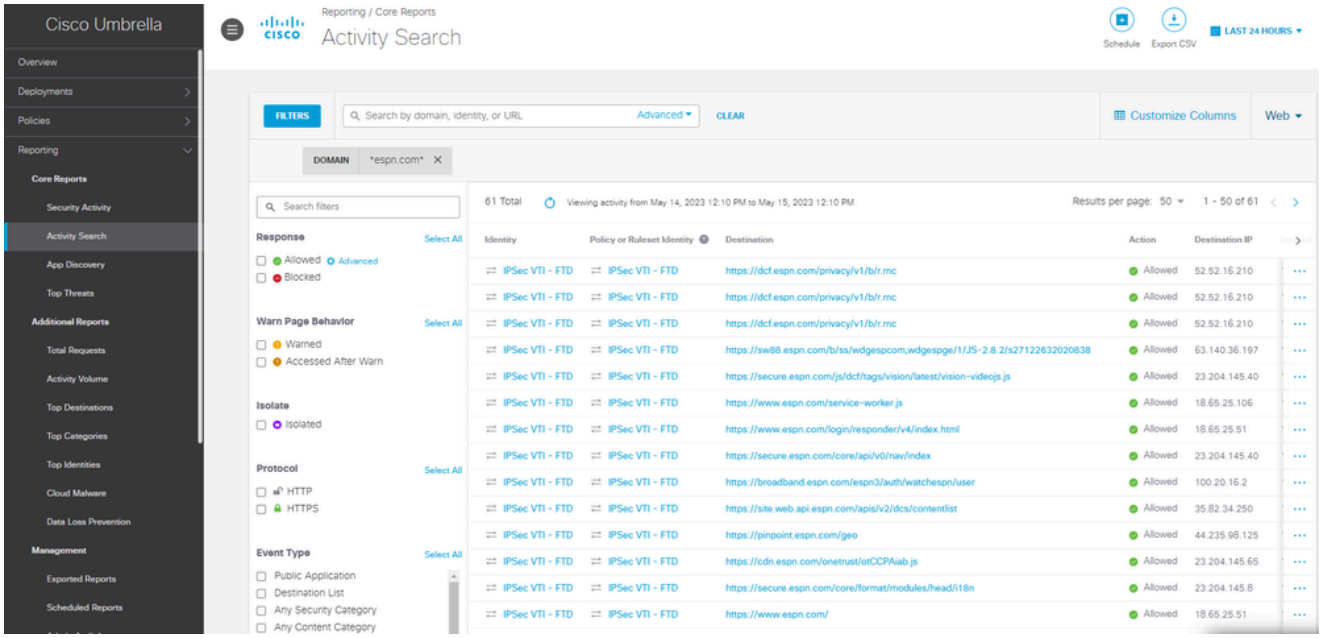
15670635784852

- `packet-tracer input inside tcp 172.16.72.10 1234 fqdn office.com 443 detailed` (vérifie que l'interface externe est utilisée comme sortie et non pas comme interface VTI)

- Sur le tableau de bord Umbrella, sous recherche d'activité, vous pouvez voir que le trafic Web allant vers office.com n'a jamais été envoyé à Umbrella, alors que le trafic allant vers espn.com a été envoyé.



15671098042516



15671302832788

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.