FTD Application-Based PBR configureren voor Umbrella SIG

Inhoud

Inleiding

In dit document wordt beschreven hoe u Firewall Threat Defense (FTD) op toepassing gebaseerde beleidsgebaseerde routering (PBR) configureert voor Umbrella SIG.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot het Umbrella Dashboard
- Beheerderstoegang tot de FMC met 7.1.0+ om de configuratie te implementeren naar FTD versie 7.1.0+. PBR op basis van apps wordt alleen ondersteund op versie 7.1.0 en hoger
- (Voorkeur) Kennis over FMC/FTD-configuratie en paraplu-SIG
- (Optioneel, maar sterk aanbevolen): Umbrella Root Certificate geïnstalleerd, dit wordt gebruikt door SIG wanneer het verkeer wordt proxied of geblokkeerd. Voor meer informatie over de installatie van het basiscertificaat leest u meer in de documentatie van de paraplu.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella Secure Internet Gateway (SIG).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

De informatie in dit document is bedoeld om de configuratiestappen te beschrijven voor het implementeren van Application-Based PBR op de FTD bij het opzetten van een SIG IPsec VTI Tunnel naar Umbrella, zodat u verkeer op een VPN kunt uitsluiten of opnemen op basis van toepassingen die PBR gebruiken.

Het configuratievoorbeeld dat in dit artikel wordt beschreven, richt zich op het uitsluiten van bepaalde toepassingen van de IPsec VPN terwijl al het andere via de VPN wordt verzonden.

Alle informatie over PBR over FMC is te vinden in de Cisco-documentatie.

Beperkingen

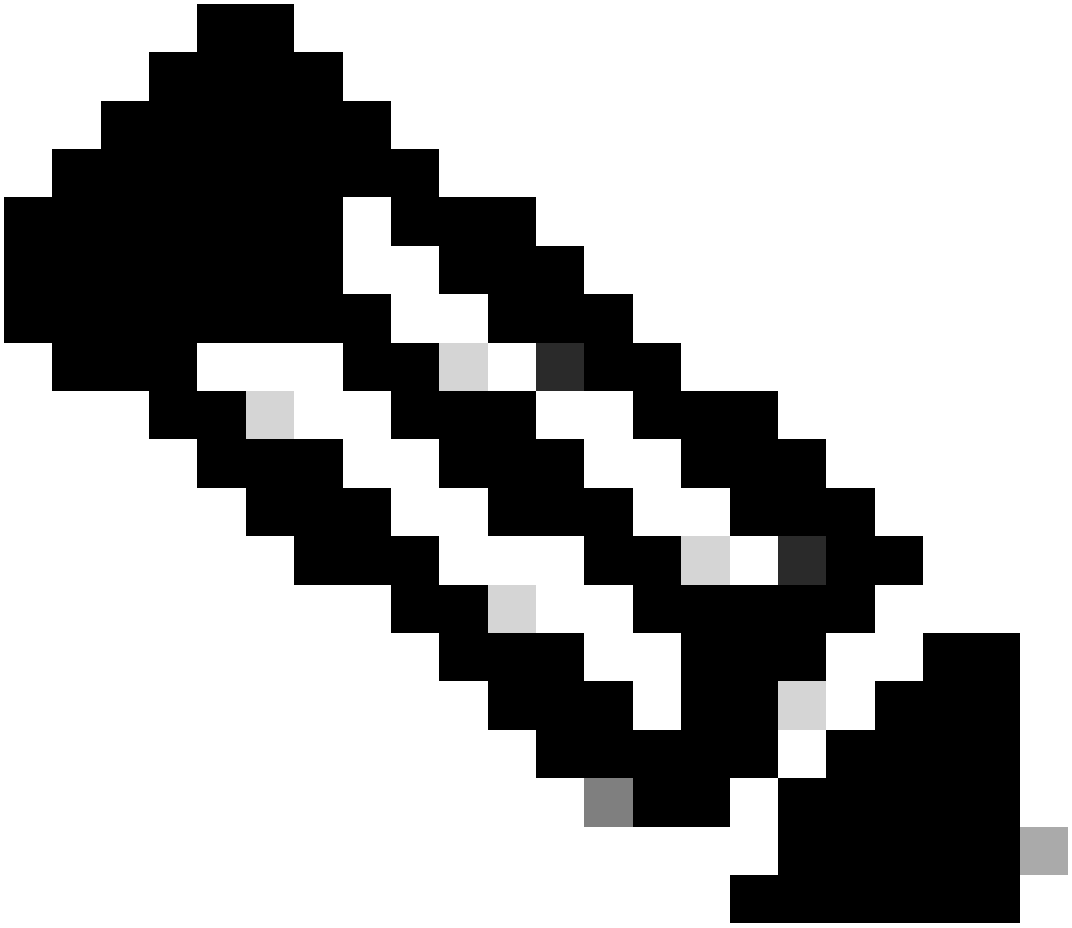
- Het is niet mogelijk om zowel het toepassings- als het bestemmingsadres in een ACE te definiëren.
- Terwijl u de ACL definieert voor de criteria voor beleidsovereenkomst, kunt u meerdere toepassingen selecteren uit een lijst met vooraf gedefinieerde toepassingen om een Access Control Entry (ACE) te vormen.
  Op dit moment kunt u de lijst met vooraf gedefinieerde toepassingen niet toevoegen of wijzigen.
- Voor toepassingen die niet op de lijst met vooraf gedefinieerde toepassingen in de FMC staan of voor onverwacht gedrag met een toepassing, kunnen IP's worden gebruikt in plaats van toepassingen in het PBR.
- Voor een volledige lijst van beperkingen verwijzen wij u naar de documentatie van het PBR.

Toepassingsgebaseerde PBR

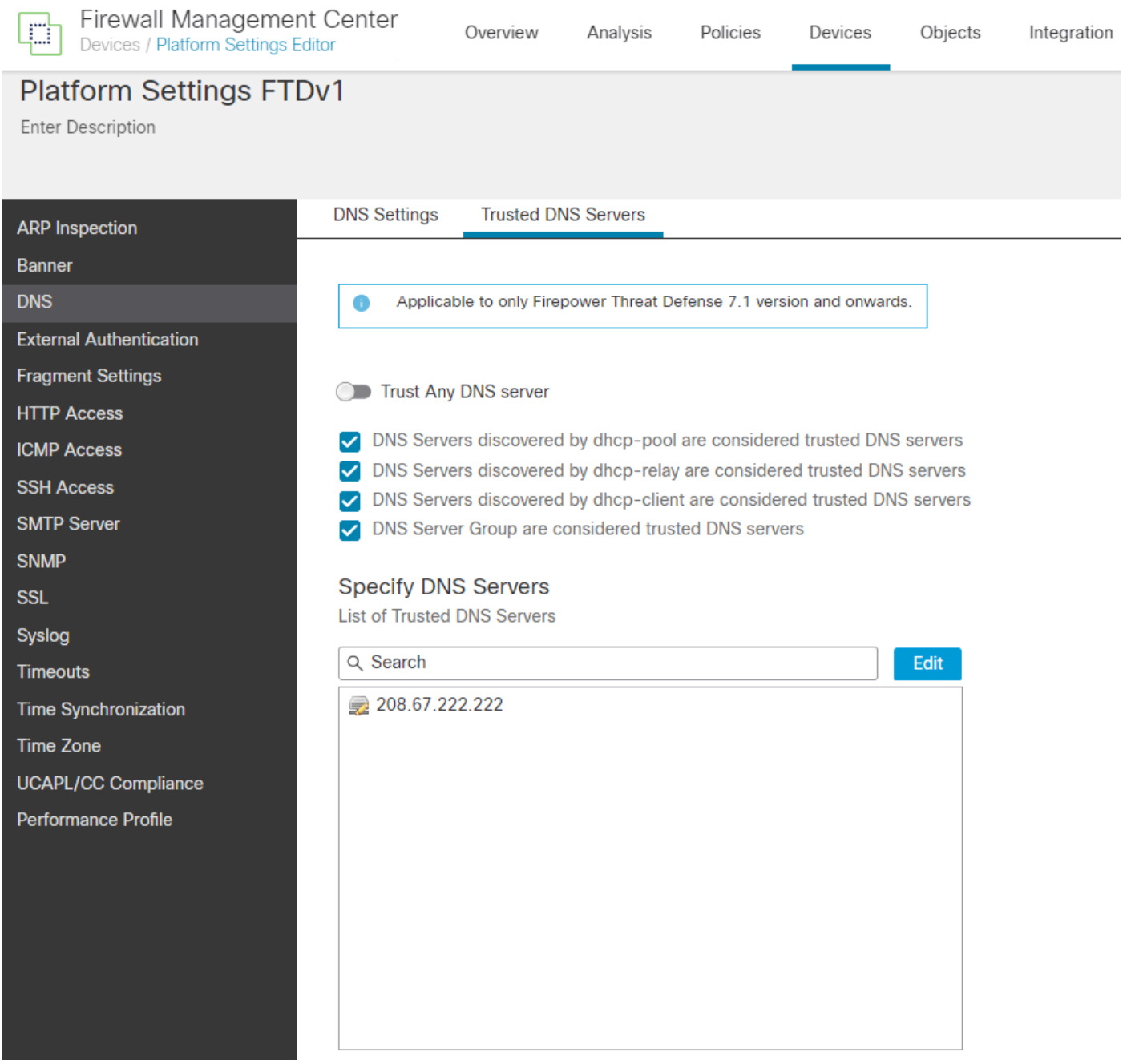
1. Begin met het configureren van de IPsec-tunnel op het VCC en op het Umbrella Dashboard. De instructies voor het uitvoeren van deze configuratie kunt u vinden in de overkoepelende documentatie.

2. Zorg ervoor dat de DNS-server die het apparaat van de eindgebruiker achter de FTD gebruikt, wordt vermeld als een vertrouwde DNS-server onder Apparaten > Platforminstellingen > DNS > Vertrouwde DNS-servers.

Als de apparaten een DNS-server gebruiken die niet wordt vermeld, kan de DNS-snooping mislukken en daarom kan de PBR op basis van apps niet werken. Optioneel (maar niet aanbevolen om veiligheidsredenen), kunt u schakelen tussen Trust Any DNS-server zodat het toevoegen van de DNS-server(s) vereist is.



Opmerking: als VA's worden gebruikt als interne DNS-resolvers, moeten ze worden toegevoegd als vertrouwde DNS-servers.



15669097907860

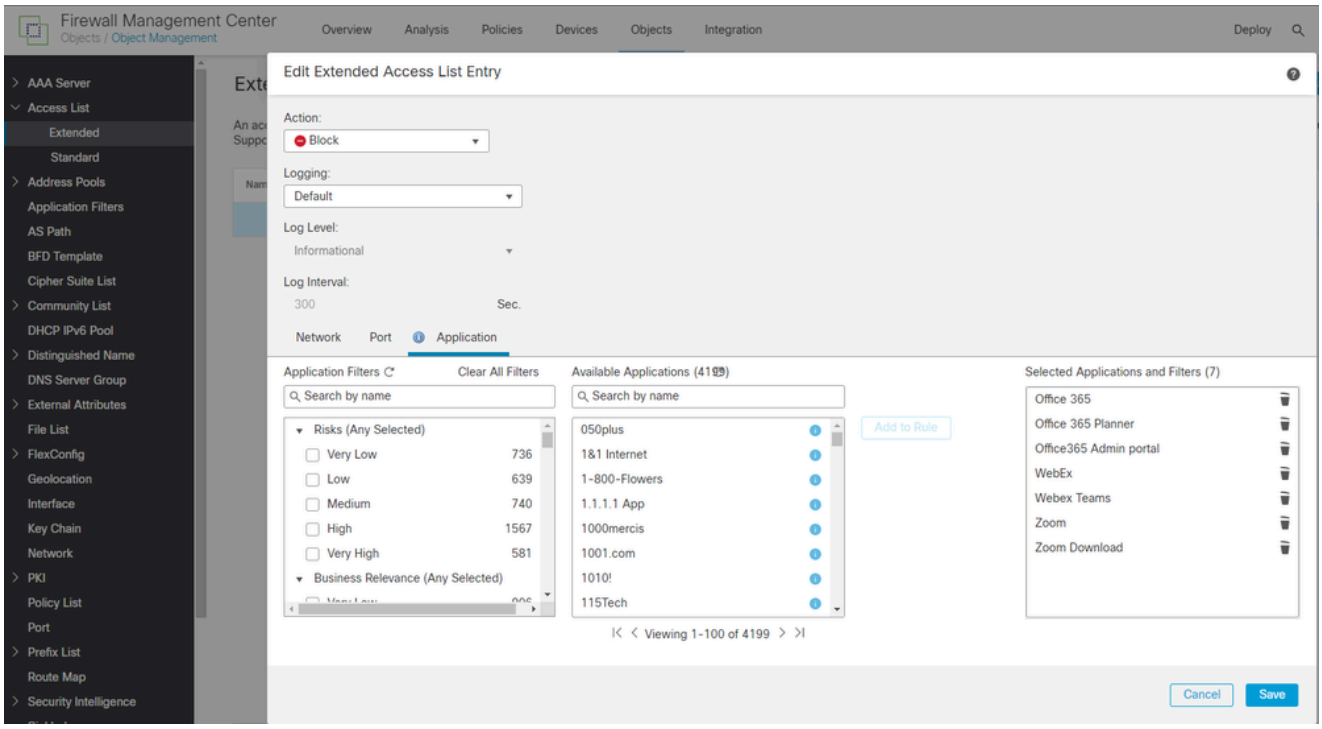
3. Maak een uitgebreide ACL die door de FTD kan worden gebruikt voor het PBR-proces om te beslissen of het verkeer naar Umbrella voor SIG wordt verzonden of dat het wordt uitgesloten van de IPsec en helemaal niet naar Umbrella wordt verzonden.

- Een weigering ACE op de ACL betekent dat het verkeer is uitgesloten van SIG.
- Een ACE-vergunning op de ACL betekent dat het verkeer over de IPsec wordt verzonden en een SIG-beleid kan toepassen (CDFW, SWG, enz.).

In dit voorbeeld worden de toepassingen "Office365", "Zoom" en "Cisco Webex" met een ACE-weigering uitgesloten. De rest van het verkeer wordt naar Umbrella gestuurd voor verdere inspectie.

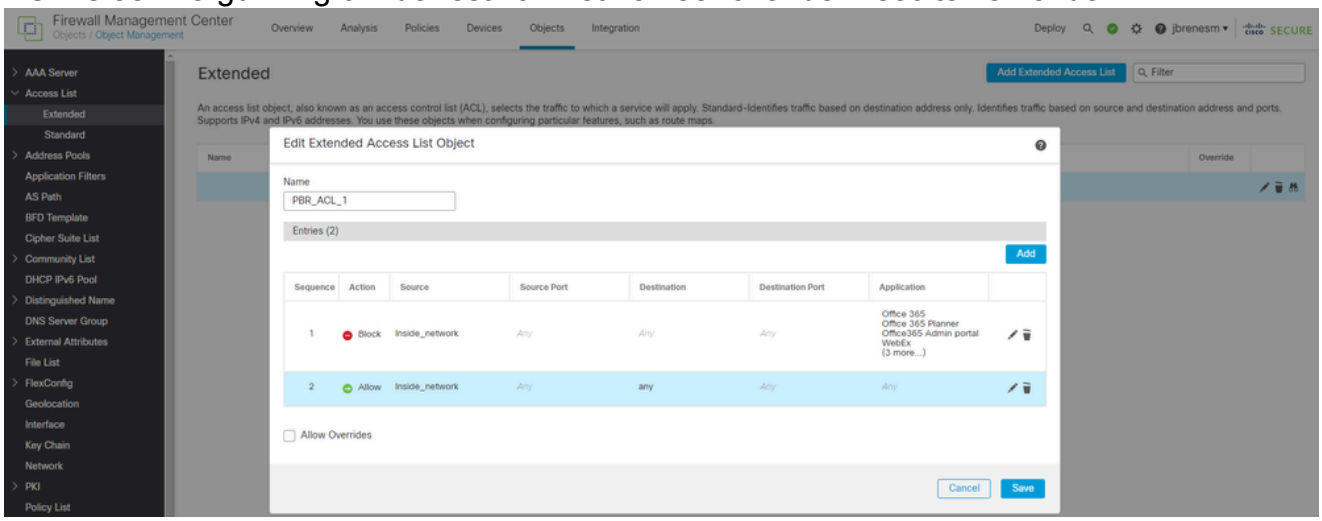
1. Ga naar Object > Objectbeheer > Toegangslijst > Uitgebreid.
2. Definieer het bronnetwerk en de poorten zoals u normaal zou doen en voeg vervolgens de

toepassingen toe om deel te nemen aan het PBR.



15669947000852

De eerste ACE kan "ontkennen" voor de eerder genoemde toepassingen, en de tweede ACE is een vergunning om de rest van het verkeer over de IPsec te verzenden.

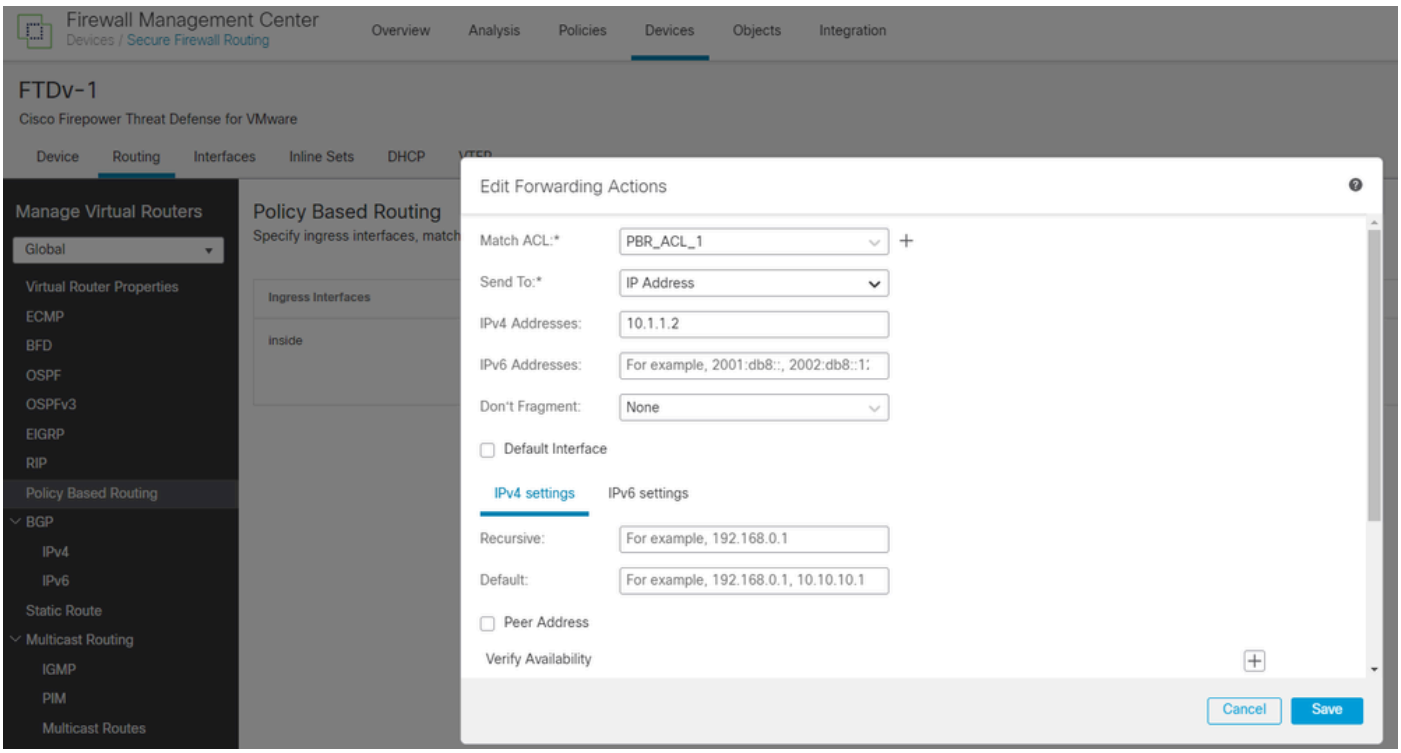


15670006987156

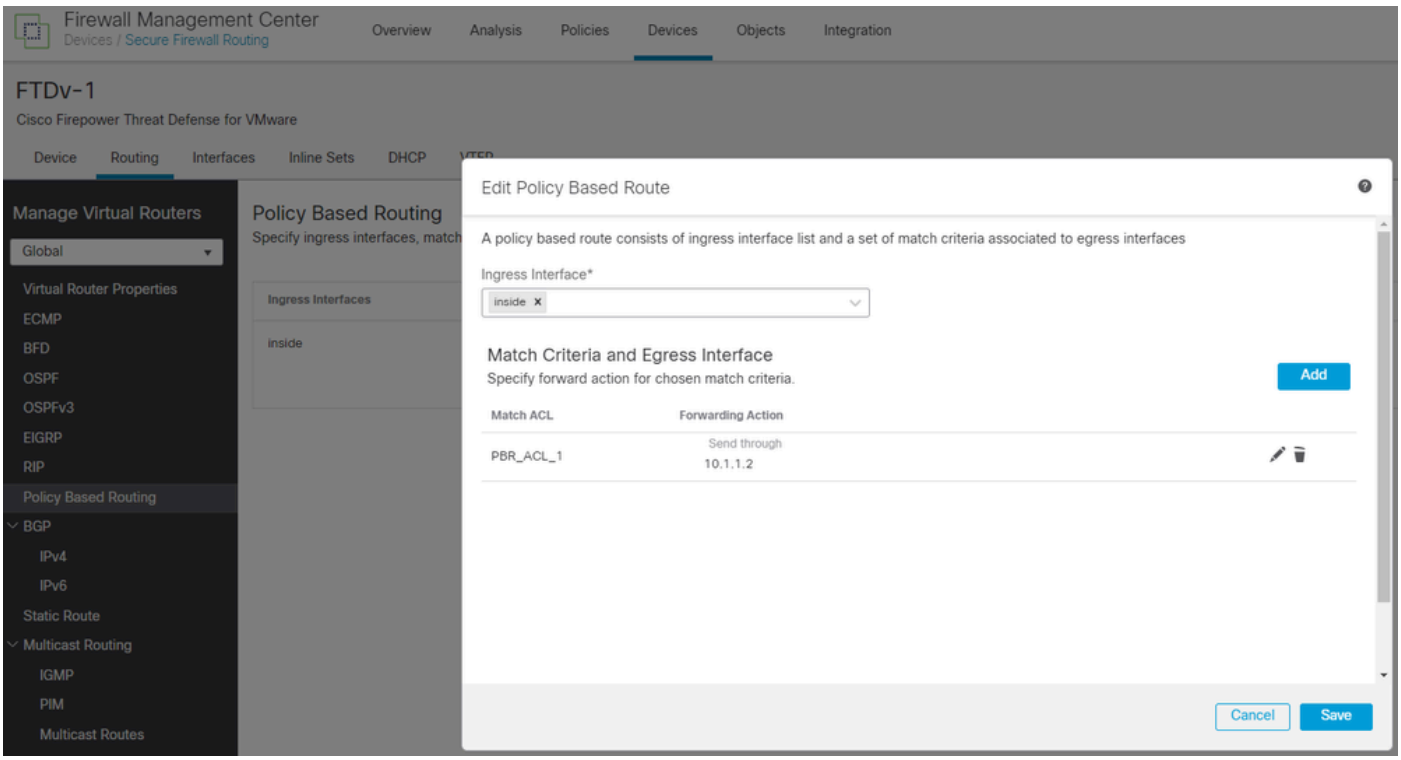
4. Maak de PBR aan onder Apparaten > Apparaatbeheer > [selecteer het FTD-apparaat] > Routering > Op beleid gebaseerde routering.

- Ingress Interface: de interface waar het lokale verkeer vandaan komt.
- Overeenkomende ACL: Uitgebreide ACL gemaakt op vorige stap, ACL "PBR_ACL_1".
- Verzenden naar: IP-adres
- IPv4-adressen: Ga als volgt te werk wanneer de PBR een vergunningsverklaring vindt, zodat het verkeer wordt geleid naar het IP dat u hier toevoegt. In dit voorbeeld is dit Umbrella's

IPsec IP. Als het IP-adres van uw VTI VPN 10.1.1.1 is, dan is het IPsec-adres van de paraplu iets binnen hetzelfde netwerk (bijvoorbeeld 10.1.1.2).



15670209158036



15670247521556

5. De wijzigingen in het VCC implementeren.

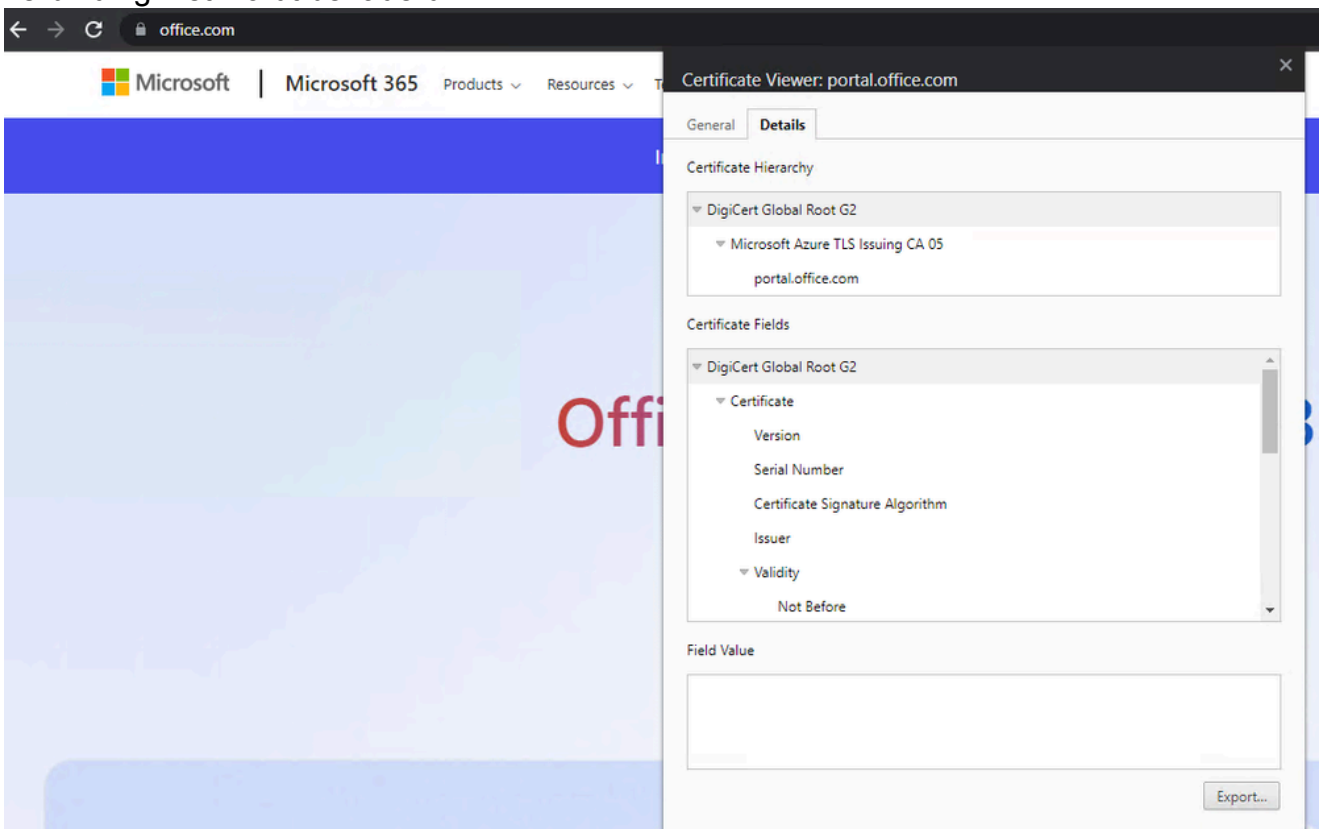
Verificatie

Controleer op de test-pc achter de FTD:

- Het verkeer van de pc wordt eigenlijk via de IPsec naar Umbrella verzonden.
  Ga naar: https://policy-debug.checkumbrella.com/

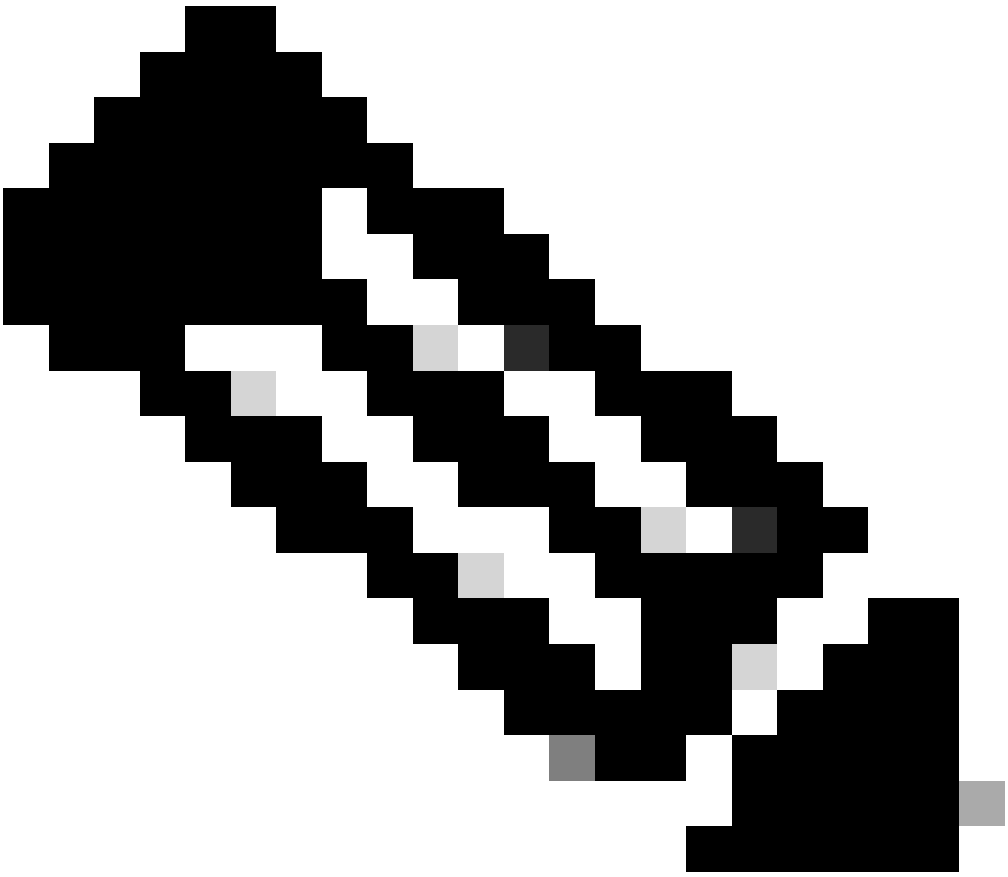
15670737148948

- Probeer naar een van de sites te gaan die zijn uitgesloten in de PBR/ACL-configuratie en zorg ervoor dat de CA Umbrella Root niet wordt weergegeven, wat betekent dat de verbinding niet wordt benaderd:

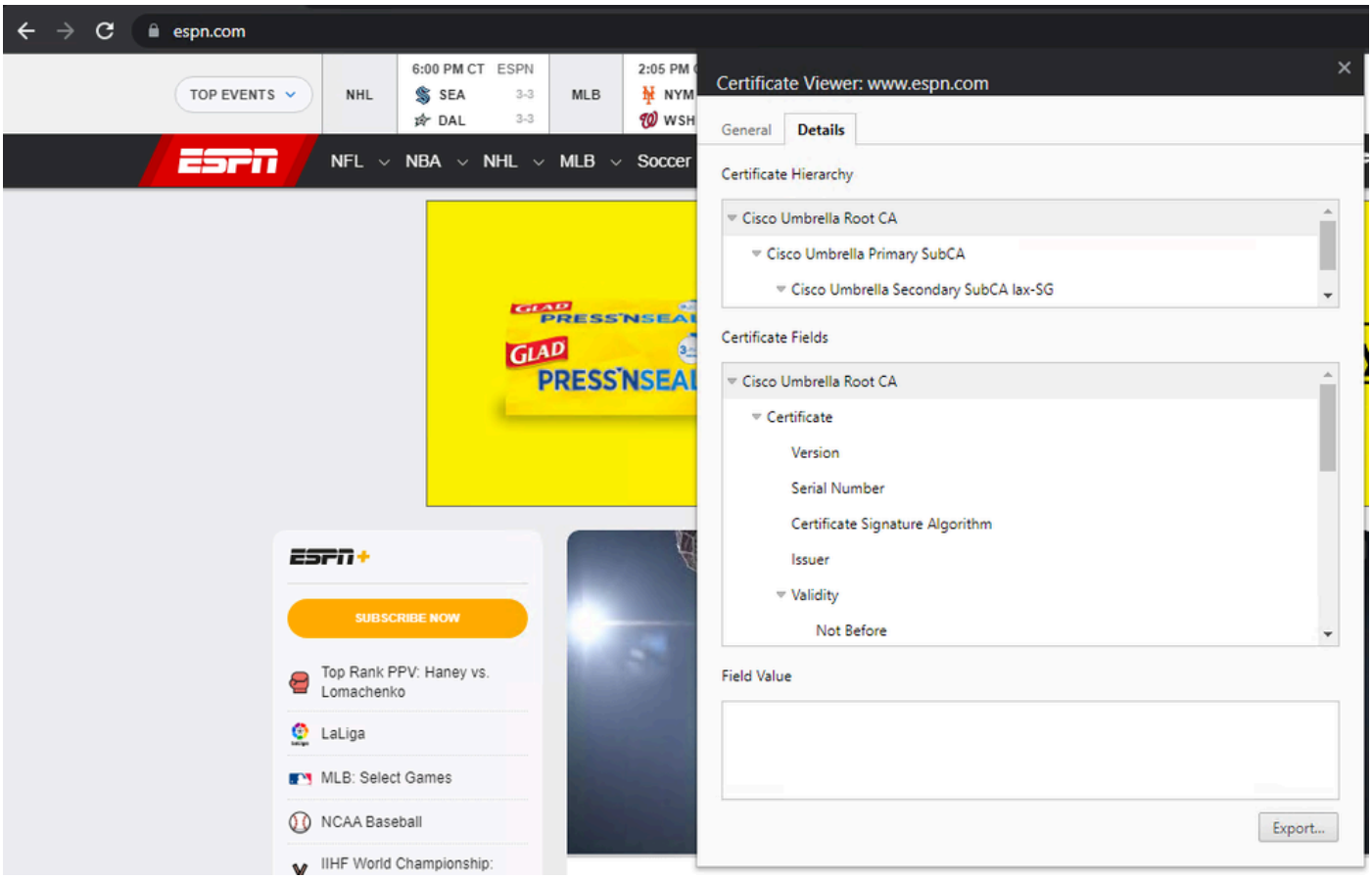


15670820980756

- Probeer naar een andere site te gaan die niet is gebaseerd op de toepassingen die zijn uitgesloten van het PBR en zorg ervoor dat Umbrella inderdaad de verbinding proxyneert:



Opmerking: om problemen te voorkomen met een waarschuwingspagina die niet wordt vertrouwd, moet u ervoor zorgen dat het CA-certificaat voor de hoofdmap is geïnstalleerd.



- Op de CLI van de FTD kunt u een paar opdrachten uitvoeren om te bevestigen dat de configuratie correct is gepusht en werkt:
  - `routekaart weergeven` (controleert de PBR-configuratie):

```
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#
```

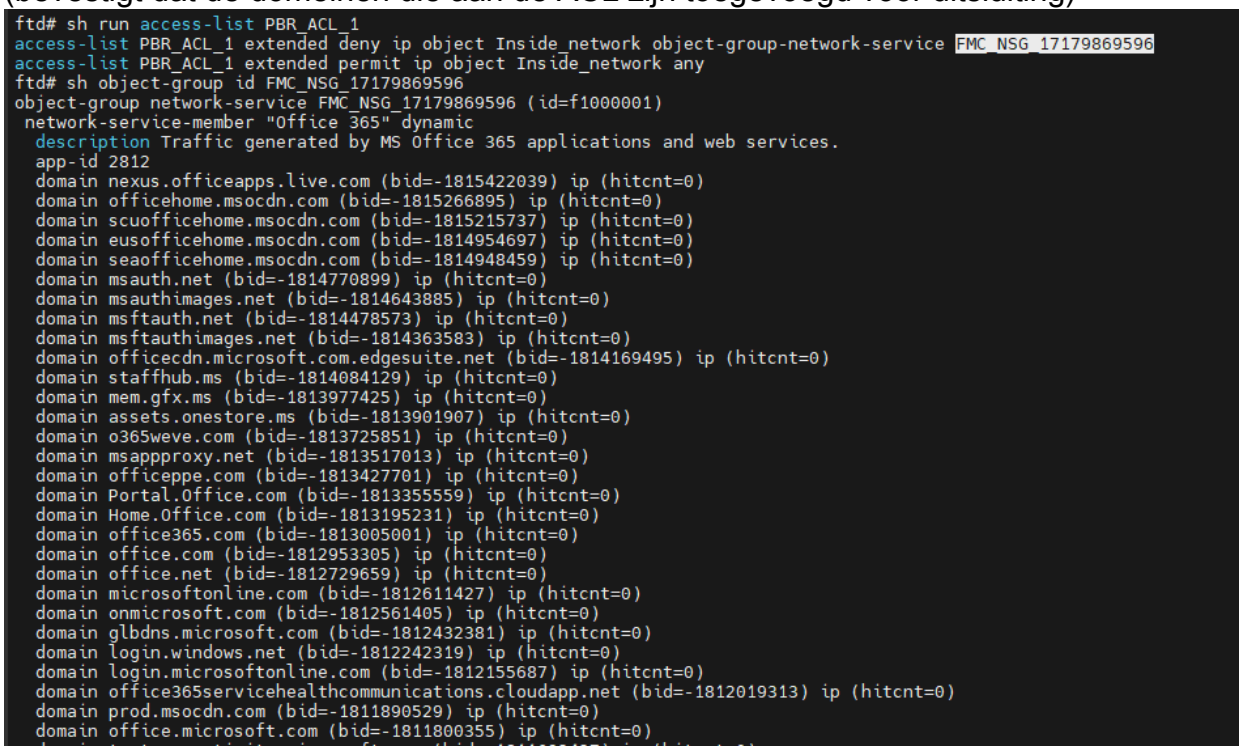
15670322054036

  - `toon run interface gigabitEthernet 0/1` (controleert of de PBR op de juiste interface is toegepast)

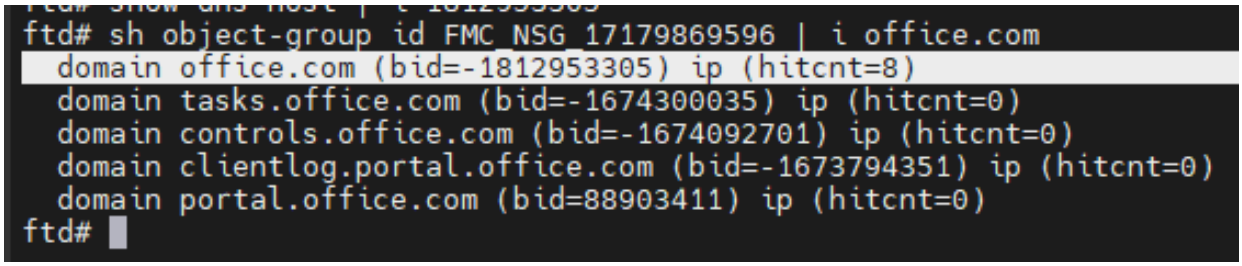
```
ftd# sh run interface gigabitEthernet 0/1
!
interface GigabitEthernet0/1
 nameif inside
 security-level 0
 ip address 172.16.72.1 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1682004086289
ftd#
```

15678344219540

- `run access-list PBR_ACL_1 weergeven, object-group id FMC_NSG_17179869596 weergeven` (bevestigt dat de domeinen die aan de ACL zijn toegevoegd voor uitsluiting)



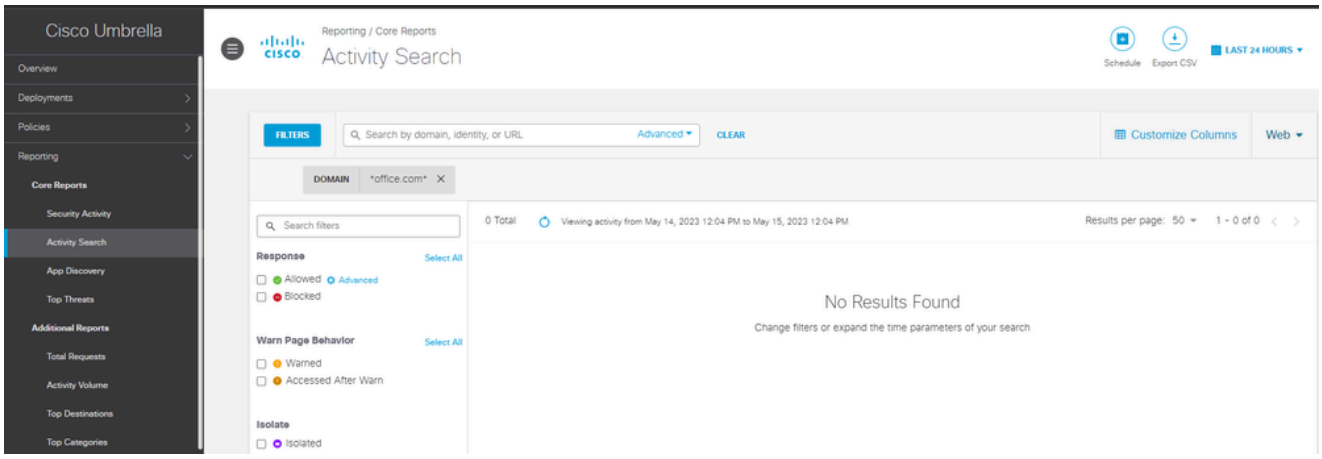
15670420887316



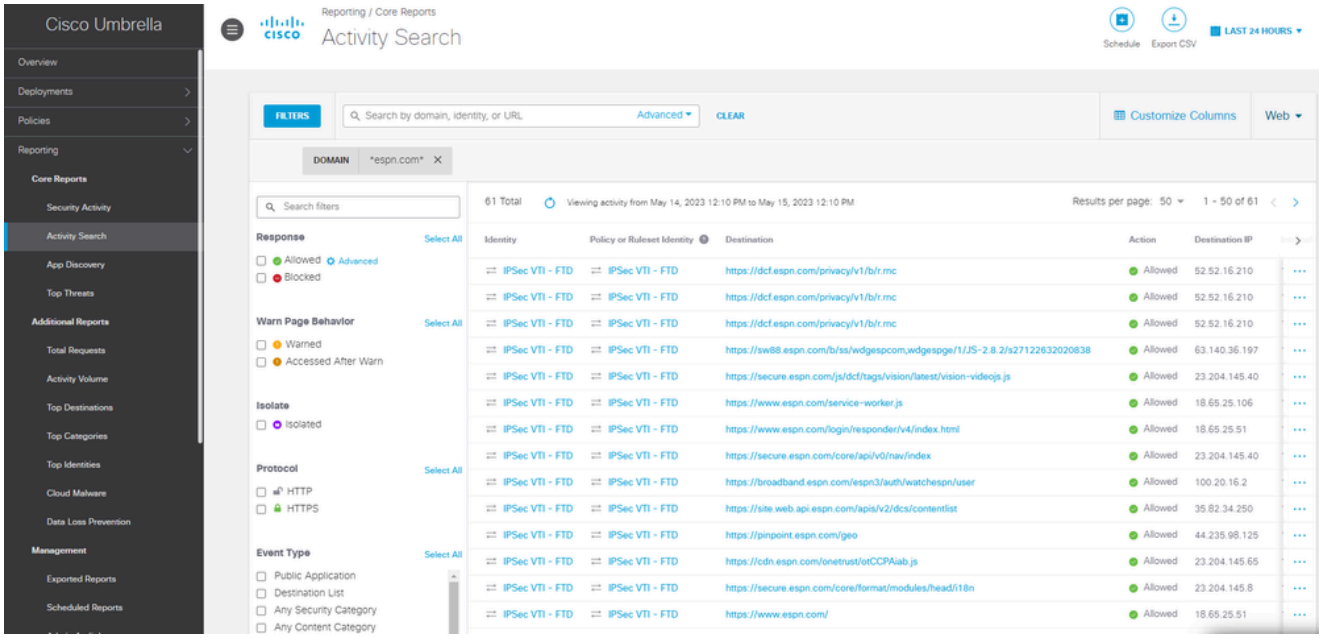
15670635784852

- `packet-tracer invoer binnen tcp 172.16.72.10 1234 fqdn office.com 443 gedetailleerd` (controleert of de buiteninterface wordt gebruikt als uitvoer en niet de VTI één)

- Op het Umbrella Dashboard, onder activiteit zoeken, kunt u zien dat webverkeer naar office.com nooit naar Umbrella is verzonden, terwijl verkeer naar espn.com is verzonden.



15671098042516



15671302832788

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.