為Umbrella SIG配置基於應用的FTD PBR

目錄

簡介

本檔案介紹如何為Umbrella SIG設定防火牆威脅防禦(FTD)應用型原則型路由(PBR)。

必要條件

需求

思科建議您瞭解以下主題：

- 對Umbrella控制面板的訪問許可權
- 對運行7.1.0+的FMC的管理員訪問許可權，以將配置部署到FTD 7.1.0+版。基於應用的PBR僅在7.1.0版及更高版本上受支援
- （首選）瞭解FMC/FTD配置和Umbrella SIG
- （可選，但強烈推薦）：已安裝Umbrella根證書，SIG在代理或阻止流量時使用此證書。有關根證書安裝的更多詳細資訊，請參閱Umbrella文檔中的詳細資訊。

採用元件

本檔案中的資訊是根據Cisco Umbrella安全網際網路閘道(SIG)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

本文中的資訊旨在涵蓋建立到Umbrella的SIG IPsec VTI通道時，如何在FTD上部署基於應用的PBR的設定步驟，以便您可以根據使用PBR的應用在VPN上排除或包含流量。

本文中描述的配置示例重點介紹如何在通過VPN傳送所有其他內容時從IPsec VPN中排除某些應用

。

有關FMC上的PBR的完整資訊，請參閱思科文檔。

限制

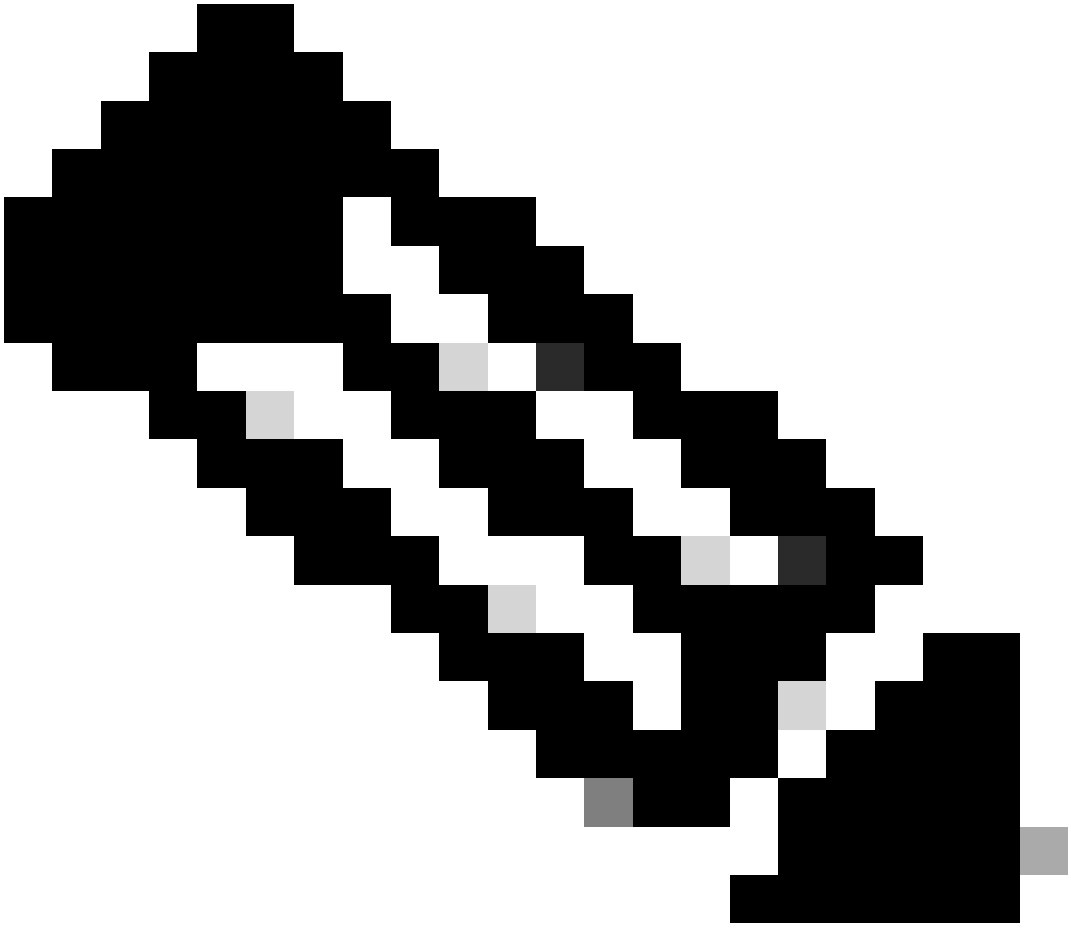
- 不能在ACE中同時定義應用程式和目標地址。
- 在為策略匹配條件定義ACL時，您可以從預定義的應用程式清單中選擇多個應用程式，以形成訪問控制條目(ACE)。
  目前，您無法新增或修改預定義的應用程式清單。
- 對於未列在FMC預定義的應用清單上的應用或應用的任何意外行為，可以使用IP來代替PBR中的應用。
- 有關全部限制的清單，請參考PBR的文檔。

基於應用的PBR

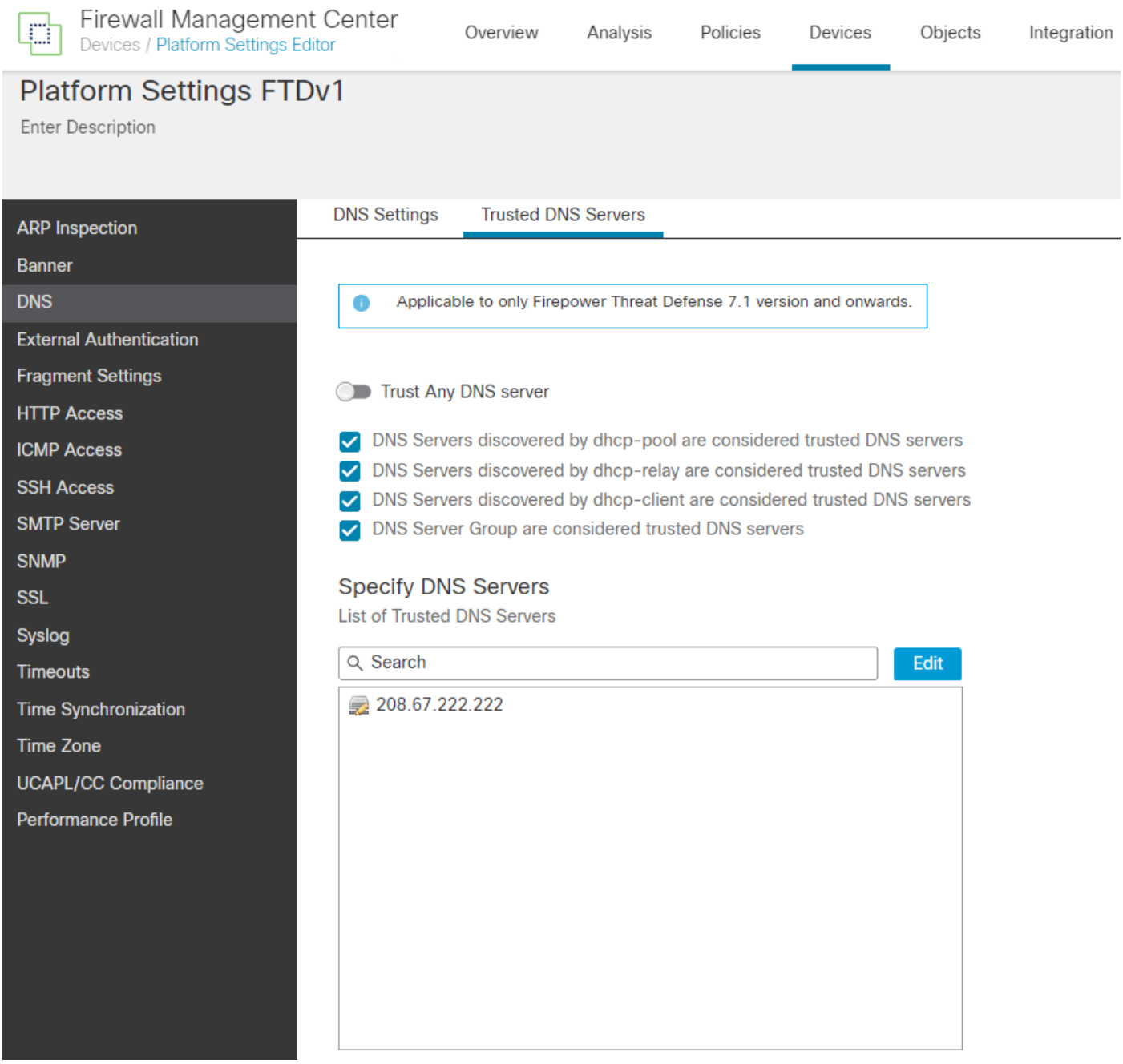
1.首先在FMC和Umbrella Dashboard上配置IPsec隧道。有關如何執行此配置的說明，請參閱Umbrella文檔。

2.確保FTD後方終端使用者裝置使用的DNS伺服器在Devices > Platform Settings > DNS > Trusted DNS Servers下列為受信任DNS伺服器。

如果裝置使用未列出的DNS伺服器，則DNS監聽可能失敗，因此基於應用的PBR無法工作。或者（出於安全原因不建議使用），您可以開啟Trust Any DNS server，以便需要新增DNS伺服器。



附註：如果將VA用作內部DNS解析器，則必須將其新增為受信任DNS伺服器。



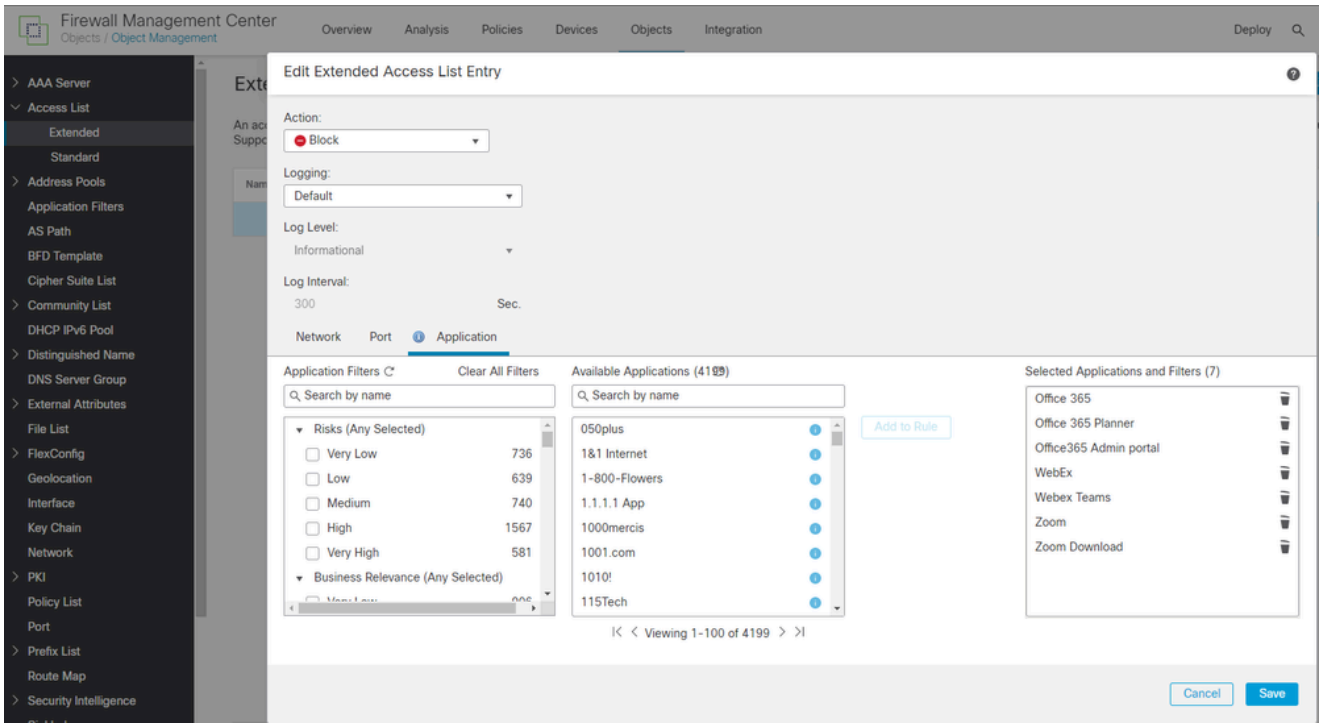
15669097907860

3.建立一個擴展ACL，FTD可將其用於PBR進程，以決定流量是傳送到Umbrella以進行SIG，還是將其從IPsec中排除，而根本不傳送到Umbrella。

- ACL上的deny ACE表示流量從SIG中排除。
- ACL上的permit ACE表示流量是透過IPsec傳送的，且可套用SIG原則（CDFW、SWG等）。

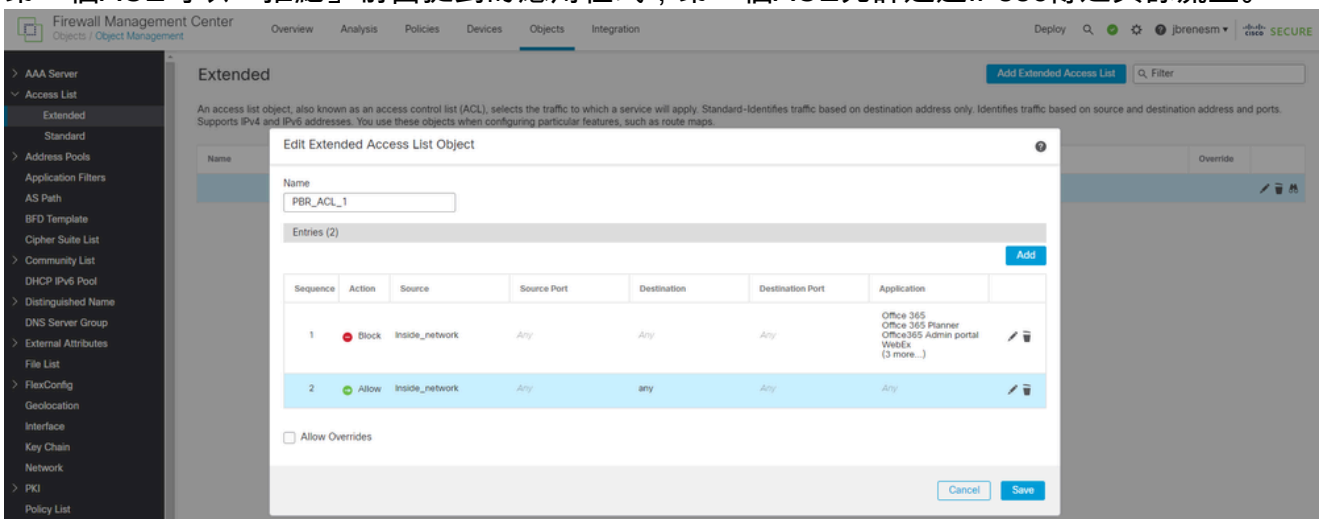
此示例不包括帶有拒絕ACE的應用程式「Office365」、「Zoom」和「Cisco Webex」。其餘流量將傳送到Umbrella進行進一步檢查。

1. 轉至Object > Object Management > Access List > Extended。
2. 按照正常方式定義源網路和埠，然後新增要參與PBR的應用程式。



15669947000852

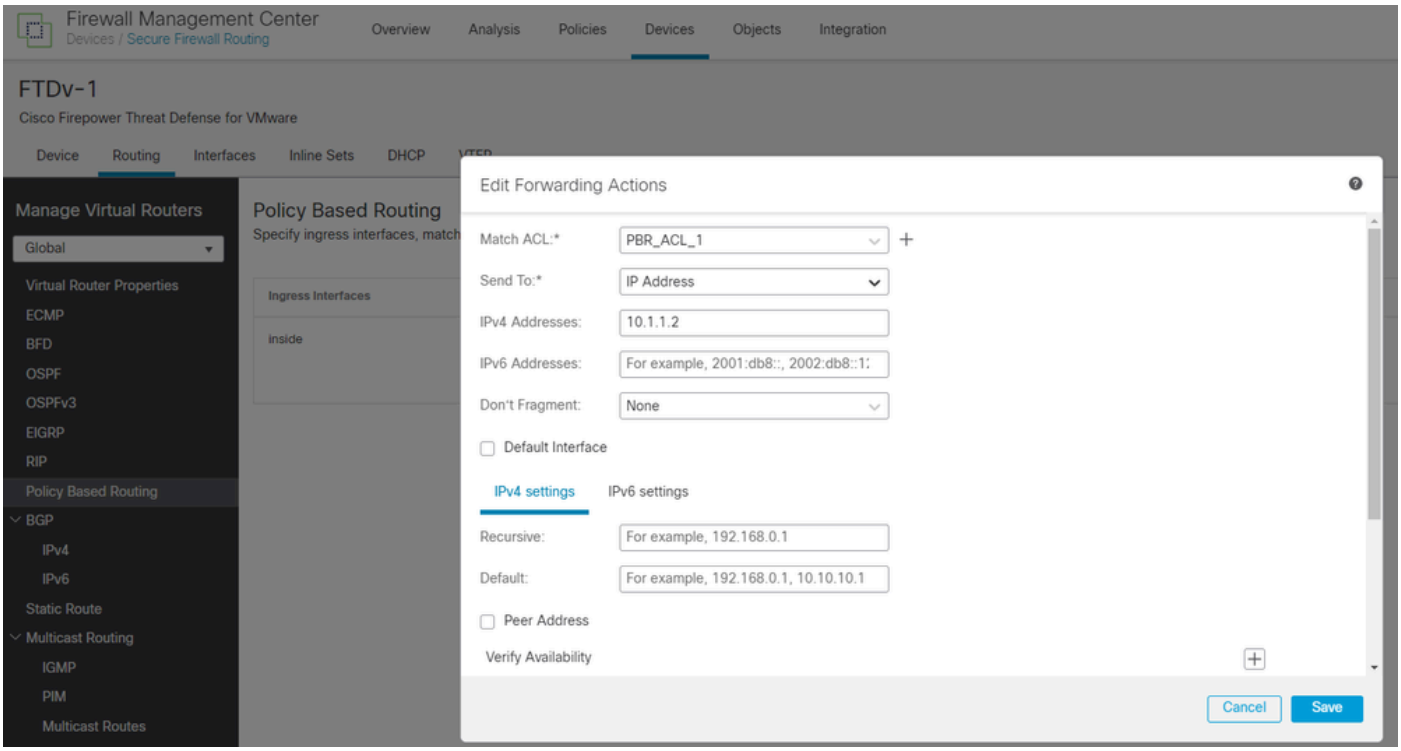
第一個ACE可以「拒絕」前面提到的應用程式，第二個ACE允許通過IPsec傳送其餘流量。



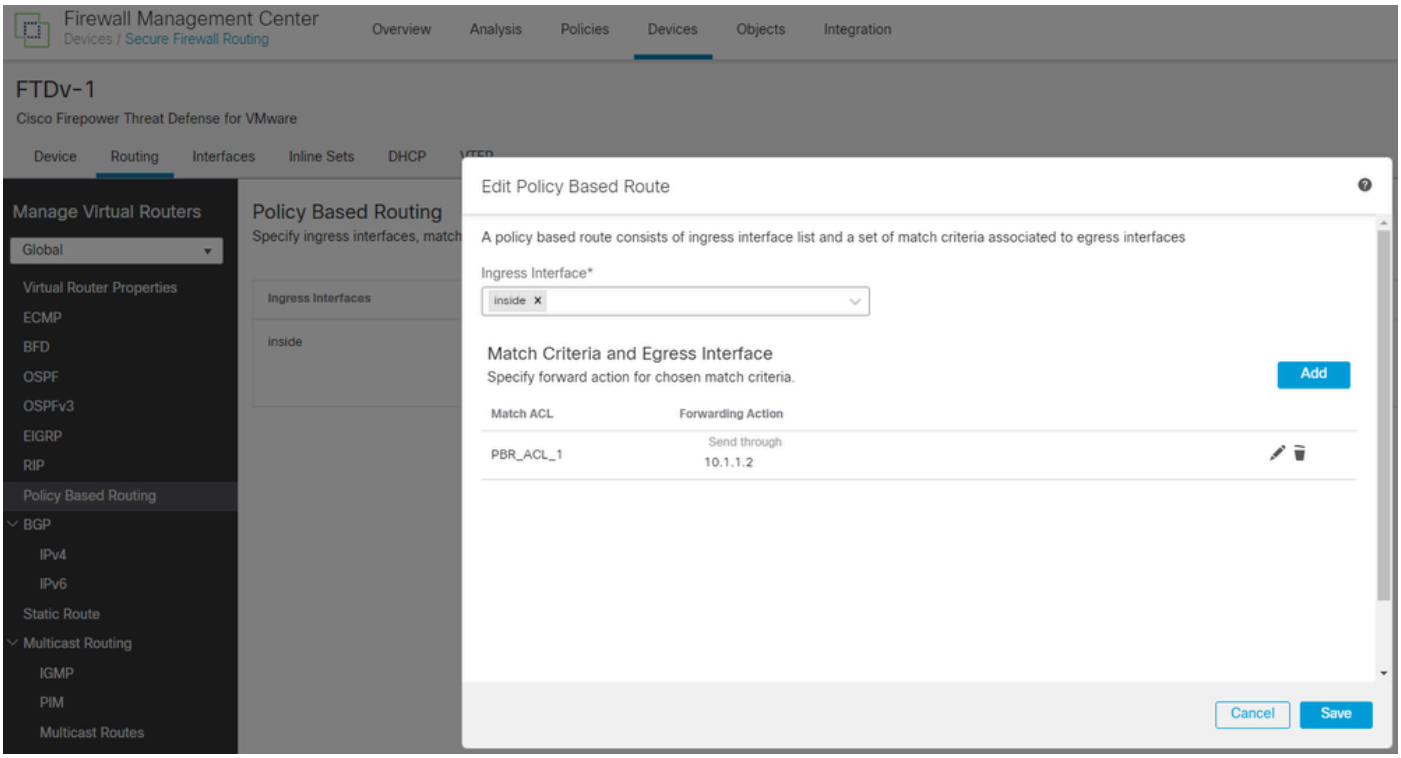
15670006987156

4.在Devices > Device Management > [選擇FTD Device] > Routing > Policy Based Routing下建立PBR。

- Ingress Interface:本地流量來自的介面。
- 相符的ACL:在上一步建立的擴展ACL，即ACL "PBR_ACL_1"。
- 傳送至：IP 位址
- IPv4地址：PBR找到permit語句時的下一跳，因此流量將路由到您在此處新增的IP。在本示例中，這是Umbrella的IPsec IP。如果您的VTI VPN的IP是10.1.1.1，則Umbrella的IPsec IP將是同一網路內的任何內容（例如10.1.1.2）。



15670209158036



15670247521556

5.在FMC上部署更改。

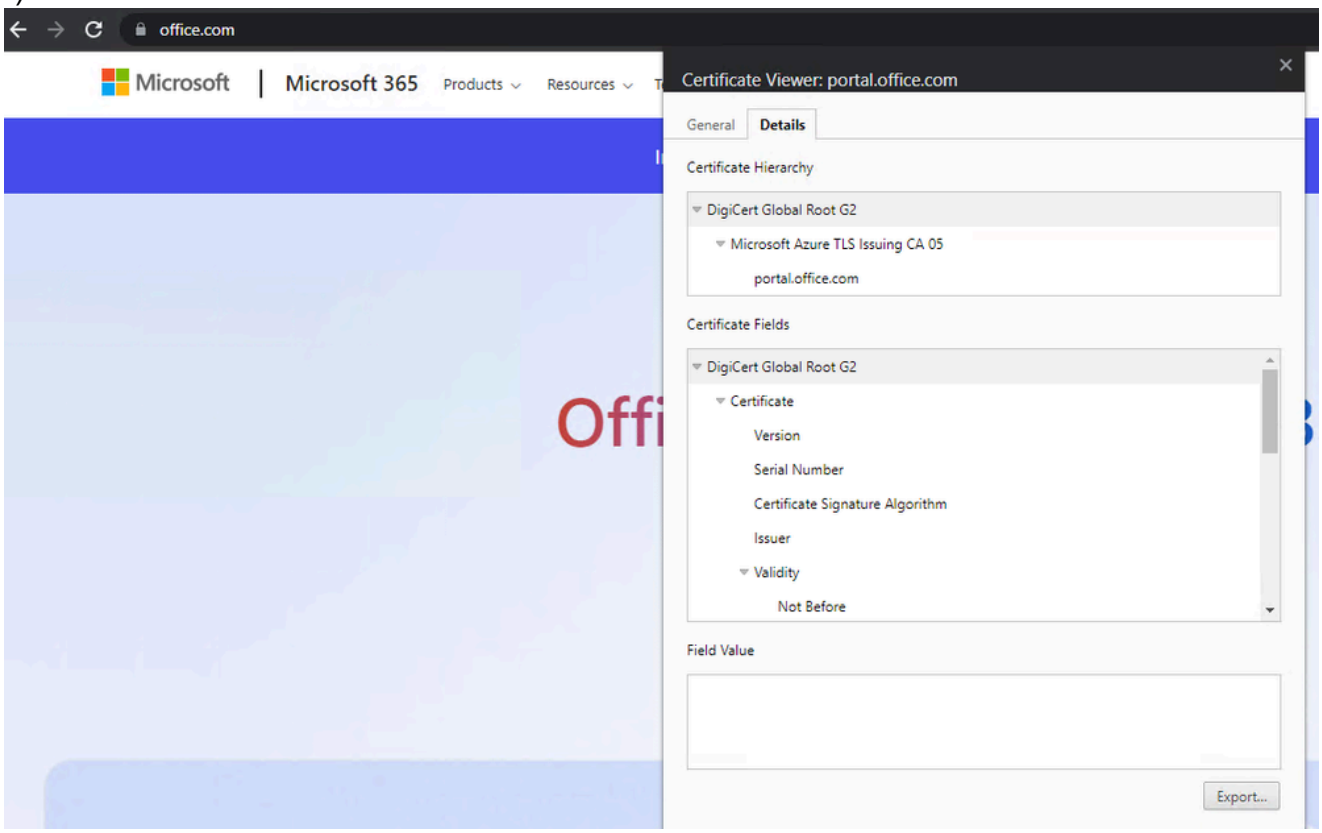
驗證

在FTD後面的測試PC上，檢查：

- 來自PC的流量實際上通過IPsec傳送到Umbrella。
  轉到：https://policy-debug.checkumbrella.com/

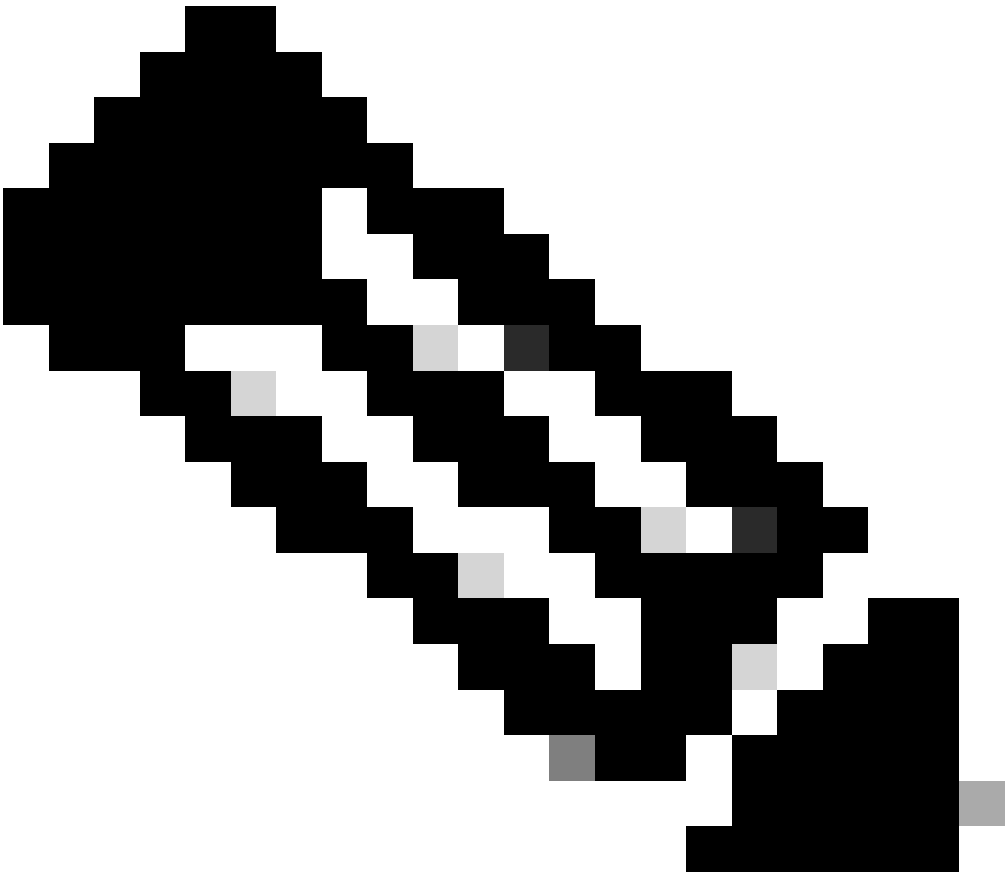
15670737148948

- 嘗試轉到PBR/ACL配置中排除的任何站點，並確保未顯示Umbrella根CA（表示未代理連線）：

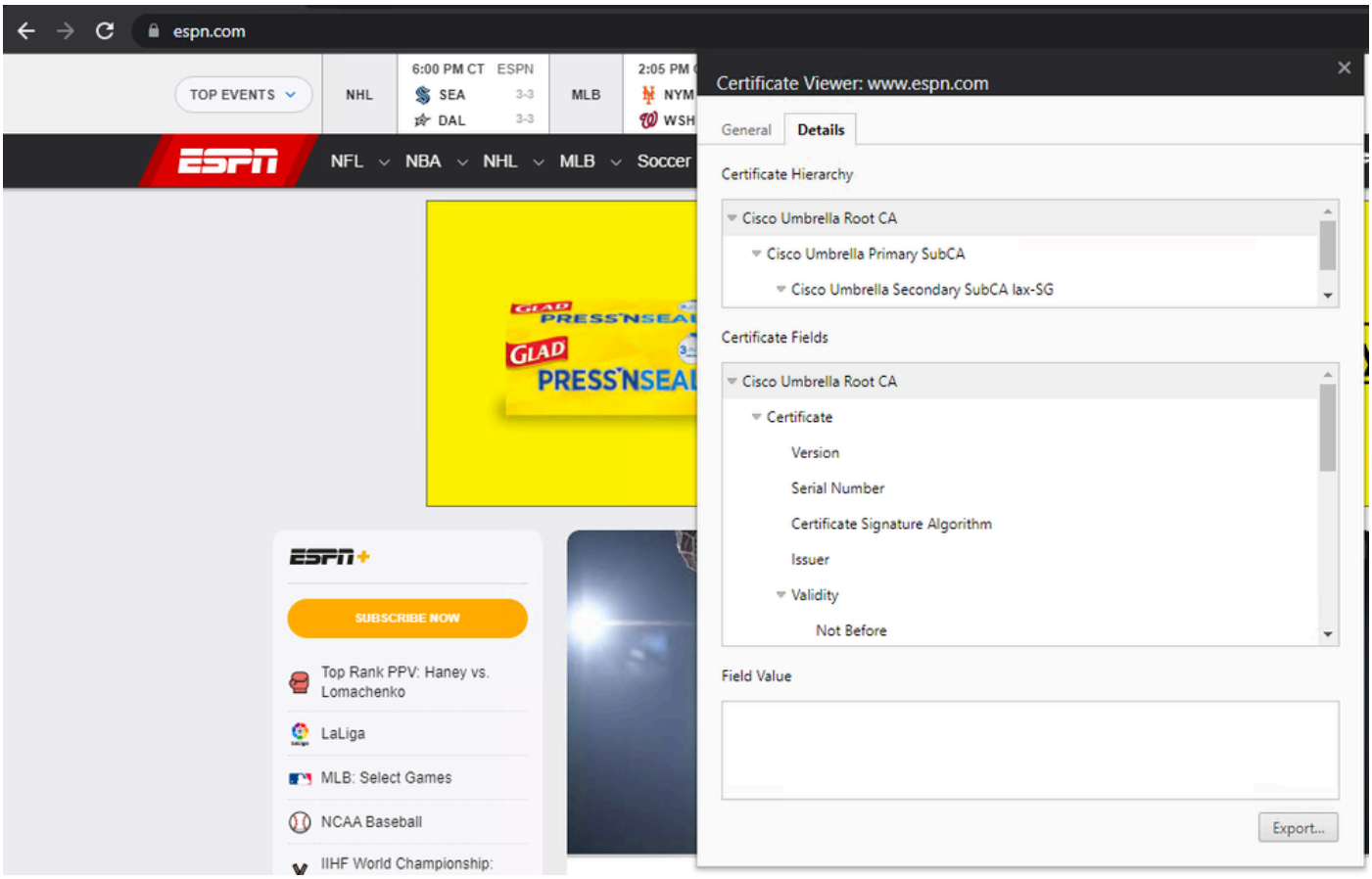


15670820980756

- 嘗試轉到不基於從PBR排除的應用程式的任何其他站點，並確保Umbrella確實正在代理連線：



附註：為了避免警告頁面不受信任的問題，請確保已安裝Umbrella根CA證書。



- 在FTD的CLI上，您可以執行幾個命令以確認組態是否正確推送且運作正常：
  - `show run route-map`（檢查PBR配置）：

```
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`（檢查PBR是否應用於正確的介面）

```
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(確`

認新增到ACL的域以便排除)

```
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)
```

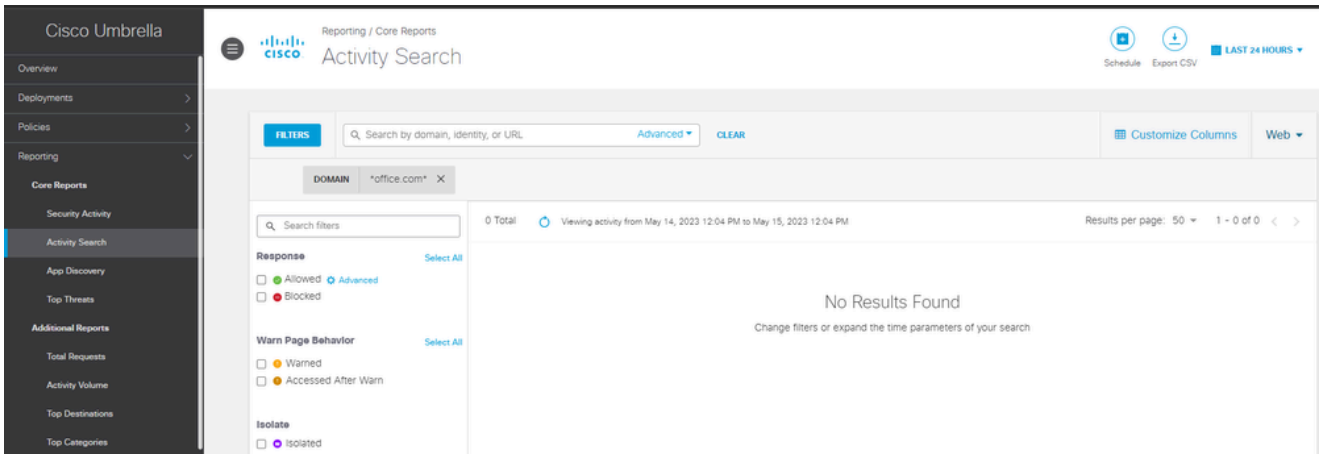
15670420887316

```
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#
```

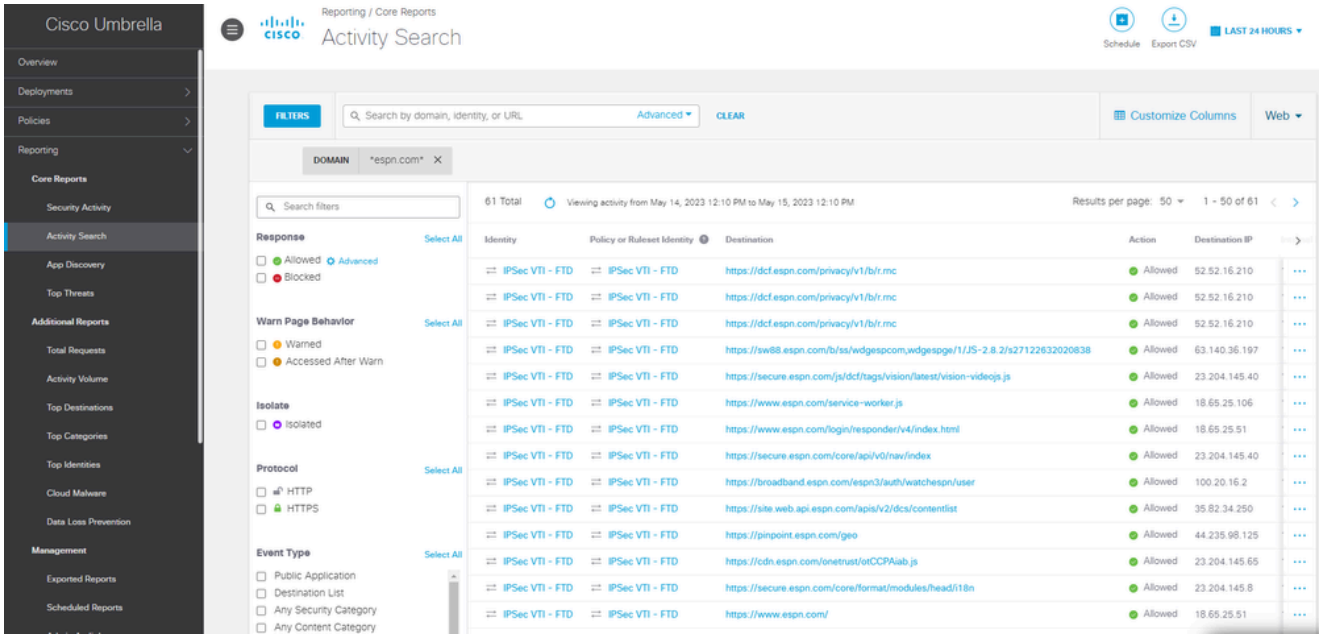
15670635784852

- `packet tracer input inside tcp 172.16.72.10 1234 fqdn office.com 443 detailed`（驗證外部介面是否用作輸出，而不是VTI介面）

- 在Umbrella Dashboard（Umbrella控制面板）的活動搜尋下，您可以看到轉到office.com的網路流量從未傳送到Umbrella，而轉到espn.com的網路流量則已傳送。



15671098042516



15671302832788

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。