Umbrella SIG用のFTDアプリケーションベースPBRの設定

内容

はじめに

このドキュメントでは、Umbrella SIGに対してファイアウォール脅威対策(FTD)アプリケーションベースのポリシーベースルーティング(PBR)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Umbrellaダッシュボードへのアクセス
- FTDバージョン7.1.0+に設定を展開するための、7.1.0+を実行するFMCへの管理アクセス。アプリケーションベースのPBRは、バージョン7.1.0以降でのみサポートされます
- （推奨）FMC/FTD設定とUmbrella SIGに関する知識
- （オプションですが、強くお勧めします）：包括ルート証明書がインストールされています。これは、トラフィックがプロキシまたはブロックされるときにSIGによって使用されます。ルート証明書のインストールの詳細については、Umbrellaのドキュメントを参照してください。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaセキュアインターネットゲートウェイ(SIG)に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

このドキュメントの情報は、UmbrellaへのSIG IPSec VTIトンネルを確立するときに、アプリケーションベースのPBRをFTDに導入する方法の設定手順を説明することを目的としています。これにより、PBRを使用するアプリケーションに基づいてVPN上のトラフィックを除外または包含できます。

この記事で説明する設定例では、VPN経由で他のすべてを送信しながら、IPSec VPNから特定のアプリケーションを除外する方法に焦点を当てています。

FMCのPBRについての詳細は、『シスコのドキュメント』を参照してください。

制限事項

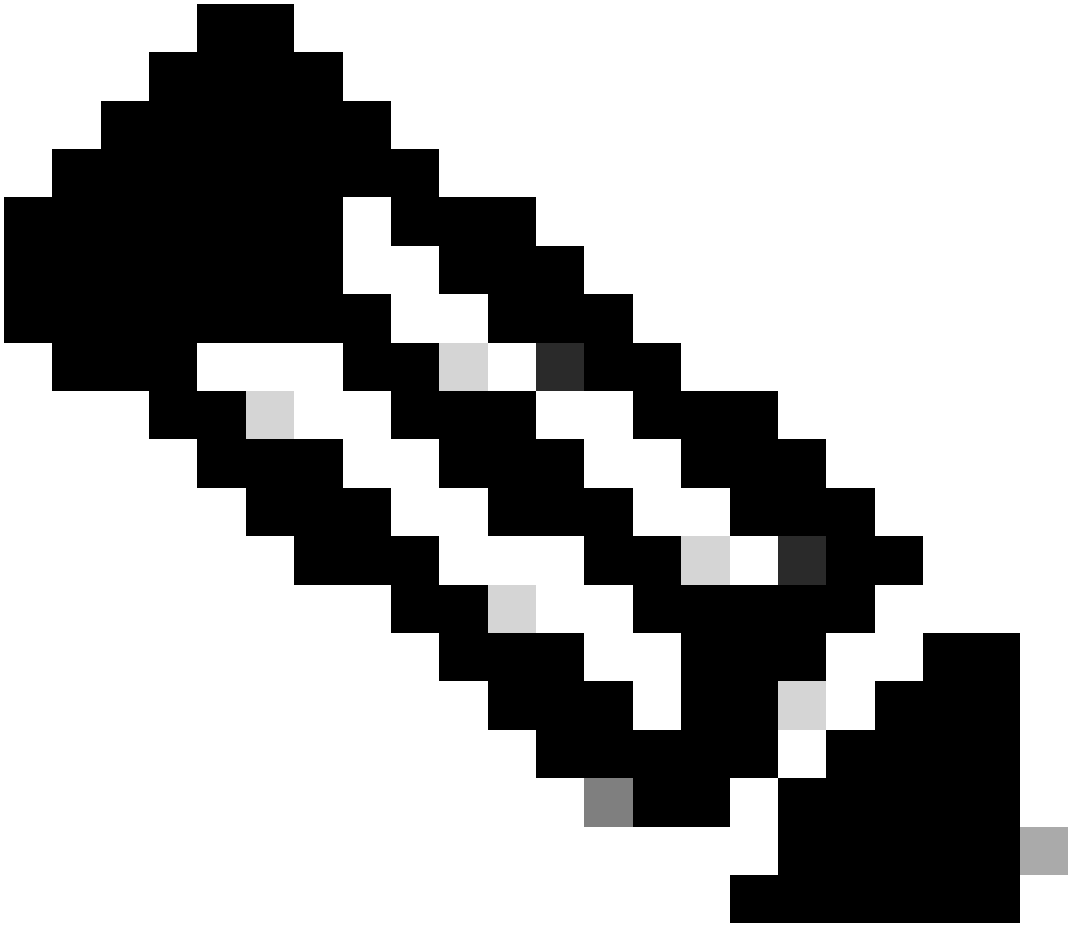
- ACEでアプリケーションアドレスと宛先アドレスの両方を定義することはできません。
- ポリシーー致基準のACLを定義するときに、定義済みアプリケーションのリストから複数のアプリケーションを選択して、アクセスコントロールエントリ(ACE)を形成できます。
  現在、定義済みアプリケーションリストに追加したり、定義済みアプリケーションリストを変更することはできません。
- FMCの定義済みアプリケーションリストに含まれていないアプリケーションや、アプリケーションに関する予期しない動作については、PBRのアプリケーションの代わりにIPを使用できます。
- 制限事項についての詳細は、PBRのドキュメントを参照してください。

アプリケーションベースのPBR

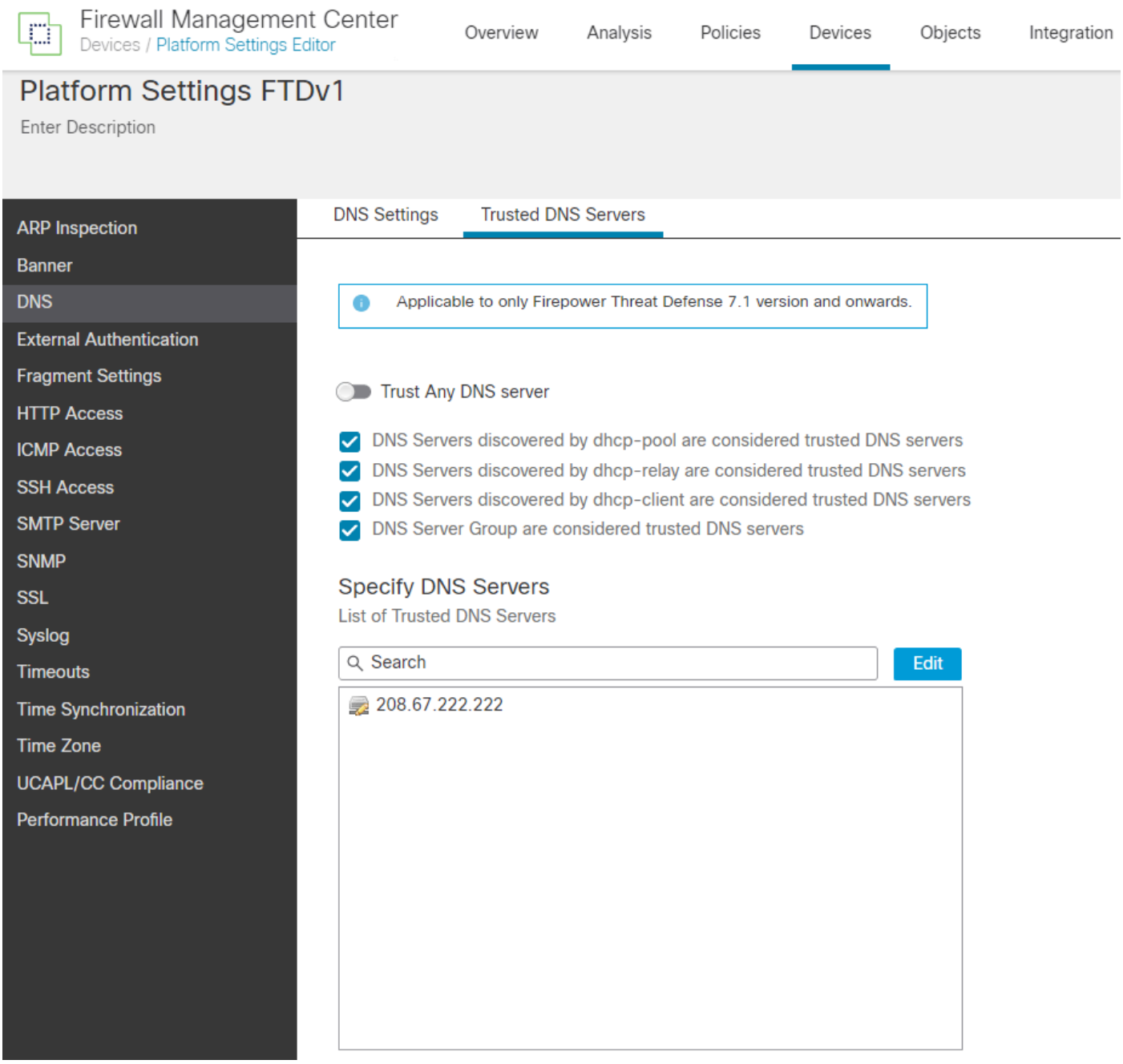
1. FMCとUmbrellaダッシュボードでIPsecトンネルを設定することから始めます。この設定の実行方法については、Umbrellaのドキュメントを参照してください。

2. FTDの背後にあるエンドユーザのデバイスが使用しているDNSサーバが、Devices > Platform Settings > DNS > Trusted DNS Serversの下に信頼できるDNSサーバとしてリストされていることを確認します。

リストにないDNSサーバをデバイスが使用している場合、DNSスヌーピングが失敗する可能性があるため、アプリケーションに基づくPBRは機能しません。オプションで（セキュリティ上の理由から推奨しません）、「Trust Any DNS server」をオンに切り替えてDNSサーバの追加が必要になるようにすることもできます。



注:VAを内部DNSリゾルバとして使用する場合、VAを信頼できるDNSサーバとして追加する必要があります。



15669097907860

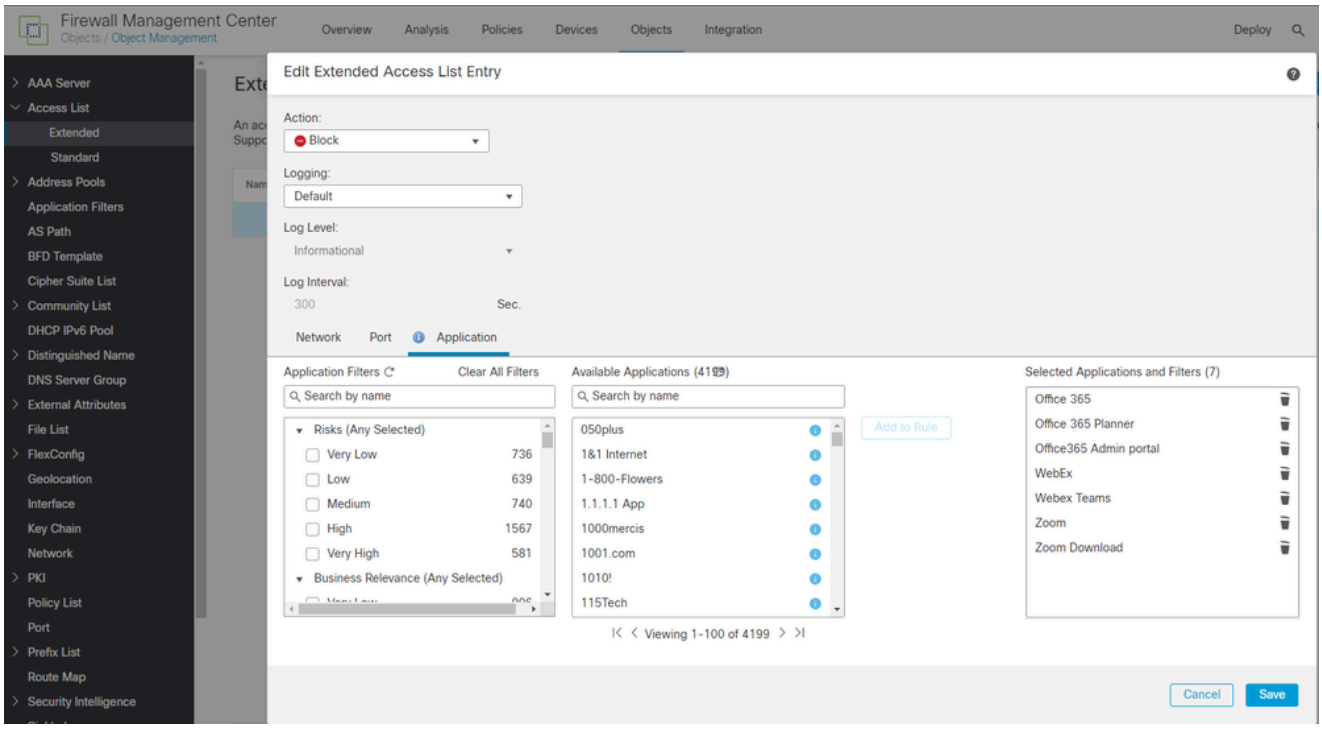
3. トラフィックがSIGのためにUmbrellaに送信されるのか、またはトラフィックがIPSecから除外され、Umbrellaにまったく送信されないのかを判断するためにPBRプロセス用にFTDで使用できる拡張ACLを作成します。

- ACLのdeny ACEは、トラフィックがSIGから除外されることを意味します。
- ACLのpermit ACEは、トラフィックがIPSec経由で送信され、SIGポリシー（CDFW、SWGなど）を適用できることを意味します。

この例では、アプリケーション「Office365」、「Zoom」、および「Cisco Webex」をdeny ACEで除外しています。残りのトラフィックは、さらに検査するためにUmbrellaに送信されます。

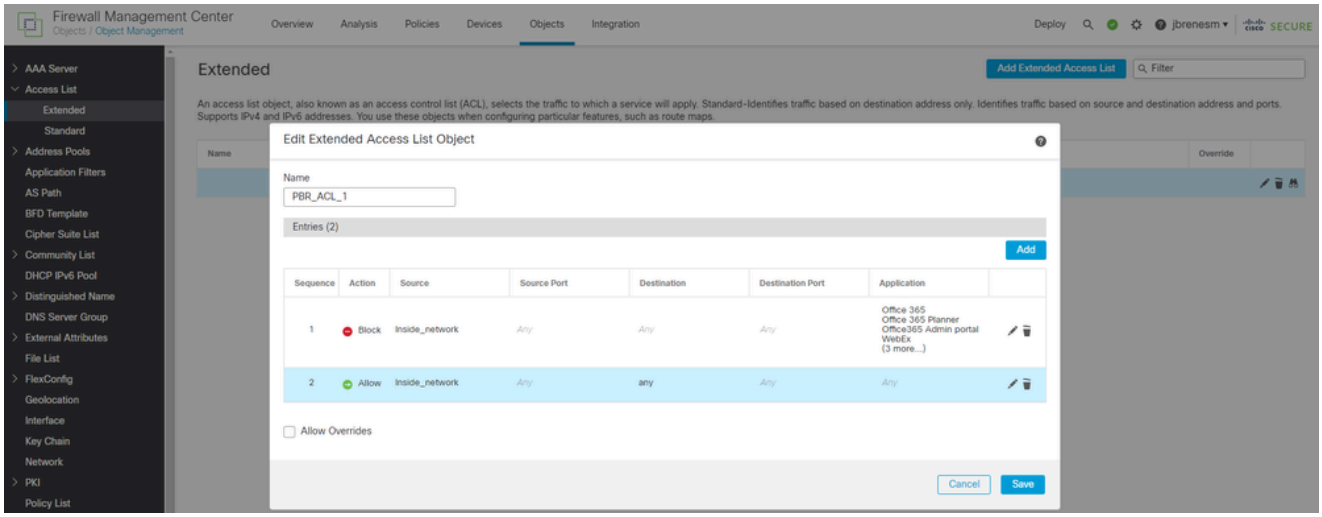
1. Object > Object Management > Access List > Extendedの順に選択します。
2. 通常どおりに送信元ネットワークとポートを定義し、PBRに参加するアプリケーションを追

加します。



15669947000852

最初のACEでは前述のアプリケーションを「拒否」でき、2番目のACEでは残りのトラフィックをIPsec経由で送信する許可を指定できます。

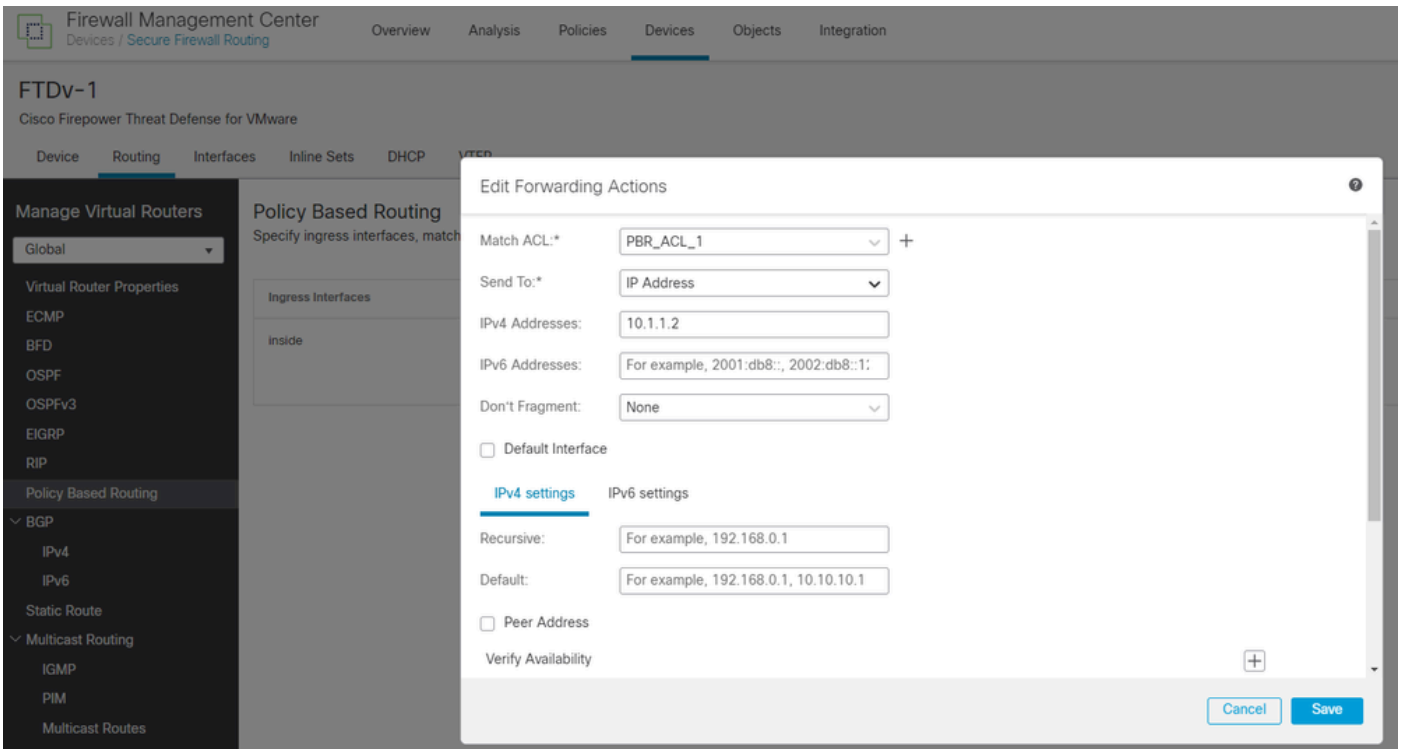


15670006987156

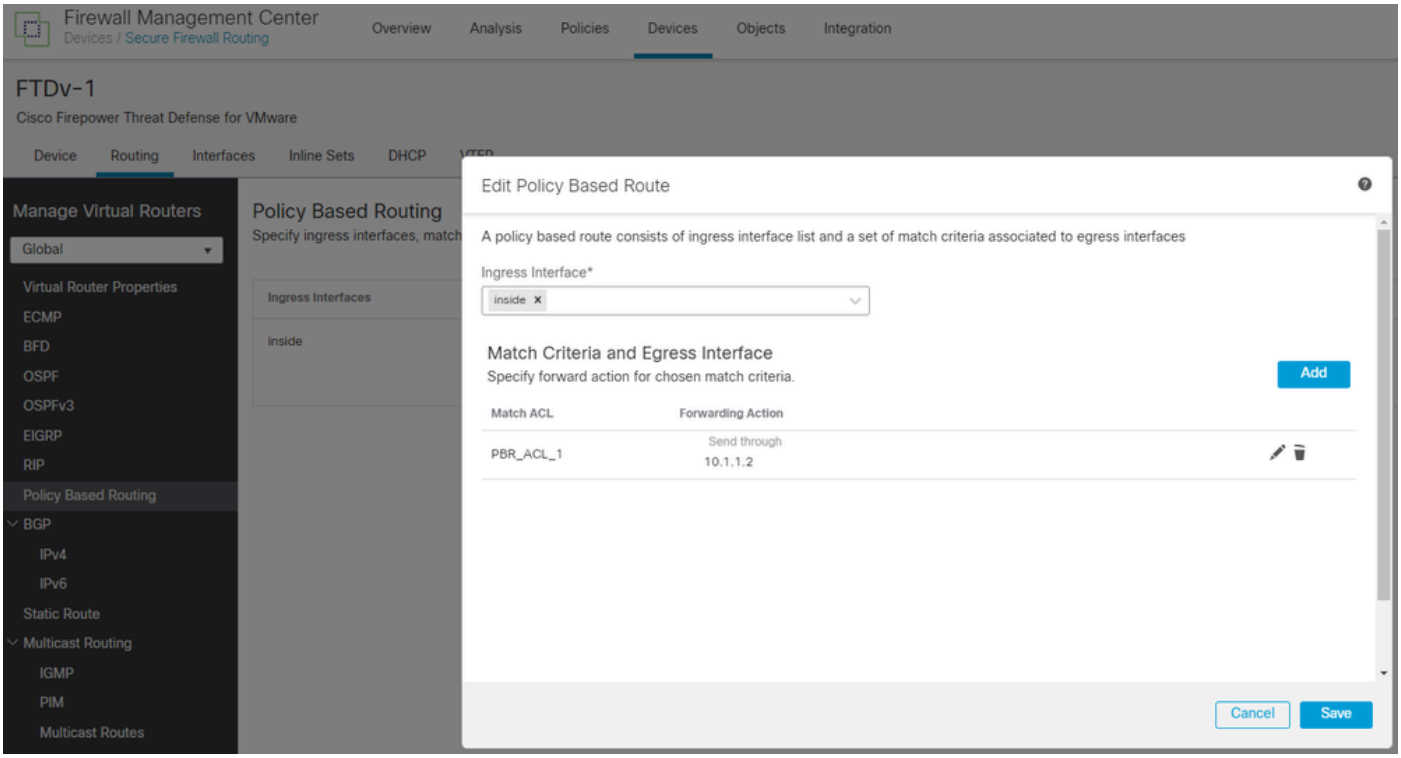
4. Devices > Device Management > [select the FTD Device] > Routing > Policy Based Routingの順に選択し、PBRを作成します。

- 入力インターフェイス：ローカルトラフィックの送信元のインターフェイス。
- 一致するACL：前の手順で作成した拡張ACL、ACL「PBR_ACL_1」
- 送信先：IPアドレス
- IPv4アドレス：PBRがpermit文を検出した場合のネクストホップ。トラフィックはここで追加したIPにルーティングされます。この例では、これはUmbrellaのIPsec IPです。VTI

VPNのIPが10.1.1.1の場合、UmbrellaのIPsec IPはその同じネットワーク内の任意のアドレス（10.1.1.2など）になります。



15670209158036



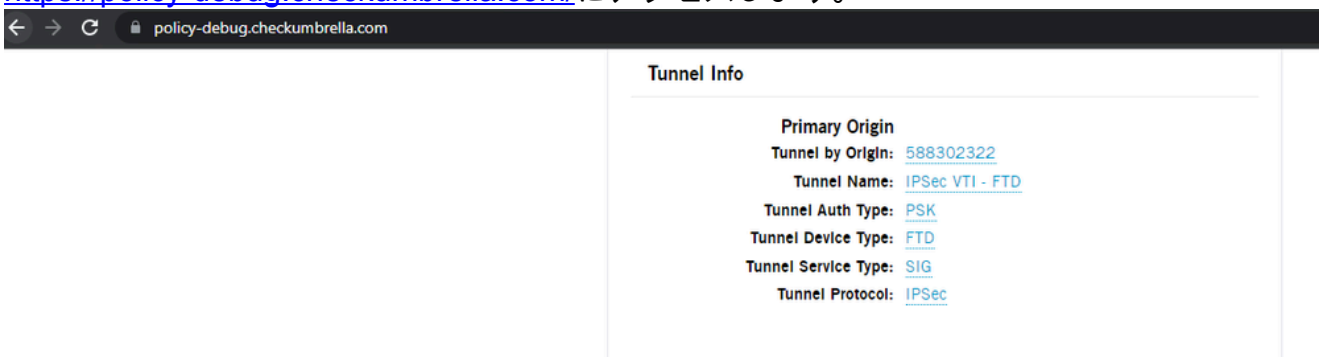
15670247521556

5. FMCに変更を展開します。

検証

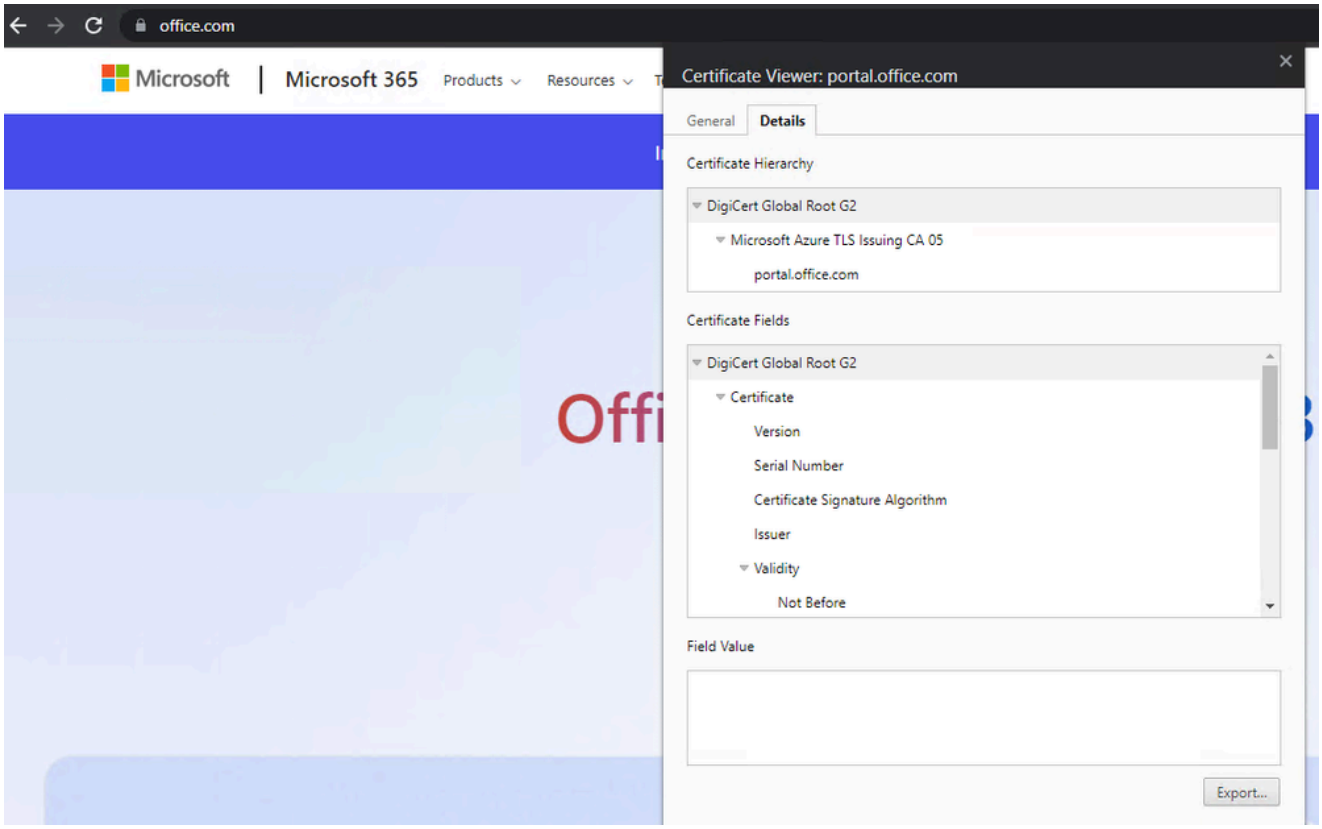
FTDの背後にあるテスト用PCで、次の項目を確認します。

- PCからのトラフィックは、実際にはIPSec経由でUmbrellaに送信されています。https://policy-debug.checkumbrella.com/にアクセスします。



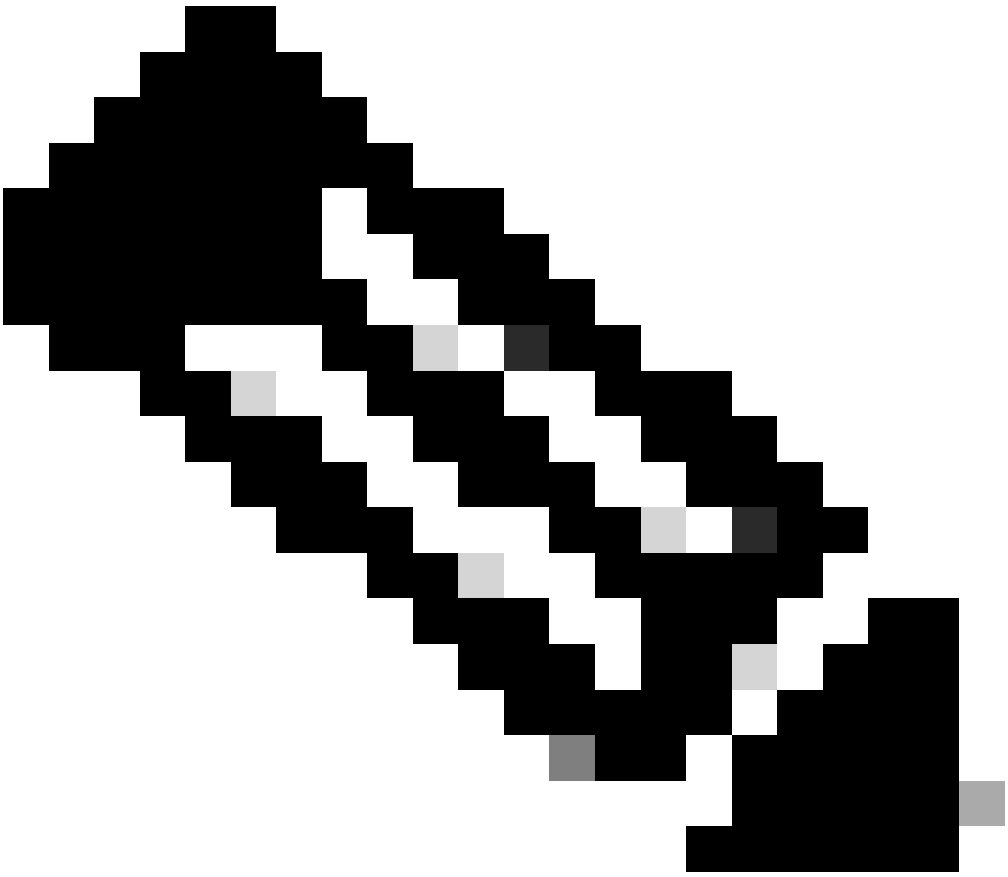
15670737148948

- PBR/ACL設定で除外されているサイトのいずれかに移動し、UmbrellaルートCAが表示されないこと、つまり接続がプロキシされていないことを確認します。

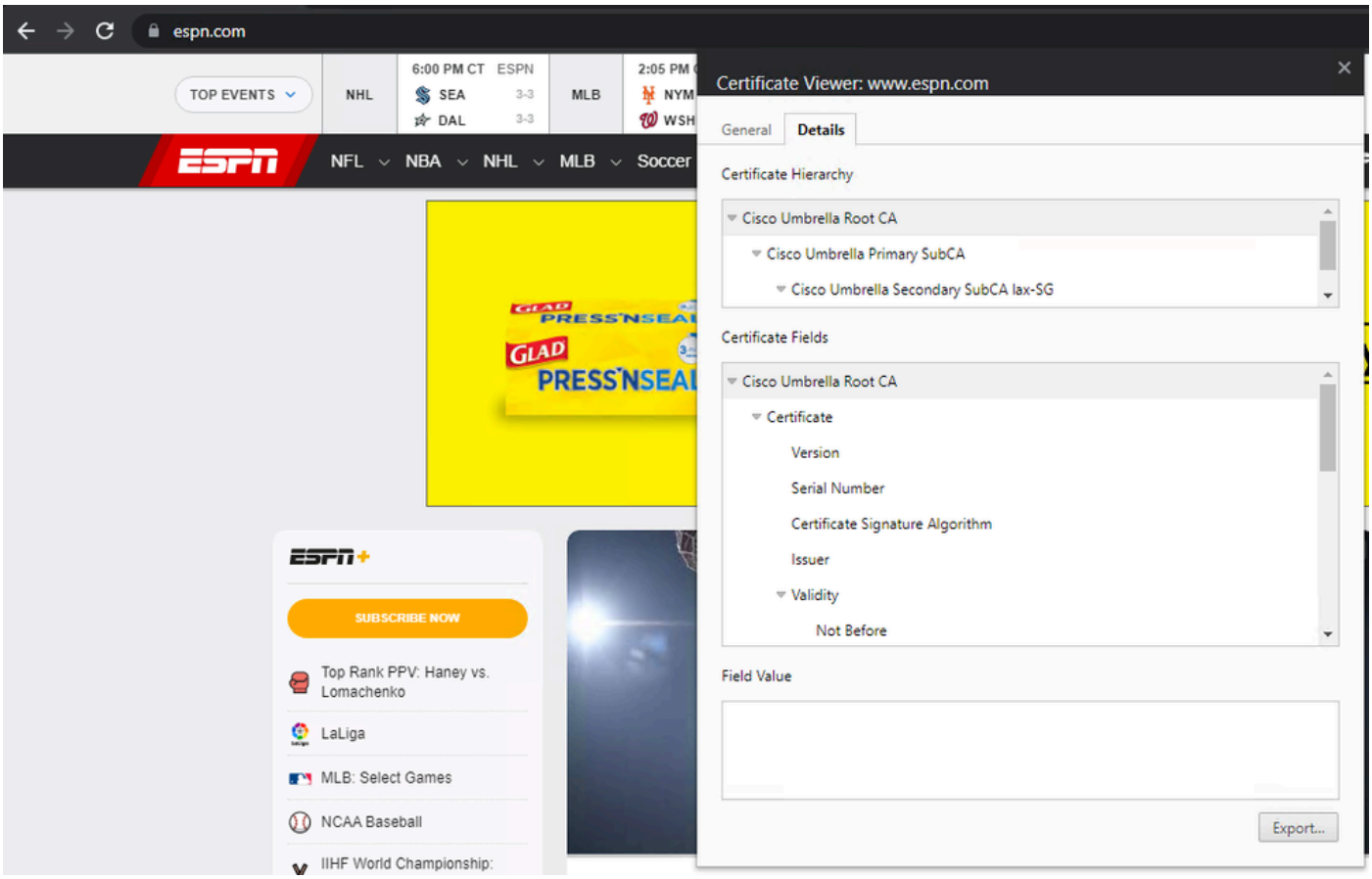


15670820980756

- PBRから除外されたアプリケーションに基づかない他のサイトに移動し、Umbrellaが実際に接続をプロキシしていることを確認します。



注：信頼できない警告ページに関する問題を回避するには、UmbrellaルートCA証明書がインストールされていることを確認します。



- FTDのCLIで、いくつかのコマンドを実行して、設定が正しくプッシュされて動作していることを確認できます。
  - `show run route-map`（PBR設定をチェックします）：

```
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`（PBRが適切なインターフェイスに適用されていることを確認します）

```
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`（除外のためにACLに追加されたドメインを確認する）

```
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)
```

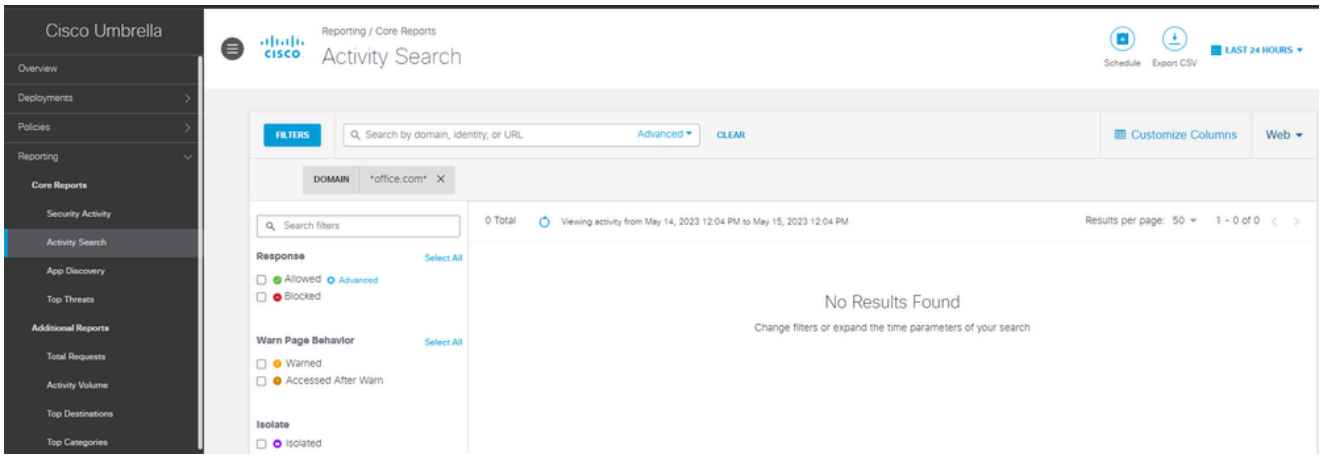
15670420887316

```
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#
```

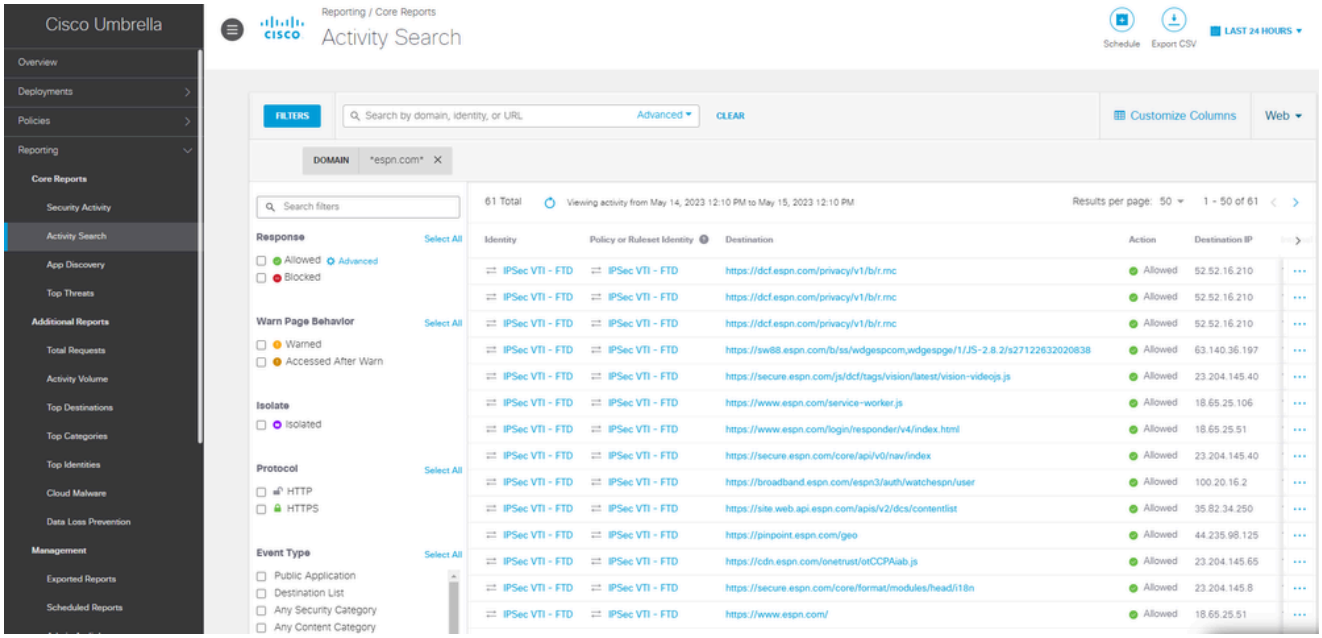
15670635784852

- `packet-tracer input inside tcp 172.16.72.10 1234 fqdn office.com 443 detailed`（VTIインターフェイスではなく、外部インターフェイスが出力として使用されることを確認）

- Umbrellaダッシュボードのアクティビティ検索で、office.com宛てのWebトラフィックはUmbrellaに送信されず、espn.com宛てのトラフィックは送信されたことを確認できます。



15671098042516



15671302832788

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。