为Umbrella SIG配置基于应用的FTD PBR

目录

简介

本文档介绍如何为Umbrella SIG配置防火墙威胁防御(FTD)基于应用的策略路由(PBR)。

先决条件

要求

Cisco 建议您了解以下主题：

- 访问Umbrella控制面板
- 对运行7.1.0+的FMC的管理员访问权限，以便将配置部署到FTD版本7.1.0+。基于应用的PBR仅在7.1.0版及更高版本上受支持
- （首选）了解FMC/FTD配置和Umbrella SIG
- （可选，但强烈推荐）：Umbrella Root Certificate已安装，SIG会在代理或阻止流量时使用此证书。有关根证书安装的更多详细信息，请参阅Umbrella文档。

使用的组件

本文档中的信息基于Cisco Umbrella安全互联网网关(SIG)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

本文档中的信息旨在介绍在向Umbrella建立SIG IPsec VTI隧道时，如何在FTD上部署基于应用的PBR的配置步骤，以便您可以排除或包含基于使用PBR的应用的VPN上的流量。

本文中描述的配置示例重点介绍如何在通过VPN发送其他内容时从IPsec VPN中排除某些应用。

有关FMC上的PBR的完整信息，请参阅Cisco文档。

限制

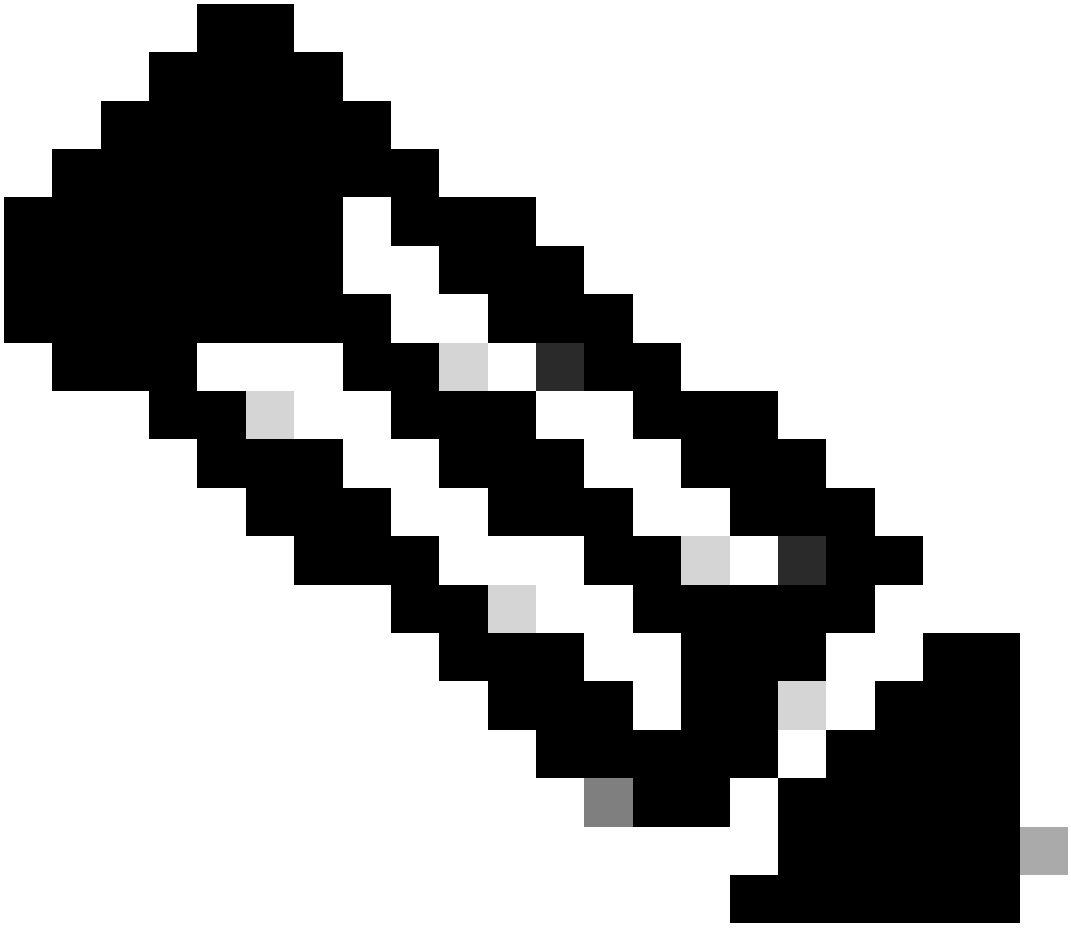
- 不能在ACE中同时定义应用程序和目标地址。
- 在为策略匹配条件定义ACL时，您可以从预定义应用列表中选择多个应用，以形成访问控制条目(ACE)。
  目前，您无法添加或修改预定义的应用列表。
- 对于未列在FMC上的预定义应用列表中的那些应用或应用的任何意外行为，可以使用IP代替PBR中的应用。
- 有关全部限制的列表，请参考PBR的文档。

基于应用的PBR

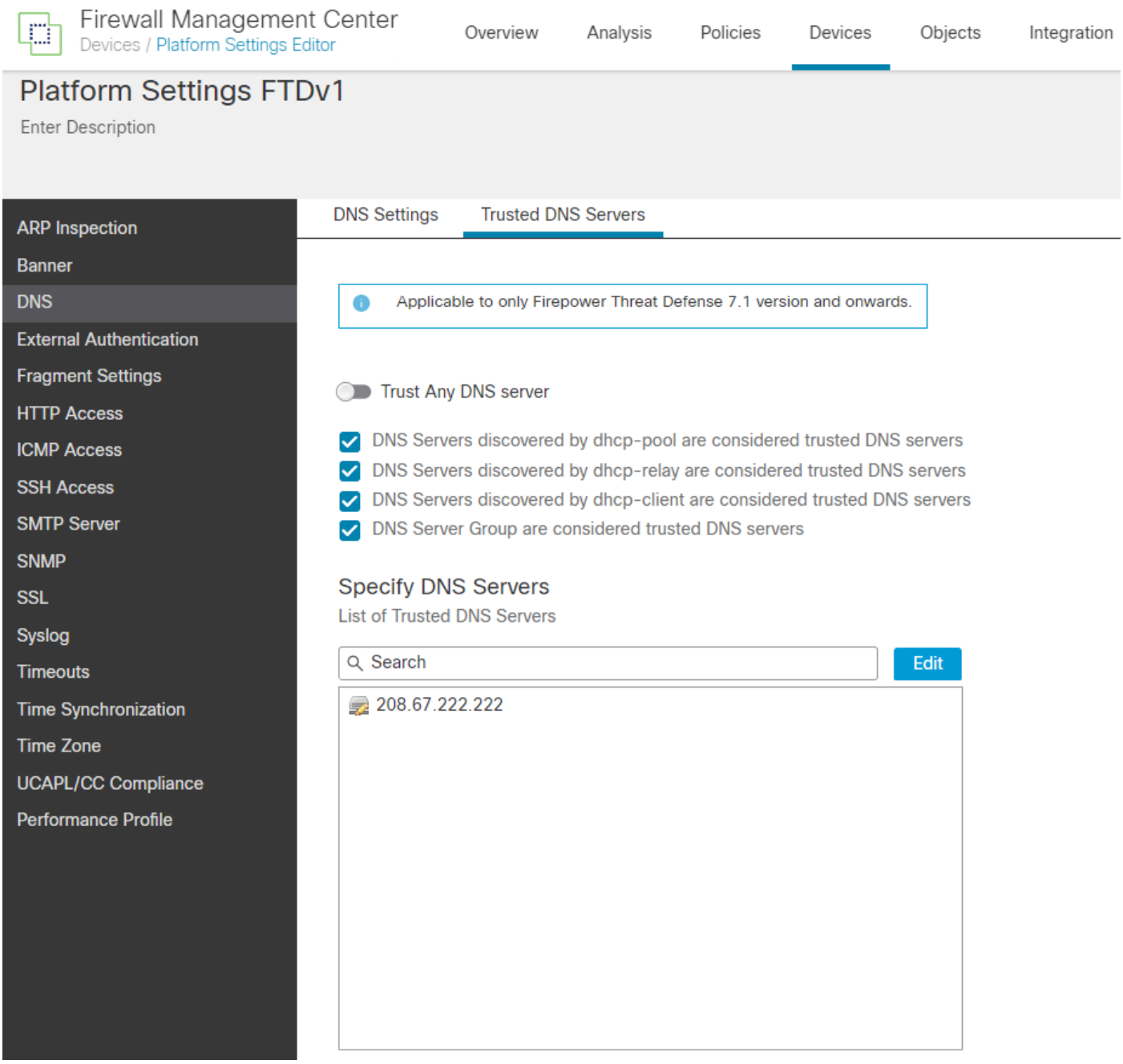
1.首先在FMC和Umbrella Dashboard上配置IPsec隧道。有关如何执行此配置的说明，请参阅Umbrella文档。

2.确保FTD后面的最终用户的设备所使用的DNS服务器在Devices > Platform Settings > DNS > Trusted DNS Servers下列为受信任DNS服务器。

如果设备使用未列出的DNS服务器，则DNS监听可能失败，因此基于应用的PBR无法工作。或者（出于安全原因不建议使用），您可以切换Trust Any DNS server，以便需要添加DNS服务器。



注意：如果VA用作内部DNS解析器，则必须将其添加为受信任DNS服务器。



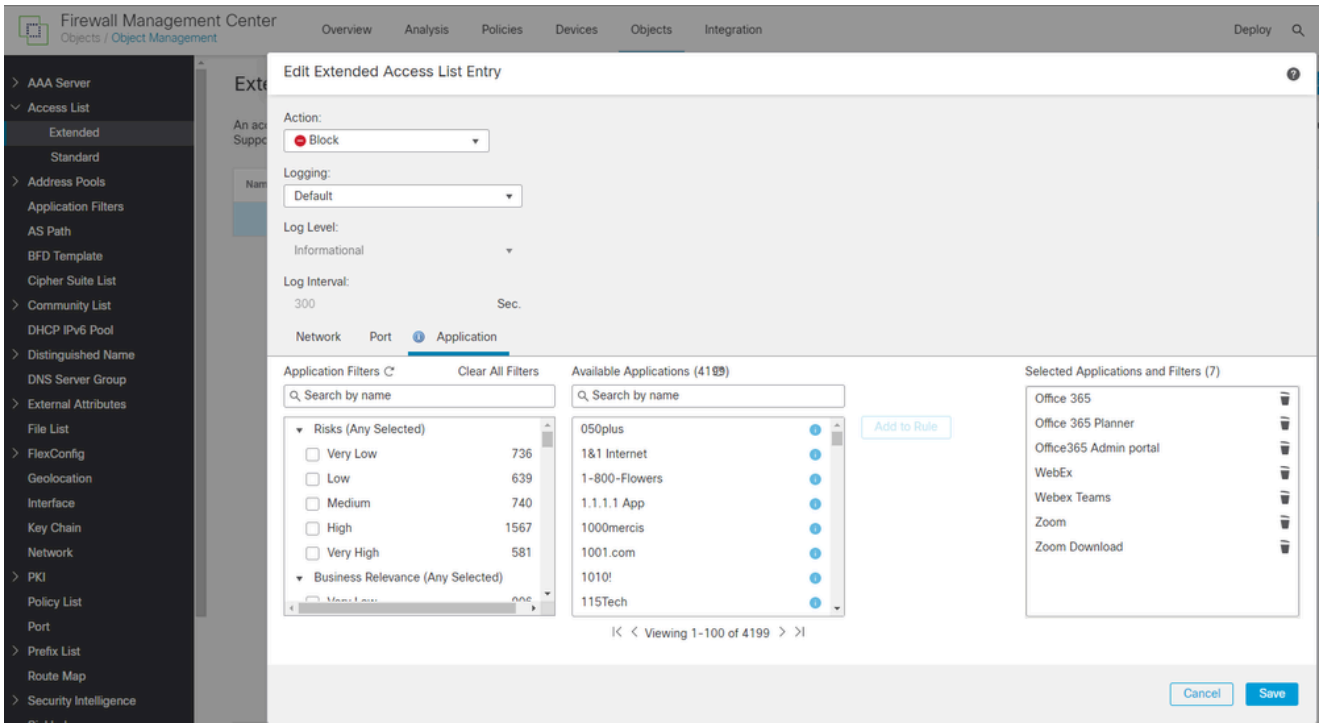
15669097907860

3.创建扩展ACL，FTD可将其用于PBR进程，以便决定流量是发送到Umbrella for SIG，还是从IPsec中排除，而根本未发送到Umbrella。

- ACL上的deny ACE表示流量从SIG中排除。
- ACL上的permit ACE表示流量通过IPsec发送，并且可以应用SIG策略（CDFW、SWG等）。

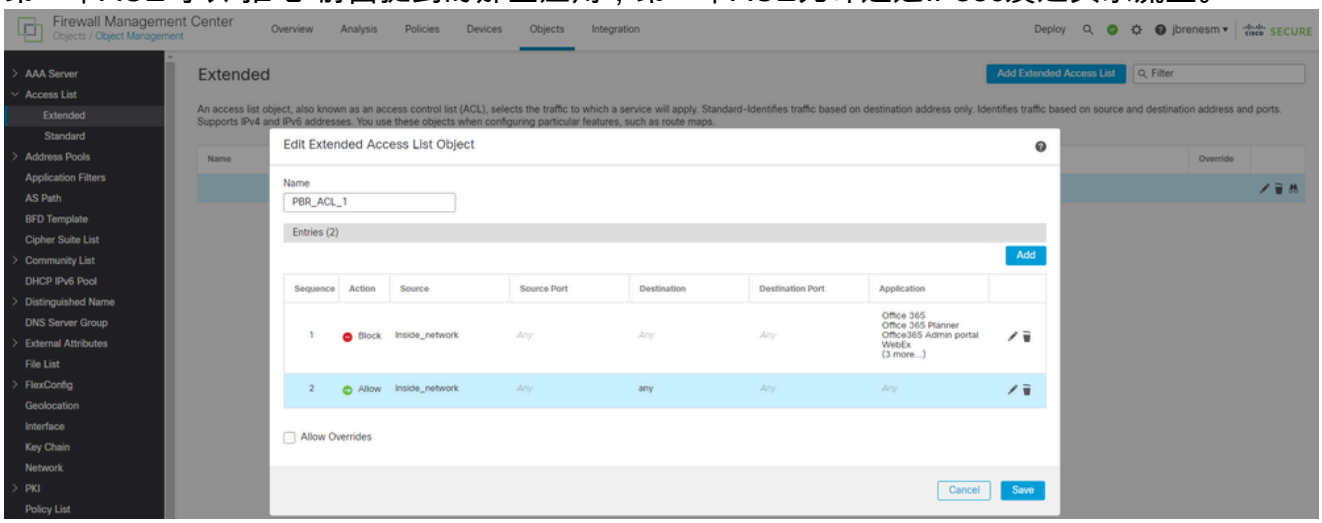
此示例不包括带拒绝ACE的应用“Office365”、“Zoom”和“Cisco Webex”。其余流量将发送到Umbrella进行进一步检查。

1. 转至Object > Object Management > Access List > Extended。
2. 按照正常方式定义源网络和端口，然后添加要参与PBR的应用。



15669947000852

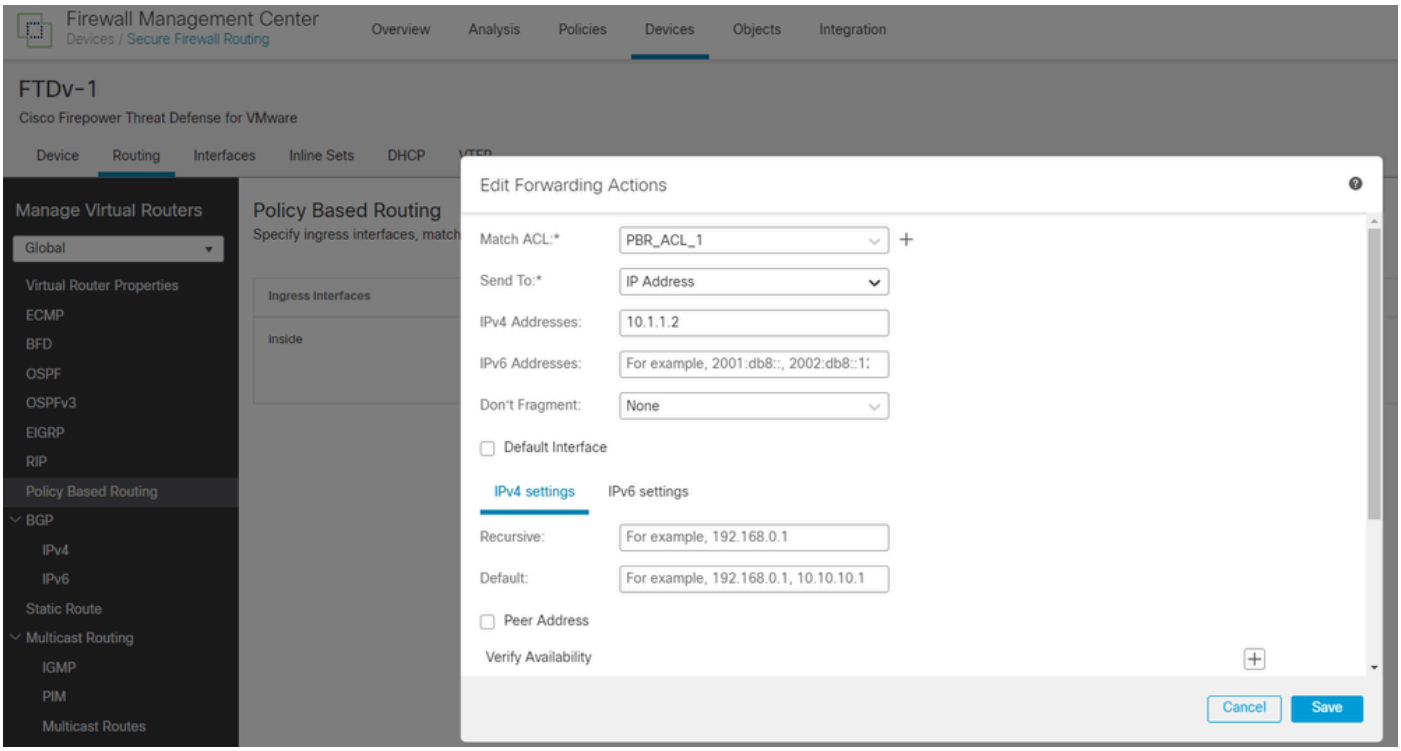
第一个ACE可以“拒绝”前面提到的那些应用，第二个ACE允许通过IPsec发送其余流量。



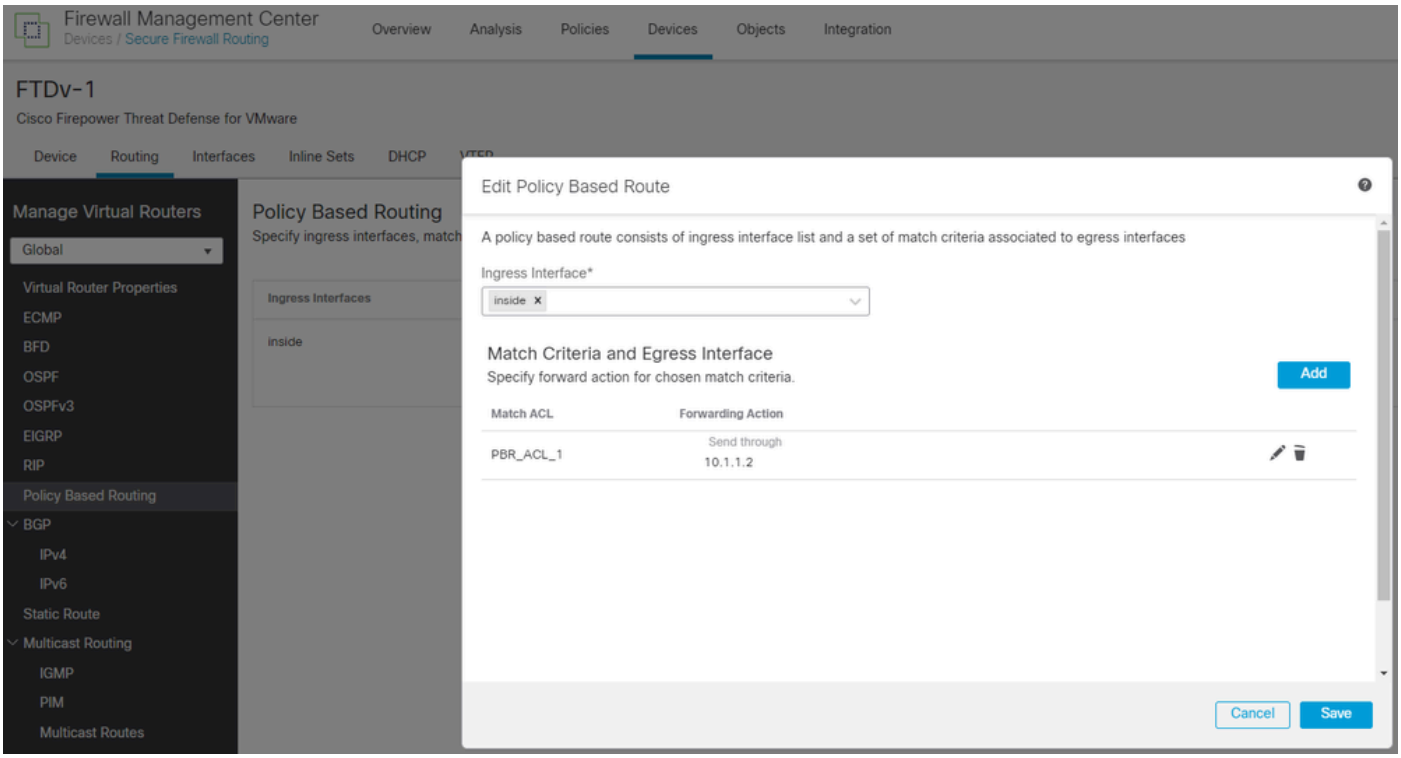
15670006987156

4.在Devices > Device Management > [选择FTD Device] > Routing > Policy Based Routing下创建PBR。

- Ingress 接口:本地流量来自的接口。
- 匹配的ACL:在上一步骤中创建的扩展ACL“PBR_ACL_1”。
- 发送至:IP Address
- IPv4地址：PBR找到permit语句时的下一跳，因此流量将路由到您在此处添加的IP。在本示例中，这是Umbrella的IPsec IP。如果您的VTI VPN的IP是10.1.1.1，则Umbrella的IPsec IP将是同一网络内的任何内容（例如10.1.1.2）。



15670209158036



15670247521556

5.在FMC上部署更改。

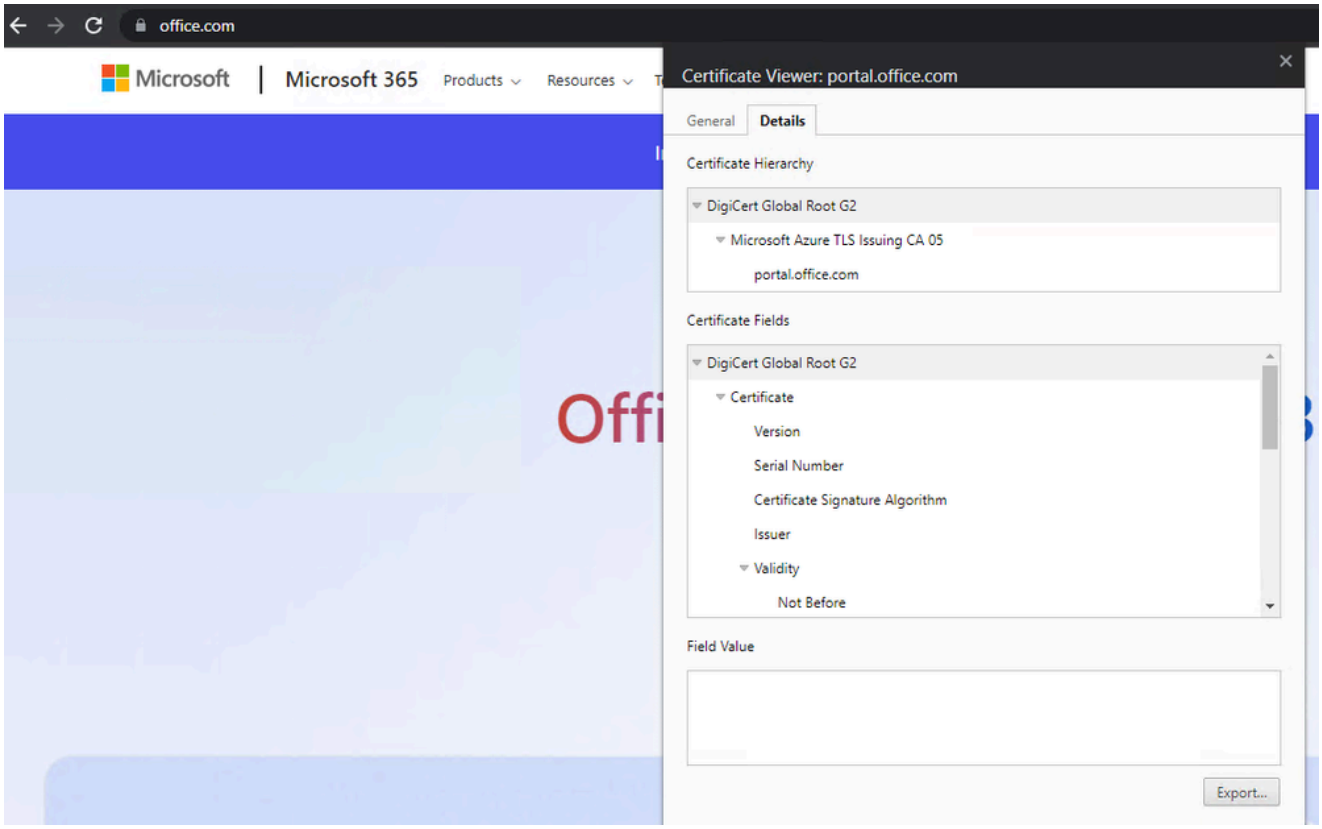
确认

在位于FTD后面的测试PC上，检查：

- 来自PC的流量实际上通过IPsec发送到Umbrella。
  转到:https://policy-debug.checkumbrella.com/

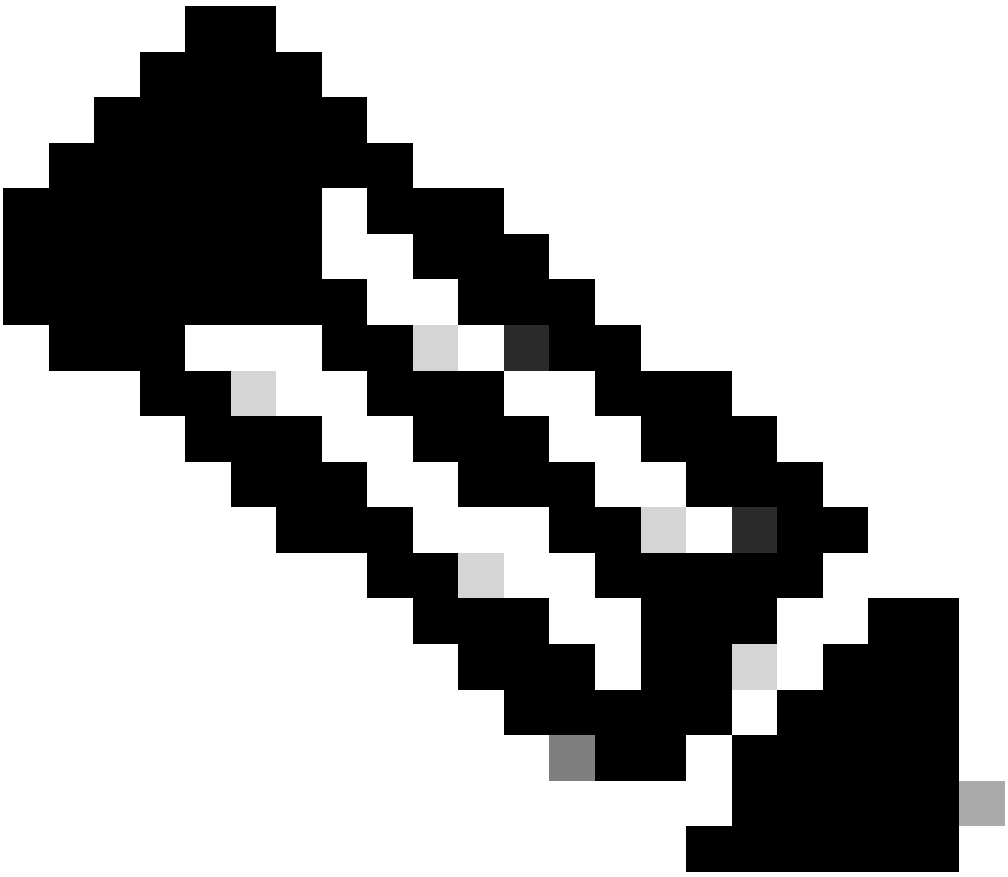
15670737148948

- 尝试转到PBR/ACL配置中排除的任何站点，并确保未显示Umbrella Root CA，这意味着未代理连接：

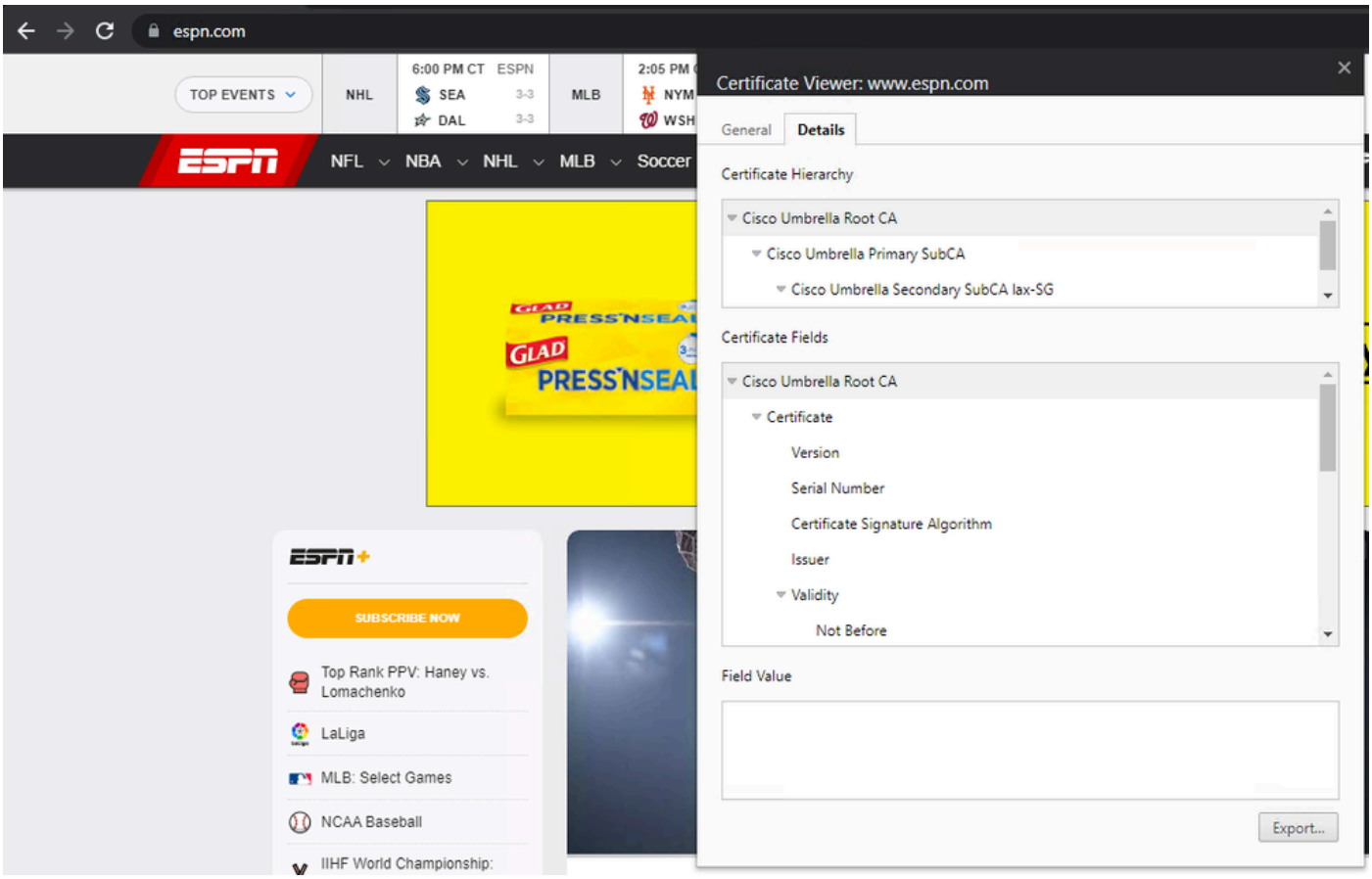


15670820980756

- 尝试访问不基于PBR排除的应用的任何其他站点，并确保Umbrella确实代理了连接：



注意：为了避免警告页面不受信任的问题，请确保已安装Umbrella Root CA证书。



- 在FTD的CLI上，您可以运行几个命令来确认配置已正确推送且工作正常：
  - `show run route-map`（检查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`（检查PBR是否已应用到正确的接口）

```
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`(确认添加到

ACL的域以排除)

```
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)
```

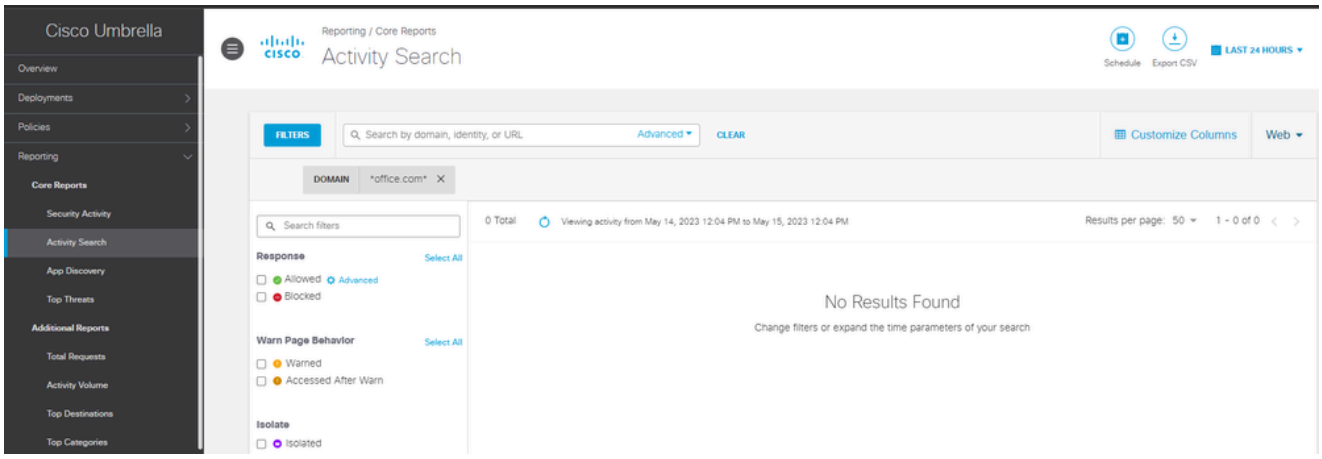
15670420887316

```
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#
```

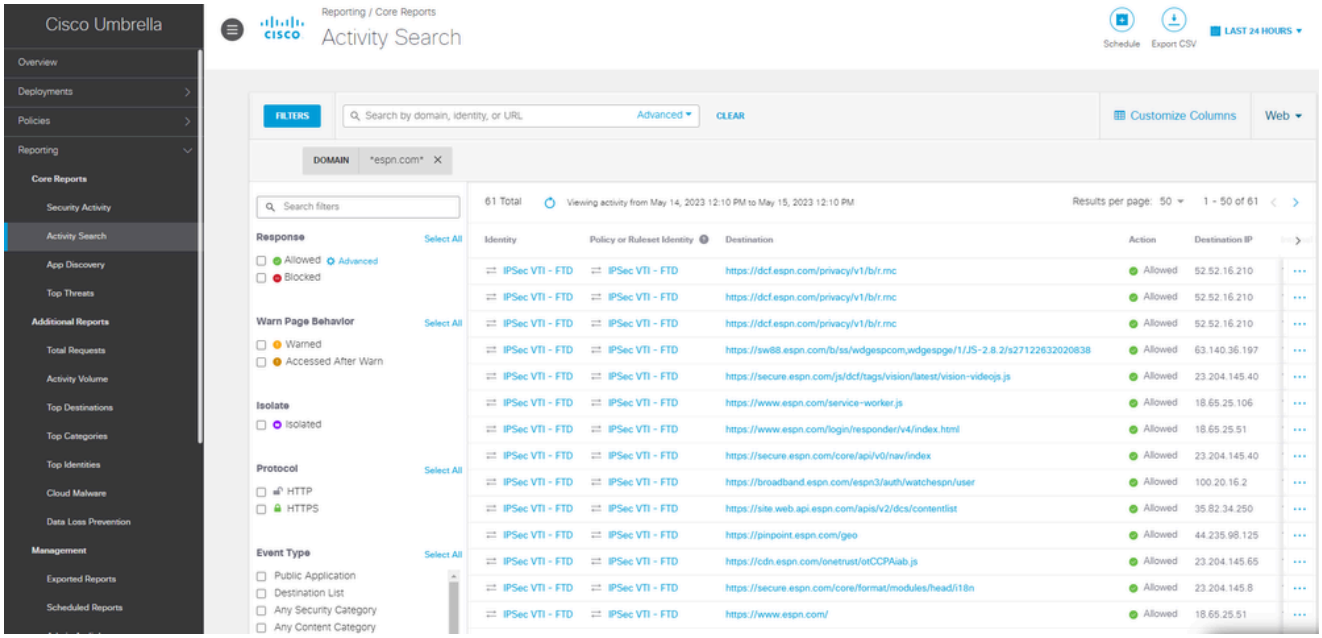
15670635784852

- packet-tracer input inside tcp 172.16.72.10 1234 fqdn office.com 443 detailed(验证外部接口是否用作输出，而不是VTI接口)

- 在Umbrella Dashboard（Umbrella控制面板）的活动搜索下，您可以看到转到office.com的网络流量从未发送到Umbrella，而转到espn.com的网络流量发送了。



15671098042516



15671302832788

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。