Umbrella SIG에 대한 FTD 애플리케이션 기반 PBR 구성

목차

소개

이 문서에서는 Umbrella SIG에 대해 FTD(Firewall Threat Defense) PBR(application-based policy based routing)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Umbrella 대시보드 액세스
- 7.1.0 이상을 실행하는 FMC에 대한 관리자 액세스를 통해 FTD 버전 7.1.0 이상에 컨피그레이션을 구축합니다. 앱 기반 PBR은 버전 7.1.0 이상에서만 지원됩니다
- (권장) FMC/FTD 컨피그레이션 및 Umbrella SIG에 대한 지식
- (선택 사항이지만 매우 권장): Umbrella Root Certificate가 설치되면 트래픽이 프록시되거나 차단될 때 SIG에서 사용됩니다. 루트 인증서 설치에 대한 자세한 내용은 Umbrella 설명서에서 자세히 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella SIG(Secure Internet Gateway)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

이 문서의 정보는 Umbrella에 대한 SIG IPsec VTI 터널을 설정할 때 FTD에 애플리케이션 기반 PBR을 구축하는 방법에 대한 컨피그레이션 단계를 다룹니다. 따라서 PBR을 사용하는 애플리케이션을 기반으로 VPN에서 트래픽을 제외하거나 포함할 수 있습니다.

이 문서에서 설명하는 컨피그레이션 예는 VPN을 통해 다른 모든 것을 전송하면서 특정 애플리케이션을 IPsec VPN에서 제외하는 방법에 초점을 맞추고 있습니다.

FMC의 PBR에 대한 자세한 내용은 Cisco 설명서를 참조하십시오.

제한 사항

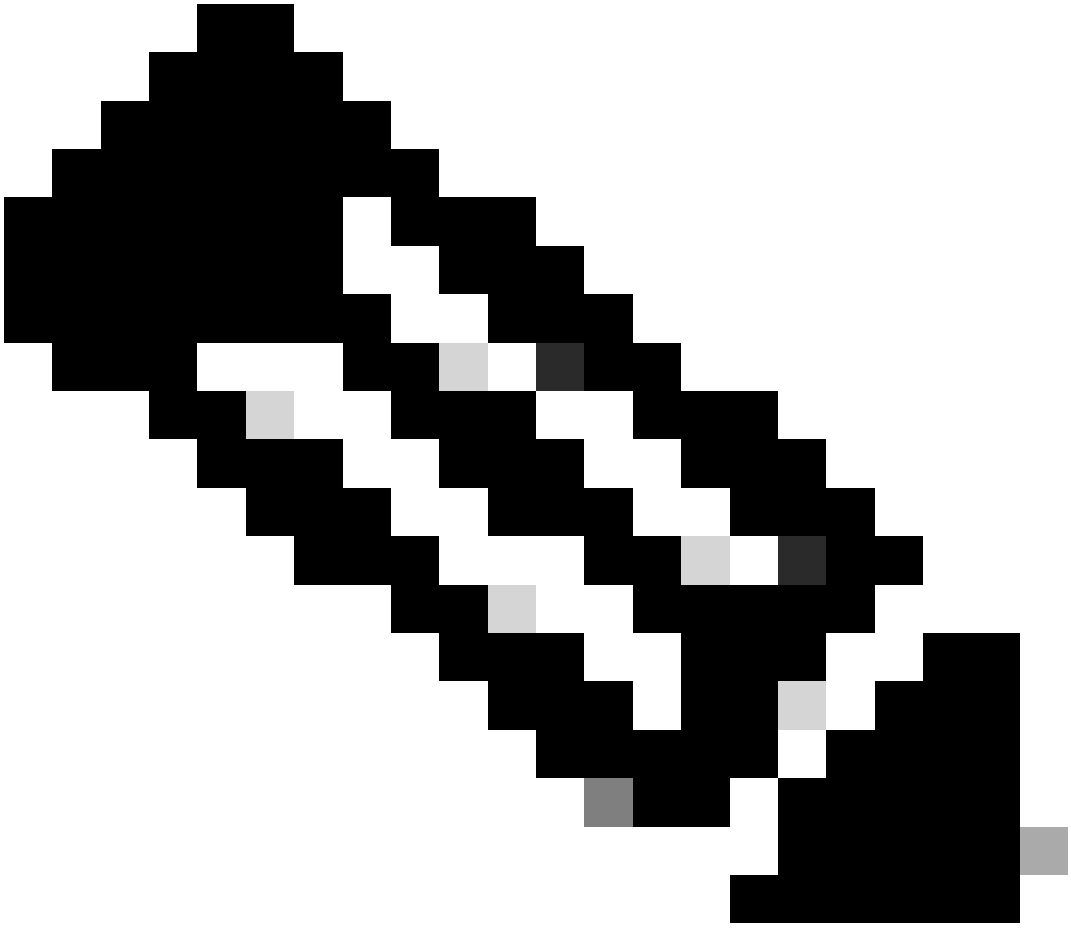
- ACE에 애플리케이션 주소와 목적지 주소를 모두 정의할 수는 없습니다.
- 정책 일치 기준에 대한 ACL을 정의하는 동안 미리 정의된 애플리케이션 목록에서 여러 애플리케이션을 선택하여 ACE(Access Control Entry)를 구성할 수 있습니다.
  현재 사전 정의된 애플리케이션 목록에 추가하거나 수정할 수 없습니다.
- FMC의 미리 정의된 애플리케이션 목록에 나열되지 않은 애플리케이션이나 애플리케이션의 예기치 않은 동작에 대해서는 PBR의 애플리케이션 대신 IP를 사용할 수 있습니다.
- 전체 제한 사항의 목록은 PBR 설명서를 참조하십시오.

애플리케이션 기반 PBR

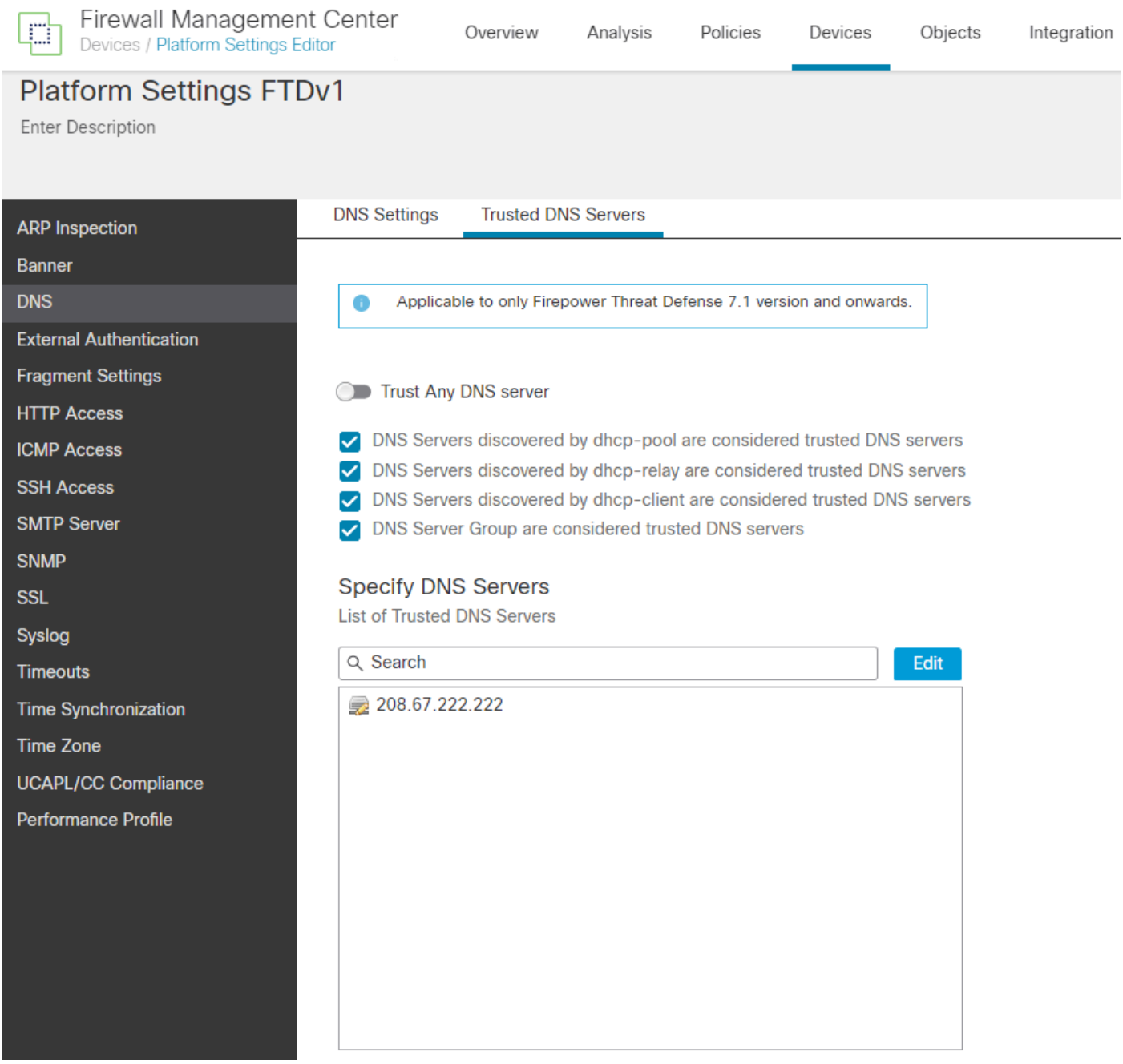
1. FMC와 Umbrella Dashboard에서 IPsec 터널을 구성합니다. 이 컨피그레이션을 수행하는 방법에 대한 지침은 Umbrella 설명서에서 확인할 수 있습니다.

2. FTD 뒤에 있는 최종 사용자의 장치가 사용 중인 DNS 서버가 Devices(장치) > Platform Settings(플랫폼 설정) > DNS > Trusted DNS Servers(신뢰할 수 있는 DNS 서버)에서 신뢰할 수 있는 DNS 서버로 나열되어 있는지 확인합니다.

디바이스가 나열되지 않은 DNS 서버를 사용하는 경우 DNS 스누핑이 실패할 수 있으므로 앱 기반 PBR이 작동하지 않습니다. 선택적으로(보안상의 이유로 권장되지 않음) Trust Any DNS 서버를 토글하여 DNS 서버를 추가해야 합니다.



참고: VA가 내부 DNS 확인자로 사용되는 경우 신뢰할 수 있는 DNS 서버로 추가해야 합니다.



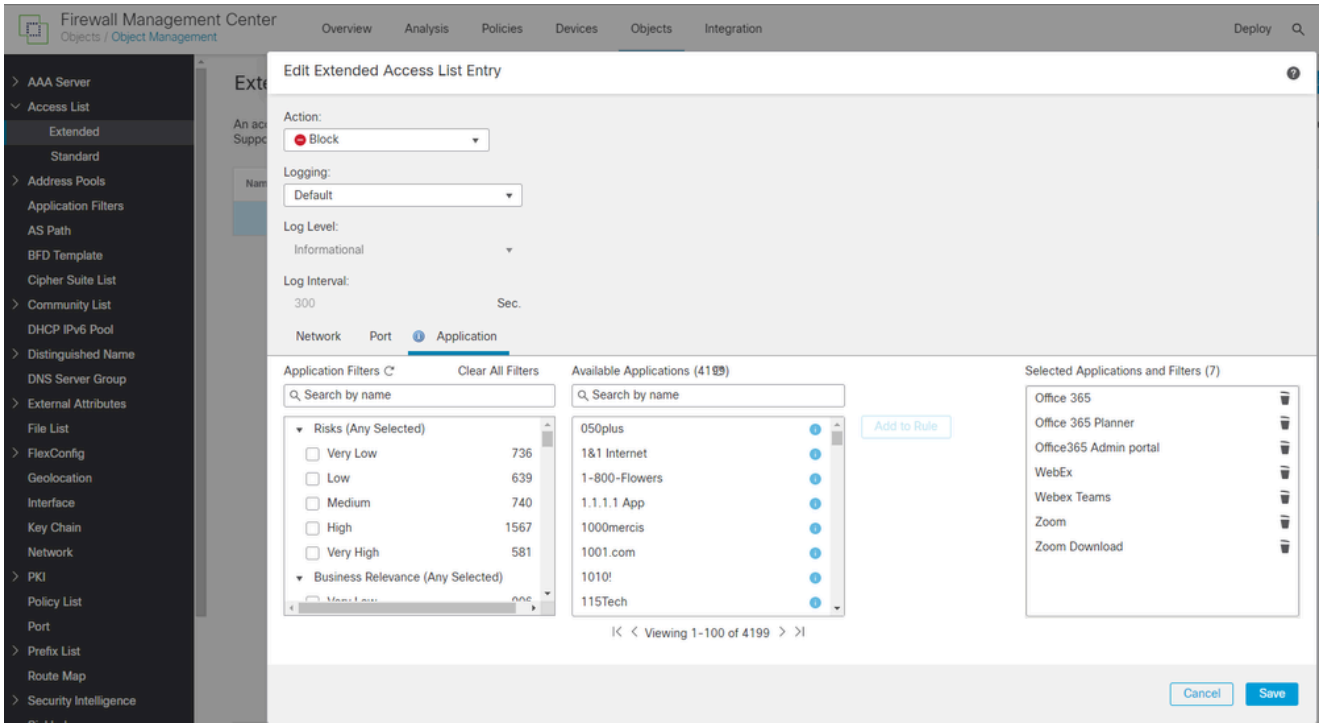
15669097907860

3. 트래픽이 SIG용 Umbrella로 전송되는지 또는 IPsec에서 제외되어 Umbrella로 전송되지 않는지 여부를 결정하기 위해 PBR 프로세스를 위해 FTD에서 사용할 수 있는 확장 ACL을 생성합니다.

- ACL에서 거부 ACE는 트래픽이 SIG에서 제외됨을 의미합니다.
- ACL에서 permit ACE는 트래픽이 IPsec을 통해 전송되며 SIG 정책(CDFW, SWG 등)을 적용할 수 있음을 의미합니다.

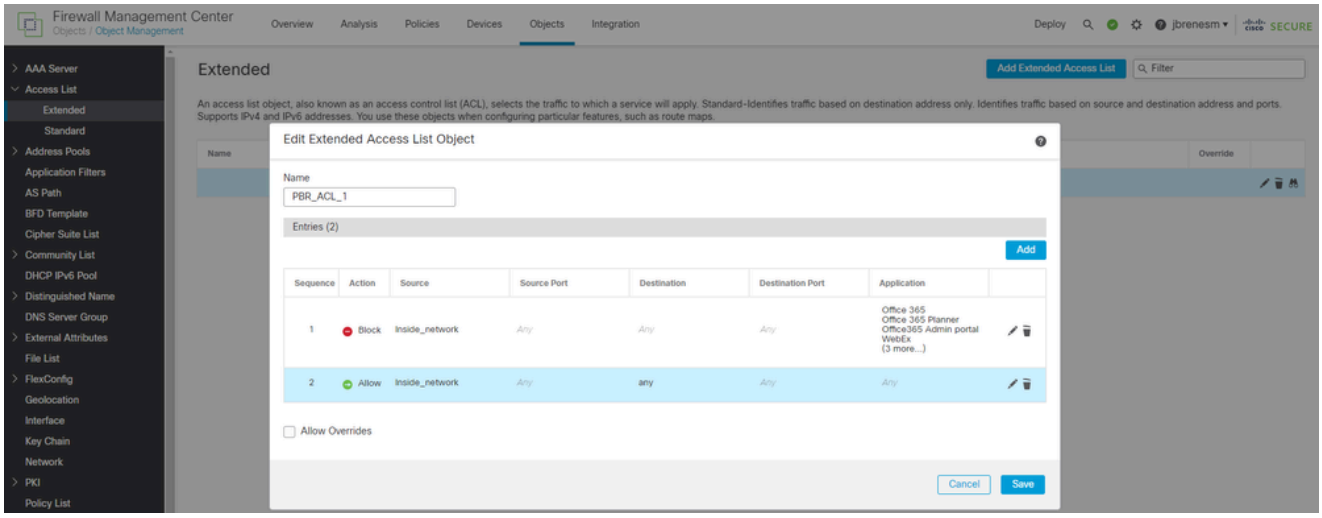
이 예에서는 거부 ACE가 있는 애플리케이션 "Office365", "Zoom" 및 "Cisco Webex"를 제외합니다. 나머지 트래픽은 추가 검사를 위해 Umbrella로 전송 중입니다.

1. Object(개체) > Object Management(개체 관리) > Access List(액세스 목록) > Extended(확장)로 이동합니다.
2. 평소와 같이 소스 네트워크 및 포트를 정의한 다음 PBR에 참여할 애플리케이션을 추가합니다.



15669947000852

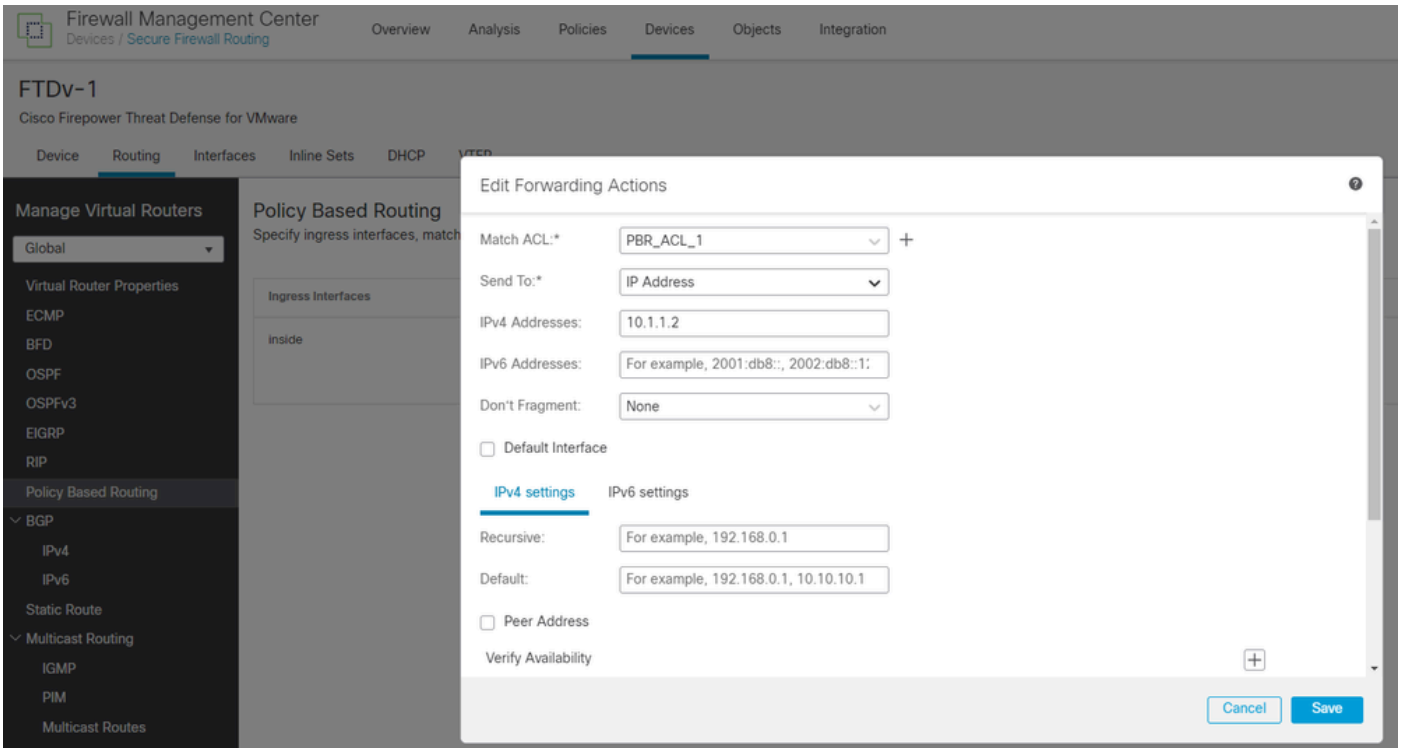
첫 번째 ACE는 앞서 언급한 애플리케이션에 대해 "거부"할 수 있으며, 두 번째 ACE는 나머지 트래픽을 IPsec을 통해 전송하도록 허용하는 것입니다.



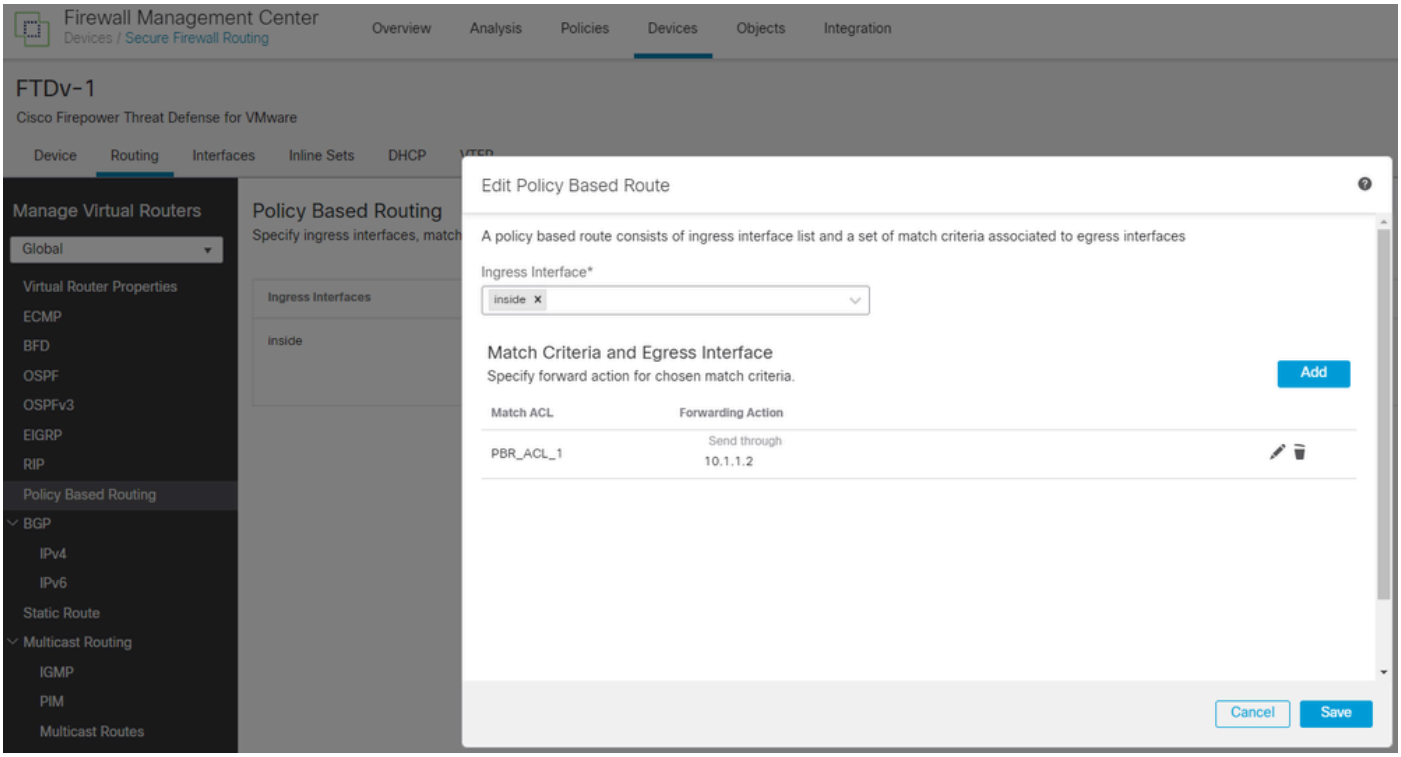
15670006987156

4. Devices(디바이스) > Device Management(디바이스 관리) > [select the FTD Device](FTD 디바이스 선택) > Routing(라우팅) > Policy Based Routing(정책 기반 라우팅)에서 PBR을 생성합니다.

- 인그레스 인터페이스: 로컬 트래픽이 들어오는 인터페이스.
- 일치하는 ACL: 이전 단계에서 생성한 확장 ACL, ACL "PBR_ACL_1".
- 전송 대상: IP 주소
- IPv4 주소: PBR이 permit 문을 발견하여 여기에 추가한 IP로 트래픽이 라우팅되는 경우 next-hop을 선택합니다. 이 예에서는 Umbrella의 IPsec IP입니다. VTI VPN의 IP가 10.1.1.1인 경우 Umbrella의 IPsec IP는 동일한 네트워크(예: 10.1.1.2) 내의 모든 IP가 됩니다.



15670209158036



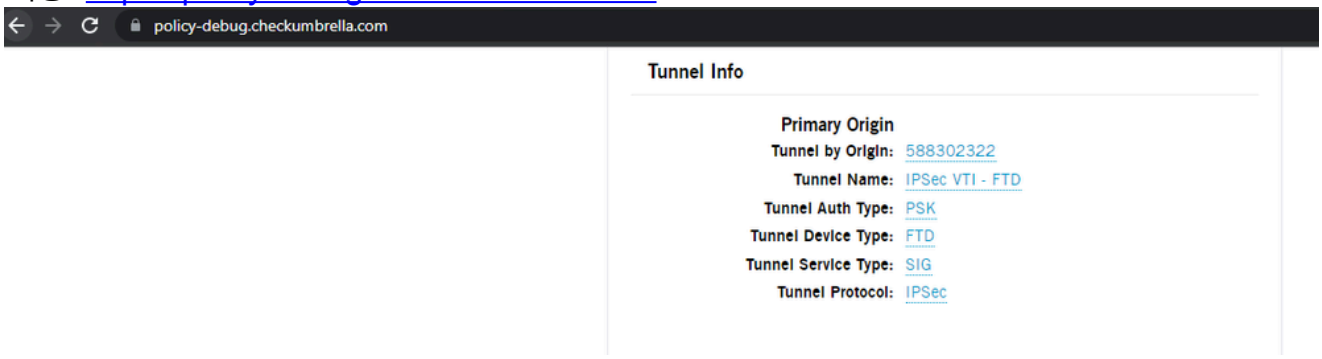
15670247521556

5. FMC에 변경 사항을 구축합니다.

확인

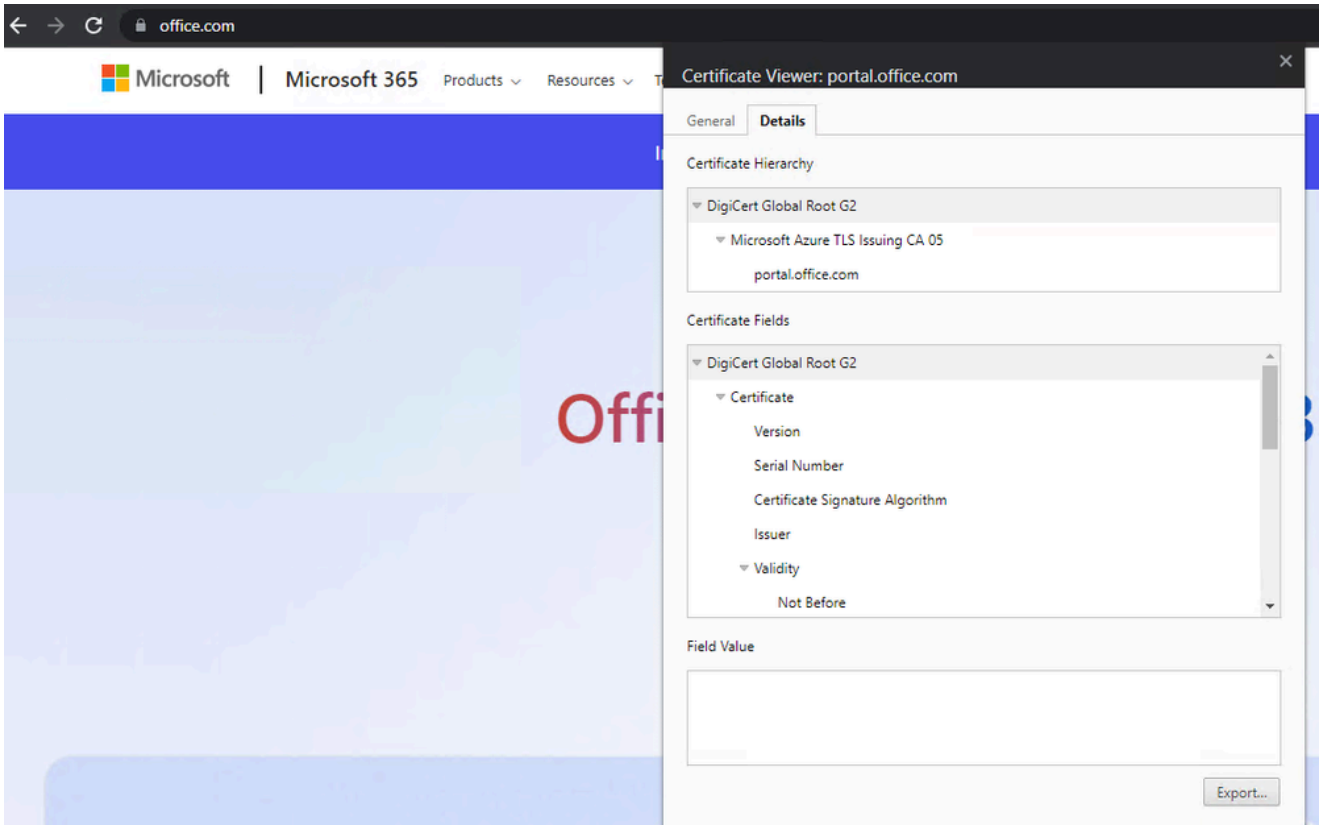
FTD 뒤에 있는 테스트 PC에서 다음을 확인합니다.

- PC의 트래픽이 실제로 IPsec을 통해 Umbrella로 전송되고 있습니다.
  이동: https://policy-debug.checkumbrella.com/



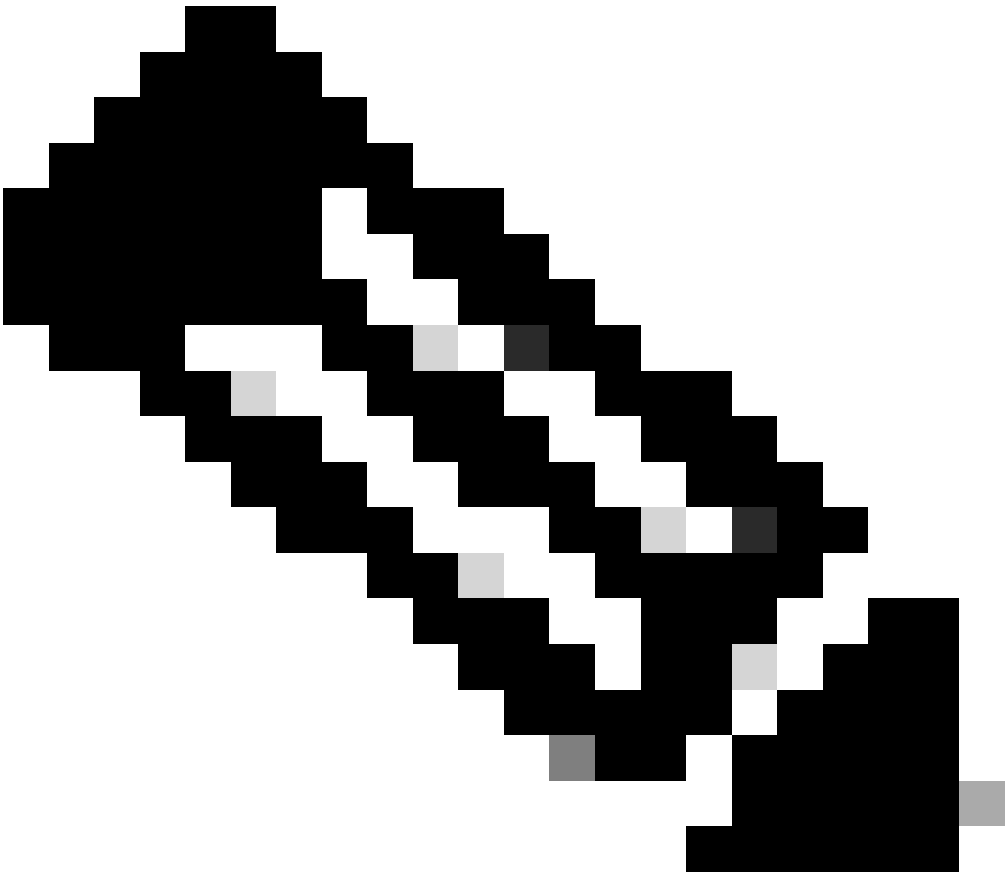
15670737148948

- PBR/ACL 컨피그레이션에서 제외된 사이트로 이동하여 Umbrella Root CA가 표시되지 않는지 확인합니다. 즉 연결이 프록시되지 않습니다.

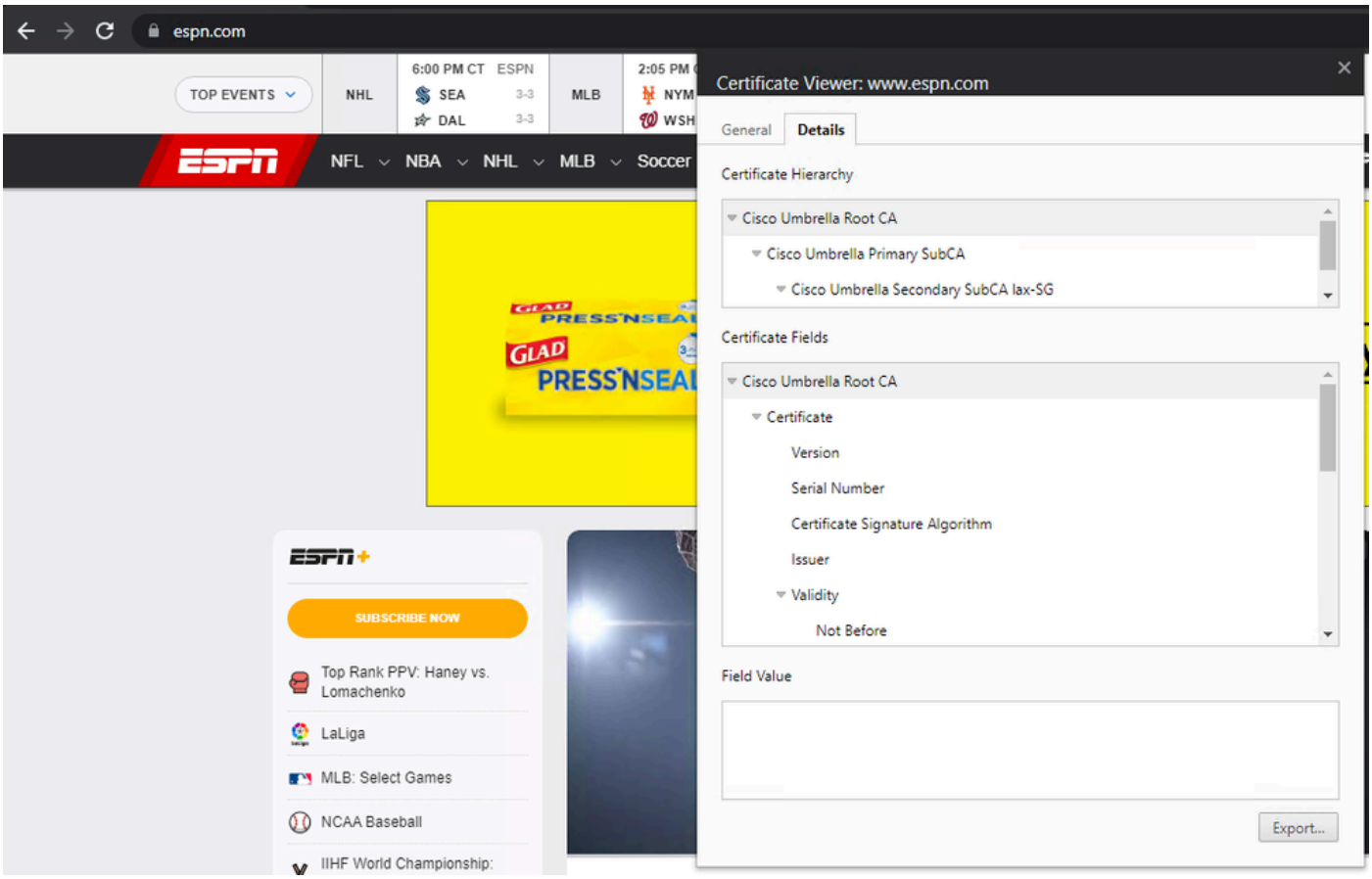


15670820980756

- PBR에서 제외된 애플리케이션을 기반으로 하지 않는 다른 사이트로 이동하여 Umbrella가 실제로 연결을 프록시하는지 확인합니다.



참고: 경고 페이지를 신뢰할 수 없는 문제가 발생하지 않도록 하려면 Umbrella Root CA Certificate가 설치되어 있는지 확인합니다.



- FTD의 CLI에서 몇 가지 명령을 실행하여 컨피그레이션이 제대로 푸시되고 작동하는지 확인할 수 있습니다.
  - `show run route-map`(PBR 컨피그레이션 확인):

```
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#
```

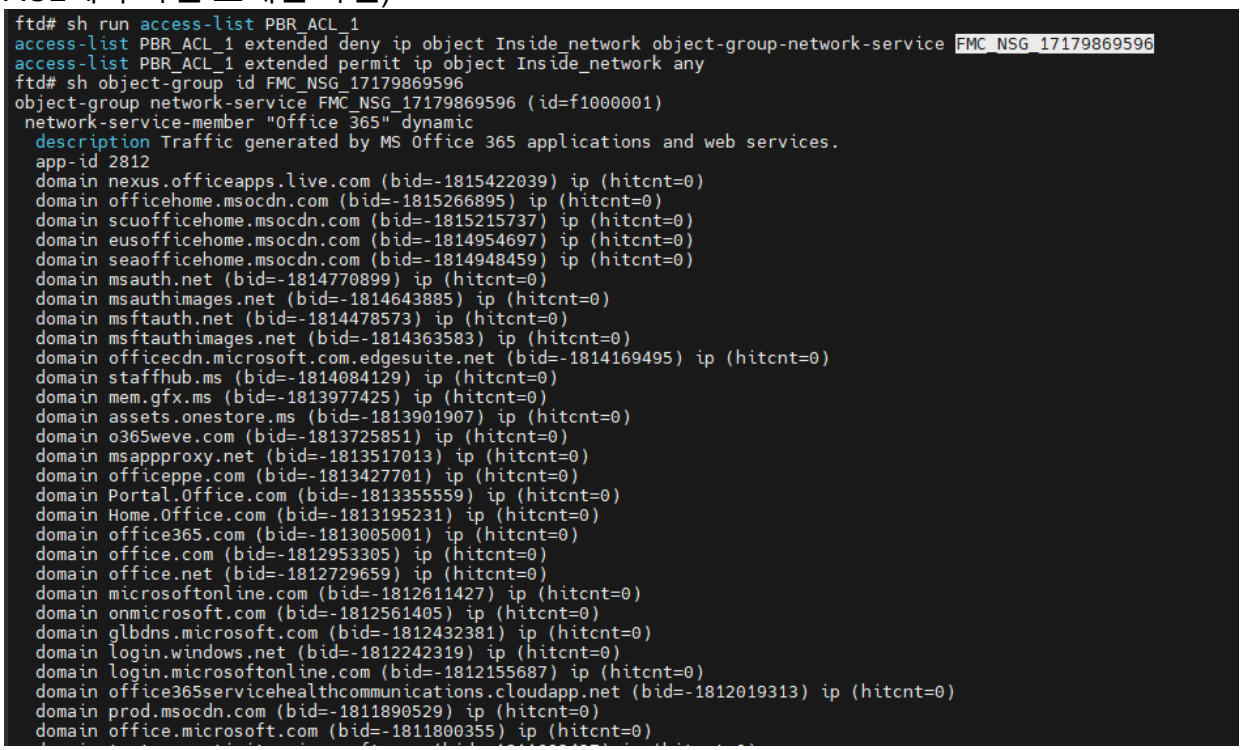
15670322054036

  - `show run interface gigabitEthernet 0/1`(PBR이 적절한 인터페이스에 적용되었는지 확인)

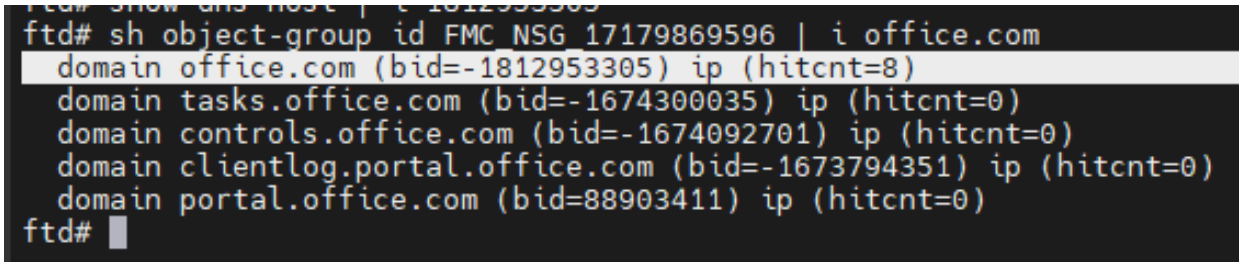
```
ftd# sh run interface gigabitEthernet 0/1
!
interface GigabitEthernet0/1
 nameif inside
 security-level 0
 ip address 172.16.72.1 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1682004086289
ftd#
```

15678344219540

- `show run access-list PBR_ACL_1`, `show object-group id FMC_NSG_17179869596`(제외를 위해 ACL에 추가된 도메인 확인)



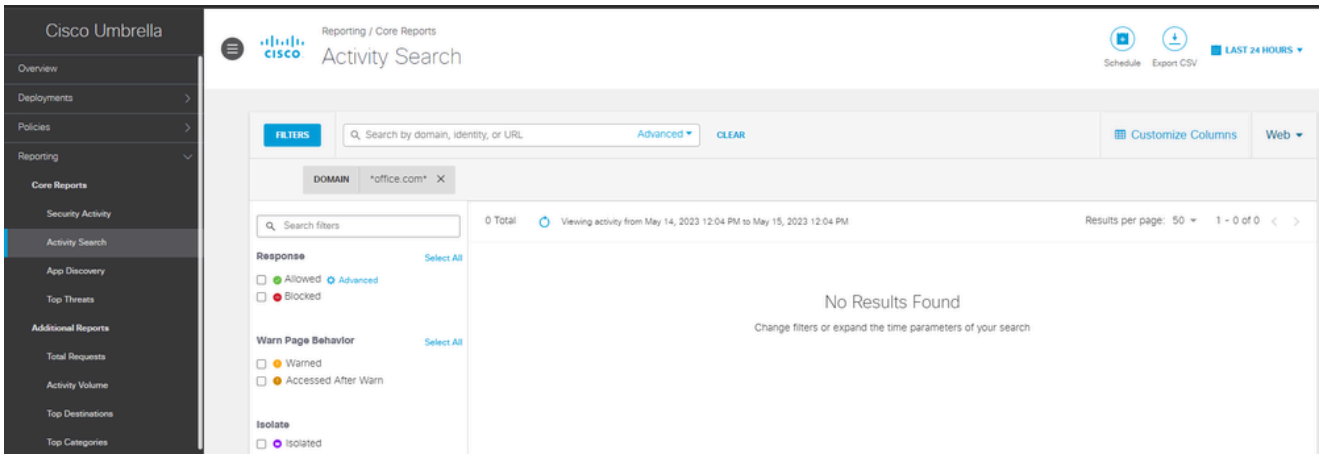
15670420887316



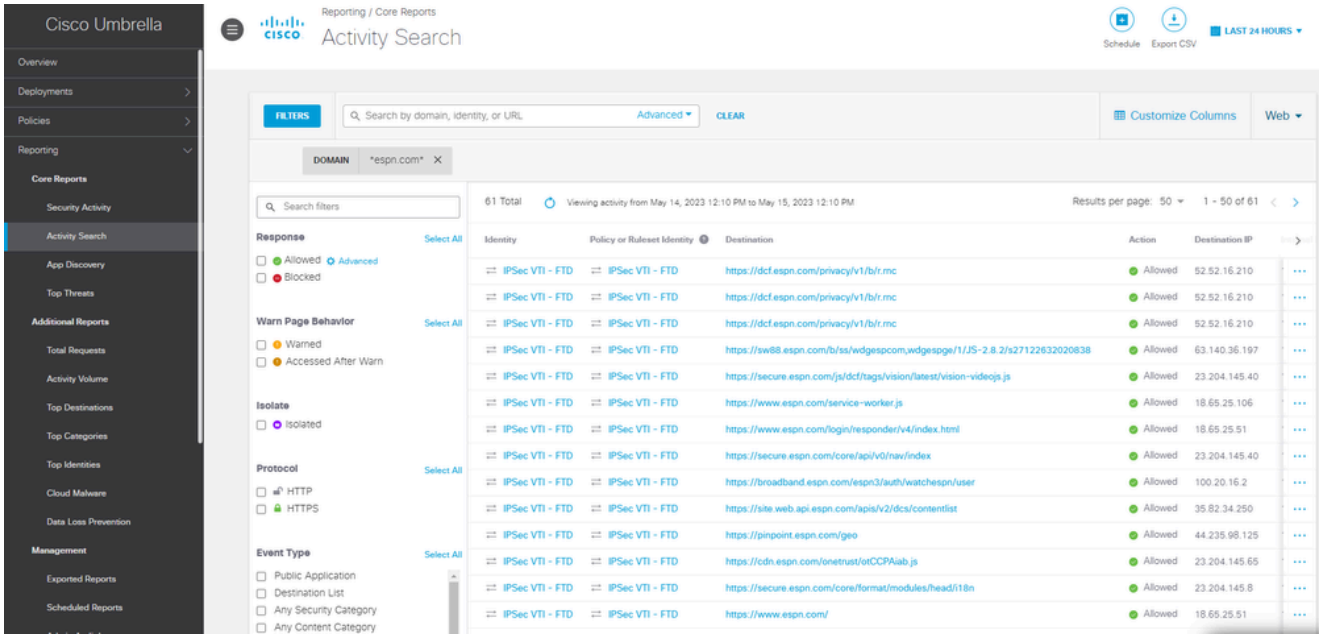
15670635784852

- `tcp 172.16.72.10 1234 fqdn office.com 443 상세` 정보(외부 인터페이스가 VTI 인터페이스가 아닌 출력으로 사용되는지 확인)

- Umbrella Dashboard(Umbrella 대시보드)의 활동 검색 아래에서 office.com으로 이동하는 웹 트래픽은 Umbrella로 전송되지 않았고 espn.com으로 이동하는 트래픽은 전송된 것을 확인할 수 있습니다.



15671098042516



15671302832788

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.