Configure FTD Application-Based PBR for Umbrella SIG

Contents

Introduction

This document describes how to configure Firewall Threat Defense (FTD) application-based policy based routing (PBR) for Umbrella SIG.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to Umbrella Dashboard
- Admin access to the FMC running 7.1.0+ to deploy the configuration to the FTD version 7.1.0+. PBR based on apps is supported only on version 7.1.0 and higher
- (Preferred) Knowledge on FMC/FTD configuration and Umbrella SIG
- (Optional but highly recommended): Umbrella Root Certificate installed, this is used by SIG when the traffic is either proxied or blocked. For further details of the Root Certificate installation, read more in the Umbrella documentation.

Components Used

The information in this document is based on Cisco Umbrella Secure Internet Gateway (SIG).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

The information in this document is meant to cover the configuration steps on how to deploy Application-Based PBR on the FTD when establishing a SIG IPsec VTI Tunnel to Umbrella, so you can exclude or include traffic on a VPN based on applications using PBR.

The configuration example described in this article focuses on how to **exclude** certain applications from the IPsec VPN while sending everything else over the VPN.

Full information about PBR on FMC can be found in the Cisco documentation.

Limitations

- You cannot have both application and destination address defined in an ACE.

- While defining the ACL for the policy match criteria, you can select multiple applications from a list of predefined applications to form an Access Control Entry (ACE).
  Currently, you cannot add to or modify the predefined applications list.
- For those applications not listed on the predefined applications list on the FMC or any unexpected behavior with an application, IPs can be used instead of applications in the PBR.
- For a list of full limitations please referrer to the PBR's documentation.

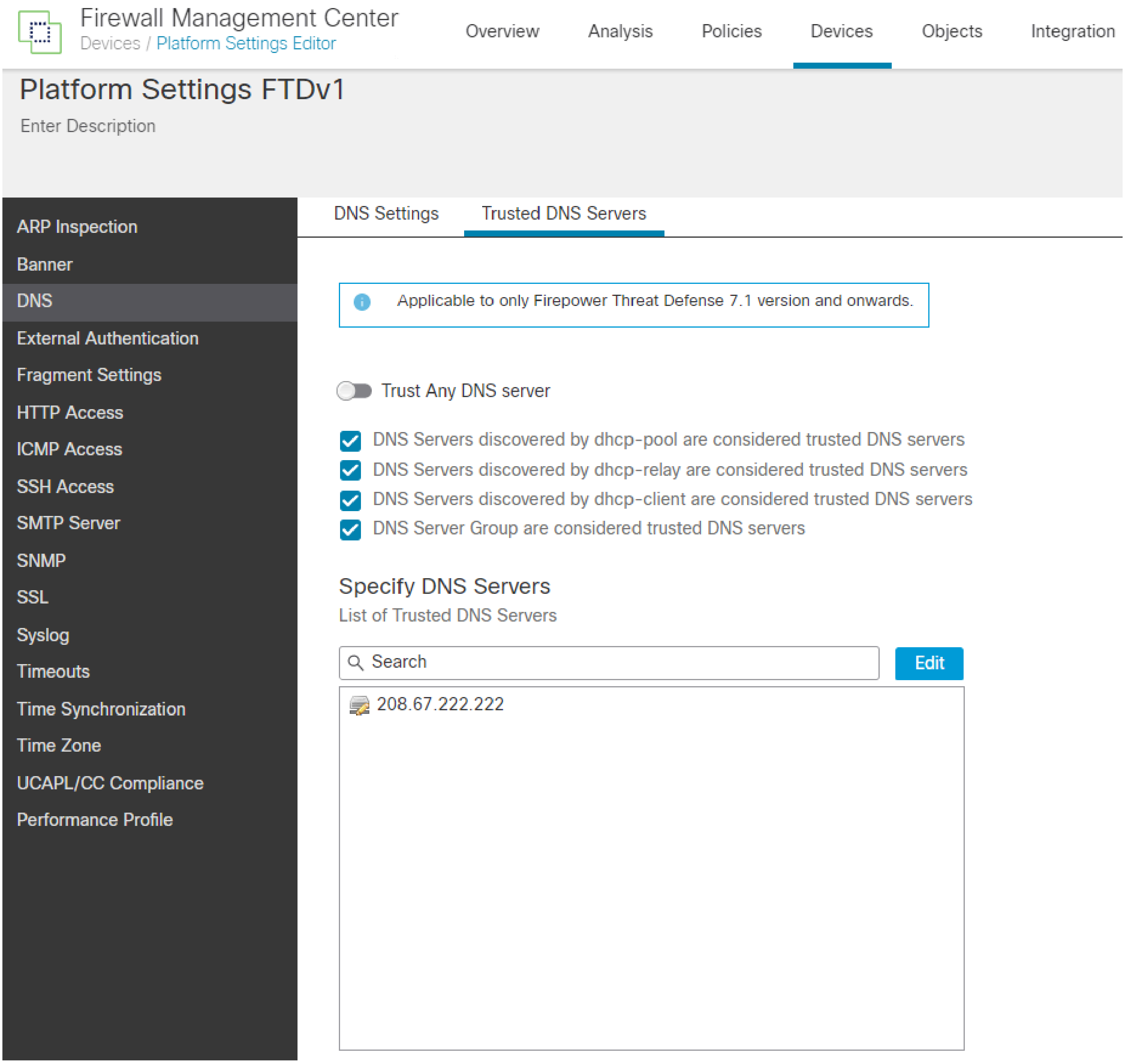
Application-Based PBR

1. Start by configuring the IPsec tunnel on the FMC as well as on the Umbrella Dashboard. The instructions of how to perform this configuration can be found in the Umbrella documentation.

2. Make sure that the DNS server that the end user's device behind the FTD is using is listed as a trusted DNS server under **Devices > Platform Settings > DNS > Trusted DNS Servers**.

If the devices are using a DNS server that is not listed, the DNS snooping can fail, and therefore the PBR based on apps cannot work. Optionally (but not recommended for security reasons), you can toggle on **Trust Any DNS server** so that adding the DNS server(s) is required.

Note: If VAs are used as internal DNS resolvers, they must be added as Trusted DNS Servers.



Firewall Management Center

Devices / Platform Settings Editor

Platform Settings FTDv1

Enter Description

Applicable to only Firepower Threat Defense 7.1 version and onwards.

○ Trust Any DNS server

☑ DNS Servers discovered by dhcp-pool are considered trusted DNS servers

☑ DNS Servers discovered by dhcp-relay are considered trusted DNS servers

☑ DNS Servers discovered by dhcp-client are considered trusted DNS servers

☑ DNS Server Group are considered trusted DNS servers

Specify DNS Servers

List of Trusted DNS Servers

208.67.222.222

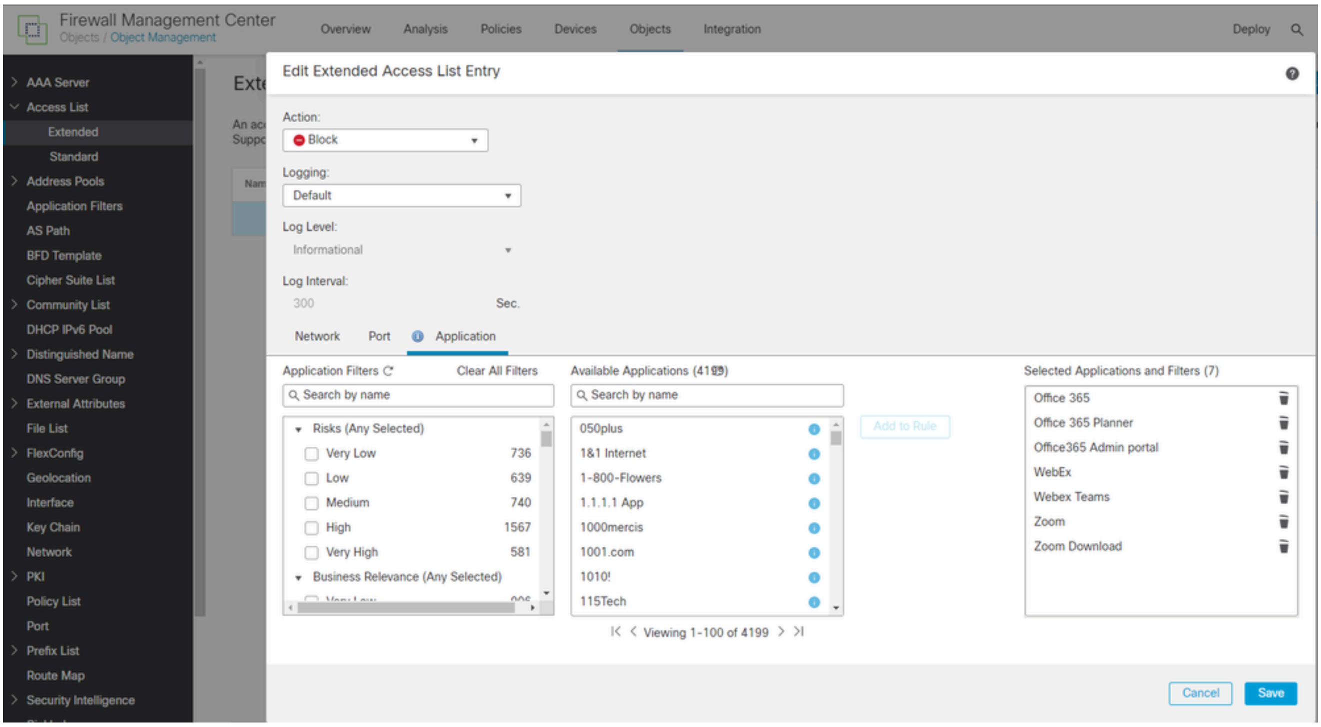
15669097907860

3. Create an extended ACL that can be used by the FTD for the PBR process in order to decide whether traffic is sent to Umbrella for SIG or if it is excluded from the IPsec and not sent to Umbrella at all.

- A deny ACE on the ACL means the traffic is excluded from SIG.
- A permit ACE on the ACL means the traffic is sent over the IPsec and can apply a SIG policy (CDFW, SWG, etc).

This example is excluding the applications "Office365", "Zoom" and "Cisco Webex" with a deny ACE. The rest of the traffic is being sent to Umbrella for further inspection.

1. Go to **Object > Object Management > Access List > Extended**.
2. Define the source network and ports as you normally would, and then add the applications to participate on the PBR.



Edit Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Network Port Application

Application Filters — Risks (Any Selected): □ Very Low 736, □ Low 639, □ Medium 740, □ High 1567, □ Very High 581; Business Relevance (Any Selected)

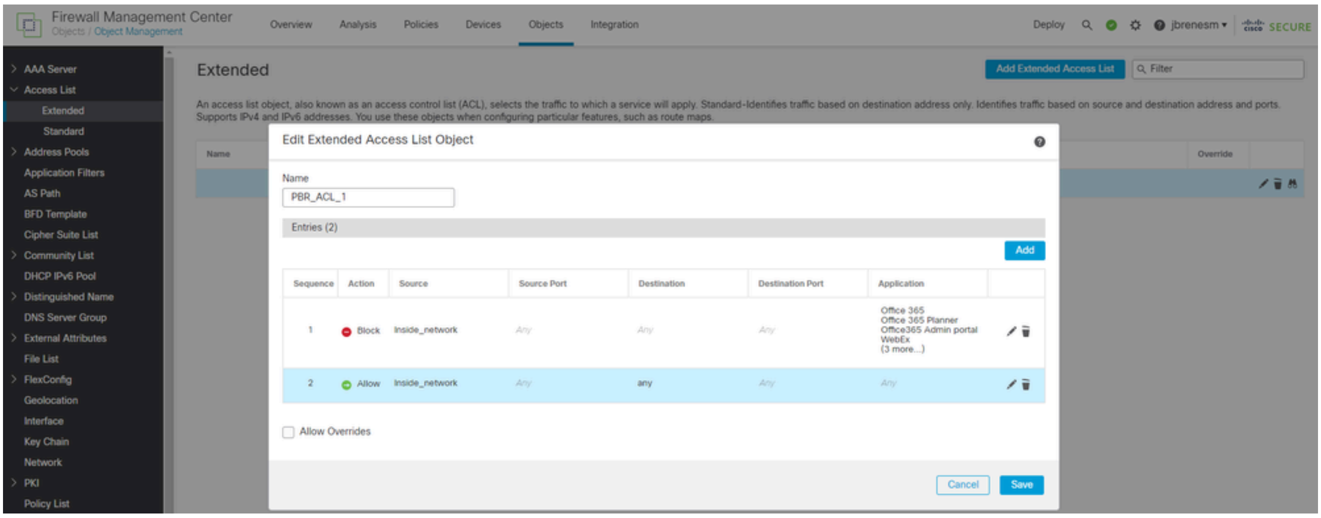
Available Applications (4199): 050plus, 1&1 Internet, 1-800-Flowers, 1.1.1.1 App, 1000mercis, 1001.com, 1010!, 115Tech — Viewing 1-100 of 4199

Selected Applications and Filters (7):

- Office 365
- Office 365 Planner
- Office365 Admin portal
- WebEx
- Webex Teams
- Zoom
- Zoom Download

15669947000852

The first ACE can "deny" for those applications mentioned earlier, and the second ACE is a permit to send the rest of the traffic over the IPsec.



Edit Extended Access List Object

Name: PBR_ACL_1

Entries (2)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application
1	Block	Inside_network	Any	Any	Any	Office 365 Office 365 Planner Office365 Admin portal WebEx (3 more...)
2	Allow	Inside_network	Any	any	Any	Any

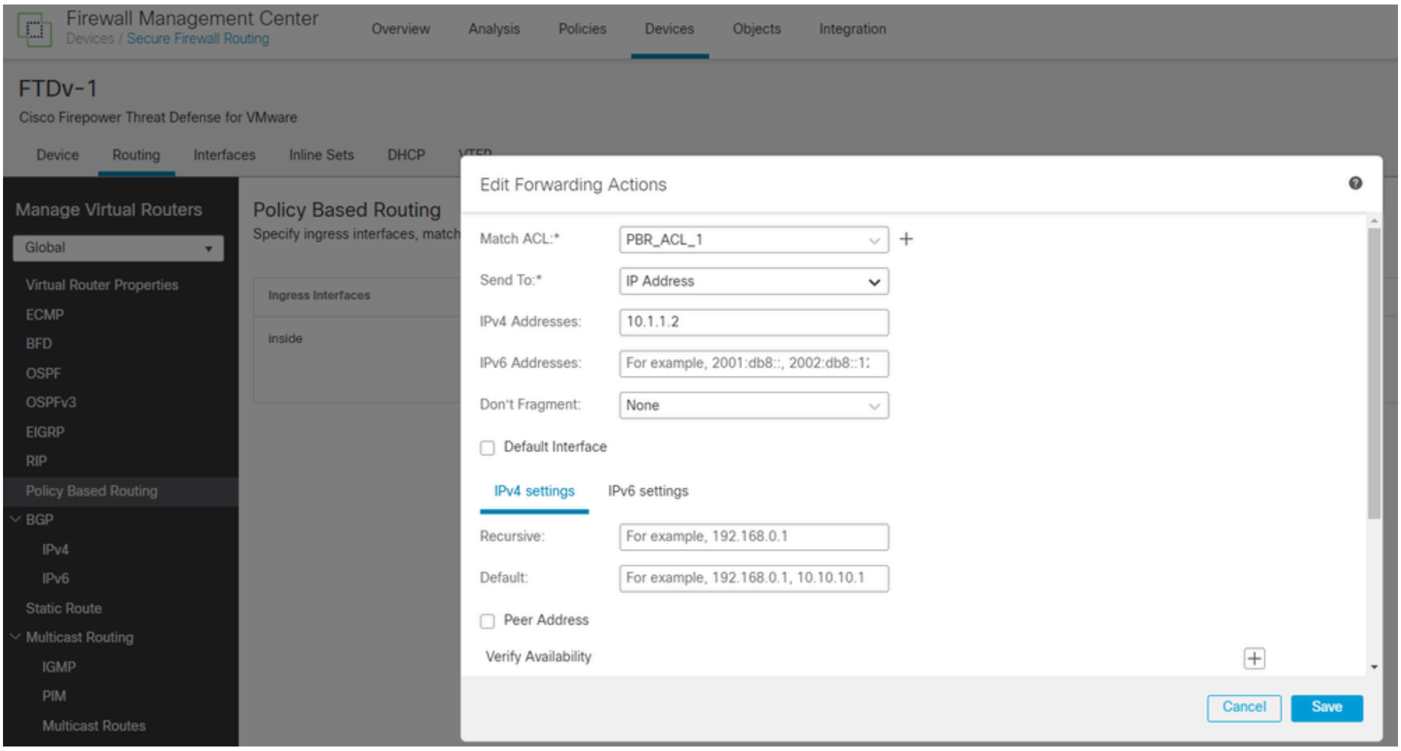
□ Allow Overrides

Firewall Management Center
Objects / Object Management
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
jbrenesm
SECURE
Extended
Add Extended Access List
Filter
An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.
Name
Override
Add
Cancel
Save

15670006987156

4. Create the PBR under **Devices > Device Management > [select the FTD Device] > Routing > Policy Based Routing.**

- Ingress Interface: The interface where the local traffic is coming from.
- Matching ACL: Extended ACL created on previous step, ACL "PBR_ACL_1".
- Send To: IP Address
- IPv4 Addresses: Next-hop when the PBR finds a permit statement, so the traffic is routed to the IP you add here. In this example, this is Umbrella's IPsec IP. If your VTI VPN's IP is 10.1.1.1, then the Umbrella's IPsec IP would be anything inside that same network (10.1.1.2 for example).



Edit Forwarding Actions

Match ACL:* PBR_ACL_1

Send To:* IP Address

IPv4 Addresses: 10.1.1.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:

Don't Fragment: None

□ Default Interface

IPv4 settings | IPv6 settings

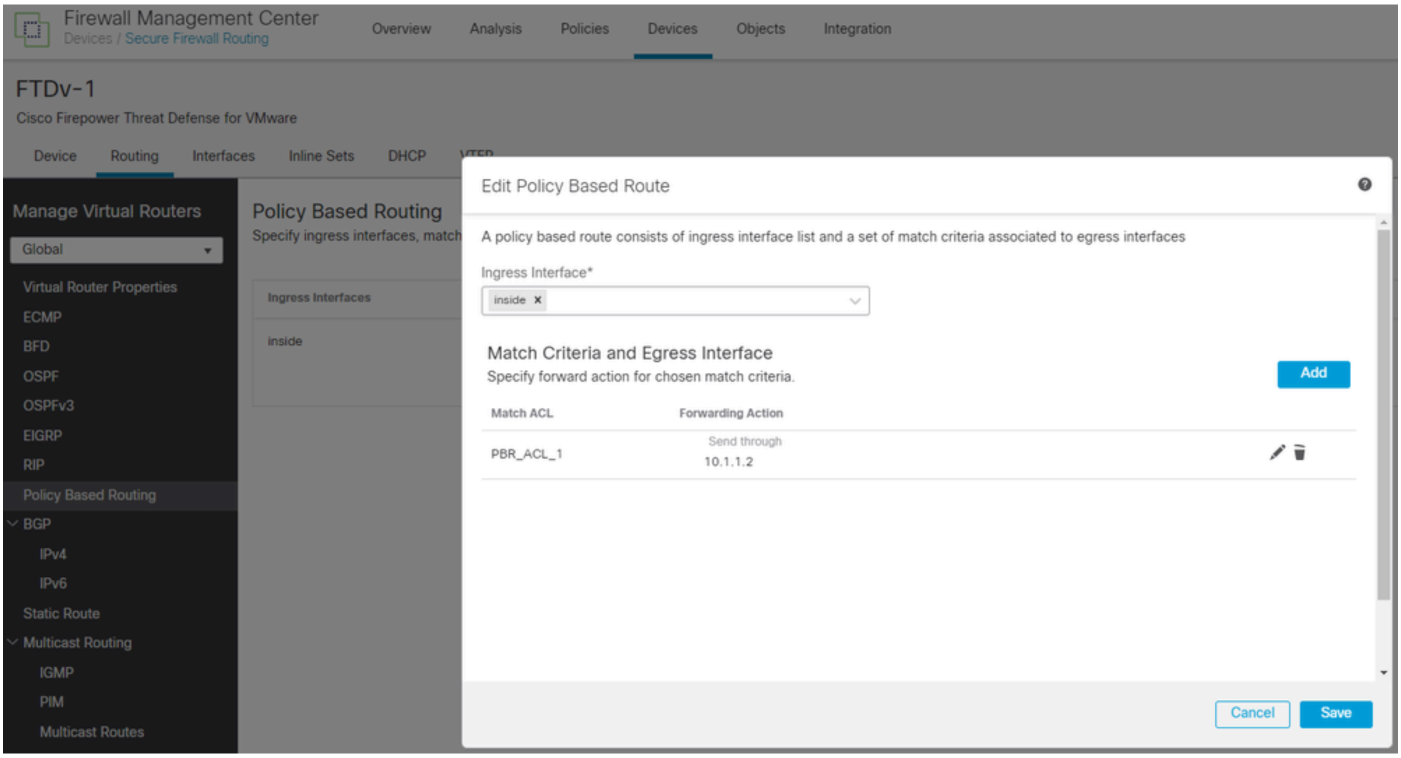
Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

□ Peer Address

Verify Availability

15670209158036



Edit Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface* inside

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Match ACL	Forwarding Action
PBR_ACL_1	Send through 10.1.1.2

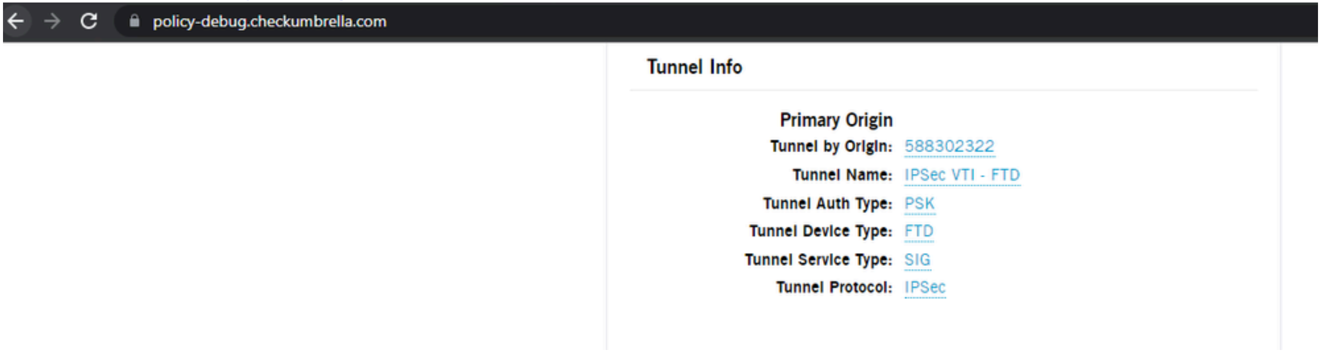
15670247521556

5. Deploy the changes on the FMC.

Verification

On the testing PC located behind the FTD, check:

- The traffic from the PC is actually being sent over the IPsec to Umbrella.
  Go to: https://policy-debug.checkumbrella.com/



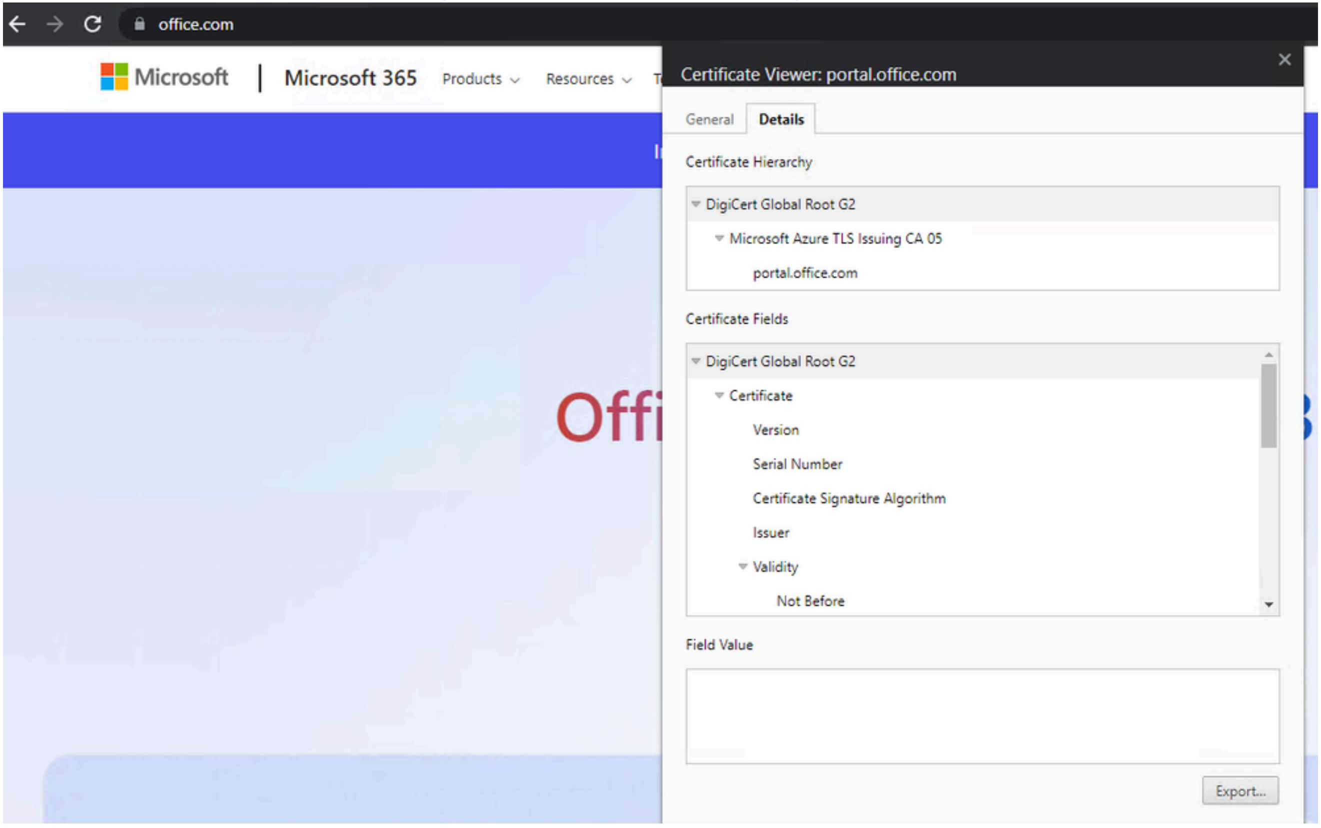
Tunnel Info

Primary Origin

Tunnel by Origin: 588302322
Tunnel Name: IPSec VTI - FTD
Tunnel Auth Type: PSK
Tunnel Device Type: FTD
Tunnel Service Type: SIG
Tunnel Protocol: IPSec

15670737148948

- Try going to any of the sites that are excluded on the PBR/ACL config and make sure the Umbrella Root CA is not presented, meaning the connection is not being proxied:



Certificate Viewer: portal.office.com

Certificate Hierarchy
- DigiCert Global Root G2
  - Microsoft Azure TLS Issuing CA 05
    - portal.office.com

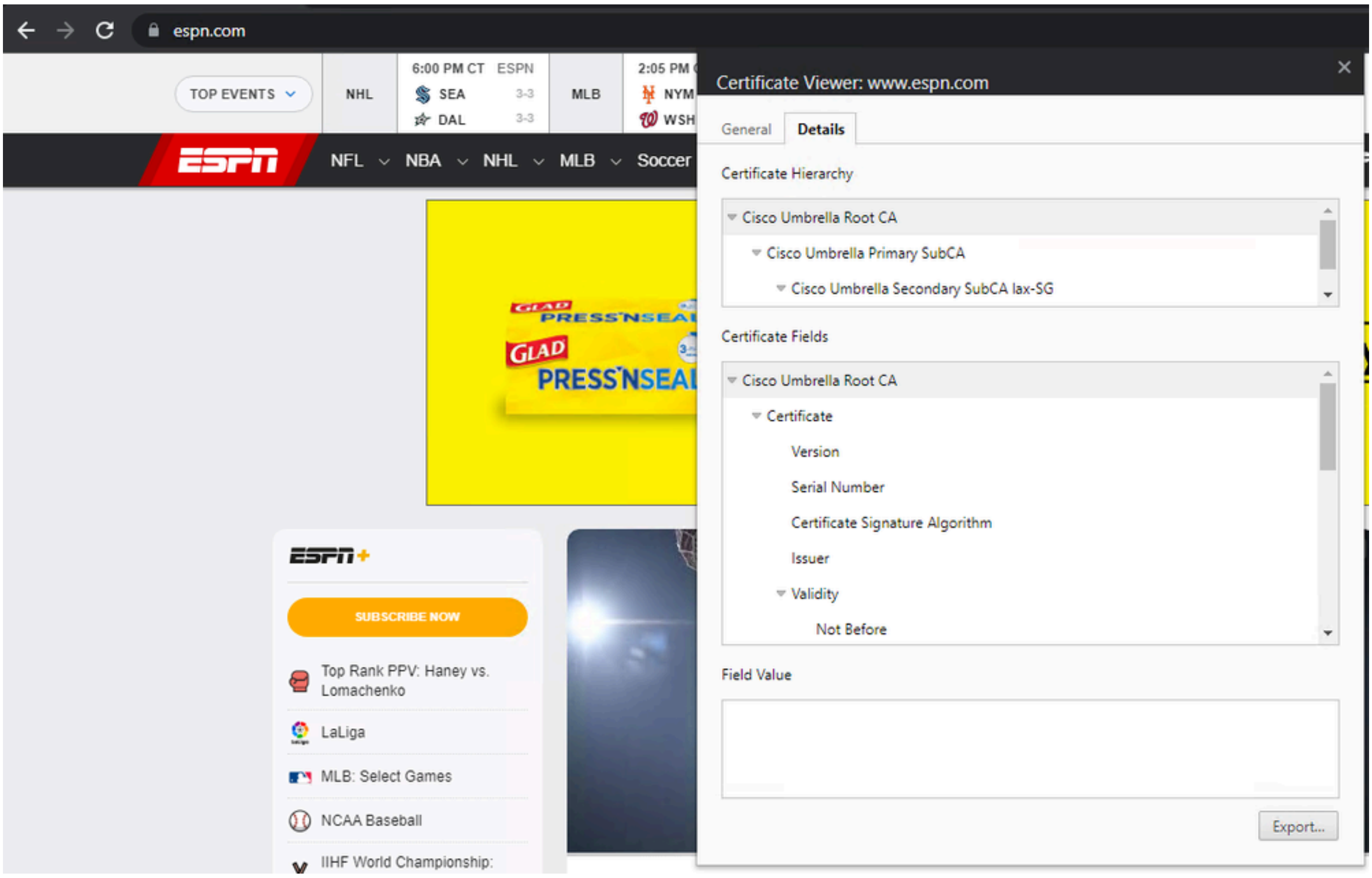
Certificate Fields
- DigiCert Global Root G2
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

Field Value

15670820980756

- Try going to any other site that is not based on the applications excluded from the PBR and make sure Umbrella is indeed proxying the connection:

Note: In order to avoid issues with a warning page not being trusted, make sure the Umbrella Root CA Certificate is installed.



Certificate Viewer: www.espn.com

General | Details

Certificate Hierarchy

- Cisco Umbrella Root CA
  - Cisco Umbrella Primary SubCA
    - Cisco Umbrella Secondary SubCA lax-SG

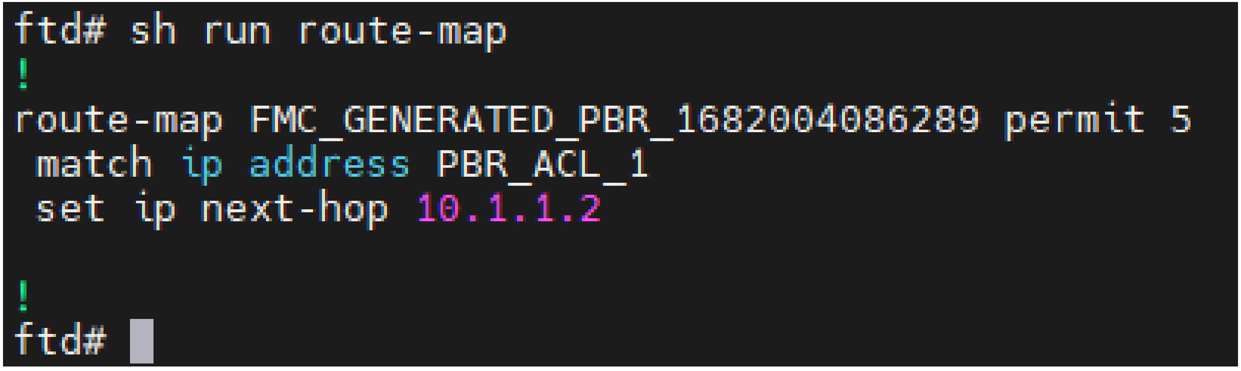
Certificate Fields

- Cisco Umbrella Root CA
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

Field Value

Export...

- On the FTD's CLI, you can run a few commands to confirm the configuration was properly pushed and working:
  - `show run route-map` (checks the PBR configuration):

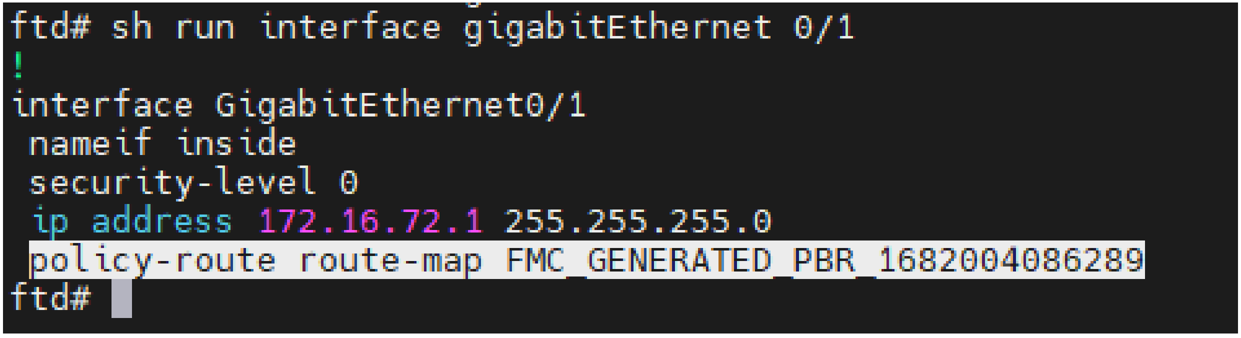


```
ftd# sh run route-map
!
route-map FMC_GENERATED_PBR_1682004086289 permit 5
 match ip address PBR_ACL_1
 set ip next-hop 10.1.1.2

!
ftd#
```

15670322054036

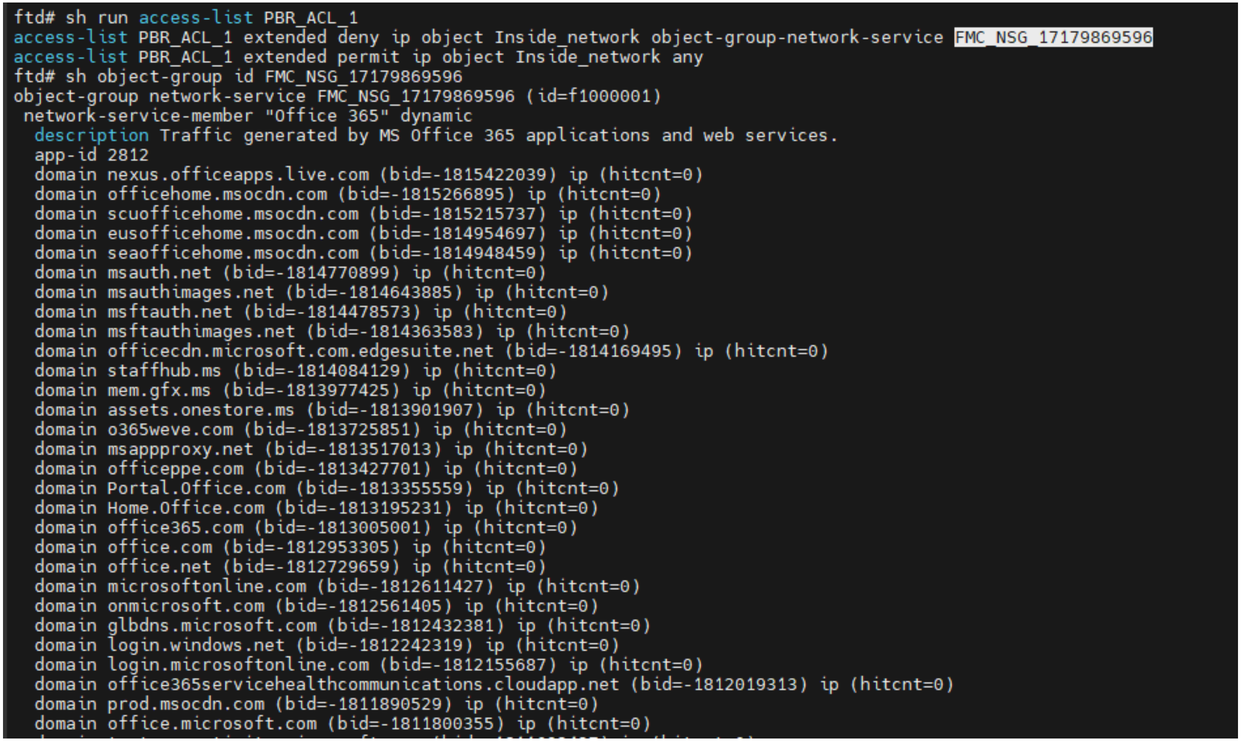
  - `show run interface gigabitEthernet 0/1` (checks the PBR is applied to the proper interface)



```
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#
```

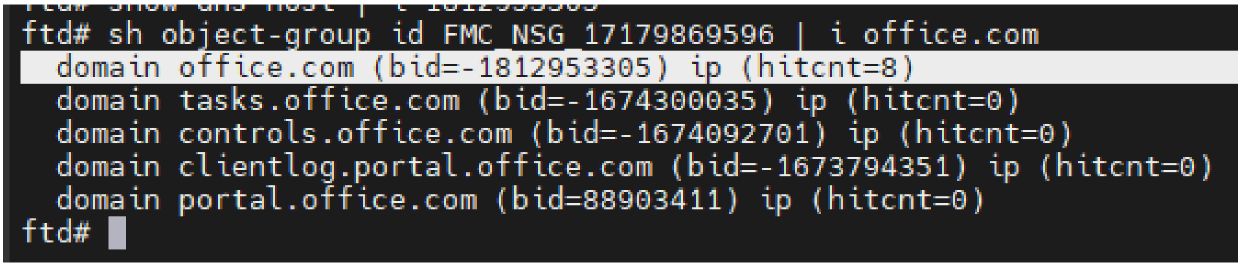
15678344219540

  - `show run access-list PBR_ACL_1, show object-group id FMC_NSG_17179869596` (confirms the domains added to the ACL for exclusion)



```
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

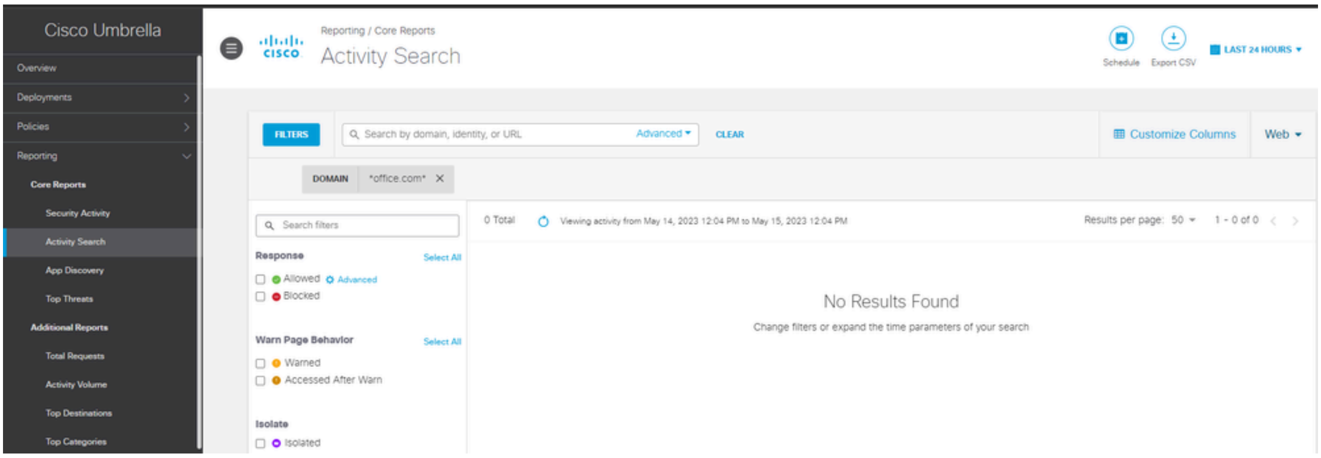


```
ftd# sh object-group id FMC_NSG_17179869596 | i office.com
  domain office.com (bid=-1812953305) ip (hitcnt=8)
  domain tasks.office.com (bid=-1674300035) ip (hitcnt=0)
  domain controls.office.com (bid=-1674092701) ip (hitcnt=0)
  domain clientlog.portal.office.com (bid=-1673794351) ip (hitcnt=0)
  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` (verifies the outside interface is used as output and not the VTI one)

- On the Umbrella Dashboard, under activity search, you can see that web traffic going to office.com was never sent to Umbrella, while traffic going to espn.com was sent.



Reporting / Core Reports

Activity Search

DOMAIN *office.com*

Response: □ Allowed □ Blocked

Warn Page Behavior: □ Warned □ Accessed After Warn

Isolate: □ Isolated

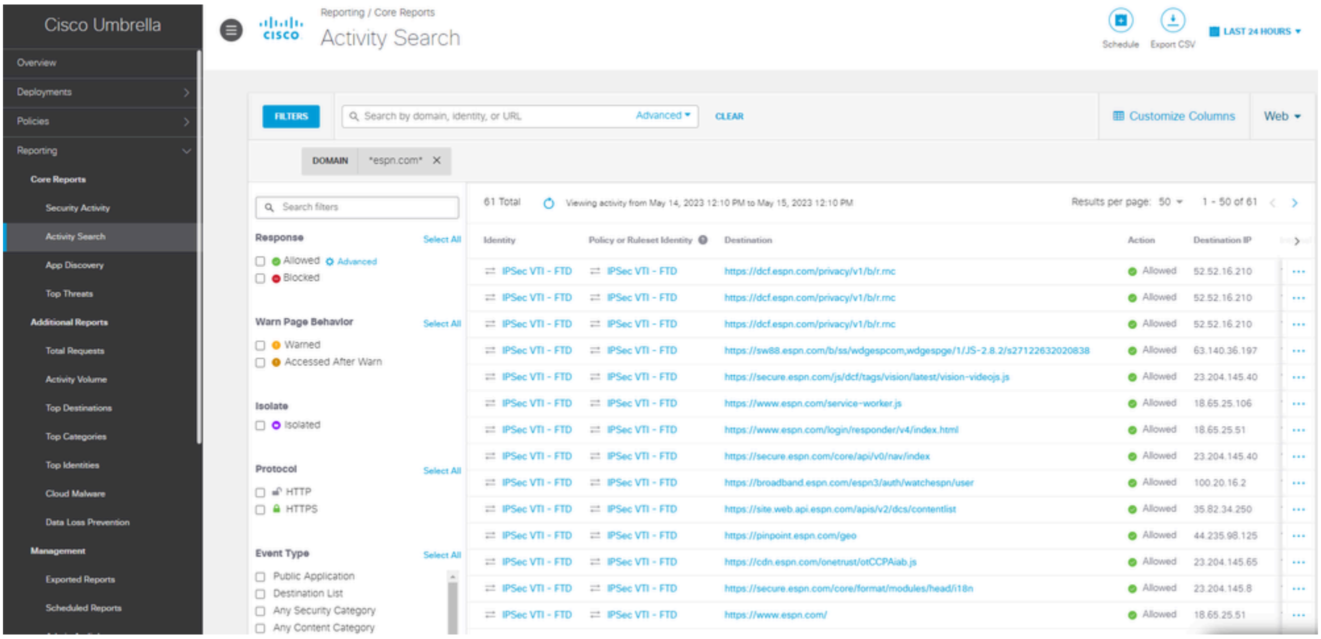
0 Total Viewing activity from May 14, 2023 12:04 PM to May 15, 2023 12:04 PM

Results per page: 50 1 - 0 of 0

No Results Found

Change filters or expand the time parameters of your search

15671098042516



Reporting / Core Reports

Activity Search

DOMAIN *espn.com*

Response: □ Allowed □ Blocked

Warn Page Behavior: □ Warned □ Accessed After Warn

Isolate: □ Isolated

Protocol: □ HTTP □ HTTPS

Event Type: □ Public Application □ Destination List □ Any Security Category □ Any Content Category

61 Total Viewing activity from May 14, 2023 12:10 PM to May 15, 2023 12:10 PM

Results per page: 50 1 - 50 of 61

Identity	Policy or Ruleset Identity	Destination	Action	Destination IP
IPSec VTI - FTD	IPSec VTI - FTD	https://dcf.espn.com/privacy/v1/b/r.mc	Allowed	52.52.16.210
IPSec VTI - FTD	IPSec VTI - FTD	https://dcf.espn.com/privacy/v1/b/r.mc	Allowed	52.52.16.210
IPSec VTI - FTD	IPSec VTI - FTD	https://dcf.espn.com/privacy/v1/b/r.mc	Allowed	52.52.16.210
IPSec VTI - FTD	IPSec VTI - FTD	https://sw88.espn.com/b/ss/wdgespcom,wdgespge/1/JS-2.8.2/s27122632020838	Allowed	63.140.36.197
IPSec VTI - FTD	IPSec VTI - FTD	https://secure.espn.com/js/dcf/tags/vision/latest/vision-videojs.js	Allowed	23.204.145.40
IPSec VTI - FTD	IPSec VTI - FTD	https://www.espn.com/service-worker.js	Allowed	18.65.25.106
IPSec VTI - FTD	IPSec VTI - FTD	https://www.espn.com/login/responder/v4/index.html	Allowed	18.65.25.51
IPSec VTI - FTD	IPSec VTI - FTD	https://secure.espn.com/core/api/v0/nav/index	Allowed	23.204.145.40
IPSec VTI - FTD	IPSec VTI - FTD	https://broadband.espn.com/espn3/auth/watchespn/user	Allowed	100.20.16.2
IPSec VTI - FTD	IPSec VTI - FTD	https://site.web.api.espn.com/apis/v2/dcs/contentlist	Allowed	35.82.34.250
IPSec VTI - FTD	IPSec VTI - FTD	https://pinpoint.espn.com/geo	Allowed	44.235.98.125
IPSec VTI - FTD	IPSec VTI - FTD	https://cdn.espn.com/onetrust/otCCPAiab.js	Allowed	23.204.145.65
IPSec VTI - FTD	IPSec VTI - FTD	https://secure.espn.com/core/format/modules/head/i18n	Allowed	23.204.145.8
IPSec VTI - FTD	IPSec VTI - FTD	https://www.espn.com/	Allowed	18.65.25.51

15671302832788