Konfigurieren von anwendungsbasiertem FTD-PBR für Umbrella SIG

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des anwendungsbasierten richtlinienbasierten Routing (Policy Based Routing, PBR) von Firewall Threat Defense (FTD) für Umbrella SIG beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zugriff auf das Umbrella Dashboard
- Administratorzugriff auf das FMC mit Version 7.1.0+ zur Bereitstellung der Konfiguration für FTD Version 7.1.0+ PBR auf Basis von Apps wird nur von Version 7.1.0 und höher unterstützt
- (Bevorzugt) Kenntnisse über FMC/FTD-Konfiguration und Umbrella SIG
- (Optional, aber sehr empfehlenswert): Umbrella Root Certificate installiert ist, wird dies von SIG verwendet, wenn der Datenverkehr entweder proximiert oder blockiert wird. Weitere Informationen zur Installation des Stammzertifikats finden Sie in der Umbrella-Dokumentation.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella Secure Internet Gateway (SIG).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Die Informationen in diesem Dokument beziehen sich auf die Konfigurationsschritte bei der Bereitstellung von anwendungsbasiertem PBR auf dem FTD bei der Einrichtung eines SIG IPsec VTI-Tunnels zu Umbrella, sodass Sie Datenverkehr auf einem VPN basierend auf Anwendungen, die PBR verwenden, ausschließen oder einschließen können.

Das in diesem Artikel beschriebene Konfigurationsbeispiel konzentriert sich darauf, wie bestimmte Anwendungen vom IPsec-VPN ausgeschlossen werden, während alle anderen Anwendungen über das VPN gesendet werden.

Weitere Informationen zu PBR auf FMC finden Sie in der Cisco Dokumentation.

Einschränkungen

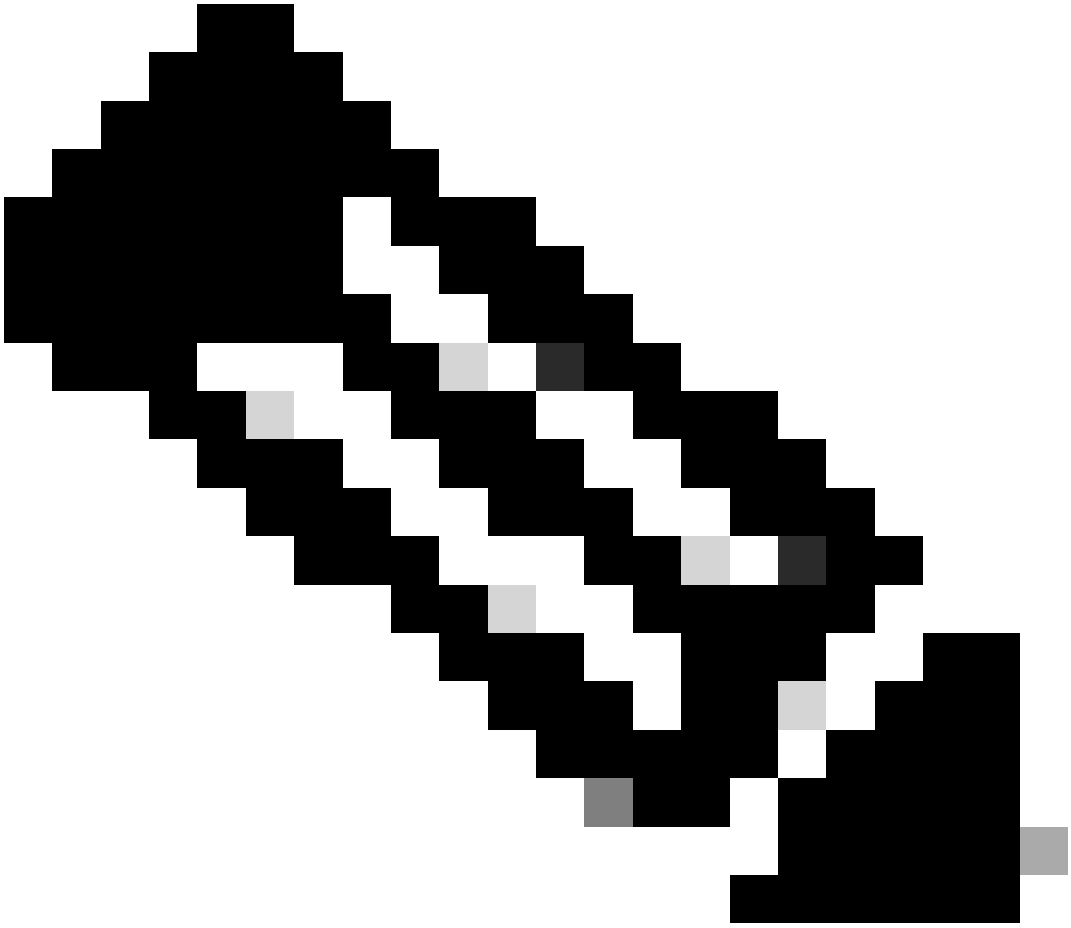
- In einem ACE können nicht sowohl Anwendungs- als auch Zieladresse definiert sein.
- Bei der Definition der ACL für die Kriterien für die Richtlinienzuordnung können Sie mehrere Anwendungen aus einer Liste vordefinierter Anwendungen auswählen, um einen Access Control Entry (ACE) zu bilden.
  Zurzeit können Sie die vordefinierte Anwendungsliste nicht hinzufügen oder ändern.
- Für Anwendungen, die nicht in der Liste der vordefinierten Anwendungen im FMC aufgeführt sind, oder für unerwartetes Verhalten mit einer Anwendung können IPs anstelle von Anwendungen im PBR verwendet werden.
- Eine Liste der vollständigen Einschränkungen finden Sie in der Dokumentation des PBR.

Anwendungsbasiertes PBR

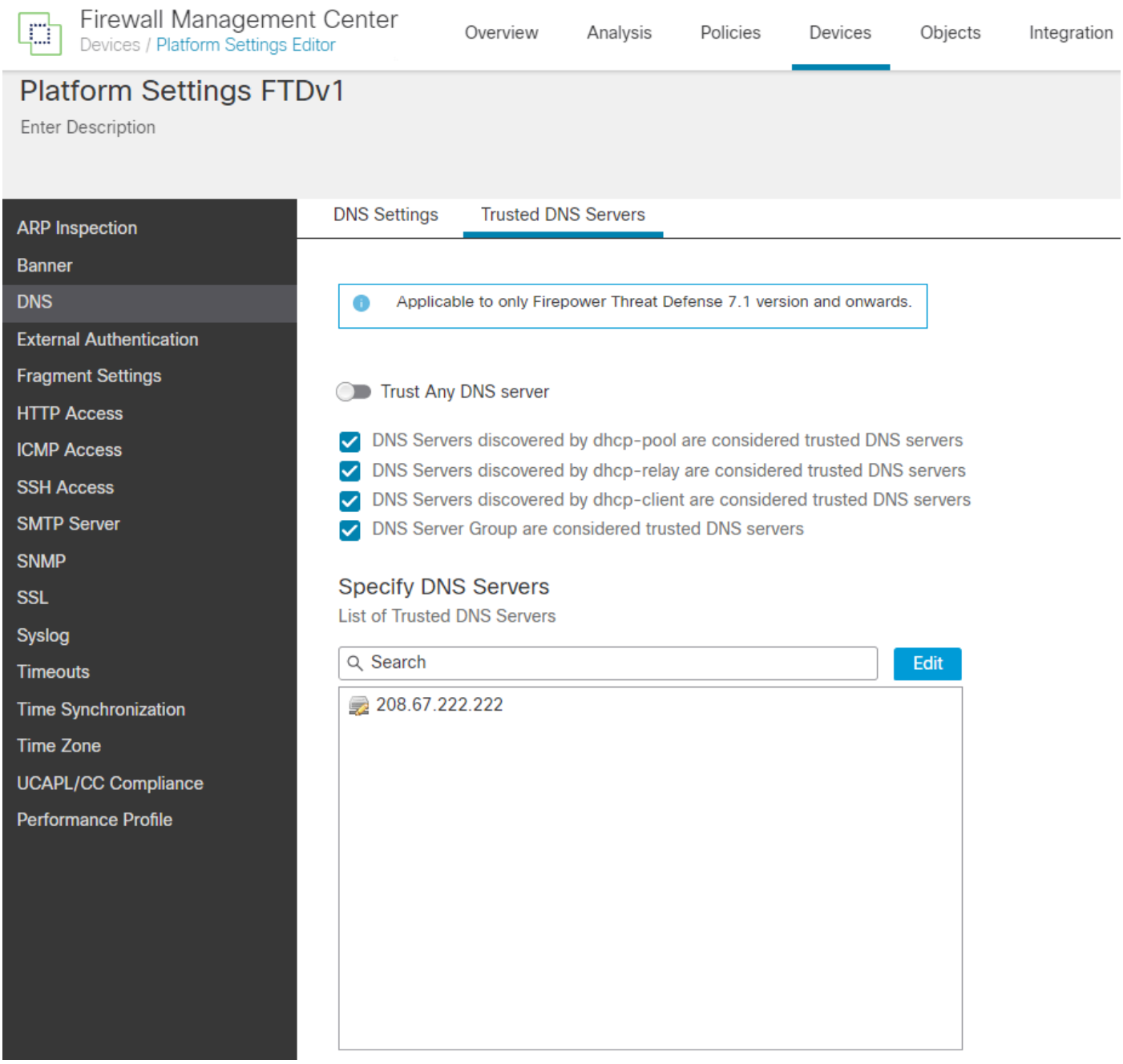
1. Konfigurieren Sie zunächst den IPsec-Tunnel auf dem FMC und auf dem Umbrella Dashboard. Eine Anleitung zum Durchführen dieser Konfiguration finden Sie in der Umbrella-Dokumentation.

2. Stellen Sie sicher, dass der DNS-Server, den das Endbenutzergerät hinter der FTD verwendet, unter Geräte > Plattformeinstellungen > DNS > Vertrauenswürdige DNS-Server als vertrauenswürdiger DNS-Server aufgeführt ist.

Wenn die Geräte einen DNS-Server verwenden, der nicht aufgeführt ist, kann das DNS-Snooping fehlschlagen, und der PBR auf Basis von Apps kann daher nicht funktionieren. Optional (aber aus Sicherheitsgründen nicht empfohlen) können Sie die Option Jeder DNS-Server vertrauen aktivieren, sodass Sie die DNS-Server hinzufügen müssen.



Anmerkung: Wenn VAs als interne DNS-Resolver verwendet werden, müssen sie als vertrauenswürdige DNS-Server hinzugefügt werden.



15669097907860

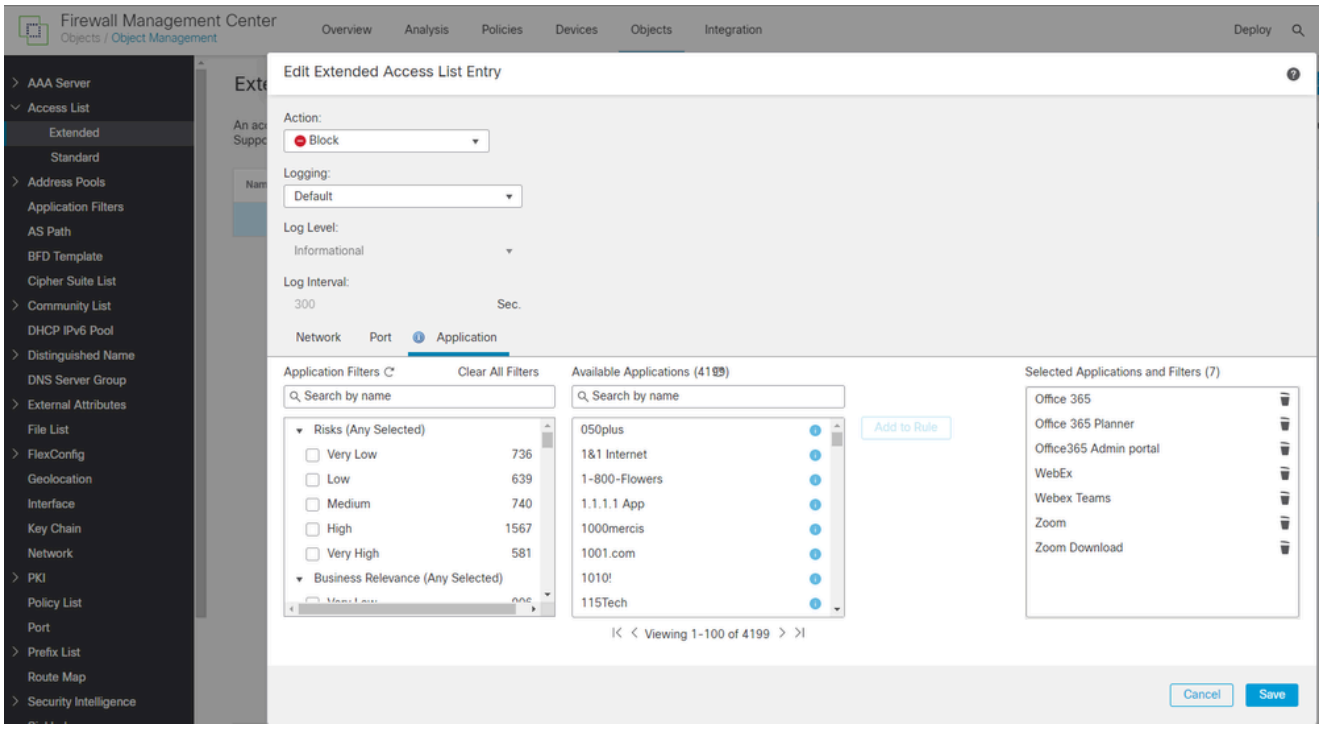
3. Erstellen Sie eine erweiterte Zugriffskontrollliste, die vom FTD für den PBR-Prozess verwendet werden kann, um zu entscheiden, ob der Datenverkehr für SIG an Umbrella gesendet wird oder ob er von IPsec ausgeschlossen und überhaupt nicht an Umbrella gesendet wird.

- Verweigert der ACE auf der ACL, wird der Datenverkehr von der SIG ausgeschlossen.
- Ein permit ACE auf der ACL bedeutet, dass der Datenverkehr über IPsec gesendet wird und eine SIG-Richtlinie (CDFW, SWG usw.) anwenden kann.

In diesem Beispiel werden die Anwendungen "Office365", "Zoom" und "Cisco WebEx" mit einem deny ACE ausgeschlossen. Der restliche Verkehr wird zur weiteren Überprüfung an Umbrella gesendet.

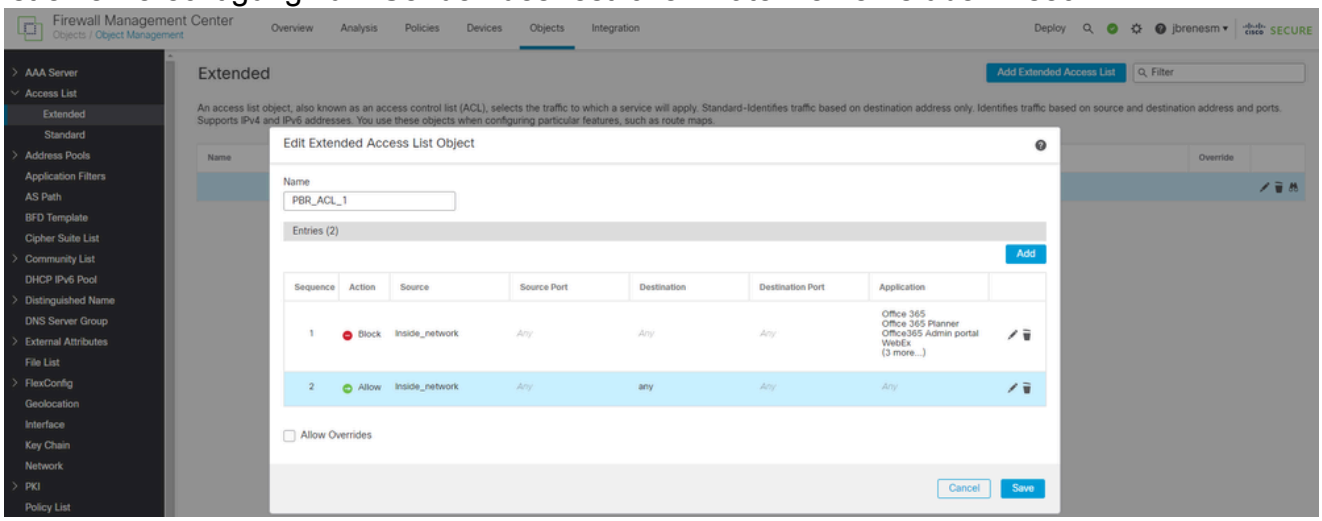
1. Gehen Sie zu Objekt > Objektverwaltung > Zugriffsliste > Erweitert.
2. Definieren Sie das Quellnetzwerk und die Ports wie gewohnt, und fügen Sie dann die

Anwendungen für den PBR hinzu.



15669947000852

Der erste ACE kann für die zuvor erwähnten Anwendungen "leugnen", und der zweite ACE ist eine Berechtigung zum Senden des restlichen Datenverkehrs über IPsec.

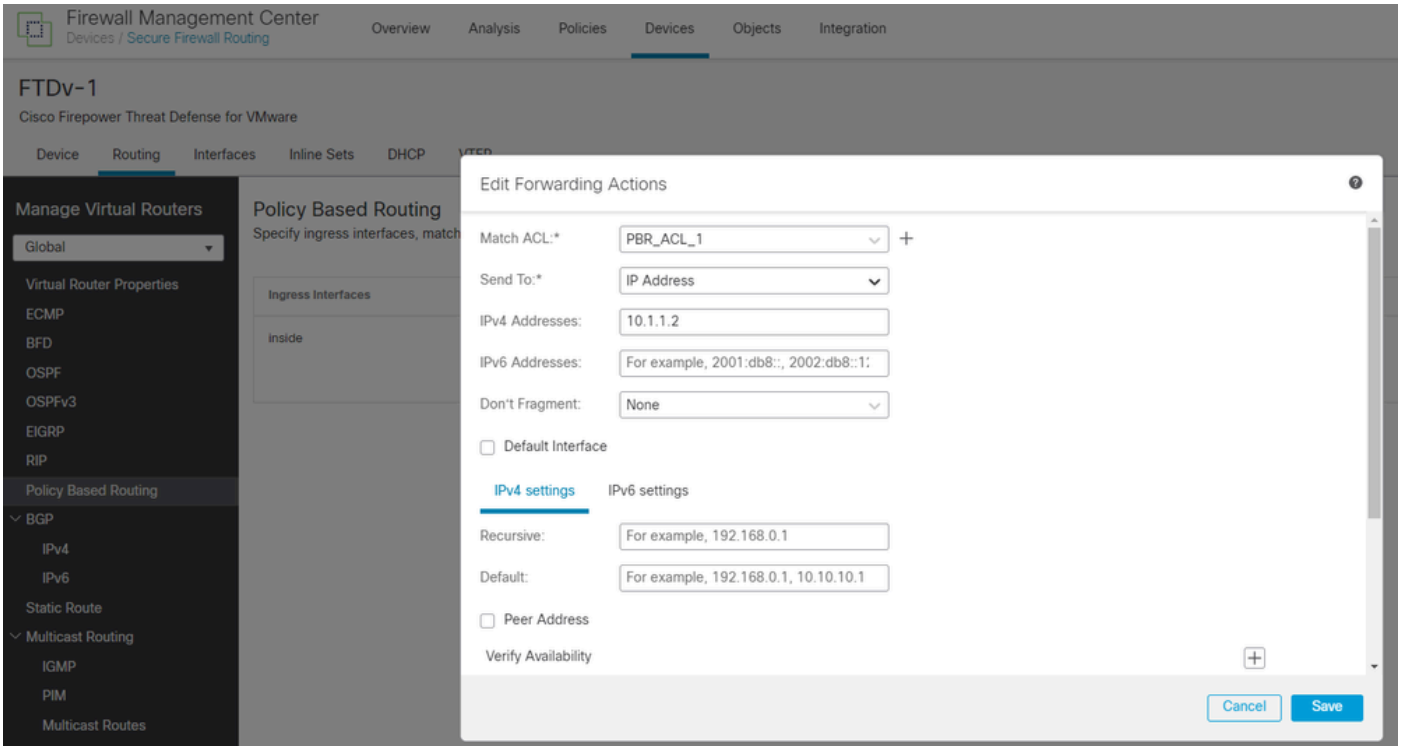


15670006987156

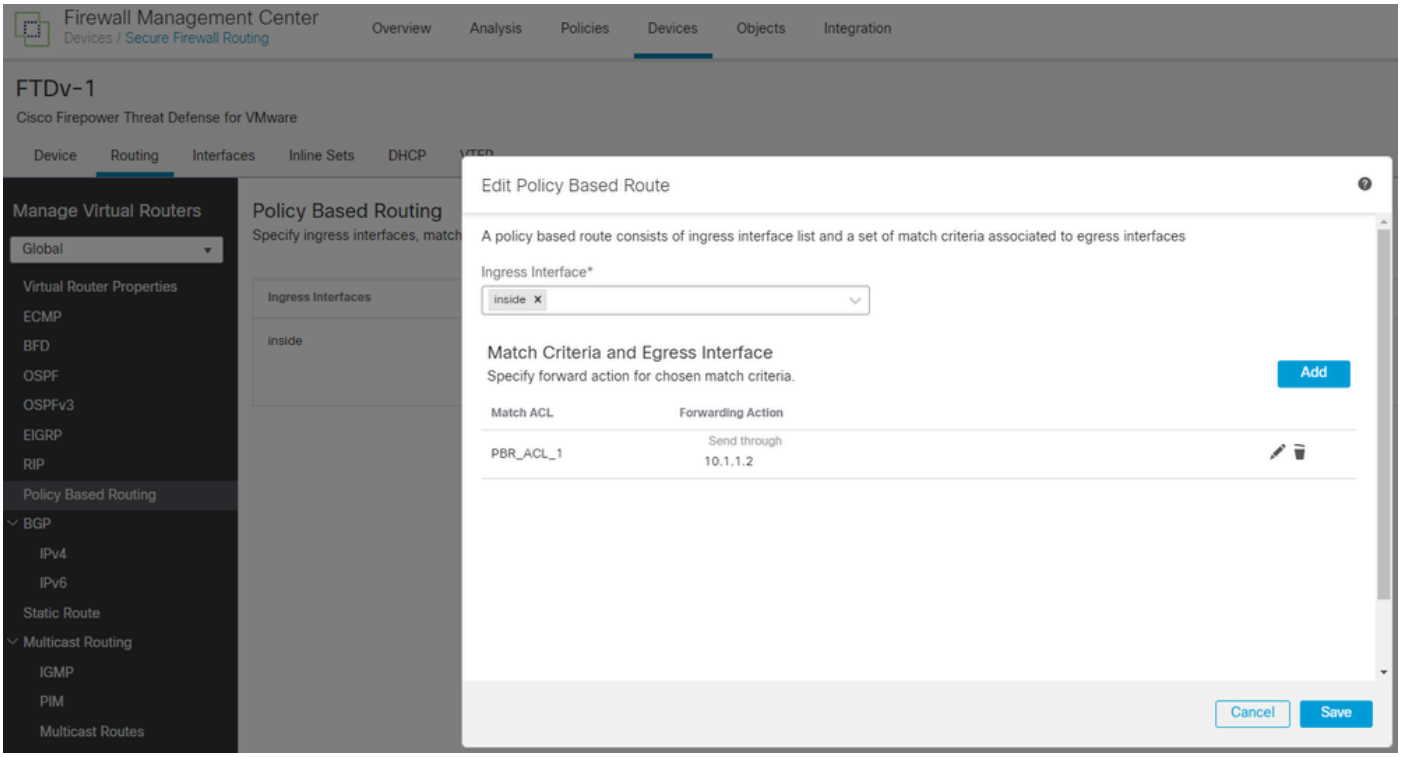
4. Erstellen Sie den PBR unter Devices (Geräte) > Device Management (Geräteverwaltung) > [FTD-Gerät auswählen] > Routing (Routing) > Policy Based Routing (Richtlinienbasiertes Routing).

- Eingangsschnittstelle: Die Schnittstelle, von der der lokale Datenverkehr stammt.
- Übereinstimmende ACL: Die erweiterte ACL wurde im vorherigen Schritt erstellt: ACL "PBR_ACL_1".
- Senden an: IP-Adresse

- IPv4-Adressen: Next-Hop, wenn der PBR eine Anweisung zum Zulassen findet, sodass der Datenverkehr zu der IP geroutet wird, die Sie hier hinzufügen. In diesem Beispiel ist dies die IPsec-IP von Umbrella. Wenn die IP-Adresse Ihres VTI VPNs 10.1.1.1 lautet, würde die IPsec-Adresse von Umbrella aus einem beliebigen Element innerhalb desselben Netzwerks bestehen (z. B. 10.1.1.2).



15670209158036



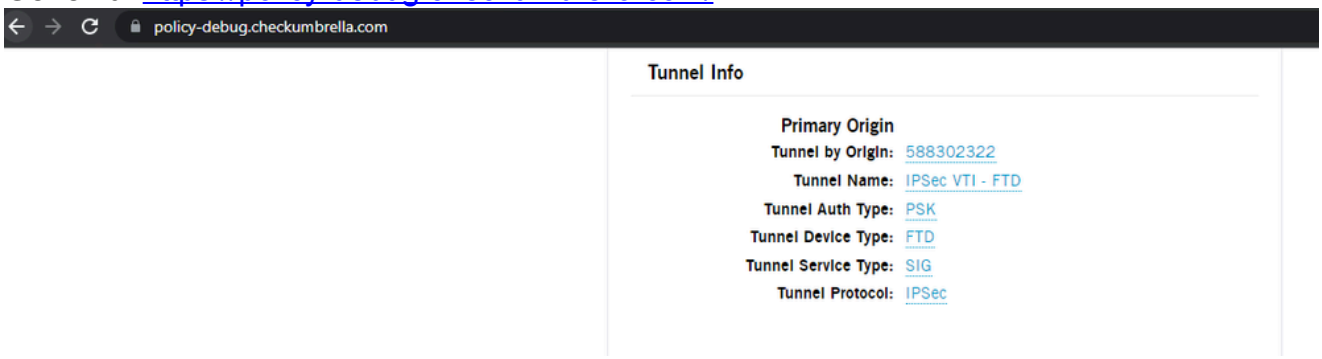
15670247521556

5. Bereitstellen der Änderungen auf dem FMC

Verifizierung

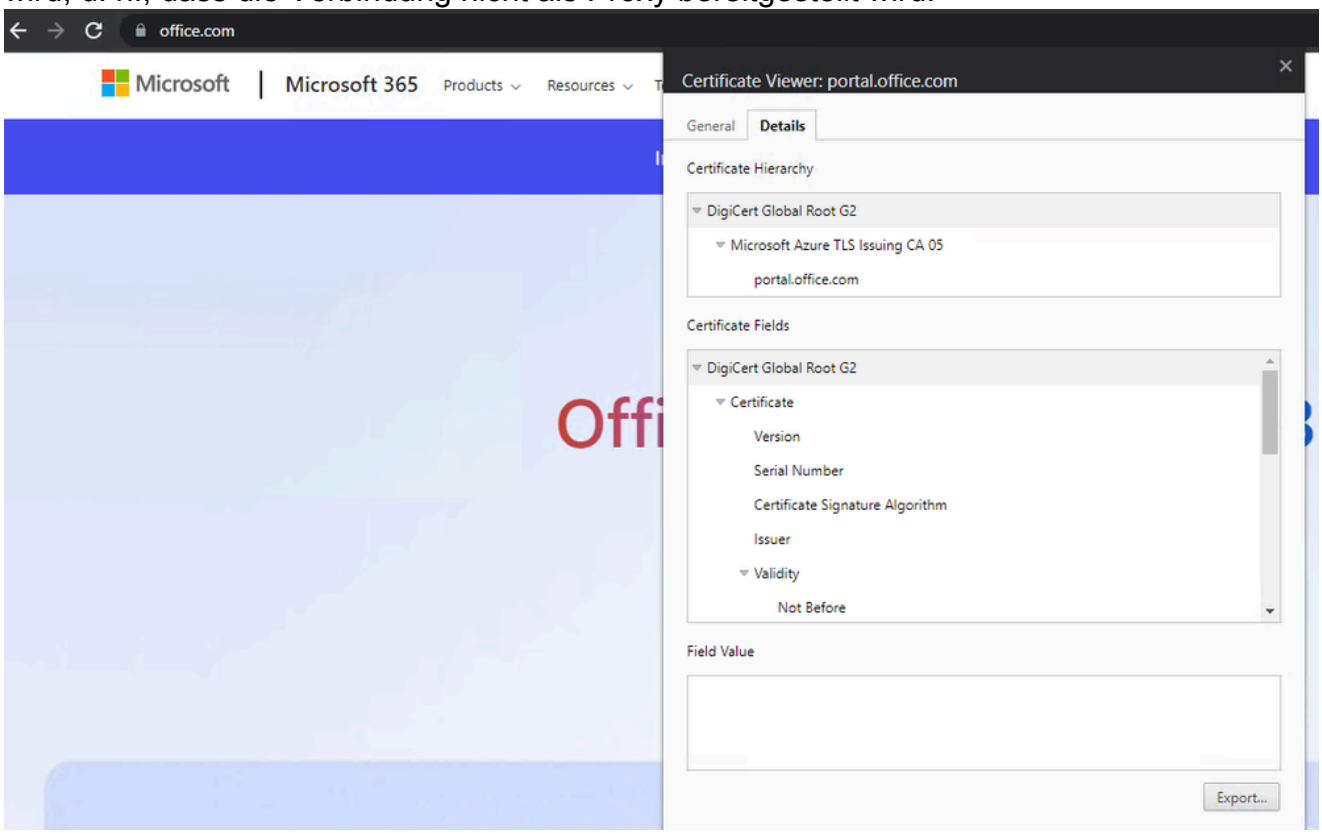
Überprüfen Sie auf dem Test-PC hinter dem FTD Folgendes:

- Der Datenverkehr vom PC wird tatsächlich über IPsec an Umbrella gesendet.
  Gehe zu: https://policy-debug.checkumbrella.com/



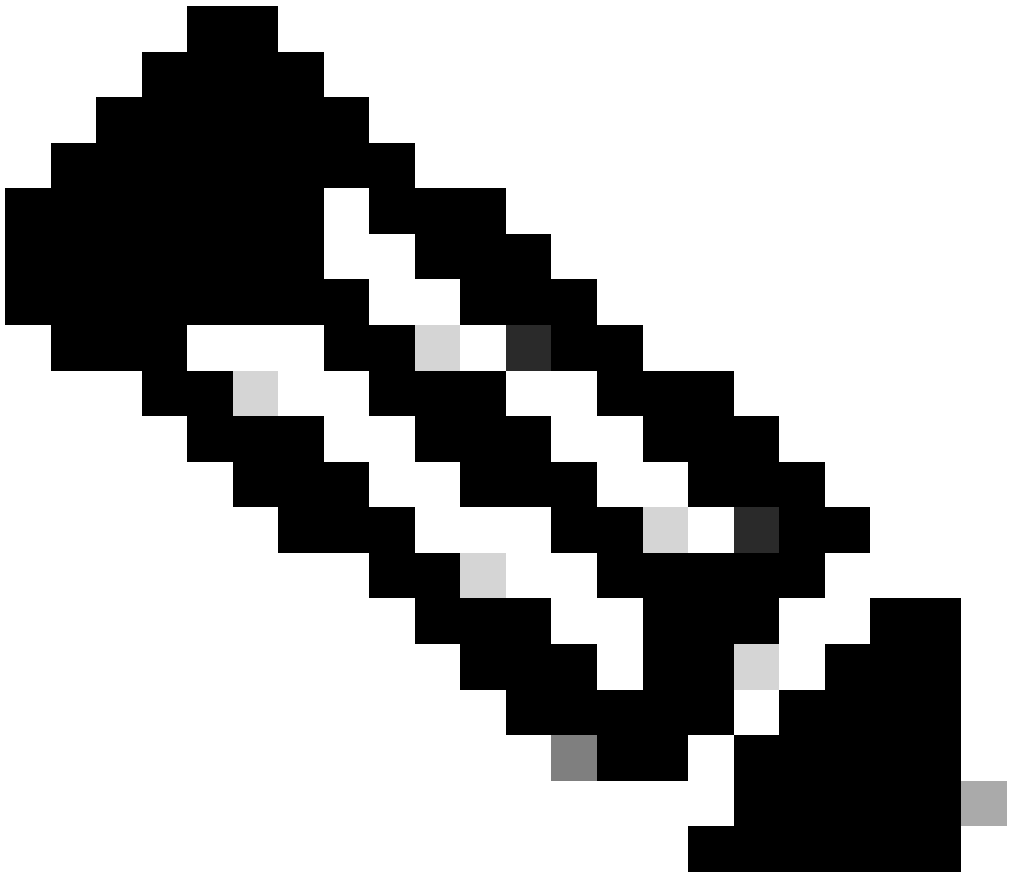
15670737148948

- Versuchen Sie, einen der Standorte aufzurufen, die in der PBR/ACL-Konfiguration ausgeschlossen sind, und stellen Sie sicher, dass die Umbrella-Root-CA nicht angezeigt wird, d. h., dass die Verbindung nicht als Proxy bereitgestellt wird:

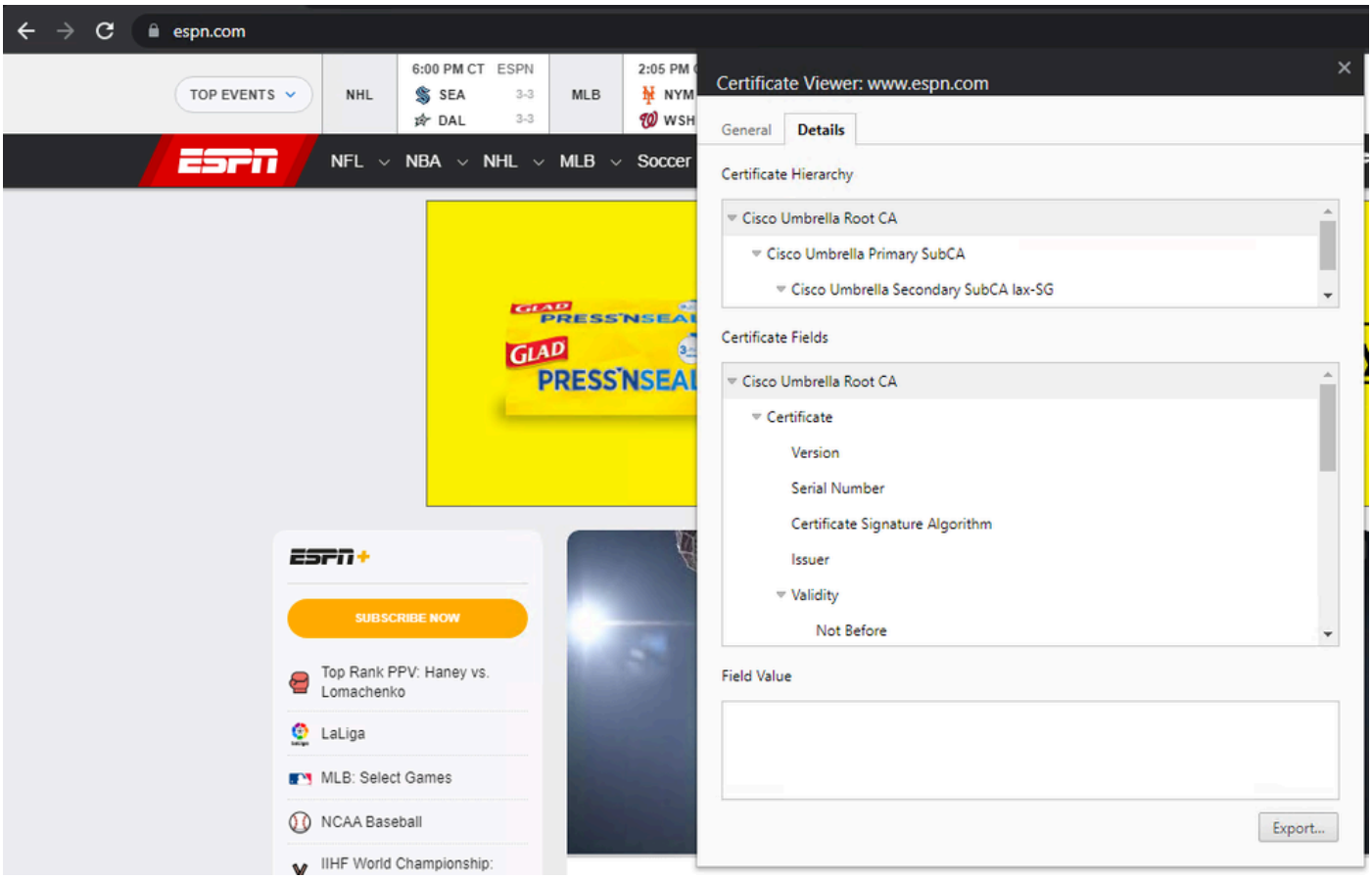


15670820980756

- Versuchen Sie, einen anderen Standort aufzurufen, der nicht auf den vom PBR ausgeschlossenen Anwendungen basiert, und vergewissern Sie sich, dass Umbrella tatsächlich ein Proxy für die Verbindung ist:



Anmerkung: Um Probleme mit einer nicht vertrauenswürdigen Warnseite zu vermeiden, stellen Sie sicher, dass das Umbrella Root CA-Zertifikat installiert ist.



- In der Kommandozeile der FTD können Sie einige Befehle ausführen, um zu bestätigen, dass die Konfiguration ordnungsgemäß weitergeleitet wurde und funktioniert:
  - `show run route-map` (prüft die PBR-Konfiguration):

```
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#
```

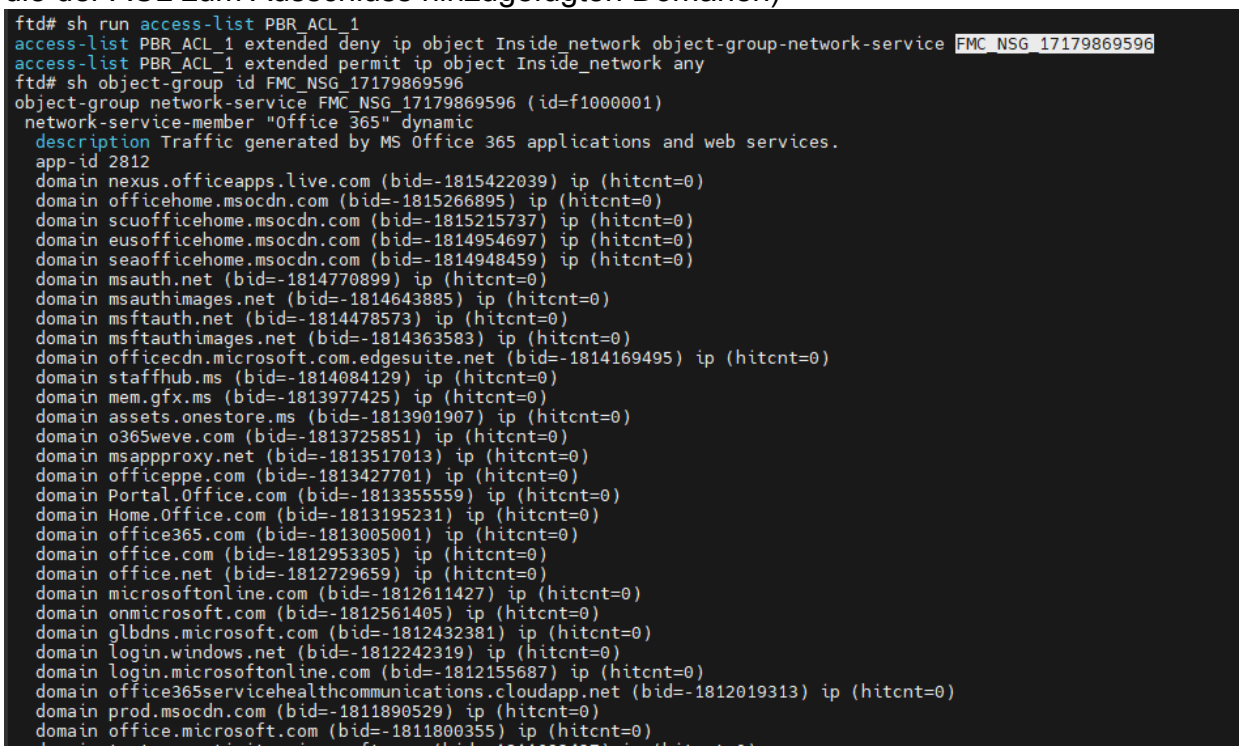
15670322054036

  - `show run interface gigabitEthernet 0/1` (überprüft, ob PBR auf die richtige Schnittstelle angewendet wird)

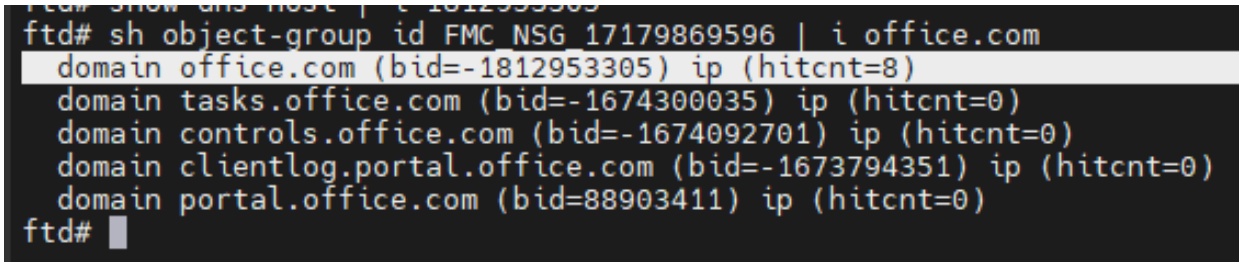
```
ftd# sh run interface gigabitEthernet 0/1
!
interface GigabitEthernet0/1
 nameif inside
 security-level 0
 ip address 172.16.72.1 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1682004086289
ftd#
```

15678344219540

- `show run access-list PBR_ACL_1, show object-group id FMC_NSG_17179869596` (bestätigt die der ACL zum Ausschluss hinzugefügten Domänen)



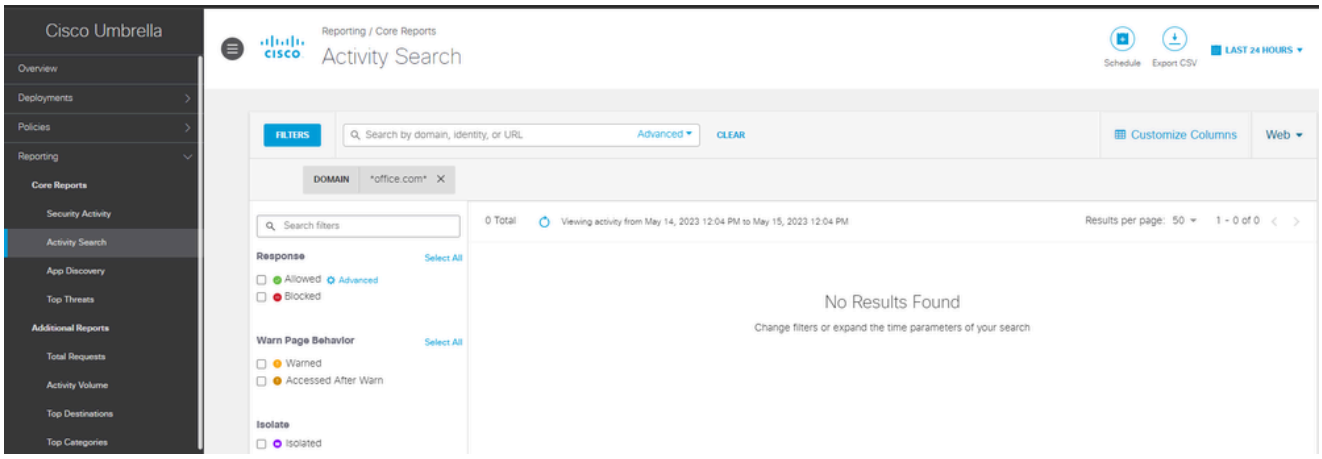
15670420887316



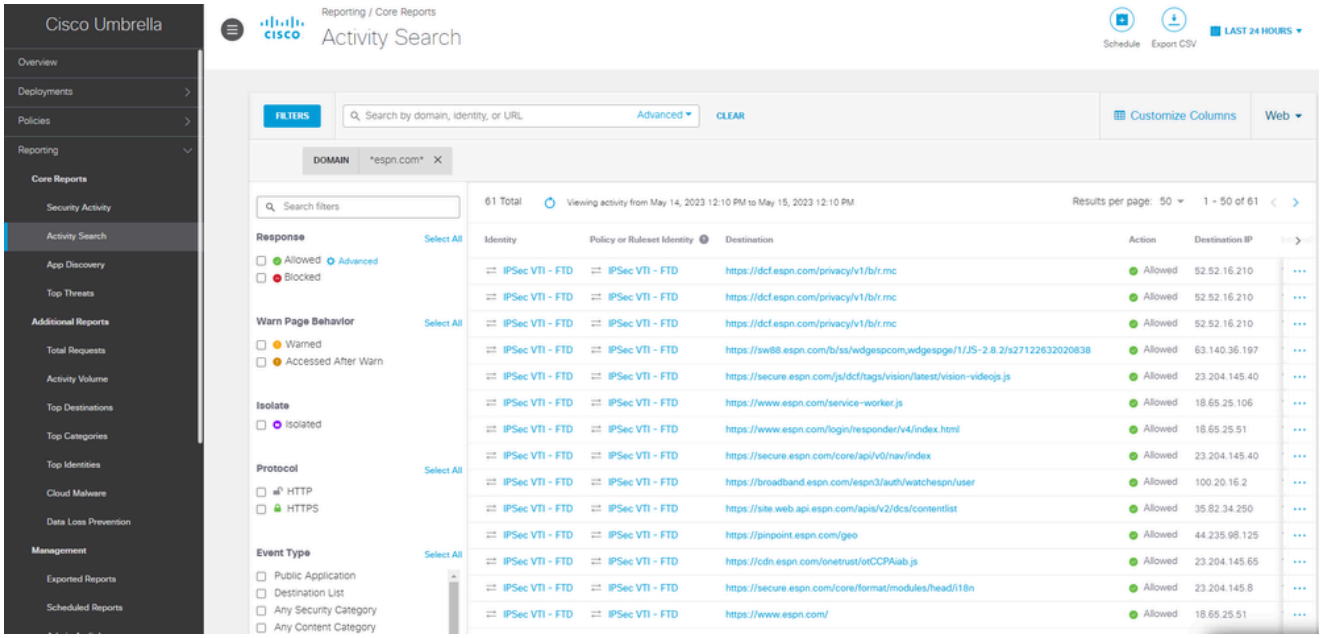
15670635784852

- `Packet-Tracer-Eingabe in tcp 172.16.72.10 1234 fqdn office.com 443 detailliert` (verifiziert, dass die externe Schnittstelle als Ausgabe verwendet wird und nicht die VTI-Schnittstelle)

- Auf dem Umbrella Dashboard können Sie unter Aktivitätssuche sehen, dass der Webdatenverkehr unter office.com nie an Umbrella gesendet wurde, während der Datenverkehr unter espn.com gesendet wurde.



15671098042516



15671302832788

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.