Configurare PBR basato sull'applicazione FTD per Umbrella SIG

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Panoramica

- Limitazioni

PBR basato sull'applicazione

Verifica

Introduzione

In questo documento viene descritto come configurare Firewall Threat Defense (FTD) Application-Based Policy Based Routing (PBR) per Umbrella SIG.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso a Umbrella Dashboard
- Accesso amministrativo al FMC che esegue 7.1.0+ per distribuire la configurazione al FTD versione 7.1.0+. Il PBR basato sulle app è supportato solo nella versione 7.1.0 e successive
- (Preferito) Conoscenza della configurazione di FMC/FTD e Umbrella SIG
- (Facoltativo ma consigliato): Certificato radice Umbrella installato. Utilizzato da SIG quando il traffico è inoltrato o bloccato. Per ulteriori dettagli sull'installazione del certificato radice, consultare la documentazione di Umbrella.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il SIG (Cisco Umbrella Secure Internet Gateway).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Le informazioni discusse in questo documento permettono di configurare la modalità di distribuzione del PBR basato su applicazioni sull'FTD quando si stabilisce un tunnel VTI SIG IPsec per Umbrella, in modo da poter escludere o includere il traffico su una VPN basata su applicazioni che usano il PBR.

Nell'esempio di configurazione descritto in questo articolo viene illustrato come escludere alcune applicazioni dalla VPN IPsec durante l'invio di tutti gli altri elementi tramite la VPN.

Per informazioni complete su PBR in FMC, vedere la documentazione di Cisco.

Limitazioni

- Impossibile definire sia l'indirizzo di applicazione che quello di destinazione in una voce ACE.

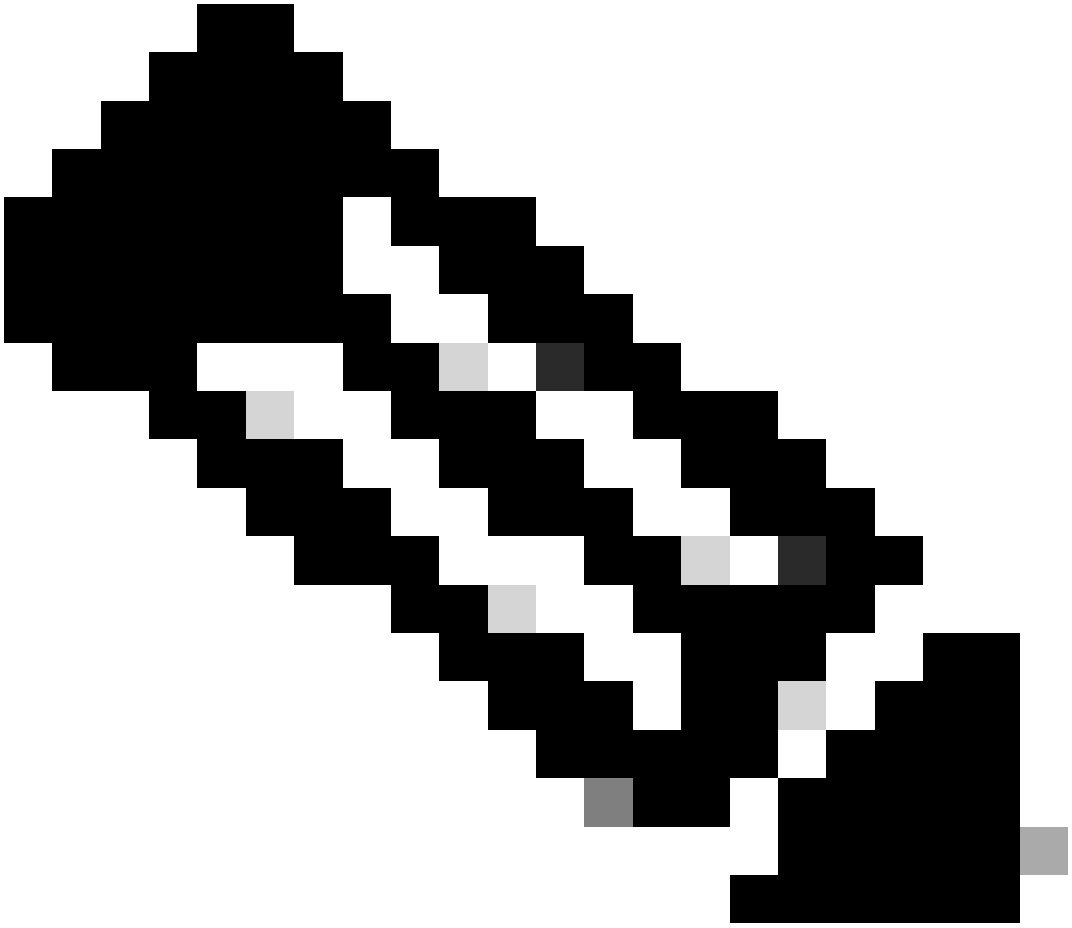
- Durante la definizione dell'ACL per i criteri di corrispondenza dei criteri, è possibile selezionare più applicazioni da una lista di applicazioni predefinite per formare una voce di controllo di accesso (ACE, Access Control Entry).
  Al momento non è possibile aggiungere o modificare l'elenco delle applicazioni predefinite.
- Per le applicazioni non elencate nell'elenco delle applicazioni predefinite in FMC o per qualsiasi comportamento imprevisto con un'applicazione, è possibile utilizzare IP anziché applicazioni in PBR.
- Per un elenco completo delle limitazioni, fare riferimento alla documentazione del PBR.

PBR basato sull'applicazione

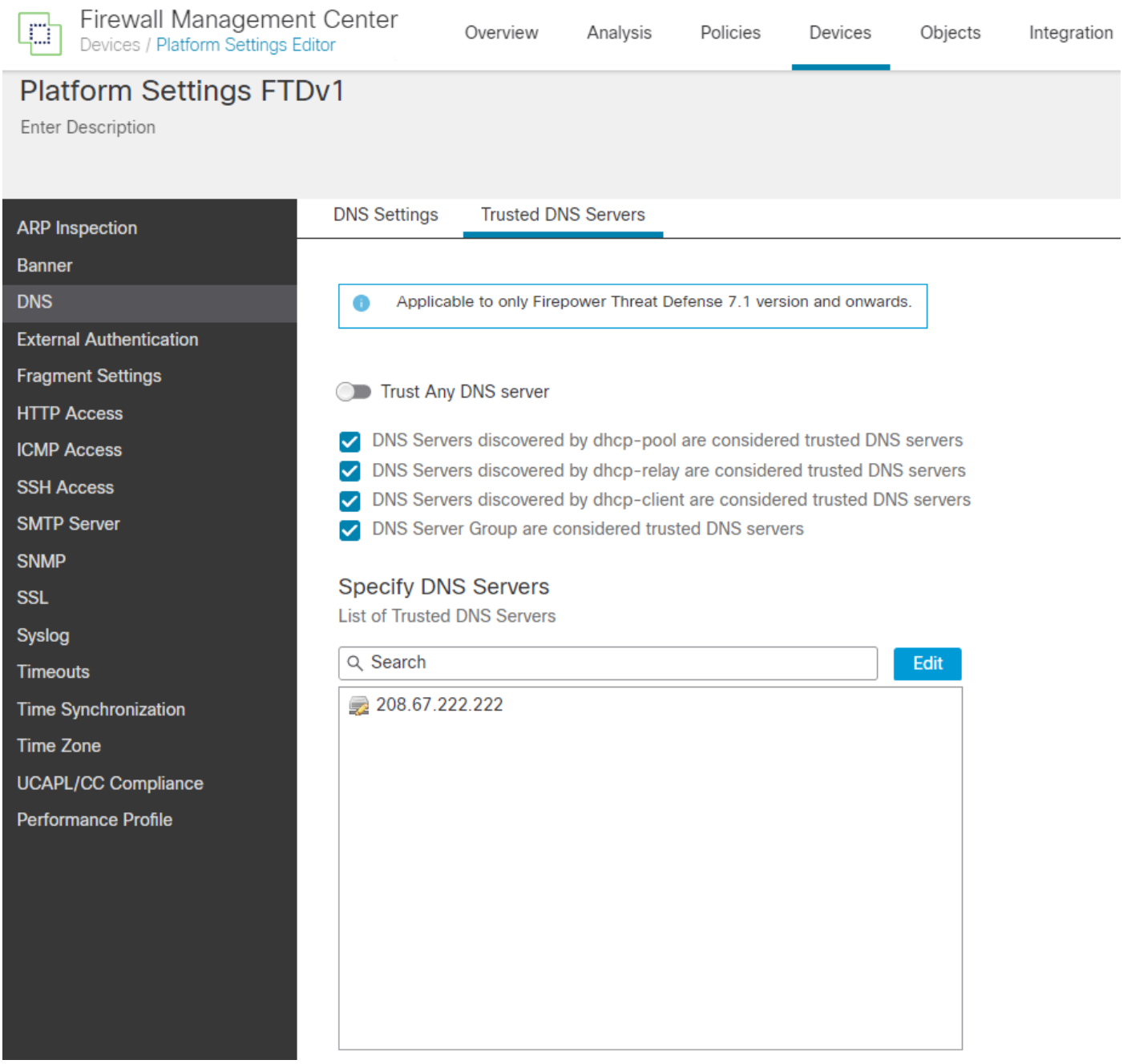
1. Iniziare configurando il tunnel IPsec sul FMC e sul dashboard Umbrella. Le istruzioni su come eseguire questa configurazione sono disponibili nella documentazione di Umbrella.

2. Verificare che il server DNS utilizzato dal dispositivo dell'utente finale dietro l'FTD sia elencato come server DNS trusted in Dispositivi > Impostazioni piattaforma > DNS > Server DNS trusted.

Se i dispositivi utilizzano un server DNS non presente nell'elenco, lo snooping DNS può non riuscire e pertanto il PBR basato sulle app non può funzionare. Facoltativamente (ma non consigliato per motivi di sicurezza), è possibile attivare l'opzione Considera attendibili tutti i server DNS in modo che sia necessario aggiungere i server DNS.



Nota: Se i server di virtualizzazione vengono utilizzati come resolver DNS interni, è necessario aggiungerli come server DNS trusted.



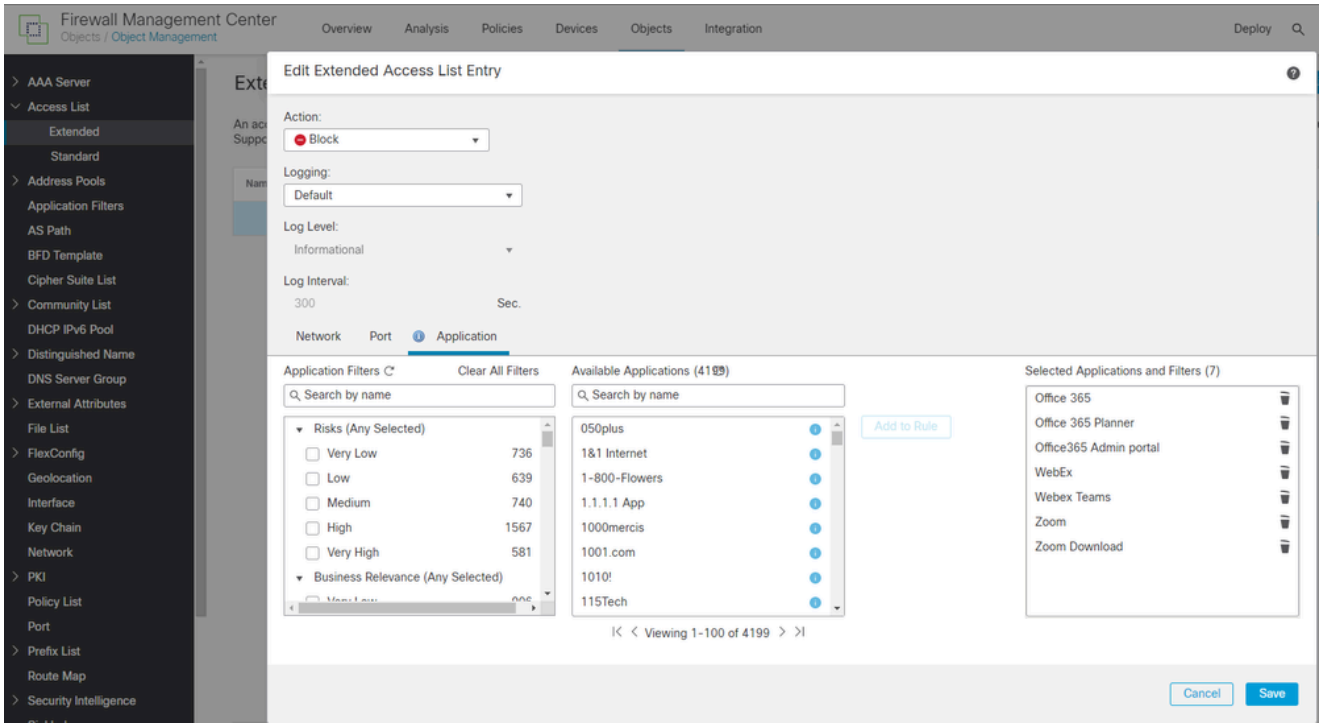
15669097907860

3. Creare un ACL esteso che possa essere usato dall'FTD per il processo PBR al fine di decidere se il traffico venga inviato alla Umbrella per il SIG o se venga escluso dall'IPsec e non venga inviato affatto alla Umbrella.

- Se si nega l'ACE nell'ACL, il traffico viene escluso dal SIG.
- Una voce ACE consentita sull'ACL indica che il traffico viene inviato tramite IPsec e può applicare una policy SIG (CDFW, SWG, ecc.).

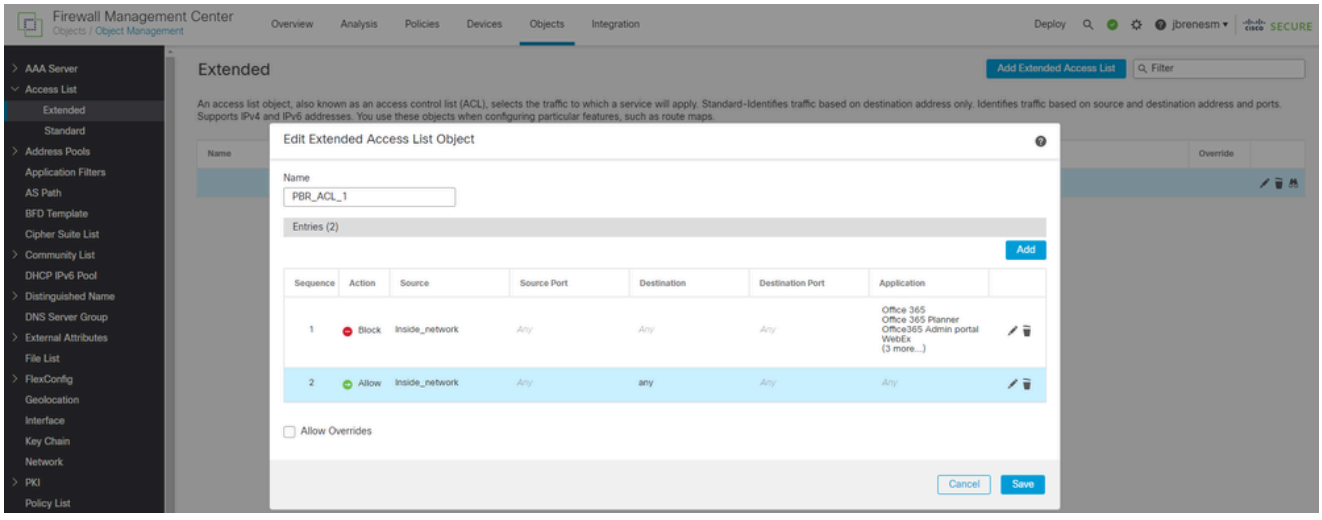
Nell'esempio vengono escluse le applicazioni "Office365", "Zoom" e "Cisco Webex" con una voce di accesso negata. Il resto del traffico è stato inviato alla Umbrella per ulteriori ispezioni.

1. Selezionare Oggetto > Gestione oggetti > Elenco accessi > Esteso.
2. Definire la rete di origine e le porte come di consueto, quindi aggiungere le applicazioni da utilizzare nel PBR.



15669947000852

La prima ACE può "negare" per le applicazioni menzionate in precedenza, mentre la seconda ACE è un'autorizzazione a inviare il resto del traffico su IPsec.

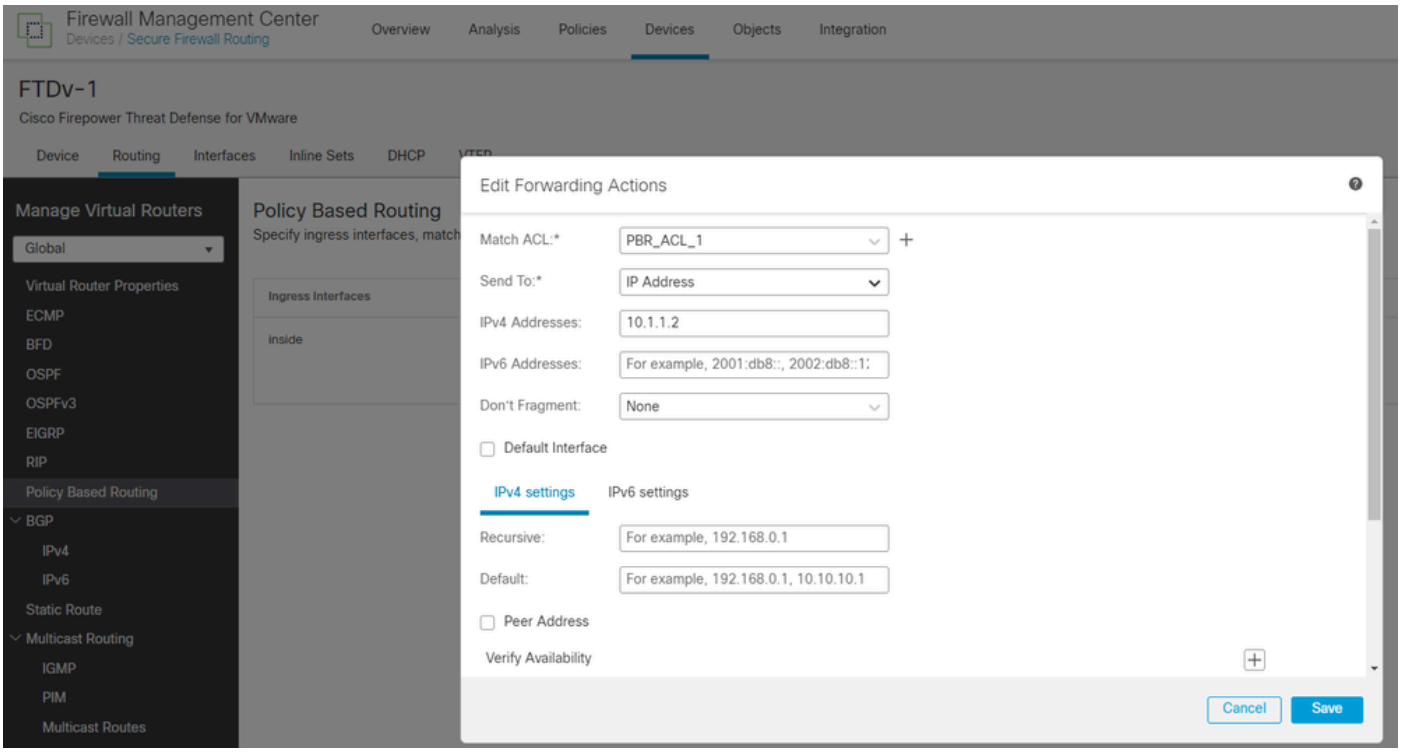


15670006987156

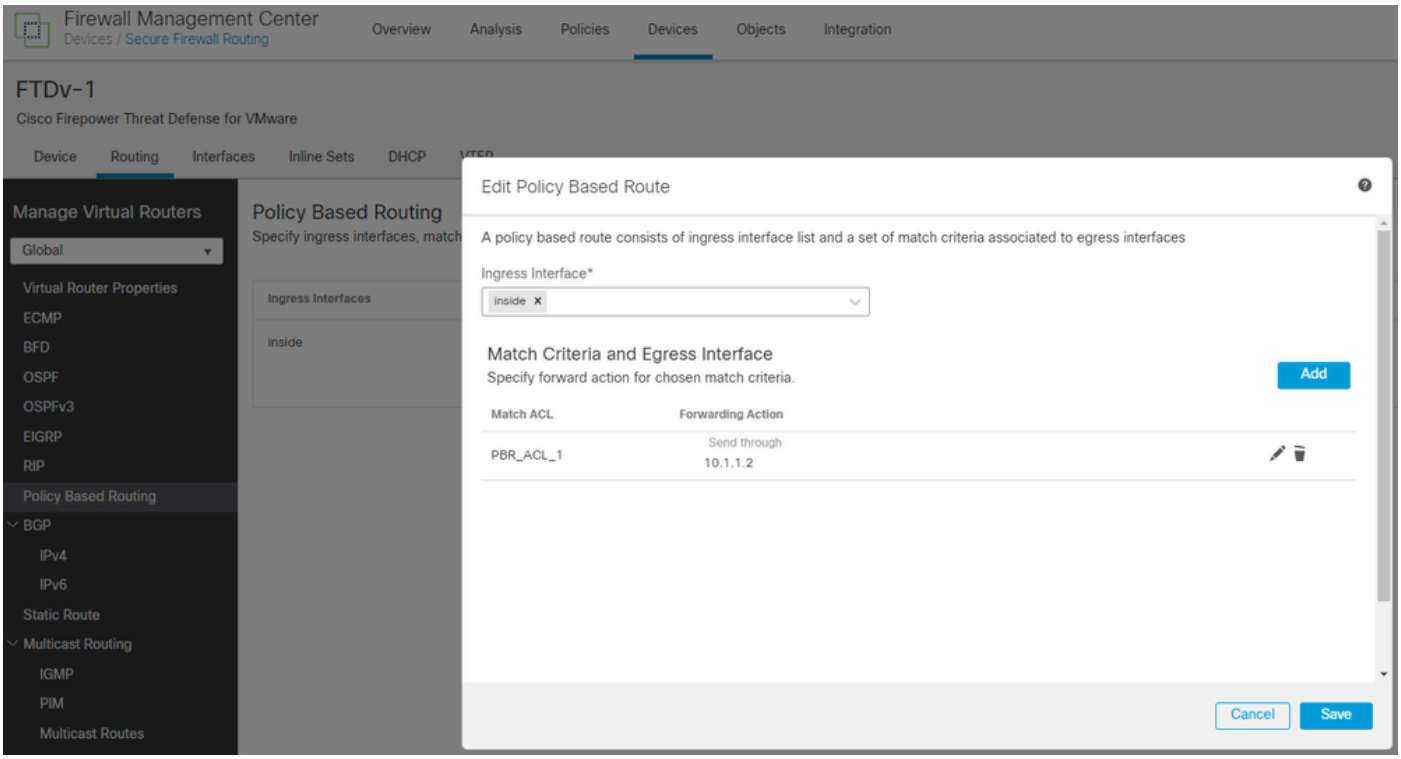
4. Creare il PBR in Dispositivi > Gestione dispositivi > [selezionare il dispositivo FTD] > Routing > Policy Based Routing.

- Interfaccia in ingresso: Interfaccia da cui proviene il traffico locale.
- ACL corrispondente: ACL esteso creato nel passaggio precedente, ACL "PBR_ACL_1".
- Invia a: Indirizzo IP
- Indirizzi IPv4: L'hop successivo viene eseguito quando il PBR trova un'istruzione di autorizzazione, in modo che il traffico venga instradato all'IP aggiunto qui. In questo esempio, questo è l'IPsec di Umbrella. Se l'IP della tua VPN VTI è 10.1.1.1, l'IPsec della

Umbrella sarà qualsiasi cosa all'interno della stessa rete (ad esempio, 10.1.1.2).



15670209158036



15670247521556

5. Apportare le modifiche al CCP.

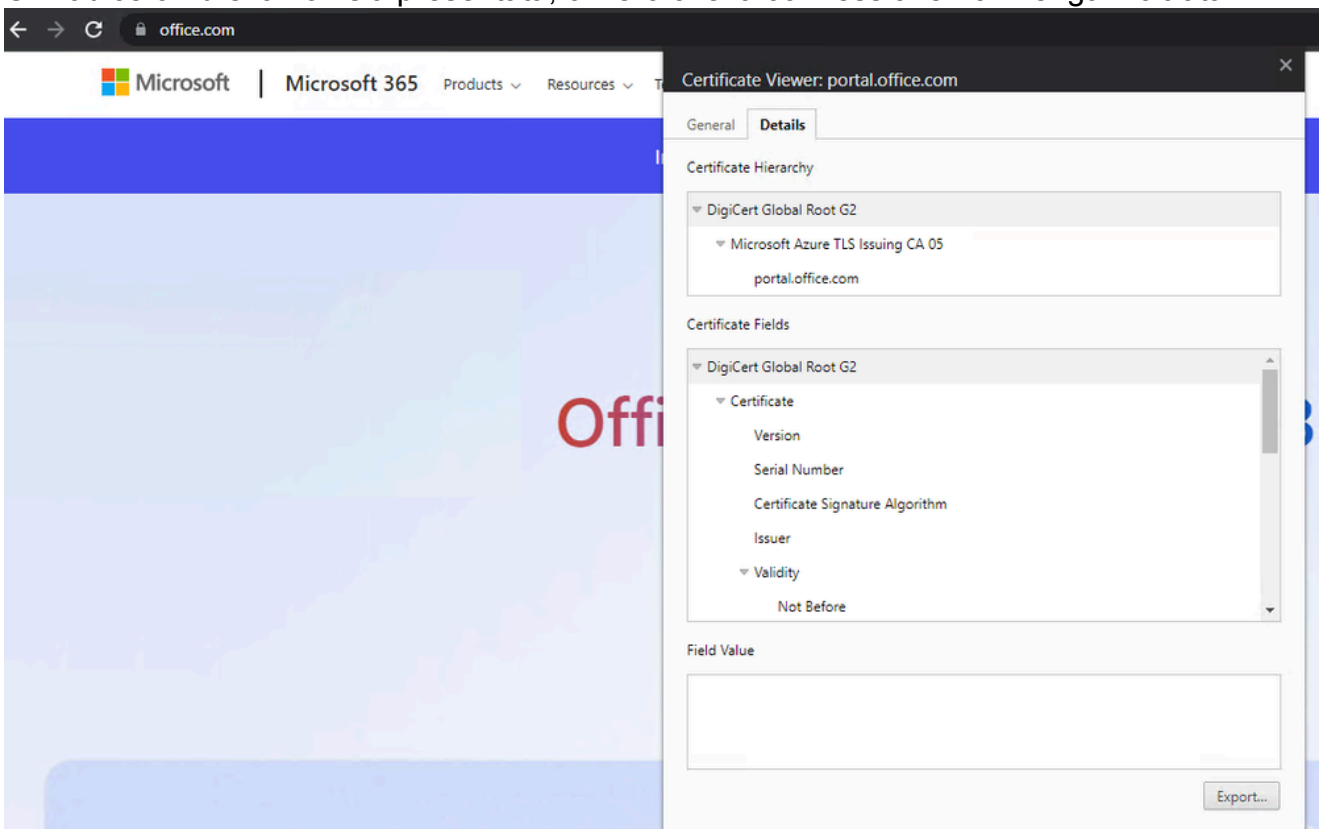
Verifica

Sul PC di prova situato dietro l'FTD, controllare:

- Il traffico proveniente dal PC viene in realtà inviato tramite IPsec a Umbrella.
  Vai a: https://policy-debug.checkumbrella.com/

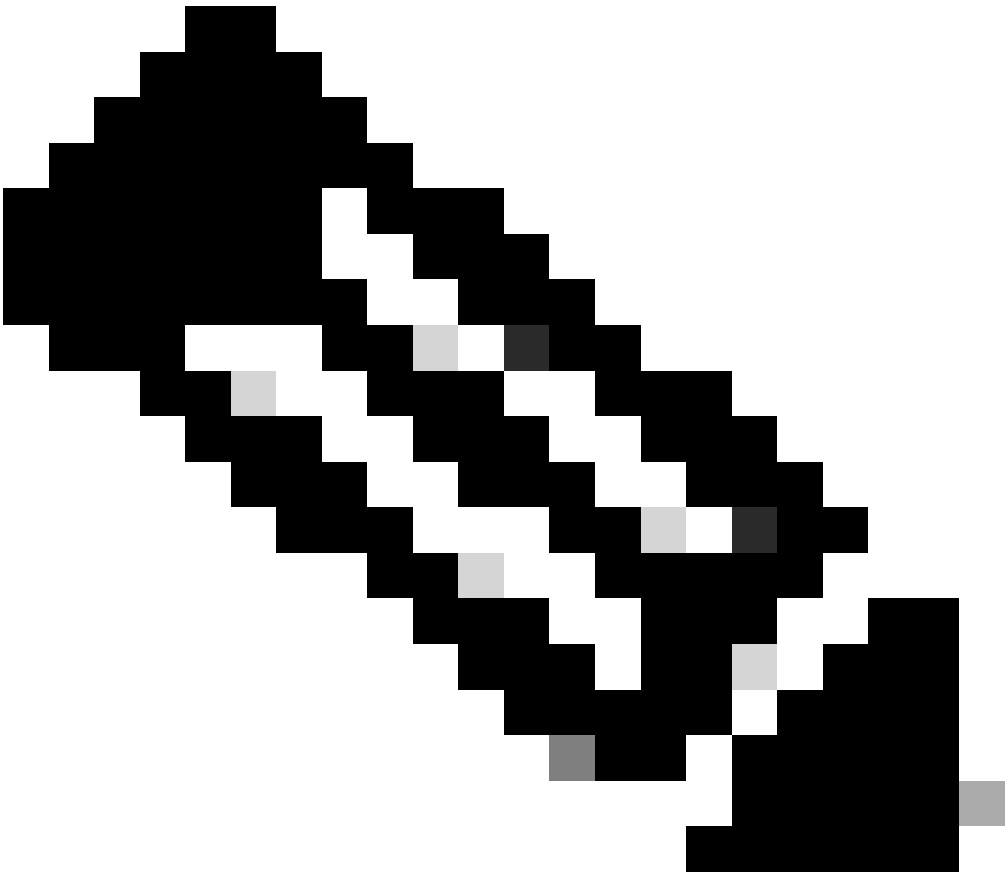
15670737148948

- Provare ad accedere a uno dei siti esclusi dalla configurazione PBR/ACL e verificare che la CA radice ombrello non sia presentata, ovvero che la connessione non venga inoltrata:

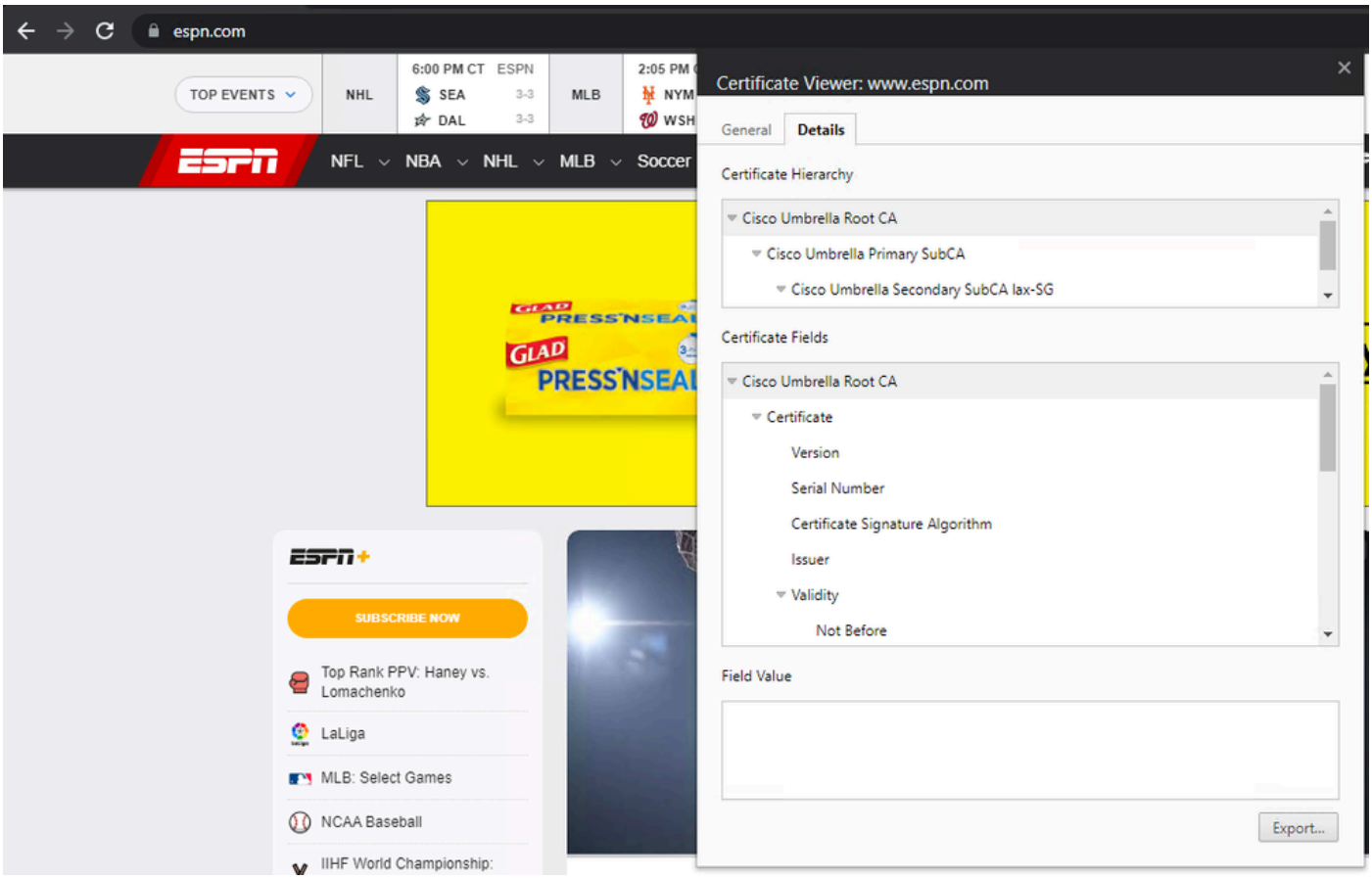


15670820980756

- Provare a visitare qualsiasi altro sito non basato sulle applicazioni escluse dal PBR e verificare che Umbrella stia effettivamente eseguendo il proxy della connessione:



Nota: Per evitare problemi quando una pagina di avviso non è considerata attendibile, verificare che il certificato CA radice Umbrella sia installato.



- Dalla CLI dell'FTD, è possibile eseguire alcuni comandi per verificare che la configurazione sia stata spinta correttamente e funzioni correttamente:
  - `show run route-map` (verifica la configurazione PBR):

```
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#
```

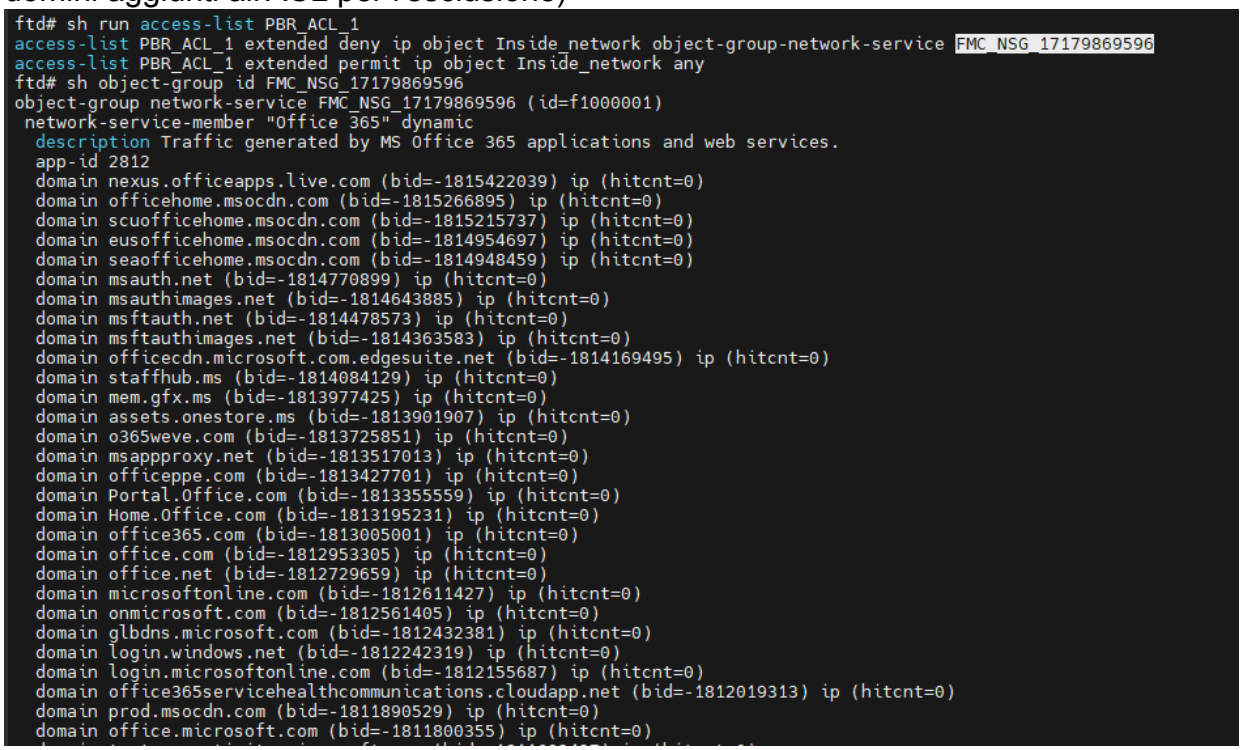
15670322054036

  - `show run interface gigabit Ethernet 0/1` (controlla che il PBR sia applicato all'interfaccia corretta)

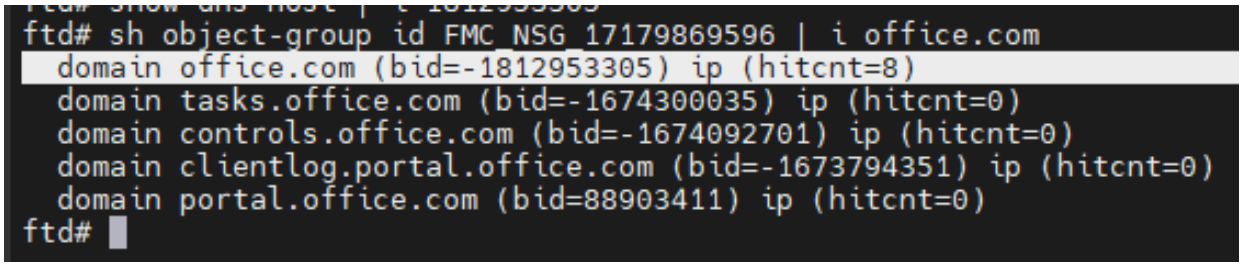
```
ftd# sh run interface gigabitEthernet 0/1
!
interface GigabitEthernet0/1
 nameif inside
 security-level 0
 ip address 172.16.72.1 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1682004086289
ftd#
```

15678344219540

- `show run access-list PBR_ACL_1, show object-group id FMC_NSG_17179869596` (conferma i domini aggiunti all'ACL per l'esclusione)



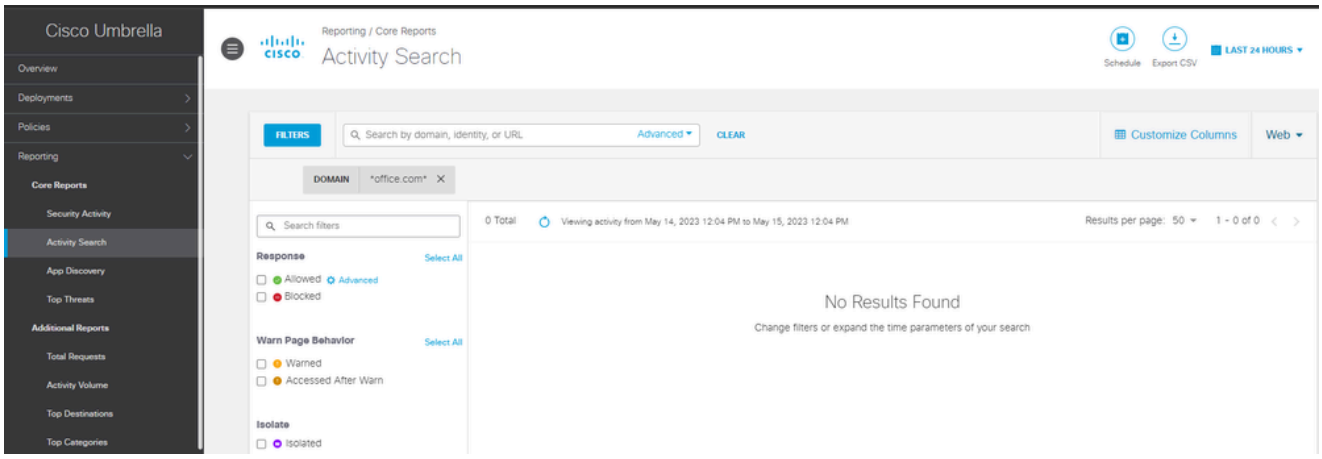
15670420887316



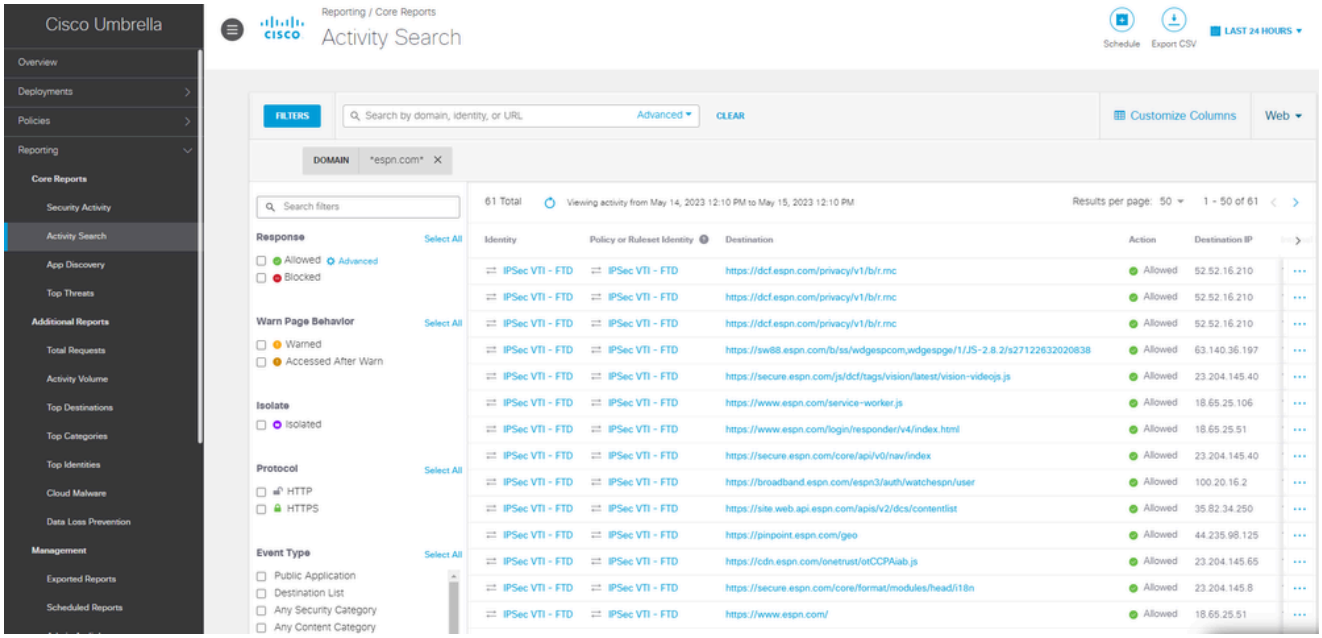
15670635784852

- `input packet-tracer all'interno di tcp 172.16.72.10 1234 fqdn office.com 443 dettagliato` (verifica che l'interfaccia esterna venga utilizzata come output e non quella VTI)

- Sulla pagina Umbrella Dashboard, in activity search, si vede che il traffico web diretto a office.com non è mai stato inviato a Umbrella, mentre il traffico diretto a espn.com è stato inviato.



15671098042516



15671302832788

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).