Configurazione e risoluzione dei problemi di Cisco Threat Intelligence Director

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Threat Intelligence Director (TID) e risolvere i relativi problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione di Firepower Management Center (FMC).

Prima di configurare la funzionalità Cisco Threat Intelligence Director, è necessario verificare le seguenti condizioni:

- Firepower Management Center (FMC):
  - Deve essere eseguito nella versione 6.2.2 (o successiva) (può essere ospitato in un FMC fisico o virtuale).
  - Deve essere configurato con almeno 15 GB di memoria RAM.
  - Deve essere configurato con l'accesso all'API REST abilitato.
- Il sensore deve eseguire la versione 6.2.2 (o successiva).
- Nella scheda Impostazioni avanzate dell'opzione dei criteri di controllo di accesso, è necessario abilitare Abilita Threat Intelligence Director.
- Aggiungere regole ai criteri di controllo di accesso se non sono già presenti.
- Se si desidera che gli oggetti osservabili SHA-256 generino osservazioni ed eventi di

Firepower Management Center, creare una o più regole per i file di ricerca nel cloud di malware o di blocco del malware e associare i criteri dei file a una o più regole nei criteri di controllo di accesso.
- Se si desidera che le osservazioni relative a IPv4, IPv6, URL o nome di dominio generino eventi di intelligence di sicurezza e connessione, abilitare la registrazione di intelligence di sicurezza e connessione nei criteri di controllo di accesso.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

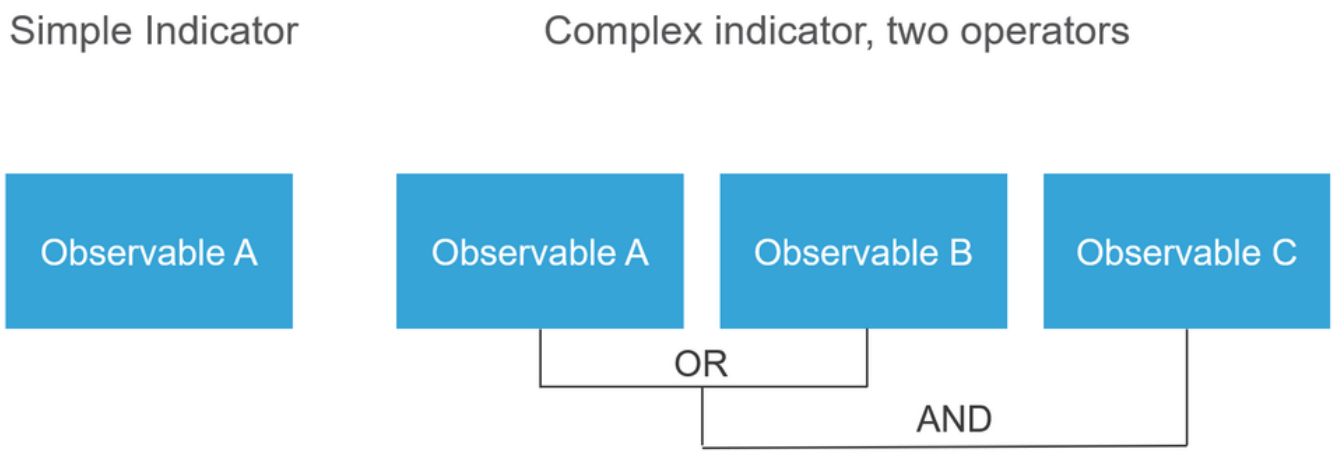
- Cisco Firepower Threat Defense (FTD) Virtual con 6.2.2.81
- Firepower Management Center Virtual (vFMC) con 6.2.2.81

Nota: 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.

Premesse

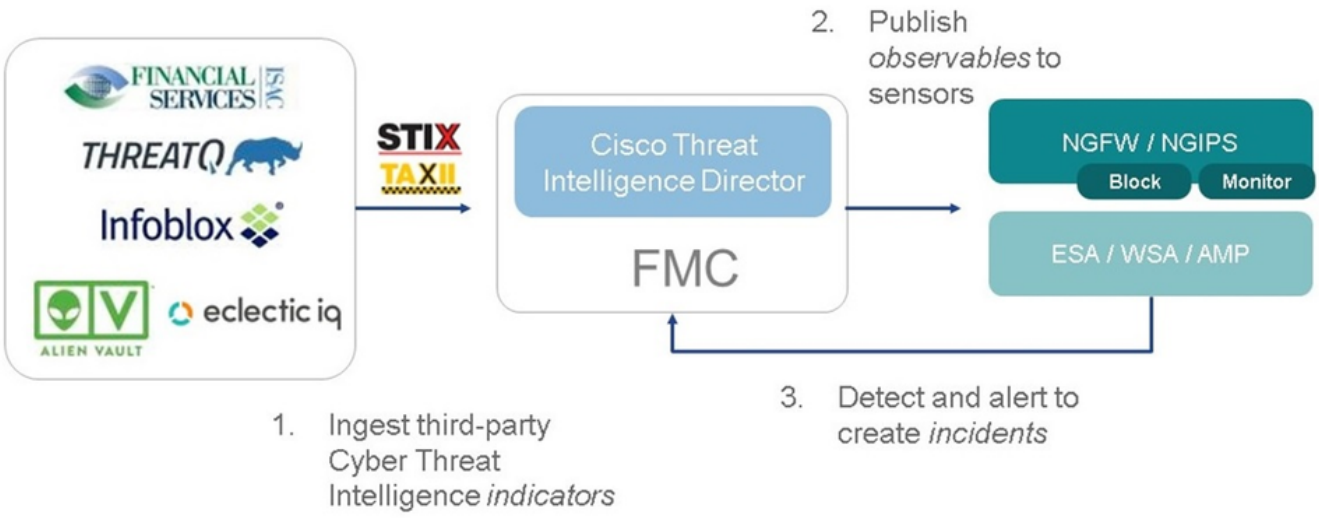
Cisco Threat Intelligence Director (TID) è un sistema che rende operative le informazioni di intelligence sulle minacce. Il sistema utilizza e normalizza l'intelligence eterogenea delle minacce informatiche di terze parti, pubblica l'intelligence sulle tecnologie di rilevamento e mette in correlazione le osservazioni dalle tecnologie di rilevamento.

Ci sono tre nuovi termini: osservabili, indicatori e incidenti. Observable è solo una variabile, che può essere ad esempio URL, dominio, indirizzo IP o SHA256. Gli indicatori sono ricavati da osservabili. Esistono due tipi di indicatori. Un indicatore semplice contiene solo un indicatore osservabile. Nel caso di indicatori complessi, esistono due o più osservabili che sono collegati tra loro utilizzando funzioni logiche quali AND e OR. Quando il sistema rileva traffico che deve essere bloccato o monitorato sul CCP, l'incidente viene visualizzato.



Come funziona?

Come mostrato nell'immagine, sulla FMC è necessario configurare le fonti da cui si desidera scaricare le informazioni di intelligence sulle minacce. Il CCP trasmette poi tali informazioni (osservabili) ai sensori. Quando il traffico corrisponde agli oggetti osservabili, gli incidenti vengono visualizzati nell'interfaccia utente (GUI) del CCP.



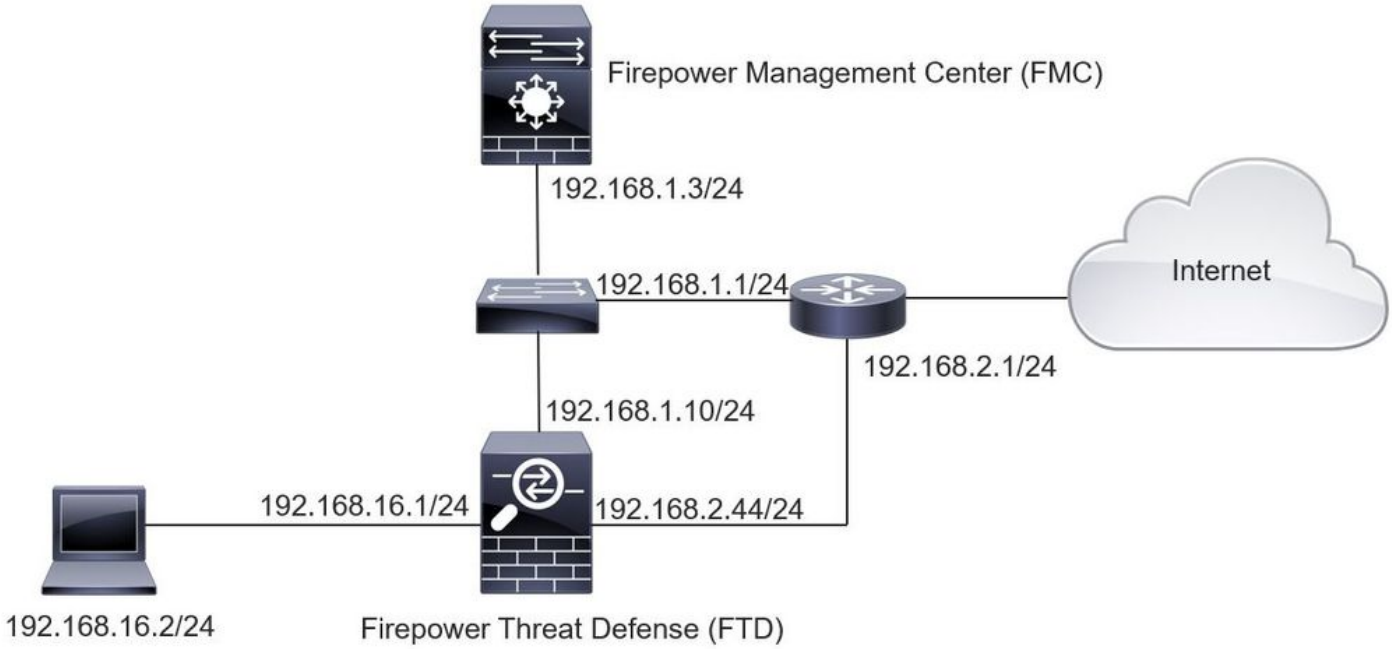
Sono disponibili due nuovi termini:

- STIX (Structured Threat Intelligence eXpression) è uno standard per la condivisione e l'utilizzo di informazioni di intelligence sulle minacce. Gli elementi funzionali chiave sono tre: Indicatori, Osservabili e Incidenti.
- TAXII (Trusted Automated eXchange of Indicator Information) è un meccanismo di trasporto per informazioni sulle minacce.

Configurazione

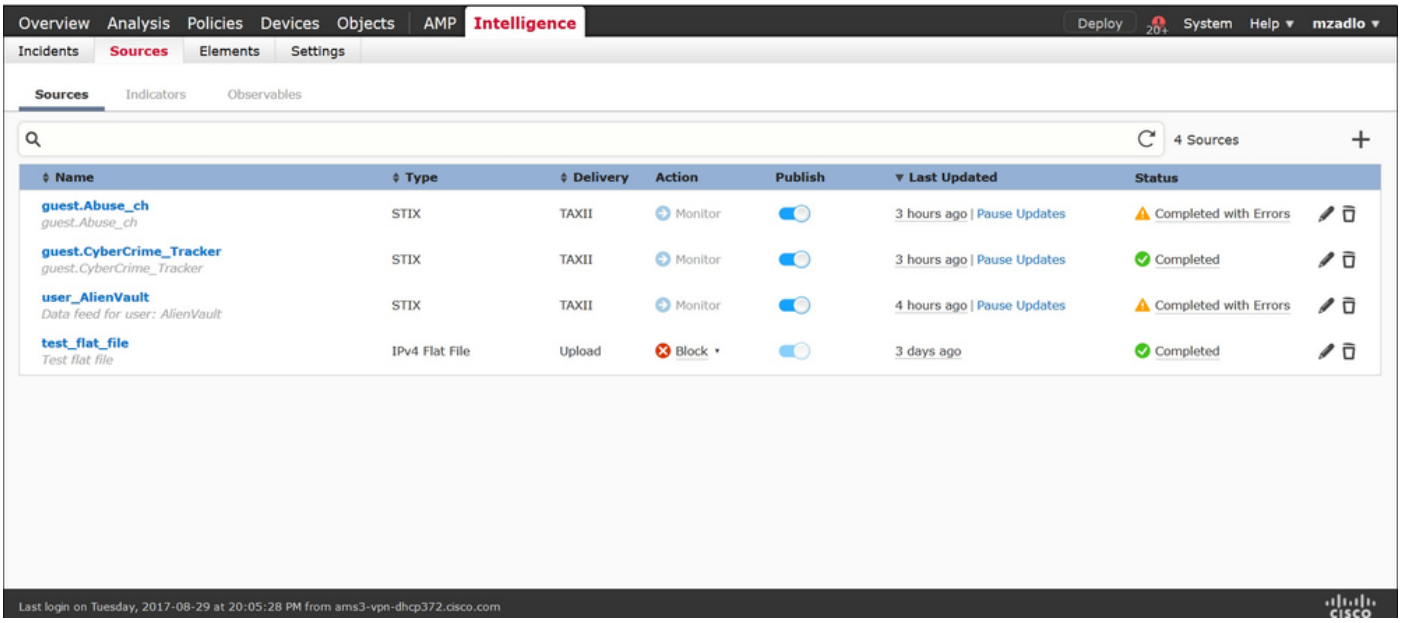
Per completare la configurazione, prendere in considerazione le seguenti sezioni:

Esempio di rete



Configurazione

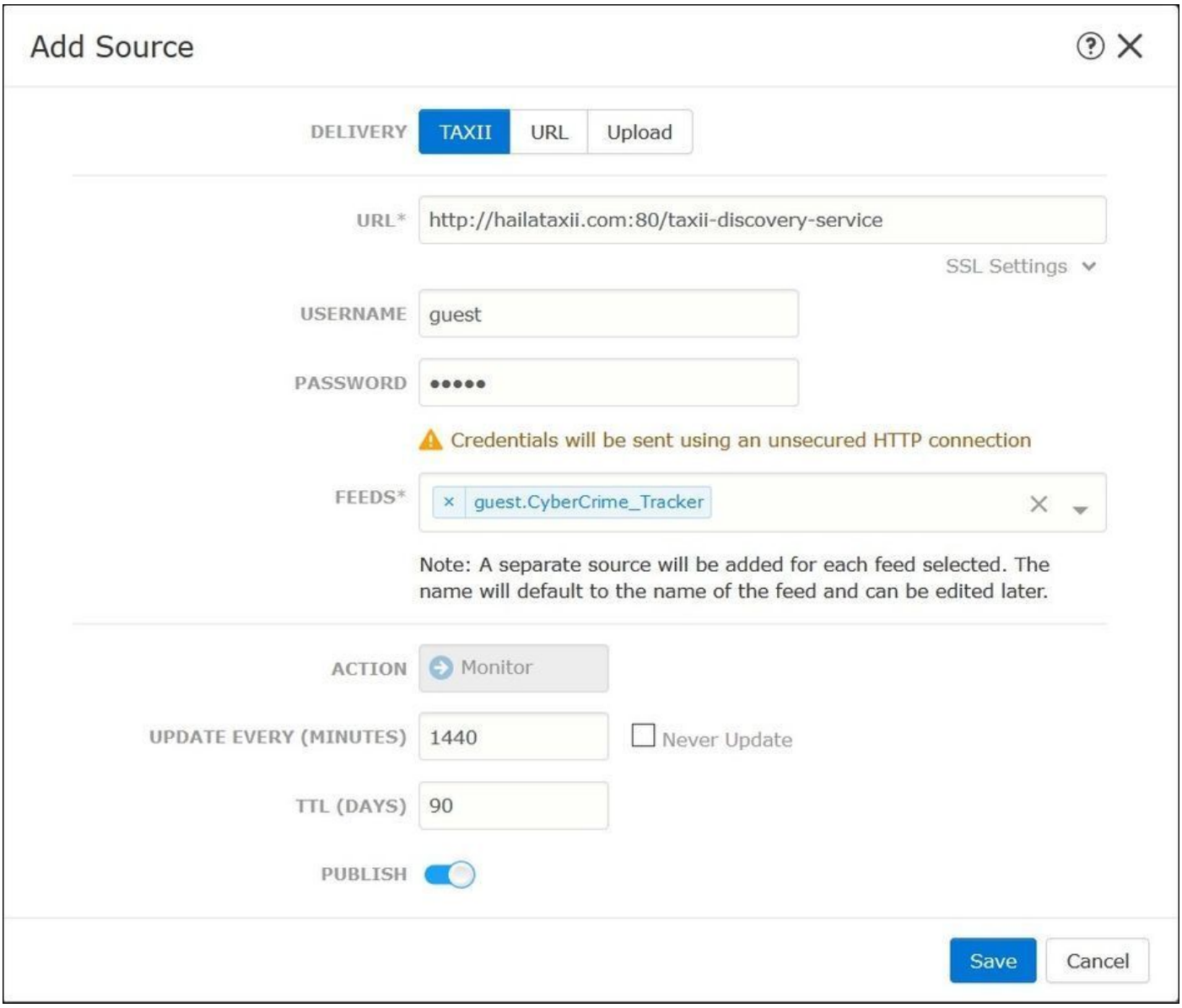
Passaggio 1. Per configurare TID, è necessario passare alla scheda Intelligence, come mostrato nell'immagine.



Nota: lo stato 'Completato con errori' è previsto nel caso in cui un feed contenga elementi osservabili non supportati.

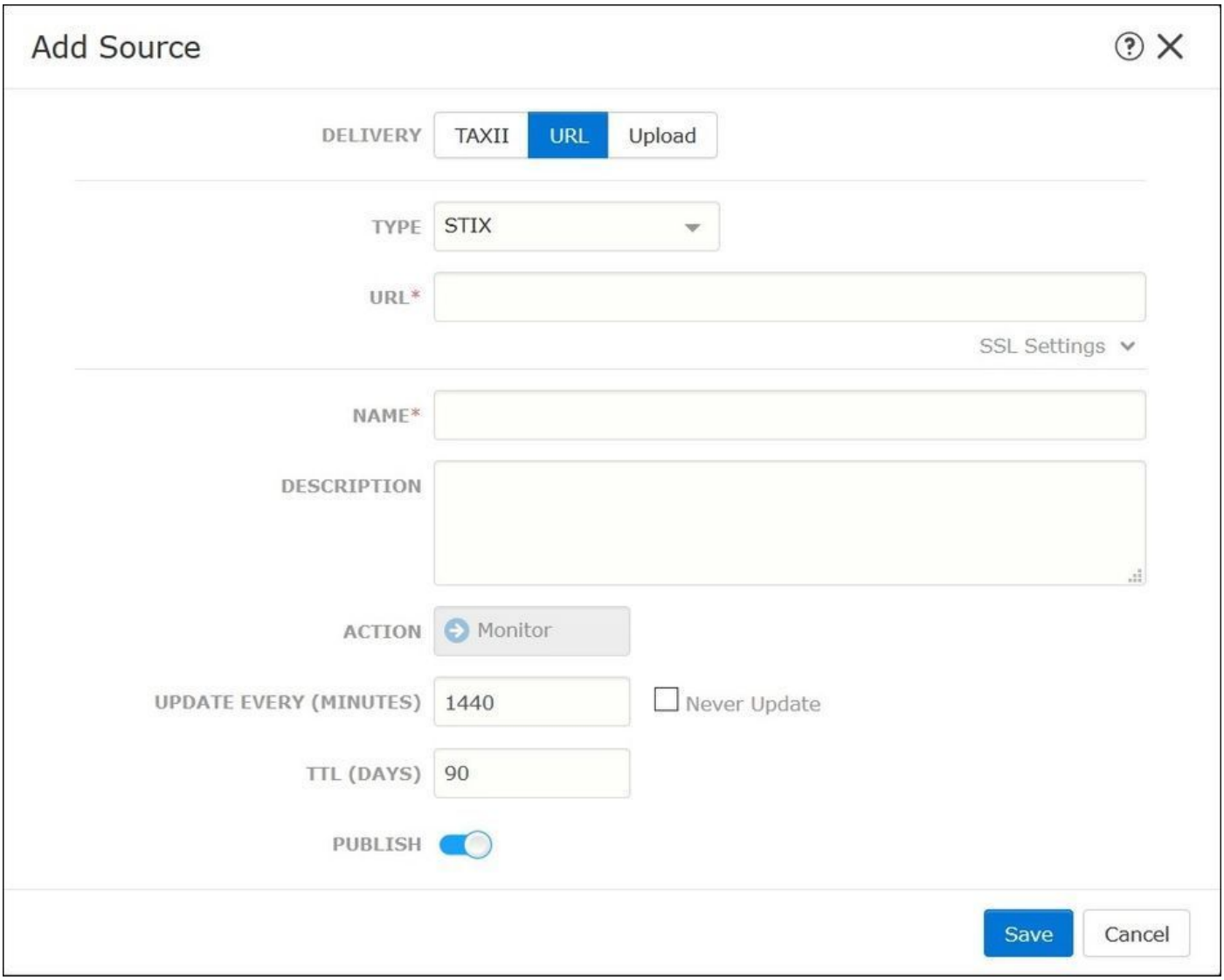
Passaggio 2. Bisogna aggiungere delle fonti di minaccia. È possibile aggiungere origini in tre modi:

- TAXII - Quando si utilizza questa opzione, è possibile configurare un server in cui le informazioni sulle minacce sono memorizzate in formato STIX.

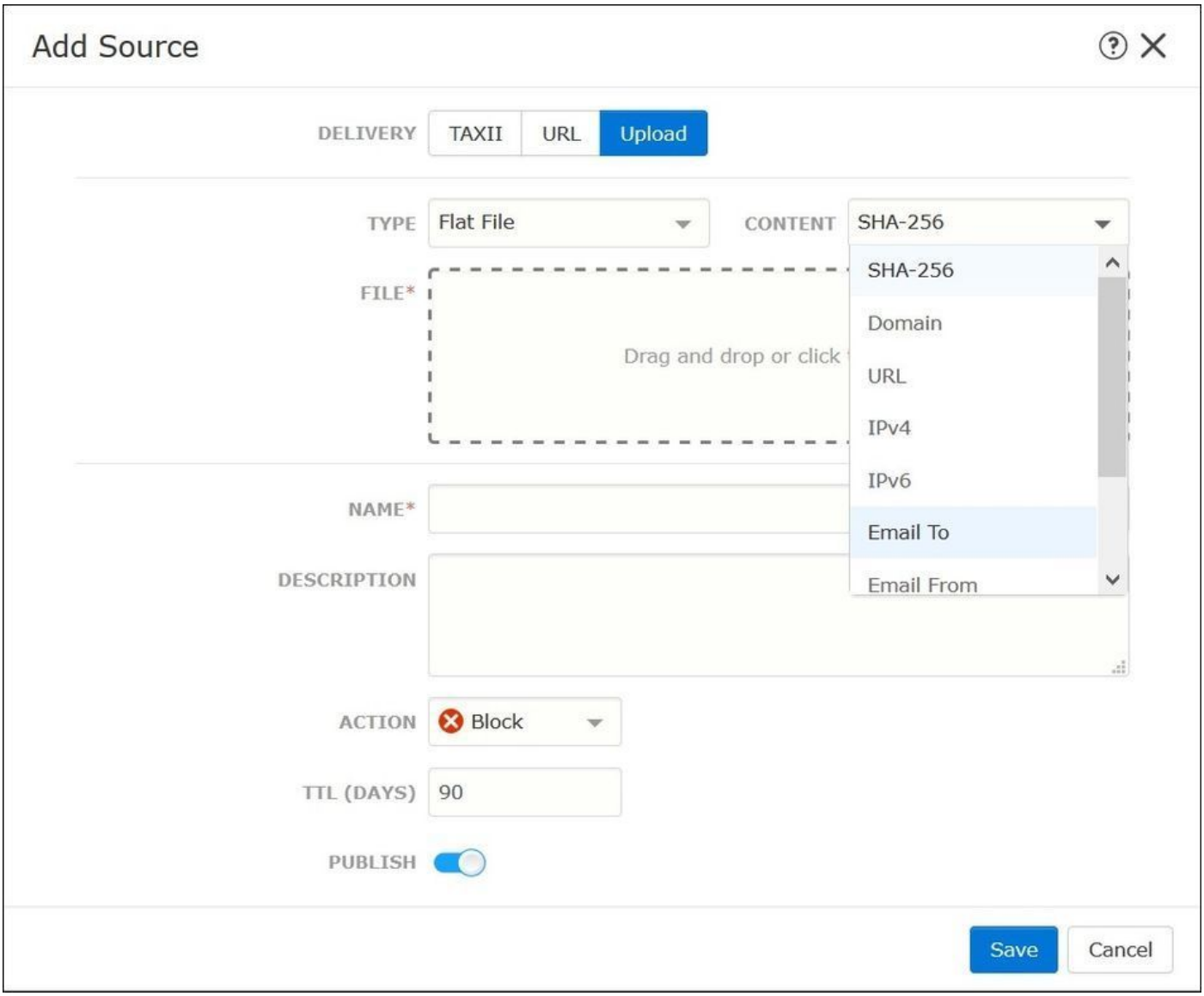


Nota: l'unica azione disponibile è Monitor. Non è possibile configurare l'azione di blocco per le minacce in formato STIX.

- URL: è possibile configurare un collegamento a un server locale HTTP/HTTPS in cui si trova la minaccia STIX o il file flat.

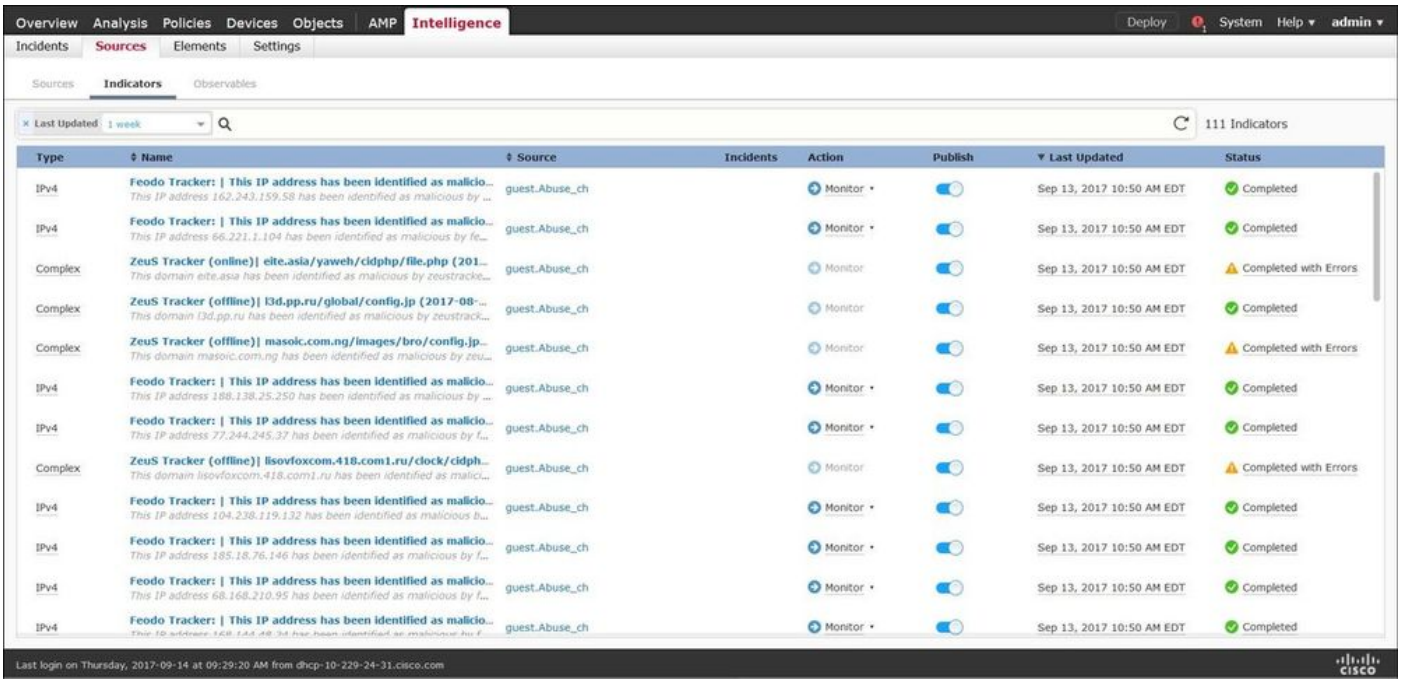


- File flat: è possibile caricare un file in formato *.txt ed è necessario specificare il contenuto del file. Il file deve contenere una voce di contenuto per riga.



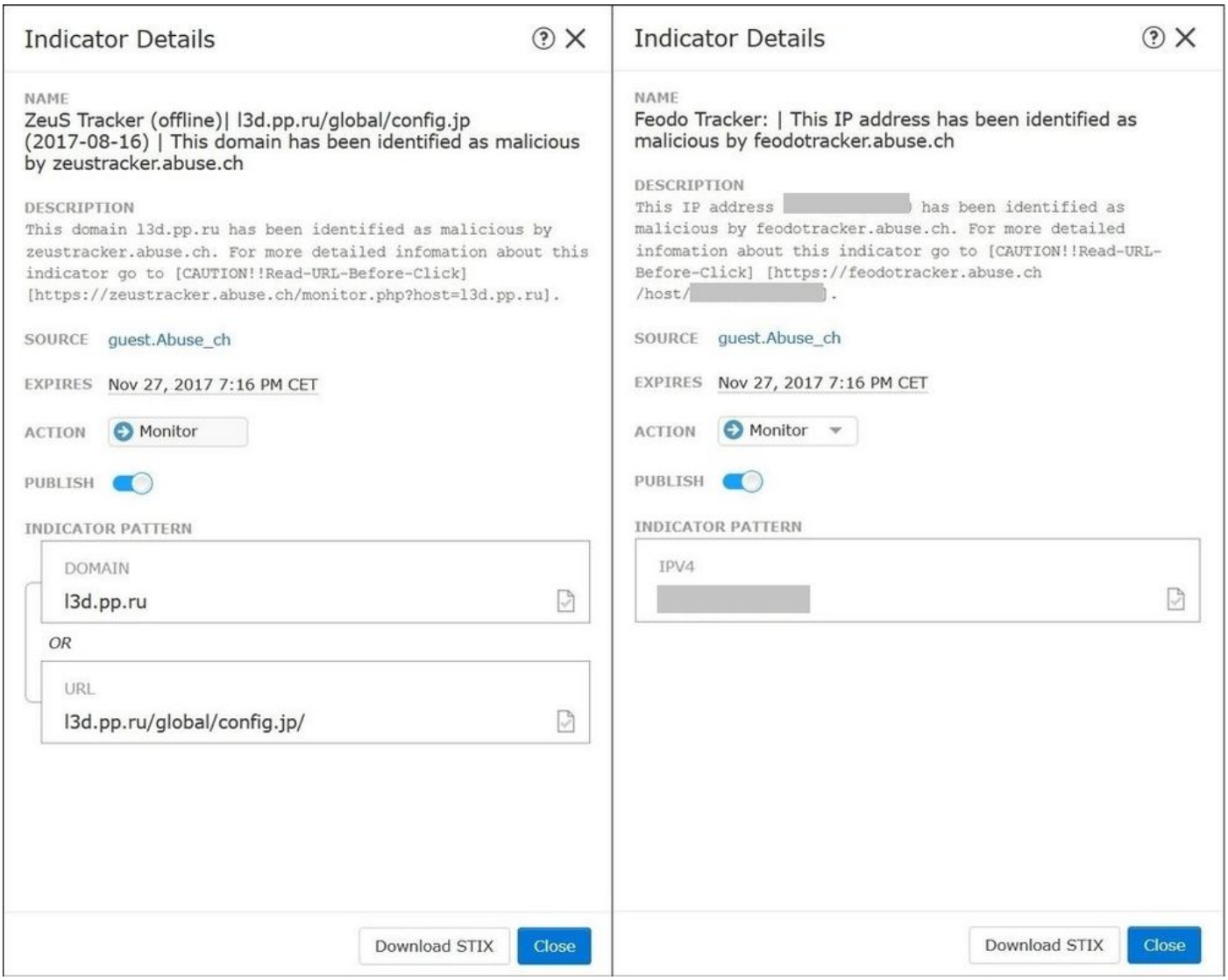
Nota: per impostazione predefinita, tutte le fonti vengono pubblicate, ovvero vengono inviate ai sensori. Questo processo può richiedere fino a 20 minuti o più.

Passaggio 3. Nella scheda Indicatore è possibile verificare se gli indicatori sono stati scaricati dalle origini configurate:

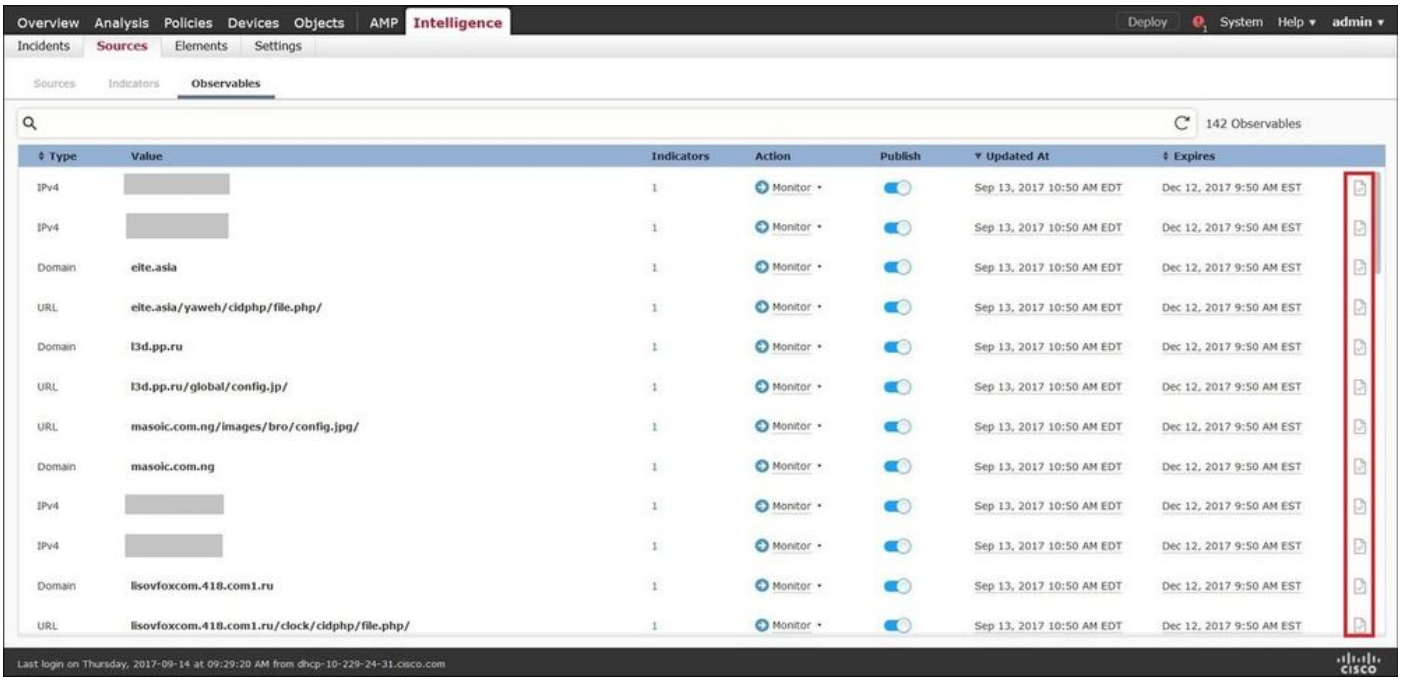


Passaggio 4. Dopo aver selezionato il nome di un indicatore, è possibile visualizzare ulteriori dettagli. Inoltre, è possibile decidere se si desidera pubblicarlo sul sensore o se si desidera modificare l'azione (nel caso di un semplice indicatore).

Come mostrato nell'immagine, viene elencato un indicatore complesso con due oggetti osservabili collegati dall'operatore OR:



Passaggio 5. Passare alla scheda Osservabili, in cui è possibile trovare gli URL, gli indirizzi IP, i domini e SHA256 inclusi negli indicatori. È possibile decidere quali oggetti osservabili si desidera spingere ai sensori e, facoltativamente, modificare l'azione per loro. Nell'ultima colonna è presente un pulsante con l'elenco vuoto equivalente a un'opzione di pubblicazione/non pubblicazione.

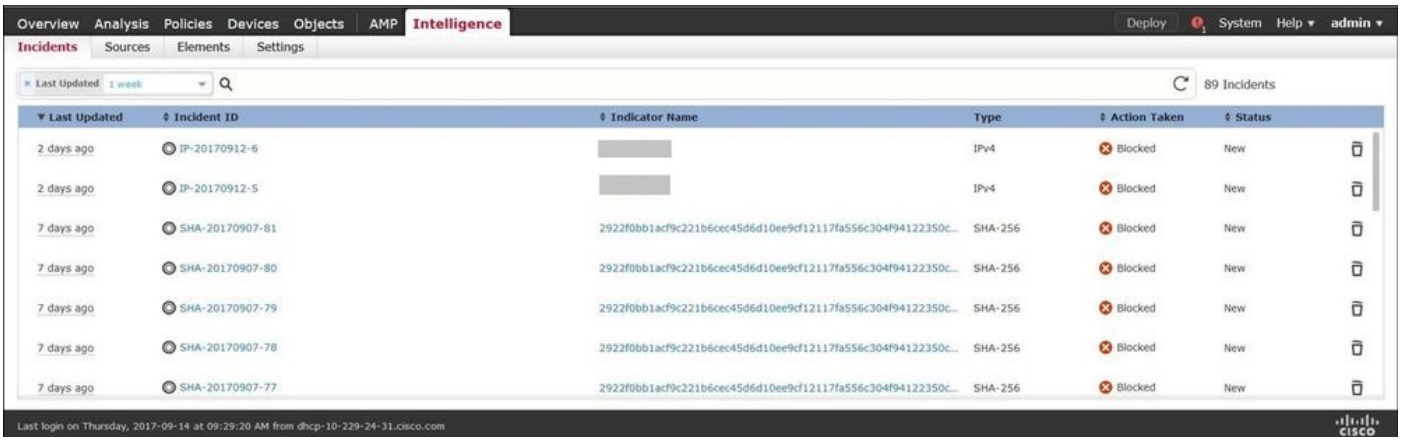


Passaggio 6. Passare alla scheda Elementi per verificare l'elenco dei dispositivi in cui è abilitato TID:

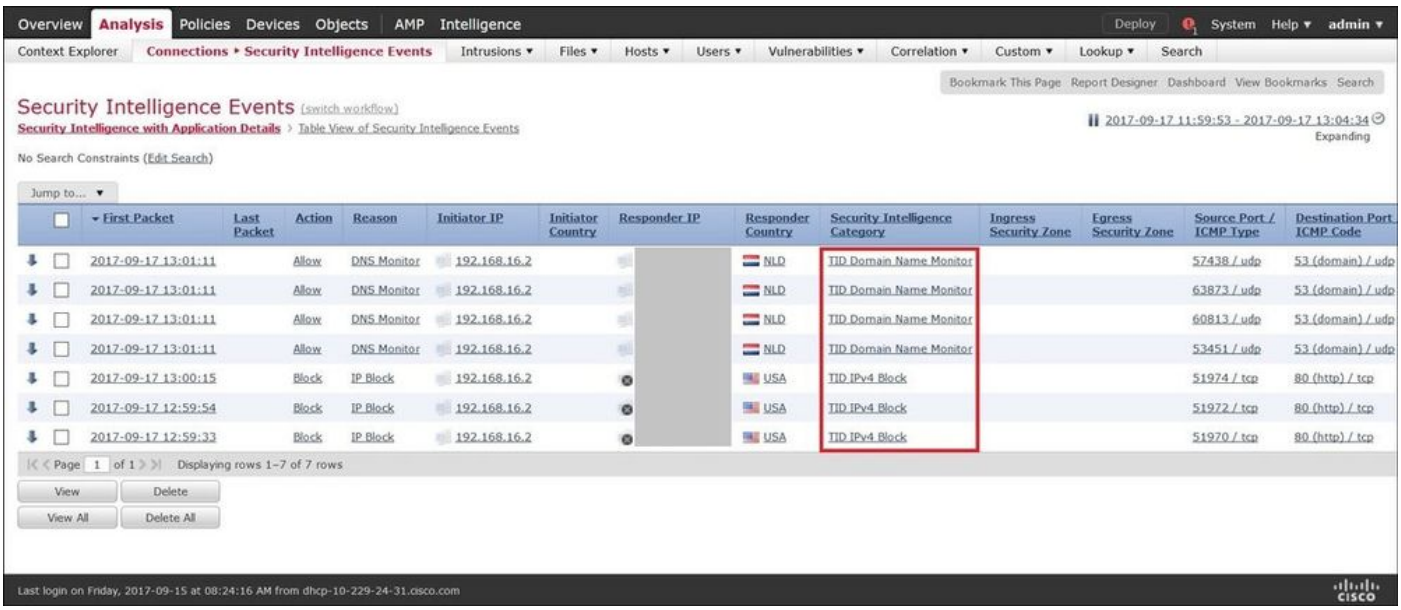
Passaggio 7 (facoltativo). Passare alla scheda Settings (Impostazioni) e selezionare il pulsante Pause (Pausa) per interrompere il push degli indicatori ai sensori. L'operazione può richiedere fino a 20 minuti.

Verifica

Metodo 1. Per verificare se TID ha agito sul traffico, è necessario passare alla scheda Incidenti.



Metodo 2. Gli incidenti sono disponibili nella scheda Eventi di Security Intelligence sotto un tag TID.



Nota: TID ha una capacità di archiviazione di 1 milione di incidenti.

Metodo 3. È possibile verificare se sul FMC e su un sensore sono presenti sorgenti (feed) configurate. A tale scopo, è possibile passare ai seguenti percorsi nella CLI:

/var/sf/siurl_download/

/var/sf/sidns_download/

/var/sf/iprep_download/

È stata creata una nuova directory per i feed SHA256: /var/sf/sifile_download/

<#root>

```
root@ftd622:
/var/sf/sifile_download
```

```
# ls -l
total 32
-rw-r--r-- 1 root root  166 Sep 14 07:13 8ba2b2c4-9275-11e7-8368-f6cc0e401935.lf
-rw-r--r-- 1 root root   38 Sep 14 07:13 8ba40804-9275-11e7-8368-f6cc0e401935.lf
-rw-r--r-- 1 root root   16 Sep 14 07:13 IPRVersion.dat
-rw-rw-r-- 1 root root 1970 Sep 14 07:13 dm_file1.acl
-rw-rw-r-- 1 www  www   167 Sep 14 07:13 file.rules
drwxr-xr-x 2 www  www  4096 Sep  4 16:13 health
drwxr-xr-x 2 www  www  4096 Sep  7 22:06 peers
drwxr-xr-x 2 www  www  4096 Sep 14 07:13 tmp
root@ftd622:/var/sf/sifile_download#
```

cat 8ba2b2c4-9275-11e7-8368-f6cc0e401935.lf

```
#Cisco TID feed:TID SHA-256 Block:1
7a00ef4b801b2b2acd09b5fc72d7c79d20094ded6360fb936bf2c65a1ff16907
2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c2bcbdc
```

Nota: TID è abilitato solo nel dominio globale del CCP.

Nota: se TID viene ospitato su Firepower Management Center attivo in una configurazione ad alta disponibilità (appliance FMC fisiche), il sistema non sincronizza le configurazioni TID e i dati TID con Firepower Management Center in standby.

Risoluzione dei problemi

Esiste un processo di primo livello chiamato tid. Questo processo dipende da tre processi: mongo, RabbitMQ, e redis. Per verificare i processi eseguire pmtool status | grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - " comando.

<#root>

```
root@fmc622:/Volume/home/admin#
```

pmtool status | grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - "

```
RabbitMQ (normal) - Running 4221
mongo (system) - Running 4364
redis (system) - Running 4365
tid (normal) - Running 5128
root@fmc622:/Volume/home/admin#
```

Per verificare in tempo reale l'azione intrapresa, è possibile eseguire il comando system support firewall-engine-debug o il comando system support trace.

<#root>

```
>
```

```
system support firewall-engine-debug


Please specify an IP protocol:
Please specify a client IP address: 192.168.16.2
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages
...
192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1

URL SI: ShmDBLookupURL("http://www.example.com/") returned 1

...
192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1

URL SI: Matched rule order 19, Id 19, si list id 1074790455, action 4

192.168.16.2-59122 > 129.21.1.40-80 6 AS 1 I 1 deny action
```

Esistono due possibilità d'azione:

- URL SI: ordine regola corrispondente 19, ID 19, ID elenco 1074790455, azione 4 - traffico bloccato.
- URL SI: ordine regola corrispondente 20, ID 20, ID elenco si 1074790456, azione 6 - il traffico è stato monitorato.

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).