

Configure and Troubleshoot Cisco Threat Intelligence Director

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[How does it work?](#)

[Configure](#)

[Network Diagram](#)

[Configuration](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure and troubleshoot Cisco Threat Intelligence Director (TID).

Prerequisites

Requirements

Cisco recommends that you know these topics:

- Firepower Management Center (FMC) administration.

You need to ensure these conditions before you configure the Cisco Threat Intelligence Director feature:

- The Firepower Management Center (FMC):
 - Must run on 6.2.2 (or later) version (can be hosted on physical or virtual FMC).
 - Must be configured with a minimum of 15 GB of RAM memory.
 - Must be configured with REST API access enabled.
- The sensor must run 6.2.2 version (or later).
- In the Advanced Settings tab of the access control policy option, **Enable Threat Intelligence Director** has to be enabled.
- Add rules to the access control policy if they are not already present.
- If you want SHA-256 observables to generate observations and Firepower Management Center events, create one or more **Malware Cloud Lookup** or **Block Malware** file rules and associate the file policy with one or more rules in the access control policy.
- If you want IPv4, IPv6, URL, or Domain Name observations to generate connection and security intelligence events, enable connection and security intelligence logging in the access control policy.

Components Used

The information in this document is based on these software versions:

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

 Note: 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.

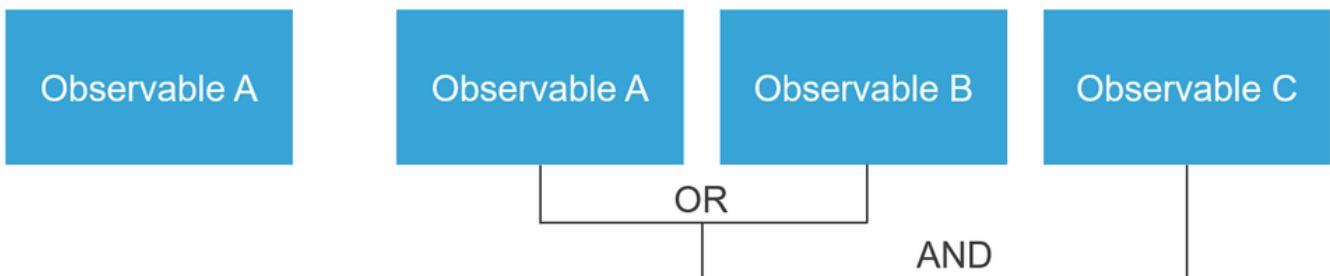
Background Information

Cisco Threat Intelligence Director (TID) is a system that operationalizes threat intelligence information. The system consumes and normalizes heterogeneous third-party cyber threat intelligence, publishes the intelligence to detection technologies, and correlates the observations from the detection technologies.

There are three new terms: **observables**, **indicators**, and **incidents**. Observable is just a variable, which can be for example URL, domain, IP address, or SHA256. Indicators are made from observables. There are two types of indicators. A simple indicator contains only one observable. In the case of complex indicators, there are two or more observables that are connected to each other using logical functions like AND and OR. Once the system detects traffic that should be blocked or monitored on the FMC the incident appears.

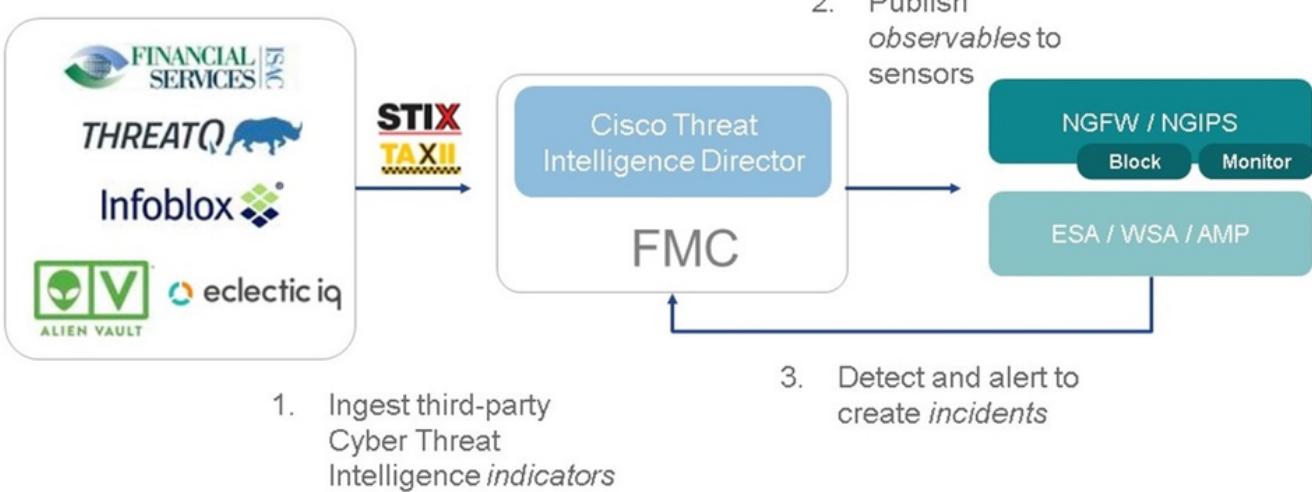
Simple Indicator

Complex indicator, two operators



How does it work?

As shown in the image, on the FMC you have to configure sources from where you would like to download threat intelligence information. The FMC then pushes that information (observables) to sensors. When the traffic matches the observables, the incidents appear in the FMC user interface (GUI).



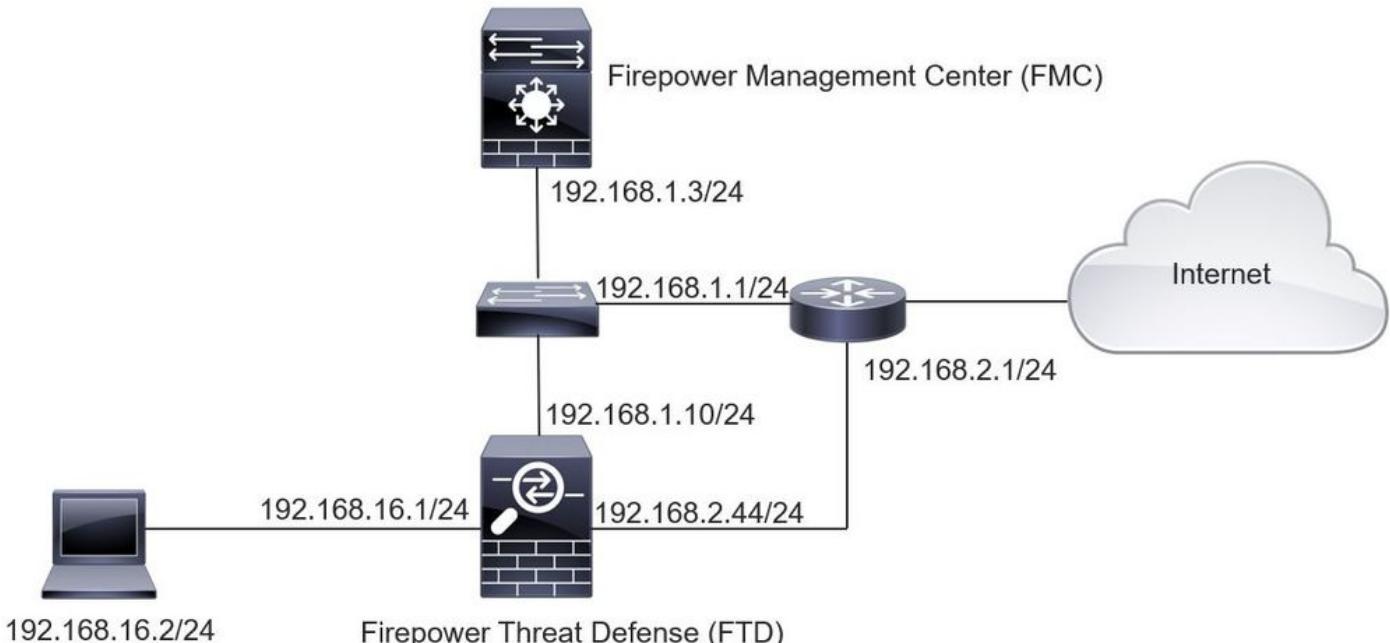
There are two new terms:

- STIX (Structured Threat Intelligence eXpression) is a standard for sharing and using threat intelligence information. There are three key functional elements: Indicators, Observables, and Incidents.
- TAXII (Trusted Automated eXchange of Indicator Information) is a transport mechanism for threat information.

Configure

To complete the configuration take into consideration these sections:

Network Diagram



Configuration

Step 1. To configure TID, you have to navigate to the **Intelligence** tab, as shown in the image.

Screenshot of the Cisco Umbrella Intelligence interface showing the Sources list.

The top navigation bar includes: Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Deploy, 20+, System, Help, and mzadlo.

The Sources tab is selected in the left sidebar, with sub-options: Sources, Indicators, and Observables.

The main table displays the following data:

| Name | Type | Delivery | Action | Publish | Last Updated | Status |
|--|----------------|----------|---------|-------------------------------------|-----------------------------|---|
| <code>guest.Abuse_ch</code> <code>guest.Abuse_ch</code> | STIX | TAXII | Monitor | <input checked="" type="checkbox"/> | 3 hours ago Pause Updates | ⚠ Completed with Errors |
| <code>guest.CyberCrime_Tracker</code> <code>guest.CyberCrime_Tracker</code> | STIX | TAXII | Monitor | <input checked="" type="checkbox"/> | 3 hours ago Pause Updates | ✓ Completed |
| <code>user_AlienVault</code> Data feed for user: AlienVault | STIX | TAXII | Monitor | <input checked="" type="checkbox"/> | 4 hours ago Pause Updates | ⚠ Completed with Errors |
| <code>test_flat_file</code> Test flat file | IPv4 Flat File | Upload | Block | <input checked="" type="checkbox"/> | 3 days ago | ✓ Completed |

Bottom status bar: Last login on Tuesday, 2017-08-29 at 20:05:28 PM from ams3-vpn-dhcp372.cisco.com

 Note: Status 'Completed with Errors' is expected in case a feed contains unsupported observables.

Step 2. You have to add sources of threats. There are three ways to add sources:

- TAXII - When you use this option, you can configure a server where threat information is stored in STIX format.

Add Source



DELIVERY

TAXII

URL

Upload

URL*

http://hailataxii.com:80/taxii-discovery-service

SSL Settings ▾

USERNAME

guest

PASSWORD

⚠ Credentials will be sent using an unsecured HTTP connection

FEEDS*

x guest.CyberCrime_Tracker



Note: A separate source will be added for each feed selected. The name will default to the name of the feed and can be edited later.

ACTION

Monitor

UPDATE EVERY (MINUTES)

1440

 Never Update

TTL (DAYS)

90

PUBLISH



Save

Cancel



Note: The only Action available is Monitor. You cannot configure the Block Action for threats in STIX format.

- URL - You can configure a link to an HTTP/HTTPS local server where the STIX threat or flat file is located.

Add Source



DELIVERY TAXII URL Upload

TYPE STIX ▾

URL*

SSL Settings ▾

NAME*

DESCRIPTION

ACTION Monitor

UPDATE EVERY (MINUTES) Never Update

TTL (DAYS)

PUBLISH

Save

Cancel

- Flat file - You can upload a file in ***.txt** format and you have to specify the content of the file. The file must contain one content entry per line.

Add Source



DELIVERY TAXII URL Upload

TYPE Flat File

CONTENT

SHA-256

FILE*

Drag and drop or click

NAME*

DESCRIPTION

SHA-256

Domain

URL

IPv4

IPv6

Email To

Email From

ACTION Block

TTL (DAYS) 90

PUBLISH

Save

Cancel

Note: By default, all sources are published, this means that they are pushed to sensors. This process can take up to 20 minutes or more.

Step 3. Under the Indicator tab, you can confirm if indicators were downloaded properly from the configured sources:

| Intelligence | | | | | | | Deploy | System | Help | admin |
|---------------|---|----------------------|-------------|----------|-------------------------------------|---------------------------|-----------------------|--------|------|-------|
| Incidents | | Sources | Elements | Settings | | | | | | |
| Sources | | Indicators | Observables | | | | | | | |
| Last Updated: | 1 week | <input type="text"/> | | | | | | | | |
| Type | # Name | Source | Incidents | Action | Publish | >Last Updated | Status | | | |
| IPv4 | Feodo Tracker: This IP address has been identified as malicious by feodo... This IP address 162.243.159.58 has been identified as malicious by feodo... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |
| IPv4 | Feodo Tracker: This IP address has been identified as malicious by feodo... This IP address 66.221.1.104 has been identified as malicious by feodo... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |
| Complex | ZeuS Tracker (online) elite.asia/yaweh/cldphp/file.php (201... This domain elite.asia has been identified as malicious by zeustrack... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed with Errors | | | |
| Complex | ZeuS Tracker (offline) 13d.pp.ru/global/config.jp (2017-08-1... This domain 13d.pp.ru has been identified as malicious by zeustrack... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |
| Complex | ZeuS Tracker (offline) masoic.com.ng/images/bro/config.jp... This domain masoic.com.ng has been identified as malicious by zeu... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed with Errors | | | |
| IPv4 | Feodo Tracker: This IP address has been identified as malicious by feodo... This IP address 188.138.25.250 has been identified as malicious by feodo... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |
| IPv4 | Feodo Tracker: This IP address has been identified as malicious by feodo... This IP address 77.244.245.37 has been identified as malicious by feo... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |
| Complex | ZeuS Tracker (offline) lsovofoxcom.418.com1.ru/clock/cldph... This domain lsovofoxcom.418.com1.ru has been identified as malici... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed with Errors | | | |
| IPv4 | Feodo Tracker: This IP address has been identified as malicious by feodo... This IP address 104.238.119.132 has been identified as malicious by feodo... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |
| IPv4 | Feodo Tracker: This IP address has been identified as malicious by feodo... This IP address 185.18.76.146 has been identified as malicious by feo... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |
| IPv4 | Feodo Tracker: This IP address has been identified as malicious by feodo... This IP address 68.168.210.95 has been identified as malicious by feo... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |
| IPv4 | Feodo Tracker: This IP address has been identified as malicious by feodo... This IP address 149.148.148.148 has been identified as malicious by feo... | guest.Abuse_ch | | Monitor | <input checked="" type="checkbox"/> | Sep 13, 2017 10:50 AM EDT | Completed | | | |

Last login on Thursday, 2017-09-14 at 09:29:20 AM from dnclp-10-229-24-31.cisco.com



Step 4. Once you select the name of an indicator you can see more details about it. Additionally, you can decide if you want to publish it to the sensor or if you want to change the action (in the case of a simple indicator).

As shown in the image, a complex indicator is listed with two observables that are connected by the OR operator:

| Indicator Details | Indicator Details | | | | | | | | | | | | |
|---|----------------------------|-----------|--|----|--|--|-----|----------------------------|--|---|------|------------|--|
| <p>NAME Zeus Tracker (offline)] l3d.pp.ru/global/config.jp (2017-08-16) This domain has been identified as malicious by zeustracker.abuse.ch</p> <p>DESCRIPTION This domain l3d.pp.ru has been identified as malicious by zeustracker.abuse.ch. For more detailed information about this indicator go to [CAUTION!!Read-URL-Before-Click] [https://zeustracker.abuse.ch/monitor.php?host=l3d.pp.ru].</p> <p>SOURCE guest.Abuse_ch</p> <p>EXPIRES Nov 27, 2017 7:16 PM CET</p> <p>ACTION Monitor</p> <p>PUBLISH </p> <p>INDICATOR PATTERN</p> <table border="1"> <tr> <td>DOMAIN</td> <td>l3d.pp.ru</td> <td></td> </tr> <tr> <td>OR</td> <td></td> <td></td> </tr> <tr> <td>URL</td> <td>l3d.pp.ru/global/config.jp</td> <td></td> </tr> </table> <p style="text-align: right;">Download STIX Close</p> | DOMAIN | l3d.pp.ru | | OR | | | URL | l3d.pp.ru/global/config.jp | | <p>NAME Feodo Tracker: This IP address has been identified as malicious by feodotracker.abuse.ch</p> <p>DESCRIPTION This IP address [REDACTED] has been identified as malicious by feodotracker.abuse.ch. For more detailed information about this indicator go to [CAUTION!!Read-URL-Before-Click] [https://feodotracker.abuse.ch/host/[REDACTED]].</p> <p>SOURCE guest.Abuse_ch</p> <p>EXPIRES Nov 27, 2017 7:16 PM CET</p> <p>ACTION Monitor</p> <p>PUBLISH </p> <p>INDICATOR PATTERN</p> <table border="1"> <tr> <td>IPV4</td> <td>[REDACTED]</td> <td></td> </tr> </table> <p style="text-align: right;">Download STIX Close</p> | IPV4 | [REDACTED] | |
| DOMAIN | l3d.pp.ru | | | | | | | | | | | | |
| OR | | | | | | | | | | | | | |
| URL | l3d.pp.ru/global/config.jp | | | | | | | | | | | | |
| IPV4 | [REDACTED] | | | | | | | | | | | | |

Step 5. Navigate to the Observables tab where you can find URLs, IP addresses, domains, and SHA256 that are included in the indicators. You can decide which observables you would like to push to sensors and optionally change the action for them. In the last column, there is a whitelist button that is equivalent to a publish/not publish option.

Screenshot of the Cisco Firepower Threat Defense interface showing the 'Observables' tab under the 'Intelligence' section. The table lists various observables with columns for Type, Value, Indicators, Action, Publish, Updated At, and Expires. A red box highlights the 'Expires' column.

| Type | Value | Indicators | Action | Publish | Updated At | Expires |
|--------|--|------------|---------|---------|---------------------------|--------------------------|
| IPv4 | [REDACTED] | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| IPv4 | [REDACTED] | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| Domain | elite.asia | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| URL | elite.asia/yaweh/cidphp/file.php/ | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| Domain | i3d.pp.ru | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| URL | i3d.pp.ru/global/config.jp/ | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| URL | masoic.com.ng/images/bro/config.jpg/ | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| Domain | masoic.com.ng | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| IPv4 | [REDACTED] | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| IPv4 | [REDACTED] | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| Domain | lisovfoxcom.418.com1.ru | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |
| URL | lisovfoxcom.418.com1.ru/clock/cidphp/file.php/ | 1 | Monitor | On | Sep 13, 2017 10:50 AM EDT | Dec 12, 2017 9:50 AM EST |

Last login on Thursday, 2017-09-14 at 09:29:20 AM from dhcp-10-229-24-31.cisco.com

Step 6. Navigate to the Elements tab to verify the list of devices where TID is enabled:

Screenshot of the Cisco Firepower Threat Defense interface showing the 'Elements' tab under the 'Intelligence' section. The table shows one element named FTD_622, which is a Cisco Firepower Threat Defense for VMware device registered on Sep 5, 2017, with access control policy acp_policy.

| Name | Element Type | Registered On | Access Control Policy |
|---------|---|-------------------------|-----------------------|
| FTD_622 | Cisco Firepower Threat Defense for VMware | Sep 5, 2017 4:00 PM EDT | acp_policy |

Step 7 (Optional). Navigate to the Settings tab and select the Pause button to stop pushing indicators to sensors. This operation can take up to 20 minutes.

Screenshot of the Cisco Firepower Threat Defense interface showing the 'Settings' tab under the 'Intelligence' section. The 'TID Detection' section indicates that the system is currently publishing TID observables to elements. It includes a 'Pause' button to stop publishing and a 'Resume' button to resume it.

Verify

Method 1. To verify if TID acted on the traffic, you need to navigate to the Incidents tab.

Screenshot of the Cisco Firepower Threat Defense interface showing the 'Incidents' tab under the 'Intelligence' section. The table lists 89 incidents, all of which are New and have been blocked. The incidents are categorized by Last Updated (2 days ago, 7 days ago) and Incident ID.

| Last Updated | Incident ID | Indicator Name | Type | Action Taken | Status |
|--------------|-----------------|---|---------|--------------|--------|
| 2 days ago | IP-20170912-6 | [REDACTED] | IPv4 | Blocked | New |
| 2 days ago | IP-20170912-5 | [REDACTED] | IPv4 | Blocked | New |
| 7 days ago | SHA-20170907-81 | 2922f0bb1acf9c221b6cec45d6d10ee9df12117fa556c304f94122350c... | SHA-256 | Blocked | New |
| 7 days ago | SHA-20170907-80 | 2922f0bb1acf9c221b6cec45d6d10ee9df12117fa556c304f94122350c... | SHA-256 | Blocked | New |
| 7 days ago | SHA-20170907-79 | 2922f0bb1acf9c221b6cec45d6d10ee9df12117fa556c304f94122350c... | SHA-256 | Blocked | New |
| 7 days ago | SHA-20170907-78 | 2922f0bb1acf9c221b6cec45d6d10ee9df12117fa556c304f94122350c... | SHA-256 | Blocked | New |
| 7 days ago | SHA-20170907-77 | 2922f0bb1acf9c221b6cec45d6d10ee9df12117fa556c304f94122350c... | SHA-256 | Blocked | New |

Last login on Thursday, 2017-09-14 at 09:29:20 AM from dhcp-10-229-24-31.cisco.com

Method 2. The incidents can be found under the Security Intelligence Events tab under a TID tag.

The screenshot shows the FMC interface with the 'Analysis' tab selected. Under 'Connections > Security Intelligence Events', a table displays various security incidents. The columns include First Packet, Last Packet, Action, Reason, Initiator IP, Initiator Country, Responder IP, Responder Country, Security Intelligence Category, Ingress Security Zone, Egress Security Zone, Source Port / ICMP Type, and Destination Port / ICMP Code. Several rows are highlighted with a red border, specifically those categorized as 'TID Domain Name Monitor' or 'TID IPv4 Block'. The table shows a mix of Allow and Block actions, with reasons like 'DNS Monitor' or 'IP Block'. The responder country for most entries is NLD, while some are USA. The destination port includes 53 (domain) / udp, 63873 / udp, 60813 / udp, 53451 / udp, 51974 / tcp, 51972 / tcp, and 51970 / tcp.

Note: TID has a storage capacity of 1 million incidents.

Method 3. You can confirm if configured sources (feeds) are present on the FMC and a sensor. To do that, you can navigate to these locations on the CLI:

/var/sf/siurl_download/

/var/sf/sidns_download/

/var/sf/iprep_download/

There is a new directory created for SHA256 feeds: /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-f6cc0e401935.1f
-rw-r--r-- 1 root root 38 Sep 14 07:13 8ba40804-9275-11e7-8368-f6cc0e401935.1f
-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-f6cc0e401935.1f

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

 **Note:** TID is enabled only on the Global Domain on the FMC.

 **Note:** If you host TID on the active Firepower Management Center in a high availability configuration (physical FMC appliances), the system does not synchronize TID configurations and TID data to the standby Firepower Management Center.

Troubleshoot

There is a top-level process which is called **tid**. This process depends on three processes: **mongo**, **RabbitMQ**, and **redis**. To verify processes run **pmtool status | grep 'RabbitMQ\|mongo\|redis\|tid' | grep " - "** command.

```
<#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#
```

In order to verify in real-time what action is taken, you can execute **system support firewall-engine-debug** or **system support trace** command.

```
<#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
```

There are two possibilities in terms of action:

- **URL SI: Matched rule order 19, Id 19, si list id 1074790455, action 4** - traffic was blocked.
- **URL SI: Matched rule order 20, Id 20, si list id 1074790456, action 6** - traffic was monitored.