

# 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.

---

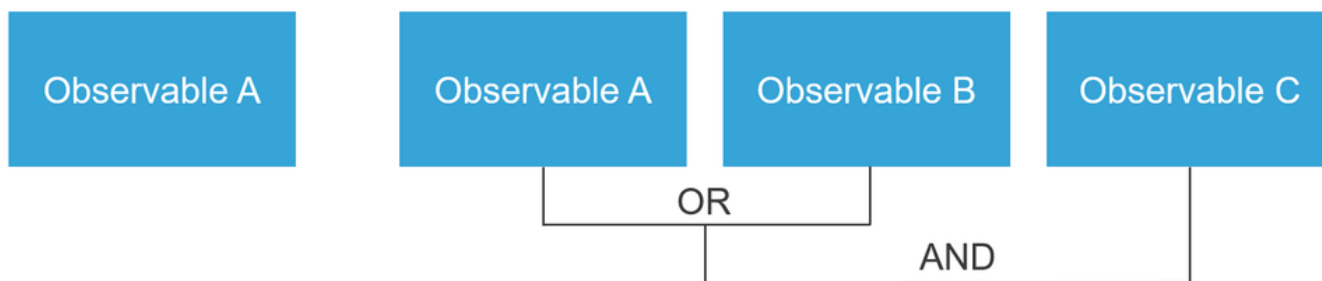
## Background Information

**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.

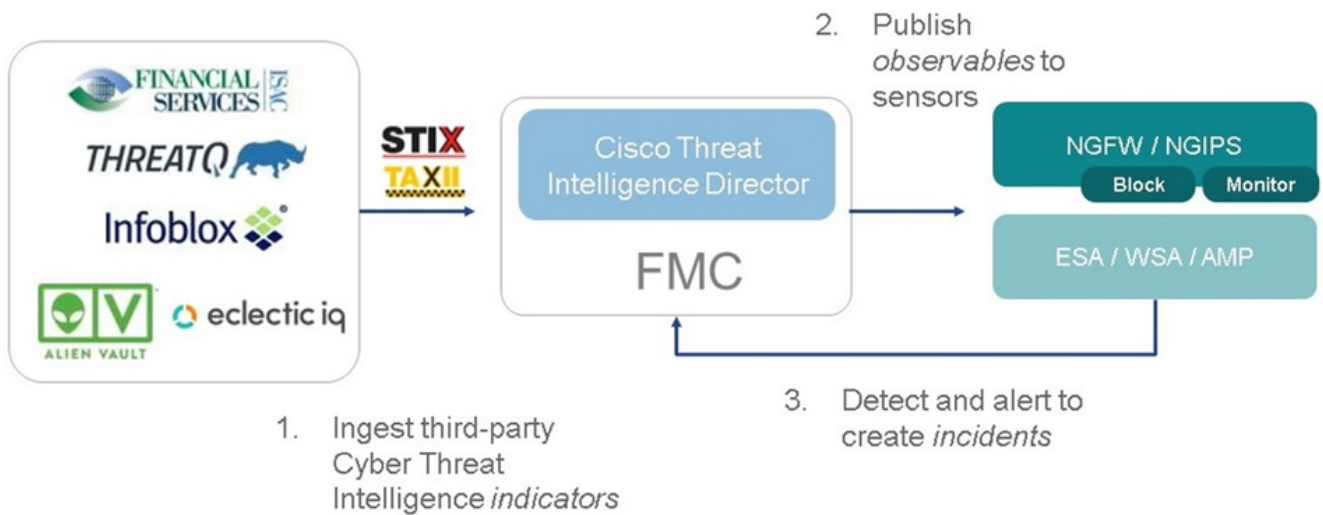
Simple Indicator

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).



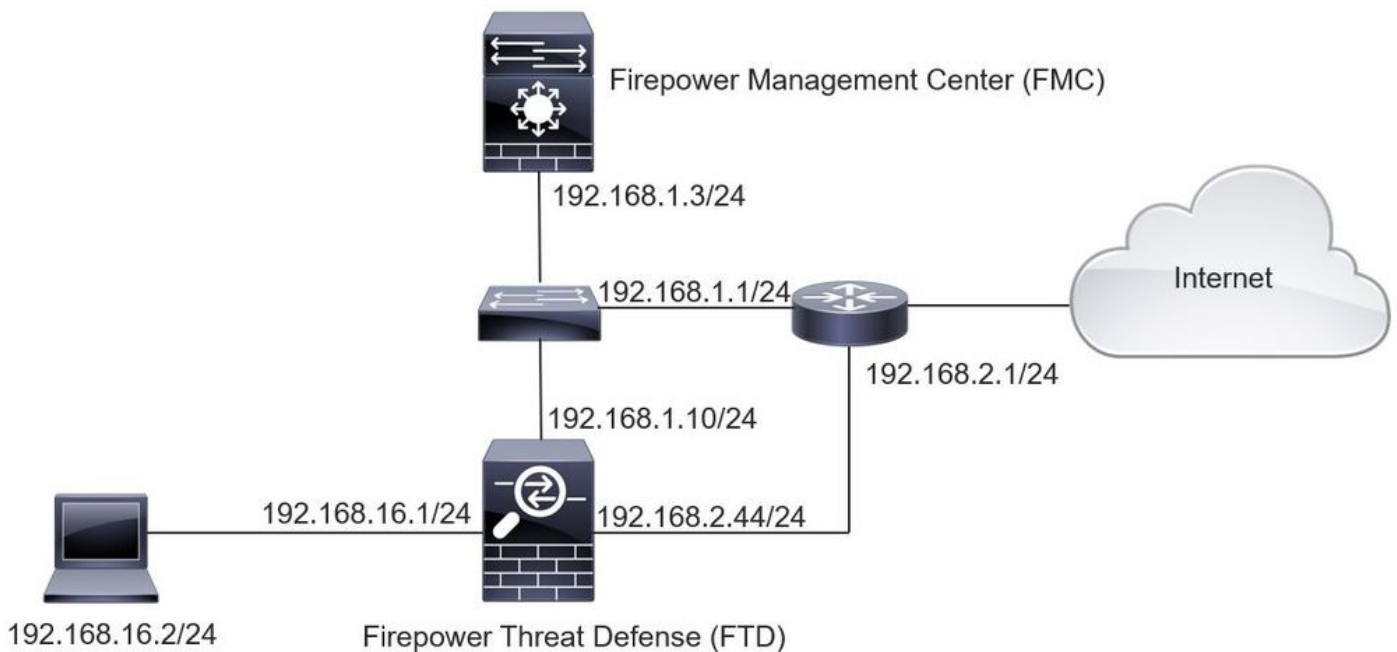
There are two new terms:

- 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.

Intelligence							Deploy	20+	System	Help	mzadlo
Sources											
Sources											
4 Sources											
Name	Type	Delivery	Action	Publish	Last Updated	Status					
<a href="#">guest.Abuse_ch</a> <small>guest.Abuse_ch</small>	STIX	TAXII	Monitor	<input checked="" type="checkbox"/>	3 hours ago   <a href="#">Pause Updates</a>	Completed with Errors					
<a href="#">guest.CyberCrime_Tracker</a> <small>guest.CyberCrime_Tracker</small>	STIX	TAXII	Monitor	<input checked="" type="checkbox"/>	3 hours ago   <a href="#">Pause Updates</a>	Completed					
<a href="#">user.AlienVault</a> <small>Data feed for user: AlienVault</small>	STIX	TAXII	Monitor	<input checked="" type="checkbox"/>	4 hours ago   <a href="#">Pause Updates</a>	Completed with Errors					
<a href="#">test_flat_file</a> <small>Test flat file</small>	IPv4 Flat File	Upload	Block	<input checked="" type="checkbox"/>	3 days ago	Completed					

 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\*  SSL Settings ▾

USERNAME

PASSWORD

**⚠** Credentials will be sent using an unsecured HTTP connection

FEEDS\*  × ▾

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

UPDATE EVERY (MINUTES)   Never Update

TTL (DAYS)

PUBLISH

**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** ? X

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

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 property from the configured sources:

Intelligence								Deploy	System	Help	admin
Sources		Indicators	Observables								
Type	Name	Source	Incidents	Action	Publish	Last Updated	Status				
IPv4	Feodo Tracker:   This IP address has been identified as malicious... <small>This IP address 162.243.159.58 has been identified as malicious by ...</small>	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... <small>This IP address 66.221.1.104 has been identified as malicious by fe...</small>	guest.Abuse_ch		Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				
Complex	Zeus Tracker (online)   elite.asia/yaweh/cidphp/file.php (201... <small>This domain elite.asia has been identified as malicious by zeustracke...</small>	guest.Abuse_ch		Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed with Errors				
Complex	Zeus Tracker (offline)   l3d.pp.ru/global/config.jp (2017-08... <small>This domain l3d.pp.ru has been identified as malicious by zeustrack...</small>	guest.Abuse_ch		Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				
Complex	Zeus Tracker (offline)   masok.com.ng/images/bro/config.jp... <small>This domain masok.com.ng has been identified as malicious by zeu...</small>	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 malicio... <small>This IP address 188.138.25.250 has been identified as malicious by ...</small>	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 malicio... <small>This IP address 77.244.245.37 has been identified as malicious by l...</small>	guest.Abuse_ch		Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				
Complex	Zeus Tracker (offline)   lsofoxcom.418.com1.ru/clock/cidph... <small>This domain lsofoxcom.418.com1.ru has been identified as malici...</small>	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 malicio... <small>This IP address 104.238.119.132 has been identified as malicious b...</small>	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 malicio... <small>This IP address 185.18.76.146 has been identified as malicious by l...</small>	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 malicio... <small>This IP address 68.168.210.95 has been identified as malicious by l...</small>	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 malicio... <small>This IP address 169.144.48.34 has been identified as malicious by l...</small>	guest.Abuse_ch		Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				

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 ? X

**NAME**  
Zeus Tracker (offline) | l3d.pp.ru/global/config.jp (2017-08-16) | This domain has been identified as malicious by zeustracker.abuse.ch

**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].

**SOURCE** guest.Abuse\_ch

**EXPIRES** Nov 27, 2017 7:16 PM CET

**ACTION** ➔ Monitor

**PUBLISH**

**INDICATOR PATTERN**

DOMAIN

l3d.pp.ru 📄

OR

URL

l3d.pp.ru/global/config.jp/ 📄

Download STIX Close

### Indicator Details ? X

**NAME**  
Feodo Tracker: | This IP address has been identified as malicious by feodotracker.abuse.ch

**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]].

**SOURCE** guest.Abuse\_ch

**EXPIRES** Nov 27, 2017 7:16 PM CET

**ACTION** ➔ Monitor ▼

**PUBLISH**

**INDICATOR PATTERN**

IPV4

[REDACTED] 📄

Download STIX Close

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.

Overview Analysis Policies Devices Objects AMP **Intelligence** Deploy System Help admin

Incidents Sources Elements Settings

Sources Indicators **Observables**

142 Observables

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	eite.asia	1	Monitor	On	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
URL	eite.asia/yaweh/cidphp/file.php/	1	Monitor	On	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
Domain	l3d.pp.ru	1	Monitor	On	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST
URL	l3d.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:

Overview Analysis Policies Devices Objects AMP **Intelligence** Deploy System Help admin

Incidents Sources **Elements** Settings

1 Element

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.

Overview Analysis Policies Devices Objects AMP **Intelligence** Deploy System Help admin

Incidents Sources Elements **Settings**

TID Detection

✔ The system is currently publishing TID observables to elements. Click Pause to stop publishing and purge TID observables stored on your elements.

Pause Resume

## Verify

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

Overview Analysis Policies Devices Objects AMP **Intelligence** Deploy System Help admin

Incidents Sources Elements Settings

Last Updated: 1 week

89 Incidents

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	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New
7 days ago	SHA-20170907-80	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New
7 days ago	SHA-20170907-79	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New
7 days ago	SHA-20170907-78	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	SHA-256	Blocked	New
7 days ago	SHA-20170907-77	2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c...	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.

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	Destination Port / ICMP Code
2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			57438 / udp	53 (domain) / udp
2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			63873 / udp	53 (domain) / udp
2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			60813 / udp	53 (domain) / udp
2017-09-17 13:01:11		Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			53451 / udp	53 (domain) / udp
2017-09-17 13:00:15		Block	IP Block	192.168.16.2	USA		USA	TID IPv4 Block			51974 / tcp	80 (http) / tcp
2017-09-17 12:59:54		Block	IP Block	192.168.16.2	USA		USA	TID IPv4 Block			51972 / tcp	80 (http) / tcp
2017-09-17 12:59:33		Block	IP Block	192.168.16.2	USA		USA	TID IPv4 Block			51970 / tcp	80 (http) / 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.ac1

-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.