

# Cisco Threat Intelligence Directorの設定とトラブルシューティング

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[この仕組みを説明しましょう](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、Cisco Threat Intelligence Director(TID)の設定およびトラブルシューティング方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center(FMC)の管理

Cisco Threat Intelligence Director機能を設定する前に、次の条件を確認する必要があります。

- Firepower Management Center(FMC): 6.2.2 ( またはそれ以降 ) バージョンで実行する必要があります ( 物理または仮想FMCでホスト可能 )。15 GB以上のRAMメモリで設定する必要があります。REST APIアクセスを有効にして設定する必要があります。
- センサーは、6.2.2以降のバージョンを実行する必要があります。
- アクセスコントロールポリシーオプションの[詳細設定]タブで、[脅威インテリジェンスディレクタを有効にする]を有効にする必要があります。
- アクセスコントロールポリシーがまだ存在しない場合は、ルールを追加します。
- SHA-256観測結果とFirepower Management Centerイベントを生成する場合は、1つ以上のMalware Cloud LookupまたはBlock Malwareファイルルールを作成し、そのファイルポリシーをアクセスコントロールポリシーの1つ以上のルールに関連付けます。
- IPv4、IPv6、URL、またはドメイン名の観測によって接続およびセキュリティインテリジェンスイベントを生成する場合は、アクセスコントロールポリシーで接続およびセキュリティインテリジェンスロギングを有効にします。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- 6.2.2.81を実行するCisco Firepower Threat Defense(FTD)仮想
- 6.2.2.81が稼働するFirepower Management Center Virtual(vFMC)

注：このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

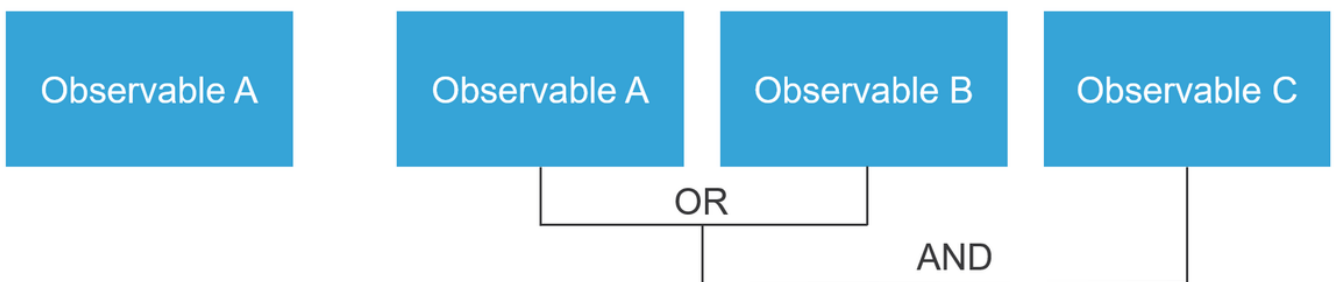
## 背景説明

Cisco Threat Intelligence Director(TID)は、脅威インテリジェンス情報を操作するシステムです。このシステムは、異種のサードパーティ製のサイバー脅威インテリジェンスを消費して正規化し、検出テクノロジーにインテリジェンスを公開し、検出テクノロジーからの観測を関連付けます。

次の3つの新しい用語があります。回答、インジケータ、インシデーション。Observableは変数にすぎず、例えばURL、ドメイン、IPアドレス、SHA256などです。インジケータには2つのタイプがあります。単純なインジケータには、1つの観察可能なインジケータだけが含まれます。複雑な指標の場合は、ANDやORなどの論理機能を使用して相互に接続された2つ以上の観測者があります。FMCでブロックまたはモニタする必要があるトラフィックがシステムで検出されると、インシデントが発生します。

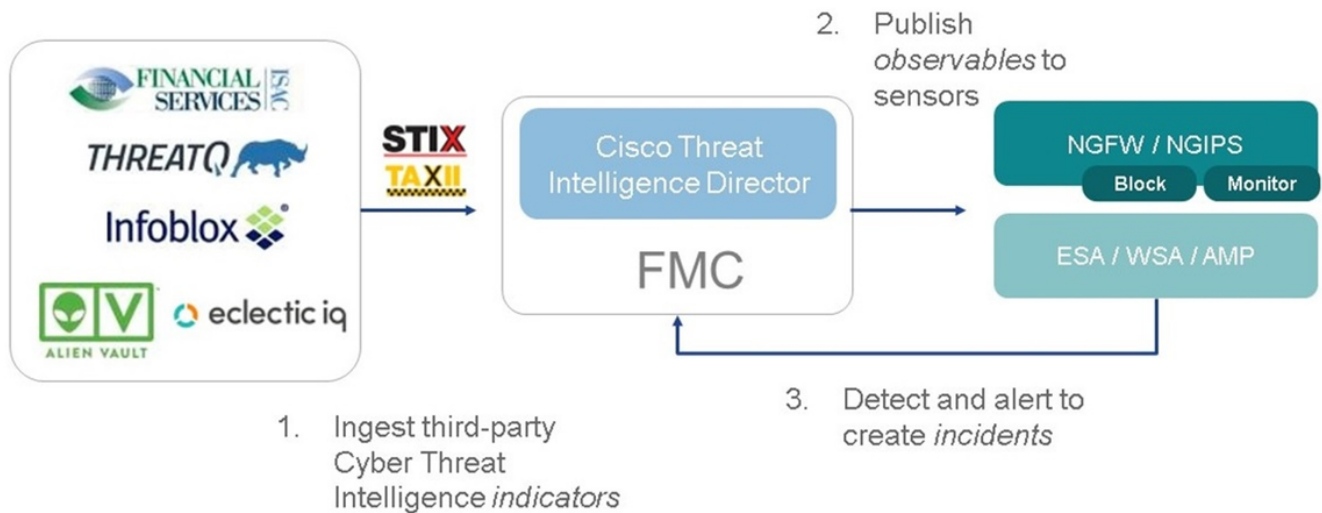
Simple Indicator

Complex indicator, two operators



## この仕組みを説明しましょう

図に示すように、FMCでは、脅威インテリジェンス情報をダウンロードするソースを設定する必要があります。その後、FMCはその情報（観測量）をセンサーにプッシュします。トラフィックが回答に一致すると、FMCユーザインターフェイス(GUI)にインシデントが表示されます。



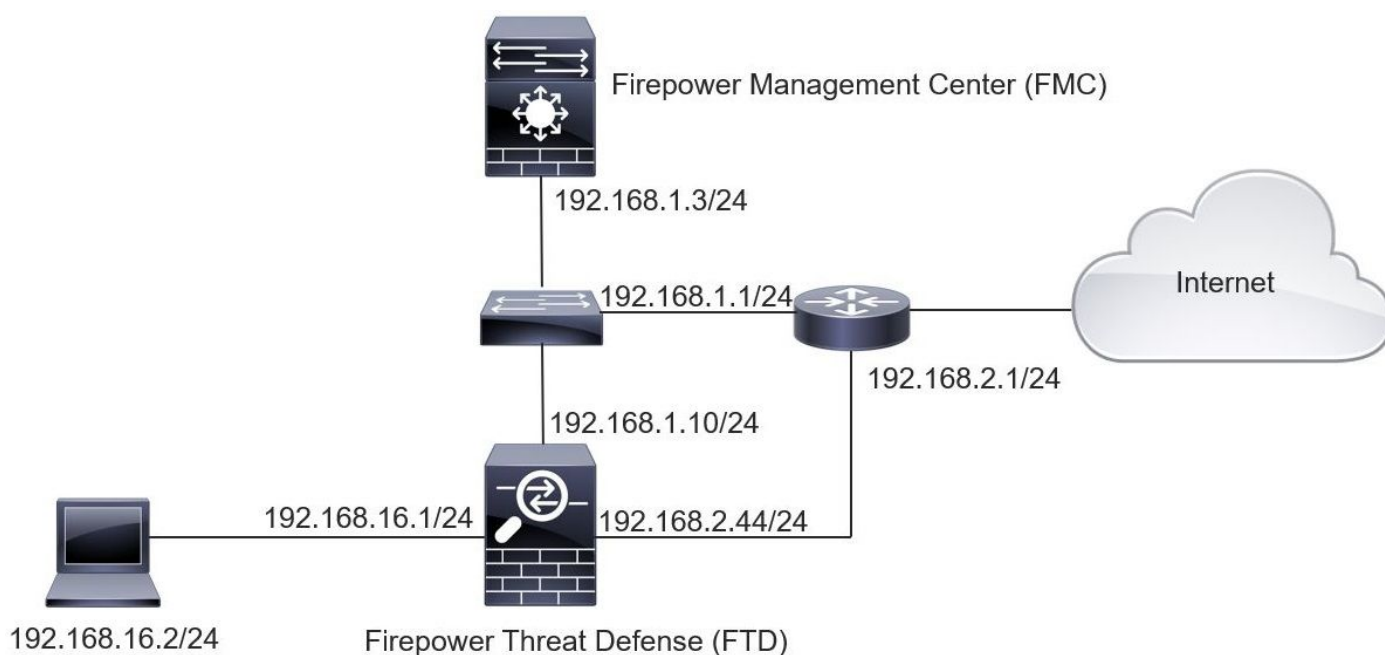
新しい用語は2つあります。

- STIX(Structured Threat Intelligence eXpression)は、脅威インテリジェンス情報を共有および使用するための標準です。主な機能要素は3つあります。指標、回答、およびインシデント
- TAXII(Trusted Automated eXchange of Indicator Information)は、脅威情報の転送メカニズムです

## 設定

設定を完了するには、次のセクションを考慮してください。

### ネットワーク図



## コンフィギュレーション

ステップ1:TIDを設定するには、図に示すように[Intelligence]タブに移動する必要があります。

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

注：フィードにサポートされていない回答が含まれている場合、状態'エラーで完了'が必要です。

ステップ2：脅威の原因を追加する必要があります。ソースを追加するには、次の3つの方法があります。

- TAXII：このオプションを使用すると、脅威情報がSTIX形式で保存されるサーバを設定できます

## Add Source ? X

DELIVERY **TAXII** URL Upload

---

URL\*  SSL Settings ▾

USERNAME

PASSWORD

⚠ Credentials will be sent using an unsecured HTTP connection

FEEDS\*  X ▾

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

注：使用できるアクションは[Monitor]のみです。脅威に対するブロックアクションをSTIX形式で設定することはできません。

- URL:STIXの脅威またはフラットファイルが配置されているHTTP/HTTPSローカルサーバへのリンクを設定できます。

## Add Source



DELIVERY TAXII **URL** Upload

TYPE STIX

URL\*

SSL Settings

NAME\*

DESCRIPTION

ACTION Monitor

UPDATE EVERY (MINUTES)

1440

Never Update

TTL (DAYS)

90

PUBLISH



Save

Cancel

- フラットファイル：ファイルを\*.txt形式でアップロードでき、ファイルの内容を指定する必要があります。ファイルには、1行に1つのコンテンツエントリが含まれている必要があります。

**Add Source** ? X

DELIVERY

---

TYPE  CONTENT

FILE\* 

Drag and drop or click

NAME\*

DESCRIPTION

ACTION

TTL (DAYS)

PUBLISH

注：デフォルトでは、すべてのソースがパブリッシュされ、センサーにプッシュされます。  
このプロセスには最大20分以上かかる場合があります。

ステップ3:[Indicator (インジケータ)]タブで、設定されたソースからインジケータがダウンロードされたかどうかを確認できます。

Intelligence								Deploy	System	Help	admin
Sources											
Indicators											
Sources											
Indicators											
Observables											
x Last Updated 1 week											
111 Indicators											
Type	Name	Source	Incidents	Action	Publish	Last Updated	Status				
IPv4	Feodo Tracker:   This IP address has been identified as malicious by ... <small>This IP address 162.243.159.58 has been identified as malicious by ...</small>	guest.Abuse_ch	1	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 fe... <small>This IP address 66.221.1.104 has been identified as malicious by fe...</small>	guest.Abuse_ch	1	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 zeustrack...</small>	guest.Abuse_ch	1	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	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				
Complex	Zeus Tracker (offline)   masoic.com.ng/images/bro/config.jp-... <small>This domain masoic.com.ng has been identified as malicious by zeu...</small>	guest.Abuse_ch	1	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 ... <small>This IP address 188.138.25.250 has been identified as malicious by ...</small>	guest.Abuse_ch	1	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 f...</small>	guest.Abuse_ch	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				
Complex	Zeus Tracker (offline)   lisovfoxcom.418.com1.ru/clock/cidph... <small>This domain lisovfoxcom.418.com1.ru has been identified as malici...</small>	guest.Abuse_ch	1	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	1	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 f...</small>	guest.Abuse_ch	1	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 f...</small>	guest.Abuse_ch	1	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 f...</small>	guest.Abuse_ch	1	Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				

ステップ4：インジケータの名前を選択すると、インジケータの詳細が表示されます。さらに、センサーにパブリッシュするか、アクションを変更するかを決定できます（単純なインジケータの場合）。

図に示すように、OR演算子によって接続された2つの観測値を含む複合インジケータがリストされます。



### Indicator Details

**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/

### Indicator Details

**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

ステップ5:[Responsive]タブに移動すると、インジケータに含まれているURL、IPアドレス、ドメイン、およびSHA256が表示されます。センサーにプッシュする回答を決定し、必要に応じてアクションを変更できます。最後の列には、公開/非公開のオプションに相当するホワイトリストボタンがあります。

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

Incidents Sources Elements Settings

Sources Indicators **Observables**

Q 142 Observables

Type	Value	Indicators	Action	Publish	Updated At	Expires	
IPV4	[REDACTED]	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
IPV4	[REDACTED]	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
Domain	eite.asia	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
URL	eite.asia/yaweh/cidphp/file.php/	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
Domain	l3d.pp.ru	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
URL	l3d.pp.ru/global/config.jp/	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
URL	masoic.com.ng/images/bro/config.jpg/	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
Domain	masoic.com.ng	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
IPV4	[REDACTED]	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
IPV4	[REDACTED]	1	➔ Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Dec 12, 2017 9:50 AM EST	
Domain	lisovfoxcom.418.com1.ru	1	➔ Monitor	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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

ステップ6:[Elements]タブに移動して、TIDが有効になっているデバイスのリストを確認します。

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

ステップ7 ( オプション ) : [Settings]タブに移動し、[Pause]ボタンを選択して、センサーへのインジケータのプッシュを停止します。この操作には最大20分かかります。

TID Detection

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

## 確認

方法1. TIDがトラフィックに対してアクションを実行したかどうかを確認するには、[Incidents]タブに移動する必要があります。

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

方法2. インシデントは、TIDタグの下の[Security Intelligence Events]タブで確認できます。

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

注：TIDのストレージ容量は100万インシデントです。

方法3.設定済みのソース ( フィード ) がFMCとセンサーに存在するかどうかを確認できます。これを行うには、CLIで次の場所に移動します。

`/var/sf/siurl_download/`

`/var/sf/sidns_download/`

`/var/sf/iprep_download/`

SHA256フィード用に新しいディレクトリが作成されます。`/var/sf/sifile_download/` にアクセスしてください。

```
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
7a00ef4b801b2b2acd09b5fc72d7c79d20094ded6360fb936bf2c65aff16907
2922f0bb1acf9c221b6cec45d6d10ee9cf12117fa556c304f94122350c2bcdbc
```

注：TIDは、FMCのグローバルドメインでのみ有効です

注：ハイアベイラビリティ設定 ( 物理FMCアプライアンス ) でアクティブなFirepower Management Center(FMC)でTIDをホストする場合、システムはTID設定とTIDデータをスタンバイのFirepower Management Centerに同期しません。

## トラブルシューティング

tidと呼ばれるトップレベルのプロセスがあります。このプロセスは、次の3つのプロセスに依存します。RabbitMQ、Redis、mongo。プロセスを確認するには、pmtoolのステータスを実行します | `grep 'RabbitMQ|mongo|redis|tid' | grep " - "`

```
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#
```

どのようなアクションが行われたかをリアルタイムで確認するには、`system support firewall-engine-debug`コマンドまたは`system support trace`コマンドを実行することができます。

```
> 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
```

アクションの観点では、次の2つの可能性があります。

- URL SI:ルールの順序19、ID 19、SIリストID 1074790455、アクション4 – トラフィックがブロックされました
- URL SI:ルールの順序20、ID 20、SIリストID 1074790456、アクション6 – トラフィックが監視されました。