

# Configurar e solucionar problemas do Cisco Threat Intelligence Diretor

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Como funciona?](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Verificar](#)

[Troubleshooting](#)

---

## Introdução

Este documento descreve como configurar e solucionar problemas do Cisco Threat Intelligence Diretor (TID).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Administração do Firepower Management Center (FMC).

Você precisa garantir essas condições antes de configurar o recurso Cisco Threat Intelligence Diretor:

- O Firepower Management Center (FMC):
  - Deve ser executado na versão 6.2.2 (ou posterior) (pode ser hospedado em FMC físico ou virtual).
  - Deve ser configurado com um mínimo de 15 GB de memória RAM.
  - Deve ser configurado com acesso à API REST habilitado.
- O sensor deve executar a versão 6.2.2 (ou posterior).
- Na guia Advanced Settings da opção de política de controle de acesso, Enable Threat Intelligence Diretor deve ser habilitado.
- Adicione regras à política de controle de acesso se elas ainda não estiverem presentes.
- Se você quiser que os observáveis SHA-256 gerem observações e eventos do Firepower


Management Center, crie uma ou mais regras de arquivo Malware Cloud Lookup ou Block Malware e associe a política de arquivo a uma ou mais regras na política de controle de acesso.

- Se desejar que as observações de IPv4, IPv6, URL ou Nome do domínio gerem eventos de inteligência de conexão e segurança, habilite o registro de inteligência de conexão e segurança na política de controle de acesso.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Firepower Threat Defense (FTD) Virtual, que executa a versão 6.2.2.81
- Firepower Management Center Virtual (vFMC) que executa a versão 6.2.2.81

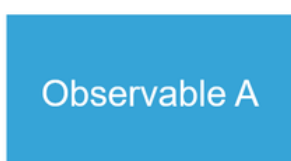
 Observação: as informações neste documento foram criadas a partir dos dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

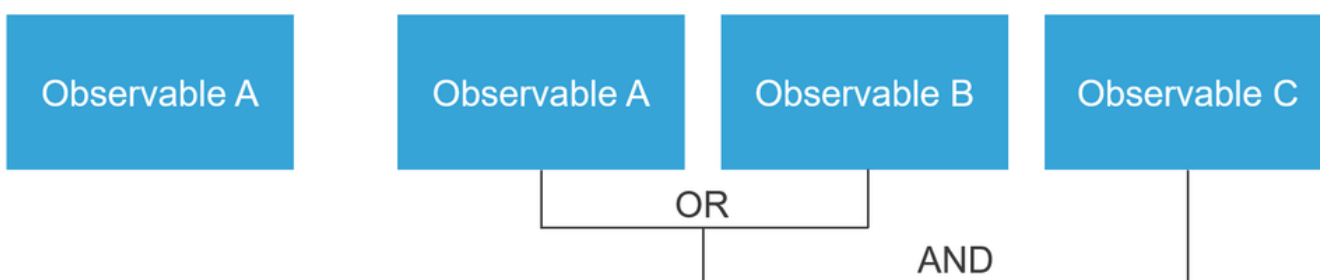
O Cisco Threat Intelligence Diretor (TID) é um sistema que operacionaliza as informações de inteligência de ameaças. O sistema consome e normaliza a inteligência de ameaças cibernéticas heterogêneas de terceiros, publica a inteligência para tecnologias de detecção e correlaciona as observações das tecnologias de detecção.

Há três termos novos: observáveis, indicadores e incidentes. Observável é apenas uma variável, que pode ser por exemplo URL, domínio, endereço IP ou SHA256. Os indicadores são feitos a partir de observáveis. Existem dois tipos de indicadores. Um indicador simples contém apenas um que pode ser observado. No caso de indicadores complexos, há dois ou mais observáveis que estão conectados um ao outro usando funções lógicas como AND e OR. Quando o sistema detecta o tráfego que deve ser bloqueado ou monitorado no FMC, o incidente aparece.

### Simple Indicator

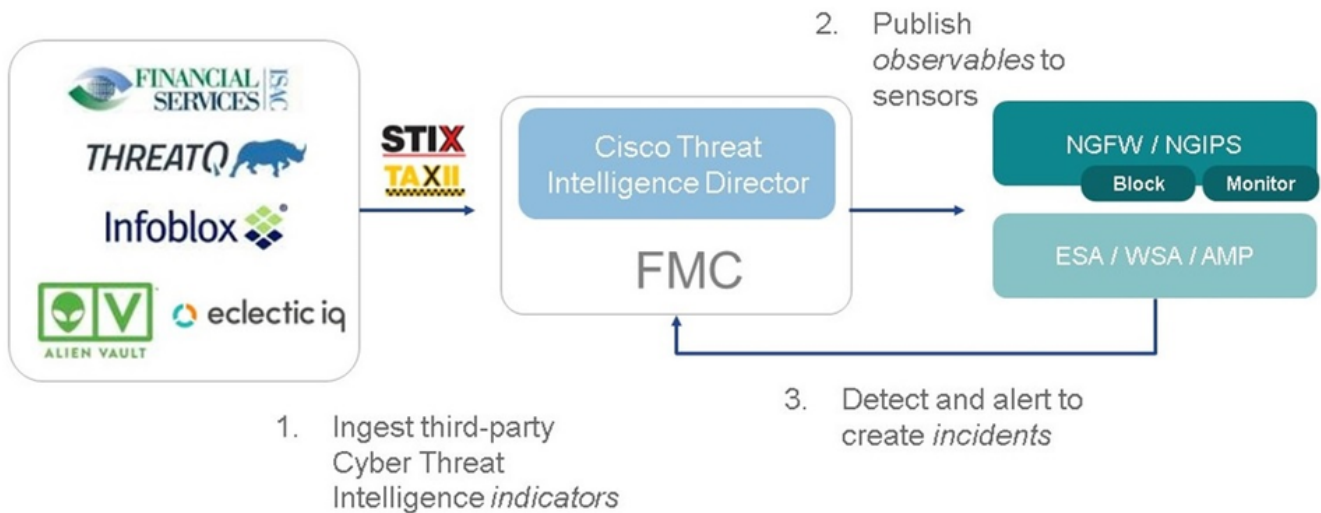


### Complex indicator, two operators



## Como funciona?

Como mostrado na imagem, no FMC você precisa configurar fontes de onde gostaria de fazer o download de informações de inteligência de ameaças. Em seguida, o FMC envia essas informações (observáveis) aos sensores. Quando o tráfego corresponde aos observáveis, os incidentes aparecem na interface de usuário (GUI) do FMC.



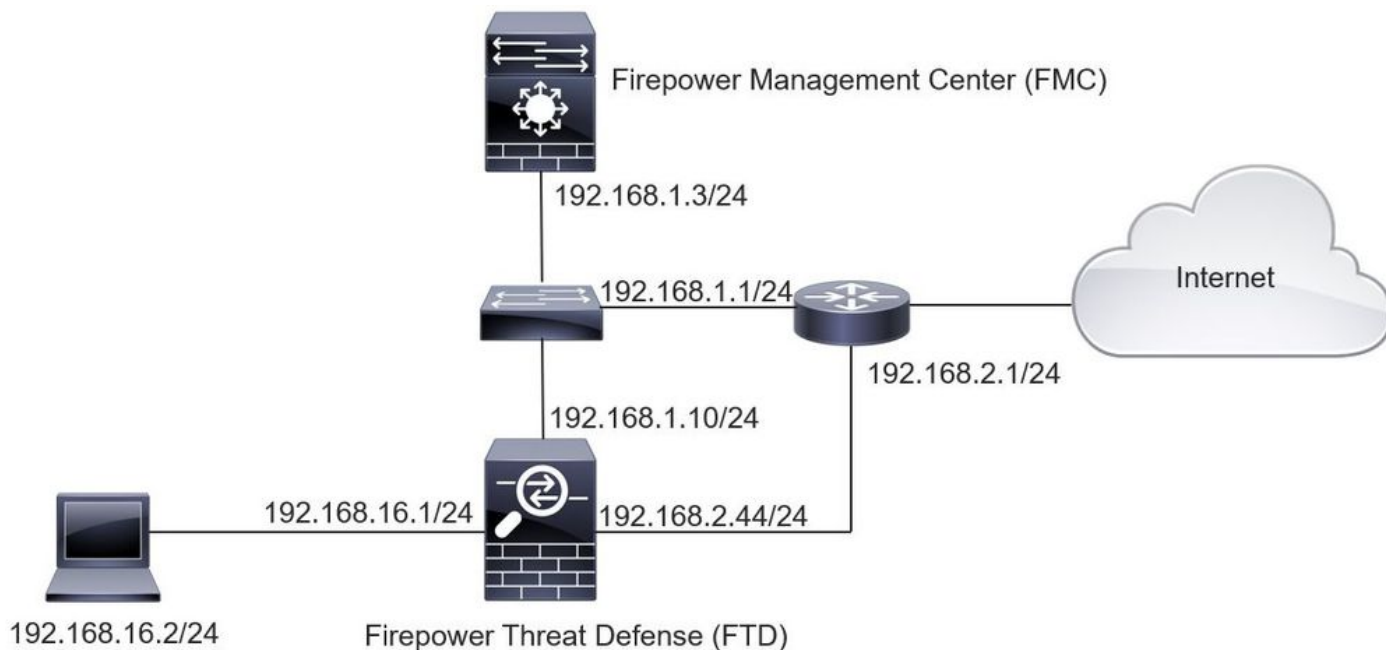
Há dois novos termos:

- STIX (Structured Threat Intelligence eXpression) é um padrão para compartilhar e usar informações de inteligência de ameaças. Há três elementos funcionais principais: indicadores, observáveis e incidentes.
- O TAXII (Trusted Automated eXchange of Indicator Information) é um mecanismo de transporte para informações sobre ameaças.

## Configurar

Para concluir a configuração, leve em consideração estas seções:

### Diagrama de Rede



## Configuração

Etapa 1. Para configurar o TID, você precisa navegar até a guia Intelligence, como mostrado na imagem.

The screenshot shows the 'Intelligence' tab in the FMC interface. The 'Sources' sub-tab is active, displaying a table of configured sources. The table has columns for Name, Type, Delivery, Action, Publish, Last Updated, and Status. There are four sources listed:

Name	Type	Delivery	Action	Publish	Last Updated	Status
guest.Abuse_ch <i>guest.Abuse_ch</i>	STIX	TAXII	Monitor	On	3 hours ago   Pause Updates	Completed with Errors
guest.CyberCrime_Tracker <i>guest.CyberCrime_Tracker</i>	STIX	TAXII	Monitor	On	3 hours ago   Pause Updates	Completed
user.AlienVault <i>Data feed for user: AlienVault</i>	STIX	TAXII	Monitor	On	4 hours ago   Pause Updates	Completed with Errors
test_flat_file <i>Test flat file</i>	IPv4 Flat File	Upload	Block	On	3 days ago	Completed

Observação: o status 'Concluído com erros' é esperado caso um feed contenha observáveis sem suporte.

Etapa 2. Você precisa adicionar fontes de ameaças. Há três maneiras de adicionar origens:

- TAXII - Ao usar essa opção, você pode configurar um servidor no qual as informações sobre ameaças são armazenadas no formato STIX.

## 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

 Observação: a única ação disponível é Monitorar. Você não pode configurar a Ação de bloqueio para ameaças no formato STIX.

- URL - Você pode configurar um link para um servidor local HTTP/HTTPS onde a ameaça STIX ou o arquivo simples está localizado.

### 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

- Arquivo simples - Você pode carregar um arquivo no formato \*.txt e deve especificar o conteúdo do arquivo. O arquivo deve conter uma entrada de conteúdo por linha.

### Add Source ? X

DELIVERY TAXII URL Upload

---

TYPE Flat File CONTENT SHA-256

FILE\* Drag and drop or click

NAME\*

DESCRIPTION

ACTION Block

TTL (DAYS)

PUBLISH

Save Cancel

SHA-256

SHA-256

Domain


URL

IPv4

IPv6

Email To

Email From

 Observação: por padrão, todas as fontes são publicadas, o que significa que elas são enviadas aos sensores. Esse processo pode levar até 20 minutos ou mais.

Etapa 3. Na guia Indicador, você pode confirmar se os indicadores foram baixados das propriedades das fontes configuradas:

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 zeustrack...</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)   lsovofoxcom.418.com1.ru/clock/cidph... <small>This domain lsovofoxcom.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 169.148.48.34 has been identified as malicious by f...</small>	guest.Abuse_ch		Monitor	<input checked="" type="checkbox"/>	Sep 13, 2017 10:50 AM EDT	Completed				

Etapa 4. Depois de selecionar o nome de um indicador, você poderá ver mais detalhes sobre ele. Além disso, você pode decidir se deseja publicá-lo no sensor ou se deseja alterar a ação (no caso de um indicador simples).

Como mostrado na imagem, um indicador complexo é listado com dois observáveis que estão conectados pelo operador OR:



<h3>Indicator Details</h3> <p><b>NAME</b> 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><b>DESCRIPTION</b> 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><b>SOURCE</b> guest.Abuse_ch</p> <p><b>EXPIRES</b> Nov 27, 2017 7:16 PM CET</p> <p><b>ACTION</b> <input type="button" value="Monitor"/></p> <p><b>PUBLISH</b> <input checked="" type="checkbox"/></p> <p><b>INDICATOR PATTERN</b></p> <p>DOMAIN l3d.pp.ru</p> <p>OR</p> <p>URL l3d.pp.ru/global/config.jp/</p> <p><input type="button" value="Download STIX"/> <input type="button" value="Close"/></p>	<h3>Indicator Details</h3> <p><b>NAME</b> Feodo Tracker:   This IP address has been identified as malicious by feodotracker.abuse.ch</p> <p><b>DESCRIPTION</b> 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><b>SOURCE</b> guest.Abuse_ch</p> <p><b>EXPIRES</b> Nov 27, 2017 7:16 PM CET</p> <p><b>ACTION</b> <input type="button" value="Monitor"/></p> <p><b>PUBLISH</b> <input checked="" type="checkbox"/></p> <p><b>INDICATOR PATTERN</b></p> <p>IPV4 [REDACTED]</p> <p><input type="button" value="Download STIX"/> <input type="button" value="Close"/></p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Etapa 5. Navegue até a guia Observáveis, onde você pode encontrar URLs, endereços IP, domínios e SHA256 incluídos nos indicadores. Você pode decidir quais observáveis gostaria de enviar aos sensores e, opcionalmente, alterar a ação deles. Na última coluna, há um botão da lista branca que é equivalente a uma opção de publicar/não publicar.

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

Etapa 6. Navegue até a guia Elementos para verificar a lista de dispositivos onde o TID está habilitado:

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

Etapa 7 (opcional). Navegue até a guia Configurações e selecione o botão Pausar para parar de enviar indicadores aos sensores. Essa operação pode levar até 20 minutos.

**TID Detection**

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

## Verificar

Método 1. Para verificar se o TID agiu no tráfego, você precisa navegar até a guia Incidentes.

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

Método 2. Os incidentes podem ser encontrados na guia Security Intelligence Events sob uma marca TID.

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	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	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	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	2017-09-17 13:01:11	Allow	DNS Monitor	192.168.16.2	NLD		NLD	TID Domain Name Monitor			53451 / tcp	53 (domain) / udp
2017-09-17 13:00:15	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	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	2017-09-17 12:59:33	Block	IP Block	192.168.16.2	USA		USA	TID IPv4 Block			51970 / tcp	80 (http) / tcp

Observação: o TID tem uma capacidade de armazenamento de 1 milhão de incidentes.

Método 3. Você pode confirmar se as fontes configuradas (feeds) estão presentes no FMC e em um sensor. Para fazer isso, você pode navegar para estes locais na CLI:

```
/var/sf/siurl_download/
```

```
/var/sf/sidns_download/
```

```
/var/sf/iprep_download/
```

Há um novo diretório criado para feeds 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-f6cc0e401935.1f
-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
```

---

 Observação: o TID está habilitado somente no domínio global no FMC.

---

 Observação: se você hospedar o TID no Firepower Management Center ativo em uma configuração de alta disponibilidade (dispositivos físicos do FMC), o sistema não sincronizará as configurações do TID e os dados do TID com o Firepower Management Center em espera.

---

## Troubleshooting

Há um processo de nível superior chamado tid. Este processo depende de três processos: mongo, RabbitMQ, e redis. Para verificar o status de execução de processos pmtool | grep 'RabbitMQ\|mongo\|redis\|tid' | comando grep " - " .

<#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#
```

Para verificar em tempo real qual ação é tomada, você pode executar o comando system support firewall-engine-debug ou 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
```

Existem duas possibilidades em termos de ação:

- URL SI: ordem de regra correspondente 19, ID 19, id de lista 1074790455, ação 4 - o tráfego foi bloqueado.
- URL SI: ordem de regra correspondente 20, ID 20, id de lista 1074790456, ação 6 - o tráfego foi monitorado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.