

# Configure SecureX Threat Response Feeds to Block URL on Firepower

## Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Create SecureX Threat Response Feed](#)

[Configure FMC Threat Intelligence Director to consume Threat Response Feed](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes how to create threat intelligence from URLs and IPs found during Threat Response investigations to be consumed by Firepower.

## Background Information

Cisco Threat Response is a powerful tool capable of investigate threats across the entire environment thanks to the information from multiple modules. Each module provides the information generated by security product like Firepower, Secure Endpoint, Umbrella, and other third-party vendors. These investigations can not only help to reveal if a threat exist on the system but also help to generate important Threat intelligence, which can be sourced back to the security product to enhance the security in the environment.

Some important terminology used by SecureX Threat Response:

- **Indicator** is a collection of observables which are logically related with AND and OR operators. There are complex Indicators which combine multiple observables, in addition there are also simple indicators which are made of only one observable.
- **Observable** is a variable which can be an IP, Domain, URL or a sha256.
- **Judgments** are created by the user and used to link an observable with a disposition for a specific period of time.
- **Feeds** are created to share the Threat Intelligence generated by SecureX Threat Response investigation with other security products like firewalls and email content filters like Firepower and ESA.

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- SecureX CTR ( Cisco Threat Response .
- Firepower TID ( Threat Intelligence Director ).
- Firepower Access Control Policies configuration.

This document uses Firepower TID to enforce the Threat Intelligence generated on SecureX Threat Response. The requirements to use TID on your FMC deployment as for FMC version 7.3 are:

- Version 6.2.2 or later.
- configured with a minimum of 15 GB of memory.
- configured with REST API access enabled. See Enable REST API Access in the Cisco Secure Firewall Management Center Administration Guide .
- You can use FTD as a threat intelligence director element if the device is on Version 6.2.2 or higher.

**Note:** This Documents considers that Threat Intelligence Director is already active on the system. For more information about TID initial configuration and troubleshoot check the links available on the Related Information section.

## Components Used

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

- SecureX Cisco Threat Response Dashboard
- FMC (Firewall Management Center) version 7.3
- FTD (Firewall Threat Response) version 7.2

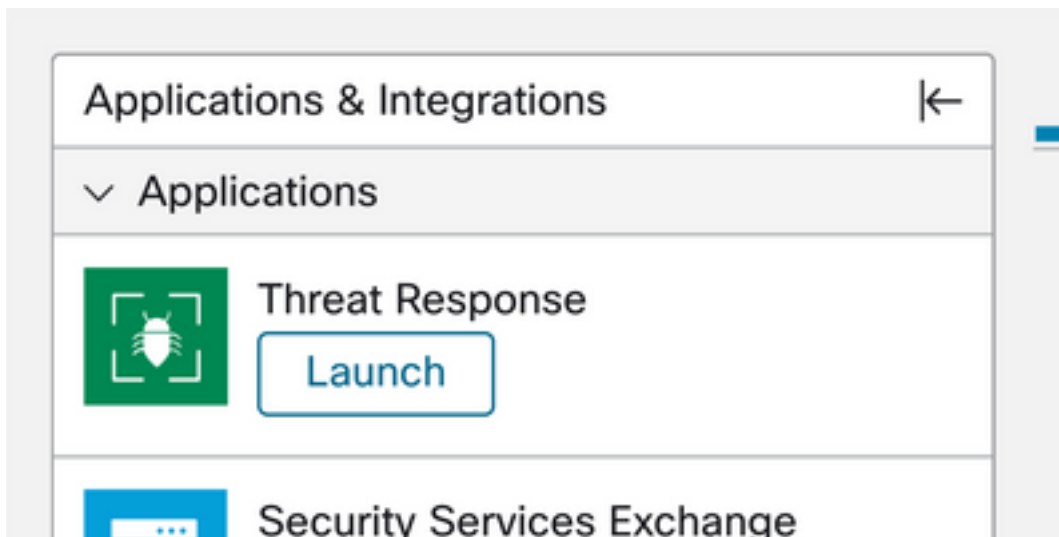
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configure

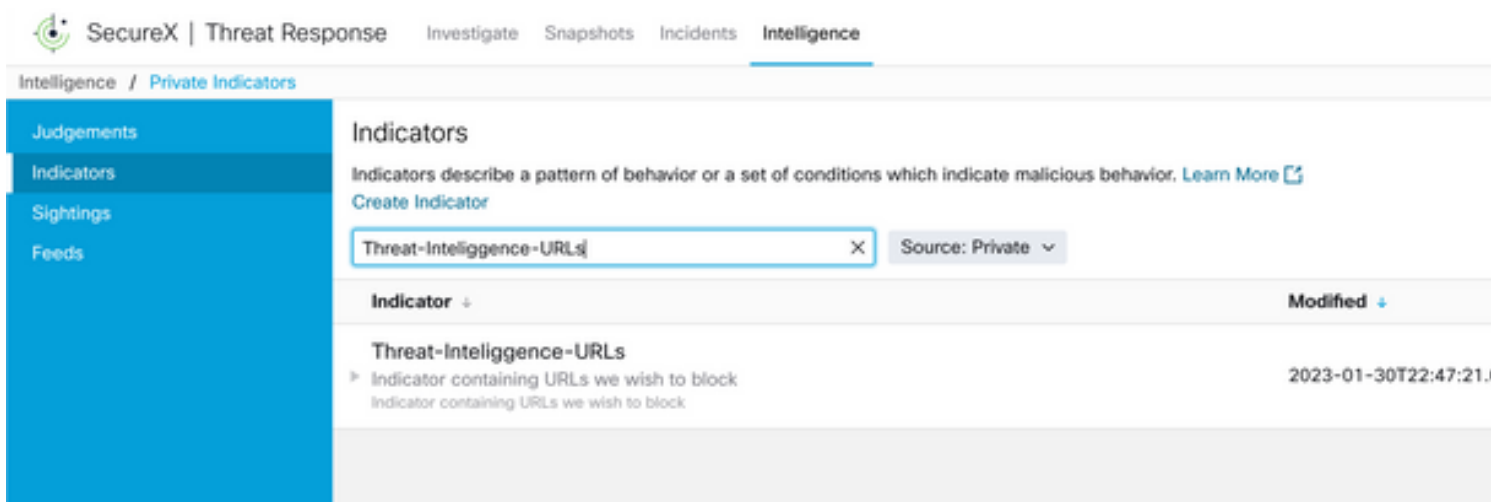
### Create SecureX Threat Response Feed

SecureX Threat Response allows to start an investigation on the environment with an observable as input. Threat Response engine queries the modules to search for any activity related to the observable. Investigation returns any match found by the modules, this information can include IPs, Domains, Urls emails or files. Next steps create a feed to consume information with other Security Products.

**Step 1** Log in into your SecureX dashboard and click **Launch** button for Threat Response Module. This opens Threat Response page on a new windows:



**Step 2** In the Threat Response page click Intelligence > Indicators and then change the Source dropdown List from Public to Private. This must allow you to click Create Indicator link. Once inside the Indicator creator wizard choose any meaningful Title and Description for your Indicator, after that check the URL Watchlist check box. At this moment you can save the indicator, no further information is needed, however, you can choose to configure the rest of available options.



**Step 3** Navigate to **Investigate** tab and paste any observable you would like to investigate into the investigation box. For demonstrative purposes the fake URL `https://malicious-fake-domain.com` was used for this configuration example. Click **Investigate** and wait for the investigation to finish. As expected the dummy URL disposition is unknown. Proceed to right click on the **Down** side arrow to expand the contextual menu and click **create Judgement**.



**Step 4** Click **Link Indicators** and select the indicator from step 2. Select disposition as **Malicious** and choose the Expiration day as you consider appropriate. Finally Click the **Create** button. The URL must be now visible under **Intelligence > Indicators > View Full Indicator**.

### Create Judgement

Create a new Judgement for *domain:malicious-fake-domain.com*

Indicators\* ?

Threat-Intelligence-URLs 🗑️

[Link Indicators](#)

Disposition\* ▼

Malicious

Expiration\* ▼

31 ↕ Days

TLP ▼

Amber

Reason

[Cancel](#)
[Create](#)

## Threat-Intelligence-URLs [Edit Indicator](#)

### Description

Indicator containing URLs we wish to block

### Short Description

Indicator containing URLs we wish to block

### Likely Impact

None Included

### Kill Chain Phases

None Included

### Judgements

Judgement	Type	Start/End Times	...
<span style="font-size: 0.8em;">▶</span> <span style="font-size: 0.8em;">malicious-fake-domain.com</span> <span style="font-size: 0.8em; color: red;">Malicious</span> <span style="font-size: 0.8em;">🗑️</span>	Domain	2023-01-30T23:34:24.5... 2023-03-02T23:34:24.5...	

<
>
5 per page
Showing 1-1 of 1

<b>ID</b>	https://private.intel.amp.cisco.com
<b>Producer</b>	Cisco - MSSP - Jobarrie
<b>Source</b>	None Included
<b>Create Date</b>	2023-01-30T22:47:21.076Z
<b>Last Modified</b>	2023-01-30T22:47:21.055Z
<b>Expires</b>	Indefinite
<b>Revisions</b>	1
<b>Confidence</b>	High
<b>Severity</b>	High
<b>TLP</b>	Red

**Step 5** Navigate to **Intelligence > Feeds** and click **Create Feed URL**. Fill the **Title** field and then **select** the **Indicator** created in Step 2. Make sure to leave **Output** dropdown list as **observables** and Click **Save**.

## Create Feed URL

Title\* ⓘ  
Threat-Intelligence-TR-URLs

Indicator\* ⓘ  
Threat-Intelligence-URLs - Indicator containing URLs we wish to block

Output ⓘ  
Observables

Expiration\* ⓘ  
January 30, 2023

Forever

Anyone with the URL will be able to view this feed.

Cancel Save

**Step 6** Verify Feed was created under **Intelligence > Feeds** and then click to expand on the feed details. Click on the **URL** to visualize that the expected URLs is listed on the feed.

SecureX | Threat Response Investigate Snapshots Incidents **Intelligence**

Intelligence / Feeds

Judgements  
Indicators  
Sightings  
**Feeds**

### Feeds

These feeds were created or saved from private sources. Anyone with the URL can view the feed.  
Create Feed URL

Search

Feed	Created ↓
Threat-Intelligence-TR-URLs Observables	2023-01-31T00:33:26.288Z Admin El mero mero 2

**Title:** Threat-Intelligence-TR-URLs  
**Output:** Observables  
**Created:** 2023-01-31T00:33:26.288Z  
**Creator:** Admin El mero mero 2  
**Expiration:** Indefinite  
**URL:** <https://private.intel.amp.cisco.com:443/ctia/feed/feed-166dd95a-815a-4a0e-9b38-1c1a89145479/view.txt?s=c8bee89a-7e12-4d8b-a3d7-751014cedc20>

Show JSON

## Cofigure FMC Threat Intelligence Director to consume Threat Response Feed

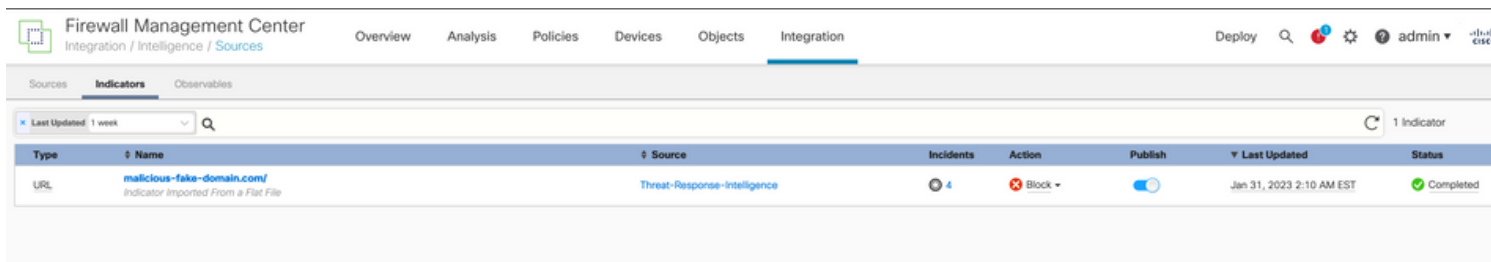
**Step 1** Log in into your FMC dashboard and navigate to **Integration > Intelligence > Sources**. Click the **plus** sigh to add a new Source.

## Step 2 Create the new source with these settings:

- Delivery > Select URL
- Type > Select Flat File
- Content > Select URL
- Url > Paste the URL from section "Create SecureX Threat Response Feed" step 5.
- Name > Choose any name you see fit
- Action > Select Block
- Update Every > Select 30 min ( for quick updates for Threat Intelligence feed )

Click **Save**.

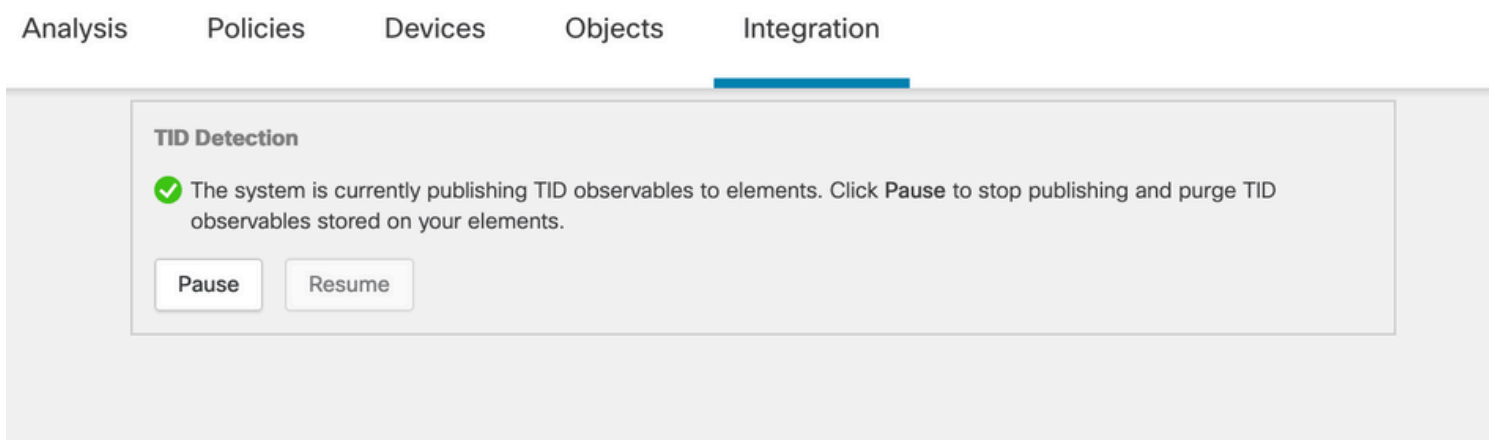
## Step 3 Under Indicators and Observables verify domain is listed:



The screenshot shows the 'Indicators' tab in the Firewall Management Center. A table lists one indicator with the following details:

Type	Name	Source	Incidents	Action	Publish	Last Updated	Status
URL	malicious-fake-domain.com/ <small>Indicator Imported From a Flat File</small>	Threat-Response-Intelligence	4	Block	<input checked="" type="checkbox"/>	Jan 31, 2023 2:10 AM EST	Completed

## Step 4 Make sure Threat Intelligence Director is Active and keeps the elements up to date ( FTDs devices ). Navigate to **Integrations > Intelligence > Elements**:



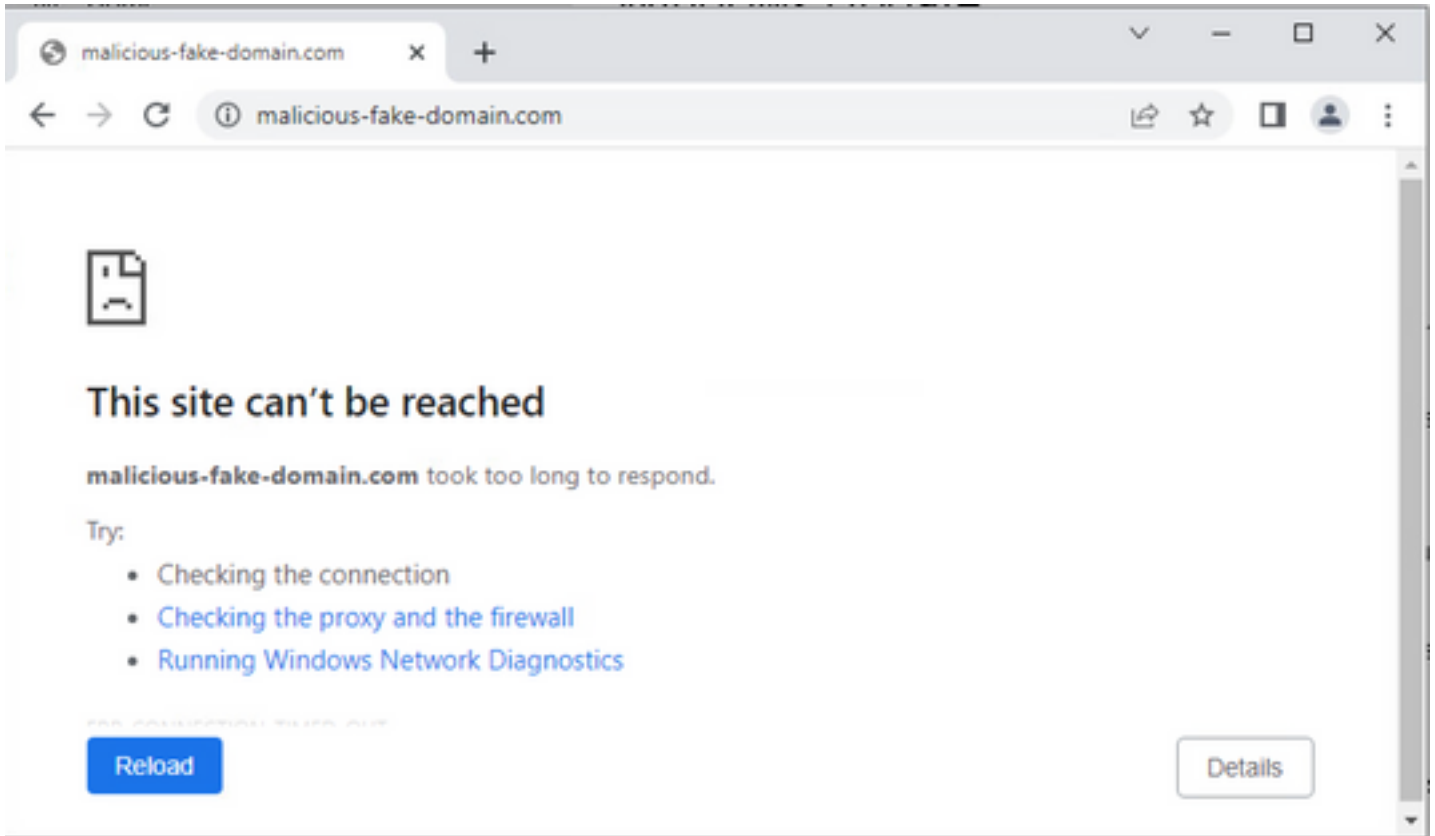
The screenshot shows the 'TID Detection' status panel. It indicates that the system is currently publishing TID observables to elements. Below the status message are two buttons: 'Pause' and 'Resume'.

**TID Detection**

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

## Verify

After the configuration is complete, endpoint tries to connect to the `https://malicious-fake-domain[.]com` URL which is hosted on the Outside zone but the connections fails as expected.



To verify if the connection failure is due the Threat Intelligence feed navigate to Integrations > Intelligence > Incidents. Blocked events must be listed on this page.

Firewall Management Center  
Integration / Intelligence / Incidents

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin

Last Updated: 6 hours 🔍 4 Incidents

Last Updated	Incident ID	Indicator Name	Type	Action Taken	Status
6 seconds ago	URL-20230131-4	malicious-fake-domain.com/	URL	Blocked	New
6 seconds ago	URL-20230131-3	malicious-fake-domain.com/	URL	Blocked	New
6 seconds ago	URL-20230131-1	malicious-fake-domain.com/	URL	Blocked	New
6 seconds ago	URL-20230131-2	malicious-fake-domain.com/	URL	Blocked	New

You can verify these block events under Analysis > Connections > Security-Related Events:

Firewall Management Center  
Analysis / Connections / Security-Related Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin

Bookmark This Page | Reporting | Dashboard | View Bookmarks

Security-Related Connection Events [\[watch workflow\]](#) II 2023-01-31 08:30:18 - 2023-01-31

No Search Constraints [\(Edit Search\)](#)

Security-Related Connections with Application Details Table View of Security-Related Connection Events

Jump to...

	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	Application Protocol	Client	Web Application	URL
▼	2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	31604 / tcp	443 (https) / tcp	HTTPS	SSL client		https://
▼	2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	24438 / tcp	443 (https) / tcp	HTTPS	SSL client		https://
▼	2023-01-31 09:24:03	2023-01-31 09:24:03	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	59088 / tcp	443 (https) / tcp	HTTPS	SSL client		https://
▼	2023-01-31 09:24:02	2023-01-31 09:24:03	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	59087 / tcp	443 (https) / tcp	HTTPS	SSL client		https://
▼	2023-01-31 09:18:33	2023-01-31 09:18:33	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	58956 / tcp	443 (https) / tcp	HTTPS	SSL client		https://
▼	2023-01-31 09:18:33	2023-01-31 09:18:33	Block	URL Block	10.5.5.5		10.31.124.250		TID URL Block	Inside	Outside	23474 / tcp	443 (https) / tcp	HTTPS	SSL client		https://

A FTD LINA capture allows to see the traffic from the endpoint to the malicious URL over the multiple check. Please, note that Snort Engine Phase 6 check gives back a drop result, since

Threat Intelligence feature use the snort engine for advanced traffic detection. Be aware, that Snort engine needs to allow the first couple of packets in order to analyze and understand the nature of the connection to correctly trigger a detection. Check Related Information section for more information about FTD LINA captures.

```
7: 18:28:46.965449 0050.56b3.fd77 0050.56b3.de22 0x0800 Length: 571
10.5.5.5.63666 > 10.31.124.250.443: P [tcp sum ok] 2993282128:2993282645(517) ack 2622728404 win
1024 (DF) (ttl 128, id 2336)
```

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Elapsed time: 1926 ns

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x14745cf3b800, priority=13, domain=capture, deny=false

hits=553, user\_data=0x14745cf4b800, cs\_id=0x0, l3\_type=0x0

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0000.0000.0000

input\_ifc=Inside, output\_ifc=any

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 1926 ns

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x14745c5c80, priority=1, domain=permit, deny=false

hits=7098895, user\_data=0x0, cs\_id=0x0, l3\_type=0x8

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0100.0000.0000

input\_ifc=Inside, output\_ifc=any

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Elapsed time: 3852 ns

Config:

Additional Information:

Found flow with id 67047, using existing flow

Module information for forward flow ...

snp\_fp\_inspect\_ip\_options

snp\_fp\_tcp\_normalizer

snp\_fp\_tcp\_proxy

snp\_fp\_snort

snp\_fp\_tcp\_proxy

snp\_fp\_translate

snp\_fp\_tcp\_normalizer

snp\_fp\_adjacency

snp\_fp\_fragment

snp\_ifc\_stat

Module information for reverse flow ...

snp\_fp\_inspect\_ip\_options

snp\_fp\_tcp\_normalizer

snp\_fp\_translate



```
snp_fp_tcp_proxy
snp_fp_snort
snp_fp_tcp_proxy
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat
```

```
Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 31244 ns
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 5
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 655704 ns
Config:
Additional Information:
service: HTTPS(1122), client: SSL client(1296), payload: (0), misc: (0)
```

```
Phase: 6
Type: SNORT
Subtype: SI-URL
Result: DROP
Elapsed time: 119238 ns
Config:
URL list id 1074790412
Additional Information:
Matched url malicious-fake-domain.com, action Block
```

```
Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
Action: drop
Time Taken: 813890 ns
Drop-reason: (si) Blocked or blacklisted by the SI preprocessor, Drop-location: frame
0x000056171ff3c0b0 flow (NA)/NA
```

## Troubleshoot

- To make Sure Threat Response keeps the feed up to date with the correct information you can navigate on your browser to the Feed URL and see the observables shared.



- For troubleshooting FMC Threat Intelligence Director please check the link on Related

Information.

## Related Information

- [Configure and Troubleshoot Cisco Threat Intelligence Director](#)
- [Configure Secure Firewall Threat Intelligence Director on FMC 7.3](#)
- [Use Firepower Threat Defense Captures and Packet Tracer](#)