

# Configurar feeds de resposta a ameaças do SecureX para bloquear URL no Firepower

## Contents

[Introduction](#)

[Informações de Apoio](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Criar feed de resposta a ameaças SecureX](#)

[Configurar o FMC Threat Intelligence Diretor para consumir o feed de resposta a ameaças](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como criar inteligência de ameaças a partir de URLs e IPs encontrados durante investigações de Resposta a ameaças a serem consumidos pelo Firepower.

## Informações de Apoio

O Cisco Threat Response é uma ferramenta poderosa capaz de investigar ameaças em todo o ambiente graças às informações de vários módulos. Cada módulo fornece as informações geradas por produtos de segurança como Firepower, Secure Endpoint, Umbrella e outros fornecedores. Essas investigações podem não apenas ajudar a revelar se existe uma ameaça no sistema, mas também a gerar informações importantes sobre ameaças, que podem ser fornecidas de volta ao produto de segurança para aumentar a segurança no ambiente.

Alguns termos importantes usados pelo SecureX Threat Response:

- **Indicador** é uma coleção de observáveis que estão logicamente relacionados com os operadores AND e OR. Existem Indicadores complexos que combinam múltiplos observáveis, além disso, há também indicadores simples que são feitos de apenas um observável.
- **Observável** é uma variável que pode ser um IP, Domínio, URL ou um sha256.
- **Os julgamentos** são criados pelo usuário e usados para vincular um item observável a uma disposição por um período de tempo específico.
- **Os feeds** são criados para compartilhar a inteligência de ameaças gerada pela investigação do SecureX Threat Response com outros produtos de segurança, como firewalls e filtros de conteúdo de e-mail, como Firepower e ESA.

# Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SecureX CTR (Cisco Threat Response).
- TID do Firepower ( Threat Intelligence Diretor ).
- Configuração das Políticas de controle de acesso do Firepower.

Este documento usa o TID do Firepower para aplicar a inteligência de ameaças gerada no SecureX Threat Response. Os requisitos para utilizar o TID na instalação do CVP, tal como para o CVP versão 7.3, são os seguintes:

- Versão 6.2.2 ou posterior.
- configurada com um mínimo de 15 GB de memória.
- configurado com o acesso à API REST habilitado. Consulte [Habilitar acesso à API REST no Guia de administração do Cisco Secure Firewall Management Center](#) .
- Você pode usar o FTD como um elemento do diretor de inteligência de ameaças se o dispositivo estiver na versão 6.2.2 ou superior.

**Observação:** este documento considera que o Threat Intelligence Diretor já está ativo no sistema. Para obter mais informações sobre a configuração inicial do TID e solução de problemas, verifique os links disponíveis na seção [Informações Relacionadas](#).

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Painel SecureX Cisco Threat Response
- FMC (Firewall Management Center) versão 7.3
- FTD (Firewall Threat Response) versão 7.2

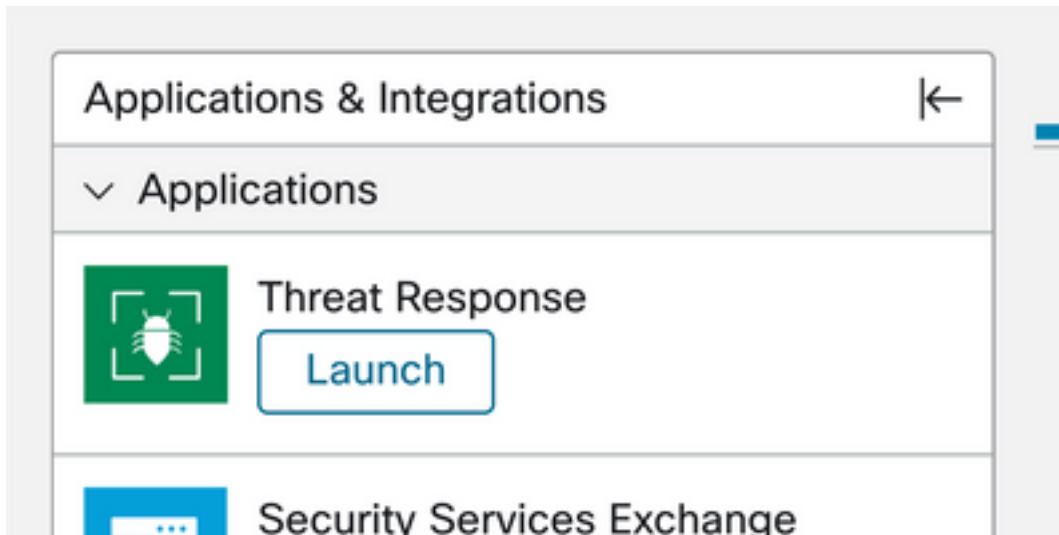
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

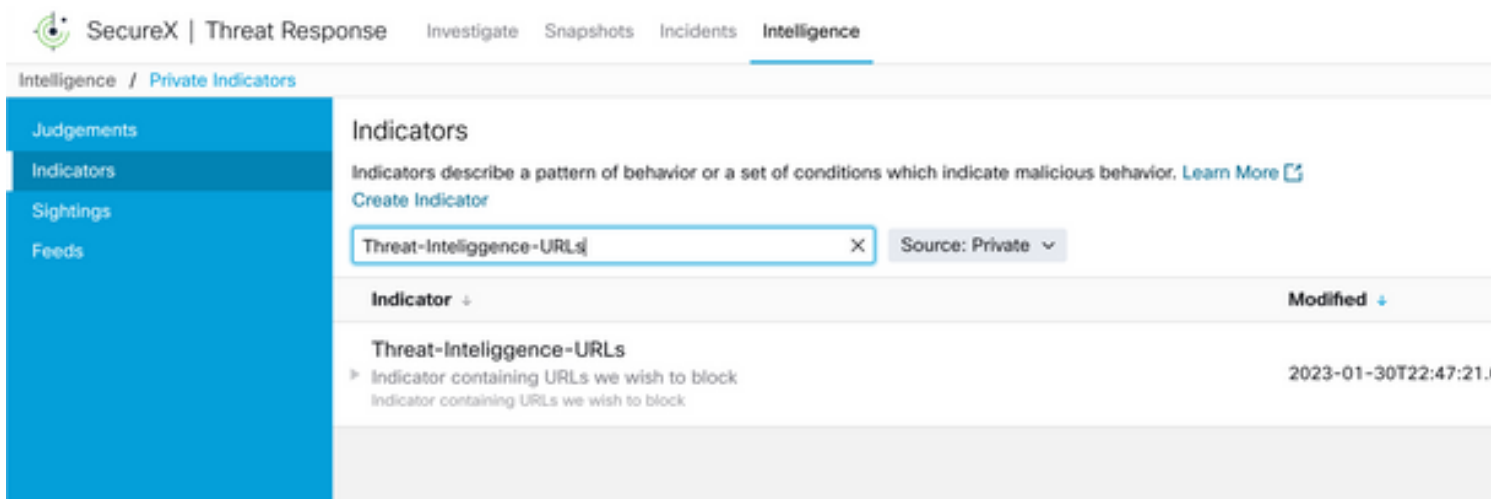
### Criar feed de resposta a ameaças SecureX

O SecureX Threat Response permite iniciar uma investigação no ambiente com uma entrada observável. O mecanismo de Resposta a Ameaças consulta os módulos para procurar qualquer atividade relacionada ao observável. A investigação retorna qualquer correspondência encontrada pelos módulos. Essas informações podem incluir IPs, domínios, URLs, e-mails ou arquivos. As próximas etapas criam um feed para consumir informações com outros produtos de segurança.

**Etapa 1** Efetue login no painel do SecureX e clique no botão **Launch** (Iniciar) para obter o Threat Response Module (Módulo de resposta a ameaças). Isso abre a página Resposta a ameaças em uma nova janela:



**Etapa 2** Na página Resposta a ameaças, clique em Inteligência > Indicadores e altere a lista suspensa de Origem de Pública para Privada. Isso deve permitir que você clique no link Criar Indicador. Uma vez dentro do assistente criador de indicador escolher qualquer título significativo e descrição para o seu Indicador, depois que marcar a caixa de verificação URL Watchlist. Neste momento você pode salvar o indicador, nenhuma informação adicional é necessária, no entanto, você pode optar por configurar o resto das opções disponíveis.



**Etapa 3** Navegue até a **guia Investigar** e cole qualquer item de observação que você gostaria de investigar na caixa de investigação. Para fins demonstrativos, o URL falso <https://malicious-fake-domain.com> foi usado para este exemplo de configuração. Clique em **Investigar** e aguarde a conclusão da investigação. Como esperado, a disposição da URL fictícia é desconhecida. Continue clicando com o botão direito do mouse na seta do lado de **Baixo** para expandir o menu contextual e clique em **Criar julgamento**.



**Etapa 4** Clique em **Link Indicators** e **selecione o indicador na etapa 2**. Selecione o descarte como **Mal-intencionado** e escolha o Dia de expiração conforme considerar apropriado. Finalmente, clique no botão **Create**. O URL deve estar visível agora em **Intelligence > Indicators > View Full Indicator**.

### Create Judgement ✕

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

Indicators\* ℹ

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;">🗑</span> <span style="color: red; font-size: 0.8em;">Malicious</span>	Domain	<span style="font-size: 0.8em;">2023-01-30T23:34:24.5...</span> <span style="font-size: 0.8em;">2023-03-02T23:34:24.5...</span>	

< >
5 per page
Showing 1-1 of 1

**ID** <https://private.intel.amp.cisco.com>

**Producer** Cisco - MSSP - Jobarrie

**Source** None Included

**Create Date** 2023-01-30T22:47:21.076Z

**Last Modified** 2023-01-30T22:47:21.055Z

**Expires** Indefinite

**Revisions** 1

**Confidence** High

**Severity** High

**TLP** Red

**Etapa 5** Navegue até **Intelligence > Feeds** e clique em **Create Feed URL (Criar URL do feed)**. Preencha o campo **Título** e **selecione** o **Indicador** criado na Etapa 2. Certifique-se de deixar a lista suspensa **Saída** como **observáveis** e clique em **Salvar**.

## 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

Etapa 6 Verifique se o feed foi criado em **Inteligência > Feeds** e clique em para expandir os detalhes do feed. Clique no **URL** para visualizar se os URLs esperados estão listados no 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

## Configurar o FMC Threat Intelligence Diretor para consumir o feed de resposta a ameaças

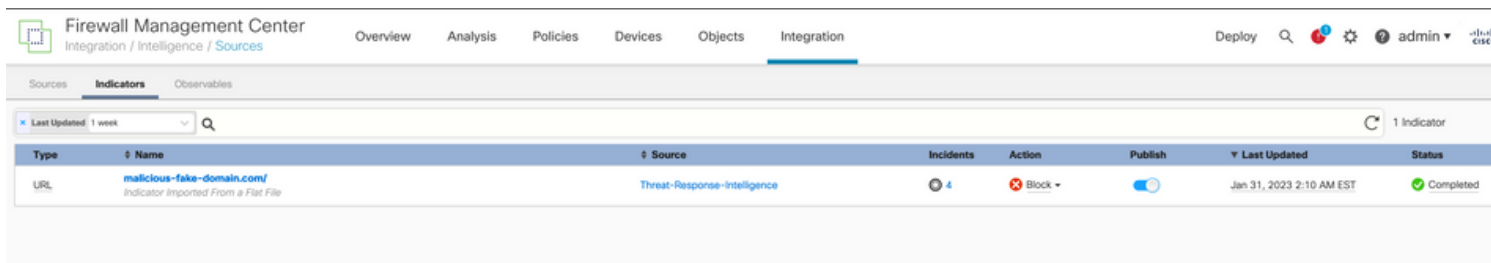
Etapa 1 Faça login no painel do FMC e navegue até **Integração > Inteligência > Fontes**. Clique no sinal de mais para adicionar uma nova Origem.

## Etapa 2 Crie a nova origem com estas configurações:

- Entrega > Selecionar URL
- 'Tipo' > 'Selecionar arquivo simples'
- Conteúdo > Selecionar URL
- Url > Cole o URL da seção "Create SecureX Threat Response Feed" (Criar feed de resposta a ameaças SecureX) etapa 5.
- Nome > Escolha qualquer nome que achar adequado
- Ação > Selecionar bloco
- Atualizar a cada > Selecione 30 min (para obter atualizações rápidas do feed Threat Intelligence)

Click **Save**.

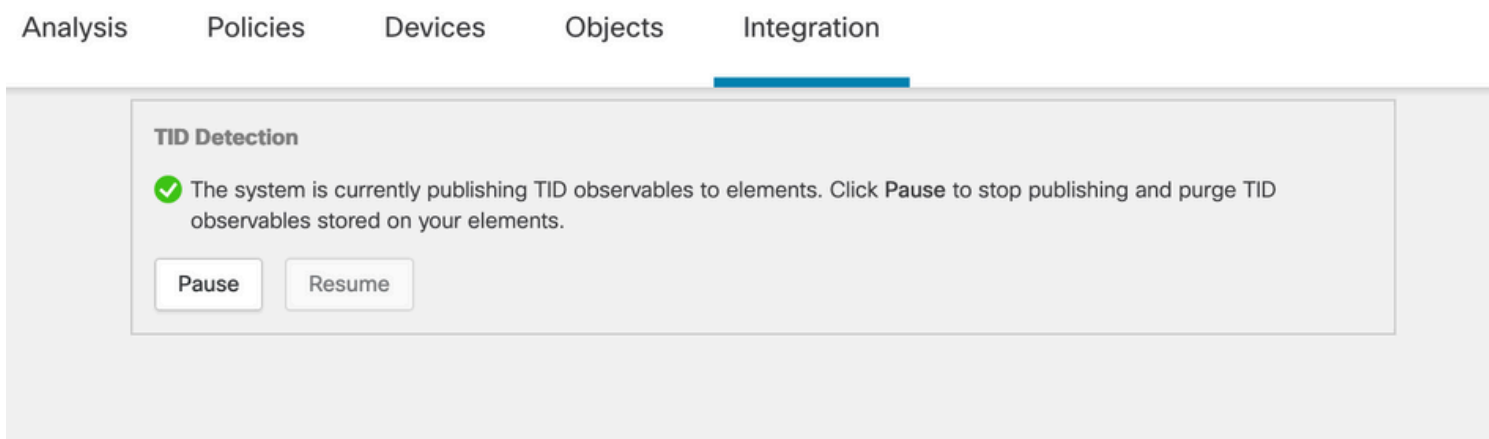
## Etapa 3 Em Indicadores e Observáveis, verifique se o domínio está listado:



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

## Etapa 4 Certifique-se de que o Threat Intelligence Diretor esteja Ativo e mantenha os elementos atualizados ( dispositivos FTDs ). Navegue até **Integrações > Inteligência > Elementos**:



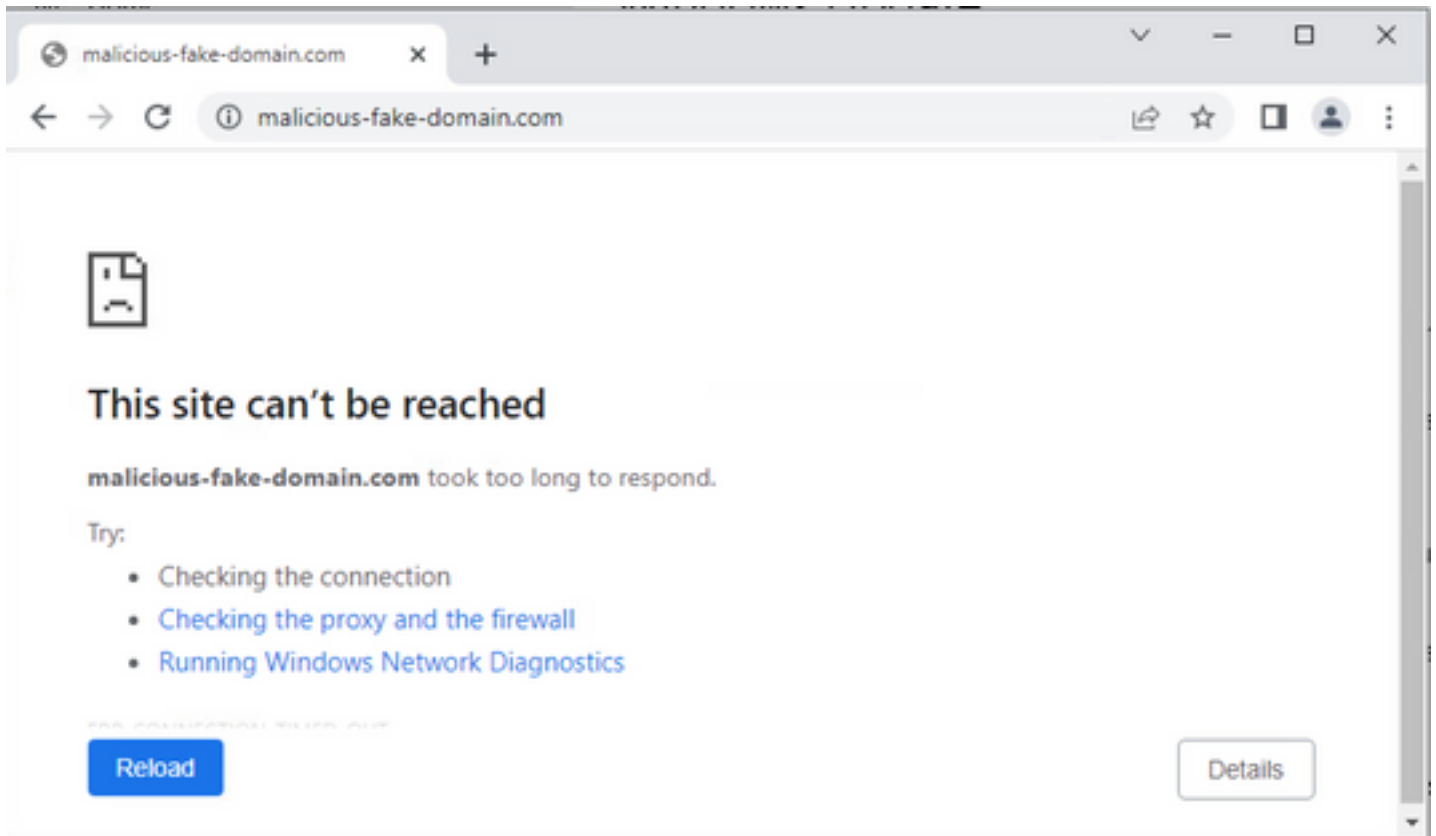
The screenshot shows the 'TID Detection' status page. It indicates that the system is currently publishing TID observables to elements. There are 'Pause' and 'Resume' buttons available.

**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

Após a conclusão da configuração, o endpoint tenta se conectar à URL [https://malicious-fake-domain\[.\]com](https://malicious-fake-domain[.]com) que está hospedada na zona externa, mas as conexões falham conforme esperado.



Para verificar se a falha de conexão ocorre devido ao feed Threat Intelligence, navegue para Integrations > Intelligence > Incident. Os eventos bloqueados devem ser listados nesta página.

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

Você pode verificar esses eventos de bloqueio em 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 Bookmark

Security-Related Connection Events [switch workflow](#) || 2023-01-31 08:30:18 - 2023-01-31 08:30:18

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://

Uma captura LINA de FTD permite ver o tráfego do endpoint para o URL mal-intencionado

através da verificação múltipla. Observe que a verificação da Fase 6 do Mecanismo de Snort retorna um resultado de queda, já que o recurso de Inteligência de ameaças usa o mecanismo de snort para detecção avançada de tráfego. Esteja ciente de que o mecanismo Snort precisa permitir o primeiro par de pacotes para analisar e entender a natureza da conexão para disparar corretamente uma detecção. Consulte a seção Informações Relacionadas para obter mais informações sobre capturas LINA FTD.

```
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=0x14745c5c5c80, 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

- Para garantir que o Threat Response mantenha o feed atualizado com as informações corretas, você pode navegar no navegador até a URL do feed e ver os itens de observação compartilhados.



- Para solucionar problemas do FMC Threat Intelligence Diretor, consulte o link em Informações relacionadas.

## Informações Relacionadas

- [Configurar e solucionar problemas do Cisco Threat Intelligence Diretor](#)
- [Configurar o Secure Firewall Threat Intelligence Diretor no FMC 7.3](#)
- [Use as capturas do Firepower Threat Defense e o Packet Tracer](#)

## 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.