

SecureX-respons configureren om URL op FirePOWER te blokkeren

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[SecureX-respons voor bedreigingen maken](#)

[Configuratie van de "Threat Intelligence Director" van het VCC voor gebruik van bedreigingsresponsfeed](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u bedreigingsinformatie kunt maken van URL's en IP's die worden gevonden tijdens Threat Response-onderzoeken die worden gebruikt door Firepower.

Achtergrondinformatie

Cisco Threat Response is een krachtig hulpmiddel dat in staat is bedreigingen in de hele omgeving te onderzoeken dankzij de informatie van meerdere modules. Elke module biedt de informatie die wordt gegenereerd door security producten zoals Firepower, Secure Endpoint, Umbrella en andere externe leveranciers. Deze onderzoeken kunnen niet alleen helpen om aan het licht te brengen of er een dreiging bestaat op het systeem, maar ook helpen om belangrijke informatie over bedreigingen te genereren, die kan worden teruggehaald naar het beveiligingsproduct om de veiligheid in het milieu te verbeteren.

Enkele belangrijke terminologie die wordt gebruikt door SecureX Threat Response:

- **Indicator** is een verzameling van waarneembare gegevens die logisch gerelateerd zijn aan EN en OR-operatoren. Er zijn complexe indicatoren die meerdere waarneembare punten combineren, daarnaast zijn er ook eenvoudige indicatoren die slechts van één waarneembaar zijn gemaakt.
- **Waarneembaar** is een variabele die een IP, Domain, URL of sha256 kan zijn.
- **Beslissingen** worden gemaakt door de gebruiker en gebruikt om een waarneembare te koppelen aan een regeling voor een bepaalde periode.
- **Feeds** worden gemaakt om de Threat Intelligence die door SecureX Threat Response-onderzoek wordt gegenereerd te delen met andere beveiligingsproducten zoals firewalls en e-mailinhoudsfilters zoals Firepower en ESA.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SecureX CTR (Cisco-bedreigingsrespons).
- Firepower TID (Threat Intelligence Director).
- Configuratie van FirePOWER Access Control Policy.

Dit document gebruikt Firepower TID om de Threat Intelligence af te dwingen die bij SecureX Threat Response is gegenereerd. De vereisten voor het gebruik van TID bij de inzet van uw FMC zoals voor FMC versie 7.3 zijn:

- Versie 6.2.2 of hoger.
- geconfigureerd met minimaal 15 GB geheugen.
- geconfigureerd met REST API-toegang ingeschakeld. Zie REST API-toegang inschakelen in de beheershandleiding van Cisco Secure Firewall Management Center.
- U kunt FTD gebruiken als bedreigingsintelligentie Director element als het apparaat zich op Versie 6.2.2 of hoger bevindt.

Opmerking: in dit document wordt ervan uitgegaan dat Threat Intelligence Director al actief is op het systeem. Voor meer informatie over TID initiële configuratie en probleemoplossing controleer de koppelingen die beschikbaar zijn in de sectie *Verwante informatie*.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

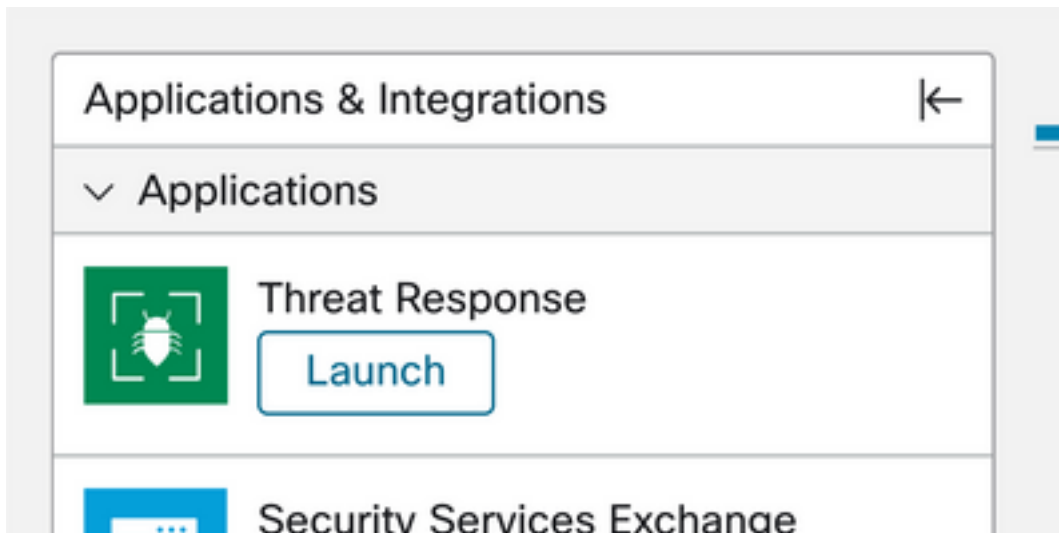
Configureren

SecureX-respons voor bedreigingen maken

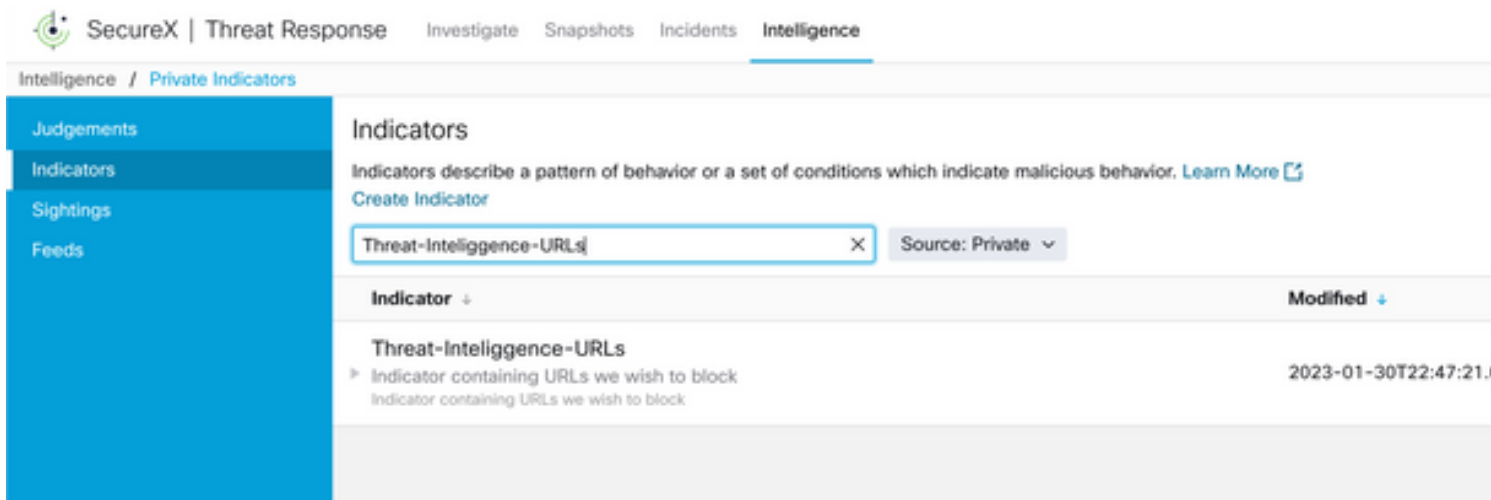
SecureX Threat Response maakt het mogelijk om een onderzoek naar de omgeving te starten met een waarneembare input. Threat Response-engine vraagt de modules om naar elke activiteit te zoeken die verband houdt met de waarneembare activiteit. Onderzoek retourneert elke overeenkomst gevonden door de modules, deze informatie kan IP's, domeinen, URL's e-mails of bestanden omvatten. Volgende stappen maken een feed om informatie te consumeren met andere Security producten.

Stap 1 Meld u aan bij uw SecureX-dashboard en klik op **Start** knop voor Threat Response Module.

Dit opent de pagina Threat Response in een nieuw venster:



Stap 2 Klik op de pagina Threat Response op Intelligence > Indicatoren en verander vervolgens de bronvervolgkeuzelijst van Public naar Private. Hiermee moet u op Indiciatielink maken kunnen klikken. Eenmaal binnen de Indicator creator wizard kiest elke betekenisvolle Titel en Beschrijving voor uw Indicator, na die controle van de URL Watchlist aanvinkvakje. Op dit moment kunt u de indicator opslaan, is er geen verdere informatie nodig, maar u kunt ervoor kiezen om de rest van de beschikbare opties te configureren.



Stap 3 Navigeer naar het tabblad **Onderzoek** en plak alle waarneembare die u wilt onderzoeken in het onderzoeksvak. Voor demonstratieve doeleinden wordt de nep-URL gebruikt `https://malicious-fake-domain.com` werd gebruikt voor dit configuratievoorbeeld. Klik op **Onderzoeken** en wacht tot het onderzoek is afgerond. Zoals verwacht is de dummy URL dispositie onbekend. Klik met de rechtermuisknop op de **pijl-omlaag** om het contextmenu uit te vouwen en klik op **Oordeel maken**.



Stap 4 Klik op **Link Indicators** en selecteer de indicator uit stap 2. Selecteer regeling als **boosaardig** en kies de Verloopdag zoals u geschikt acht. Klik tot slot op de knop **Maken**. De URL moet nu zichtbaar zijn onder **Intelligence > Indicatoren > Volledig indicatielampje bekijken**.

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	...
malicious-fake-domain.com Malicious	Domain	2023-01-30T23:34:24.5... 2023-03-02T23:34:24.5...	

< > 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

Stap 5 Navigeer naar **Intelligence > Feeds** en klik op **Voer URL's maken**. Vul het veld **Title in** en selecteer de indicator die in Stap 2 is gemaakt. Zorg ervoor dat de vervolgkeuzelijst **Uitvoer** als **waarneembaar** blijft en klik op **Opslaan**.

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

Stap 6 Controleer dat de feed is gemaakt onder **Intelligence > Feeds** en klik vervolgens om de feed details uit te vouwen. Klik op de **URL** om te visualiseren dat de verwachte URL's in de feed worden vermeld.

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

Configuratie van de "Threat Intelligence Director" van het VCC voor gebruik van bedreigingsresponsfeed

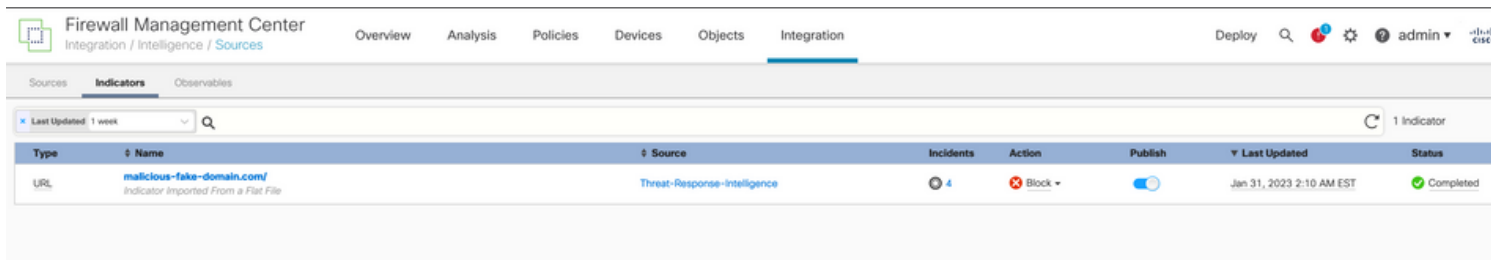
Stap 1 Meld u aan bij uw FMC-dashboard en navigeer naar **Integratie > Intelligence > Bronnen**. Klik op de **plus** zucht om een nieuwe bron toe te voegen.

Stap 2 Maak de nieuwe bron met deze instellingen:

- Levering > URL selecteren
- Type > Vlak bestand selecteren
- Content > URL selecteren
- URL > Plakt de URL uit de sectie "SecureX Threat Response Feed maken" stap 5.
- Naam > Kies een naam die u geschikt acht
- Actie > Blok selecteren
- Update Elke > Select 30 min (voor snelle updates voor Threat Intelligence feed)

Klik op **Save** (Opslaan).

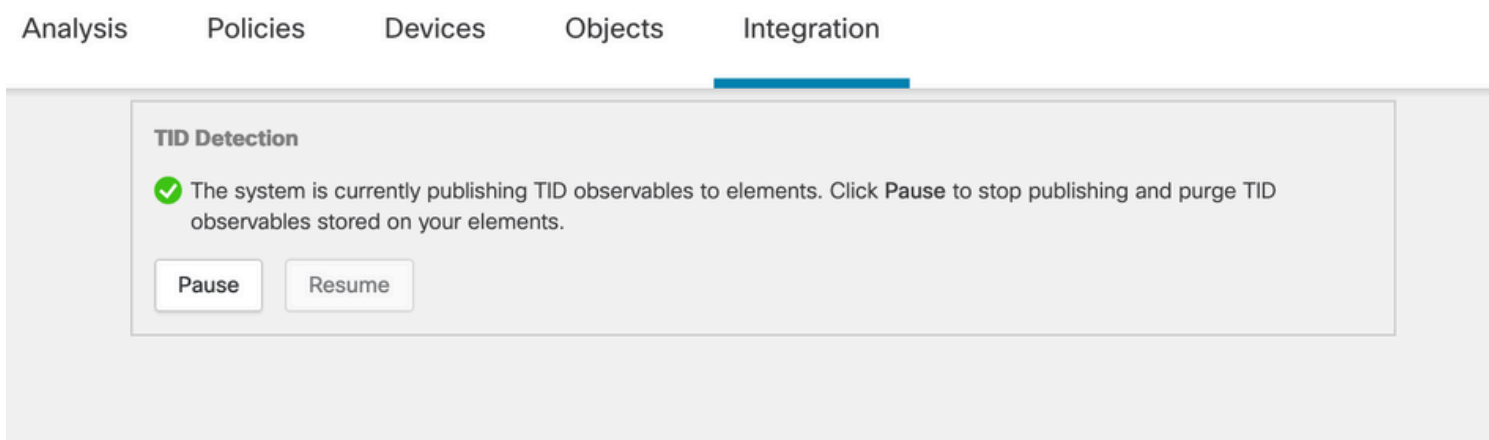
Stap 3 Onder Indicatoren en Waarnemingspunten verifieert domein is vermeld:



The screenshot shows the 'Firewall Management Center' interface. The navigation menu includes Overview, Analysis, Policies, Devices, Objects, and Integration. The 'Integration' tab is active, and the 'Indicators' sub-tab is selected. A table displays 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

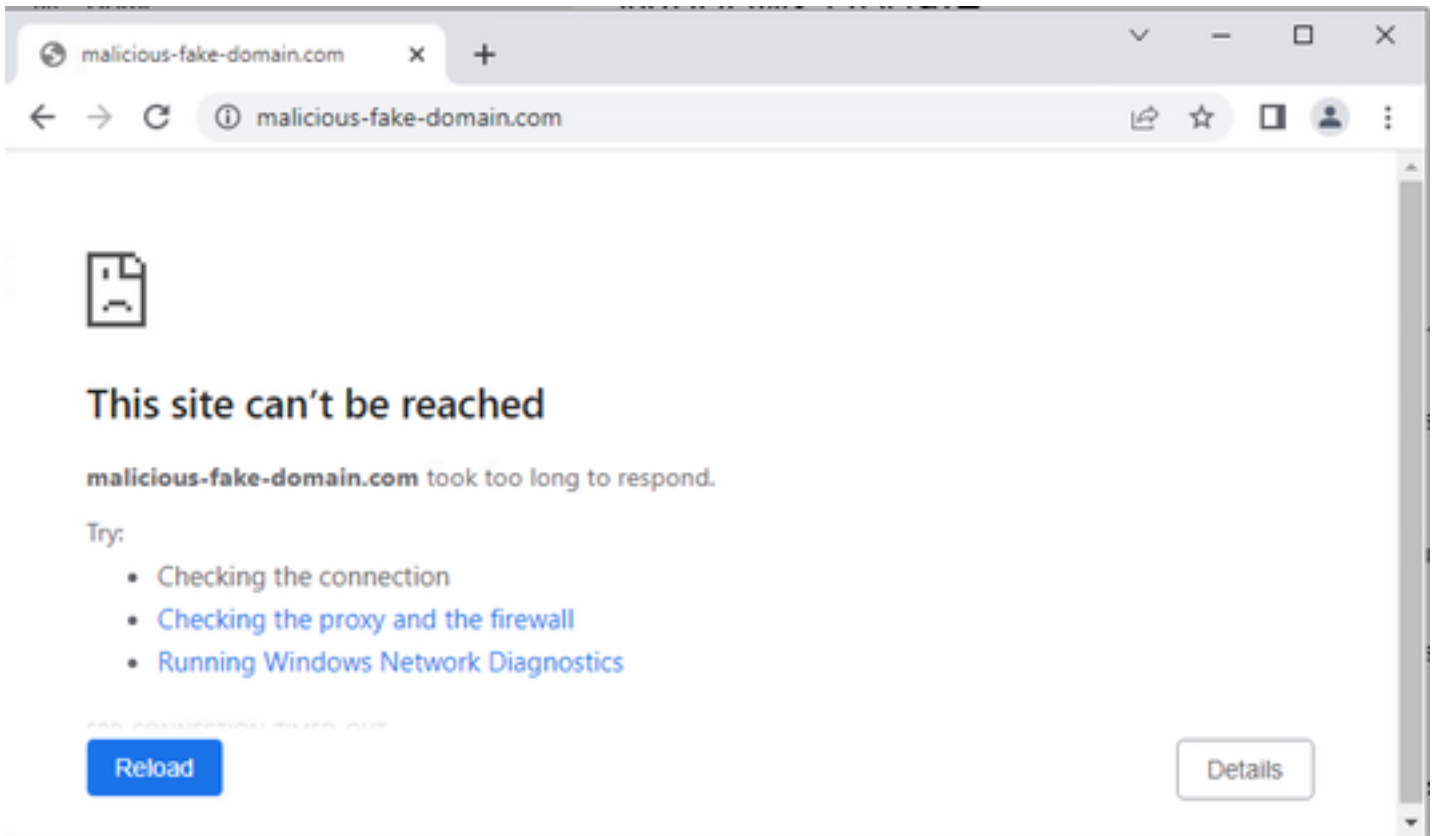
Stap 4 Zorg ervoor dat Threat Intelligence Director actief is en de onderdelen up-to-date houdt (FTDs-apparaten). Navigeren naar **integraties > Intelligence > Elementen**:



The screenshot shows the 'Integration' tab in the Firewall Management Center. A panel titled 'TID Detection' is displayed, indicating that the system is currently publishing TID observables to elements. The panel includes a green checkmark icon and the following text: "The system is currently publishing TID observables to elements. Click Pause to stop publishing and purge TID observables stored on your elements." Below the text are two buttons: 'Pause' and 'Resume'.

Verifiëren

Nadat de configuratie is voltooid, probeert endpoint verbinding te maken met de `https://malicious-fake-domain[.]com` URL die wordt gehost op de buitenzone, maar de verbindingen mislukken zoals verwacht.



Om te controleren of de verbinding is mislukt, kunt u in de Threat Intelligence-feed navigeren naar Integraties > Intelligence > Incidenten. Geblokkeerde gebeurtenissen moeten op deze pagina worden vermeld.

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

U kunt deze blokgebeurtenissen verifiëren onder Analyse > Verbindingen > Beveiligingsgerelateerde gebeurtenissen:

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 [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	31604 / tcp	443 (https) / tcp	HTTPS	SSL client		https://

Met een FTD LINA Capture kunt u het verkeer zien van het eindpunt naar de kwaadaardige URL via de meervoudige controle. Houd er rekening mee dat de controle van Snort Engine Phase 6 een valresultaat oplevert, omdat de functie Threat Intelligence de snortmotor gebruikt voor geavanceerde verkeersdetectie. Houd in acht dat Snort-engine het eerste paar pakketten moet toestaan om de aard van de verbinding te analyseren en te begrijpen om een detectie correct te starten. Kijk in het gedeelte Verwante informatie voor meer informatie over FTD LINA-opnamen.

```
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'
```

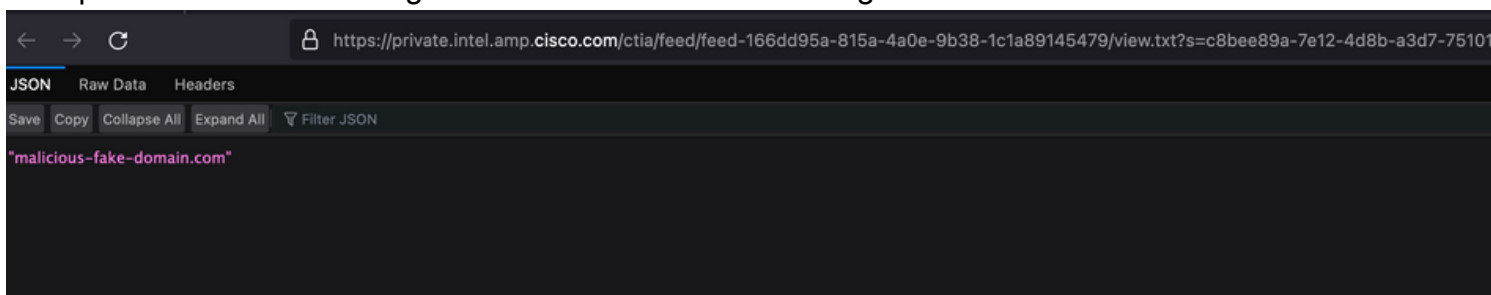
```
Phase: 5
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 655704 ns
Config:
Additional Information:
service: HTTPS(1122), client: SSL client(1296), payload: (0), misc: (0)
```

```
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
```

Problemen oplossen

- Om Sure Threat Response te maken houdt de feed up-to-date met de juiste informatie die u op uw browser kunt navigeren naar de Feed URL en de gedeelde observables.



- Voor problemen oplossen VCC Threat Intelligence Director raadpleegt u de link naar [Verwante informatie](#).

Gerelateerde informatie

- [Cisco Threat Intelligence Director configureren en probleemoplossing bieden](#)
- [Configureer Secure Firewall Threat Intelligence Director op FMC 7.3](#)
- [Gebruik Firepower Threat Defence Capture en Packet Tracer](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.