AppID vroege pakketdetectie configureren in Secure Firewall Threat Defence 7.4

Inhoud

Inleiding

Dit document beschrijft hoe u AppID vroege pakketdetectie in Cisco Secure Firewall 7.4 kunt configureren.

Achtergrond - Probleem (klantvereisten)

- Toepassingsdetectie door Deep Packet Inspection kan meer dan één pakket kosten om verkeer te identificeren.
- Soms, waar IP en/of de poort voor een toepassingsserver bekend is, kunt u vermijden inspecterend extra pakketten.

Nieuw

- Er is een nieuwe op Snort gebaseerde Lua AppID API gemaakt waarmee we een IP-adres, poort en protocol kunnen toewijzen aan de respectievelijke:
  - Toepassingsprotocol (serviceaanvraag)
  - Clienttoepassing (client toegepast) en
  - Web applicatie (payload toegepast).
- Op FMC kunnen aangepaste toepassingsdetectoren worden gemaakt met behulp van deze API voor toepassingsdetectie.
- Zodra deze detector is geactiveerd, zou deze nieuwe API ons in staat stellen om toepassingen te identificeren op het allereerste pakket in een sessie.

Overzicht van functies

- De API wordt geïdentificeerd als:
  - **addHostFirstPktApp** (protocol_appId, client_appId, payload_appId, IP-adres, poort, protocol, opnieuw inspecteren)

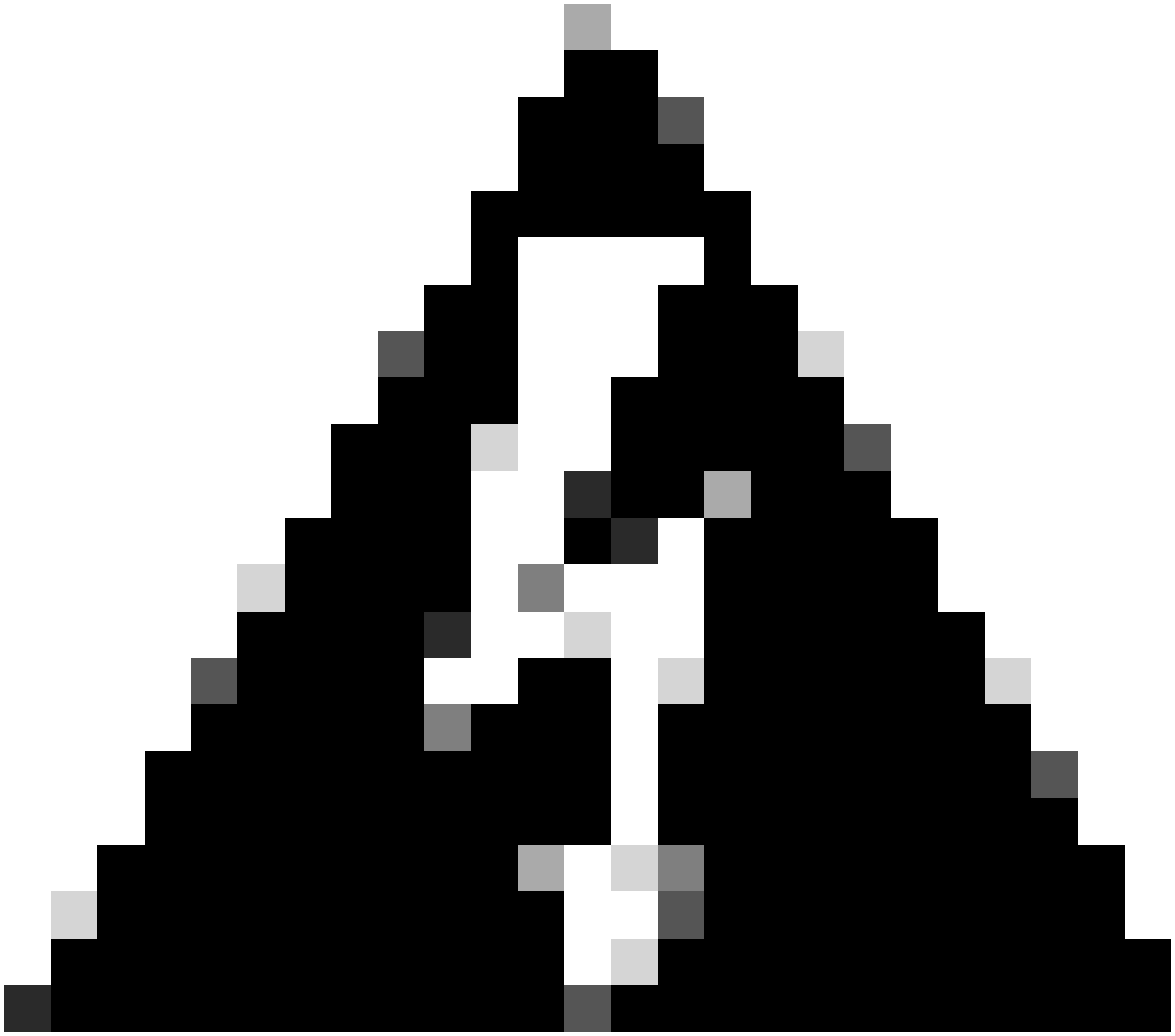
- Er wordt een cache-ingang gemaakt voor elke afbeelding die in de aangepaste app-detector wordt gemaakt.
- Het eerste pakket van alle inkomende sessies wordt geïnspecteerd om te zien of er een overeenkomst in de cache wordt gevonden.
- Zodra een overeenkomst is gevonden, wijzen we de bijbehorende appids toe voor de sessie en stopt het app-detectieproces.
- Gebruikers hebben de optie om verkeer opnieuw te inspecteren, zelfs nadat een overeenkomst is gevonden door de API.
- Het reinspect argument is een booleaanse waarde die aangeeft of de applicaties op het eerste pakket al dan niet opnieuw geïnspecteerd moeten worden.
- Wanneer herinspectie waar is, gaat de app-ontdekking door, zelfs als de API een overeenkomst vindt.
- In dit geval kunnen de applicaties die zijn toegewezen aan het eerste pakket, worden gewijzigd.

Voorwaarden, ondersteunde platforms, licentiëring

Minimale software- en hardwareplatforms

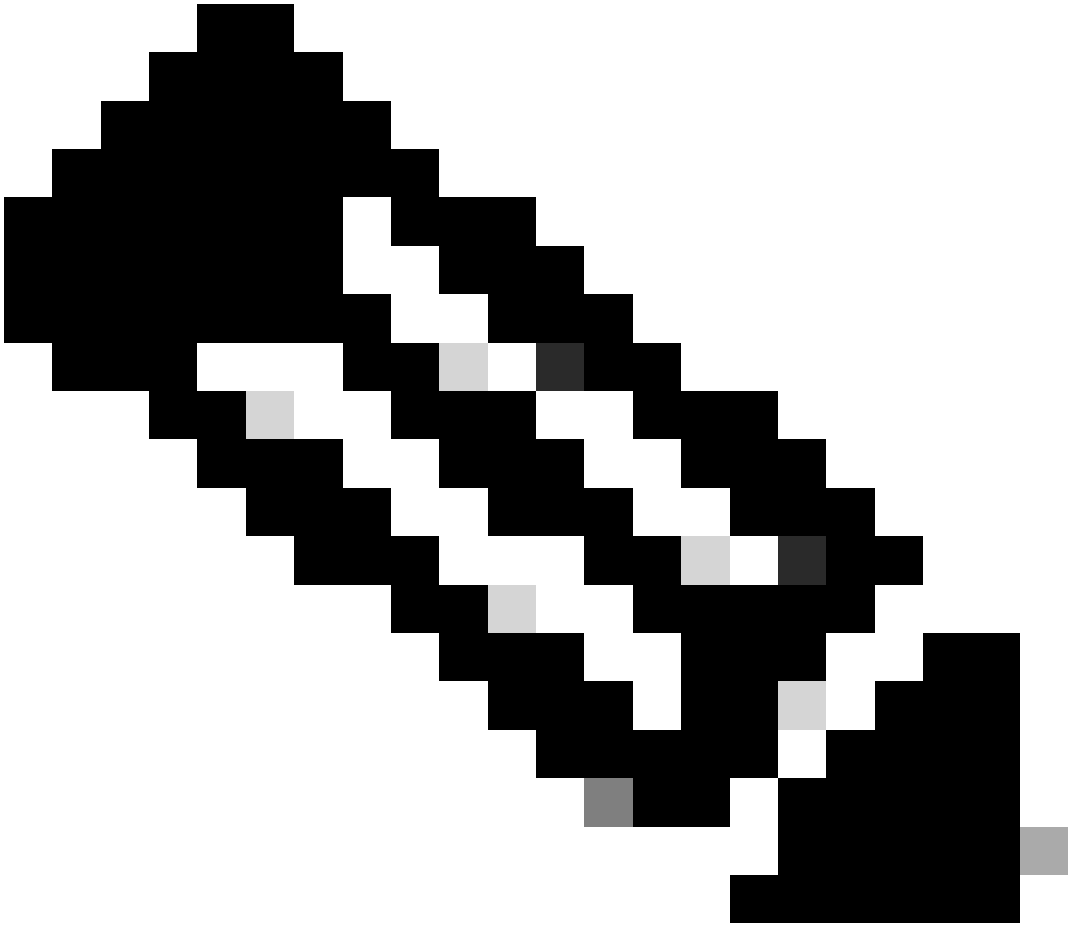
Toepassing en minimale versie	Ondersteunde beheerde platform(s) en versie	Manager(s)	Opmerkingen
Secure-firewall 7.4	Alle platforms die FTD 7.4	VCC on-premium + FTD	Dit is een apparaatzijdeeigenschap;

Snort3 gebruiken	ondersteunen		FTD moet op 7.4 zijn



Waarschuwing: snort 2 ondersteunt deze API niet.

Ondersteuning van snort 3, multi-instantie en HA/clustering



Opmerking: Vereist dat Snort 3 de detectiemotor is.

FTD	
Multi-instanties ondersteund?	Ja
Ondersteund met HA'd-apparaten	Ja
Ondersteund met geclusterde	Ja

apparaten?	

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:
· Cisco Firepower Threat Defense met 7.4 of hoger.

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.

Functiedetails

Functionele functiebeschrijving

Eerdere versies van deze release contrasteren

In Secure Firewall 7.3 en lager	Nieuw naar Secure Firewall 7.4
· Toepassingsdetectie voor een bekende combinatie van IP/poort/protocol was alleen beschikbaar als reserveoptie na uitputting van alle andere app detectiemechanismen. · De detectie van het eerste pakket in een sessie is niet ondersteund.	· De nieuwe lua detector API wordt beoordeeld vóór een ander app detectiemechanisme, · Zo in 7.4, steunen wij opsporing op het allereerste pakket in een zitting.

Hoe het werkt

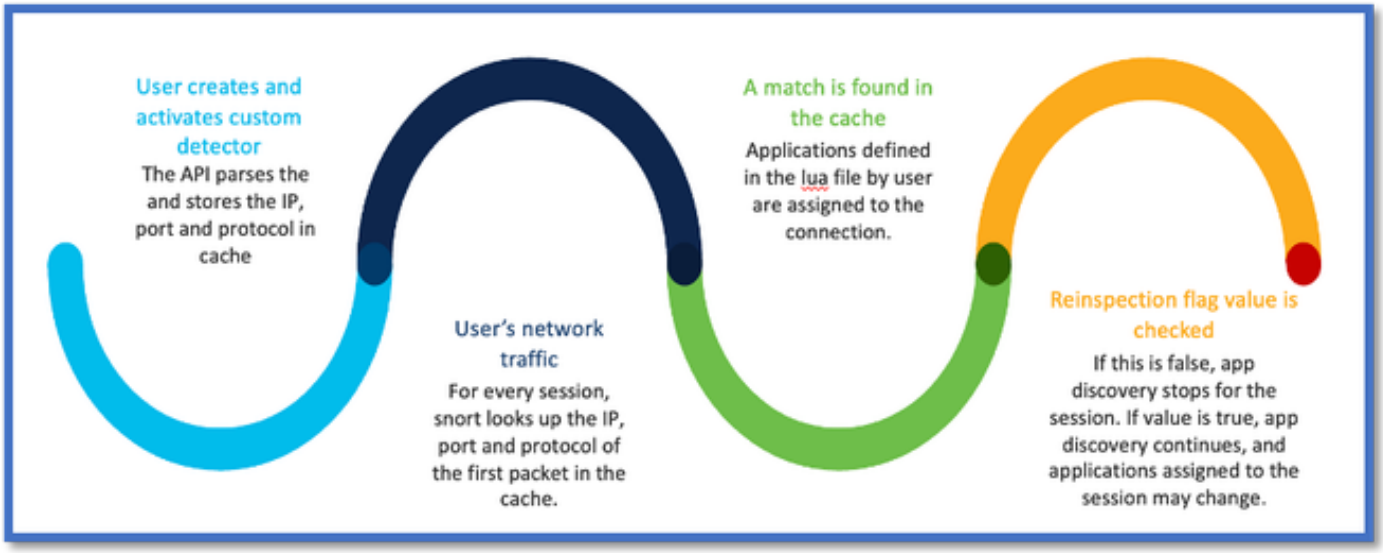
- Een lua-bestand maken: Zorg ervoor dat het bestand zich in de lua-sjabloon bevindt (geen syntaxisfouten). Controleer ook of de argumenten in het bestand juist zijn.

- Maak een nieuwe aangepaste detector: Maak een nieuwe aangepaste detector op FMC en upload uw lua-bestand erin. Activeer de detector.

- Run traffic: Verzend verkeer dat overeenkomt met de combinatie IP/poort/protocol die in de aangepaste app-detector is gedefinieerd.

- Controleer de verbindingsgebeurtenissen: controleer op FMC de verbindingsgebeurtenissen die door het IP en de poort zijn gefilterd. Door de gebruiker gedefinieerde toepassingen worden geïdentificeerd.

API-werkstroom voor vroege pakketdetectie van AppID



API Velden Beschrijving van Aangepaste Detector Voorbeeld

gDetector:addHostFirstPktApp

(gAppIDProto, gAppIDClient, gAppID, 0, "192.0.2.1", 443, DC.ipproto.tcp);

- De gemarkeerde argumenten zijn de door de gebruiker gedefinieerde waarden voor de reinspect-vlag, het IP-adres, de poort en het protocol.

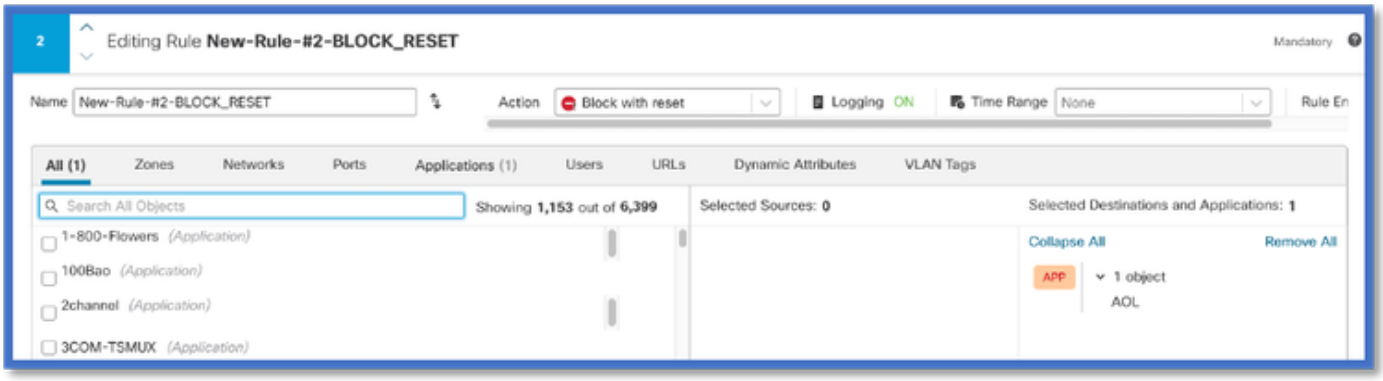
- 0 geeft een jokerteken aan.

Argumenten	Toelichting	Verwachte waarden
Vlag opnieuw inspecteren	Als een gebruiker liever het verkeer inspecteert dan firewallactie te ondernemen op basis van IP/Port/Protocol, kan hij de vlagwaarde opnieuw inspecteren op 1.	0 = opnieuw inspecteren uitgeschakeld of 1 = opnieuw inspecteren ingeschakeld
IP-adres	Doel-IP (één IP of bereik	192.168.4.198 OF

	van IP's in een subnetverbinding) van de server. Bestemming IP van het eerste pakket in een sessie.	192.168.4.198/24 OF 2a03:280:f103:83:face:b00c:0:25de OR 2a03:280:f103:83:face:b00c:0:25de/32
Port	Doelpoort van het 1e pakket in een sessie.	0 tot 65535
Protocol	Netwerkprotocol	TCP/UDP/ICMP

Use Case: Hoe blokkeer je het verkeer sneller

- Policy View: blokkeringsregel voor de toepassing "AOL".



- Het testen van verkeer met curl met: curl https://www.example.com v/s curl https://192.0.2.1/ (een van de IP-adressen van TEST)

<#root>

```
> curl https://www.example.com/
```

```
curl: (35) OpenSSL SSL_connect: SSL_ERROR_SYSCALL in connection to www.example.com:443
```

```
> curl https://192.0.2.1/
```

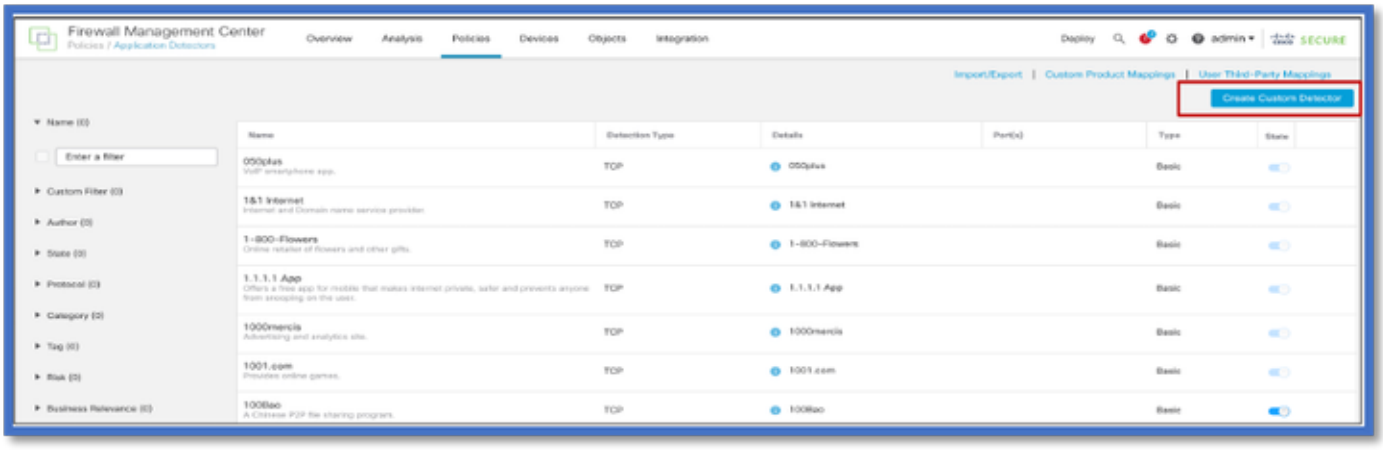
```
curl: (7) Failed to connect to 192.0.2.1 port 443: Connection refused
```

Walkthrough voor Firewall Management Center

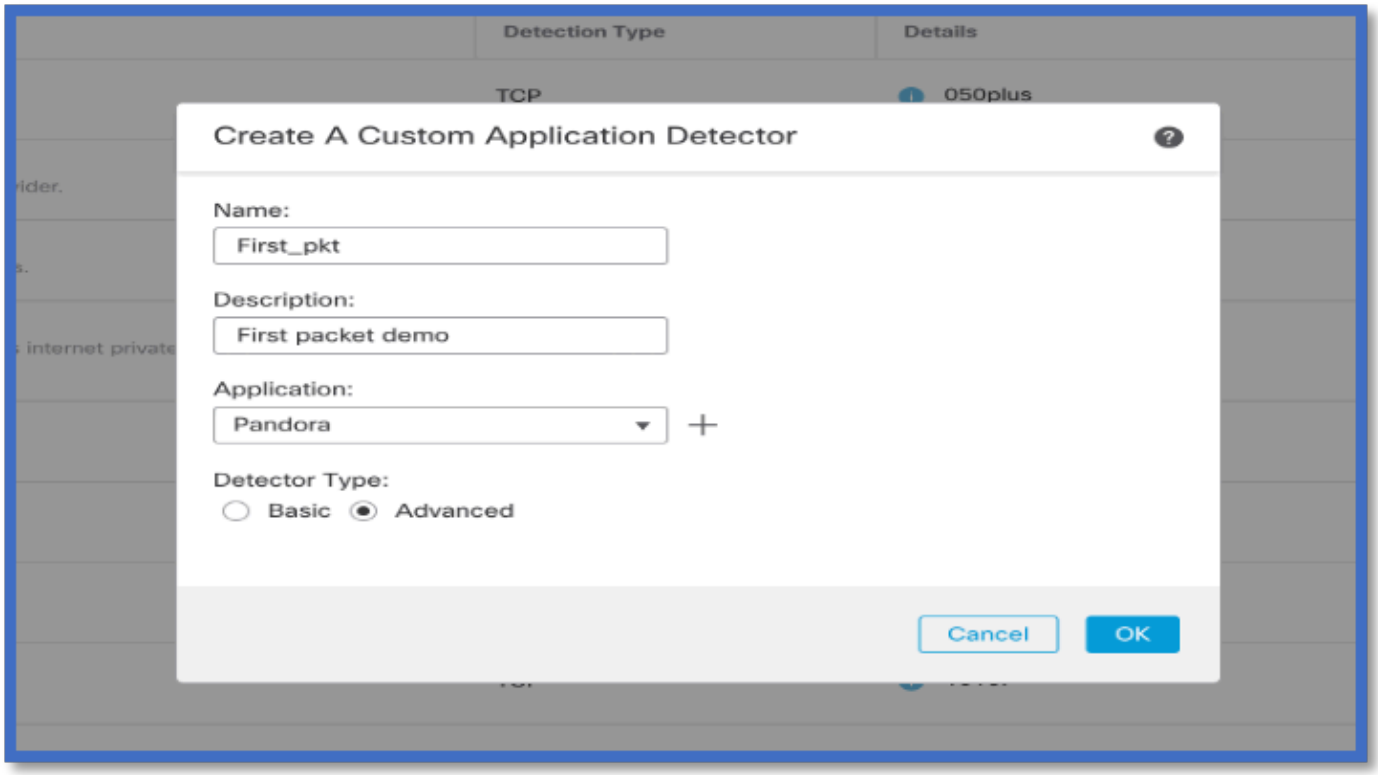
Stappen voor het maken van een aangepaste detectie met behulp van de API

Maak een nieuwe aangepaste detector aan op het VCC vanaf:

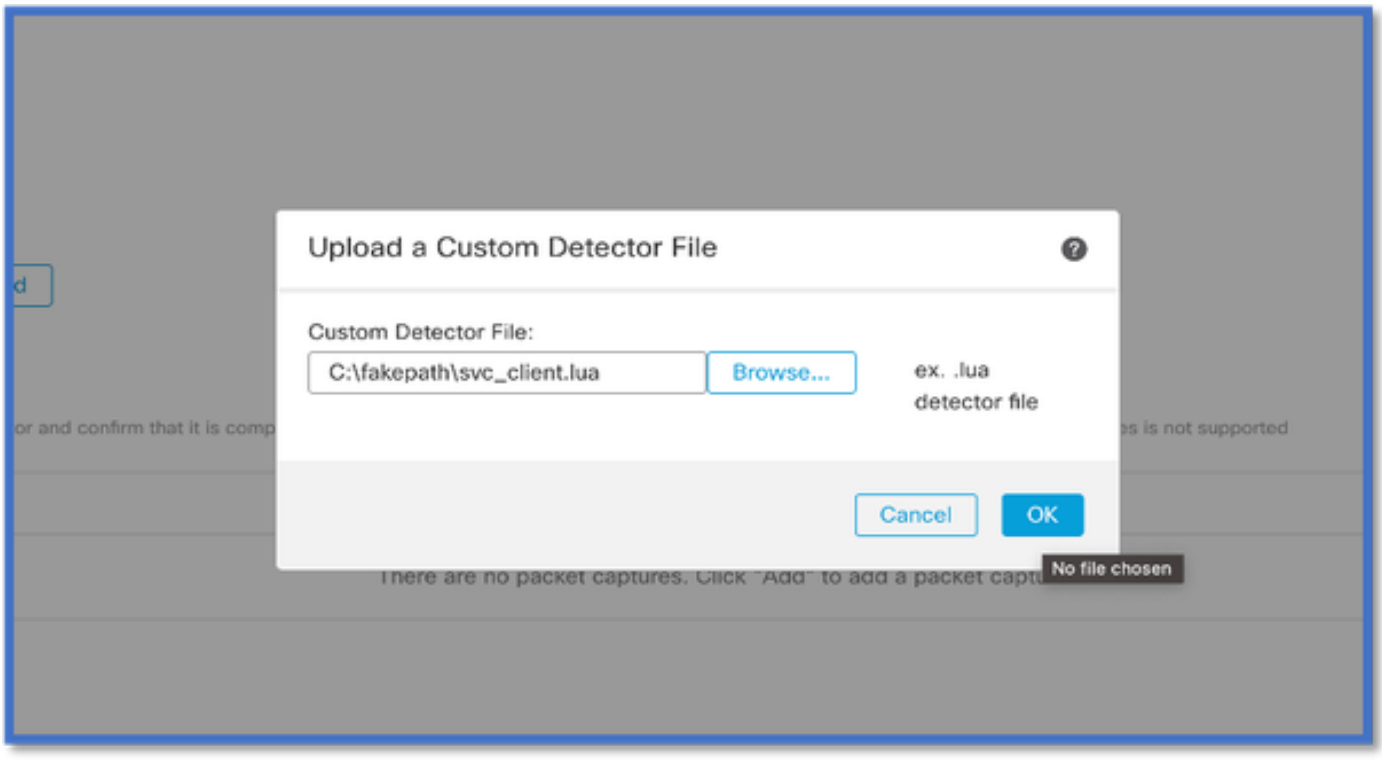
- Policies > Application Detectors > Create Custom Detector .



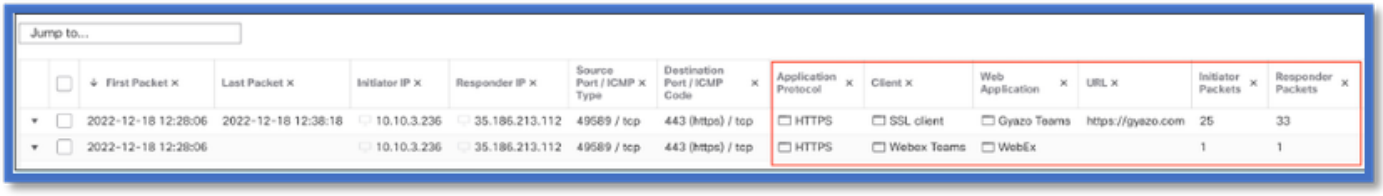
- Definieer naam en beschrijving.
    - Kies de toepassing in het keuzemenu.
    - Selecteer het type geavanceerde detector.



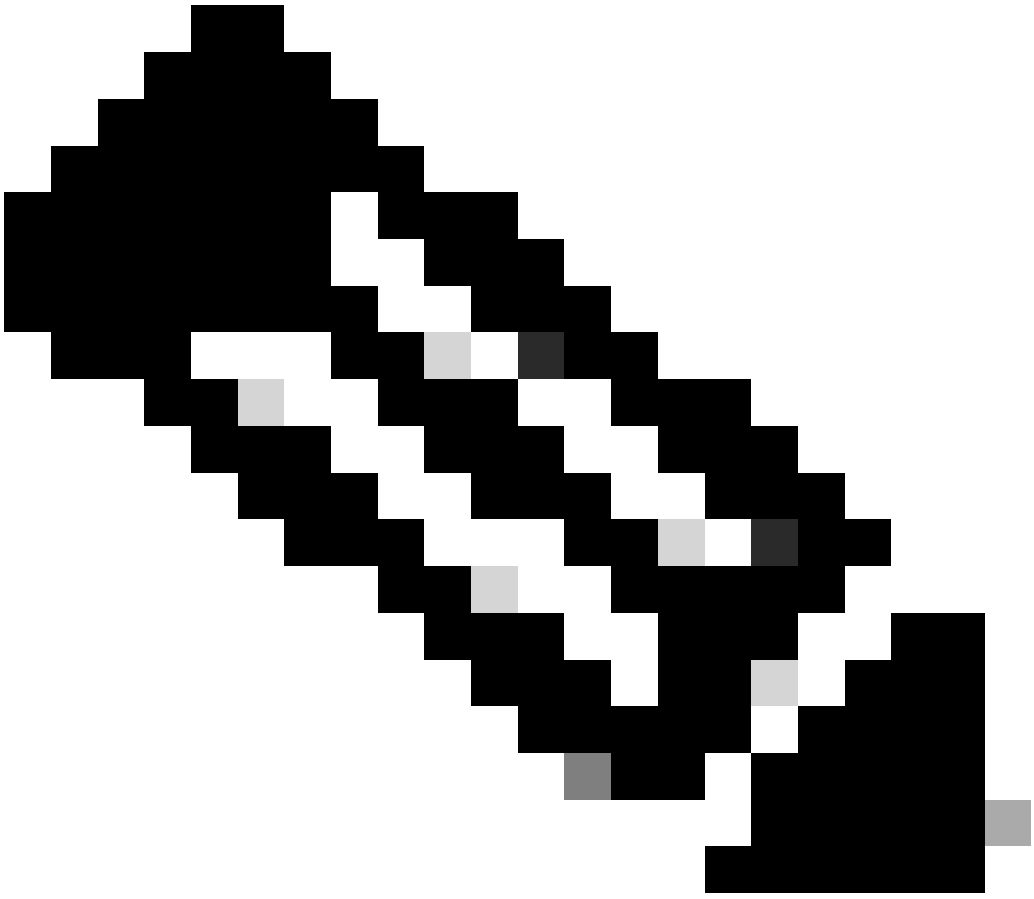
- Upload het Lua-bestand onder Detectiecriteria. Sla de detector op en activeer deze.



Uitgeschakeld v/s opnieuw inspecteren



- De twee gebeurtenissen tonen het begin van de verbinding v/s het einde van de verbinding wanneer herinspectie is ingeschakeld.



Opmerking:

1. Aan het begin van de verbinding worden "HTTPS-, Webex- en Webex Teams" geïdentificeerd door de API. Aangezien herinspectie waar is, wordt de app-detectie voortgezet en worden appIds bijgewerkt naar ‘HTTPS, SSL-client en Gyazo Teams’.

2. Merk het aantal initiator- en antwoordpakketten op. Reguliere app detectiemethoden vereisen veel meer pakketten dan de API.

Problemen oplossen/diagnostiek

Overzicht van diagnoses

- Nieuwe logbestanden worden toegevoegd in de identificatie van de systeemondersteuningstoepassing om aan te geven of er toepassingen zijn gevonden met de 1e API voor pakketdetectie.
- De logboeken tonen ook als de gebruiker herinspectie van verkeer koos.
- De inhoud van het door de gebruiker geüploade lua-detectorbestand staat op de FTD onder /var/sf/appid/custom/lua/<UUID> .
- Eventuele fouten in het lua-bestand worden op het moment dat de detector wordt geactiveerd in het FTD-bestand /var/log/message-bestand gedumpt.

CLI: applicatie-identificatie-debug voor systeemondersteuning

<#root>

192.0.2.1 443 -> 192.168.1.16 51251 6 AS=4 ID=0 New AppId session

192.0.2.1 443 -> 192.168.1.16 51251 6 AS=4 ID=0 Host cache match found on first packet, service: HTTPS(1

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 app event with client changed, service changed, payload
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 New firewall session

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 Starting with minimum 2, 'New-Rule-#1-MONITOR', and Src
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 match rule order 2, 'New-Rule-#1-MONITOR', action Audit
```

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 match rule order 3, 'New-Rule-#2-BLOCK_RESET', action Re

```
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 MidRecovery data sent for rule id: 268437504, rule_acti
192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 Generating an SOF event with rule_id = 268437504 ruleAc
```

192.168.1.16 51251 -> 192.0.2.1 443 6 AS=4 ID=0 reset action

192.0.2.1 443 > 192.168.1.16 51251 6 AS-4 ID=0 New AppId session
192.0.2.1 443 > 192.168.1.16 51251 6 AS=4 ID=0 Host cache match found on first packet, service:
HTTPS (1122), client: AOL(1419), payload: AOL (1419), reinspect: False
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 app event with client changed, service changed, payload changed, referred no change, miss no change, Mad no change, fas host no change, bits 0x1D 192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 New firewall session
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 Starting with minimum 2, 'New-Rule-#1-MONITOR', and Saclone first with zones 1 →> 1, geo 0(xff0) →> 0, yan 0, sae, sgt; 0, sag sat, type: unknown, det sat: 0, det sat type: unknown, sve 1122, payload 1419, client 1419, mise 0, user 9999997, no Mad or host, no xff
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 match rule order 2, 'New-Rule-#1-MONITOR', action Audit
192.168.1.16 51251 > 192.0.2.1 443 6 AS=4 ID=0 match rule order 3, 'New-Rule-#2-BLOCK_
_RESET', action
Reset
192.168.1.16 51251 > 192.0.2.1 443 6 AS-4 ID=0 MidRecovery, data sent for rule id: 268437504, rule_action:5, rev id:3558448739, Eule_match flag:0x1
192.168.1.16 51251 > 192.0.2.1 443 6 AS-4 ID-0 Generating an SOF event with zuleid - 268437504
ruleAction = 5 ruleReason = 0

Locatie van AppID Lua Detectors Content

Om te bevestigen of de Lua Detector met deze nieuwe API bestaat op het apparaat/FTD kunt u kijken of de addHostFirstApp API wordt gebruikt in de 2 applicatiedetectormappen:

1. VDB AppID-detectoren -/var/sf/appid/odp/lua

2. Aangepaste detectoren -/var/sf/appid/custom/lua

Bijvoorbeeld:grep addHostFirstPktApp * in elke map.

Problemen met voorbeeld:

- Probleem: Aangepaste Lua-detector niet geactiveerd op FMC.

Te controleren locatie: /var/sf/appid/custom/lua/

Verwacht resultaat: er moet hier één bestand bestaan voor elke op het VCC geactiveerde aangepaste app-detector. Controleer of de inhoud overeenkomt met het geüploade bestand.

- Probleem: Het geüploade LoA-detectorbestand bevat fouten.

Te controleren bestand: /var/log/messages on FTD

Foutenlogboek:

<#root>

Dec 18 14:17:49 intel-x86-64 SF-IMS[15741]:

Error - appid: can not set env of Lua detector /ngfw/var/sf/appid/custom/lua/6698fbd6-7ede-11ed-972c-d12

Stappen voor probleemoplossing

Probleem: toepassingen niet correct geïdentificeerd voor verkeer dat naar het door de gebruiker gedefinieerde IP-adres en poort gaat.

Stappen voor probleemoplossing:

- Controleer of de lua-detector juist is gedefinieerd en op de FTD is geactiveerd.
    - Controleer de inhoud van het lua-bestand op de FTD en controleer of er bij het activeren geen fouten worden gezien.
- Controleer de bestemming IP, poort en protocol van het eerste pakket in de verkeerssessie.
    - Het kan overeenkomen met de waarden die in de lua-detector zijn gedefinieerd.
- Controleer of de systeem-ondersteuning-toepassing-identificatie-debug.
    - Zoek de regel Host cache match found on first packet. Als die ontbreekt, geeft het aan dat de API geen overeenkomst heeft gevonden.

Beperkingen Details, algemene problemen en werkbalken

In 7.4 is er geen gebruikersinterface om de API te gebruiken. UI-ondersteuning zou worden toegevoegd in toekomstige releases.

Revisiegeschiedenis

Herziening	Publicatiedatum	Opmerkingen

1.0	18 jul.-2024	Eerste vrijgave

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.