Firepower Data Path Problemen opsporen en verhelpen fase 7: Inbraakbeleid

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Probleemoplossing voor de inbraakbeleidsfase](#)
[Gebruik van het "overtrek"-gereedschap om inbraakbeleidsdruppels te detecteren (alleen FTD)](#)
[Op onderdrukking in het inbraakbeleid controleren](#)
[Een gericht inbraakbeleid maken](#)
[Onjuist positieve probleemoplossing](#)
[Waar positief voorbeeld](#)
[Gegevens om te leveren aan TAC](#)
[Volgende stappen](#)

Inleiding

Dit artikel maakt deel uit van een reeks artikelen waarin wordt uitgelegd hoe u het gegevenspad op FirePOWER-systemen systematisch moet oplossen om te bepalen of onderdelen van Firepower invloed kunnen hebben op het verkeer. Raadpleeg het gedeelte Overzicht voor informatie over de architectuur van FirePOWER-platforms en de koppelingen naar de andere artikelen voor probleemoplossing in datacenters.

Dit artikel bestrijkt de zevende fase van de probleemoplossing bij het gebruik van FirePOWER-gegevens, de optie Inbraakbeleid.

Voorwaarden

- Dit artikel is van toepassing op alle FirePOWER-platforms die een inbraakbeleid voeren De spoorfunctie is alleen beschikbaar in versie 6.2 en hoger voor het Firepower Threat Defense (FTD) platform
- Kennis van opensource is behulpzaam, maar niet nodig Kijk op https://www.snort.org/ voor meer informatie over open source snort.

Probleemoplossing voor de inbraakbeleidsfase

Gebruik van het "overtrek"-gereedschap om inbraakbeleidsdruppels te detecteren (alleen FTD)

U kunt het traceringstool voor systeemondersteuning gebruiken vanuit de FTD Opdracht Line Interface (CLI). Dit is vergelijkbaar met het **firewall-motor-debug** gereedschap dat in het artikel van de toegangscontroleleidingsfase is vermeld, behalve dat het dieper ingaat op de innerlijke werking van de snort. Dit kan nuttig zijn om te zien of om het even welke regels van het Inbraakbeleid op

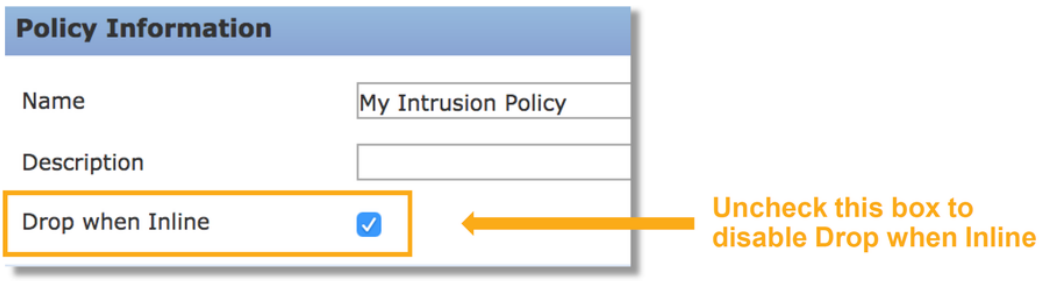
het interessante verkeer van start gaan.

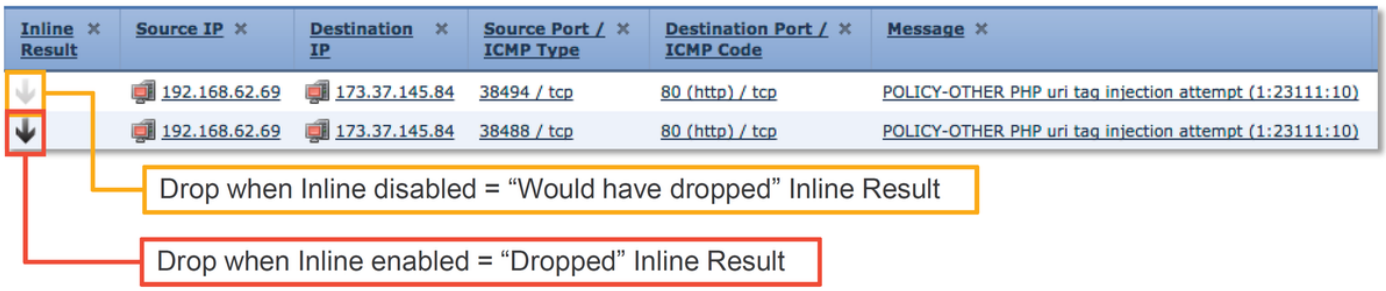
In het onderstaande voorbeeld wordt het verkeer van de host met IP-adres 192.168.62.6 geblokkeerd door een inbraakbeleidsregel (in dit geval **1:2311**)

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
...
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

Merk op dat de actie die door snort werd toegepast, **was gedaald**. Wanneer een druppel door de slang wordt gedetecteerd, wordt die specifieke sessie vervolgens in een zwarte lijst geplaatst, zodat ook extra pakketten worden verzonden.

De reden waarom snort de droogeactie kan uitvoeren is dat de "Drop Wanneer inline" optie binnen het Inbraakbeleid is ingeschakeld. Dit kan worden geverifieerd op de eerste landingspagina binnen het Inbraakbeleid. In het FireSIGHT Management Center (FMC), navigeer naar **Beleid > Toegangsbeheer > Inbraakcontrole** en klik op het pictogram naast het beleid in kwestie.





Als "Drop Wanneer inline" is uitgeschakeld, stopt u niet langer offensieve pakketten, maar waarschuwt u toch met een **inline resultaat** van "zou zijn gevallen" in de inbraakgebeurtenissen.

Met "Drop Wanneer inline" uitgeschakeld, toont de sporenuitvoer een actie voor de betreffende

verkeerssessie **zou** vallen.

```
> system support trace


Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
…
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

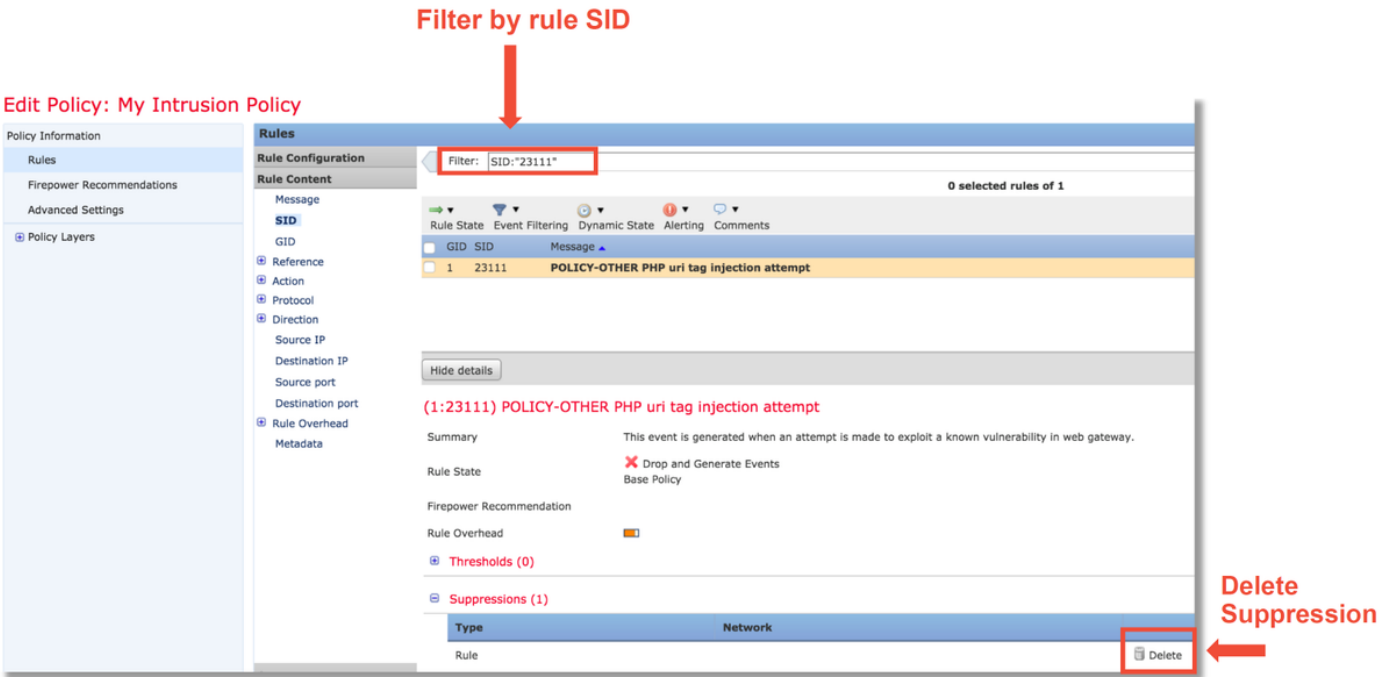
Op onderdrukking in het inbraakbeleid controleren

Het is mogelijk om het verkeer te laten vallen zonder inbraakgebeurtenissen naar de FMC te sturen (in stilte druppelen). Dit wordt bereikt door **indrukken** te configureren**.** Om te controleren of een suppressie is ingesteld in een Inbraakbeleid, kan de shell van de deskundige op de achterkant worden gecontroleerd, zoals hieronder wordt weergegeven.

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*/
$ grep -H '^suppress' intrusion/*/snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name       : My Intrusion Policy
```

Merk op dat het Inbraakbeleid dat "Mijn inbraakbeleid" heet een onderdrukking bevat voor de 1:2311-regel. Daarom kan het verkeer op grond van deze regel zonder gebeurtenissen worden teruggebracht. Dit is een andere reden waarom de sporenvoorziening behulpzaam kan zijn, omdat het nog steeds de druppels toont die plaatsvinden.

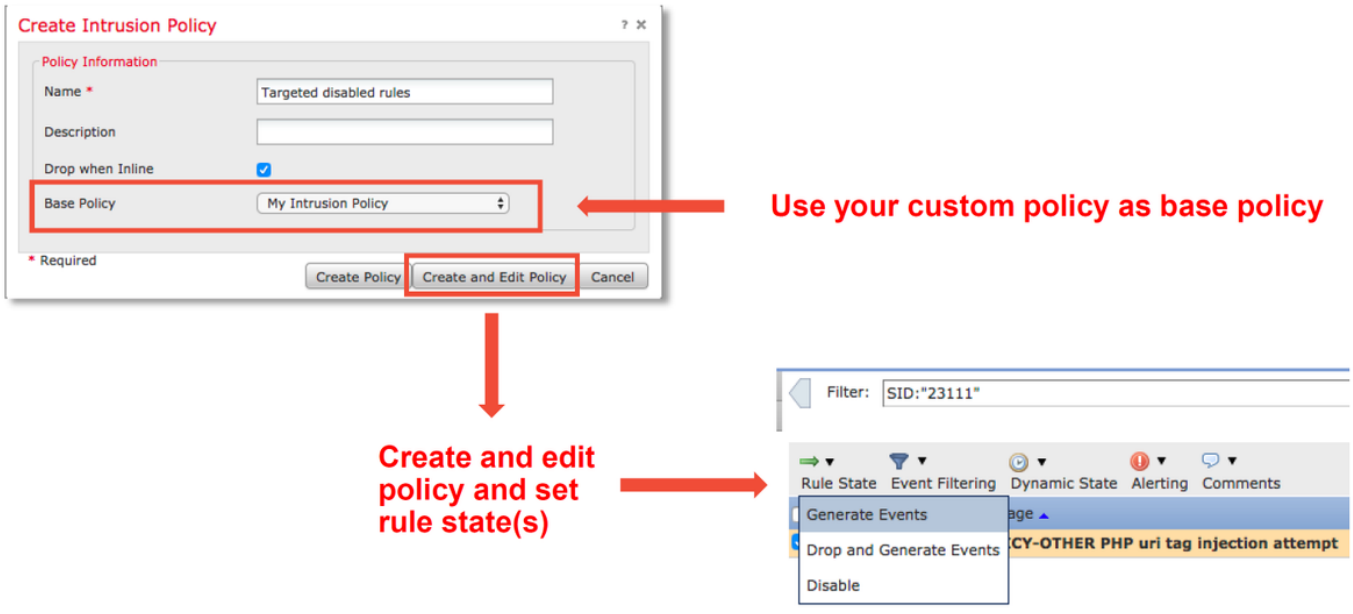
Om de onderdrukking te verwijderen kan de betreffende regel binnen de weergave **Inbraakbeleid** worden gefilterd. Dit brengt een optie op om de suppressie te verwijderen, zoals hieronder wordt getoond.



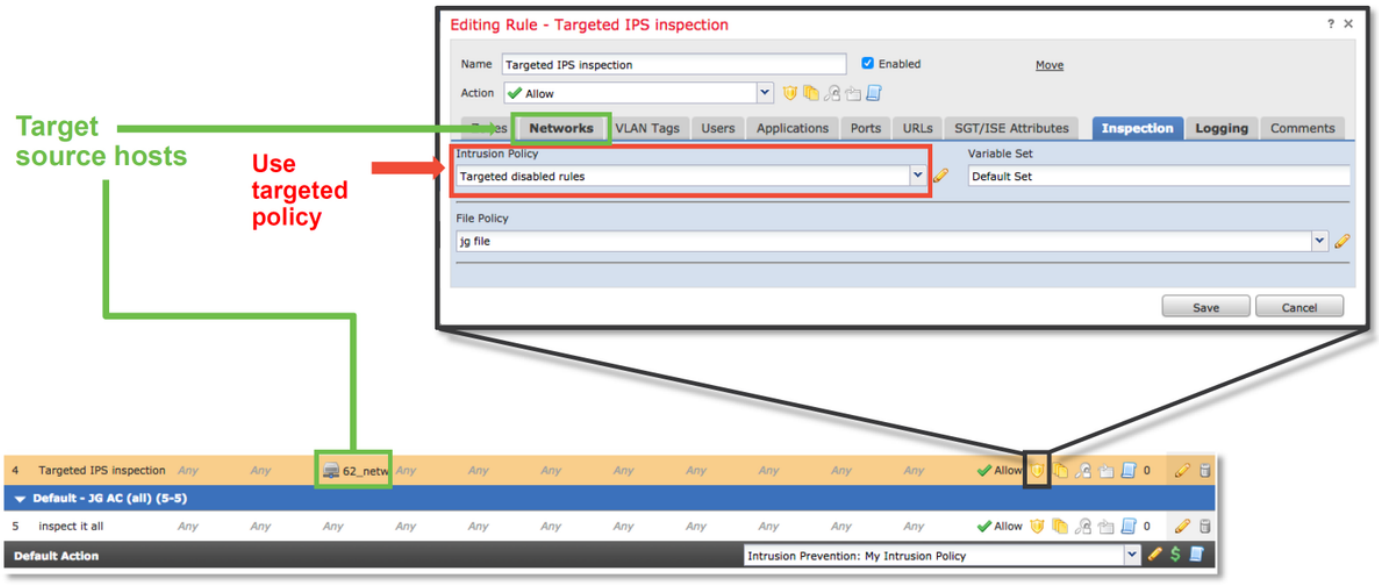
Een gericht inbraakbeleid maken

Als een bepaalde regel van het Inbraakbeleid het verkeer laat vallen wil u misschien niet dat het verkeer in kwestie wordt ingetrokken maar u kunt ook de regel niet willen uitschakelen. De oplossing is een nieuw Inbraakbeleid te creëren met de betreffende regel(en) uitgeschakeld en dan het verkeer vanaf de beoogde hosts te laten evalueren.

Hier is een illustratie van hoe je het nieuwe inbraakbeleid kunt creëren (onder **Beleid > Toegangsbeheer > Inbraakbeleid**).



Na het creëren van het nieuwe Inbraakbeleid kan het dan gebruikt worden binnen een nieuwe regel van het Toegangsbeleid, die de gastheren in kwestie richt, wiens verkeer vroeger door het oorspronkelijke Inbraakbeleid werd gedropt.



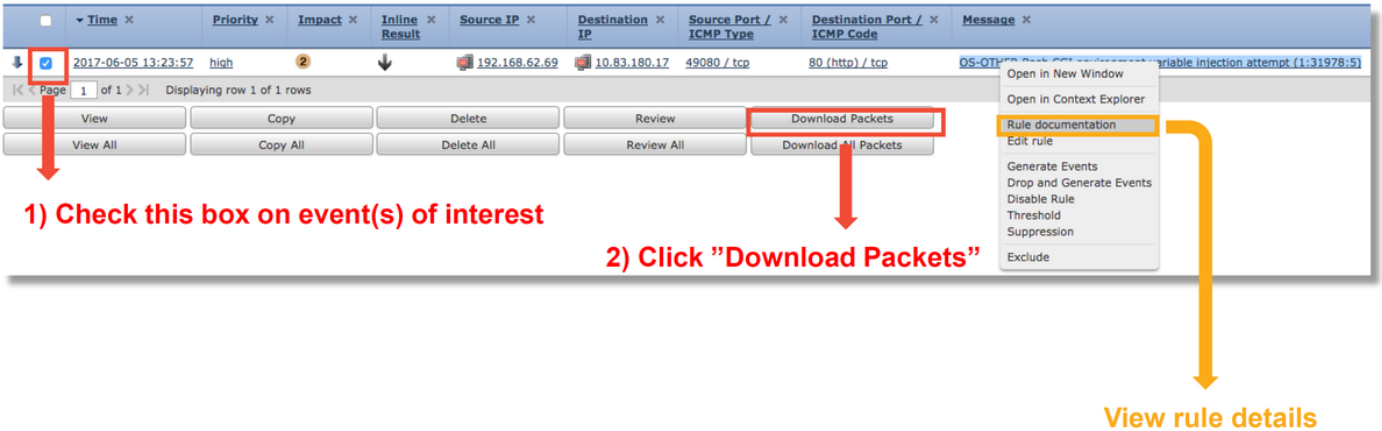
Onjuist positieve probleemoplossing

Een veelvoorkomend casescenario is een valse positieve analyse voor Inbraakgebeurtenissen. Er zijn verschillende dingen die kunnen worden gecontroleerd voordat er een fout-positief geval wordt geopend.

1. Klik vanuit de pagina **Tabelweergave van inbraakgebeurtenissen** op het selectieteken voor de betreffende gebeurtenis

2. Klik op **Download Packets** om de pakketten gevangen te krijgen door Snort toen de Inbraakgebeurtenis werd geactiveerd.

3. Klik met de rechtermuisknop op de regelnaam in de kolom **Bericht** en vervolgens **regeldocumentatie**, om de regelsyntaxis en andere relevante informatie te zien.



Hieronder is de syntax van de regel voor de regel die de gebeurtenis in het bovenstaande voorbeeld heeft geactiveerd. De delen van de regel die kunnen worden geverifieerd tegen het PCAP-bestand dat voor deze regel is gedownload van het FMC, zijn vet.

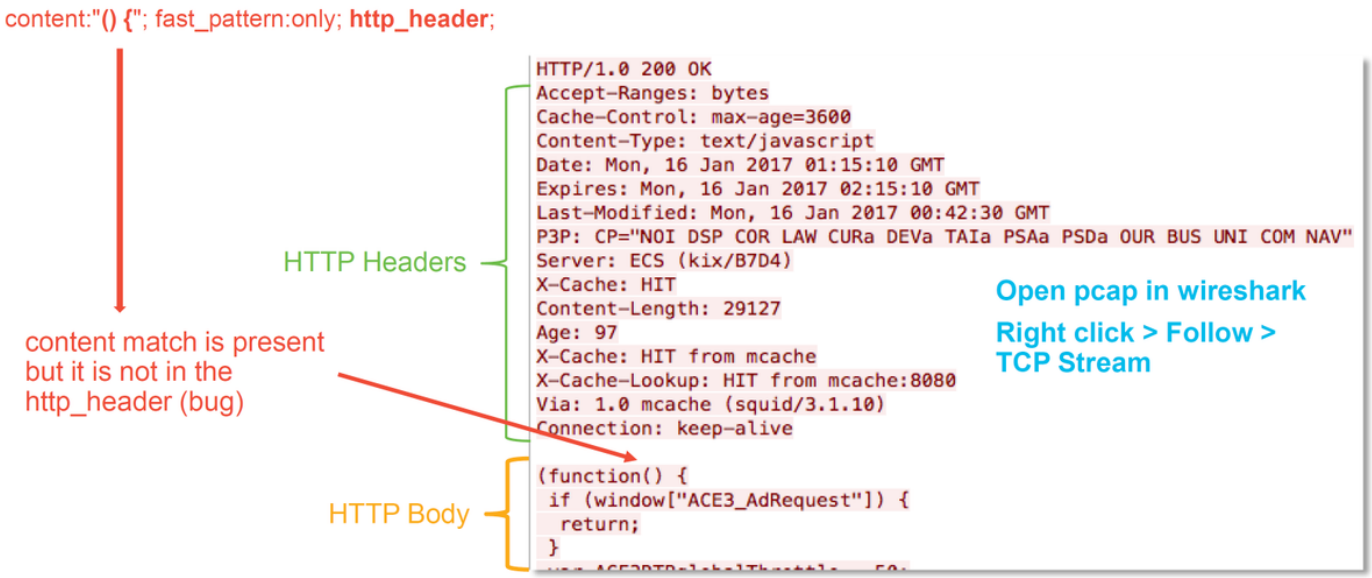
alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
(msg: "OS-OVERIGE Bash CGI milieu variabele injectiepoging"; \
flow:to_server,gevestigd; \

inhoud:"() {"; fast_patterns:alleen; http_header; \
metagegevens: beleidsevenwicht-ipsdrop, beleidsmax-detectie-ipsdrop, beleidssecurity-ipsdruppels, heerseset-gemeenschap, **service-http**; \
referentie:cve,2014-6271; referentie:cve,2014-6277; referentie:cve,2014-6278; referentie:cve,2014-7169; \
conflict:type-aanval-beheerder; \
sid:31978; rev.:5;)

Deze eerste stappen kunnen dan worden gevolgd om het analyseproces uit te voeren, om te zien of het verkeer zou moeten hebben aangepast aan de geactiveerd regel.

1. Controleer de toegangscontroleregel die op het verkeer is afgestemd. Deze informatie wordt gevonden in het kader van de kolommen in het tabblad Inbraakgebeurtenissen.
2. Vind de variabele die in genoemde toegangscontroleregel wordt gebruikt. De variabele set kan dan worden bekeken onder **Objecten > Objectbeheer > Variabele sets**
3. Zorg ervoor dat de IP adressen in de PCAP file match variabelen (in dit geval, een host opgenomen in **$EXTERNAL_NET** variabele die verbinding maakt met een host opgenomen in de **$HOME_NET** variabele configuratie)
4. Mogelijk moet er een volledige sessie/verbinding worden opgenomen. Snort vat de volledige stroom niet op vanwege prestatieredenen. In de meeste gevallen is het echter veilig om aan te nemen dat als een regel met flow:set geactiveerd was, de sessie werd ingesteld op het moment dat de regel werd geactiveerd, dus is een volledig PCAP-bestand niet nodig om deze optie in een korte regel te controleren. Maar het kan nuttig zijn om de reden waarom het werd geactiveerd beter te begrijpen.
5. Voor **service-http**, kijk naar het PCAP-bestand in Wireshark om te zien of het op HTTP-verkeer lijkt. Als de netwerkontdekking voor de host is ingeschakeld en de toepassing "HTTP" ervoor is gezien, kan de service op een sessie worden gekoppeld.

Met deze informatie in gedachten kunnen de pakketten die van het FMC worden gedownload, verder worden bekeken in Wireshark. Het PCAP-bestand kan worden geëvalueerd om te bepalen of de gebeurtenis die wordt geactiveerd een vals positief resultaat is.



In de illustratie hierboven, was de inhoud waarvoor de regel detecteert aanwezig in het PCAP bestand - **"() {"**

Echter, de regel bepaalt dat de inhoud gedetecteerd moet worden in de HTTP header van het pakket - **http_header**

In dit geval is de inhoud gevonden in het HTTP-orgaan. Dit is dus een fout-positief. Het is echter geen fout-positief in de zin dat de regel onjuist is geschreven. De regel is juist en kan in dit geval niet worden verbeterd. Dit voorbeeld stuit waarschijnlijk op een insect van de Snort, wat de snort veroorzaakt om bufferverwarring te hebben. Dit betekent dat Snort de http_headers niet correct heeft geïdentificeerd.

In dit geval kunt u op elke bestaande beugel op snort/IPS-motor controleren in de versie dat uw apparaat draait. Als er geen een is, kan een case met Cisco Technical Assistance Center (TAC) worden geopend. Volledige sessies zijn vereist om zo een probleem te onderzoeken als het Cisco-team moet bekijken hoe Snort in die status kwam, wat niet met één pakket kan worden gedaan.

Waar positief voorbeeld

De onderstaande afbeelding toont pakketanalyse voor dezelfde inbraakgebeurtenis. Deze keer is de gebeurtenis een waar positief omdat de inhoud in de HTTP header verschijnt.

Gegevens om te leveren aan TAC

Gegevens	Instructies
Probleemoplossing bestand via het FirePOWER-apparaat dat het verkeer controleert	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117
Packet Capture die gedownload zijn van het FMC	Zie dit artikel voor instructies
Alle relevante CLI-uitvoer die is verzameld, zoals spooruitvoer	Zie dit artikel voor instructies

Volgende stappen

Als is vastgesteld dat de component Inbraakbeleid niet de oorzaak van de kwestie is, zou de volgende stap de optie Problemen oplossen met de beleidsfunctie voor netwerkanalyse zijn.

Klik hier om verder te gaan naar het laatste artikel.