Snuit 3 begrijpen: stateful handtekeningevaluatie byte_jump

Inhoud

Inleiding

In dit document worden de nieuwe technieken beschreven die vanaf 7.4 zijn toegevoegd aan Snuit 3.

Achtergrondinformatie

- De Snort 3-detectiemodule werkt in de blokmodus. Hoewel die benadering een prestatievoordeel en implementatieeenvoud (relatief) biedt, zijn er enige beperkingen voor het detecteren van handtekeningen die meerdere gegevensblokken omvatten.
- Om de gebruikerservaring te vergemakkelijken, zijn al enkele verbeteringen in Snort geïmplementeerd, namelijk:
  1. Flowbits laten de regelschrijver toe om de netwerkstroom te markeren met een door de gebruiker gedefinieerde eigenschap; die eigenschap kan worden ingesteld, gewist en getest op elk pakket uit de stroom (het biedt een manier om over een grotere handtekening te concluderen over pakketten).
- Een stream module verzamelt draadpakketten in een herbouwd pakket, wat een groter en betekenisvoller blok is dan een rauw pakket; het evalueren van IPS-regels tegen het

herbouwde pakket geeft meer kansen om het hele beeld te zien en een groter patroon te matchen (handtekening).
- In sommige gevallen presenteert het opnieuw samengestelde pakket niet alleen nieuwe gegevens, maar omvat ook een deel van eerdere gegevens die al door detectie zijn verwerkt; opnieuw maakt dat blok van geaccumuleerde gegevens het mogelijk handtekeningen te detecteren die zich (tot op zekere hoogte) terugstrekken in de stroom.
- Een stream splitter snijdt de stroom in blokken, maar het snijpunt is mogelijk een zwak punt dat de aanvaller zou kunnen gebruiken om patroondetectie te vermijden; dus Snort heeft een jittering mechanisme geïmplementeerd om splitsen meer onvoorspelbaar te maken. Dit maakt de analyse voor de aanvaller nog ingewikkelder.

Nieuw

Stateful Signature evaluation is een nieuwe techniek die kan worden toegevoegd aan de lijst. Het breidt detectiemogelijkheden uit door IPS-regelevaluatie over meerdere blokken mogelijk te maken. Een regel is dus niet meteen een slechte match als het huidige blok geen gegevens heeft, maar wacht in plaats daarvan op meer gegevens om aan te komen.

Ondersteunde platforms

Minimale software- en hardwareplatforms

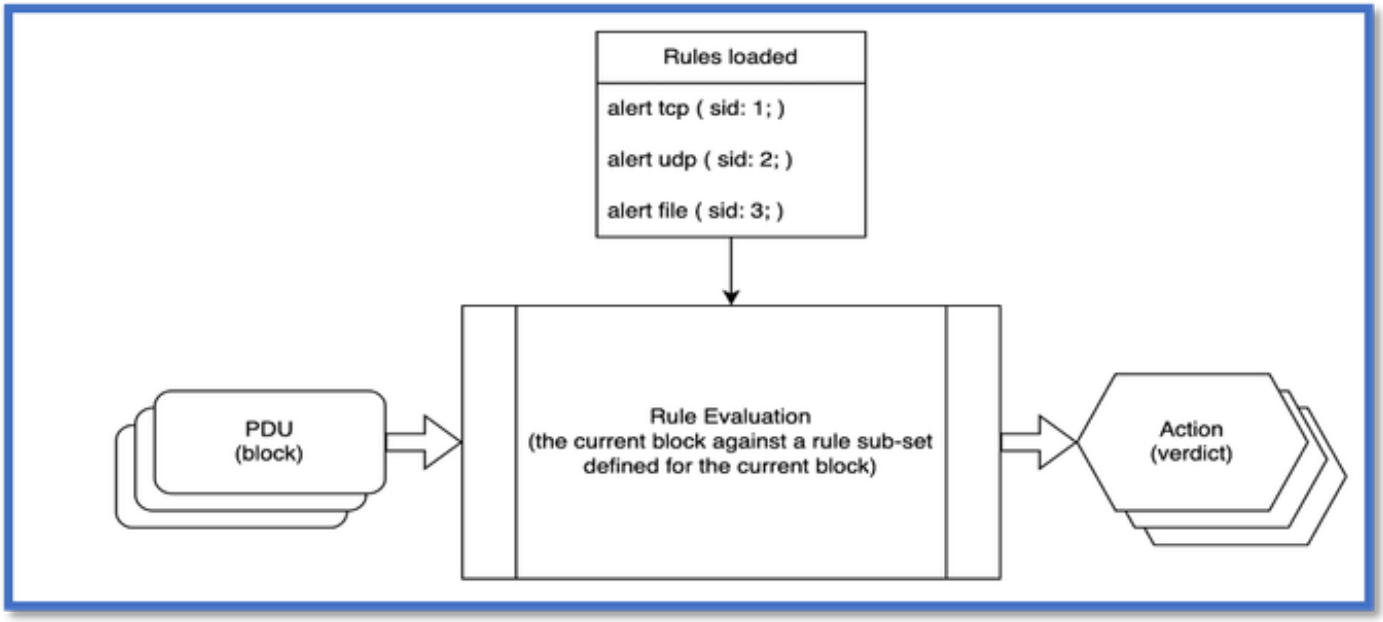
Min. ondersteunde Manager versie	Beheerde apparaten	Min. ondersteunde versie van beheerde apparaat vereist	Opmerkingen
Management Center 7.4.0	FTD	7.4.0	Alleen snurk 3
Apparaatbeheer 7.4.0	Elke FTD die FDM-beheer ondersteunt	7.4.0	Alleen snurk 3

Functiedetails

Functionele functiebeschrijving

Hoe werkt het?

De workflow van de detectiemodule wordt in het diagram weergegeven. In het stadium van de verkeersverwerking, heeft de module reeds alle geladen regels, en het accepteert gegevensblokken op een één-voor-één manier, evalueert regels, en bepaalt de acties die voor het processtateful handtekening evaluatie blok moeten worden genomen.



Opmerkingen over de regeling:

1. Zodra een regeldeelgroep is gedefinieerd voor het huidige gegevensblok, wordt elke regel ervan onafhankelijk van andere regels beoordeeld.
2. Elk gegevensblok wordt onafhankelijk van andere blokken beoordeeld.
3. Het gegevensblok is een abstractie voor een verzameling IPS-buffers die voor het huidige pakket worden geëvalueerd.
4. Action is een lijst van acties die voor het huidige pakket zijn geëvalueerd; de uiteindelijke uitspraak wordt later bepaald.

Om te begrijpen hoe de stateful handtekeningevaluatie werkt, neem een blik bij hoe een gemeenschappelijke IPS regel wordt geëvalueerd en hoe de gegevensblokken een stroom kunnen vormen.

Evaluatie van gemeenschappelijke regels

Een IPS-regel kan in deze vorm worden gepresenteerd:

```
action protocol source → destination ( option_1: parameters; option_2: parameters;
option_3: parameters; gid: 1; sid: 1; meta_option_1; meta_option_2; meta_option_3; )
```

Waarbij:

actie - IPS-actie op het pakket als de regel afvuurt

protocol-overeenkomend protocol

bron, bestemming - IP-adres en poort

option_1, option_2, option_3 - IPS-opties die deel uitmaken van de regelevaluatie

gid, sid - een uniek paar dat de regel identificeert (ze zijn net als metagegevensopties)

meta_option_1, meta_option_2, meta_option3 - regelmeta-gegevens zoals een bericht, een klassetype, of een verwijzing, deze opties nemen niet deel aan regelevaluatie.

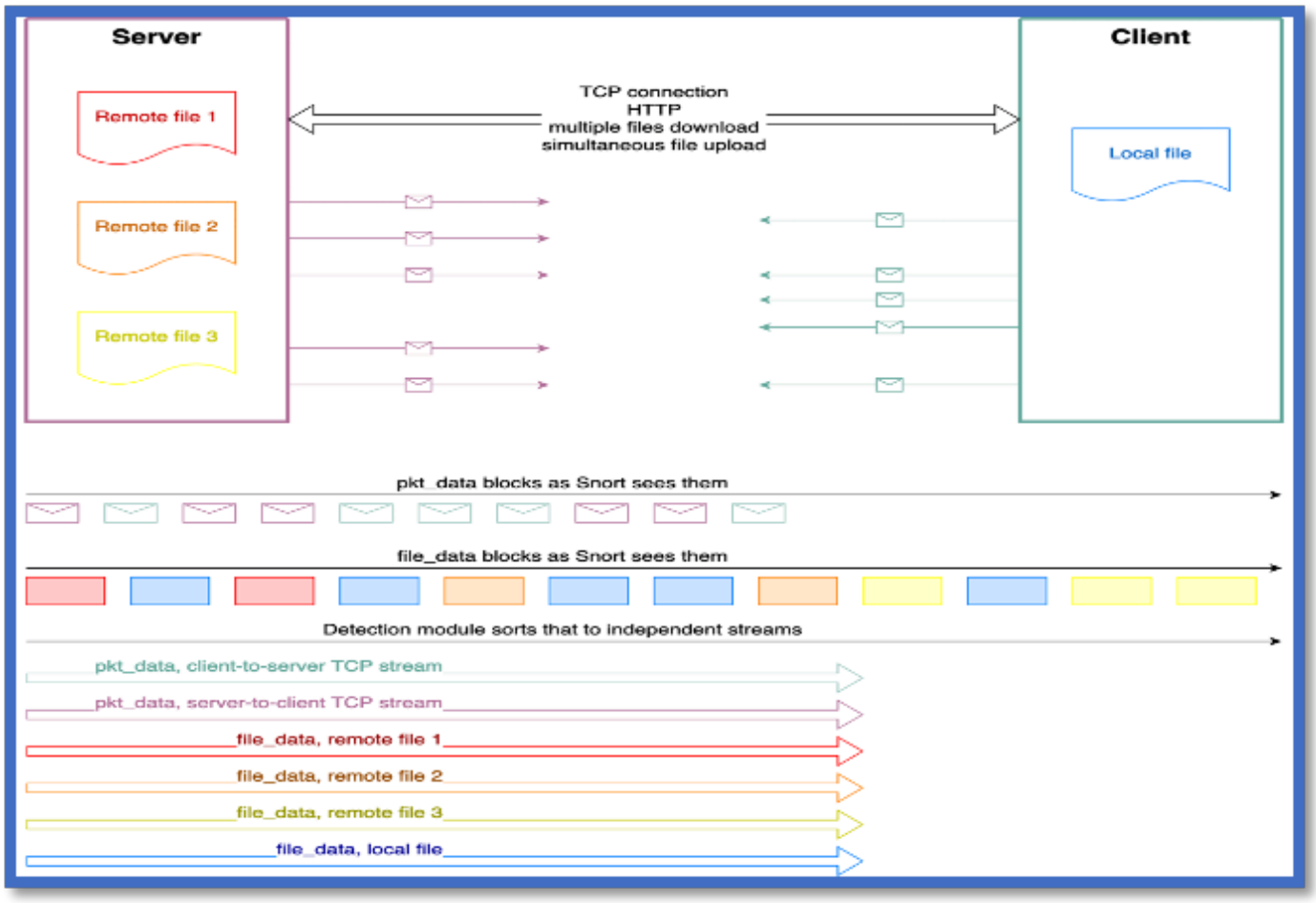
- Protocol, bron en bestemming vormen een regelkop. Het fungeert als een filter voor een netwerkstroom (die stroomt om te accepteren voor evaluatie). Alles tussen haakjes is een verzameling regels. IPS-opties (behalve regelmetagegevens) van de regelinstantie zijn de opties die voor het gegevensblok worden geëvalueerd. Zij voldoen aan deze verklaringen:
- De opties worden alleen in de volgorde van links naar rechts beoordeeld.
    1. kan één van twee belangrijke types zijn.
    2. buffer setter, selecteert de optie de IPS buffer voor het huidige pakket.
- andere (patroonzoekfunctie, wiskundige bewerking, cursormanipulatie, flowbit-bewerking)
- Een cursor wordt gebruikt om de positie in de geselecteerde IPS-buffer te volgen.

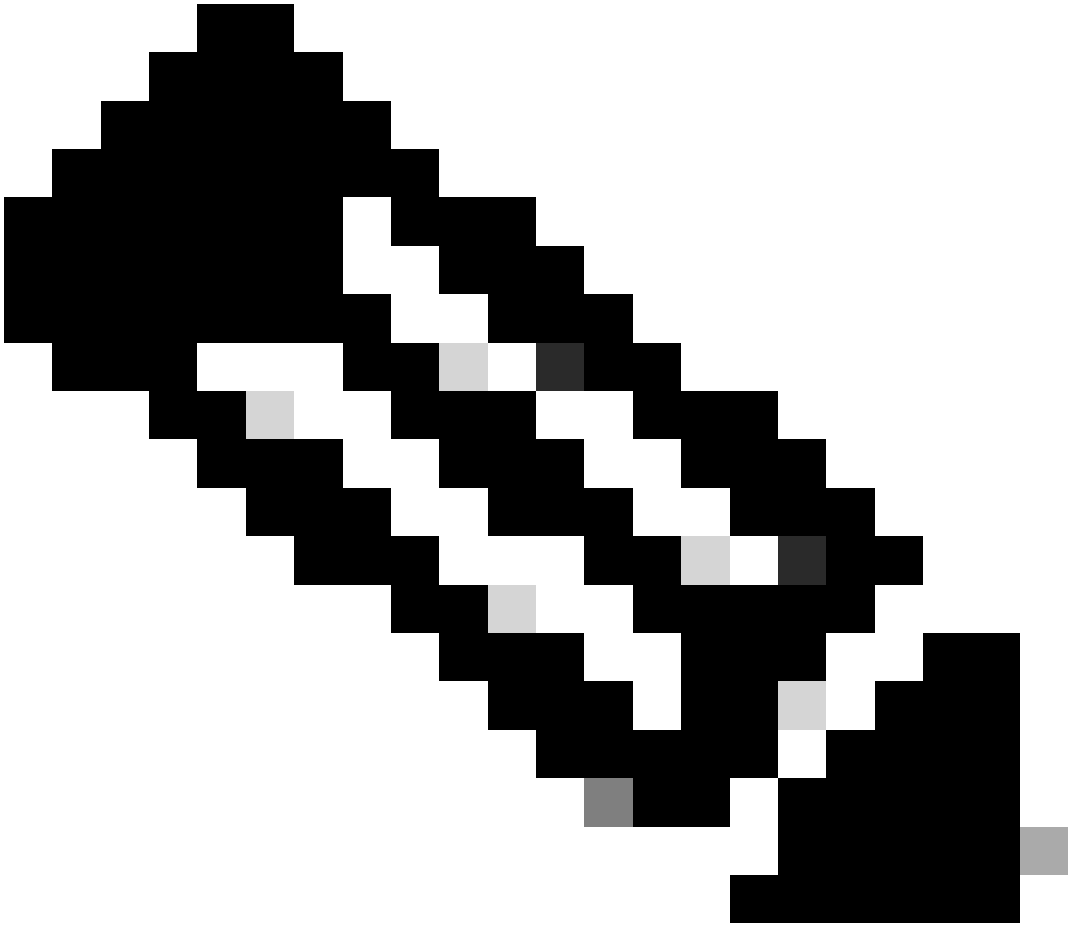
- een optie kan zijn:
    1. 'absoluut', dat wil zeggen dat het niet afhankelijk is van de positie van de cursor
    2. 'relatief' betekent dat de evaluatie begint vanaf de positie van de cursor
- als een optie probeert om de cursor uit de geselecteerde IPS buffer in te stellen, dan faalt het en de gehele regel klopt niet (door gebrek aan gegevens)
- Het laatste punt is een beperking van de detectiemodule. Als Snort onbeperkte bronnen zou kunnen hebben, zou het alle gegevens in een cache plaatsen die worden gezien om regels steeds opnieuw te evalueren wanneer gegevens beschikbaar worden (meer draadpakketten arriveren).

Gegevensstromen en IPS-buffers

- De gegevensstroom is een stroom bytes in een aangrenzende vorm uit dezelfde bron. Het is een nieuw concept dat wordt gepresenteerd om een stateful evaluation te ondersteunen. De evaluatie van regels tussen blokken moet worden uitgevoerd binnen dezelfde logische gegevens (of het nu een bestand, pure TCP-stream of JavaScript-tekst is).

- In het algemeen kan een gegevensblok dat door de detectiemodule wordt ontvangen:
    - Van een andere IPS-buffer zijn (bijvoorbeeld, pkt_data en file_data zijn niet hetzelfde)
    - Behoren tot een andere stream
    - Geen stream vormen (buffers gegenereerd uit een onbewerkt pakket)
    - Geen aangrenzende stroom (ICMP, UDP)
    - Wees niet in orde (HTTP Partial Response)
    - Bevat herhaalde gegevens (een geaccumuleerd blok, zoals in http_inspect.script_detectie of HTTP Chunked Response)
- De detectiemodule kan dingen sorteren om alleen blokken van dezelfde stroom te schakelen, anders zou het evaluatieproces ongewenste interferentie van interleaving blokken zien.


Server
Remote file 1
Remote file 2
Remote file 3
TCP connection
HTTP
multiple files download
simultaneous file upload
Client
Local file
pkt_data blocks as Snort sees them
file_data blocks as Snort sees them
Detection module sorts that to independent streams
pkt_data, client-to-server TCP stream
pkt_data, server-to-client TCP stream
file_data, remote file 1
file_data, remote file 2
file_data, remote file 3
file_data, local file



Opmerking: het voorbeeld hier presenteert een case waarin een HTTP-client meerdere bestanden tegelijk uploadt en downloadt.

- Momenteel, kunnen slechts twee IPS buffers een stroom vertegenwoordigen: pkt_data en file_data, waar:
    1. pkt_data van twee stromen voor TCP protocol (client-naar-server en server-naar-client richtingen)
    2. file_data moet stromen voor bestanden, MIME bijlagen en andere protocol gegevens (zoals HTTP HTML pagina en/of andere Content-Type)
- De stateful evaluatie wordt alleen binnen de gegevensstroom uitgevoerd.

Regelvoortzetting

- De sectie eindigt eerder met een verklaring dat de IPS optie niet aansluit als het de cursor uit de huidige IPS buffer plaatst. Maar wanneer de IPS-buffer een gegevensstroom vormt, stapt de stateful Signatuur-evaluatie binnen en slaat de regelevaluatie-context op in het Snelstroom-object. De opgeslagen evaluatiecontext (status) wordt regelvoortzetting

genoemd. De stateful handtekeningsevaluatie stelt de definitieve uitspraak van de regel uit tot meer gegevens beschikbaar worden.

- De voortzetting van de regel heeft drie belangrijke delen: IPS buffernaam, bufferbron en gerichte cursorpositie (de bufferbron is een uniek herkenningsteken voor de gegevensstroom).
- Wanneer een gegevensblok door de detectiemodule wordt verwerkt, vinden de volgende handelingen plaats:-
    - De stateful handtekeningsevaluatie leidt tot een regelvoortzetting en maakt het aan de stroom vast als:
        - IPS optie (byte_jump, content, pcre of iets anders dat de cursorpositie bijwerkt) stelt de cursor in na de huidige IPS buffer
        - De huidige IPS-buffer ondersteunt de gegevensstroom.
        - De huidige IPS-buffer vormt momenteel een gegevensstroom.
- Stateful Signature evaluation trekt pas gecreëerde regelvoortzetting in en verwijdert deze uit de stroom als:
    - De IPS-regel is in brand gestoken op het huidige gegevensblok (de regel komt overeen met andere plaatsen in het blok)
- Stateful handtekeningevaluatie verwerpt hangende regelvoortzettingen en verwijdert ze uit de stroom als:
    - IPS-buffer vormt geen aaneengesloten stroom (de blokken hebben bijvoorbeeld herhaalde gegevens in zich, of er is een gat (een deel van de gegevens werd gemist of het blok is niet in orde).
- Stateful handtekeningevaluatie werkt de beoogde cursorpositie bij met nieuwe gegevens die beschikbaar zijn wanneer:
    - De bufferbron van de regelvoortzetting is hetzelfde als de geselecteerde bufferbron
    - IPS-buffer vormt een aaneengesloten stroom
- De stateful handtekeningevaluatie verstuurt de regelvoortzetting terug naar de IPS-regelengine wanneer:
    1. Gerichte cursorpositie punten binnen de geselecteerde IPS buffer (wat betekent dat het eindelijk alle gegevens die nodig zijn om de regelevaluatie te voltooien).

Gebruikersconfiguraties

- Aangezien regelvoortzettingen geheugen in beslag nemen, kan Snort geen onbeperkt aantal van hen opslaan. Er is een configuratieoptie om de limiet te controleren:
    1. Detectie.max_continuations_per_flow = 1024: maximaal aantal continueringen dat gelijktijdig op de stroom wordt opgeslagen { 0:65535}
- Wanneer stateful handtekening evaluatie de limiet bereikt, vervangt het de oudste regel voortzetting met een nieuwe.
- De oudste regelvoortzetting die zich op de stroom bevindt is er te lang, wat betekent dat het nog steeds niet voldoet aan een voorwaarde om de regelevaluatie te hervatten.
- Bovendien zijn er tal van peg counts beschikbaar om IPS-regels te verfijnen (die de belangrijkste focus moeten zijn) en de limiet (indien nodig):
    1. detectie.cont_creations: totaal aantal gecreëerde continueringen (som)
    2. detectie.cont_recalls: totaal aantal opgeroepen continueringen (som)
    3. detectie.cont_flows: totaal aantal stromen met behulp van voortzetting (som)

4. Detectie.cont_evals: totaal aantal aan de voorwaarde beantwoordende voortzettingen (som)
5. detectie.cont_matches: totaal aantal overeenkomende voortzettingen (som)
6. detectie.cont_mismatches: totaal aantal niet-overeenkomende voortzettingen (som)
7. detectie.cont_max_num: piekaantal gelijktijdige continueringen per stroom (max)
8. Detectie.cont_match_Distance: totaal aantal bytes overgesprongen door overeenkomende continueringen (som)
9. Detectie.cont_mismatch_afstand: totaal aantal bytes omgesprongen door niet-overeenkomende continueringen (som)

Probleemoplossing

De functie is een verbetering van het bestaande detectieproces, dus kan het probleem niet expliciet worden opgelost. In het geval van een storing in de detectie moeten regels, configuratie of verkeer worden onderzocht.

Probleem met voorbeeld

Probleem: beschrijving

- Laten we zeggen dat een handtekening het begin en de staart van het bestand tegelijkertijd moet controleren.
- Bijvoorbeeld, in een gericht bestand van deze structuur (header, body, metagegevens) moeten we zien of een van de metagegevens een 0-waarde heeft.

- Bestandsbytes: e1 f3 22 03 7f xx xx ... xx 01 00 02 00 waarin

    - e1 f3 22 03 - 4 bytes voor magisch nummer, dat het bestandstype identificeert
    - 7f ff - 2 bytes voor lichaamsomvang
    - xx xx xx ... xx - 32kb van sommige gegevens
    - 01 00 02 00 - 4 bytes metagegevens, in tagwaarde-indeling (1 bytes voor elk)
- IPS-regel ziet er zo uit: alarmbestand (file_data; inhoud:"|e1f32203|", fast_patterns; byte_jump:2,0,relatief; inhoud:"00", binnen:4, relatief; zijde: 1;)

    - Waarbij

        - Het protocol van het dossier zorgt ervoor dat de regel herbouwde pakketten slechts goedkeurt (de ruwe pakketten nemen niet aan stateful handtekeningsevaluatie deel)
        - De ‘file_data optie selecteert een file data buffer, die een stream kan vormen
        - 1e inhoudsoptie is een snel patroon en het controleert op het magische getal (als dat het bedoelde bestandstype is)
        - de optie byte_jump leest de grootte van het bestand en springt over het bestand
        - De tweede inhoudsoptie voert de definitieve controle voor metagegevenswaarden uit, binnen parameter grenzen zoekdiepte en maakt de optie relatief.

Probleem: oplossing

De regel zou op deze manier worden beoordeeld:

Op het 1ste pakket (van 8kB grootte), dat een bestandskop en een deel van het lichaam draagt:

1. IPS buffer file_data is geselecteerd. De cursor wijst naar de 0de byte e1.
2. De snelle patroonoptie komt overeen met de positie van de cursor direct na het magische nummer, en wordt ingesteld op byte 7f.
3. De byte_jump optie leest twee bytes van de grootte van het dossier lichaam. De cursor wordt bijgewerkt door deze twee bytes. Vervolgens berekent byte_jump een sprong voor meer dan 32768 bytes.
4. stateful signatuur evaluatie creëert een regelvoortzetting, waar het 24578 bytes meer nodig heeft (32768 - (8kB - 4 bytes header - 2 bytes van lichaamsgrootte)).
5. De hele regel klopt niet met elkaar, omdat de optie byte_jump er niet in slaagt om de cursorpositie zo ver in te stellen.

Op het 2e pakket (van 16kB grootte), dat het deel van de bestandskant draagt:

1. stateful handtekening evaluatie ziet hangende regelvoortzetting.
2. Hij selecteert de buffer op basis van zijn naam en ziet dat file_data beschikbaar is en de nieuwe grootte van de data 16384.
3. De bijgewerkte cursor toont dat 8194 bytes nog steeds nodig zijn (24578 - 16384)
4. De regel wordt niet hervat.

Op het 3e pakket (van 8198 maten), dat bestandsdeel en metagegevens draagt:

1. stateful handtekening evaluatie ziet hangende regelvoortzetting.
2. Hij selecteert de buffer op zijn naam en ziet dat file_data beschikbaar is en de nieuwe datagrootte 8198 is.
3. De bijgewerkte cursor toont dat de buffer genoeg gegevens heeft, de cursorpositie is 8194.
4. bij stateful signed evaluation wordt de voortzetting van de regel verwijderd.
5. stateful handtekening evaluatie hervat regel evaluatie van de 2e content optie met de cursor aanwijzen op byte 01.
6. De inhoudsoptie vindt een overeenkomst op de tweede gezochte byte.
7. De hele regel schiet eindelijk in brand.

Beperkingen Details en algemene problemen

Beperkingen en andere overwegingen

- Vanwege de stateful handtekening evaluatie implementatie, snort laat alle hangende regelvoortzettingen vallen wanneer het herlaadt zijn configuratie. Merk op dat de regelvoortzettingen ondanks wordt gelaten vallen nog Snortgeheugen bezetten tot het volgende gegevensblok wordt verzonden naar de opsporingsmodule.
- De regellatentieeigenschap voor de IPS regel in stateful evaluatie handelt het zelfde alsof het een gemeenschappelijke regelevaluatie was. De evaluatietijd voor regelonderdelen op

verschillende gegevensblokken wordt samengevat. Als de tijd de grens overschrijdt, sluit de regelevaluatie vroeger een kort circuit af.

- Flowbits-bewerkingen behouden hun betekenis, hoewel ze nog steeds functioneren als 'statische' opties.
  Een flowbit set/clear/test operatie wordt uitgevoerd binnen een momenteel bekende context. Dus, als de flowbit optie wordt geëvalueerd in een regel voortzetting, zou het rekening houden met de huidige omgeving (flowbits set), niet de omgeving toen de regel begon met de evaluatie.

Een regelschrijver moet ook aandacht besteden aan de snel-patroonlocatie.

Zelfs als het in elk deel van de regel kan zijn, wordt de fast-patroonoptie beoordeeld vóór de gehele regel. Het leidt tot regelevaluatie. Voor stateful handtekening evaluatie-gebaseerde regel betekent het dat de regel voortzettingspunt moet zijn na de snel-patroonoptie.
Bovendien kan de IPS-regel meerdere regelvoortzettingen in de evaluatie hebben (de een na de ander, niet tegelijkertijd). Aangezien elke optie van de regelinstantie kan zijn voortzetting hebben, staat het de regelschrijver toe om extra controles in verschillende plaatsen van de gegevensstroom met de zelfde IPS regel uit te voeren.

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.