Comprendre Snort 3 : Byte_Jump d'évaluation des signatures avec état

Table des matières

- Introduction
- Informations générales
- Nouveautés de Cisco
- Plates-formes prises en charge
  - Plates-formes logicielles et matérielles minimales
- Détails des fonctionnalités
  - Description des fonctionnalités
    - Comment cela fonctionne-t-il?
    - Évaluation des règles communes
- Flux de données et tampons IPS
  - Continuation des règles
  - Configurations utilisateur
- Dépannage
- Exemple de problème
  - Problème : description
  - Problème : solution
- Limitations, détails et problèmes courants
  - Limitations Et Autres Considérations

Introduction

Ce document décrit les nouvelles techniques ajoutées dans Snort 3 à partir de la version 7.4.

Informations générales

- Le module de détection Snort 3 fonctionne en mode bloc. Bien que cette approche offre un avantage en termes de performances et de simplicité de mise en oeuvre (relativement), elle présente certaines limites en matière de détection des signatures qui couvrent plusieurs blocs de données.
- Pour faciliter l'expérience utilisateur, certaines améliorations sont déjà mises en oeuvre dans Snort, à savoir :
  1. Les bits de flux permettent à l'enregistreur de règles de marquer le flux réseau avec une propriété définie par l'utilisateur ; cette propriété peut être définie, effacée et testée sur n'importe quel paquet du flux (elle permet de conclure à une signature plus importante sur des paquets).
- Un module de flux accumule les paquets de fils dans un paquet reconstruit, qui est un bloc plus grand et plus significatif qu'un paquet brut ; l'évaluation des règles IPS par rapport au

paquet reconstruit donne plus de chances de voir l'ensemble et de correspondre à un modèle plus grand (signature).
- Dans certains cas, le paquet reconstruit présente non seulement de nouvelles données, mais inclut une partie des données précédentes déjà traitées par la détection ; là encore, ce bloc de données accumulées permet de détecter des signatures qui s'étendent vers l'arrière sur le flux (dans une certaine mesure).
- Un séparateur de flux coupe le flux en blocs, mais le point de coupure est potentiellement un point faible que le pirate pourrait utiliser pour éviter la détection de modèle ; ainsi Snort a un mécanisme de gigue mis en oeuvre pour rendre le fractionnement plus imprévisible. Cela complique encore l'analyse pour le pirate.

Nouveautés de Cisco

L'évaluation dynamique des signatures est une nouvelle technique qui peut être ajoutée à la liste. Il étend les capacités de détection en activant l'évaluation des règles IPS sur plusieurs blocs. Ainsi, une règle ne fait pas immédiatement défaut de correspondance si le bloc actuel manque de données, mais attend plutôt que d'autres données arrivent.

Plates-formes prises en charge

Plates-formes logicielles et matérielles minimales

Version min. du gestionnaire supportée	Périphériques gérés	Version minimale du périphérique géré prise en charge requise	Remarques
Centre de gestion 7.4.0	FTD	7.4.0	Snort 3 uniquement
Gestionnaire de périphériques 7.4.0	Tout FTD prenant en charge la gestion FDM	7.4.0	Snort 3 uniquement

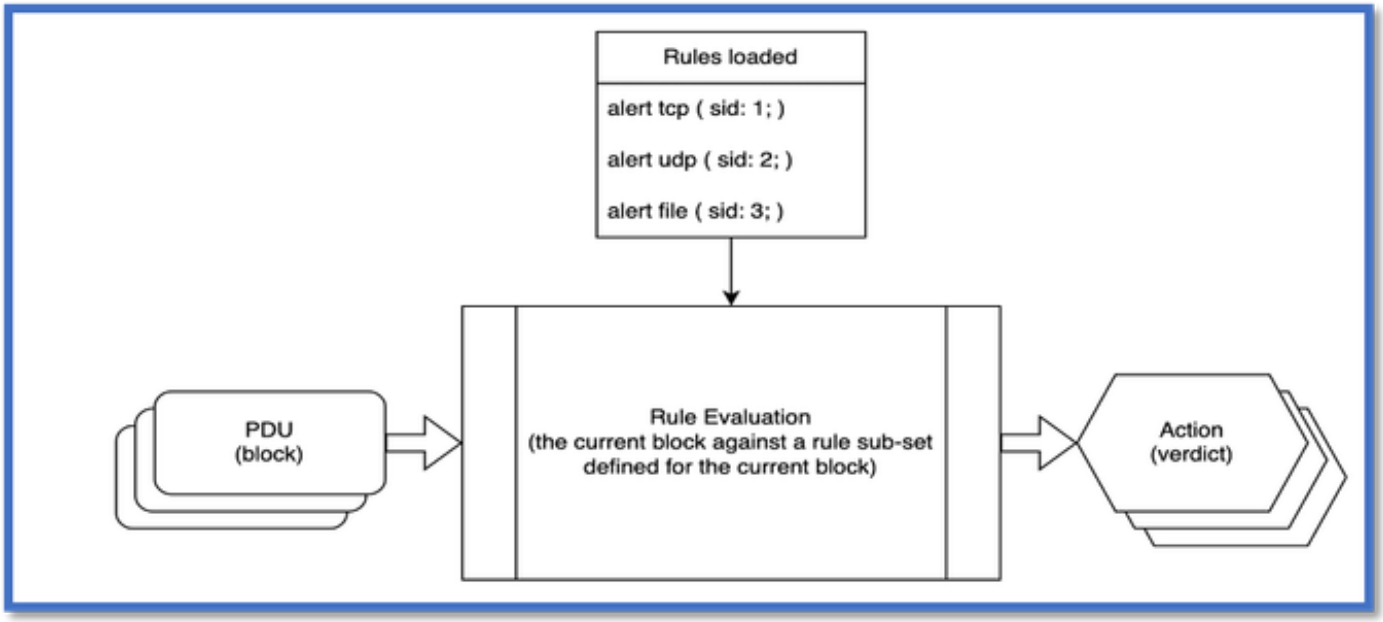
Détails des fonctionnalités

Description des fonctionnalités

Comment cela fonctionne-t-il?

Le workflow du module de détection est représenté sur le schéma. Au stade du traitement du trafic, le module a déjà toutes les règles chargées, et il accepte les blocs de données un par un,

évalue les règles et définit les actions à entreprendre pour le bloc d'évaluation de la signature avec état du processus.



Remarques sur le régime :

1. Une fois qu'un sous-ensemble de règles est défini pour le bloc de données en cours, chaque règle qu'il contient est évaluée indépendamment des autres règles.
2. Chaque bloc de données est évalué indépendamment des autres blocs.
3. Le bloc de données est une abstraction pour un ensemble de tampons IPS qui sont évalués pour le paquet en cours.
4. Action est une liste d'actions évaluées pour le paquet en cours ; le verdict final est déterminé ultérieurement.

Pour comprendre le fonctionnement de l'évaluation des signatures avec état, observez comment une règle IPS commune est évaluée et comment les blocs de données peuvent former un flux.

Évaluation des règles communes

Une règle IPS peut être présentée sous la forme suivante :

```
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; )
```

Where:

action - Action IPS sur le paquet si la règle se déclenche

protocole - protocole correspondant

source, destination - adresse IP et port

option_1, option_2, option_3 - options IPS qui font partie de l'évaluation des règles

gid, sid - paire unique qui identifie la règle (ce sont des options de métadonnées similaires)

meta_option_1, meta_option_2, meta_option3 - métadonnées de règle comme un message, un type de classe ou une référence, ces options ne participent pas à l'évaluation de règle.

- Le protocole, la source et la destination forment un en-tête de règle. Il agit comme un filtre pour un flux réseau (flux à accepter pour évaluation). Tout entre parenthèses est un corps de règles. Les options IPS (à l'exception des métadonnées de règle) du corps de la règle sont celles qui sont évaluées pour le bloc de données. Ils se conforment à ces déclarations :
- les options sont évaluées strictement dans l'ordre de gauche à droite.
    1. peut être l'un des deux principaux types.
    2. buffer setter, l'option sélectionne le tampon IPS pour le paquet en cours.
- autres (recherche de motif, opération mathématique, manipulation du curseur, opération bit de flux)
- Un curseur est utilisé pour suivre la position dans la mémoire tampon IPS sélectionnée.

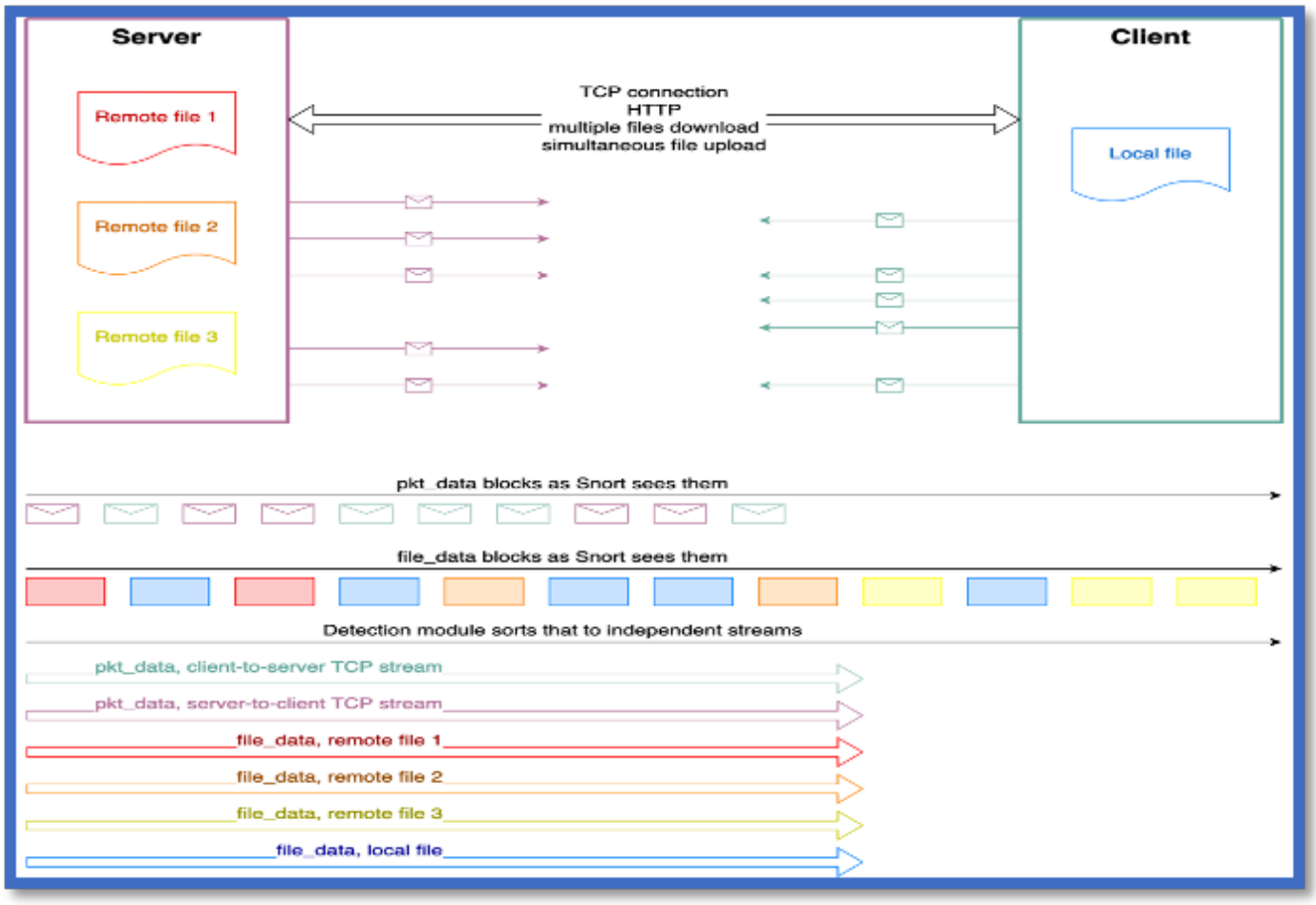
- une option peut être :
    1. 'absolu', ce qui signifie qu'il ne dépend pas de la position du curseur
    2. 'relative', ce qui signifie qu'elle commence son évaluation à partir de la position du curseur
- si une option tente de sortir le curseur de la mémoire tampon IPS sélectionnée, elle échoue et la règle entière ne correspond pas (en raison d'un manque de données)
- Le dernier point est une limitation du module de détection. Si Snort pouvait disposer de ressources illimitées, il mettrait en cache toutes les données vues pour évaluer les règles encore et encore lorsque les données deviennent disponibles (plus de paquets de fils arrivent).

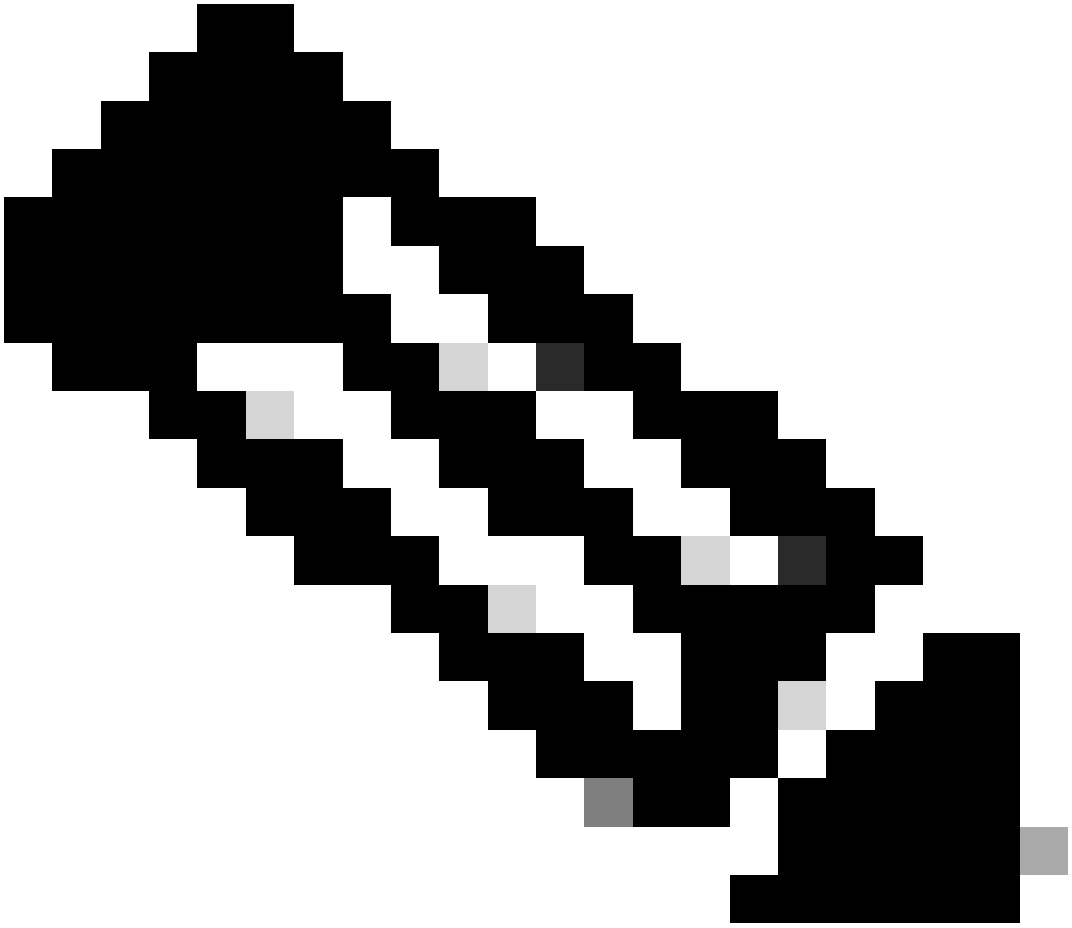
Flux de données et tampons IPS

- Le flux de données est un flux d'octets sous une forme contiguë provenant de la même source. Il s'agit d'un nouveau concept présenté pour soutenir l'évaluation dynamique. L'évaluation des règles entre les blocs doit être effectuée dans les mêmes données logiques (qu'il s'agisse d'un fichier, d'un flux TCP pur ou d'un texte JavaScript).

- En général, un bloc de données reçu par le module de détection pourrait :
    - Provient d'un tampon IPS différent (par exemple, pkt_data et file_data ne sont pas identiques)
    - Appartient à un autre flux
    - Ne pas former de flux (mémoires tampons générées à partir d'un paquet brut)
    - Ne forment pas un flux contigu (ICMP, UDP)
    - Pas dans l'ordre (réponse partielle HTTP)
    - Contenir des données répétées (un bloc cumulé, comme dans http_inspect.script_detection ou HTTP Chunked Response)
- Le module de détection peut trier les éléments pour concaténer des blocs à partir du même flux uniquement, sinon le processus d'évaluation verrait des interférences indésirables

provenant de blocs entrelacés.





Remarque : l'exemple présenté ici présente un cas où un client HTTP télécharge et télécharge plusieurs fichiers simultanément.

- Actuellement, seuls deux tampons IPS peuvent représenter un flux : pkt_data et file_data, où :
  1. pkt_data forme deux flux pour le protocole TCP (sens client-serveur et serveur-client)
  2. file_data doit former des flux pour les fichiers, les pièces jointes MIME et d'autres données de protocole (comme la page HTML HTTP et/ou un autre type de contenu)
- L'évaluation avec état est effectuée strictement dans le flux de données.

Continuation des règles

- La section précédente se termine par une instruction indiquant que l'option IPS ne correspond pas si elle place le curseur hors de la mémoire tampon IPS actuelle. Mais lorsque la mémoire tampon IPS forme un flux de données, la fonction d'évaluation de signature avec état s'insère et enregistre le contexte d'évaluation de règle dans l'objet de flux Snort. Le contexte d'évaluation enregistré (état) est appelé continuation de règle.

L'évaluation dynamique des signatures reporte le verdict final de la règle jusqu'à ce que davantage de données soient disponibles.

- La continuation de règle comporte trois parties principales : le nom de la mémoire tampon IPS, la source de la mémoire tampon et la position du curseur ciblé (la source de la mémoire tampon est un identificateur unique pour le flux de données).
- Lorsqu'un bloc de données est traité par le module de détection, les actions suivantes ont lieu : -
    - L'évaluation dynamique des signatures crée une continuation de règle et l'attache au flux si :
        - L'option IPS (byte_jump, content, pcre ou toute autre option qui met à jour la position du curseur) définit le curseur après la mémoire tampon IPS actuelle
        - La mémoire tampon IPS actuelle prend en charge le flux de données.
        - Le tampon IPS actuel forme un flux de données en ce moment.
- L'évaluation avec état des signatures supprime la continuation de la règle que vous venez de créer et la supprime du flux si :
    - La règle IPS s'est déclenchée sur le bloc de données actuel (la règle correspond à d'autres emplacements du bloc)
- L'évaluation dynamique des signatures rejette les continuations de règles en attente et les supprime du flux si :
    - La mémoire tampon IPS ne forme pas de flux contigu (par exemple, les blocs contiennent des données répétées ou il y a un vide (une partie des données a été manquée ou le bloc n'est pas en ordre).
- L'évaluation dynamique des signatures met à jour la position du curseur cible avec les nouvelles données disponibles lorsque :
    - La source de tampon de la continuation de règle est la même que la source de tampon sélectionnée
    - La mémoire tampon IPS forme un flux contigu
- L'évaluation de la signature avec état renvoie la continuation de la règle au moteur de règles IPS lorsque :
    1. La position du curseur ciblé pointe à l'intérieur de la mémoire tampon IPS sélectionnée (ce qui signifie qu'il a finalement reçu toutes les données nécessaires pour terminer l'évaluation de la règle).

Configurations utilisateur

- Comme les continuations de règles prennent de la mémoire, Snort ne peut pas en stocker un nombre illimité. Il existe une option de configuration pour contrôler la limite :
    1. Detection.max_continuations_per_flow = 1024 : nombre maximal de continuations stockées simultanément sur le flux { 0:65535 }
- Lorsque l'évaluation des signatures avec état atteint la limite, elle remplace la plus ancienne continuation de règle par une nouvelle.
- La plus ancienne continuation de règle résidant sur le flux est là depuis trop longtemps, ce qui signifie qu'elle ne remplit toujours pas une condition pour reprendre l'évaluation de règle.
- En outre, il existe de nombreux comptes de parité disponibles pour affiner les règles IPS (qui doivent être le point central) et la limite (si nécessaire) :
    1. detection.cont_creations : nombre total de continuations créées (somme)

2. detection.cont_rappels : nombre total de continuations rappelées (somme)
3. detection.cont_flows : nombre total de flux utilisant la continuation (somme)
4. detection.cont_evals : nombre total de continuations de conditions remplies (somme)
5. detection.cont_matches : nombre total de continuations rapprochées (somme)
6. detection.cont_mismatches : nombre total de continuations non concordantes (somme)
7. detection.cont_max_num : nombre maximal de continuations simultanées par flux (max)
8. detection.cont_match_distance : nombre total d'octets ignorés par les continuations correspondantes (somme)
9. detection.cont_mismatch_distance : nombre total d'octets ignorés par les continuations incompatibles (somme)

Dépannage

Cette fonctionnalité étant une amélioration du processus de détection existant, elle ne peut pas être explicitement dépannée. En cas de défaillance de la détection, les règles, la configuration ou le trafic doivent être examinés.

Exemple de problème

Problème : description

- Disons qu'une signature doit à la fois vérifier le début du fichier et sa fin.
- Par exemple, dans un fichier ciblé de cette structure (en-tête, corps, métadonnées), nous devons voir si l'une de ses métadonnées a une valeur 0.

- Octets du fichier : e1 f3 22 03 7f ff xx ... xx 01 00 02 00 où

    - e1 f3 22 03 - 4 octets pour le numéro magique, qui identifie le type de fichier
    - 7f ff - 2 octets pour la taille du corps
    - xx xx ... xx - 32 ko de certaines données
    - 01 00 02 00 - 4 octets de métadonnées, au format tag-value (1 octet pour chaque)
- La règle IPS ressemblerait à : fichier d'alerte (données_fichier ; contenu : "|e1f32203|",fast_pattern ; byte_jump : 2,0,relative ; contenu : "00", within : 4, relative ; sid : 1 ;)

    - Where

        - Le protocole de fichier garantit que la règle accepte uniquement les paquets reconstruits (les paquets bruts ne participent pas à l'évaluation des signatures avec état)
        - L'option « file_data » sélectionne un tampon de données de fichier, qui peut former un flux
        - La première option de contenu est un modèle rapide et elle vérifie le nombre magique (si c'est le type de fichier prévu)
        - L'option byte_jump lit la taille du corps du fichier et passe sur ce dernier

- 2nd content option effectue la vérification finale des valeurs de métadonnées, dans les limites des paramètres de profondeur de recherche et rend l'option relative.

Problème : solution

La règle serait évaluée de la manière suivante :

Sur le 1er paquet (de taille 8kB), qui porte un en-tête de fichier et une partie du corps :

1. Le tampon IPS file_data est sélectionné. Le curseur pointe vers le dixième octet e1.
2. L'option de répétition rapide correspond et définit la position du curseur juste après le nombre magique, en pointant vers l'octet 7f.
3. L'option byte_jump lit deux octets de la taille du corps du fichier. Le curseur est mis à jour par ces deux octets. Ensuite, byte_jump calcule un saut de plus de 32768 octets.
4. l'évaluation de la signature avec état crée une continuation de règle, où elle a besoin de 24578 octets de plus (32768 - (8 Ko - 4 octets d'en-tête - 2 octets de la taille du corps)).
5. La règle entière ne correspond pas, car l'option byte_jump ne parvient pas à définir la position du curseur à cette distance.

Sur le 2e paquet (de taille 16kB), qui transporte la partie corps du fichier :

1. l'évaluation des signatures avec état voit la poursuite de la règle en attente.
2. Il sélectionne le tampon par son nom et voit que file_data est disponible et que la nouvelle taille de données est 16384.
3. Le curseur mis à jour indique que 8 194 octets sont toujours nécessaires (24578 - 16384)
4. La règle n'est pas reprise.

Sur le 3e paquet (de 8198 tailles), qui transporte la partie corps du fichier et les métadonnées :

1. l'évaluation des signatures avec état voit la poursuite de la règle en attente.
2. Il sélectionne le tampon par son nom et constate que file_data est disponible et que la nouvelle taille de données est 8198.
3. Le curseur mis à jour indique que la mémoire tampon contient suffisamment de données, la position du curseur est 8194.
4. l'évaluation avec état des signatures supprime la continuation de la règle.
5. l'évaluation dynamique des signatures reprend l'évaluation des règles à partir de la deuxième option de contenu, le curseur pointant sur l'octet 01.
6. L'option de contenu trouve une correspondance sur le 2e octet recherché.
7. Toute la règle finit par se déclencher.

Limitations, détails et problèmes courants

Limitations Et Autres Considérations

- En raison de l'implémentation de l'évaluation dynamique des signatures, Snort supprime toutes les continuations de règles en attente lorsqu'il recharge sa configuration. Notez que

les continuations de règle malgré leur abandon occupent toujours la mémoire Snort jusqu'à ce que le prochain bloc de données soit envoyé au module de détection.
- La fonctionnalité de latence de règle pour la règle IPS dans l'évaluation avec état fonctionne de la même manière que s'il s'agissait d'une évaluation de règle commune. Le temps d'évaluation des parties de règle sur différents blocs de données est résumé. Si la durée dépasse la limite, l'évaluation de la règle effectue un court-circuit et se termine plus tôt.
- Les opérations de bits de flux conservent leur signification, bien qu'elles fonctionnent toujours comme des options « statiques ».
  Une opération d'établissement/d'effacement/de test de bit de flux est effectuée dans un contexte connu. Ainsi, si l'option flowbit est évaluée dans une continuation de règle, elle prend en compte l'environnement actuel (bits de flux définis), et non celui où la règle a commencé son évaluation.

En outre, un rédacteur de règles doit prêter attention à l'emplacement du modèle rapide.

Même si elle peut être dans n'importe quelle partie de la règle, l'option de schéma rapide est évaluée avant la règle entière. Elle déclenche l'évaluation des règles. Pour une règle basée sur l'évaluation de la signature avec état, cela signifie que le point de continuation de la règle doit se situer après l'option fast-pattern.
En outre, l'évaluation de la règle IPS peut comporter plusieurs continuations de règle (l'une après l'autre, pas en même temps). Comme toute option du corps de la règle peut se poursuivre, elle permet à l'enregistreur de règles d'effectuer des vérifications supplémentaires à différents endroits du flux de données avec la même règle IPS.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.