Descripción de Snort 3: Stateful Signature Evaluation Byte_Jump

Contenido

Introducción

Este documento describe las nuevas técnicas añadidas en Snort 3 a partir de la versión 7.4.

Antecedentes

- El módulo de detección de Snort 3 funciona en modo de bloque. Aunque este enfoque ofrece una ventaja en cuanto a rendimiento y simplicidad en la implementación (relativamente), tiene algunas limitaciones en la detección de firmas que abarcan varios bloques de datos.
- Para facilitar la experiencia del usuario, ya se han implementado algunas mejoras en Snort, a saber:
  1. Los bits de flujo permiten que el escritor de reglas marque el flujo de red con una propiedad definida por el usuario; esa propiedad se puede establecer, borrar y probar en cualquier paquete del flujo (presenta una manera de concluir acerca de una firma más grande sobre los paquetes).
- Un módulo de flujo acumula paquetes de cable en un paquete reconstruido, que es un bloque más grande y más significativo que un paquete sin procesar; la evaluación de las

reglas IPS frente al paquete reconstruido ofrece más oportunidades de ver la imagen completa y hacer coincidir un patrón más grande (firma).
- En algunos casos, el paquete reconstruido no solo presenta datos nuevos, sino que incluye parte de los datos anteriores ya procesados por la detección; de nuevo, ese bloque de datos acumulados permite detectar firmas que se extienden hacia atrás en el flujo (hasta cierto punto).
- Un divisor de flujo corta el flujo en bloques, pero el punto de corte es potencialmente un punto débil que el atacante podría usar para evitar la detección de patrones; por lo tanto, Snort tiene un mecanismo de fluctuación implementado para hacer que la división sea más impredecible. Esto complica aún más el análisis del atacante.

Qué hay de nuevo

La evaluación de firmas con estado es una nueva técnica que se puede agregar a la lista. Amplía las capacidades de detección al habilitar la evaluación de reglas IPS en varios bloques. Por lo tanto, una regla no presenta una discordancia inmediata si el bloque actual carece de datos, sino que espera a que lleguen más datos.

Plataformas Soportadas

Plataformas mínimas de software y hardware

Versión mínima del administrador admitido	Dispositivos gestionados	Versión mínima de dispositivos administrados admitidos requerida	Notas
Management Center 7.4.0	FTD	7.4.0	Sólo Snort 3
Administrador de dispositivos 7.4.0	Cualquier FTD que admita la gestión de FDM	7.4.0	Sólo Snort 3

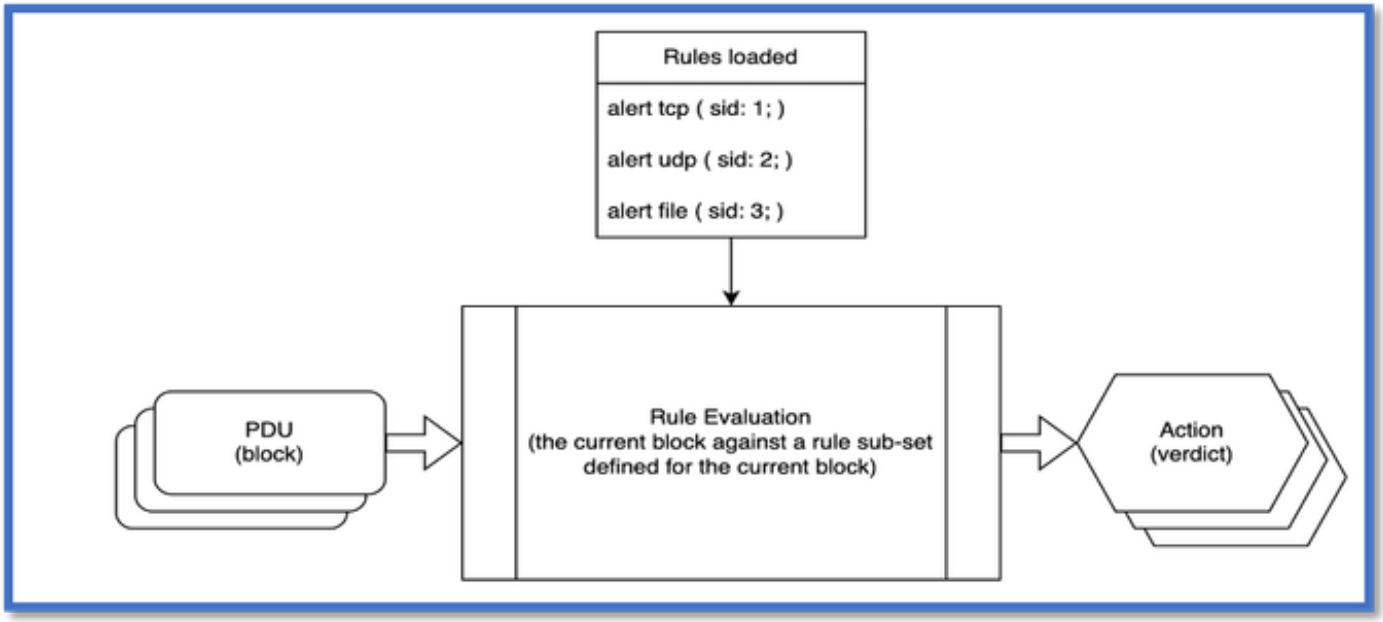
Detalles de la función

Descripción de la función funcional

¿Cómo funciona?

El flujo de trabajo del módulo de detección se representa en el diagrama. En la etapa de procesamiento del tráfico, el módulo ya tiene todas las reglas cargadas, y acepta bloques de

datos de una a una, evalúa reglas y define las acciones que se deben tomar para el bloque de evaluación de firmas con estado del proceso.



Notas sobre el régimen:

1. Una vez definido un subconjunto de reglas para el bloque de datos actual, cada regla del mismo se evalúa independientemente de las demás reglas.
2. Cada bloque de datos se evalúa independientemente de los demás bloques.
3. El bloque de datos es una abstracción para un conjunto de búferes IPS que se evalúan para el paquete actual.
4. La acción es una lista de acciones evaluadas para el paquete actual; el veredicto final se determina más adelante.

Para comprender cómo funciona la evaluación de firmas con estado, observe cómo se evalúa una regla IPS común y cómo los bloques de datos pueden formar una secuencia.

Evaluación de reglas comunes

Una regla IPS se puede presentar de la siguiente forma:

```
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 - Acción IPS en el paquete si se activa la regla

protocolo - protocolo que debe coincidir

origen, destino: dirección IP y puerto

option_1, option_2, option_3 - Opciones IPS que forman parte de la evaluación de reglas

gid, sid - un par único que identifica la regla (son como opciones de metadatos)

meta_option_1, meta_option_2, meta_option3 - metadatos de regla como un mensaje, un tipo de clase o una referencia, estas opciones no participan en la evaluación de regla.

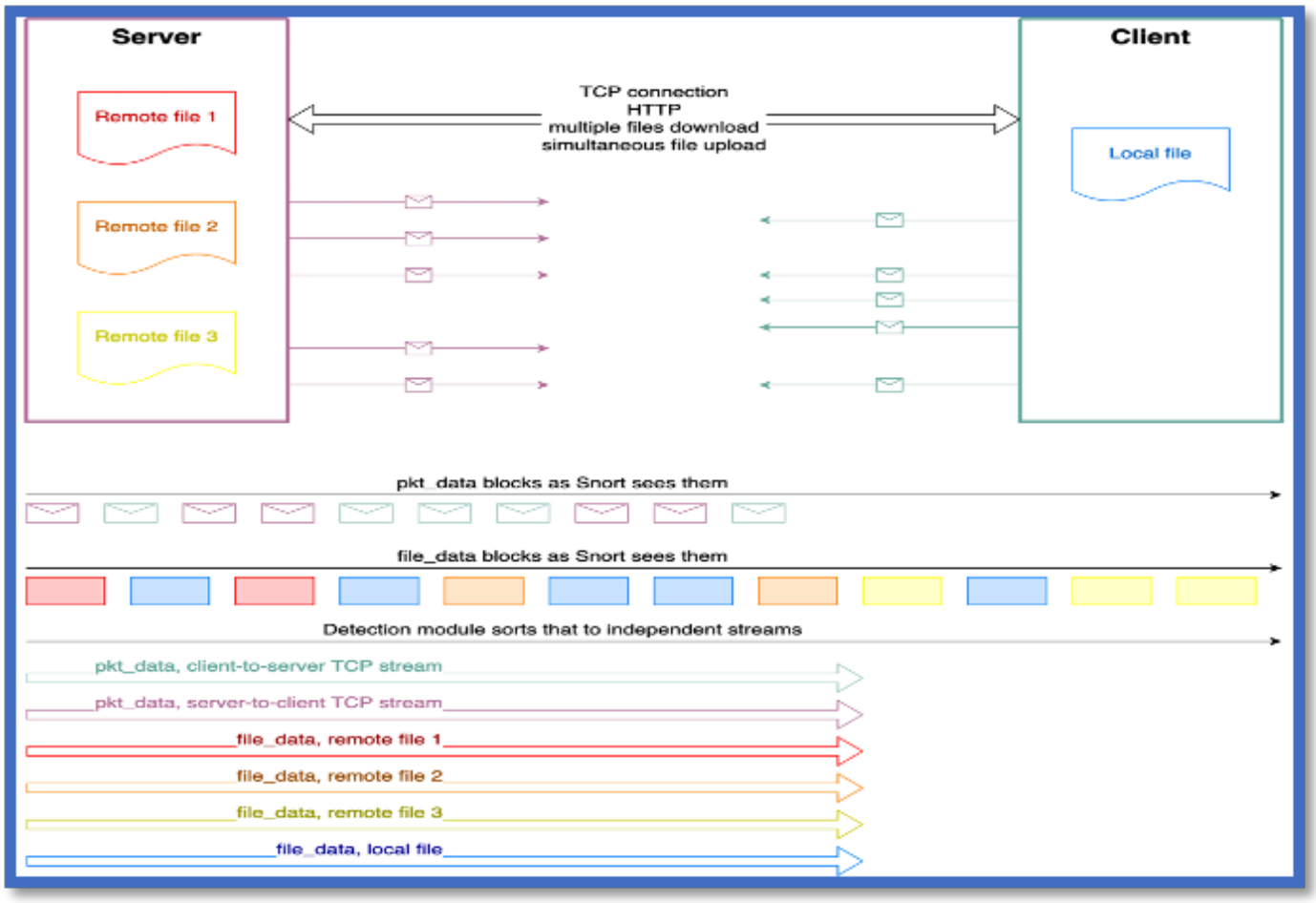
- El protocolo, el origen y el destino forman un encabezado de regla. Actúa como un filtro para un flujo de red (que se acepta para evaluación). Todo entre paréntesis es un cuerpo de regla. Las opciones IPS (excepto los metadatos de regla) del cuerpo de regla son las que se evalúan para el bloque de datos. Cumplen con estas declaraciones:
- las opciones se evalúan estrictamente de izquierda a derecha.
    1. puede ser uno de los dos tipos principales.
    2. , la opción selecciona el búfer IPS para el paquete actual.
- otros (búsqueda de patrones, operación matemática, manipulación de cursores, operación de bits de flujo)
- un cursor se utiliza para realizar un seguimiento de la posición en el búfer IPS seleccionado.

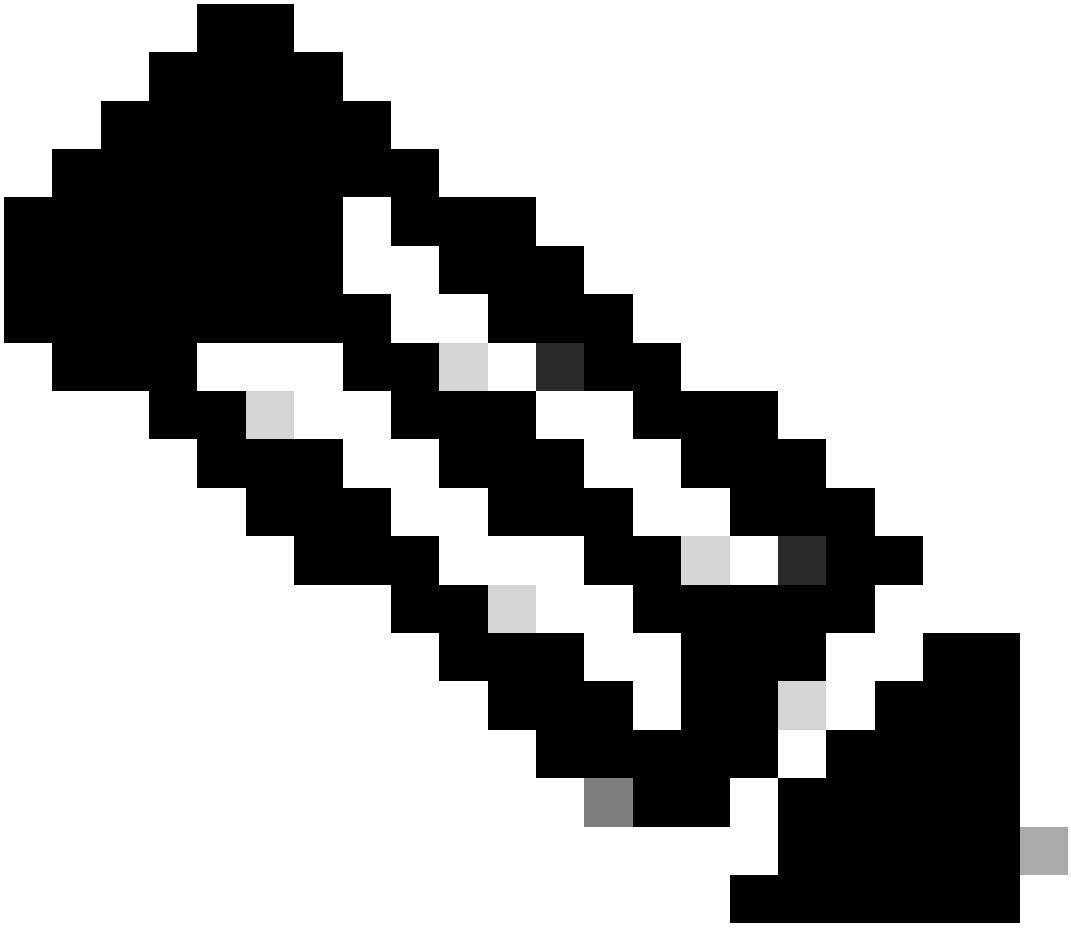
- una opción puede ser:
    1. 'absoluto', lo que significa que no depende de la posición del cursor
    2. 'relativo', lo que significa que comienza su evaluación desde la posición del cursor
- si una opción intenta sacar el cursor del búfer IPS seleccionado, se produce un error y toda la regla no coincide (debido a la falta de datos)
- El último punto es una limitación del módulo de detección. Si Snort pudiera tener recursos ilimitados, almacenaría en caché todos los datos vistos para evaluar las reglas una y otra vez cuando los datos estén disponibles (más paquetes de cable llegan).

Flujo de datos y búferes IPS

- La secuencia de datos es una secuencia de bytes en un formato contiguo desde el mismo origen. Se trata de un nuevo concepto presentado para apoyar la evaluación stateful. La evaluación de reglas entre bloques debe realizarse dentro de los mismos datos lógicos (ya sea un archivo, un flujo TCP puro o texto JavaScript).

- En general, un bloque de datos recibido por el módulo de detección podría:
    - Proceder de un búfer IPS diferente (por ejemplo, pkt_data y file_data no son iguales)
    - Pertenecer a otra corriente
    - No formar una secuencia (búferes generados a partir de un paquete sin procesar)
    - No formar una secuencia contigua (ICMP, UDP)
    - No estar en orden (respuesta parcial HTTP)
    - Contener datos repetidos (un bloque acumulado, como en http_inspect.script_detection o HTTP_Chunked Response)
- El módulo de detección puede ordenar las cosas para concatenar bloques del mismo flujo solamente; de lo contrario, el proceso de evaluación vería interferencias no deseadas de bloques de entrelazado.


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



Nota: En este ejemplo se presenta un caso en el que un cliente HTTP carga y descarga varios archivos simultáneamente.

- Actualmente, sólo dos búferes IPS pueden representar una secuencia: pkt_data y file_data, donde:
    1. pkt_data forma dos secuencias para el protocolo TCP (direcciones cliente a servidor y servidor a cliente)
    2. file_data debe formar secuencias para archivos, adjuntos MIME y otros datos de protocolo (como la página HTML HTTP u otro tipo de contenido)
- La evaluación stateful se realiza estrictamente dentro del flujo de datos.

Continuación de reglas

- La sección anterior termina con una sentencia que indica que la opción IPS no coincide si coloca el cursor fuera del búfer IPS actual. Sin embargo, cuando el búfer IPS forma un flujo de datos, la función de evaluación de firmas con estado interviene y guarda el contexto de evaluación de reglas en el objeto de flujo Snort. El contexto de evaluación (estado)

guardado se denomina continuación de regla. La evaluación de la firma con estado pospone el veredicto final de la regla hasta que haya más datos disponibles.

- La continuación de reglas tiene tres partes principales: el nombre del búfer IPS, el origen del búfer y la posición del cursor de destino (el origen del búfer es un identificador único para el flujo de datos).
- Cuando el módulo de detección procesa un bloque de datos, se llevan a cabo las siguientes acciones:
    - La evaluación de firma stateful crea una continuación de regla y la adjunta al flujo si:
        - La opción IPS (byte_jump, content, pcre o cualquier otra opción que actualice la posición del cursor) establece el cursor después del búfer IPS actual
        - El búfer IPS actual admite el flujo de datos.
        - El búfer IPS actual forma un flujo de datos en este momento.
- La evaluación de firma con estado retira la continuación de regla recién creada y la elimina del flujo si:
    - La regla IPS se ha activado en el bloque de datos actual (la regla coincide en otros lugares del bloque)
- La evaluación de firma con estado rechaza las continuaciones de regla pendientes y las elimina del flujo si:
    - El búfer IPS no forma un flujo contiguo (por ejemplo, los bloques tienen datos repetidos en ellos, o hay una brecha (se ha perdido parte de los datos o el bloque no está en orden).
- La evaluación de firmas stateful actualiza la posición del cursor de destino con nuevos datos disponibles cuando:
    - El origen de búfer de la continuación de la regla es el mismo que el origen de búfer seleccionado
    - El búfer IPS forma una secuencia contigua
- La evaluación de firma stateful devuelve la continuación de la regla al motor de reglas IPS cuando:
    1. Puntos de posición del cursor de destino dentro del búfer IPS seleccionado (lo que significa que finalmente recibió todos los datos necesarios para completar la evaluación de la regla).

Configuraciones de usuario

- Dado que las continuaciones de reglas toman memoria, Snort no puede almacenar un número ilimitado de ellas. Existe una opción de configuración para controlar el límite:
    1. Detection.max_continuations_per_flow = 1024: número máximo de continuaciones almacenadas simultáneamente en el flujo { 0:65535 }
- Cuando la evaluación de firma con estado alcanza el límite, reemplaza la continuación de regla más antigua por una nueva.
- La continuación de regla más antigua que reside en el flujo permanece allí durante demasiado tiempo, lo que significa que sigue sin cumplir una condición para reanudar la evaluación de regla.
- Además, hay muchos recuentos de clavijas disponibles para ajustar las reglas IPS (que deben ser el objetivo principal) y el límite (si es necesario):
    1. detection.cont_creations: número total de continuaciones creadas (suma)

2. detection.cont_recuperations: número total de continuaciones recuperadas (suma)
3. detection.cont_flows: número total de flujos que utilizan la continuación (suma)
4. detection.cont_evals: número total de continuaciones de condición cumplida (suma)
5. detection.cont_match: número total de continuaciones coincidentes (suma)
6. detection.cont_mismatch: número total de continuaciones no coincidentes (suma)
7. detection.cont_max_num: número máximo de continuaciones simultáneas por flujo (max)
8. detection.cont_match_distance: número total de bytes saltados por las continuaciones coincidentes (suma)
9. detection.cont_mismatch_distance: número total de bytes saltados por continuaciones no coincidentes (suma)

Resolución de problemas

La función es una mejora del proceso de detección existente, por lo que no se puede solucionar el problema de forma explícita. En caso de que se produzca algún fallo en la detección, se deben examinar las reglas, la configuración o el tráfico.

Problema de ejemplo

Problema: descripción

- Digamos que una firma tiene que verificar el comienzo del archivo y su cola al mismo tiempo.
- Por ejemplo, en un archivo de destino de esta estructura (encabezado, cuerpo, metadatos) necesitamos ver si alguno de sus metadatos tiene un valor 0.

- Bytes de archivo: e1 f3 22 03 7f ff xx xx ... xx 01 00 02 00 donde

    - e1 f3 22 03 - 4 bytes para magic number, que identifica el tipo de archivo
    - 7f ff: 2 bytes para el tamaño del cuerpo
    - xx xx ... xx - 32 kb de algunos datos
    - 01 00 02 00 - 4 bytes de metadatos, en formato tag-value (1 byte para cada uno)
- La regla IPS tendría el siguiente aspecto: archivo de alerta (file_data; content:"|e1f32203|",fast_pattern; byte_jump:2,0,relative; content:"00",inside:4, relative; sid: 1;)

    - Where

        - El protocolo de archivos garantiza que la regla acepta únicamente paquetes reconstruidos (los paquetes sin procesar no participan en la evaluación de firmas con estado)
        - La opción ‘file_data’ selecciona un buffer de datos de archivo, que puede formar una secuencia
        - La primera opción de contenido es un patrón rápido y comprueba el número mágico (si es el tipo de archivo deseado)

- la opción byte_jumping lee el tamaño del cuerpo del archivo y salta sobre el cuerpo del archivo
- La segunda opción de contenido realiza la comprobación final de los valores de metadatos, dentro de los límites de parámetros de la profundidad de búsqueda y hace que la opción sea relativa.

Problema: solución

La regla se evaluaría de esta manera:

En el primer paquete (de 8 kB de tamaño), que lleva un encabezado de archivo y una parte del cuerpo:

1. El búfer IPS file_data está seleccionado. El cursor apunta al 0º byte e1.
2. La opción de patrón rápido coincide y establece la posición del cursor justo después del número mágico, apuntando al byte 7f.
3. La opción byte_jumping lee dos bytes del tamaño del cuerpo del archivo. El cursor se actualiza con estos dos bytes. Luego byte_jump calcula un salto para más de 32768 bytes.
4. la evaluación de firmas con estado crea una continuación de regla, donde necesita 24578 bytes más (32768 - (8kB - 4 bytes de encabezado - 2 bytes de tamaño de cuerpo)).
5. Toda la regla no coincide, ya que la opción byte_jumping no puede establecer la posición del cursor tan lejos.

En el segundo paquete (de 16 kB de tamaño), que transporta la parte del cuerpo del archivo:

1. la evaluación de firma stateful ve pendiente la continuación de la regla.
2. Selecciona el búfer por su nombre y ve que file_data está disponible y que el nuevo tamaño de datos es 16384.
3. El cursor actualizado muestra que aún se necesitan 8194 bytes (24578 - 16384)
4. La regla no se reanuda.

En el tercer paquete (de 8198 tamaños), que transporta la parte del cuerpo del archivo y los metadatos:

1. la evaluación de firma stateful ve pendiente la continuación de la regla.
2. Selecciona el búfer por su nombre y ve que file_data está disponible y que el nuevo tamaño de datos es 8198.
3. El cursor actualizado muestra que el búfer tiene suficientes datos, la posición del cursor es 8194.
4. la evaluación de firma con estado elimina la continuación de la regla.
5. la evaluación de firmas con estado reanuda la evaluación de reglas desde la segunda opción de contenido con el cursor apuntando al byte 01.
6. La opción de contenido encuentra una coincidencia en el 2º byte buscado.
7. Por fin se dispara toda la regla.

Limitaciones, detalles y problemas comunes

Limitaciones Y Otras Consideraciones

- Debido a la implementación de la evaluación de firmas con estado, Snort descarta todas las continuaciones de reglas pendientes cuando recarga su configuración. Tenga en cuenta que las continuaciones de reglas a pesar de haberse caído siguen ocupando la memoria de Snort hasta que se envía el siguiente bloque de datos al módulo de detección.
- La función de latencia de regla para la regla IPS en la evaluación con estado actúa igual que si se tratara de una evaluación de regla común. Se resume el tiempo de evaluación de las partes de regla en los diferentes bloques de datos. Si el tiempo excede el límite, la evaluación de la regla realiza un cortocircuito y se cierra antes.
- Las operaciones de Flowbits conservan su significado, aunque todavía funcionan como opciones 'estáticas'.
  Se realiza una operación de conjunto/borrado/prueba de bits de flujo dentro de un contexto conocido actualmente. Por lo tanto, si la opción flowbit se evalúa en una continuación de regla, tendría en cuenta el entorno actual (conjunto flowbits), no el que existía cuando la regla comenzó su evaluación.

Además, un escritor de reglas tiene que prestar atención a la ubicación de patrón rápido.

Incluso si puede estar en cualquier parte de la regla, la opción de patrón rápido se evalúa antes que toda la regla. Activa la evaluación de reglas. Para la regla basada en la evaluación de firmas con estado, significa que el punto de continuación de la regla debe estar después de la opción de patrón rápido.
Además, la regla IPS puede tener varias continuaciones de regla en su evaluación (una tras otra, no al mismo tiempo). Dado que cualquier opción del cuerpo de la regla puede tener su continuación, permite al escritor de reglas realizar comprobaciones adicionales en diferentes lugares del flujo de datos con la misma regla IPS.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).