Fase 7 de Troubleshooting de Trayectoria de Datos de Firepower: Política de intrusiones

Contenido

Introducción

Este artículo forma parte de una serie de artículos que explican cómo resolver sistemáticamente los problemas de la ruta de datos en sistemas Firepower para determinar si los componentes de Firepower pueden estar afectando al tráfico. Consulte el artículo Descripción general para obtener información sobre la arquitectura de las plataformas Firepower y los enlaces a otros artículos de Troubleshooting de Trayectoria de Datos.

En este artículo se describe la séptima fase de la solución de problemas de la ruta de datos de Firepower, la función de política de intrusiones.

Prerequisites

- Este artículo se aplica a todas las plataformas Firepower que ejecutan una política de intrusiones La función **trace** sólo está disponible en la versión 6.2 y posteriores para la plataforma Firepower Threat Defense (FTD)
- El conocimiento de código abierto Snort es útil, aunque no es necesario Para obtener información sobre el Snort de código abierto, visite https://www.snort.org/

Solución de problemas de la fase de política de intrusiones

Uso de la herramienta "trace" para detectar caídas de políticas de intrusión (sólo FTD)

La herramienta de seguimiento de compatibilidad del sistema se puede ejecutar desde la interfaz de línea de comandos (CLI) de FTD. Esto es similar a la herramienta **firewall-motor-debug** mencionada en el artículo de la fase de la política de control de acceso, excepto que profundiza en el funcionamiento interno de Snort. Esto puede ser útil para ver si alguna regla de la política de

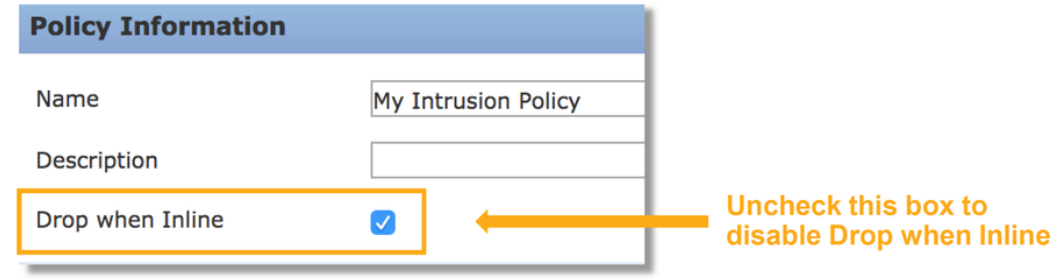
intrusiones está disparando en el tráfico interesante.

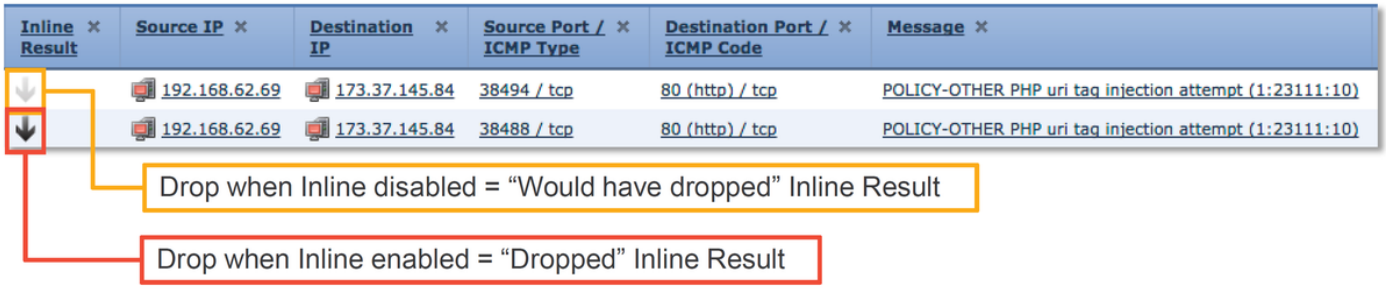
En el siguiente ejemplo, el tráfico del host con la dirección IP 192.168.62.6 está siendo bloqueado por una regla de política de intrusiones (en este caso, **1:23111**)

```
> 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
```

Observe que la acción aplicada por snort fue **descartada**. Cuando una caída es detectada por el snort, esa sesión en particular se pone en la lista negra para que también se descarten paquetes adicionales.

La razón por la que snort puede realizar la acción **drop** es que la opción "Drop when Inline" está habilitada dentro de la política de intrusiones. Esto se puede verificar en la página de inicio inicial dentro de la política de intrusiones. En Firepower Management Center (FMC), navegue hasta **Políticas > Control de acceso > Intrusión** y haga clic en el icono de edición junto a la política en cuestión.





Si se inhabilita "Drop When Inline" (Descartar cuando en línea), snort ya no descarta los paquetes ofensivos, pero sigue alertando con un **resultado en línea** de "Habría descartado" en los eventos de intrusión.

Con "Descartar cuando está en línea" inhabilitado, el resultado de seguimiento muestra una acción **descartaría** para la sesión de tráfico en cuestión.

```
> 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
```

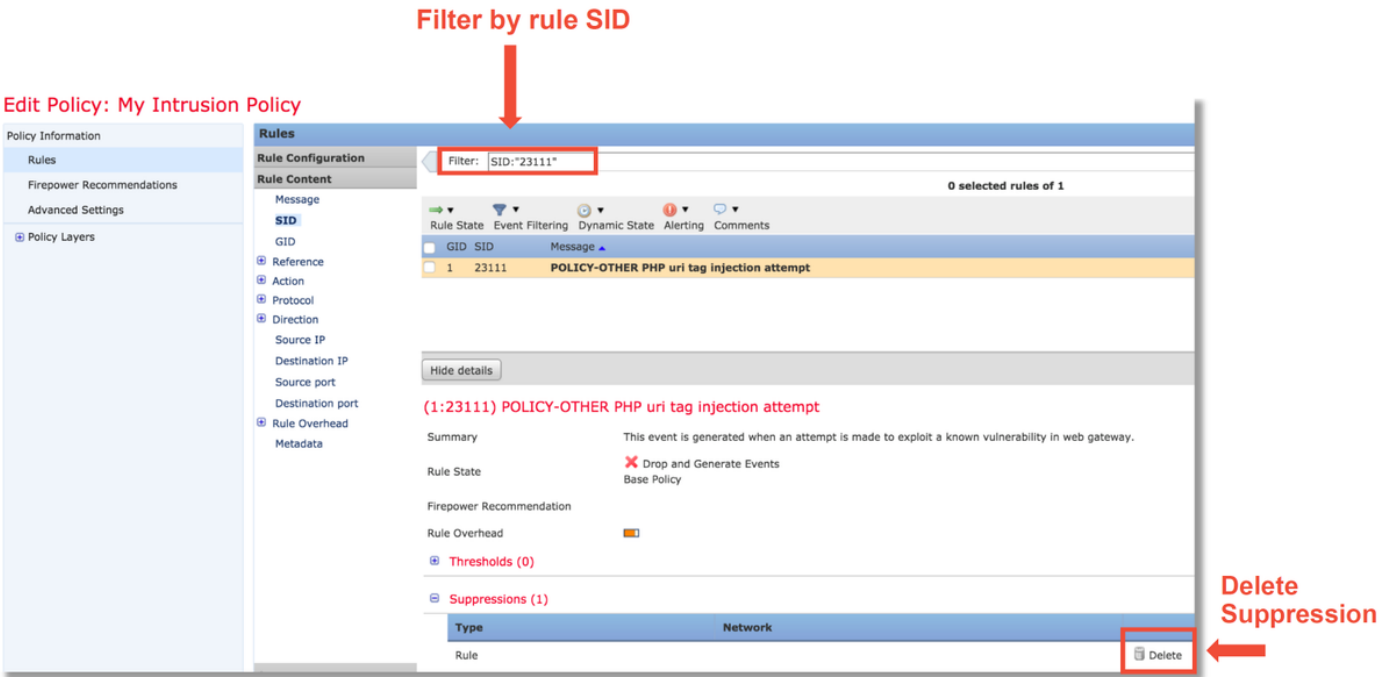
Comprobar las supresiones en las políticas de intrusión

Es posible que el snort descarte el tráfico sin enviar eventos de intrusión al FMC (caída silenciosa). Esto se logra mediante la configuración de **Supresiones.** Para verificar si se ha configurado alguna supresión en una política de intrusiones, el shell de expertos se puede verificar en el motor, como se ilustra a continuación.

```
[ 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
```

Observe que la Política de intrusiones llamada "Mi Política de intrusiones" contiene una supresión para la regla 1:2311. Por lo tanto, el tráfico puede ser descartado debido a esta regla, sin ningún evento. Esta es otra razón por la que la utilidad de seguimiento puede ser útil, ya que todavía muestra las caídas que se producen.

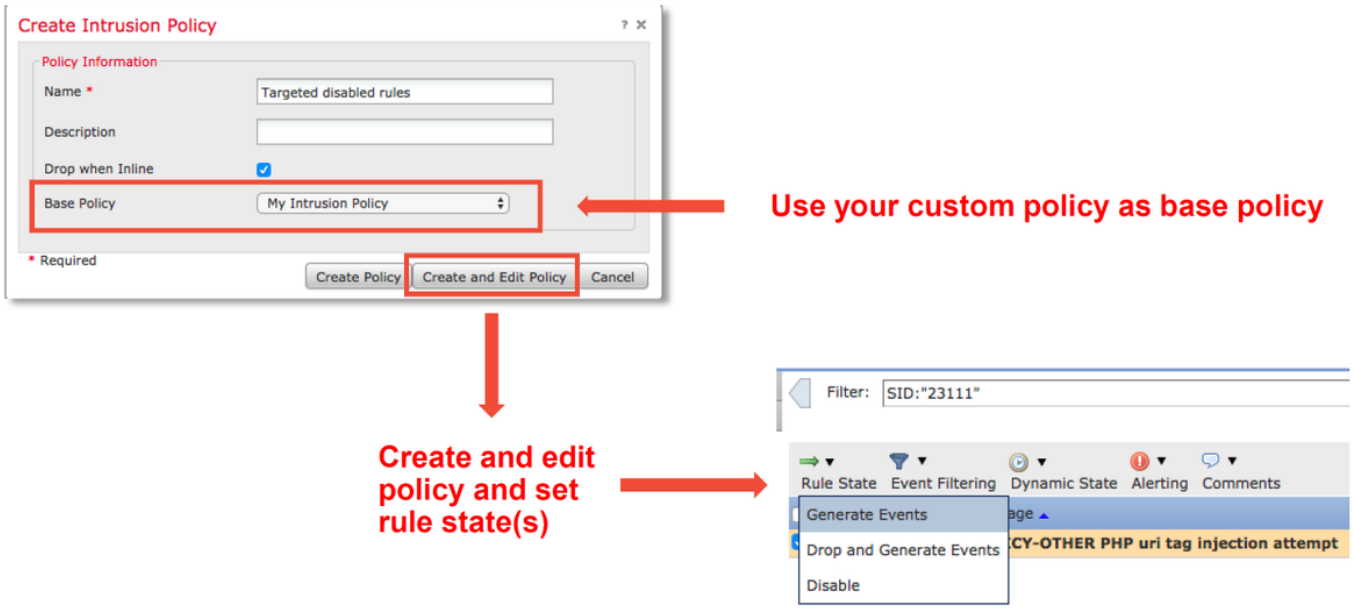
Para eliminar la supresión, la regla en cuestión se puede filtrar dentro de la vista **Reglas de** política de intrusiones. Esto muestra una opción para eliminar la supresión, como se muestra a continuación.



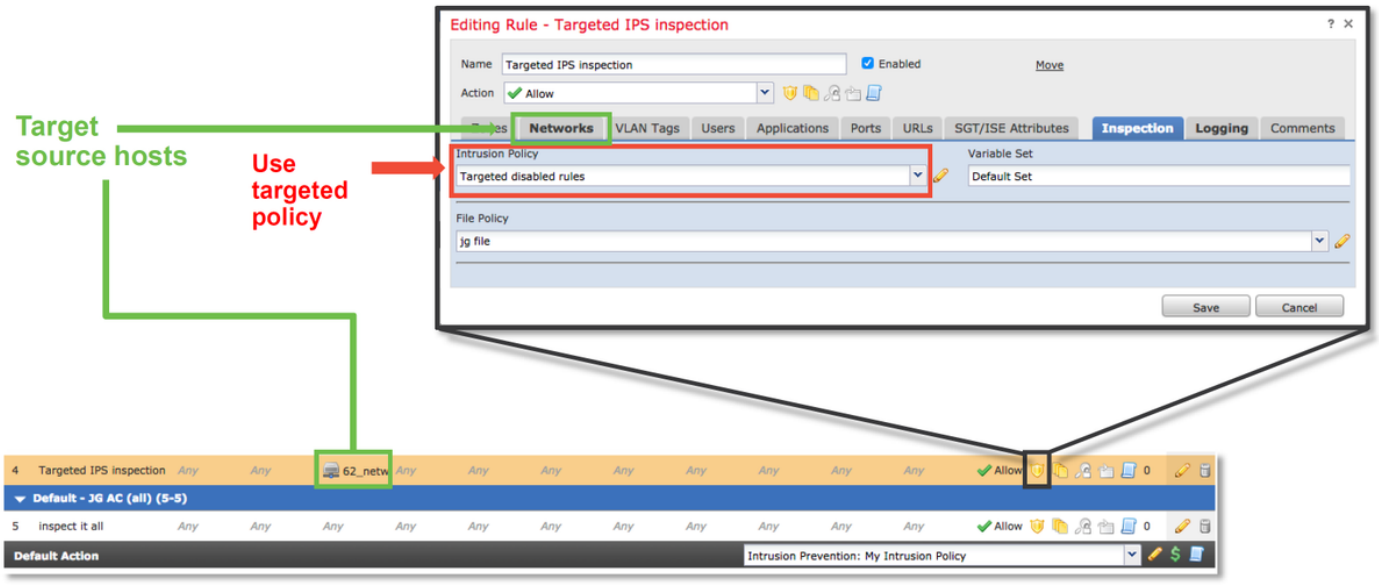
Crear una política de intrusiones dirigida

Si un tráfico está siendo descartado por una regla de política de intrusiones determinada, es posible que no desee que se descarte el tráfico en cuestión, pero es posible que tampoco desee inhabilitar la regla. La solución es crear una nueva política de intrusiones con las reglas infractoras desactivadas y luego hacer que evalúe el tráfico de los hosts objetivo.

A continuación, se muestra una ilustración de cómo crear la nueva política de intrusiones (en **Políticas > Control de acceso > Intrusión**).



Después de crear la nueva política de intrusiones, se puede utilizar dentro de una nueva regla de política de control de acceso, que se dirige a los hosts en cuestión, cuyo tráfico estaba siendo descartado previamente por la política de intrusiones original.



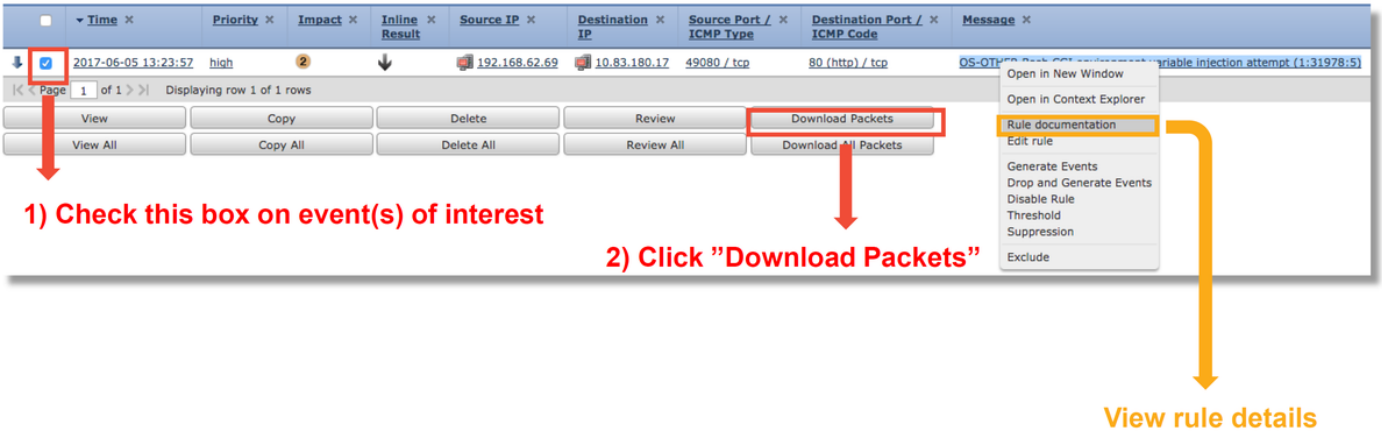
Resolución de problemas de falsos positivos

Un escenario de caso común es un análisis falso positivo para eventos de intrusión. Hay varias cosas que se pueden comprobar antes de abrir un caso de falsos positivos.

1. En la página **Vista de tabla de eventos de intrusión**, haga clic en la casilla de verificación del evento en cuestión

2. Haga clic en **Descargar paquetes** para obtener los paquetes capturados por Snort cuando se activó el evento de intrusión.

3. Haga clic con el botón derecho en el nombre de la regla en la columna **Mensaje** y, a continuación, **Documentación de Regla**, para ver la sintaxis de la regla y otra información relevante.



A continuación se muestra la sintaxis de la regla que desencadenó el evento en el ejemplo anterior. Las partes de la regla que se pueden verificar con un archivo de captura de paquetes (PCAP) descargado del FMC para esta regla se muestran en negrita.

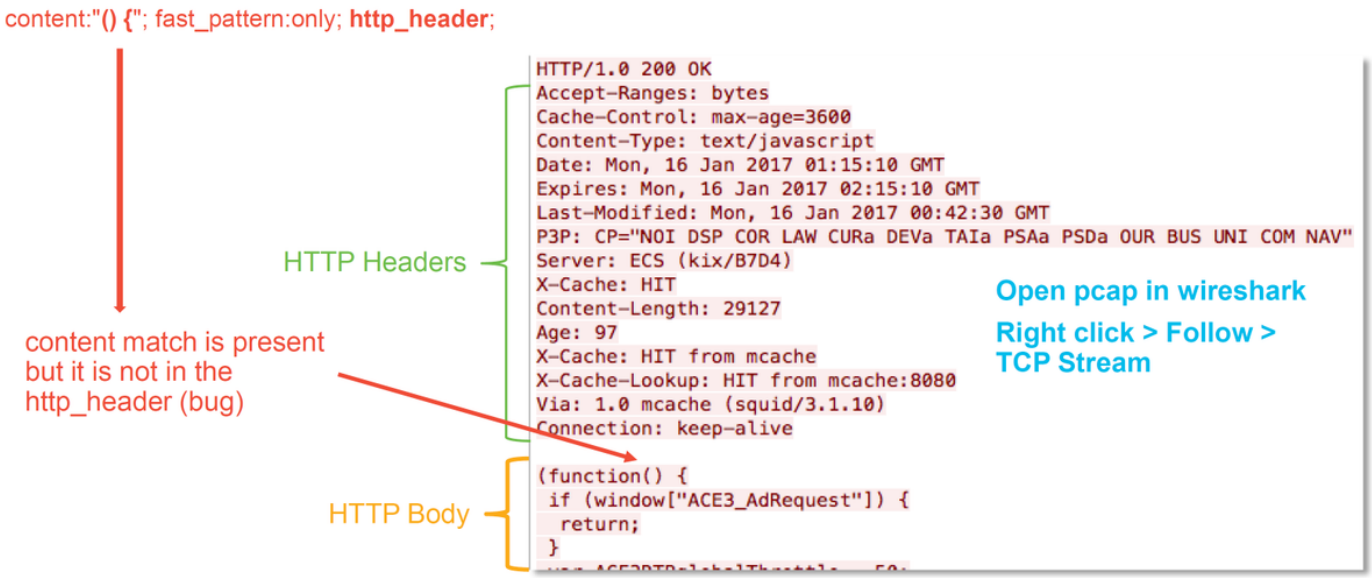
alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
(msg:"OS-OTHER Bash CGI entorno variable intento de inyección"; \
flow:to_server,establecido; \

contenido:"() {"; fast_pattern:only; http_header; \
metadatos: policy balance-ipsdrop, policy max-detect-ipsdrop, policy security-ipsdrop, comunidad de conjuntos de reglas, **service http**; \
referencia:cve,2014-6271; referencia:cve,2014-6277; referencia:cve,2014-6278; referencia:cve,2014-7169; \
tipo clásico:intento-administrador; \
sid:31978; rev:5;)

Estos pasos iniciales pueden seguirse para realizar el proceso de análisis, para ver si el tráfico debería haber coincidido con la regla que se activó.

1. Verifique la regla de control de acceso que coincide con el tráfico. Esta información se encuentra como parte de las columnas de la ficha Eventos de intrusión.
2. Busque el conjunto de variables utilizado en dicha regla de control de acceso. El conjunto de variables se puede revisar en **Objetos > Administración de objetos > Conjuntos de variables**
3. Asegúrese de que las direcciones IP del archivo PCAP coincidan con las variables (en este caso, un host incluido en la variable **$EXTERNAL_NET** que se conecta a un host incluido en la configuración de la variable **$HOME_NET**)
4. Para **flujo**, es posible que sea necesario capturar una sesión/conexión completa. Snort no capturará el flujo completo por razones de rendimiento. Sin embargo, en la mayoría de los casos, es seguro suponer que si se activa una regla con flujo:establecido, la sesión se estableció en el momento en que se activó la regla, por lo que no es necesario un archivo PCAP completo para verificar esta opción en una regla de sonido. Pero puede ser útil entender mejor la razón por la que se desencadenó.
5. Para **service http**, mire el archivo PCAP en Wireshark para ver si se parece al tráfico HTTP. Si tiene activada la detección de red para el host y ha visto la aplicación "HTTP" anteriormente, puede hacer que el servicio coincida en una sesión.

Con esta información en mente, los paquetes que se descargan del FMC pueden ser revisados en Wireshark. El archivo PCAP se puede evaluar para determinar si el evento que se activa es un falso positivo.



En la ilustración anterior, el contenido para el que la regla detecta estaba presente en el archivo PCAP - **"() {"**

Sin embargo, la regla especifica que el contenido debe ser detectado en el encabezado HTTP del paquete - **http_header**

En este caso, el contenido se encontró en el cuerpo HTTP. Por lo tanto, esto es un falso positivo. Sin embargo, no es un falso positivo en el sentido de que la regla está escrita incorrectamente. La regla es correcta y no se puede mejorar en este caso. Es probable que este ejemplo encuentre un error de Snort que está causando confusión en el búfer. Esto significa que Snort ha identificado los encabezados http_correctamente.

En este caso, puede comprobar si hay algún error de funcionamiento existente en el motor snort/IPS en la versión en la que se está ejecutando el dispositivo y, si no hay ninguno, se puede abrir un caso en el Cisco Technical Assistance Center (TAC). Las capturas de sesión completas son necesarias para investigar un problema como el que necesita el equipo de Cisco para revisar cómo Snort llegó a ese estado, que no se puede hacer con un solo paquete.

Ejemplo Verdadero Positivo

La ilustración siguiente muestra el análisis de paquetes para el mismo evento de intrusión. Esta vez, el evento es un verdadero positivo porque el contenido aparece en el encabezado HTTP.

Datos que se deben proporcionar al TAC

Datos	Instrucciones
Solución de problemas de archivo del dispositivo Firepower que inspecciona el tráfico	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn
Capturas de paquetes que se descargaron del FMC	Consulte este artículo para obtener instrucciones
Cualquier resultado relevante de CLI recopilado, como	Consulte este artículo para obtener instrucciones

resultado **de seguimiento**

Pasos siguientes

Si se ha determinado que el componente de la política de intrusiones no es la causa del problema, el siguiente paso sería solucionar el problema de la función de la política de análisis de red.

Haga clic aquí para continuar con el último artículo.