Fase 7 de solução de problemas de caminho de dados do Firepower: Política de invasão

Contents

Introduction

Este artigo faz parte de uma série de artigos que explicam como solucionar problemas sistematicamente no caminho de dados em sistemas Firepower para determinar se os componentes do Firepower podem estar afetando o tráfego. Consulte o artigo Visão geral para obter informações sobre a arquitetura das plataformas Firepower e links para outros artigos de solução de problemas de caminho de dados.

Este artigo abrange a sétima fase da solução de problemas de caminho de dados do Firepower, o recurso de política de intrusão.

Prerequisites

- Este artigo se aplica a todas as plataformas Firepower que executam uma política de intrusão O recurso **trace** só está disponível na versão 6.2 e superior para a plataforma Firepower Threat Defense (FTD)
- O conhecimento do Snort de código aberto é útil, mas não obrigatório Para obter informações sobre o Snort de código aberto, acesse https://www.snort.org/

Troubleshooting da Fase de Política de Invasão

Usando a ferramenta "trace" para detectar quedas de política de intrusão (somente FTD)

A ferramenta de rastreamento de suporte do sistema pode ser executada a partir da CLI (Command Line Interface, interface de linha de comando) do FTD. Isso é semelhante à ferramenta **firewall-engine-debug** mencionada no artigo da fase de Política de controle de acesso, exceto que se aprofunda no funcionamento interno do Snort. Isso pode ser útil para ver se alguma

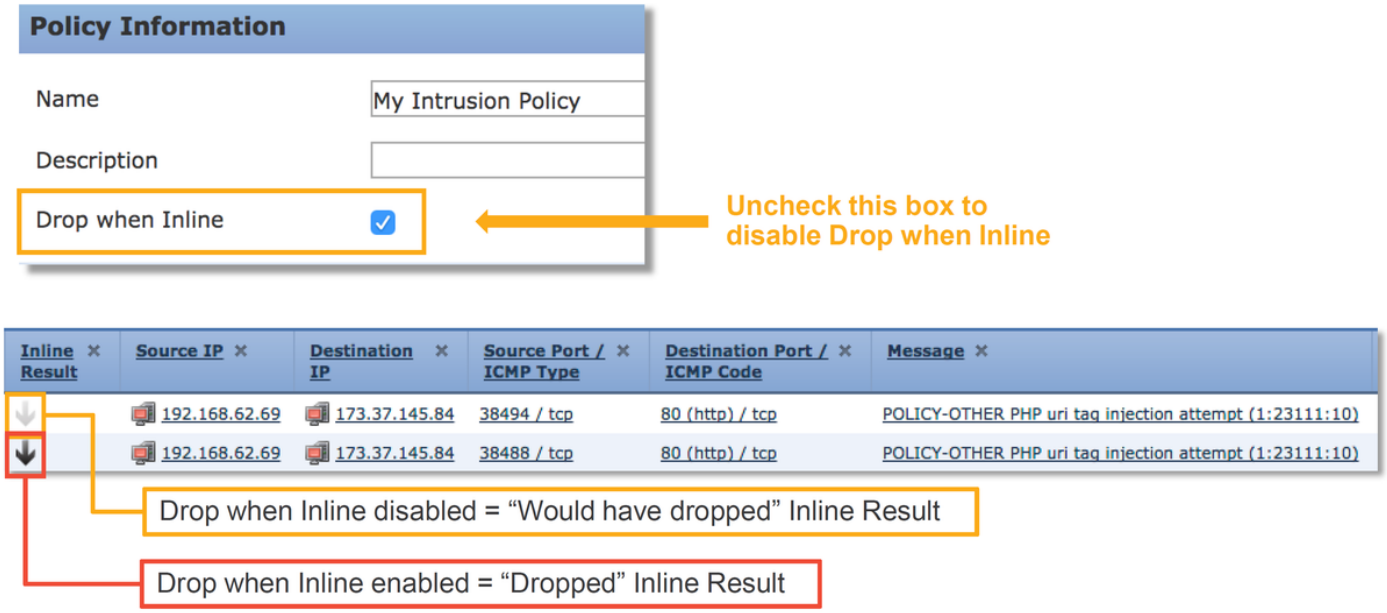
regra da política de intrusão está disparando no tráfego interessante.

No exemplo abaixo, o tráfego do host com o endereço IP 192.168.62.6 está sendo bloqueado por uma regra de política de intrusão (nesse 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 a ação aplicada pelo snort foi **suspensa**. Quando uma queda é detectada pelo snort, essa sessão específica é então colocada na lista negra para que todos os pacotes adicionais também sejam descartados.

O motivo pelo qual o snort pode executar a ação **drop** é que a opção "Drop when Inline" está habilitada na Política de intrusão. Isso pode ser verificado na página inicial da Política de intrusão. No Firepower Management Center (FMC), navegue até **Policies > Access Control > Intrusion (Políticas > Controle de acesso > Intrusão)** e clique no ícone de edição ao lado da política em questão.



Se "Drop When Inline" estiver desabilitado, o snort não descartará mais pacotes ofensivos, mas ainda alertas com um **Resultado em Linha** de "Teria Descartado" nos Eventos de Intrusão.

Com "Drop When Inline" desabilitado, a saída de rastreamento mostra uma **queda** da ação para a sessão de tráfego em questão.

```
> 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
```

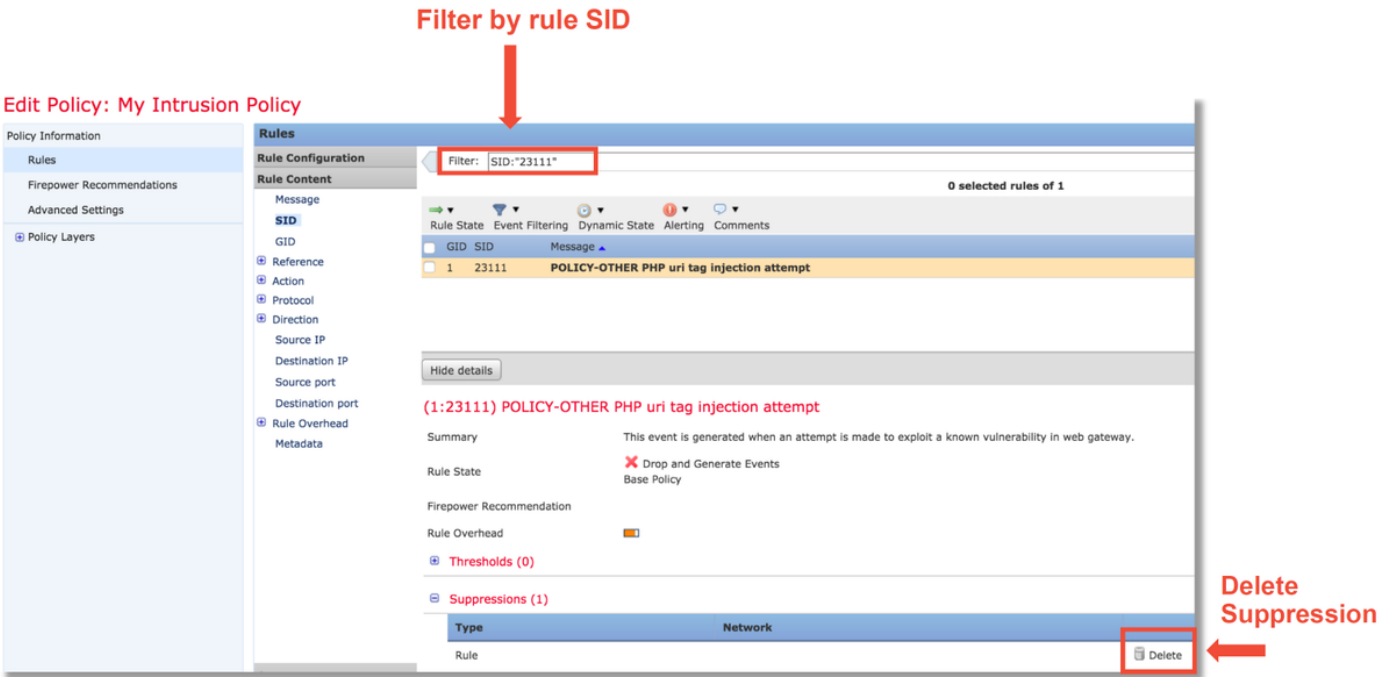
Verifique se há supressões nas políticas de intrusão

Épossível que o snort descarte o tráfego sem enviar Eventos de Intrusão ao FMC (descarte silencioso). Isso é feito configurando-se **Supressões.** Para verificar se alguma supressão foi configurada em uma política de intrusão, o shell do especialista pode ser verificado no back-end, como ilustrado abaixo.

```
[ 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 a Política de intrusão chamada "Minha política de intrusão" contém uma supressão para a regra 1:23111. Portanto, o tráfego pode ser descartado devido a essa regra, sem nenhum evento. Essa é outra razão pela qual o utilitário de rastreamento pode ser útil, pois ainda mostra as quedas ocorrendo.

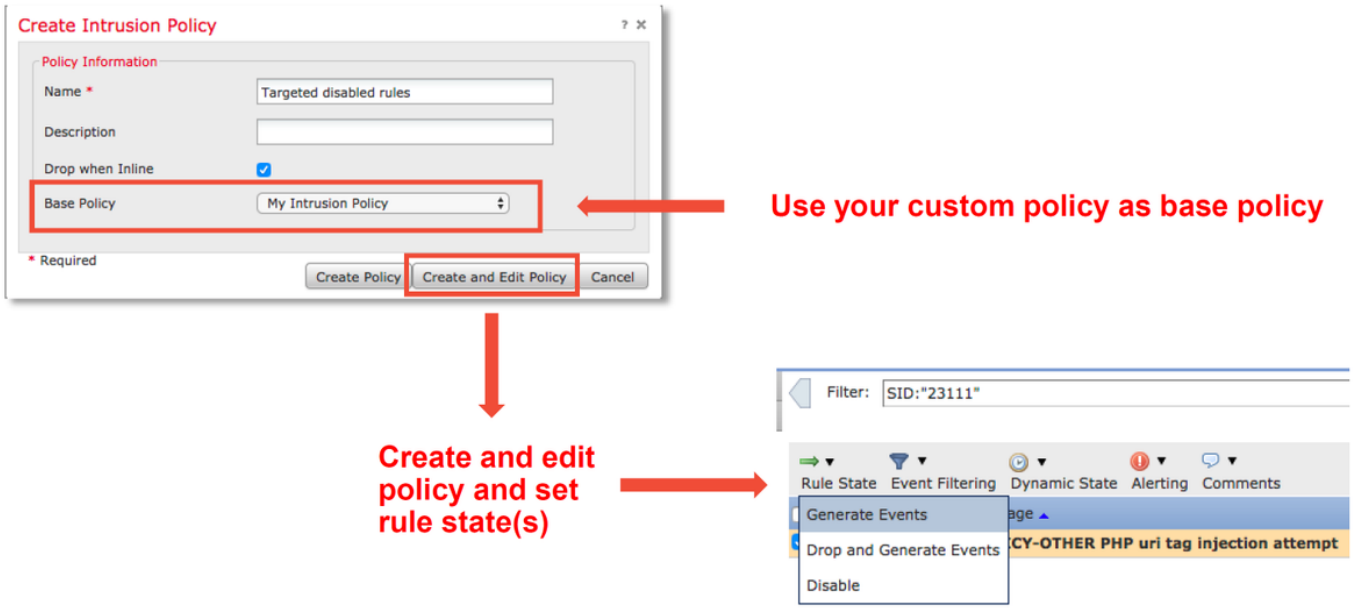
Para excluir a supressão, a regra em questão pode ser filtrada na exibição **Regras** da política de intrusão. Isso exibe uma opção para excluir a supressão, como mostrado abaixo.



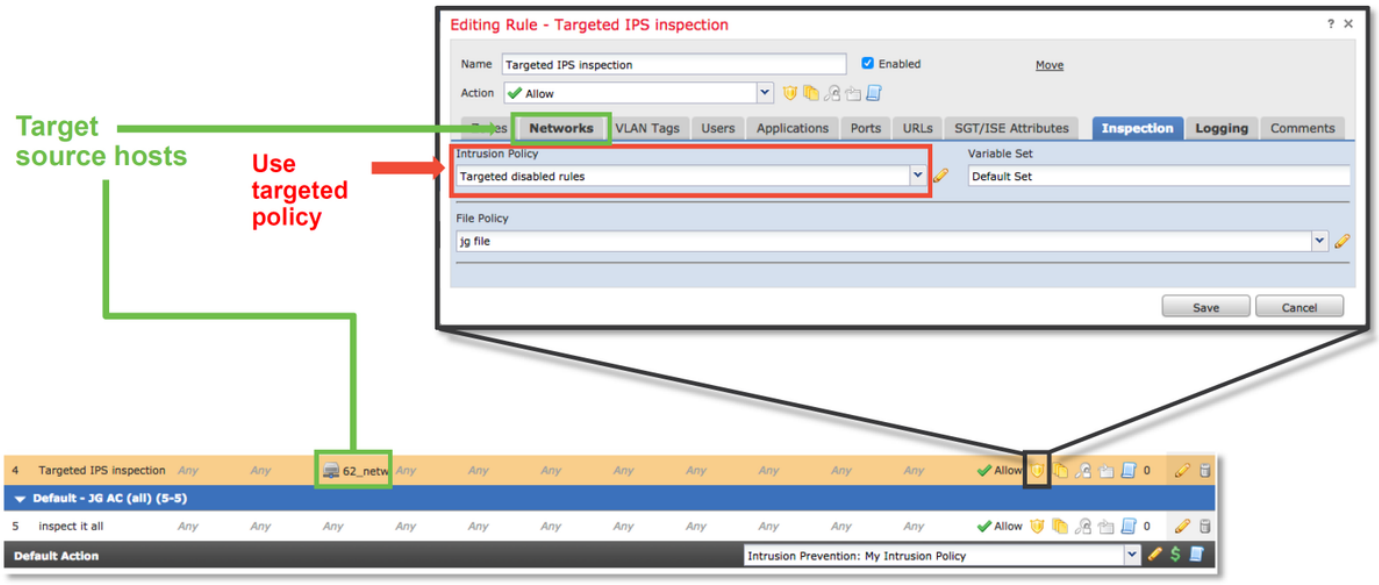
Criar uma política de invasão direcionada

Se o tráfego estiver sendo descartado por uma regra de política de intrusão específica, talvez você não queira que o tráfego em questão seja descartado, mas também não queira desabilitar a regra. A solução é criar uma nova política de intrusão com as regras ofensivas desativadas e, em seguida, fazer com que ela avalie o tráfego dos hosts de destino.

Aqui está uma ilustração de como criar a nova política de intrusão (em **Políticas > Controle de acesso > Intrusão**).



Depois de criar a nova política de intrusão, ela pode ser usada dentro de uma nova regra de política de controle de acesso, que visa os hosts em questão, cujo tráfego estava sendo anteriormente descartado pela política de intrusão original.



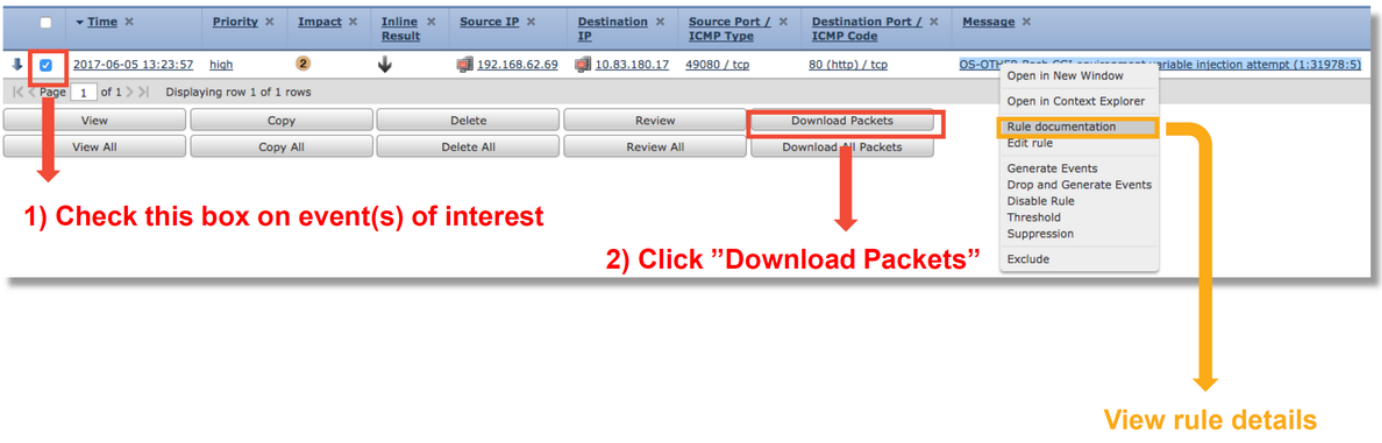
Troubleshooting Falso Positivo

Um cenário de caso comum é uma análise positiva falsa para Eventos de Intrusão. Há várias coisas que podem ser verificadas antes de se abrir um caso falso positivo.

1. Na página **Exibição da Tabela de Eventos de Invasão**, clique na caixa de seleção do evento em questão

2. Clique em **Download Packets** para obter os pacotes capturados pelo Snort quando o evento de intrusão foi disparado.

3. Clique com o botão direito do mouse no nome da regra na coluna **Mensagem** e, em seguida, na **Documentação da Regra**, para ver a sintaxe da regra e outras informações relevantes.



Abaixo está a sintaxe da regra que disparou o evento no exemplo acima. As partes da regra que podem ser verificadas em relação a um arquivo de captura de pacote (PCAP) baixado do FMC para esta regra estão em negrito.

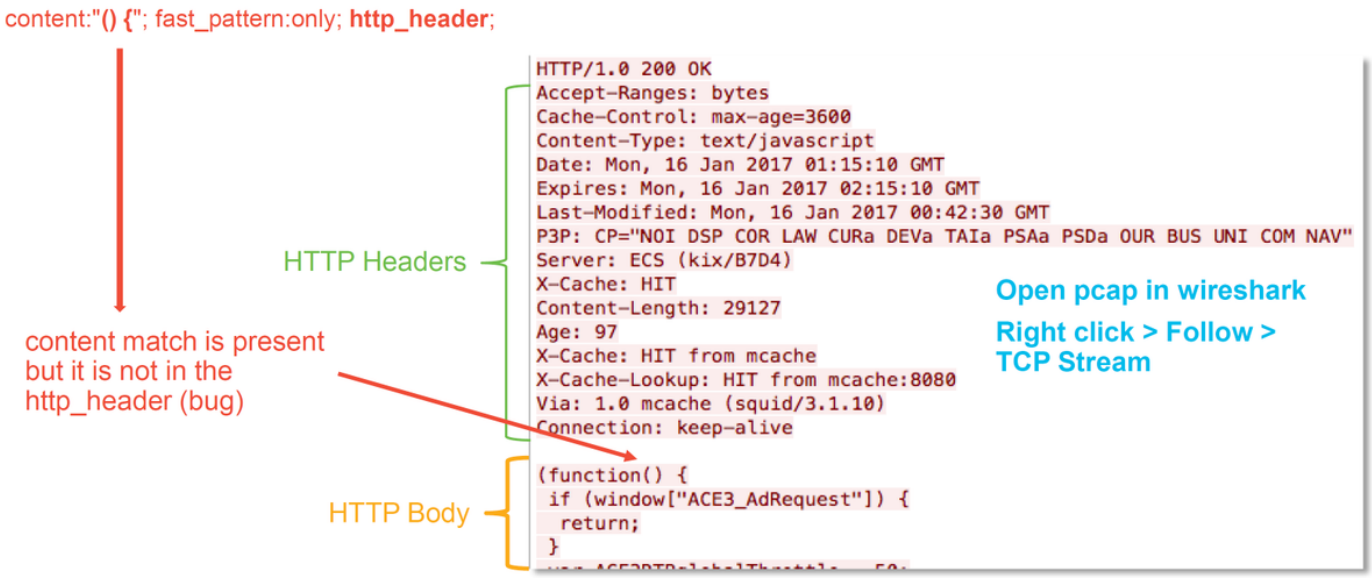
alert **tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS** \
msg:"OS-other Bash CGI environment variable inflation try"; \
fluxo:para_servidor,estabelecido; \
conteúdo:"() {"; fast_pattern:only; http_header; \

metadados:policy balance-ipsdrop, policy max-detect-ipsdrop, policy security-ipsdrop, ruleset community, **service http**; \
referência:cve,2014-6271; referência:cve,2014-6277; referência:cve,2014-6278; referência:cve,2014-7169; \
classtype:tentativa-admin; \
sid:31978; rev: 5;)

Essas etapas iniciais podem ser seguidas para executar o processo de análise, para ver se o tráfego deve corresponder à regra que disparou.

1. Verifique a regra de controle de acesso em que o tráfego correspondeu. Essas informações são encontradas como parte das colunas na guia Eventos de intrusão.
2. Localize o conjunto de variáveis usado na regra de controle de acesso. O conjunto de variáveis pode ser revisado em **Objetos > Gerenciamento de objetos > Conjuntos de variáveis**
3. Certifique-se de que os endereços IP no arquivo PCAP correspondam às variáveis (neste caso, um host incluído na variável **$EXTERNAL_NET** conectando-se a um host incluído na configuração da variável **$HOME_NET**)
4. Para **fluxo**, pode ser necessário capturar uma sessão/conexão completa. O Snort não capturará o fluxo completo devido a razões de desempenho. No entanto, na maioria dos casos, é seguro supor que se uma regra com fluxo:estabelecido disparado, a sessão foi estabelecida no momento em que a regra foi acionada, de modo que um arquivo PCAP completo não é necessário para verificar essa opção em uma regra de snort. Mas pode ser útil entender melhor a razão pela qual foi acionado.
5. Para **service http**, verifique o arquivo PCAP no Wireshark para ver se ele se parece com o tráfego HTTP. Se você tiver a descoberta de rede habilitada para o host e ele tiver visto o aplicativo "HTTP" antes, ele poderá fazer com que o serviço corresponda em uma sessão.

Com essas informações em mente, o(s) pacote(s) baixado(s) do FMC pode(m) ser revisado(s) no Wireshark. O arquivo PCAP pode ser avaliado para determinar se o evento disparado é um falso positivo.



Na ilustração acima, o conteúdo para o qual a regra detecta estava presente no arquivo PCAP - **"() {"**

No entanto, a regra especifica que o conteúdo deve ser detectado no cabeçalho HTTP do pacote - **http_header**

Nesse caso, o conteúdo foi encontrado no corpo HTTP. Portanto, isso é falso positivo. No entanto, não é um falso positivo no sentido de que a regra está escrita incorretamente. A regra está correta e não pode ser melhorada neste caso. Este exemplo provavelmente está encontrando um bug Snort que está causando confusão no buffer do snort. Isso significa que o Snort identificou os http_headers incorretamente.

Nesse caso, você pode verificar se há bugs existentes para o mecanismo snort/IPS na versão em que seu dispositivo está sendo executado e, se não houver nenhum, um caso com o Cisco Technical Assistance Center (TAC) pode ser aberto. Capturas completas de sessão são necessárias para investigar um problema como o grupo da Cisco precisa revisar como o Snort entrou nesse estado, o que não pode ser feito com um único pacote.

Exemplo positivo real

A ilustração abaixo mostra a análise de pacotes para o mesmo Evento de Intrusão. Desta vez, o evento é um verdadeiro positivo porque o conteúdo aparece no cabeçalho HTTP.

Dados a fornecer ao TAC

Dados	Instruções
Solucionar problemas do dispositivo Firepower que inspeciona o tráfego	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn
Capturas de pacotes que foram baixadas do FMC	Consulte este artigo para obter instruções
Qualquer saída de CLI relevante coletada, como a saída **de rastreamento**	Consulte este artigo para obter instruções

Próximas etapas

Se for determinado que o componente de política de intrusão não é a causa do problema, a próxima etapa será solucionar o problema do recurso de política de análise de rede.

Clique aqui para prosseguir para o último artigo.