Entenda o Snort 3: Avaliação de Assinatura Stateful Byte_Jump

Contents

Introdução

Este documento descreve as novas técnicas adicionadas no Snort 3 a partir de 7.4.

Informações de Apoio

- O módulo de detecção do Snort 3 funciona no modo de bloqueio. Embora essa abordagem ofereça uma vantagem de desempenho e simplicidade de implementação (relativamente), ela tem algumas limitações na detecção de assinaturas que abrangem vários blocos de dados.
- Para facilitar a experiência do usuário, algumas melhorias já foram implementadas no Snort, a saber:
  1. Os bits de fluxo permitem que o gerador de regras marque o fluxo de rede com uma propriedade definida pelo usuário; essa propriedade poderia ser definida, limpa e testada em qualquer pacote do fluxo (apresenta uma forma de concluir sobre uma assinatura maior em pacotes).
- Um módulo de fluxo acumula pacotes de fios em um pacote reconstruído, que é um bloco maior e mais significativo do que um pacote bruto; avaliar as regras de IPS em relação ao

pacote reconstruído dá mais chances de ver a imagem inteira e corresponder a um padrão maior (assinatura).
- Em alguns casos, o pacote reconstruído apresenta não apenas novos dados, mas inclui alguma parte dos dados anteriores já processados pela detecção; novamente, esse bloco de dados acumulados permite que as assinaturas que se estendem para trás no fluxo (até certo ponto) sejam detectadas.
- Um divisor de fluxo corta o fluxo em blocos, mas o ponto de corte é potencialmente um ponto fraco que o invasor poderia usar para evitar a detecção de padrões; assim, o Snort tem um mecanismo de jittering implementado para tornar a divisão mais imprevisível. Isso complica ainda mais a análise do invasor.

O que há de novo

A avaliação de assinatura stateful é uma nova técnica que pode ser adicionada à lista. Estende os recursos de detecção ativando a avaliação de regras de IPS para vários blocos. Assim, uma regra não é incompatível imediatamente se o bloco atual não tiver dados, mas, em vez disso, espera a chegada de mais dados.

Plataformas suportadas

Plataformas mínimas de software e hardware

Mín. de Versão do Gerenciador com Suporte	Dispositivos gerenciados	Mín. de Dispositivos Gerenciados com Suporte Versão Necessária	Notas
Centro de gerenciamento 7.4.0	FTD	7.4.0	Somente Snort 3
Gerenciador de dispositivos 7.4.0	Qualquer FTD que suporte o gerenciamento do FDM	7.4.0	Somente Snort 3

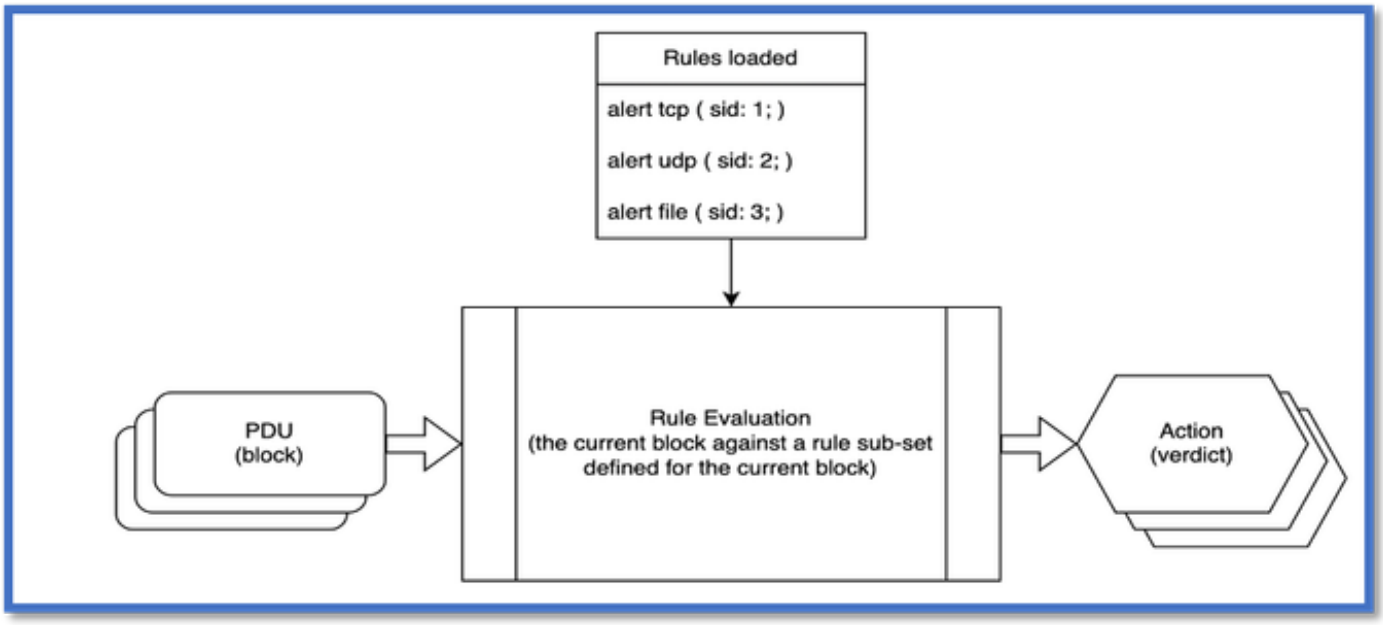
Detalhes do recurso

Descrição do recurso funcional

Como isso funciona?

O fluxo de trabalho do módulo de detecção é descrito no diagrama. No estágio de processamento

de tráfego, o módulo já tem todas as regras carregadas e aceita blocos de dados de uma forma individual, avalia regras e define as ações a serem tomadas para o bloco de avaliação de assinatura stateful do processo.



Notas sobre o regime:

1. Quando um subconjunto de regras é definido para o bloco de dados atual, cada regra dele é avaliada independentemente de outras regras.
2. Cada bloco de dados é avaliado independentemente de outros blocos.
3. O bloco de dados é uma abstração para um conjunto de buffers de IPS que são avaliados para o pacote atual.
4. Ação é uma lista de ações avaliadas para o pacote atual; o veredito final é determinado posteriormente.

Para entender como funciona a avaliação de assinatura stateful, observe como uma regra IPS comum é avaliada e como os blocos de dados podem formar um fluxo.

Avaliação de regra comum

Uma regra de IPS pode ser apresentada desta 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 - Ação de IPS no pacote se a regra for acionada

protocol - protocolo a corresponder

origem, destino - endereço IP e porta

option_1, option_2, option_3 - opções de IPS que fazem parte da avaliação da regra

gid, sid - um par exclusivo que identifica a regra (são como opções de metadados)

meta_option_1, meta_option_2, meta_option3 - metadados de regra como uma mensagem, um tipo de classe ou uma referência, essas opções não participam da avaliação da regra.

- Protocolo, origem e destino formam um cabeçalho de regra. Ele atua como um filtro para um fluxo de rede (que deve ser aceito para avaliação). Tudo entre parênteses é um corpo de regras. As opções de IPS (exceto os metadados da regra) do corpo da regra são as que são avaliadas para o bloco de dados. Eles estão em conformidade com estas declarações:
- as opções são avaliadas estritamente na ordem da esquerda para a direita.
    1. pode ser um dos dois tipos principais.
    2. definidor de buffer, a opção seleciona o buffer de IPS para o pacote atual.
- outros (pesquisa por padrão, operação matemática, manipulação de cursor, operação de fluxo de bits)
- um cursor é usado para controlar a posição no buffer IPS selecionado.

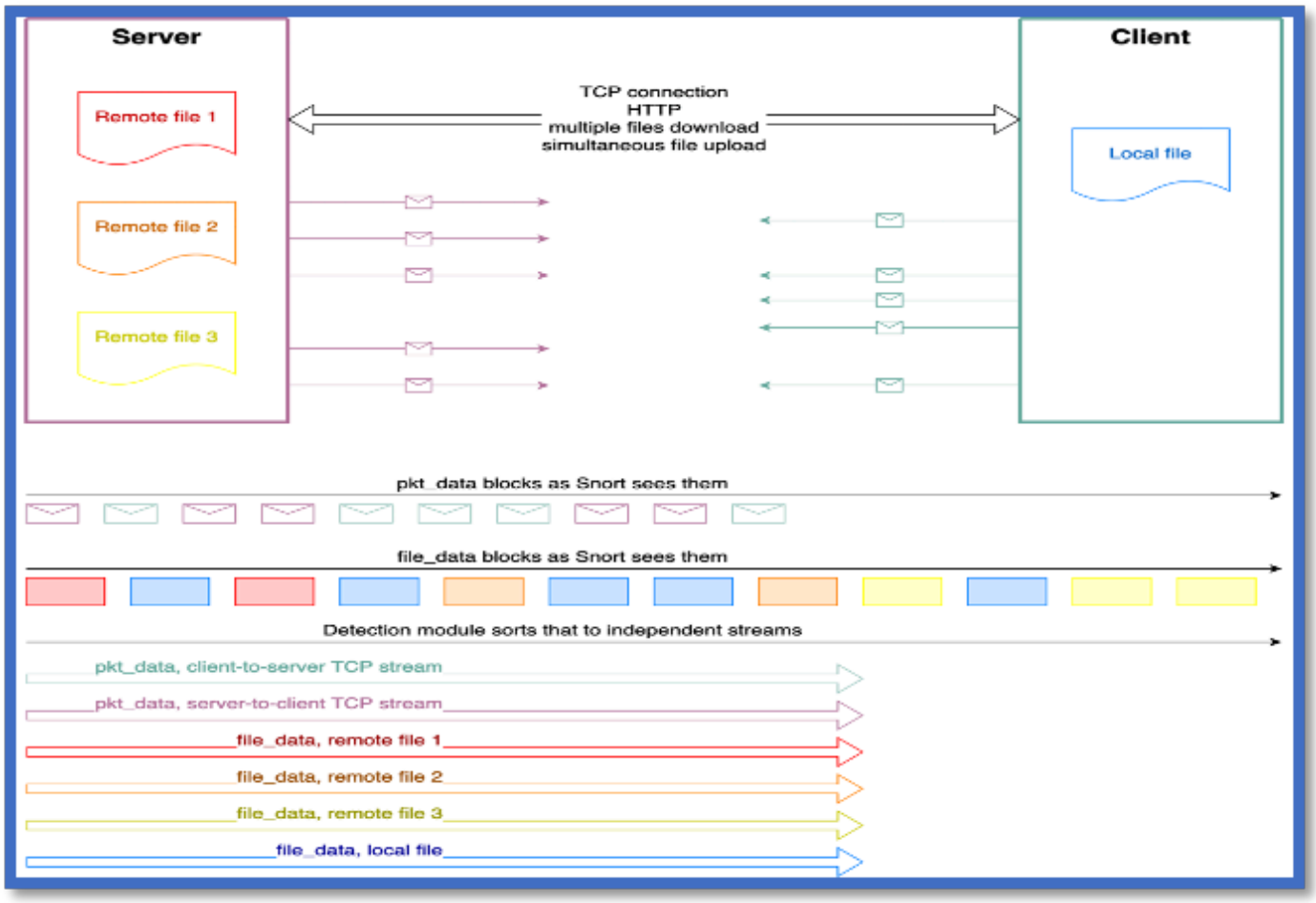
- uma opção pode ser:
    1. 'absolute', que significa que não depende da posição do cursor
    2. 'relative', o que significa que inicia sua avaliação a partir da posição do cursor
- se uma opção tentar retirar o cursor do buffer de IPS selecionado, ela falhará e a regra inteira será incompatível (devido à falta de dados)
- O último ponto é uma limitação do módulo de detecção. Se o Snort pudesse ter recursos ilimitados, ele armazenaria em cache todos os dados vistos para avaliar as regras repetidamente quando os dados se tornassem disponíveis (mais pacotes de fios chegavam).

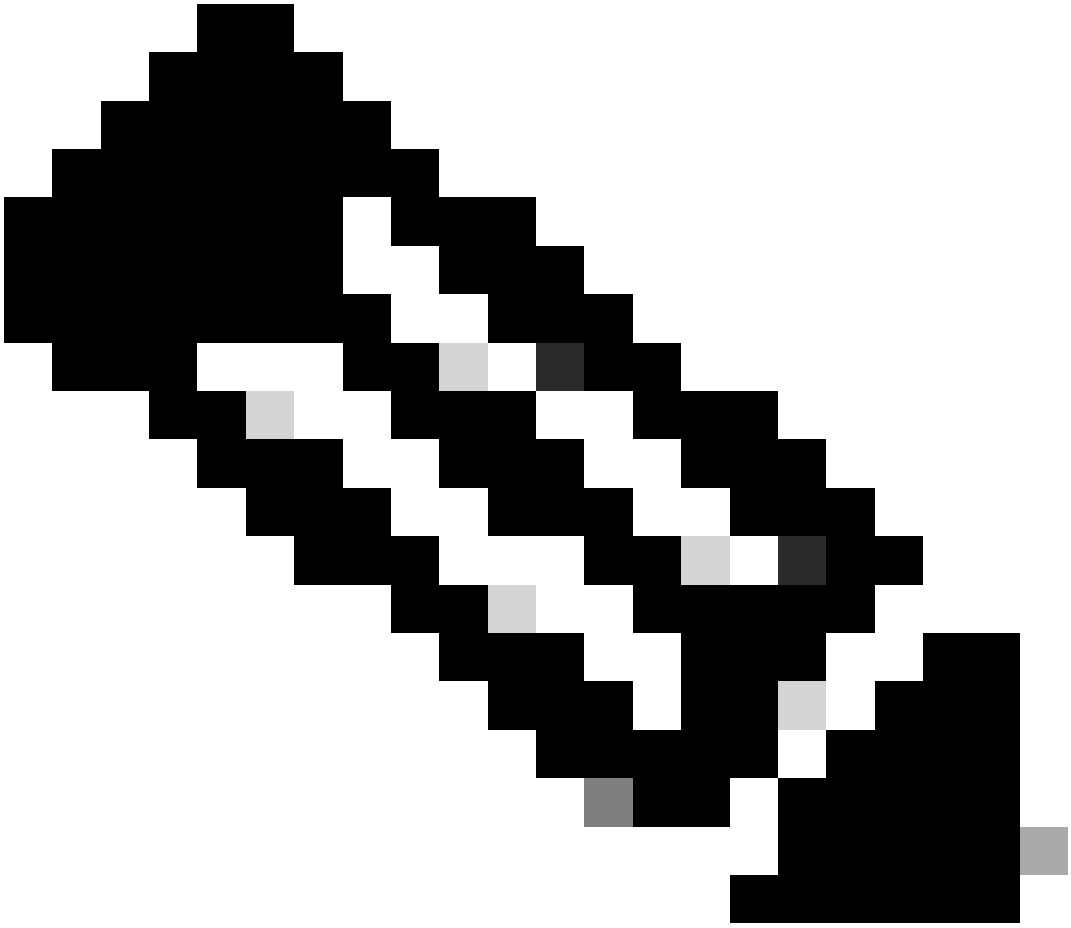
Buffers de Fluxo de Dados e IPS

- O fluxo de dados é um fluxo de bytes em um formato contíguo da mesma origem. É um novo conceito apresentado para apoiar a avaliação stateful. A avaliação de regras entre blocos deve ser feita dentro dos mesmos dados lógicos (seja um arquivo, fluxo TCP puro ou texto JavaScript).

- Em geral, um bloco de dados recebido pelo módulo de detecção pode:
    - Ser de um buffer de IPS diferente (por exemplo, pkt_data e file_data não são os mesmos)
    - Pertencer a outro fluxo
    - Não formar um fluxo (buffers gerados a partir de um pacote bruto)
    - Não formar um fluxo contíguo (ICMP, UDP)
    - Não estar em ordem (Resposta Parcial HTTP)
    - Contêm dados repetidos (um bloco acumulado, como em http_inspect.script_detection ou em Resposta em Bloco HTTP)
- O módulo de detecção pode classificar as coisas para concatenar blocos do mesmo fluxo

apenas, caso contrário, o processo de avaliação veria interferência indesejada de blocos de intercalação.





Observação: o exemplo aqui apresenta um caso em que um cliente HTTP faz upload e download de vários arquivos simultaneamente.

- Atualmente, apenas dois buffers de IPS podem representar um fluxo: pkt_data e file_data, onde:
    1. pkt_data forma dois fluxos para o protocolo TCP (direções cliente-servidor e servidor-cliente)
    2. file_data deve formar fluxos para arquivos, anexos MIME e outros dados de protocolo (como página HTML HTTP e/ou outro tipo de conteúdo)
- A avaliação stateful é feita estritamente dentro do fluxo de dados.

Continuação da regra

- A seção anterior termina com uma instrução de que a opção IPS não corresponde se definir o cursor fora do buffer IPS atual. Mas quando o buffer de IPS forma um fluxo de dados, o recurso de avaliação de assinatura stateful entra em cena e salva o contexto de avaliação da regra no objeto de fluxo Snort. O contexto (estado) de avaliação salvo é chamado de

continuação de regra. A avaliação de assinatura stateful adia o veredito final da regra até que mais dados fiquem disponíveis.

- A continuação da regra tem três partes principais: nome do buffer IPS, origem do buffer e posição do cursor de destino (a origem do buffer é um identificador exclusivo para o fluxo de dados).
- Quando um bloco de dados é processado pelo módulo de detecção, as ações subsequentes ocorrem:-
    - A avaliação de assinatura stateful cria uma continuação de regra e a anexa ao fluxo se:
        - A opção IPS (byte_jump, content, pcre ou qualquer outra coisa que atualize a posição do cursor) define o cursor após o buffer IPS atual
        - O buffer IPS atual suporta o fluxo de dados.
        - O buffer de IPS atual forma um fluxo de dados no momento.
- A avaliação de assinatura stateful retira a continuação de regra recém-criada e a remove do fluxo se:
    - A regra de IPS foi acionada no bloco de dados atual (a regra corresponde a outros locais do bloco)
- A avaliação de assinatura stateful rejeita as continuações de regra pendentes e as remove do fluxo se:
    - O buffer de IPS não forma um fluxo contíguo (por exemplo, os blocos têm dados repetidos neles ou há uma lacuna (parte dos dados foi perdida ou o bloco não está em ordem).
- A avaliação de assinatura stateful atualiza a posição do cursor com novos dados disponíveis quando:
    - A origem de buffer da continuação da regra é igual à origem de buffer selecionada
    - O buffer de IPS forma um fluxo contíguo
- A avaliação de assinatura stateful envia a continuação da regra de volta ao mecanismo de regras do IPS quando:
    1. Pontos de posição do cursor direcionados dentro do buffer IPS selecionado (o que significa que ele finalmente recebeu todos os dados necessários para concluir a avaliação da regra).

Configurações do usuário

- Como as continuações de regras consomem memória, o Snort não pode armazenar um número ilimitado delas. Há uma opção de configuração para controlar o limite:
    1. Detection.max_continuations_per_flow = 1024: número máximo de continuações armazenadas simultaneamente no fluxo { 0:65535 }
- Quando a avaliação de assinatura stateful atinge o limite, ela substitui a continuação de regra mais antiga por uma nova.
- A continuação de regra mais antiga residente no fluxo está lá por muito tempo, o que significa que ela ainda não atende a uma condição para retomar a avaliação da regra.
- Além disso, há muitas contagens de peg disponíveis para ajustar as regras de IPS (que devem ser o foco principal) e o limite (se necessário):
    1. detection.cont_criations: número total de continuações criadas (soma)
    2. detection.cont_recalls: número total de continuações canceladas (soma)

3. detection.cont_flows: número total de fluxos usando continuação (soma)
4. detection.cont_evals: número total de continuações de condição atendida (soma)
5. detection.cont_matches: número total de continuações combinadas (soma)
6. detection.cont_mismatches: número total de continuações incompatíveis (soma)
7. detection.cont_max_num: número de pico de continuações simultâneas por fluxo (máx)
8. detection.cont_match_distance: número total de bytes pulados por continuações correspondentes (soma)
9. detection.cont_mismatch_distance: número total de bytes pulados por continuações incompatíveis (soma)

Troubleshooting

O recurso é um aprimoramento do processo de detecção existente, portanto, não é possível fazer a identificação e solução de problemas explicitamente. Em caso de falhas na detecção, as regras, a configuração ou o tráfego devem ser examinados.

Exemplo de problema

Problema: Descrição

- Digamos que uma assinatura tem que verificar o início do arquivo e sua cauda ao mesmo tempo.
- Por exemplo, em um arquivo de destino dessa estrutura (cabeçalho, corpo, metadados), precisamos ver se algum de seus metadados tem um valor 0.

- Bytes de ficheiro: e1 f3 22 03 7f ff xx xx ... xx 01 00 02 00 em que

    - e1 f3 22 03 - 4 bytes para magic number, que identifica o tipo de arquivo
    - 7f ff - 2 bytes para tamanho do corpo
    - xx xx ... xx - 32kb de alguns dados
    - 01 00 02 00 - 4 bytes de metadados, em formato tag-value (1 byte para cada)
- A regra de IPS seria semelhante a: arquivo de alerta (file_data; content:"|e1f32203|",fast_pattern; byte_jump:2,0,relative; content:"00",within:4, relative; sid: 1;)

    - Where

        - O protocolo de arquivo garante que a regra aceite somente pacotes recriados (os pacotes brutos não participam da avaliação de assinatura stateful)
        - A opção 'file_data' seleciona um buffer de dados de arquivo, que pode formar um fluxo
        - 1ª opção de conteúdo é um padrão rápido e verifica o número mágico (se esse for o tipo de arquivo pretendido)
        - a opção byte_jump lê o tamanho do corpo do arquivo e salta sobre ele
        - A segunda opção de conteúdo executa a verificação final dos valores de

metadados, dentro dos limites de parâmetro, da profundidade de pesquisa e torna a opção relativa.

Problema: Solução

A regra seria avaliada desta forma:

No primeiro pacote (de 8kB), que transporta um cabeçalho de arquivo e uma parte do corpo:

1. O buffer file_data de IPS está selecionado. O cursor aponta para o 0º byte e1.
2. A opção padrão rápido corresponde e define a posição do cursor logo após o número mágico, apontando para o byte 7f.
3. A opção byte_jump lê dois bytes de tamanho do corpo do arquivo. O cursor é atualizado por esses dois bytes. Então byte_jump calcula um salto para mais de 32768 bytes.
4. a avaliação de assinatura stateful cria uma continuação de regra, na qual ela precisa de 24578 bytes a mais (32768 - (8kB - 4 bytes de cabeçalho - 2 bytes de tamanho de corpo)).
5. A regra inteira não corresponde, já que a opção byte_jump falha ao definir a posição do cursor tão longe.

Sobre o segundo pacote (de tamanho de 16kB), que transporta a parte do corpo do arquivo:

1. a avaliação de assinatura stateful vê a continuação de regra pendente.
2. Ele seleciona o buffer por seu nome e vê que file_data está disponível e o novo tamanho de dados é 16384.
3. O cursor atualizado mostra que 8194 bytes ainda são necessários (24578 - 16384)
4. A regra não é retomada.

No terceiro pacote (de tamanhos 8198), que transporta parte do corpo do arquivo e metadados:

1. a avaliação de assinatura stateful vê a continuação de regra pendente.
2. Ele seleciona o buffer por seu nome e vê que file_data está disponível e o novo tamanho de dados é 8198.
3. O cursor atualizado mostra que o buffer tem dados suficientes, a posição do cursor é 8194.
4. a avaliação de assinatura stateful exclui a continuação da regra.
5. a avaliação de assinatura stateful retoma a avaliação da regra da segunda opção de conteúdo com o cursor apontando para o byte 01.
6. A opção de conteúdo localiza uma correspondência no segundo byte pesquisado.
7. A regra toda finalmente dispara.

Detalhes das limitações e problemas comuns

Limitações E Outras Considerações

- Devido à implementação de avaliação de assinatura stateful, o Snort descarta todas as continuações de regra pendentes quando recarrega sua configuração. Observe que as continuações de regra, apesar de serem descartadas, ainda ocupam a memória Snort até que o próximo bloco de dados seja enviado para o módulo de detecção.

- O recurso de latência de regra para a regra de IPS na avaliação stateful age da mesma forma como se fosse uma avaliação de regra comum. O tempo de avaliação das partes da regra em diferentes blocos de dados é resumido. Se o tempo exceder o limite, a avaliação da regra executará um curto-circuito, saindo mais cedo.
- As operações Flowbits preservam seu significado, embora ainda sejam executadas como opções 'estáticas'.
  Uma operação de conjunto/limpeza/teste de fluxo de bits é executada dentro de um contexto conhecido atualmente. Portanto, se a opção flowbit for avaliada em uma continuação de regra, ela levará em conta o ambiente atual (conjunto de flowbits), não aquele em que a regra iniciou sua avaliação.

Além disso, um escritor de regras tem que prestar atenção à localização de padrão rápido.

Mesmo que possa estar em qualquer parte da regra, a opção fast-pattern é avaliada antes de toda a regra. Aciona a avaliação da regra. Para uma regra baseada em avaliação de assinatura stateful, isso significa que o ponto de continuação da regra deve estar depois da opção fast-pattern.
Além disso, a regra IPS pode ter várias continuações de regra em sua avaliação (uma após a outra, não ao mesmo tempo). Como qualquer opção do corpo da regra pode ter sua continuação, ela permite que o elaborador de regras execute verificações adicionais em locais diferentes do fluxo de dados com a mesma regra de IPS.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.