Permita o Preprocessor Inline da normalização e compreenda a inspeção PRE-ACK e Cargo-ACK

Índice

Introdução

Este documento descreve como permitir o preprocessor inline da normalização e ajuda-o a compreender a diferença e o impacto de duas opções avançadas da normalização inline.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do sistema de Cisco FirePOWER e ronca.

Componentes Utilizados

A informação neste documento é baseada nos dispositivos do centro de gerenciamento e do FirePOWER de Cisco FireSIGHT.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Um preprocessor inline da normalização normaliza o tráfego a fim minimizar a possibilidade que um atacante pode iludir a detecção usando disposições inline. A normalização ocorre imediatamente depois do pacote que descodifica e antes de todos os outros preprocessors, e continua das camadas internas do pacote para fora. A normalização Inline não gerencie eventos,

mas prepara pacotes para o uso de outros preprocessors.

Quando você aplica uma política da intrusão com o preprocessor inline da normalização permitido, o dispositivo de FirePOWER testa estas duas circunstâncias a fim assegurar-se de que você use um desenvolvimento inline:

- Para versões 5.4 e mais recente, o *modo Inline* é permitido na política da análise de rede (SESTA), e na *gota quando* está configurado *Inline* igualmente na política da intrusão se a política da intrusão está ajustada para deixar cair o tráfego. Para versões 5.3 e anterior, a *gota quando a* opção *Inline* for permitida na política da intrusão.

- A política é aplicada com failopen) a um grupo inline (ou inline da relação.

Consequentemente, além do que a habilitação e a configuração do preprocessor inline da normalização, você deve igualmente assegurar-se de que estas exigências estejam cumpridas, ou o preprocessor não normalizará o tráfego:

- Sua política deve ser ajustada para deixar cair o tráfego em disposições inline.

- Você deve aplicar sua política a um grupo inline.

Permita a normalização Inline

Esta seção descreve como permitir a normalização inline para versões 5.4 e mais recente, e igualmente para versões 5.3 e anterior.

Permita a normalização Inline nas versões 5.4 e mais recente

A maioria dos ajustes do preprocessor são configurados na SESTA para versões 5.4 e mais recente. Termine estas etapas a fim permitir a normalização inline na SESTA:

1. Entre à Web UI de seu centro de gerenciamento de FireSIGHT.

2. Navegue às **políticas >** ao **controle de acesso**.

3. Clique a **política da análise de rede** perto da área do direita superior da página.

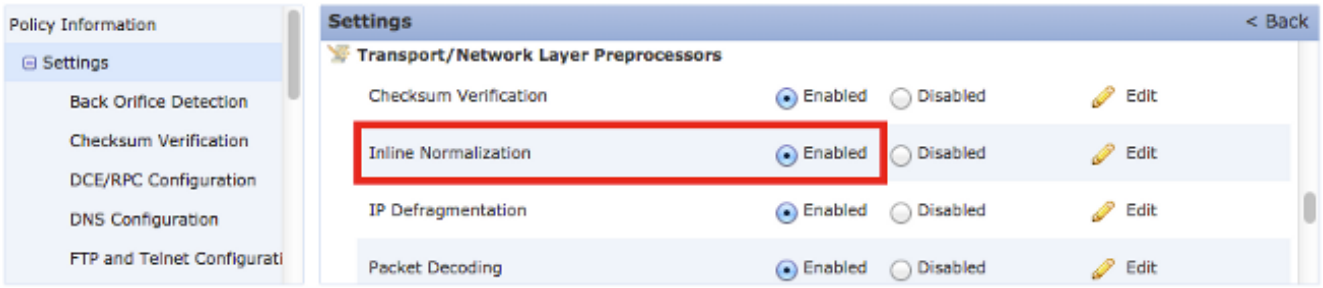
4. Selecione uma *política da análise de rede* que você queira aplicar a seu dispositivo gerenciado.

5. Clique o ícone do *lápis* a fim começar a edição, e a página da *política da edição* publica-se.

6. Clique **ajustes no** lado esquerdo da tela, e a página dos *ajustes* publica-se.

7. Encontre a opção **Inline da normalização na** área do *Preprocessor da camada do /Network do transporte*.

8. Selecione o botão de rádio **permitido** a fim permitir esta característica:



A SESTA com a normalização inline deve ser adicionada a sua política do controle de acesso para que a normalização inline ocorra. A SESTA pode ser adicionada através do *guia avançada da* política do controle de acesso:

A política do controle de acesso deve então ser aplicada ao dispositivo de inspeção.

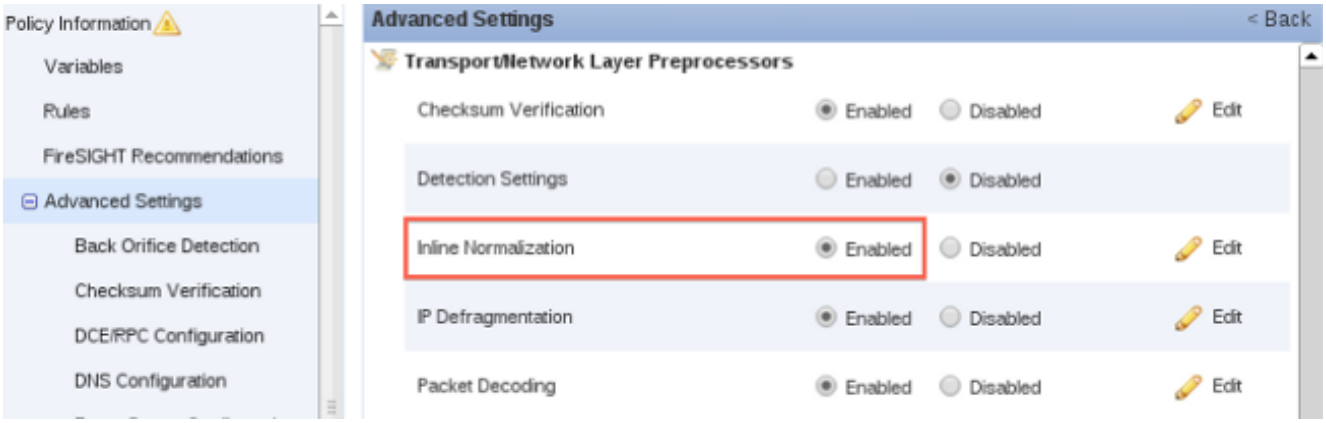
> **Note**: Para a versão 5.4 ou mais recente, você pode permitir o tráfego inline da normalização com certeza e desabilitá-lo para o outro tráfego. Se você quer o permitir para o tráfego específico, adicionar uma *regra da análise de rede* e ajuste os critérios e a política do tráfego a essa que tem a normalização inline permitida. Se você quer a permitir globalmente, a seguir ajuste a *política da análise de rede padrão a* essa que tem a normalização inline permitida.

Permita a normalização Inline nas versões 5.3 e anterior

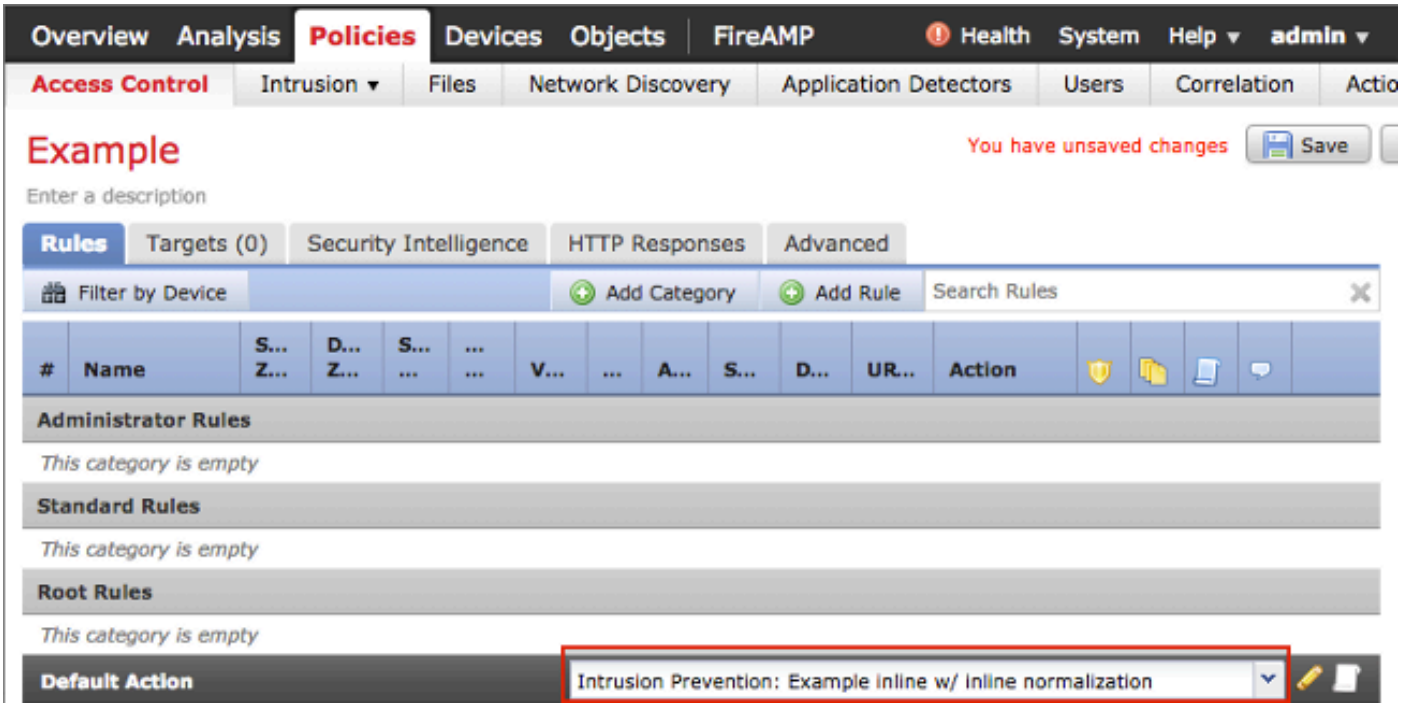
Termine estas etapas a fim permitir a normalização inline em uma política da intrusão:

1. Entre à Web UI de seu centro de gerenciamento de FireSIGHT.
2. Navegue às **políticas > à intrusão > às políticas da intrusão**.
3. Selecione uma *política da intrusão* que você queira aplicar a seu dispositivo gerenciado.
4. Clique o ícone do *lápis* a fim começar a edição, e a página da *política da edição* publica-se.
5. Clique **ajustes avançados**, e a página ***avançada dos ajustes*** publica-se.
6. Encontre a opção **Inline da normalização na** área do *Preprocessor da camada do /Network do transporte*.

7. Selecione o botão de rádio **permitido** a fim permitir esta característica:



Uma vez que a política da intrusão é configurada para a normalização inline, deve ser adicionada como a ação padrão na política do controle de acesso:



A política do controle de acesso deve então ser aplicada ao dispositivo de inspeção.

Você pode configurar o preprocessor inline da normalização a fim normalizar o IPv4, o IPv6, a versão 4 do protocolo Protocolo de control de mensajes de Internet (ICMP) (ICMPv4), o ICMPv6, e o tráfego TCP em toda a combinação. A normalização de cada protocolo ocorre automaticamente quando essa normalização do protocolo é permitida.

Permita a inspeção Cargo-ACK e a inspeção PRE-ACK

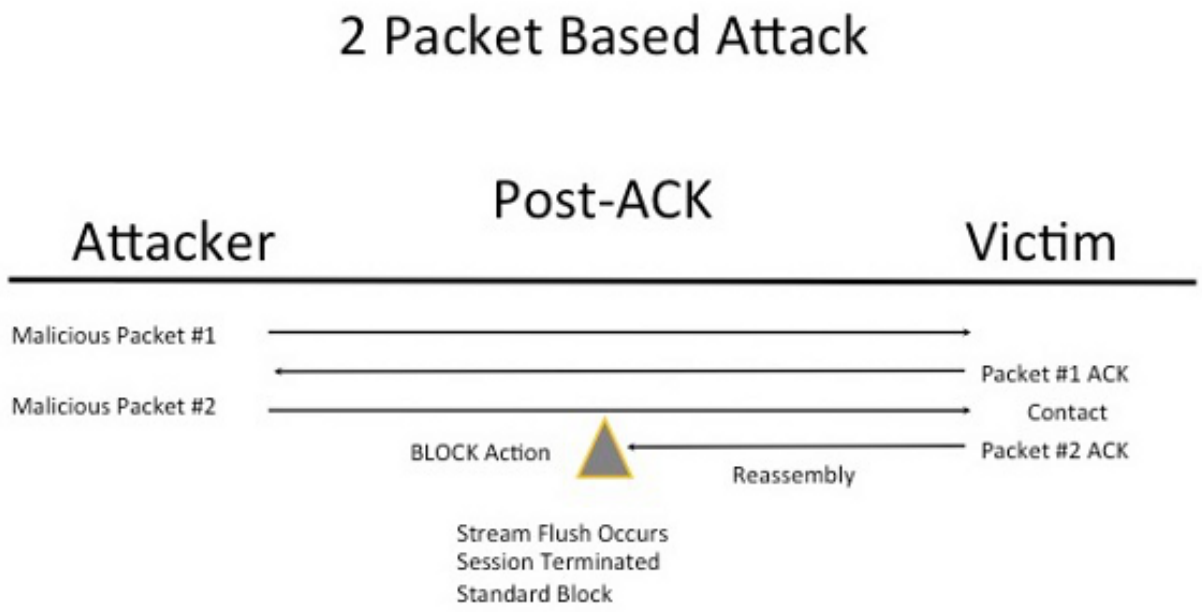
Depois que você permite o preprocessor inline da normalização, você pode editar os ajustes a fim permitir a opção do *payload de TCP da normalização*. Esta opção no preprocessor inline da normalização comuta entre dois modos diferentes de inspeção:

- Reconhecimento do cargo (Cargo-ACK)

- Pre reconhecimento (PRE-ACK)

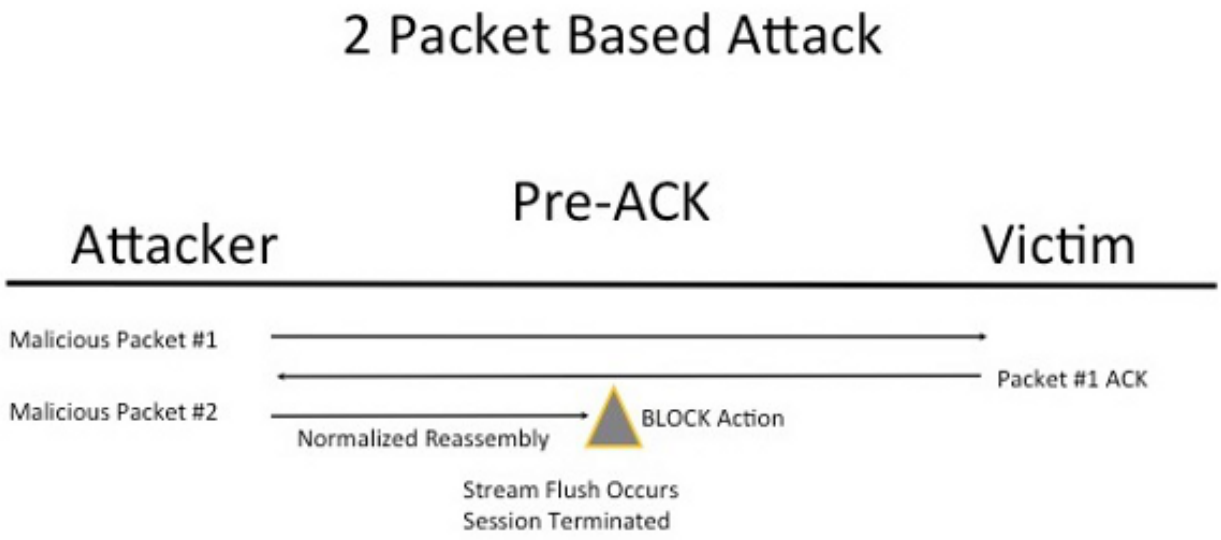
Compreenda a inspeção Cargo-ACK (normalize o payload de TCP TCP/Normalize desabilitado)

Na inspeção Cargo-ACK, a remontagem da corrente de pacote de informação, o resplendor (mão fora ao resto do processo da inspeção), e a detecção no Snort ocorrem depois que o reconhecimento (ACK) da vítima para o pacote que termina o ataque é recebido pelo Intrusion Prevention System (IPS). Antes que o resplendor do córrego ocorra, o pacote de ofensa tem alcançado já a vítima. Consequentemente, o alerta/gota ocorre depois que o pacote de ofensa alcançou a vítima. Esta ação ocorre quando o ACK da vítima para o pacote de ofensa alcança o IPS.



Compreenda a inspeção PRE-ACK (normalize o payload de TCP TCP/Normalize permitido)

Esta característica normaliza o tráfego imediatamente depois do pacote que descodifica e antes que toda a outra função do Snort estiver processada a fim minimizar esforços da evasão TCP. Isto assegura-se de que os pacotes que alcançam o IPS sejam os mesmos como aqueles que são passadas sobre à vítima. O Snort deixa cair o tráfego no pacote que termina o ataque antes que o ataque alcance sua vítima.



Quando você permite *normalize o TCP*, o tráfego que combina estas circunstâncias é deixado cair igualmente:

- Cópias retransmitidas previamente de pacotes descartado
- Trafique que tentativas de continuar uma sessão previamente deixada cair
- Trafique que combina qualqueras um regras do preprocessor do córrego TCP:

  129:1129:3129:4129:6129:8129:11129:14 a 129:19

  Note: A fim permitir os alertas para as regras do córrego TCP que são deixadas cair pelo preprocessor da normalização, você deve permitir a característica das *anomalias da inspeção stateful na* configuração do córrego TCP.