# Ative o pré-processador de normalização em linha e entenda a inspeção pré-ACK e pós-ACK

## Contents



## Introduction

Este documento descreve como ativar o pré-processador de normalização em linha e ajuda a compreender a diferença e o impacto de duas opções avançadas de normalização em linha.

## Prerequisites

### Requirements

A Cisco recomenda que você conheça o sistema Cisco Firepower e o Snort.

### Componentes Utilizados

As informações neste documento são baseadas nos dispositivos Cisco FireSIGHT Management Center e Firepower.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informações de Apoio

Um pré-processador de normalização em linha normaliza o tráfego para minimizar a possibilidade de um invasor escapar da detecção usando implantações em linha. A normalização ocorre imediatamente após a decodificação do pacote e antes de qualquer outro pré-processador e prossegue das camadas internas do pacote para fora. A normalização em linha não gera eventos, mas prepara pacotes para uso por outros pré-processadores.

Quando você aplica uma política de intrusão com o pré-processador de normalização em linha ativado, o dispositivo Firepower testa essas duas condições para garantir que você use uma implantação em linha:

- Para as versões 5.4 e posteriores, o *Modo em linha* é ativado na Política de análise de rede (NAP) e a *Eliminação quando em linha* também é configurada na política de intrusão se a política de intrusão estiver definida para eliminar o tráfego. Nas versões 5.3 e anteriores, a opção *Drop when Inline* está habilitada na política de intrusão.

- A política é aplicada a um conjunto de interfaces inline (ou inline com failopen).

Portanto, além da habilitação e configuração do pré-processador de normalização em linha, você também deve garantir que esses requisitos sejam atendidos, ou o pré-processador não normalizará o tráfego:

- Sua política deve ser definida para descartar tráfego em implantações embutidas.

- Você deve aplicar sua política a um conjunto embutido.

# Habilitar Normalização Embutida

Esta seção descreve como ativar a normalização em linha para as versões 5.4 e posteriores, e também para as versões 5.3 e anteriores.

## Ativar normalização em linha nas versões 5.4 e posteriores

A maioria das configurações de pré-processador é configurada no NAP para versões 5.4 e posteriores. Conclua estas etapas para habilitar a normalização em linha no NAP:

1. Faça login na interface do usuário da Web do FireSIGHT Management Center.

2. Navegue até **Policies > Access Control**.

3. Clique em **Política de análise de rede** próximo à área superior direita da página.

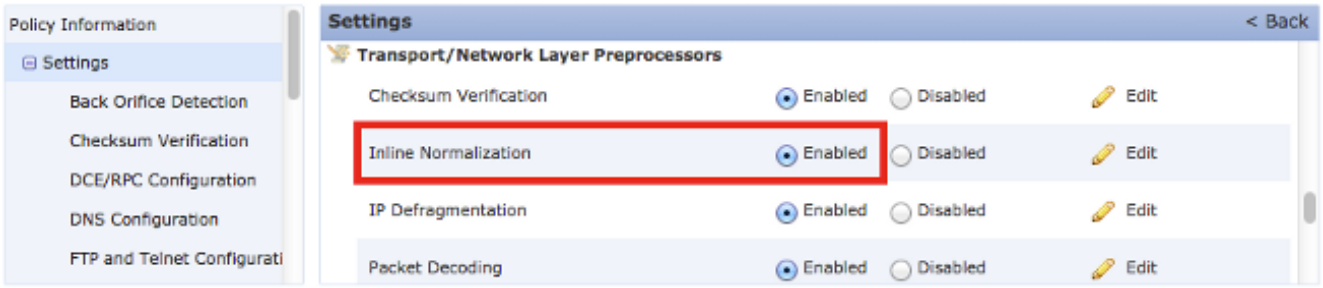
4. Selecione uma *Política de análise de rede* que você deseja aplicar ao dispositivo gerenciado.

5. Clique no ícone do *lápis* para iniciar a edição e a página *Editar política* será exibida.

6. Clique em **Settings** no lado esquerdo da tela e a página *Settings* será exibida.

7. Localize a opção **Normalização em Linha** na área *Pré-processador da Camada de Transporte/Rede*.

8. Selecione o botão de opção **Enabled** para habilitar este recurso:




O NAP com normalização embutida deve ser adicionado à sua política de controle de acesso para que ocorra a normalização embutida. O NAP pode ser adicionado através da guia *Avançado* da política de controle de acesso:

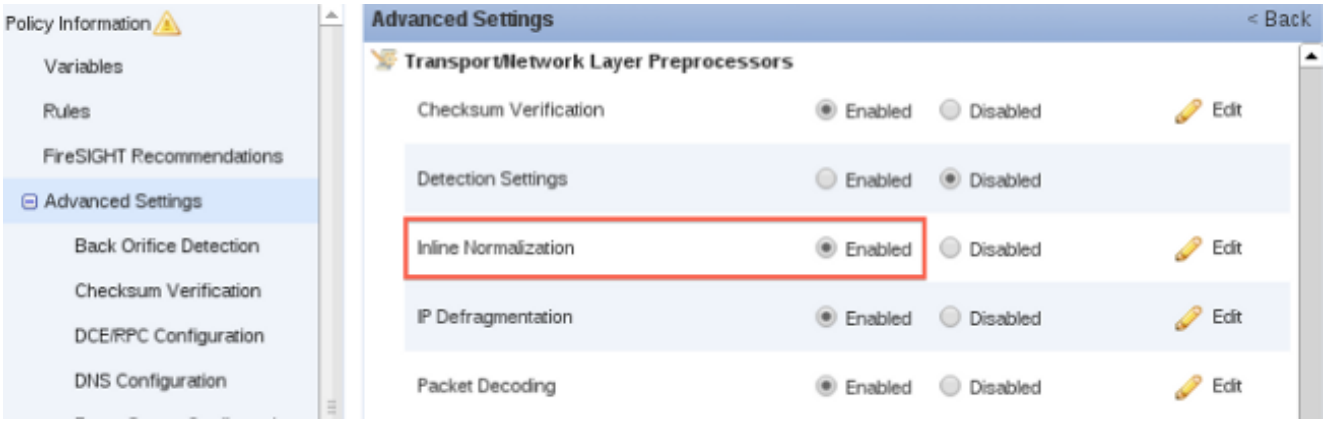

A política de controle de acesso deve ser aplicada ao dispositivo de inspeção.

> **Note**: Para a versão 5.4 ou posterior, você pode ativar a normalização em linha para determinado tráfego e desativá-la para outro tráfego. Se você quiser ativá-lo para tráfego específico, adicione uma *regra de análise de rede* e defina os critérios e a política de tráfego para aquele que tem a normalização em linha ativada. Se quiser ativá-la globalmente, defina a *política de análise de rede padrão* como aquela que tem a normalização em linha ativada.

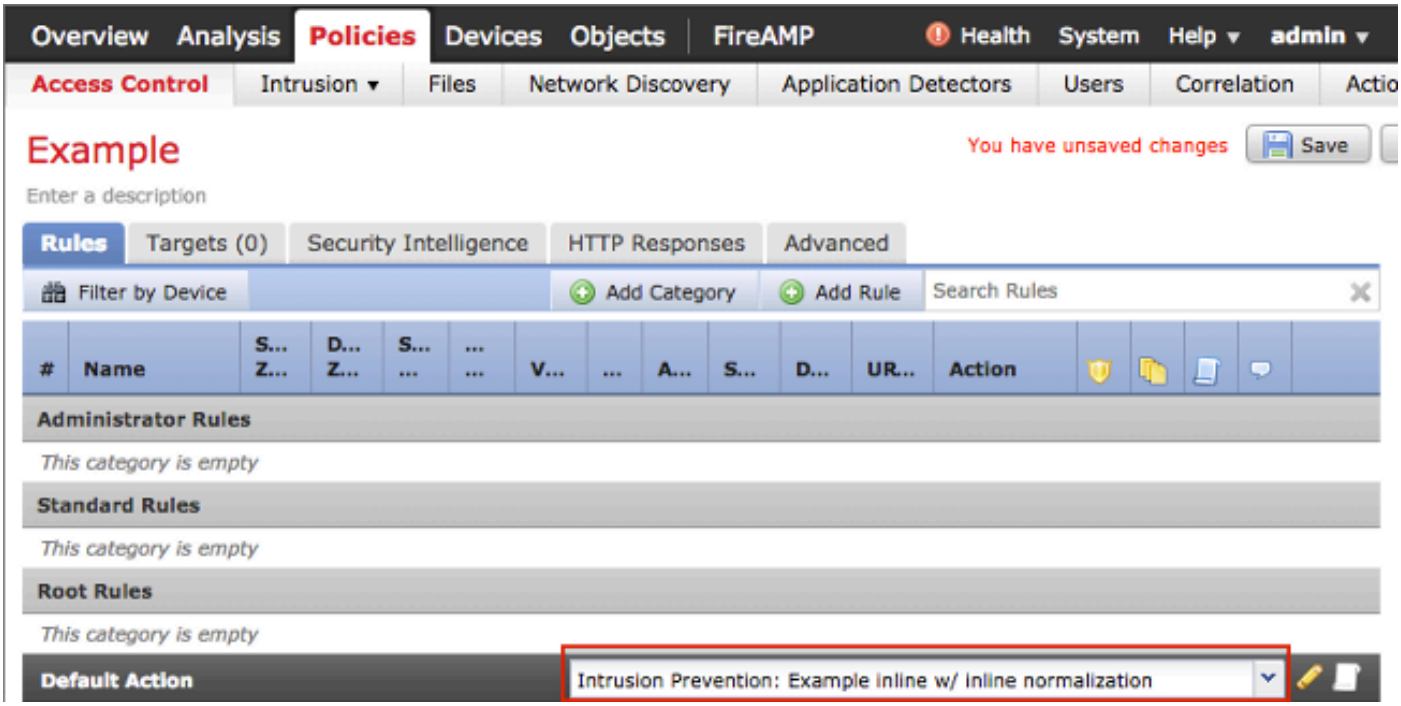
## Ativar a normalização em linha nas versões 5.3 e anteriores

Conclua estas etapas para ativar a normalização em linha em uma política de intrusão:

1. Faça login na interface do usuário da Web do FireSIGHT Management Center.
2. Navegue até **Policies > Intrusion > Intrusion Policies**.
3. Selecione uma *política de intrusão* que deseja aplicar ao dispositivo gerenciado.
4. Clique no ícone do *lápis* para iniciar a edição e a página *Editar política* será exibida.
5. Clique em **Advanced Settings** e a página ***Advanced Settings*** será exibida.
6. Localize a opção **Normalização em Linha** na área *Pré-processador da Camada de Transporte/Rede*.
7. Selecione o botão de opção **Enabled** para habilitar este recurso:




Quando a política de intrusão estiver configurada para normalização em linha, ela deverá ser adicionada como a ação padrão na política de controle de acesso:




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

Você pode configurar o pré-processador de normalização em linha para normalizar o tráfego IPv4, IPv6, Internet Control Message Protocol Versão 4 (ICMPv4), ICMPv6 e TCP em qualquer combinação. A normalização de cada protocolo ocorre automaticamente quando essa normalização de protocolo é ativada.

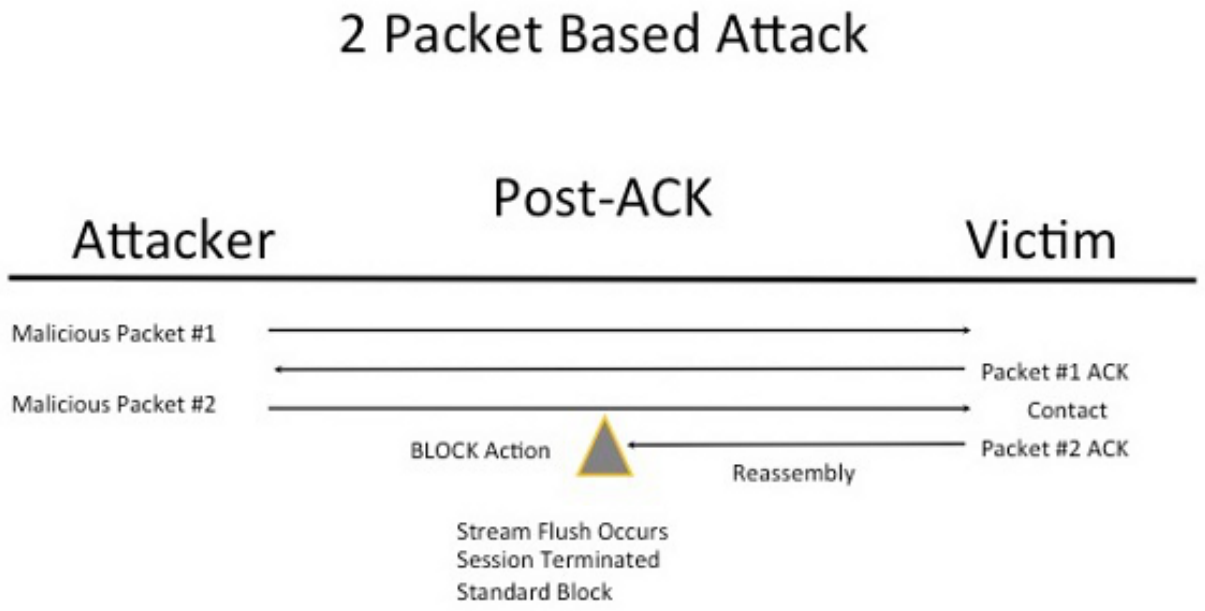
## Ativar inspeção pós-ACK e inspeção pré-ACK

Depois de ativar o pré-processador de normalização em linha, você pode editar as configurações para ativar a opção *Normalizar payload TCP*. Esta opção no pré-processador de normalização em linha alterna entre dois modos diferentes de inspeção:

- Pós-confirmação (Post-ACK)
- Pré-confirmação (Pre-ACK)

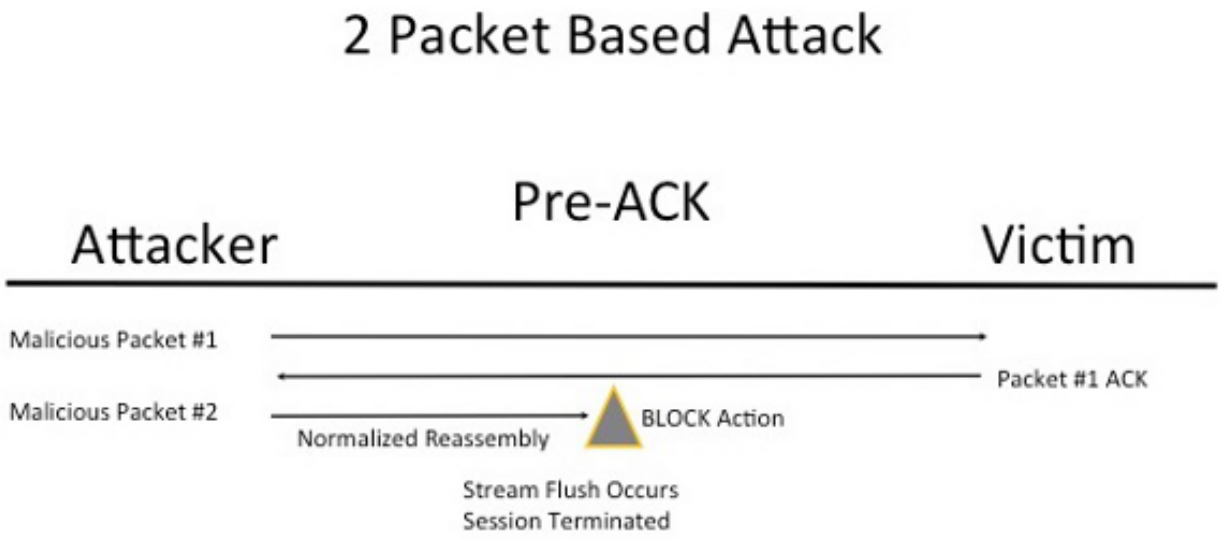
## Entender a inspeção pós-ACK (Normalizar payload TCP/Normalizar TCP desativado)

Na inspeção pós-ACK, a remontagem do fluxo de pacotes, a liberação (transferência para o restante do processo de inspeção) e a detecção no Snort ocorrem após a confirmação (ACK) da vítima do pacote que conclui o ataque ser recebido pelo IPS (Sistema de prevenção de intrusão). Antes da descarga do fluxo ocorrer, o pacote ofensivo já atingiu a vítima. Portanto, o alerta/queda ocorre depois que o pacote ofensivo chega à vítima. Essa ação ocorre quando o ACK da vítima do pacote ofensivo chega ao IPS.




## Entender a inspeção pré-ACK (Normalizar o payload TCP/Normalizar TCP ativado)

Esse recurso normaliza o tráfego imediatamente após a decodificação de pacotes e antes que qualquer outra função Snort seja processada, a fim de minimizar os esforços de evasão de TCP. Isso garante que os pacotes que chegam ao IPS sejam os mesmos que são passados para a vítima. O Snort descarta o tráfego no pacote que conclui o ataque antes que ele atinja sua vítima.




Quando você habilita *Normalize TCP*, o tráfego que corresponde a essas condições também é descartado:

- Cópias retransmitidas de pacotes descartados anteriormente
- Tráfego que tenta continuar uma sessão descartada anteriormente
- Tráfego que corresponde a qualquer uma destas regras de pré-processador de fluxo TCP:

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

  **Note**: Para habilitar os alertas para as regras de fluxo TCP que são eliminadas pelo pré-processador de normalização, você deve habilitar o recurso *Anomalias de inspeção stateful* na configuração do fluxo TCP.

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.

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.