

# 啟用內聯規範化前處理器，並瞭解ACK前和ACK後檢查

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[啟用內嵌規範化](#)

[在5.4及更新版本中啟用內嵌規範化](#)

[在5.3及更低版本中啟用內嵌規範化](#)

[啟用確認後檢查和確認前檢查](#)

[瞭解ACK後檢查 \(已禁用「規範化TCP/規範化TCP負載」\)](#)

[瞭解Pre-ACK檢查 \(已啟用規範化TCP/規範化TCP負載\)](#)

## 簡介

本文檔介紹如何啟用內聯規範化前處理器，並幫助您瞭解內聯規範化的兩個高級選項的區別和影響。

## 必要條件

### 需求

思科建議您瞭解Cisco Firepower系統和Snort。

### 採用元件

本文檔中的資訊基於Cisco FireSIGHT管理中心和Firepower裝置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

內聯規範化前處理器對流量進行規範化，以儘量減少攻擊者使用內聯部署逃避檢測的可能性。標準化在資料包解碼之後和任何其他前處理器之前立即發生，並從資料包的內層向外進行。內聯規範化不生成事件，但它準備資料包以供其他前處理器使用。

在應用啟用了內聯規範化前處理器的入侵策略時，Firepower裝置會測試以下兩個條件，以確保使用內聯部署：

- 對於5.4及更高版本，在網路分析策略(NAP)中啟用內聯模式，如果入侵策略設定為丟棄流量，則在入侵策略中也會配置*Drop when Inline*。對於5.3及更低版本，在入侵策略中啟用*Drop when Inline*選項。

- 該策略應用於內聯 ( 或帶失效開放的內聯 ) 介面集。

因此，除了啟用和配置內聯規範化前處理器外，還必須確保滿足這些要求，否則前處理器不會規範化流量：

- 必須將策略設定為丟棄內聯部署中的流量。
- 必須將策略應用於內嵌集。

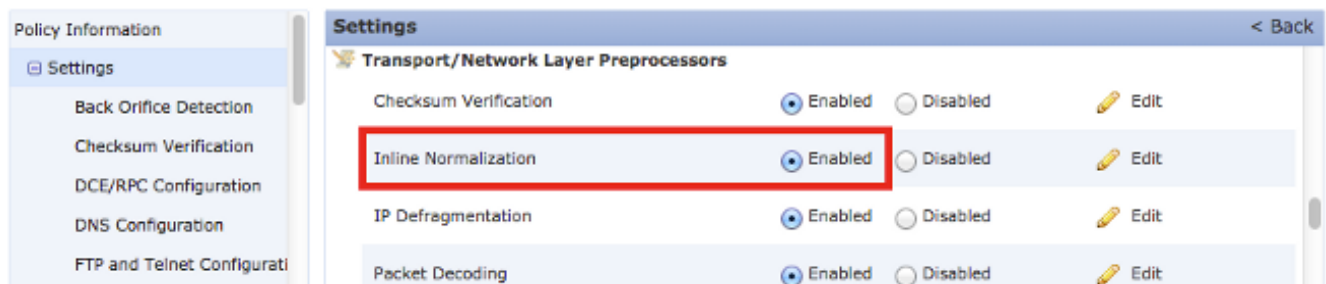
## 啟用內嵌規範化

本節介紹如何為版本5.4及更高版本以及版本5.3及更低版本啟用內嵌規範化。

### 在5.4及更新版本中啟用內嵌規範化

大多數前處理器設定在5.4版及更高版本的NAP中配置。完成以下步驟，以便在NAP中啟用內聯規範化：

1. 登入到FireSIGHT管理中心的Web UI。
2. 導覽至Policies > Access Control。
3. 點選頁面右上角區域附近的Network Analysis Policy。
4. 選擇要應用於受管裝置的Network Analysis Policy。
5. 按一下鉛筆圖示開始編輯，此時會顯示「Edit Policy」頁面。
6. 按一下螢幕左側的Settings，然後顯示Settings頁面。
7. 在Transport/Network Layer Preprocessor區域中找到Inline Normalization選項。
8. 選擇Enabled單選按鈕以啟用此功能：



必須將具有內聯規範化的NAP新增到訪問控制策略中，以便進行內聯規範化。可以通過訪問控制策略Advanced頁籤新增NAP：

Rules	Targets (0)	Security Intelligence	HTTP Responses	Advanced
<b>General Settings</b>				
Maximum URL characters to store in connection events				1024
Allow an Interactive Block to bypass blocking for (seconds)				600
SSL Policy to use for inspecting encrypted connections				None
Inspect traffic during policy apply				Yes
<b>Network Analysis and Intrusion Policies</b>				
Intrusion Policy used before Access Control rule is determined				Balanced Security and Connectivity
Intrusion Policy Variable Set				Default Set
<b>Default Network Analysis Policy</b>				Inline normalization NAP

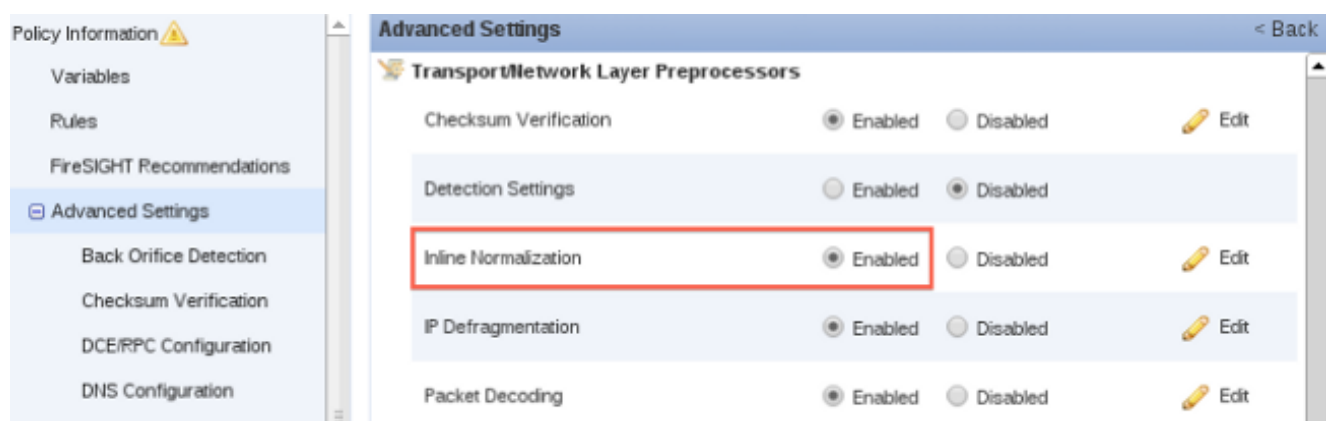
然後，必須將訪問控制策略應用到檢查裝置。

**注意：**對於5.4版或更高版本，您可以為特定流量啟用內聯規範化，並為其他流量禁用內聯規範化。如果要為特定流量啟用它，請新增網路分析規則，並將流量標準和策略設定為已啟用內聯規範化的規則。如果要全域性啟用它，請將預設網路分析策略設置為已啟用內聯規範化的策略。

## 在5.3及更低版本中啟用內嵌規範化

完成以下步驟，以在入侵策略中啟用內聯規範化：

1. 登入到FireSIGHT管理中心的Web UI。
2. 導航到Policies > Intrusion > Intrusion Policies。
3. 選擇要應用到受管裝置的入侵策略。
4. 按一下鉛筆圖示開始編輯，此時會顯示「Edit Policy」頁面。
5. 按一下Advanced Settings，然後顯示Advanced Settings頁面。
6. 在Transport/Network Layer Preprocessor區域中找到Inline Normalization選項。
7. 選擇Enabled單選按鈕以啟用此功能：



將入侵策略配置為內聯規範化後，必須將其新增為訪問控制策略中的預設操作：

Overview Analysis **Policies** Devices Objects FireAMP Health System Help admin

Access Control Intrusion Files Network Discovery Application Detectors Users Correlation Action

Example You have unsaved changes Save

Enter a description

Rules Targets (0) Security Intelligence HTTP Responses Advanced

Filter by Device Add Category Add Rule Search Rules

#	Name	S... Z...	D... Z...	S... ...	...	V... ...	A... S...	D... UR...	Action				
<b>Administrator Rules</b>													
This category is empty													
<b>Standard Rules</b>													
This category is empty													
<b>Root Rules</b>													
This category is empty													
<b>Default Action</b>													
Intrusion Prevention: Example inline w/ inline normalization													

然後，必須將訪問控制策略應用到檢查裝置。

您可以設定內嵌規範化前處理器，以便以任意組合規範化IPv4、IPv6、網際網路控制訊息通訊協定版本4(ICMPv4)、ICMPv6和TCP流量。當協定規範化被啟用時，每個協定的規範化自動發生。

## 啟用確認後檢查和確認前檢查

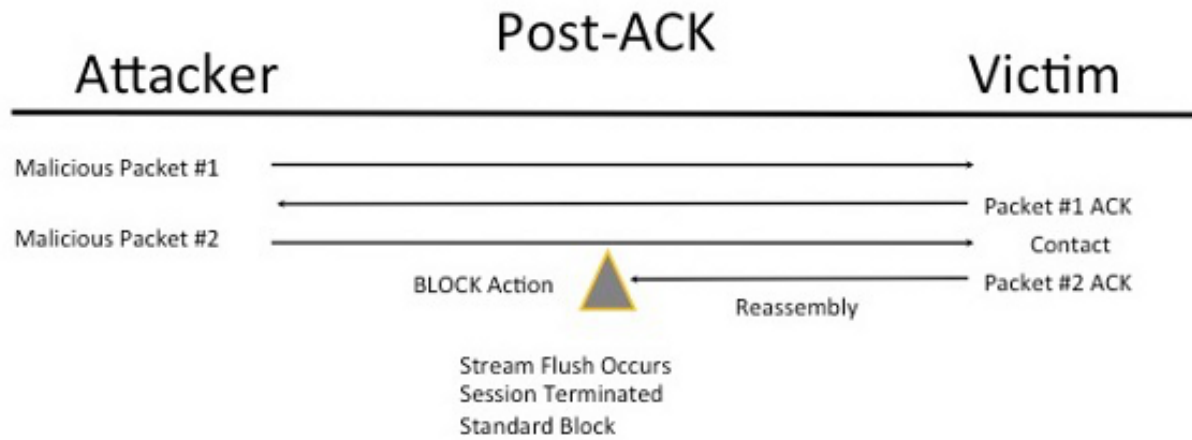
啟用內聯規範化前處理器後，您可以編輯設定以啟用 *Normalize TCP Payload* 選項。內聯規範化前處理器中的此選項可在兩種不同的檢測模式之間切換：

- Post Acknowledgement ( ACK後 )
- 預先確認(Pre-ACK)

### 瞭解ACK後檢查 ( 已禁用「規範化TCP/規範化TCP負載」 )

在Post-ACK檢測中，資料包流重組、刷新（轉移到檢測過程的其餘部分）和Snort中的檢測在入侵防禦系統(IPS)接收到來自完成攻擊資料包的受害者的確認(ACK)之後發生。在流刷新發生之前，有問題的資料包已經到達受害者。因此，當有問題的資料包到達受害者時，就會發生警報/丟棄。當來自違規資料包的受害者的ACK到達IPS時，會發生此操作。

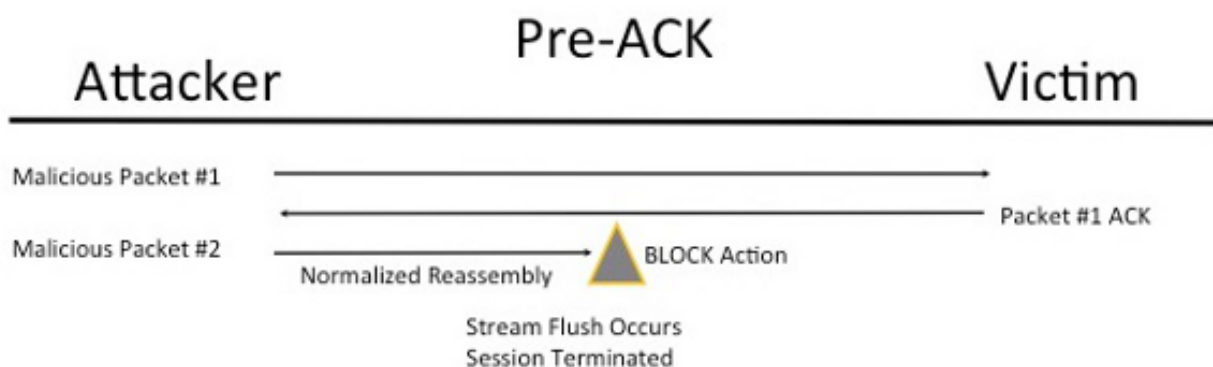
## 2 Packet Based Attack



### 瞭解Pre-ACK檢查 ( 已啟用規範化TCP/規範化TCP負載 )

此功能會在資料包解碼之後以及處理任何其他Snort函式之前立即對流量進行規範化，以便最大程度降低TCP逃避工作。這可確保到達IPS的資料包與傳遞給受害者的資料包相同。Snort會捨棄封包上在攻擊到達受害者之前完成攻擊的流量。

## 2 Packet Based Attack



啟用 *Normalize TCP* 時，符合以下條件的流量也會遭捨棄：

- 重新傳輸之前丟棄的資料包的副本
- 嘗試繼續之前丟棄的會話的流量

- 符合以下TCP串流前處理器規則的流量：

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

**注意：**為了對規範化前處理器丟棄的TCP流規則啟用警報，必須在TCP流配置中啟用狀態檢測異常功能。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。