Contents

Introduction

This document describes how to enable the inline normalization preprocessor and helps you to understand the difference and impact of two advanced options of inline normalization.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the Cisco Firepower system and Snort.

Components Used

The information in this document is based on the Cisco FireSIGHT Management Center and Firepower appliances.

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.

Background Information

An inline normalization preprocessor normalizes traffic in order to minimize the chance that an attacker can evade detection using inline deployments. Normalization occurs immediately after packet decoding and before any other preprocessors, and proceeds from the inner layers of the packet outward. Inline normalization does not generate events, but it prepares packets for use by other preprocessors.

When you apply an intrusion policy with the inline normalization preprocessor enabled, the Firepower device tests these two conditions in order to ensure that you use an inline deployment:

- For Versions 5.4 and later, the *Inline Mode* is enabled in the Network Analysis Policy (NAP), and the *Drop when Inline* is also configured in the intrusion policy if the intrusion policy is set to drop traffic. For Versions 5.3 and earlier, the *Drop when Inline* option is enabled in the intrusion policy.

- The policy is applied to an inline (or inline with failopen) interface set.

Therefore, in addition to the enablement and configuration of the inline normalization preprocessor, you must also ensure that these requirements be met, or the preprocessor will not normalize traffic:

- Your policy must be set to drop traffic in inline deployments.

- You must apply your policy to an inline set.

Enable Inline Normalization

This section describes how to enable inline normalization for Versions 5.4 and later, and also for Versions 5.3 and earlier.

Enable Inline Normalization in Versions 5.4 and Later

Most of the preprocessor settings are configured in the NAP for Versions 5.4 and later. Complete these steps in order to enable inline normalization in the NAP:

1. Log in to the web UI of your FireSIGHT Management Center.

2. Navigate to **Policies** > **Access Control**.

3. Click **Network Analysis Policy** near the top-right area of the page.

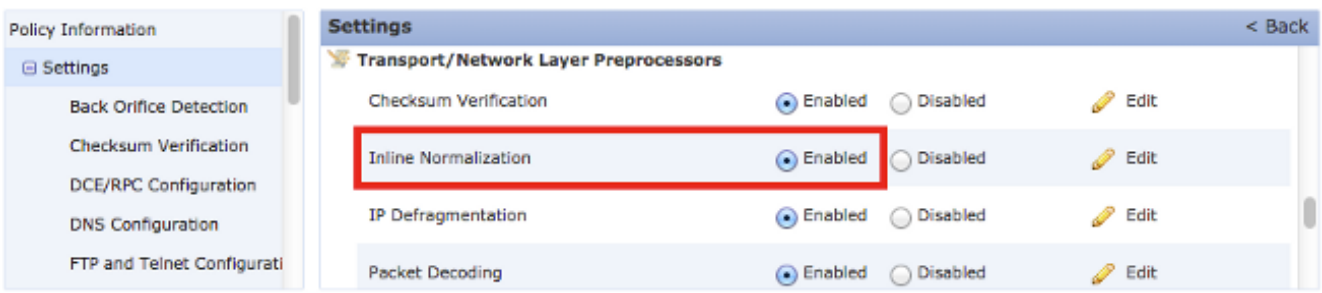
4. Select a *Network Analysis Policy* that you want to apply to your managed device.

5. Click the *pencil* icon in order to begin the edit, and the *Edit Policy* page appears.

6. Click **Settings** on the left side of the screen, and the *Settings* page appears.

7. Locate the **Inline Normalization** option in the *Transport/Network Layer Preprocessor* area.

8. Select the **Enabled** radio button in order to enable this feature:



The NAP with the inline normalization must be added to your access control policy in order for

inline normalization to occur. The NAP can be added through the access control policy *Advanced* tab:

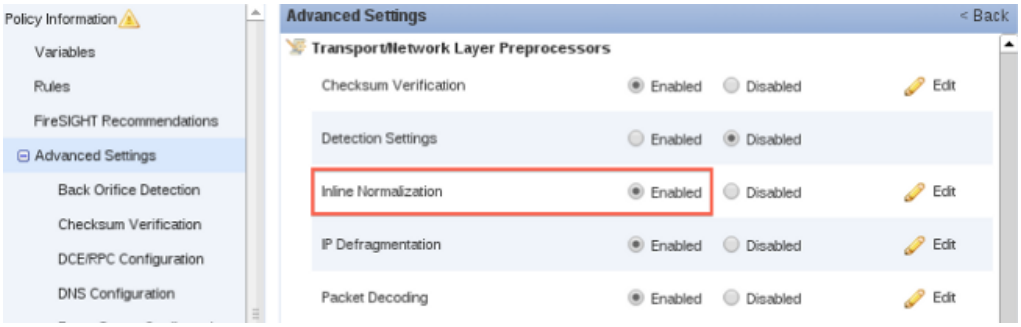
The access control policy must then be applied to the inspecting device.

> **Note**: For Version 5.4 or later, you can enable inline normalization for certain traffic and disable it for other traffic. If you want to enable it for specific traffic, add a *network analysis rule* and set the traffic criteria and policy to the one that has inline normalization enabled. If you want to enable it globally, then set the *default network analysis policy* to the one that has inline normalization enabled.

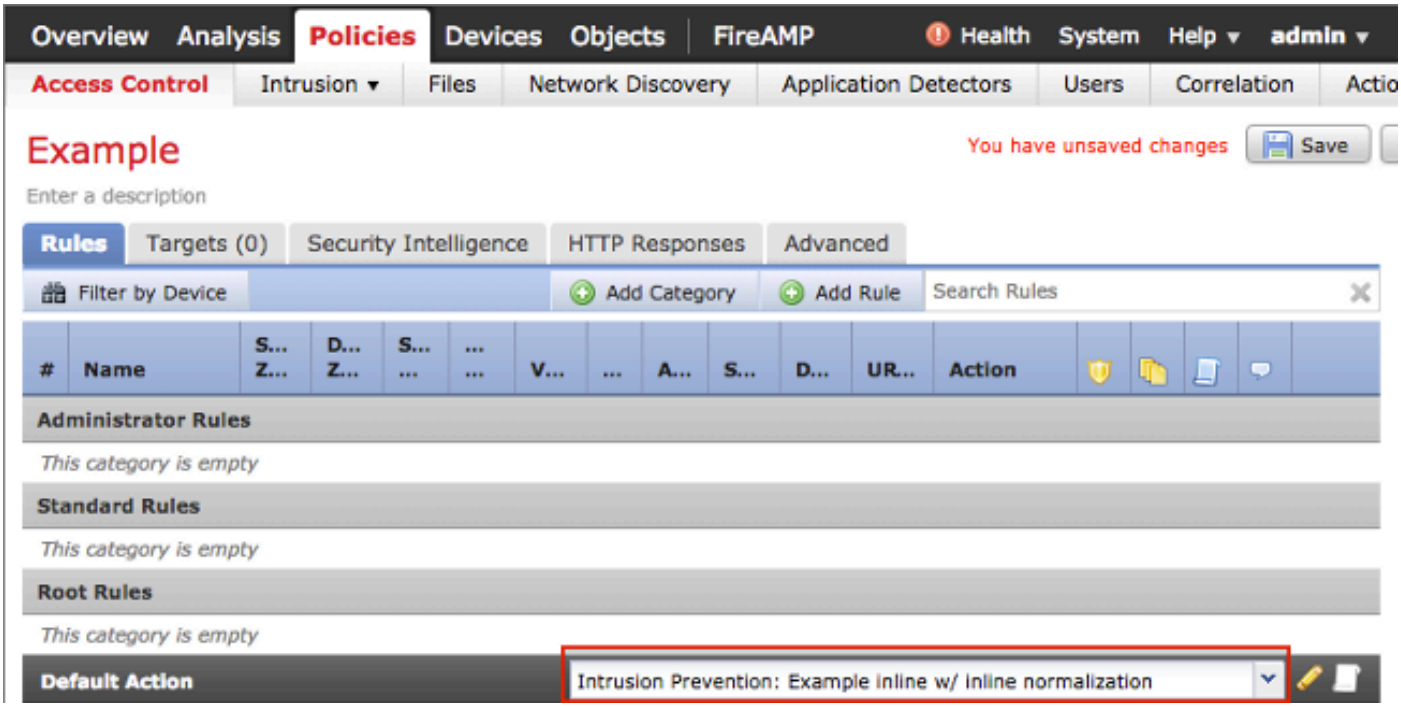
Enable Inline Normalization in Versions 5.3 and Earlier

Complete these steps in order to enable inline normalization in an intrusion policy:

1. Log in to the web UI of your FireSIGHT Management Center.
2. Navigate to **Policies > Intrusion > Intrusion Policies**.
3. Select an *intrusion policy* that you want to apply to your managed device.
4. Click the *pencil* icon in order to begin the edit, and the *Edit Policy* page appears.
5. Click **Advanced Settings**, and the ***Advanced Settings*** page appears.
6. Locate the **Inline Normalization** option in the *Transport/Network Layer Preprocessor* area.
7. Select the **Enabled** radio button in order to enable this feature:



Once the intrusion policy is configured for inline normalization, it must be added as the default action in the access control policy:



The access control policy must then be applied to the inspecting device.

You can configure the inline normalization preprocessor in order to normalize IPv4, IPv6, Internet Control Message Protocol Version 4 (ICMPv4), ICMPv6, and TCP traffic in any combination. The normalization of each protocol occurs automatically when that protocol normalization is enabled.

Enable Post-ACK Inspection and Pre-ACK Inspection

After you enable the inline normalization preprocessor, you can edit the settings in order to enable the *Normalize TCP Payload* option. This option in the inline normalization preprocessor switches between two different modes of inspection:

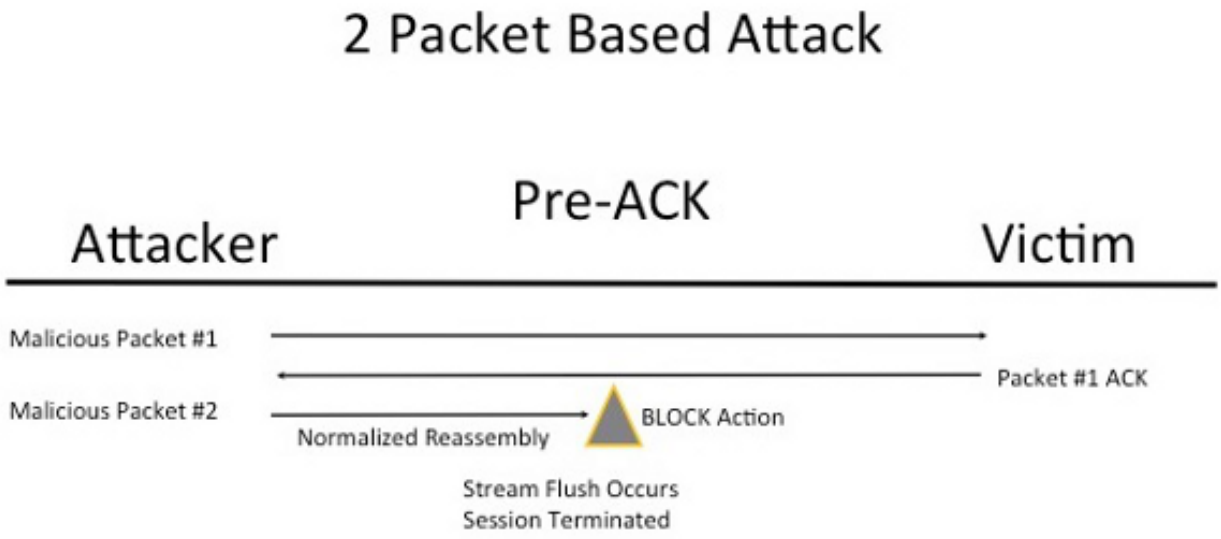
- Post Acknowledgement (Post-ACK)
- Pre Acknowledgement (Pre-ACK)

Understand Post-ACK Inspection (Normalize TCP/Normalize TCP Payload Disabled)

In Post-ACK inspection, the packet stream reassembly, flush (hand off to the rest of the inspection process), and detection in Snort occurs after the acknowledgement (ACK) from the victim for the packet that completes the attack is received by the Intrusion Prevention System (IPS). Before the stream flush occurs, the offending packet has already reached the victim. Therefore, the alert/drop occurs after the offending packet has reached the victim. This action occurs when the ACK from the victim for the offending packet reaches the IPS.

Understand Pre-ACK Inspection (Normalize TCP/Normalize TCP Payload Enabled)

This feature normalizes traffic immediately after packet decoding and before any other Snort function is processed in order to minimize TCP evasion efforts. This ensures that the packets reaching the IPS are the same as those that are passed on to the victim. Snort drops the traffic on the packet that completes the attack before the attack reaches its victim.



When you enable *Normalize TCP*, the traffic that matches these conditions is also dropped:

- Retransmitted copies of previously dropped packets
- Traffic that attempts to continue a previously dropped session
- Traffic that matches any of these TCP stream preprocessor rules:

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

  Note: In order to enable the alerts for the TCP stream rules that are dropped by the normalization preprocessor, you must enable the *Stateful Inspection Anomalies* feature in the TCP stream configuration.