Habilite el preprocesador en línea de la normalización y entienda el examen PRE-ACK y Poste-ACK

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Normalización en línea del permiso](#)
[Normalización en línea del permiso en las versiones 5.4 y posterior](#)
[Normalización en línea del permiso en las versiones 5.3 y anterior](#)
[Examen del permiso Poste-ACK y examen PRE-ACK](#)
[Entienda el examen Poste-ACK (normalice TCP/Normalize carga útil de TCP inhabilitado)](#)
[Entienda el examen PRE-ACK (normalice TCP/Normalize carga útil de TCP habilitado)](#)

Introducción

Este documento describe cómo habilitar el preprocesador en línea de la normalización y le ayuda a entender la diferencia y el impacto de dos opciones avanzadas de la normalización en línea.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento del sistema de Cisco FirePOWER y resopla.

Componentes Utilizados

La información en este documento se basa en los dispositivos del centro de administración y de FirePOWER de Cisco FireSIGHT.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Un preprocesador en línea de la normalización normaliza el tráfico para minimizar la ocasión que un atacante puede evadir la detección usando las implementaciones en línea. La normalización

ocurre inmediatamente después del paquete que decodifica y antes de cualquier otro preprocesador, y procede de las capas internas del paquete hacia fuera. La normalización en línea no genera los eventos, sino que prepara los paquetes para uso de otros preprocesadores.

Cuando usted aplica una directiva de la intrusión con el preprocesador en línea de la normalización habilitado, el dispositivo de FirePOWER prueba estas dos condiciones para asegurarse de que usted utiliza un despliegue en línea:

- Para las versiones 5.4 y posterior, el *modo en línea* se habilita en la directiva de la Análisis de red (SIESTA), y el *descenso cuando en línea* también se configura en la directiva de la intrusión si la directiva de la intrusión se fija para caer el tráfico. Para las versiones 5.3 y anterior, el *descenso cuando la* opción *en línea* se habilita en la directiva de la intrusión.

- La directiva se aplica con failopen) a un conjunto en línea (o en línea de la interfaz.

Por lo tanto, además de la habilitación y de la configuración del preprocesador en línea de la normalización, usted debe también asegurarse de que estos requisitos estén cumplidos, o el preprocesador no normalizará el tráfico:

- Su directiva se debe fijar para caer el tráfico en las implementaciones en línea.

- Usted debe aplicar su directiva a un conjunto en línea.

Normalización en línea del permiso

Esta sección describe cómo habilitar la normalización en línea para las versiones 5.4 y posterior, y también para las versiones 5.3 y anterior.

Normalización en línea del permiso en las versiones 5.4 y posterior

La mayor parte de las configuraciones del preprocesador se configuran en la SIESTA para las versiones 5.4 y posterior. Complete estos pasos para habilitar la normalización en línea en la SIESTA:

1. Inicie sesión a la red UI de su centro de administración de FireSIGHT.

2. Navegue a las **directivas >** al **control de acceso**.

3. Haga clic la **directiva de la Análisis de red** cerca del área de la esquina superior derecha de la página.

4. Seleccione una *directiva de la Análisis de red* que usted quiera aplicar a su dispositivo administrado.

5. Haga clic el icono del *lápiz* para comenzar el editar, y la página de la *directiva del editar* aparece.

6. Haga clic las **configuraciones** en el lado izquierdo de la pantalla, y la *página Configuración* aparece.

7. Localice la opción **en línea de la normalización** en el área del *preprocesador de la capa del /Network del transporte*.

8. Seleccione el botón de radio **habilitado** para habilitar esta característica:

La SIESTA con la normalización en línea se debe agregar a su directiva del control de acceso para que la normalización en línea ocurra. La SIESTA se puede agregar a través de la *ficha Avanzadas de la* directiva del control de acceso:

La directiva del control de acceso se debe entonces aplicar al dispositivo de inspección.

> **Note**: Para la versión 5.4 o posterior, usted puede habilitar el tráfico en línea de la normalización con certeza y inhabilitarlo para el otro tráfico. Si usted quiere habilitarlo para el tráfico específico, agregue una *regla de la Análisis de red* y fije los criterios y la directiva del tráfico a la que tiene normalización en línea habilitada. Si usted quiere habilitarlo global, después fije la *directiva del análisis de red predeterminada a* la que tiene normalización en línea habilitada.

Habilite la normalización en línea en las versiones 5.3 y anterior

Complete estos pasos para habilitar la normalización en línea en una directiva de la intrusión:

1. Inicie sesión a la red UI de su centro de administración de FireSIGHT.

2. Navegue a las **directivas > a la intrusión > a las directivas de la intrusión**.

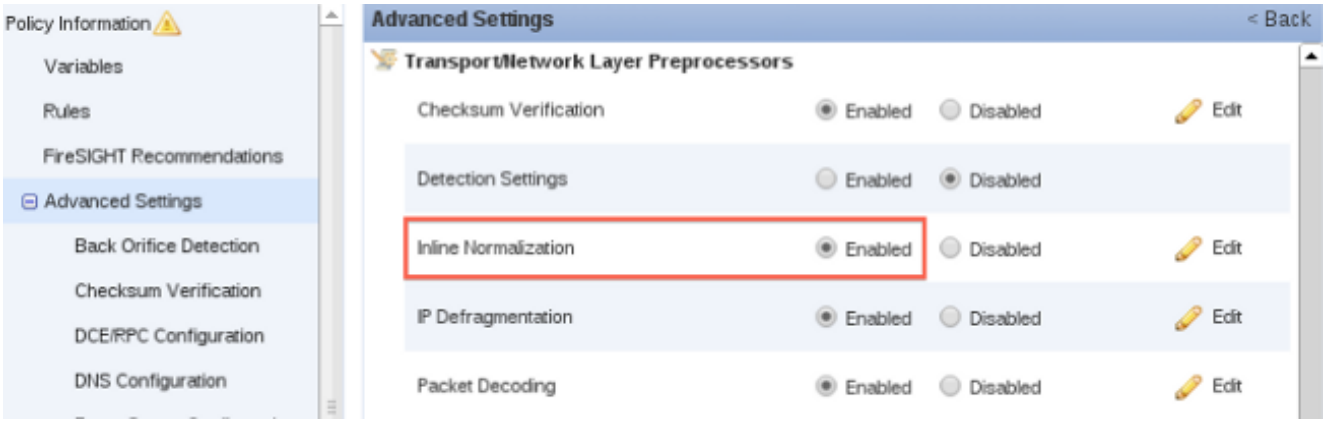
3. Seleccione una *directiva de la intrusión* que usted quiera aplicar a su dispositivo administrado.

4. Haga clic el icono del *lápiz* para comenzar el editar, y la página de la *directiva del editar* aparece.

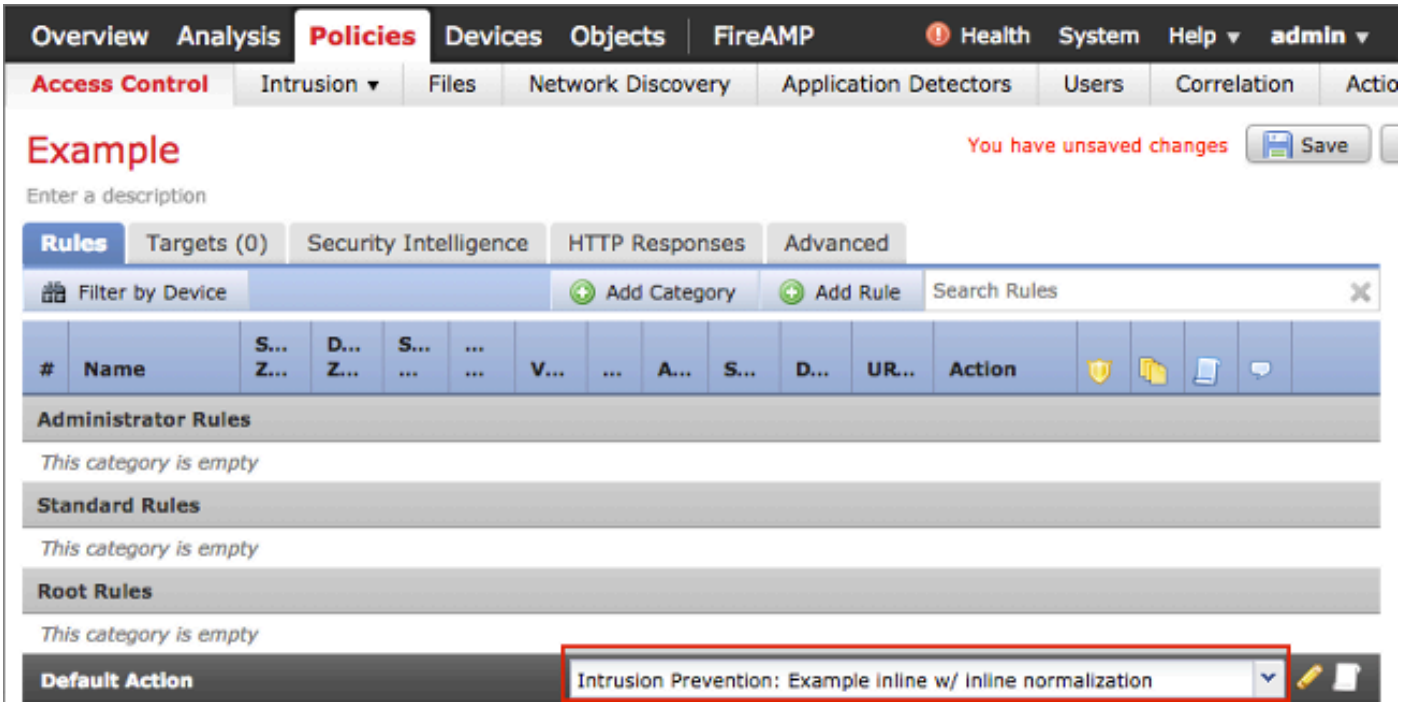
5. Haga clic las **configuraciones avanzadas**, y la ***página Configuración avanzada*** aparece.

6. Localice la opción **en línea de la normalización** en el área del *preprocesador de la capa del /Network del transporte*.

7. Seleccione el botón de radio **habilitado** para habilitar esta característica:



Una vez que la directiva de la intrusión se configura para la normalización en línea, debe ser agregada como la acción predeterminada en la directiva del control de acceso:



La directiva del control de acceso se debe entonces aplicar al dispositivo de inspección.

Usted puede configurar el preprocesador en línea de la normalización para normalizar el IPv4, el IPv6, la versión 4 (ICMPv4) del protocolo Protocolo de control de mensajes de Internet (ICMP), el ICMPv6, y tráfico TCP en cualquier combinación. La normalización de cada protocolo ocurre automáticamente cuando se habilita esa normalización del protocolo.

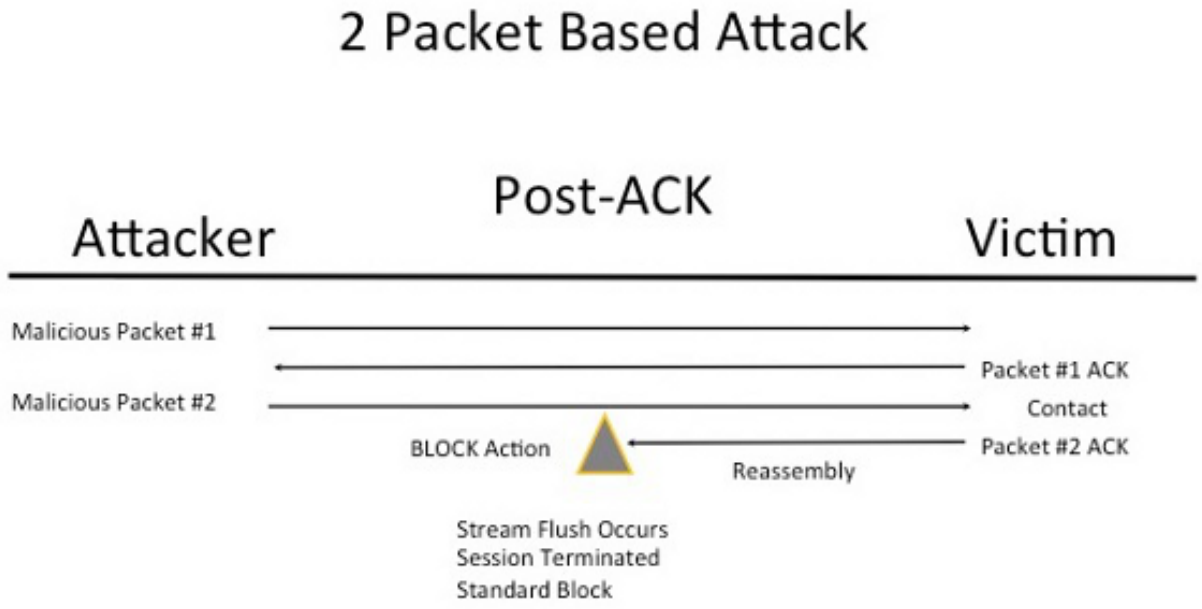
Examen del permiso Poste-ACK y examen PRE-ACK

Después de que usted habilite el preprocesador en línea de la normalización, usted puede editar las configuraciones para habilitar la opción de la *normalización carga útil de TCP*. Esta opción en el Switches en línea del preprocesador de la normalización entre dos diversos modos de examen:

- Acuse de recibo del poste (Poste-ACK)
- Pre acuse de recibo (PRE-ACK)

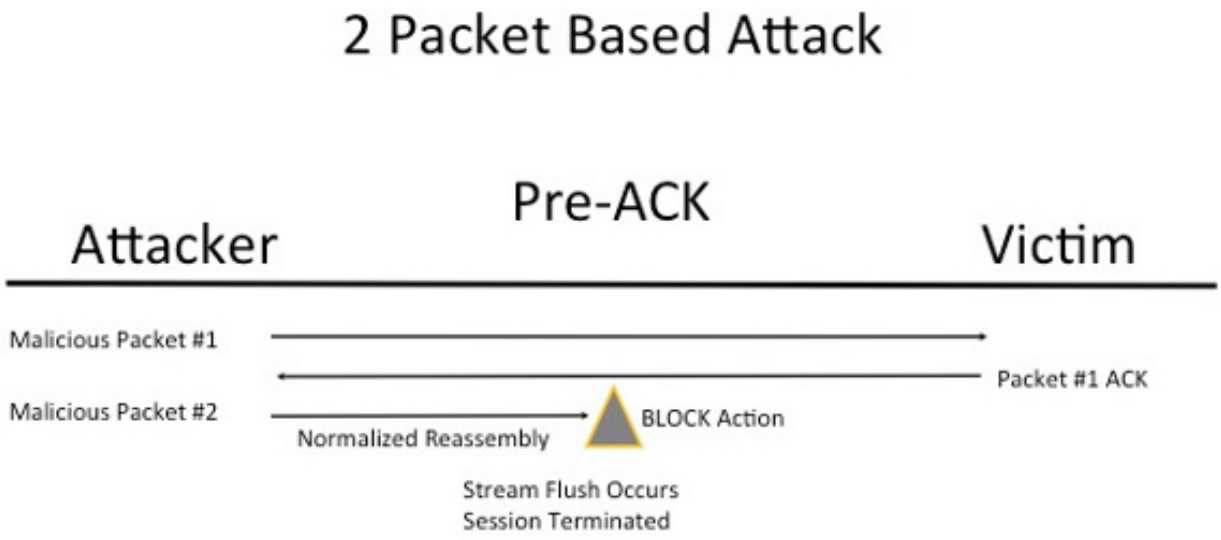
Entienda el examen Poste-ACK (normalice TCP/Normalize carga útil de TCP inhabilitado)

En el examen Poste-ACK, el nuevo ensamble de la secuencia de paquetes, el rubor (mano apagado al resto del proceso del examen), y la detección en el Snort ocurre después de que el acuse de recibo (ACK) de la víctima para el paquete que completa el ataque sea recibido por el Sistema de prevención de intrusiones (IPS). Antes de que ocurra el rubor de la secuencia, el paquete que ofendía ha alcanzado ya a la víctima. Por lo tanto, la alerta/el descenso ocurre después de que el paquete que ofendía haya alcanzado a la víctima. Esta acción ocurre cuando el ACK de la víctima para el paquete que ofende alcanza el IPS.



Entienda el examen PRE-ACK (normalice TCP/Normalize carga útil de TCP habilitado)

Esta característica normaliza el tráfico inmediatamente después del paquete que decodifica y antes de que cualquier otra función del Snort se procese para minimizar esfuerzos de la evasión TCP. Esto se asegura de que los paquetes que alcanzan el IPS sean lo mismo que los que se pasan encendido a la víctima. El Snort cae el tráfico en el paquete que completa el ataque antes de que el ataque alcance a su víctima.



Cuando usted habilita *normalice el TCP*, el tráfico que hace juego estas condiciones también se cae:

- Copias retransmitidas previamente de los paquetes perdidos
- Trafique que las tentativas de continuar una sesión previamente caída
- Trafique que hace juego ninguno de estos reglas del preprocesador de la secuencia TCP:

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

  Note: Para habilitar las alertas para las reglas de la secuencia TCP que son caídas por el preprocesador de la normalización, usted debe habilitar la característica de las *anomalías de la inspección con estado* en la configuración de la secuencia TCP.