Habilitar el preprocesador de normalización en línea y comprender la inspección previa y posterior al ACK

Contenido

Introducción

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

Prerequisites

Requirements

Cisco recomienda que conozca el sistema Cisco Firepower y Snort.

Componentes Utilizados

La información de este documento se basa en los appliances Cisco FireSIGHT Management Center y Firepower.

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). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Un preprocesador de normalización en línea normaliza el tráfico para minimizar la posibilidad de que un atacante pueda eludir la detección mediante implementaciones en línea. La normalización

se produce inmediatamente después de la decodificación del paquete y antes de cualquier otro preprocesador, y continúa desde las capas internas del paquete hacia el exterior. La normalización en línea no genera eventos, pero prepara los paquetes para que los utilicen otros preprocesadores.

Cuando se aplica una política de intrusiones con el preprocesador de normalización en línea habilitado, el dispositivo Firepower prueba estas dos condiciones para asegurarse de que se utiliza una implementación en línea:

- Para las versiones 5.4 y posteriores, el *modo en línea* se habilita en la directiva de análisis de red (NAP), y el *descartar cuando está en línea* también se configura en la directiva de intrusiones si la directiva de intrusiones está configurada para descartar tráfico. Para las versiones 5.3 y anteriores, la opción *Drop when Inline* está habilitada en la política de intrusiones.

- La política se aplica a un conjunto de interfaces en línea (o en línea con failopen).

Por lo tanto, además de habilitar y configurar el preprocesador de normalización en línea, también debe asegurarse de que se cumplan estos requisitos o el preprocesador no normalizará el tráfico:

- Su política debe configurarse para descartar tráfico en implementaciones en línea.

- Debe aplicar la directiva a un conjunto en línea.

Habilitar normalización en línea

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

Habilitar la normalización en línea en las versiones 5.4 y posteriores

La mayoría de las opciones del preprocesador se configuran en el NAP para las versiones 5.4 y posteriores. Complete estos pasos para habilitar la normalización en línea en el NAP:

1. Inicie sesión en la interfaz de usuario web de FireSIGHT Management Center.

2. Vaya a **Políticas** > **Control de acceso**.

3. Haga clic en **Política de análisis de red** cerca del área superior derecha de la página.

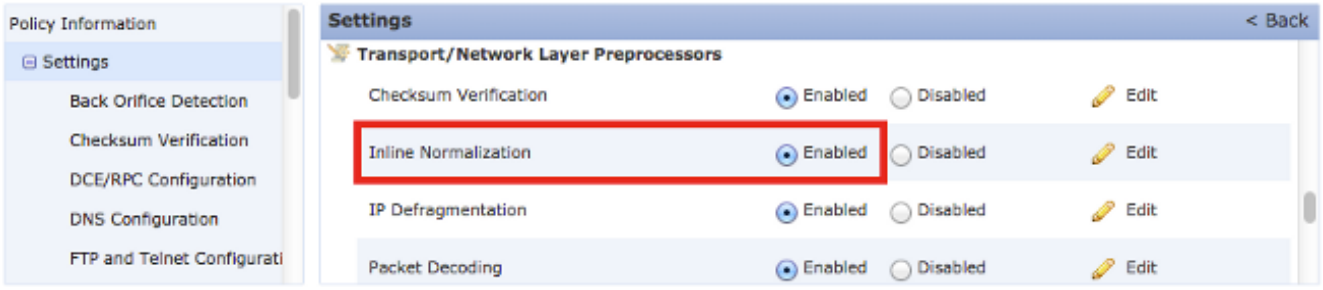
4. Seleccione una *política de análisis de red* que desee aplicar al dispositivo gestionado.

5. Haga clic en el icono del *lápiz* para comenzar la edición, y aparecerá la página *Editar Política*.

6. Haga clic en **Settings** en el lado izquierdo de la pantalla y aparecerá la página *Settings*.

7. Localice la opción **Normalización en línea** en el área *Preprocesador de capa de transporte/red*.

8. Seleccione el botón de opción **Enabled** para habilitar esta función:



El NAP con la normalización en línea debe agregarse a la directiva de control de acceso para que se produzca la normalización en línea. El NAP se puede agregar a través de la ficha *Avanzado* de la directiva de control de acceso:

La política de control de acceso se debe aplicar al dispositivo que realiza la inspección.

> **Nota**: Para la versión 5.4 o posterior, puede habilitar la normalización en línea para cierto tráfico y deshabilitarla para otro tráfico. Si desea habilitarla para tráfico específico, agregue una *regla de análisis de red* y establezca los criterios y la política de tráfico en la que tiene habilitada la normalización en línea. Si desea habilitarla globalmente, establezca la *política predeterminada de análisis de red* en la que tiene habilitada la normalización en línea.

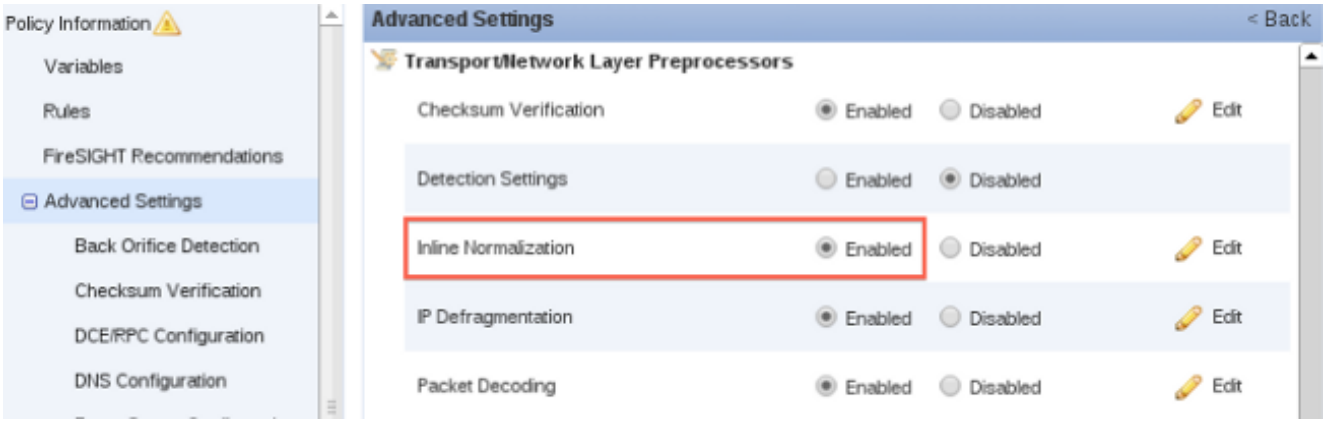
Habilitar la normalización en línea en las versiones 5.3 y anteriores

Complete estos pasos para habilitar la normalización en línea en una política de intrusiones:

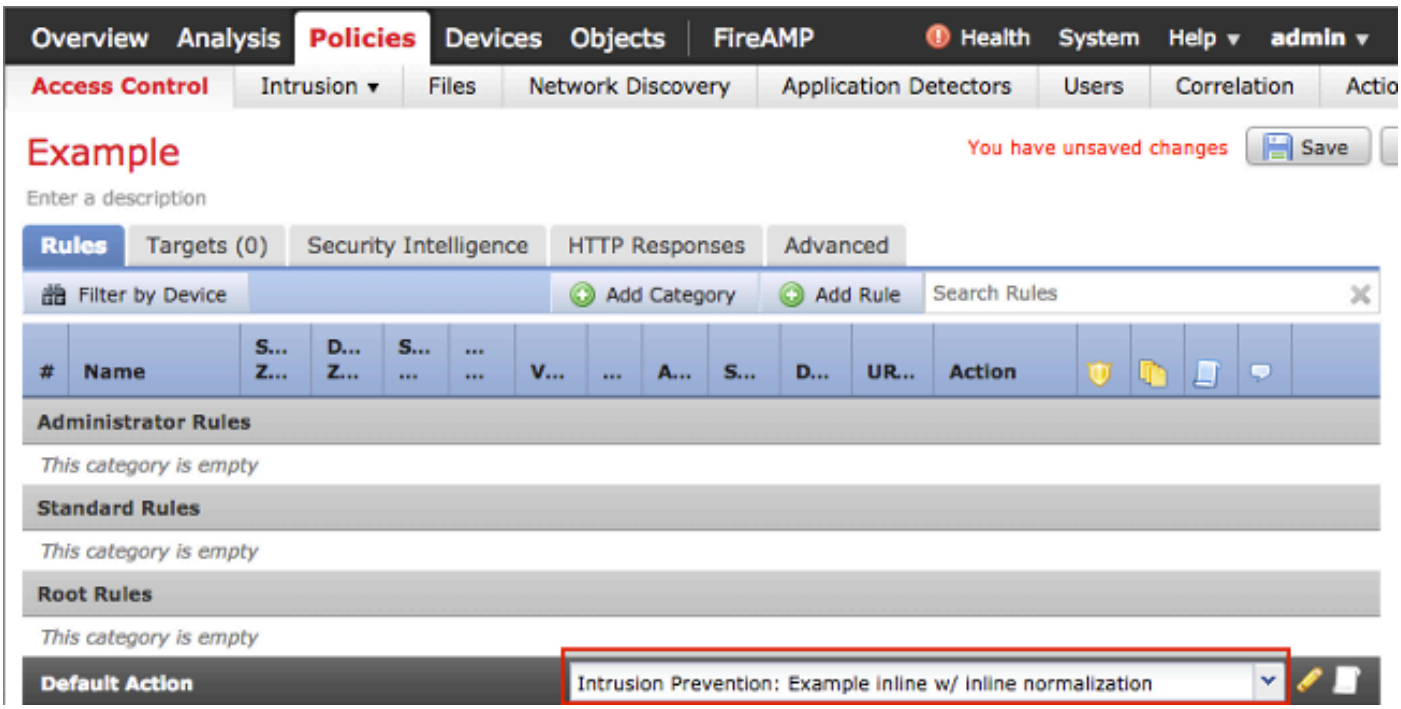
1. Inicie sesión en la interfaz de usuario web de FireSIGHT Management Center.
2. Vaya a **Políticas > Intrusión > Políticas de intrusión**.
3. Seleccione una *política de intrusiones* que desee aplicar al dispositivo gestionado.
4. Haga clic en el icono del *lápiz* para comenzar la edición, y aparecerá la página *Editar Política*.
5. Haga clic en **Advanced Settings** y aparecerá la página ***Advanced Settings***.

6. Localice la opción **Normalización en línea** en el área *Preprocesador de capa de transporte/red*.

7. Seleccione el botón de opción **Enabled** para habilitar esta función:



Una vez configurada la política de intrusiones para la normalización en línea, se debe agregar como la acción predeterminada en la política de control de acceso:



La política de control de acceso se debe aplicar al dispositivo que realiza la inspección.

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

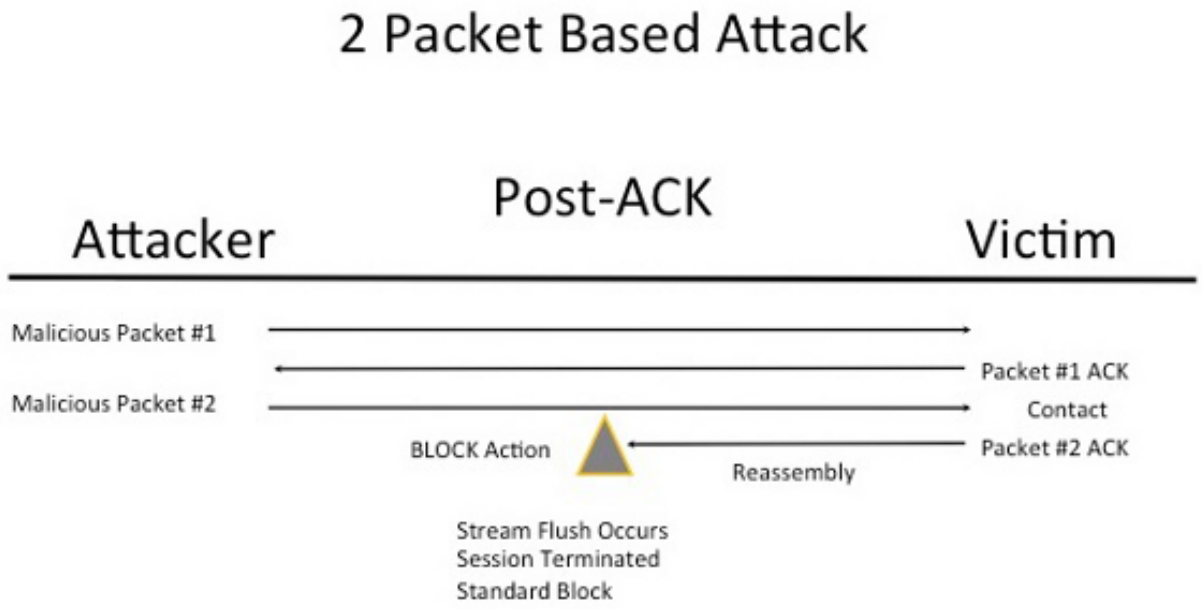
Activar inspección posterior al ACK e inspección previa al ACK

Después de habilitar el preprocesador de normalización en línea, puede editar la configuración para habilitar la opción *Normalize TCP Payload*. Esta opción del preprocesador de normalización en línea cambia entre dos modos de inspección diferentes:

- Confirmación posterior (posterior a ACK)
- Confirmación previa (previa a ACK)

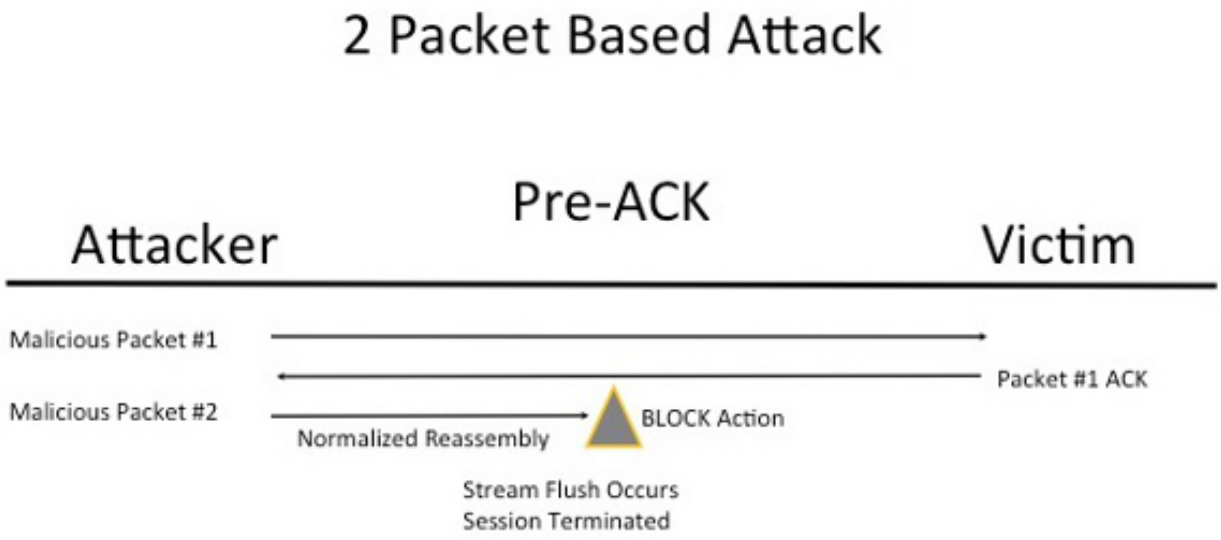
Comprender la inspección posterior al ACK (normalizar TCP/normalizar carga TCP deshabilitada)

En la inspección posterior al ACK, el sistema de prevención de intrusiones (IPS) recibe el reensamblado de flujo de paquetes, el vaciado (entrega al resto del proceso de inspección) y la detección en Snort después del reconocimiento (ACK) de la víctima del paquete que completa el ataque. Antes de que se produzca el vaciado de la secuencia, el paquete infractor ya ha llegado a la víctima. Por lo tanto, la alerta/caída se produce después de que el paquete ofensivo haya llegado a la víctima. Esta acción ocurre cuando el ACK de la víctima para el paquete ofensivo alcanza el IPS.



Comprender la inspección previa al ACK (normalizar TCP/normalizar carga útil TCP habilitada)

Esta función normaliza el tráfico inmediatamente después de la decodificación de paquetes y antes de que se procese cualquier otra función Snort para minimizar los esfuerzos de evasión de TCP. Esto garantiza que los paquetes que llegan al IPS son los mismos que los que se transmiten a la víctima. Snort descarta el tráfico en el paquete que completa el ataque antes de que el ataque llegue a su víctima.



Cuando habilita *Normalize TCP*, el tráfico que coincide con estas condiciones también se descarta:

- Copias retransmitidas de paquetes perdidos anteriormente
- Tráfico que intenta continuar una sesión que se ha interrumpido anteriormente
- Tráfico que coincide con cualquiera de estas reglas de preprocesador de flujo TCP:

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

  Nota: Para habilitar las alertas para las reglas de flujo TCP que son descartadas por el preprocesador de normalización, debe habilitar la función *Anomalías de inspección exhaustiva* en la configuración de flujo TCP.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).