# Configuración de la política de intrusiones y la configuración de firmas en el módulo Firepower (administración integrada)

## Contenido


Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configuración
Paso 1. Configuración de la política de intrusiones
Paso 1.1. Crear una política de intrusiones
Paso 1.2. Modificar la política de intrusiones
Paso 1.3. Modificar política base
Paso 1.4. Filtrado de firmas con opción de barra de filtro
Paso 1.5. Configuración del estado de regla
Paso 1.6. Configuración del filtro de eventos
Paso 1.7. Configuración del estado dinámico
Paso 2. Configuración de los conjuntos de variables y políticas de análisis de red (NAP) (opcional)
Paso 3: Configurar el control de acceso para incluir la política de intrusiones/ conjuntos de variables
Paso 4. Implementación de la política de control de acceso
Paso 5. Supervisar eventos de intrusión
Verificación
Troubleshoot
Información Relacionada


## Introducción

Este documento describe la funcionalidad del sistema de prevención de intrusiones (IPS)/sistema de detección de intrusiones (IDS) del módulo FirePOWER y varios elementos de la política de intrusiones que hacen una política de detección en el módulo FirePOWER.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

* Conocimiento del firewall Adaptive Security Appliance (ASA), Adaptive Security Device Manager (ASDM).

* Conocimiento del dispositivo FirePOWER.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X ) que ejecutan la versión de software 5.4.1 y superiores.

Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) que ejecuta la versión de software 6.0.0 y superior.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

FirePOWER IDS/IPS está diseñado para examinar el tráfico de red e identificar cualquier patrón (o firmas) malicioso que indique un ataque a la red o al sistema. El módulo FirePOWER funciona en modo IDS si la política de servicio del ASA está configurada específicamente en modo monitor (promiscuo) si no, funciona en modo en línea.

FirePOWER IPS/IDS es un enfoque de detección basado en firmas. El módulo FirePOWER en modo IDS genera una alerta cuando la firma coincide con el tráfico malintencionado, mientras que el módulo FirePOWER en modo IPS genera una alerta y bloquea el tráfico malintencionado.

> **Nota**: Asegúrese de que el módulo FirePOWER tenga la licencia **Protect** para configurar esta funcionalidad. Para verificar la licencia, navegue hasta **Configuration > ASA FirePOWER Configuration > License.**

## Configuración

### Paso 1. Configuración de la política de intrusiones

#### Paso 1.1. Crear una política de intrusiones

Para configurar la política de intrusiones, inicie sesión en Adaptive Security Device Manager (ASDM) y complete estos pasos:

Paso 1. Vaya a **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy**.

Paso 2. Haga clic en **Crear política**.

Paso 3. Introduzca el **nombre** de la política de intrusiones.

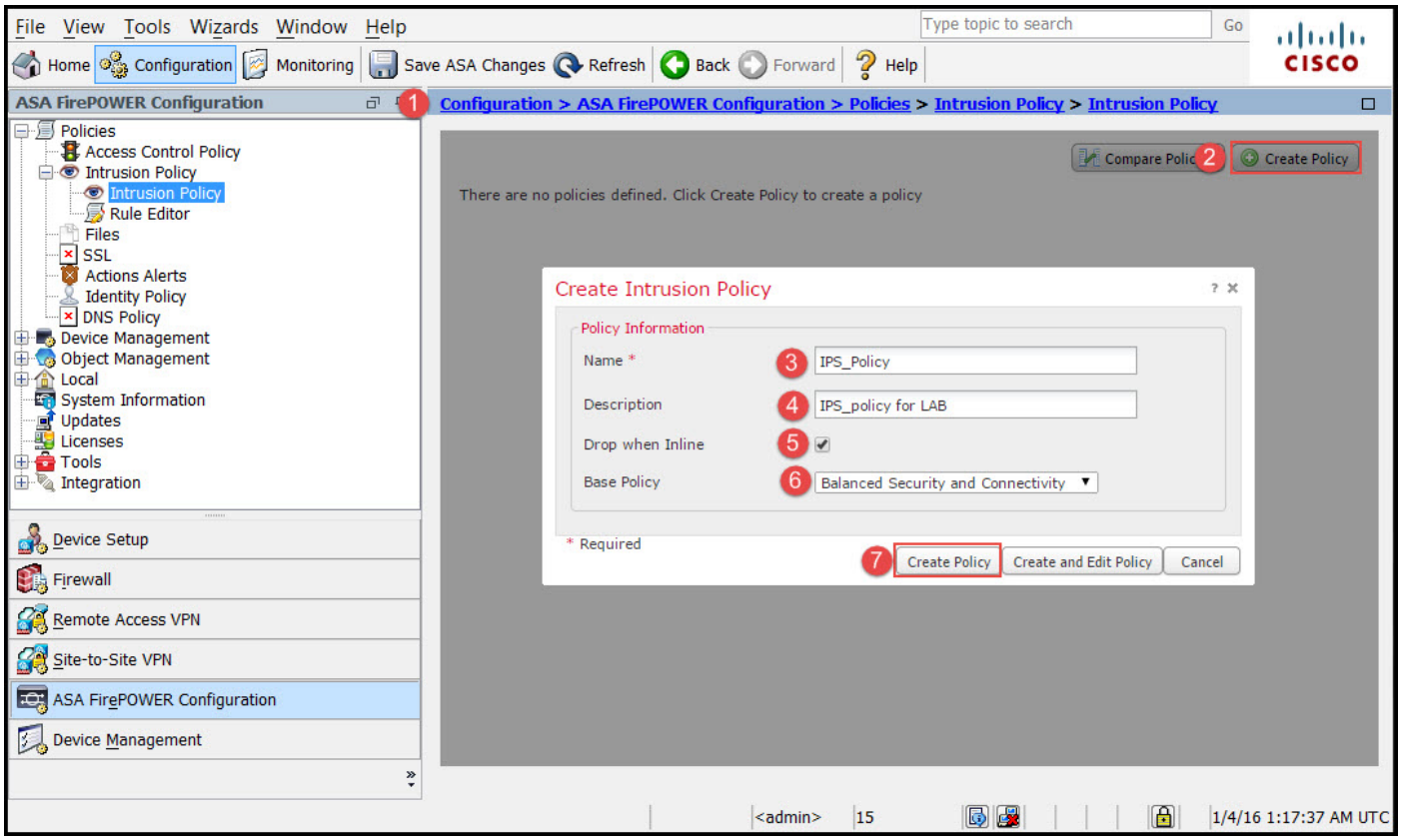
Paso 4. Introduzca la **descripción** de la política de intrusiones (opcional).

Paso 5. Especifique la opción **Drop when Inline**.

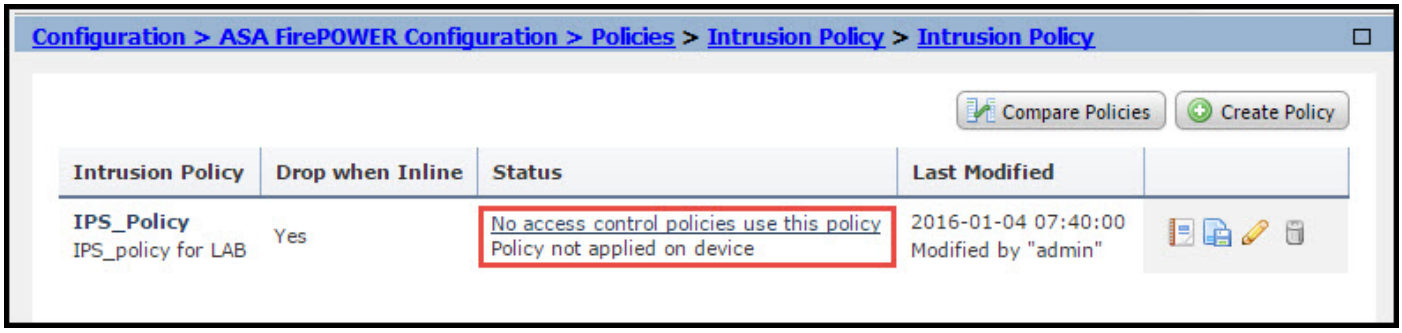
Paso 6. Seleccione la **Política base** de la lista desplegable.

Paso 7. Haga clic en **Crear política** para completar la creación de la política de intrusiones.

> **Sugerencia**: Soltar cuando la opción En línea es crucial en ciertos escenarios cuando el sensor se configura en el modo En línea y se requiere no descartar el tráfico aunque coincida con una firma que tenga una acción de descarte.

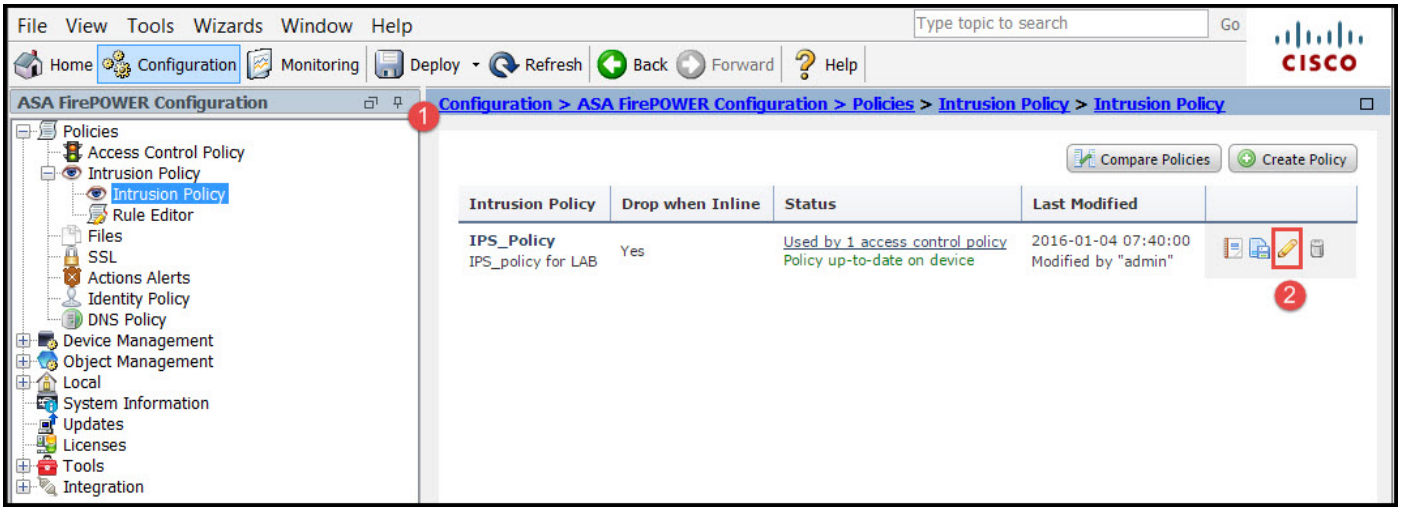



Puede observar que la política está configurada, sin embargo, no se aplica a ningún dispositivo.




## Paso 1.2. Modificar la política de intrusiones

Para modificar la política de intrusiones, navegue hasta **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy** y seleccione la **opción Edit**.

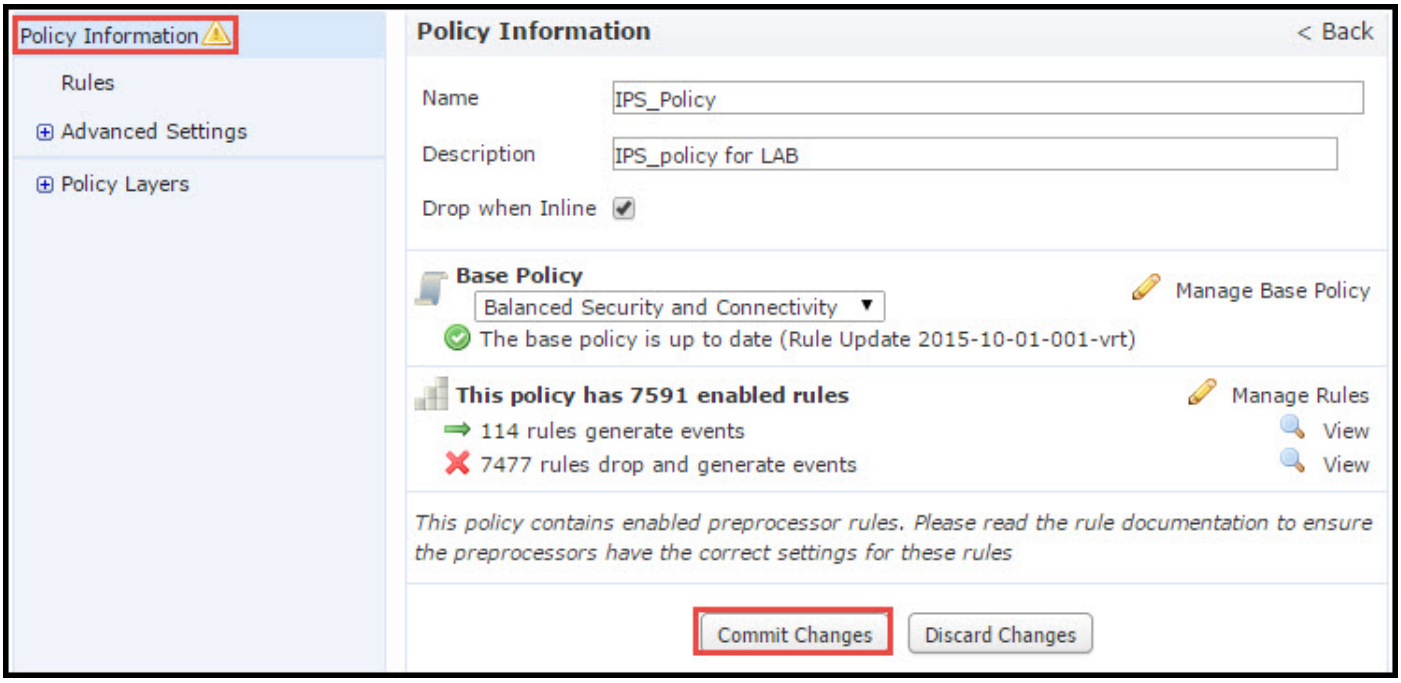



## Paso 1.3. Modificar política base

La página Intrusion Policy Management (Administración de directivas de intrusiones) ofrece la opción de cambiar la política base/ descartar cuando está en línea/ Guardar y descartar.

La política básica contiene algunas políticas proporcionadas por el sistema, que son políticas integradas.

1. Conectividad y seguridad equilibradas: se trata de una política óptima en términos de seguridad y conectividad. Esta política tiene habilitadas alrededor de 7500 reglas, algunas solo generan eventos mientras que otras generan eventos y descartan el tráfico.
2. Seguridad en lugar de conectividad: si prefiere la seguridad, puede elegir la seguridad en lugar de la política de conectividad, lo que aumenta el número de reglas activadas.
3. Conectividad sobre seguridad: si su preferencia es la conectividad en lugar de la seguridad, puede elegir la conectividad en lugar de la política de seguridad, lo que reducirá el número de reglas activadas.
4. Maximum Detection (Detección máxima): Seleccione esta política para obtener la máxima detección.
5. Sin regla activa: esta opción desactiva todas las reglas. Debe activar las reglas manualmente en función de su política de seguridad.




### Paso 1.4. Filtrado de firmas con opción de barra de filtro

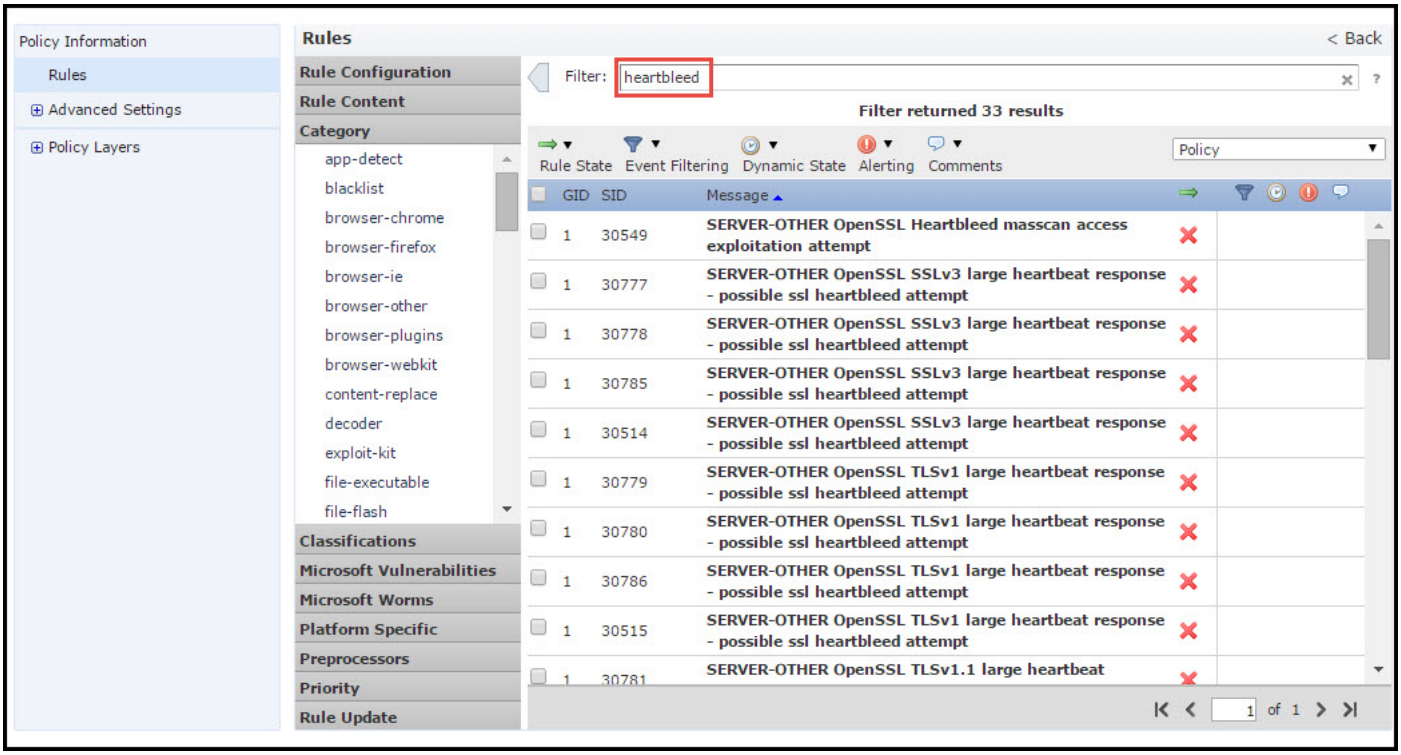
Navegue hasta la opción **Reglas** en el panel Navegación y aparecerá la página Administración de reglas. Hay miles de reglas en la base de datos de reglas. La barra de filtros proporciona una buena opción de motor de búsqueda para buscar la regla de forma eficaz.

Puede insertar cualquier palabra clave en la barra de filtros y el sistema obtiene los resultados. Si hay un requisito para encontrar la firma para la vulnerabilidad de la capa de conexión segura (SSL), puede buscar la cadena de palabras clave en la barra de filtros y obtendrá la firma para la vulnerabilidad de la hemorragia cardiaca.

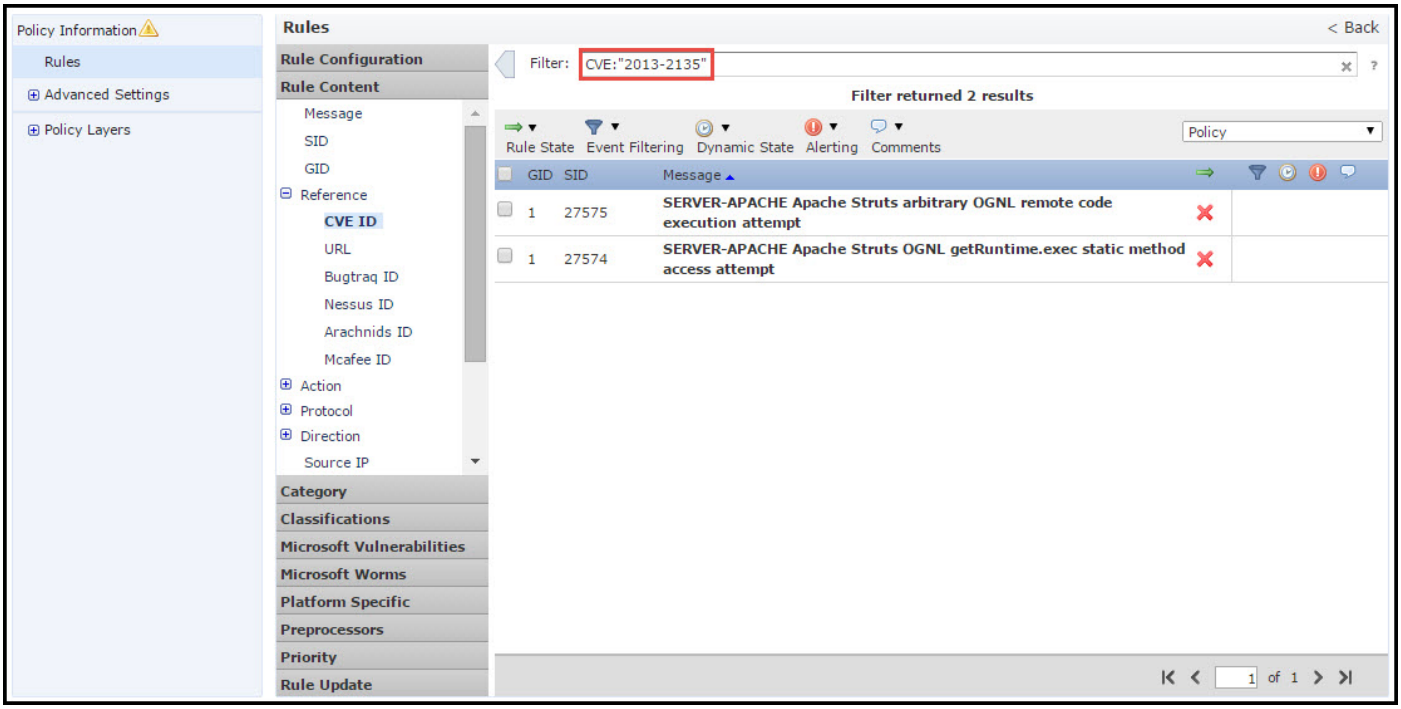
> **Sugerencia**: si se utilizan varias palabras clave en la barra de filtros, el sistema las combina utilizando la lógica AND para crear una búsqueda compuesta.

También puede buscar las reglas mediante la ID de firma (SID), la ID de generador (GID) y la Categoría: dos, etc.

Las reglas se dividen de forma eficaz en varias formas, por ejemplo, en función de categorías/clasificaciones/vulnerabilidades de Microsoft/gusanos de Microsoft/plataforma específica. Esta asociación de reglas ayuda al cliente a obtener la firma adecuada de una manera sencilla y ayuda al cliente a ajustar las firmas de forma eficaz.




También puede buscar con el número CVE para encontrar las reglas que los cubren. Puede utilizar la sintaxis **CVE: <cve-number>.**



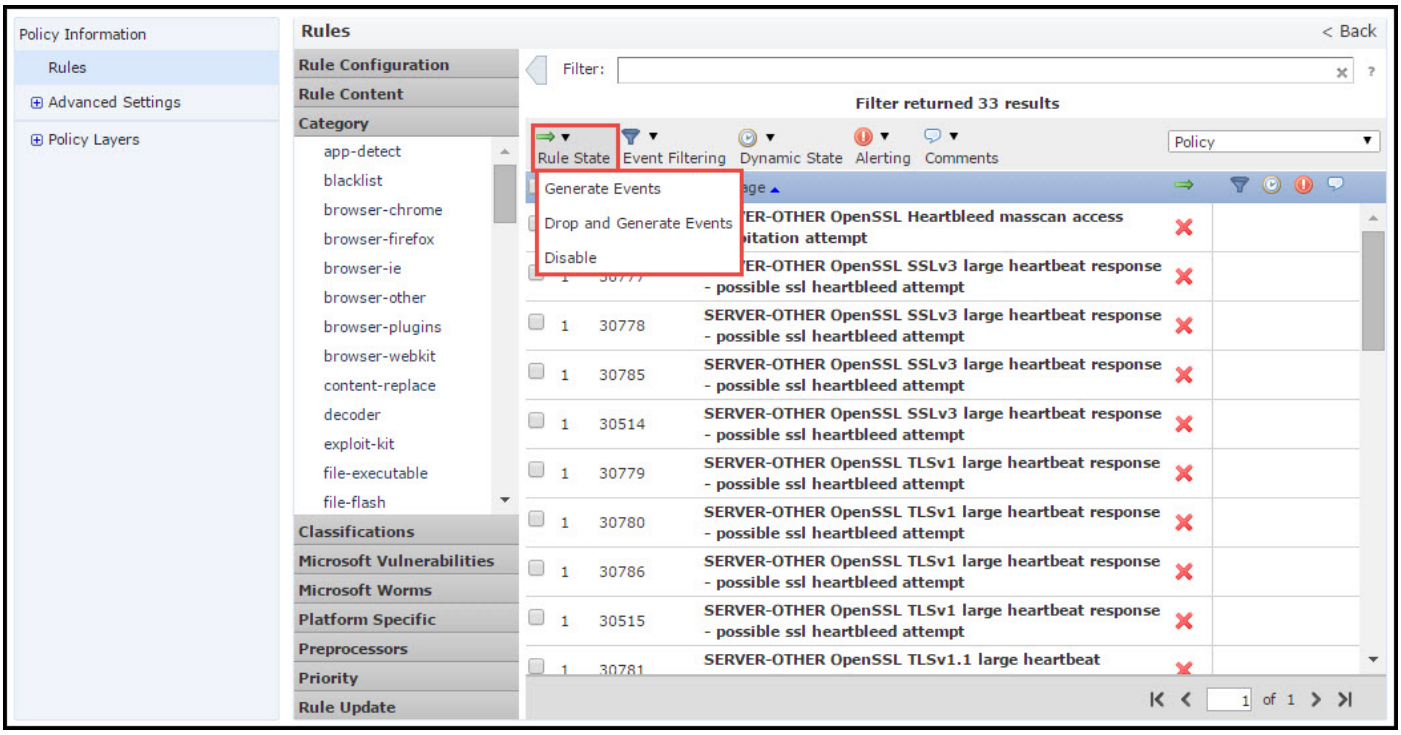

## Paso 1.5. Configuración del estado de regla

Vaya a **Reglas** en el panel de navegación y aparece la página Administración de reglas.. Seleccione las reglas y elija la opción **Estado de regla** para configurar el estado de las reglas. Hay tres estados que se pueden configurar para una regla:

1. **Generar eventos:** Esta opción genera eventos cuando la regla coincide con el tráfico.

2. **Drop and Generate Events:** Esta opción genera eventos y descarta tráfico cuando la regla coincide con el tráfico.

3. **Desactivar:** Esta opción inhabilita la regla.




## Paso 1.6. Configuración del filtro de eventos

La importancia de un evento de intrusión puede basarse en la frecuencia de aparición, o en la dirección IP de origen o de destino. En algunos casos, es posible que no le importe un evento hasta que haya ocurrido un determinado número de veces. Por ejemplo, es posible que no le preocupe si alguien intenta iniciar sesión en un servidor hasta que se produzcan fallos un determinado número de veces. En otros casos, es posible que sólo tenga que ver algunas incidencias de la regla para comprobar si existe un problema generalizado.

Hay dos maneras de lograr esto:

1. Umbral de evento.

2. Supresión de eventos.

### Umbral de evento

Puede establecer umbrales que dicten la frecuencia con la que se muestra un evento, en función del número de eventos. Puede configurar el umbral por evento y por política.

Pasos para configurar el umbral de evento:

Paso 1. Seleccione las **reglas** para las que desea configurar el umbral de evento.

Paso 2. Haga clic en **Event Filtering**.

Paso 3. Haga clic en el **Umbral**.

Paso 4. Seleccione el **tipo** de la lista desplegable. (Límite, Umbral o Ambos).

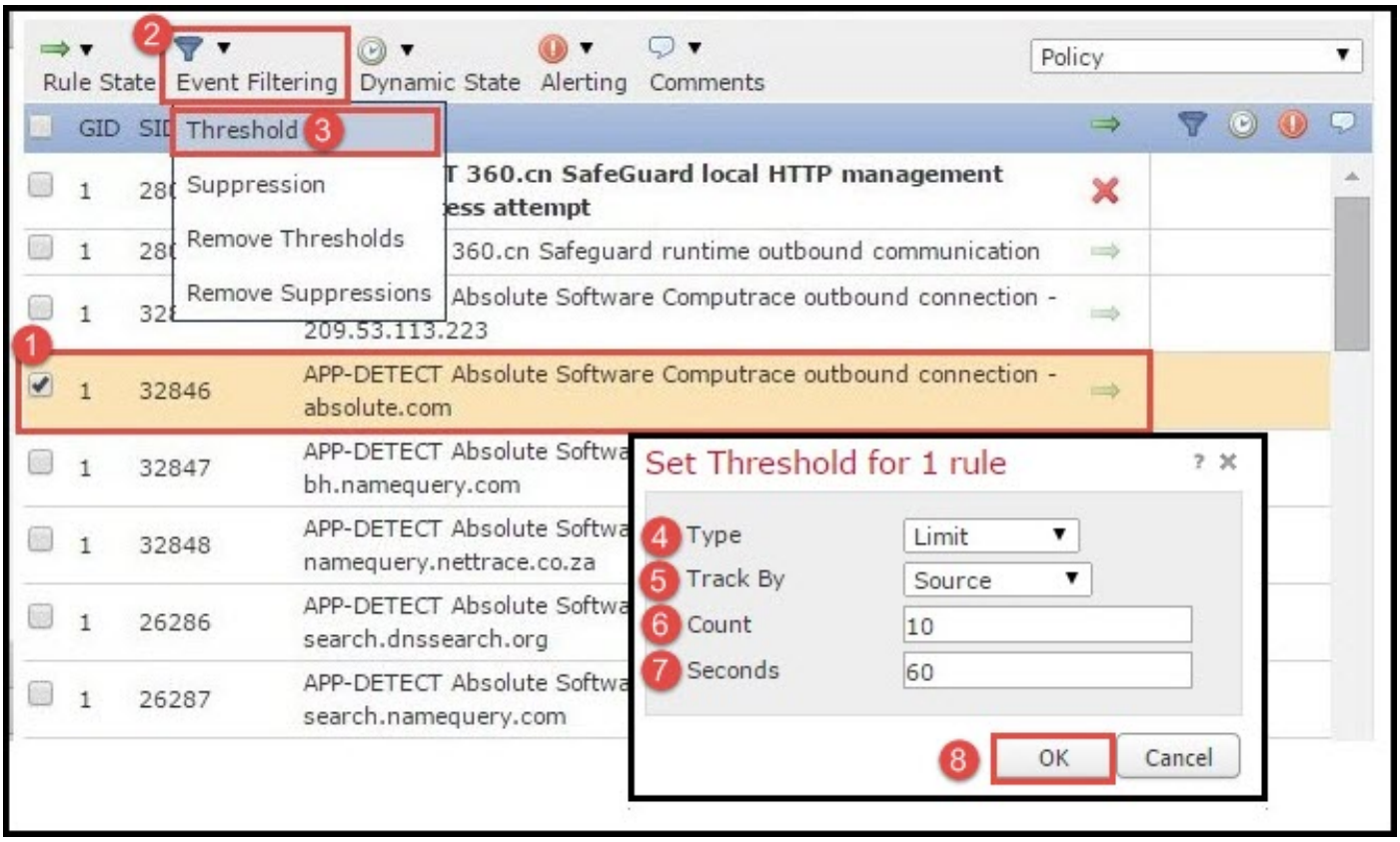
Paso 5. Seleccione cómo desea realizar el seguimiento en el cuadro de lista desplegable **Track**

**By**. (Origen o Destino).

Paso 6. Introduzca el **recuento** de eventos para cumplir el umbral.

Paso 7. Introduzca los **segundos** que deben transcurrir antes de que se reinicie el recuento.

Paso 8. Haga clic en **Aceptar** para completarlo.




Después de agregar un filtro de evento a una regla, debería poder ver un icono de filtro junto a la indicación de regla, que muestra que hay un filtrado de eventos habilitado para esta regla.

## Supresión de eventos

Las notificaciones de eventos especificados se pueden suprimir en función de la dirección IP de origen/ destino o por regla.

**Nota:** Cuando agrega supresión de eventos para una regla. La inspección de firma funciona como siempre, pero el sistema no genera los eventos si el tráfico coincide con la firma. Si especifica un origen/destino específico, los eventos no aparecen sólo para el origen/destino específico de esta regla. Si opta por suprimir la regla completa, el sistema no generará ningún evento para esta regla.

Pasos para configurar el umbral de evento:

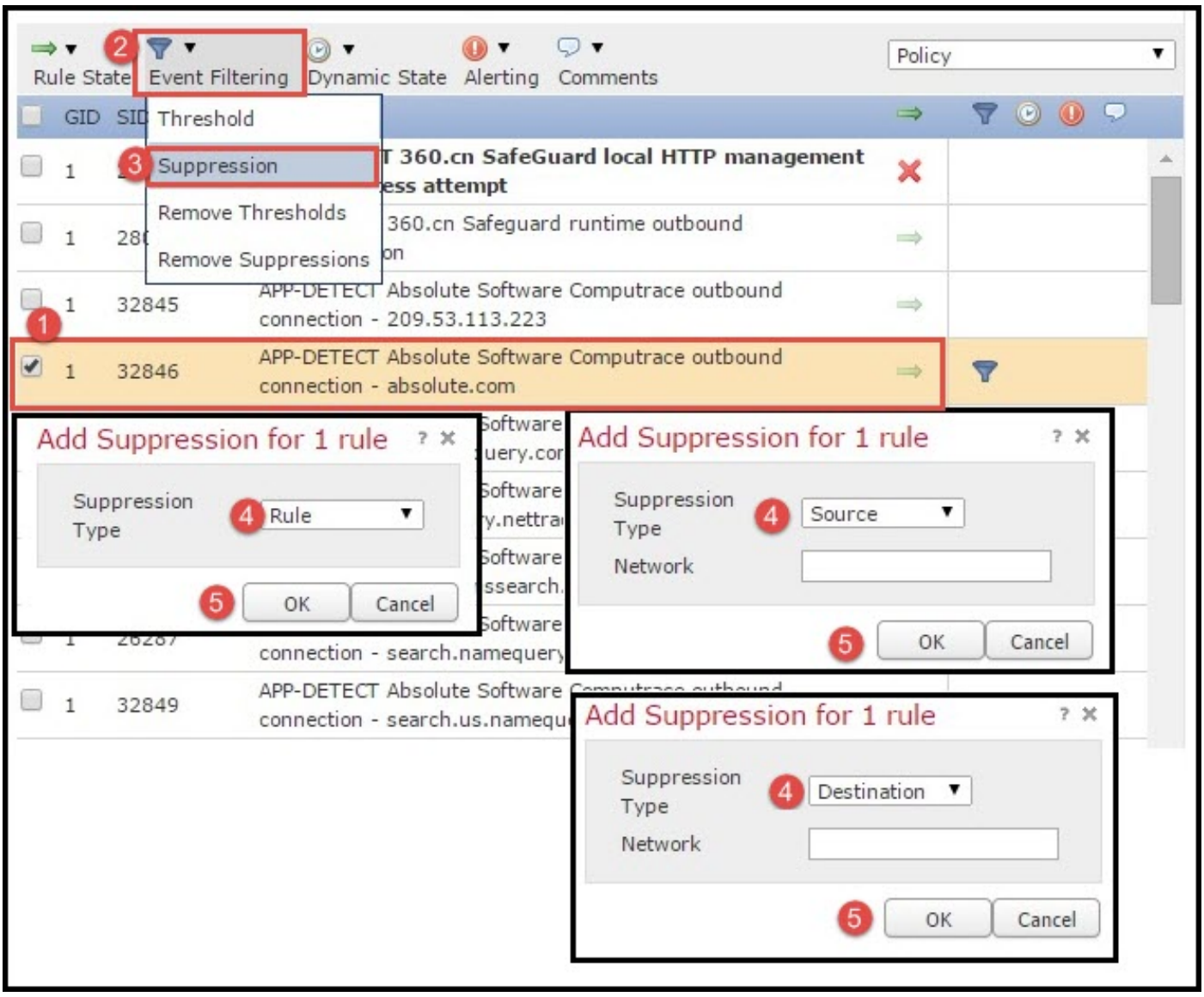
Paso 1. Seleccione las **reglas** para las que desea configurar el umbral de evento.

Paso 2. Haga clic en **Event Filtering**.

Paso 3. Haga clic en **Supresión.**

Paso 4. Seleccione **Suppression Type** en la lista desplegable. (Regla, Origen o Destino).

Paso 5. Haga clic en **Aceptar** para completarlo.




Después de agregar el filtro de eventos a esta regla, debería poder ver un icono de filtro con el recuento dos junto a la indicación de regla, que muestra que hay dos filtros de eventos habilitados para esta regla.

### Paso 1.7. Configuración del estado dinámico

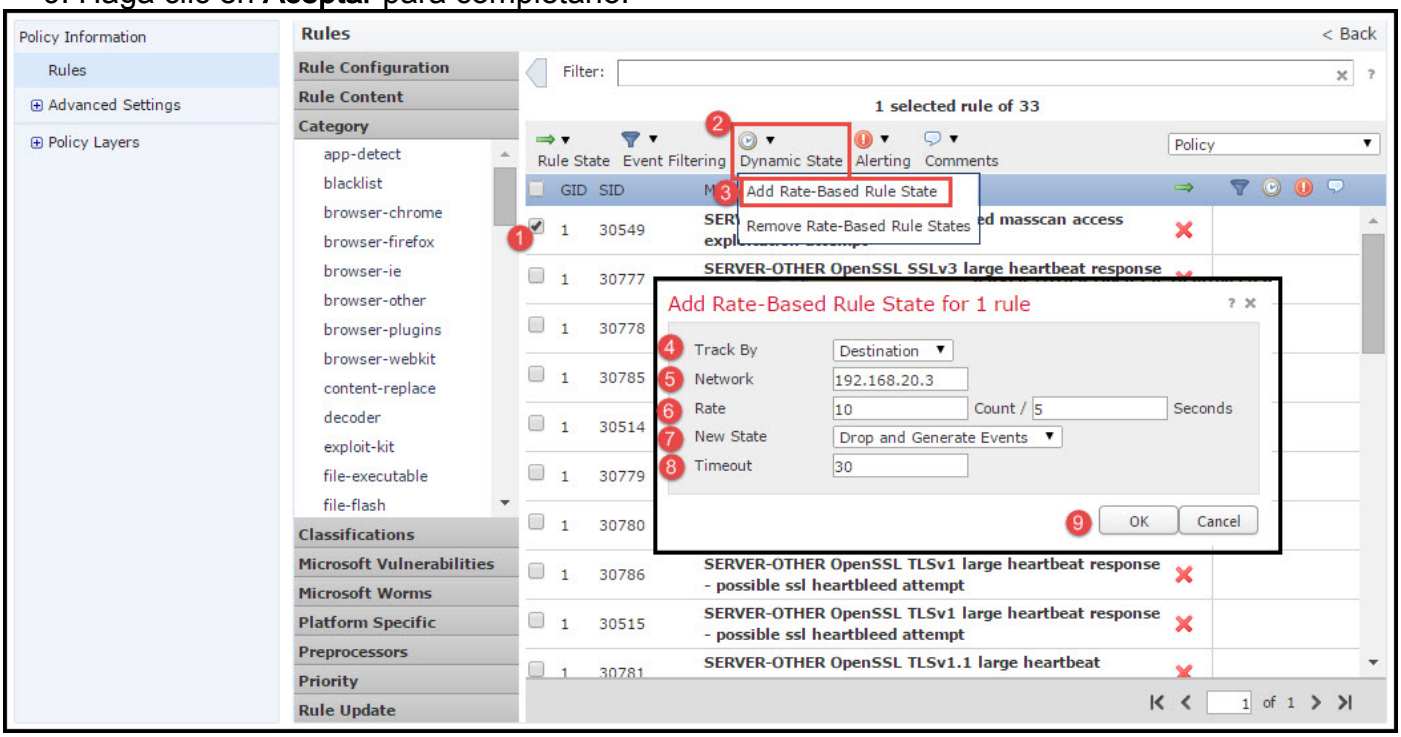
Es una función en la que podemos cambiar el estado de una regla si coincide la condición especificada.

Suponga un escenario de ataque de fuerza bruta para descifrar la contraseña. Si una firma detecta un intento de error de contraseña y la acción de regla es generar un evento. El sistema continúa generando la alerta para el intento de error de contraseña. Para esta situación, puede utilizar el **estado Dinámico** donde una acción de **Generar eventos** se puede cambiar a **Abandonar y Generar eventos** para bloquear el ataque de fuerza bruta.

Vaya a **Reglas** en el panel de navegación y en la página Administración de reglas. Seleccione la regla para la que desea habilitar el estado Dinámico y elija las opciones **Estado dinámico > Agregar un estado de regla base de velocidad.**

Para configurar el estado de regla basado en velocidad:

1. Seleccione las **reglas** para las que desea configurar el umbral de evento.
2. Haga clic en el **estado dinámico**.
3. Haga clic en **Agregar estado de regla basado en velocidad**.
4. Seleccione cómo desea realizar el seguimiento del estado de regla en el cuadro de lista desplegable **Track By**. (**Regla, Origen o Destino**).
5. Introduzca la **red**. Puede especificar una única dirección IP, bloque de direcciones, variable o una lista separada por comas que esté compuesta por cualquier combinación de estos.
6. Introduzca el **recuento** de eventos y la marca de tiempo en segundos.
7. Seleccione el **estado nuevo,** que desea definir para la regla.
8. Introduzca el **tiempo de espera** después del cual se revierte el estado de la regla.
9. Haga clic en **Aceptar** para completarlo.




## Paso 2. Configuración de los conjuntos de variables y políticas de análisis de red (NAP) (opcional)

### Configuración de la política de análisis de red

La política de acceso a la red también se conoce como preprocesadores. El preprocesador realiza el reensamblado de paquetes y normaliza el tráfico. Ayuda a identificar anomalías en la capa de red y el protocolo de capa de transporte al identificar opciones de encabezado inapropiadas.

NAP realiza la desfragmentación de los datagramas IP, proporciona la inspección con estado de TCP y el reensamblado de flujo y la validación de las sumas de comprobación. El preprocesador normaliza el tráfico, valida y verifica el estándar de protocolo.

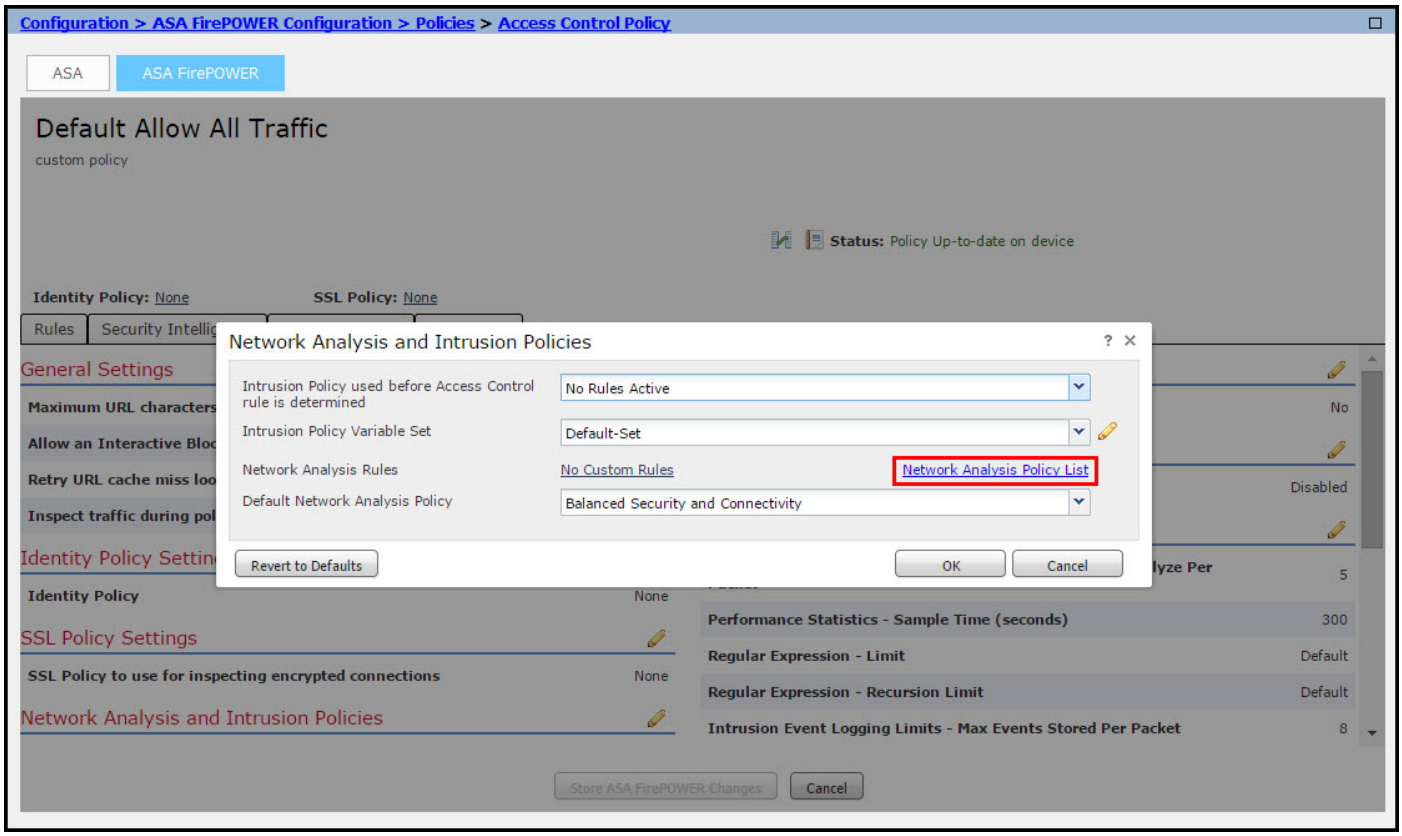
Cada preprocesador tiene su propio número GID. Representa el preprocesador que el paquete ha disparado.

Para configurar la política de análisis de red, vaya a **Configuración > Configuración de ASA FirePOWER > Políticas > Política de control de acceso > Avanzado > Análisis de red y Política de**

**intrusión**

La política de análisis de red predeterminada es Equilibrio entre seguridad y conectividad, lo que constituye una política óptima recomendada. Hay otras tres políticas NAP proporcionadas por el sistema que se pueden seleccionar en la lista desplegable.

Seleccione la opción **Network Analysis Policy** List para crear una política NAP personalizada.




**Configurar conjuntos de variables**

Los conjuntos de variables se utilizan en las reglas de intrusión para identificar las direcciones de origen y destino y los puertos. Las reglas son más eficaces cuando las variables reflejan su entorno de red con mayor precisión. La variable desempeña un papel importante en el ajuste del rendimiento.

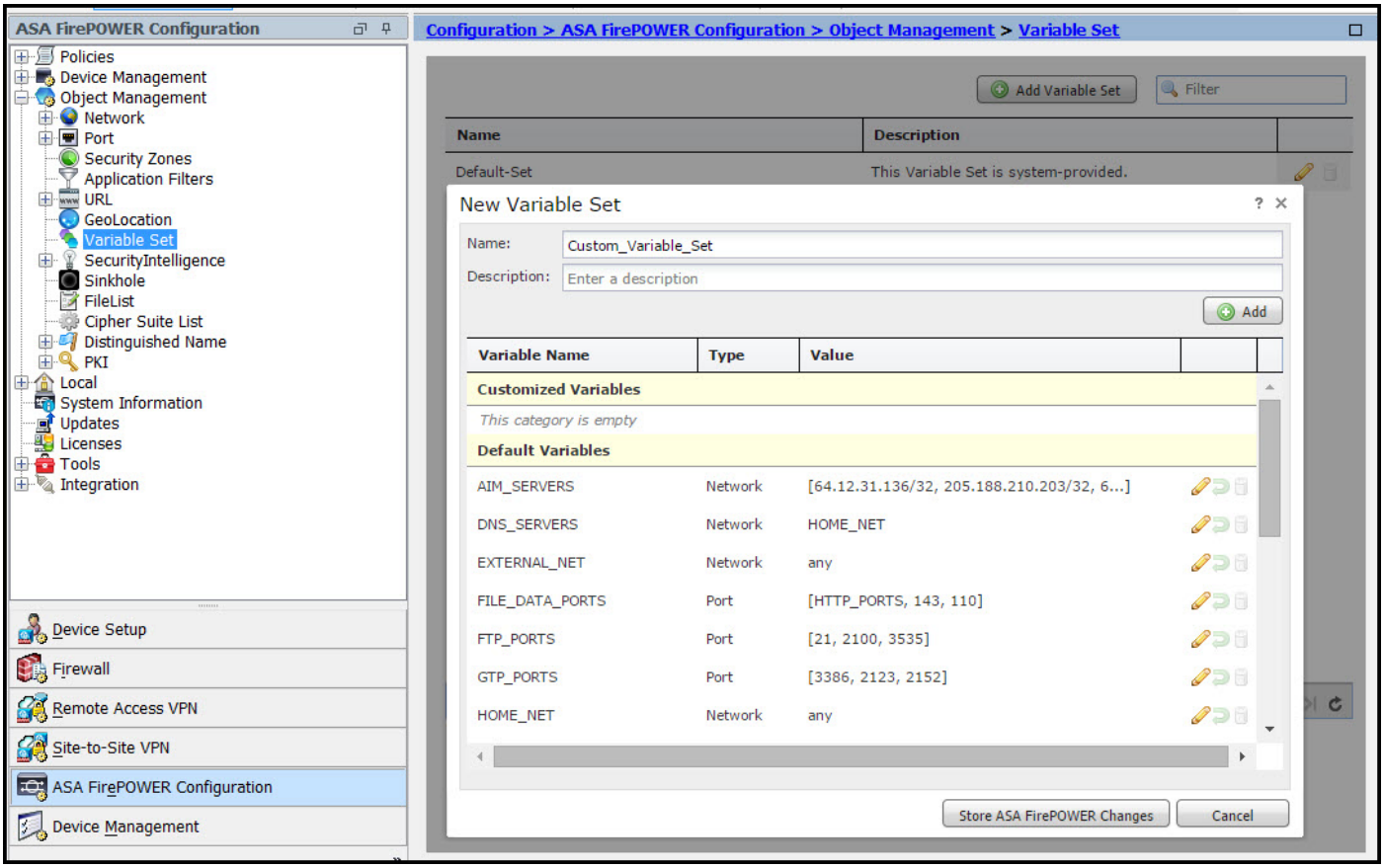
Los conjuntos de variables ya se han configurado con la opción predeterminada (Red/Puerto). Agregue nuevos conjuntos de variables si desea cambiar la configuración predeterminada.

Para configurar los conjuntos de variables, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > Variable Set**. Seleccione la opción **Añadir conjunto de variables** para agregar nuevos conjuntos de variables. Introduzca el **nombre** de los conjuntos de variables y especifique la **descripción.**

Si alguna aplicación personalizada funciona en un puerto específico, defina el número de puerto en el campo Número de puerto. Configure el parámetro de red.

**$Home_NET** especifique la red interna.

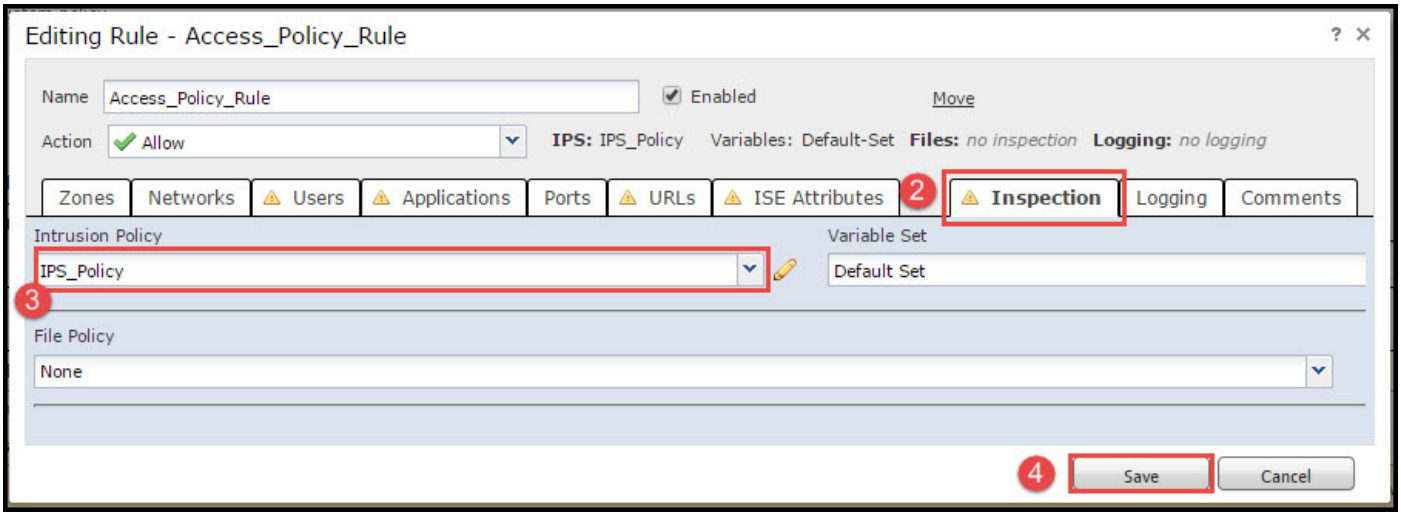
**$External_NET** especifique la red externa.



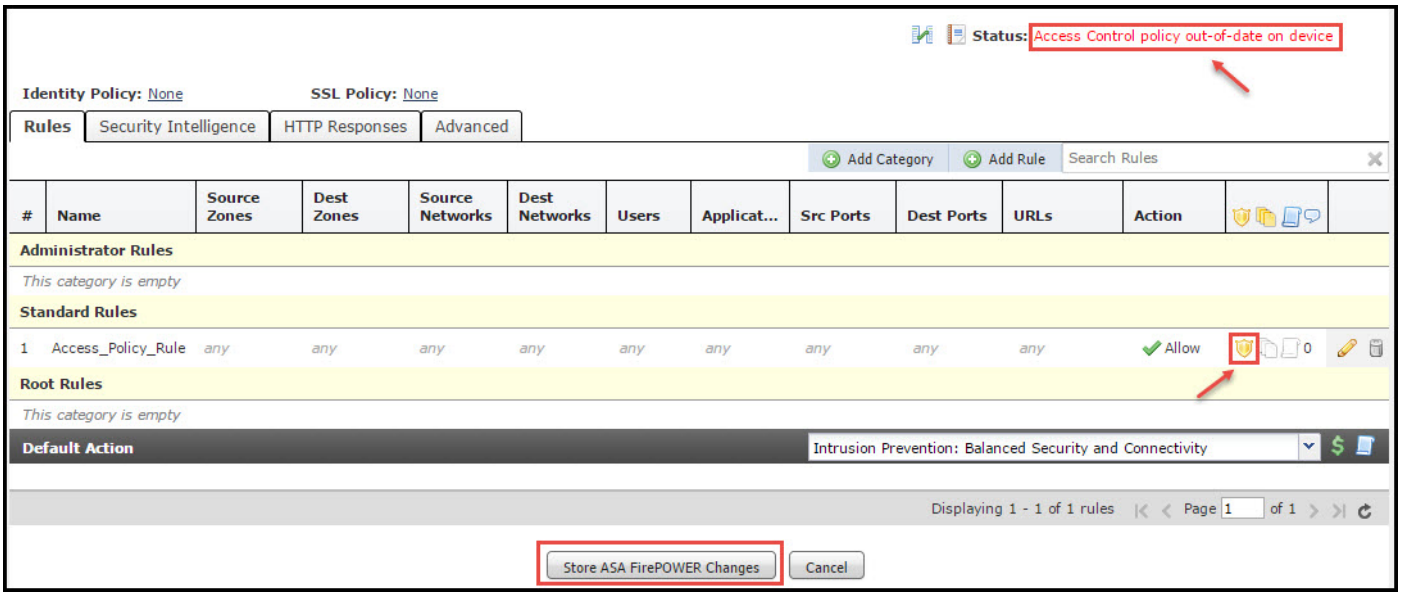

## Paso 3: Configurar el control de acceso para incluir conjuntos de políticas de intrusión/ NAP/ Variable

Vaya a **Configuration > ASA Firepower Configuration > Policies > Access Control Policy .** Debe completar estos pasos:

1. Edite la regla de directiva de acceso donde desea asignar la directiva de intrusión.
2. Elija la pestaña **Inspección.**
3. Elija la **política de intrusiones** de la lista desplegable y elija los **conjuntos de variables** de la lista desplegable
4. Click Save.

Puesto que se agrega una política de intrusiones a esta regla de directiva de acceso. Puede ver el icono de escudo en Color dorado que indica que la política de intrusiones está activada.

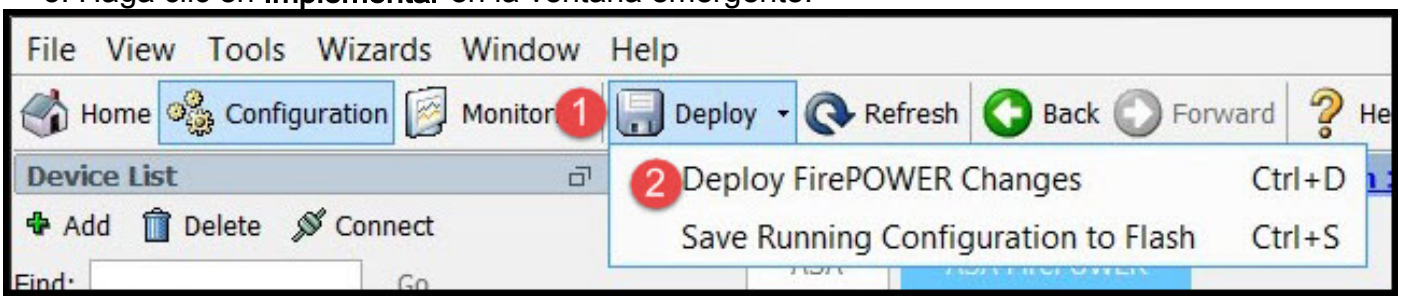



Haga clic en **Store ASA FirePOWER changes** para guardar los cambios.

## Paso 4. Implementación de la política de control de acceso

Ahora, debe implementar la política de control de acceso. Antes de aplicar la política, verá una indicación de Directiva de control de acceso desactualizada en el dispositivo. Para implementar los cambios en el sensor:

1. Haga clic en **Implementar**.
2. Haga clic en **Implementar cambios de FirePOWER**.
3. Haga clic en **Implementar** en la ventana emergente.

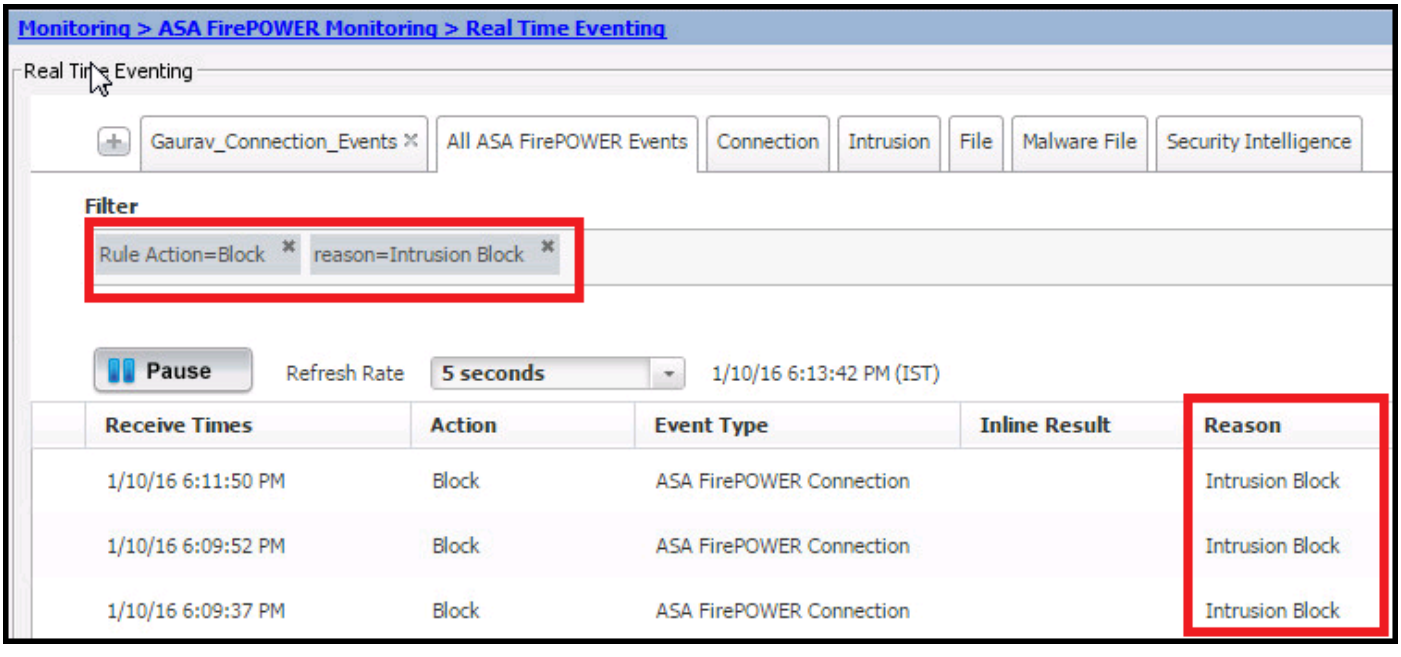



**Nota**: En la versión 5.4.x, para aplicar la política de acceso al sensor, debe hacer clic en Aplicar cambios de ASA FirePOWER

**Nota:** Vaya a **Monitoring > ASA Firepower Monitoring > Task Status .** Asegúrese de que la tarea debe completarse para aplicar el cambio de configuración.

## Paso 5. Supervisar eventos de intrusión

Para ver los eventos de intrusión generados por el módulo FirePOWER, vaya a **Monitoring > ASA FirePOWER Monitoring > Real Time Event.**



# Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

# Troubleshoot

Paso 1. Asegúrese de que el estado de regla de las reglas está configurado correctamente.

Paso 2. Asegúrese de que la política IPS correcta se ha incluido en las reglas de acceso.

Paso 3. Asegúrese de que los conjuntos de variables estén configurados correctamente. Si los conjuntos de variables no están configurados correctamente, las firmas no coincidirán con el tráfico.

Paso 4. Asegúrese de que la implementación de la política de control de acceso se complete correctamente.

Paso 5. Supervise los eventos de conexión y los eventos de intrusión para verificar si el flujo de tráfico está llegando a la regla correcta o no.

## Información Relacionada

- **Guía de inicio rápido del módulo Cisco ASA FirePOWER**
- **Soporte Técnico y Documentación - Cisco Systems**