Directiva de la intrusión de la configuración y configuración de la firma en el módulo de FirePOWER (Administración del En-cuadro)

Contenido

Introducción

Este documento describe las funciones del sistema de detección del Sistema de prevención de intrusiones (IPS) /Intrusion (IDS) del módulo de FirePOWER y los elementos de la diversa directiva de la intrusión que hacen una directiva de la detección en el módulo de FirePOWER.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

* Conocimiento del Firewall adaptante del dispositivo de seguridad (ASA), Administrador de

dispositivos de seguridad adaptante (ASDM).

* Conocimiento del dispositivo de FirePOWER.

Componentes Utilizados

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

Versión de software corriente 5.4.1 de los módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) y más alto.

Versión de software corriente 6.0.0 del módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) y más alto.

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 su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Antecedentes

FirePOWER IDS/IPS se diseña para examinar el tráfico de la red y para identificar cualquier modelo malévolo (o las firmas) que indique un ataque de la red/del sistema. El módulo de FirePOWER funciona en el modo IDS si la servicio-directiva ASA se configura específicamente en el modo monitor (promiscuo), él trabaja en el modo en línea.

FirePOWER IPS/IDS es un acercamiento basado en firmas de la detección. FirePOWERmodule en el modo IDS genera una alerta cuando la firma hace juego el tráfico malévolo, mientras que el módulo de FirePOWER en el modo IPS genera el tráfico malévolo de la alerta y del bloque.

> **Note**: Asegúrese de que el módulo de FirePOWER deba tener **proteger la** licencia de configurar estas funciones. Para verificar la licencia, navegue a la **configuración > a la configuración > a la licencia ASA FirePOWER.**

Configuración

Paso 1. Directiva de la intrusión de la configuración

Paso 1.1. Cree la directiva de la intrusión

Para configurar la directiva de la intrusión, inicie sesión al Administrador de dispositivos de seguridad adaptante (ASDM) y complete estos pasos:

Paso 1. Navegue a la **configuración > a la configuración ASA FirePOWER > a las directivas > a la directiva de la intrusión > a la directiva de la intrusión**.

Paso 2. Haga clic la **directiva del crear**.

Paso 3. Ingrese el **nombre de la** directiva de la intrusión.

Paso 4. Ingrese la **descripción de la** directiva de la intrusión (opcional).

Paso 5. Especifique el **descenso cuando** opción **en línea**.

Paso 6. Seleccione la **directiva baja del** menú desplegable.

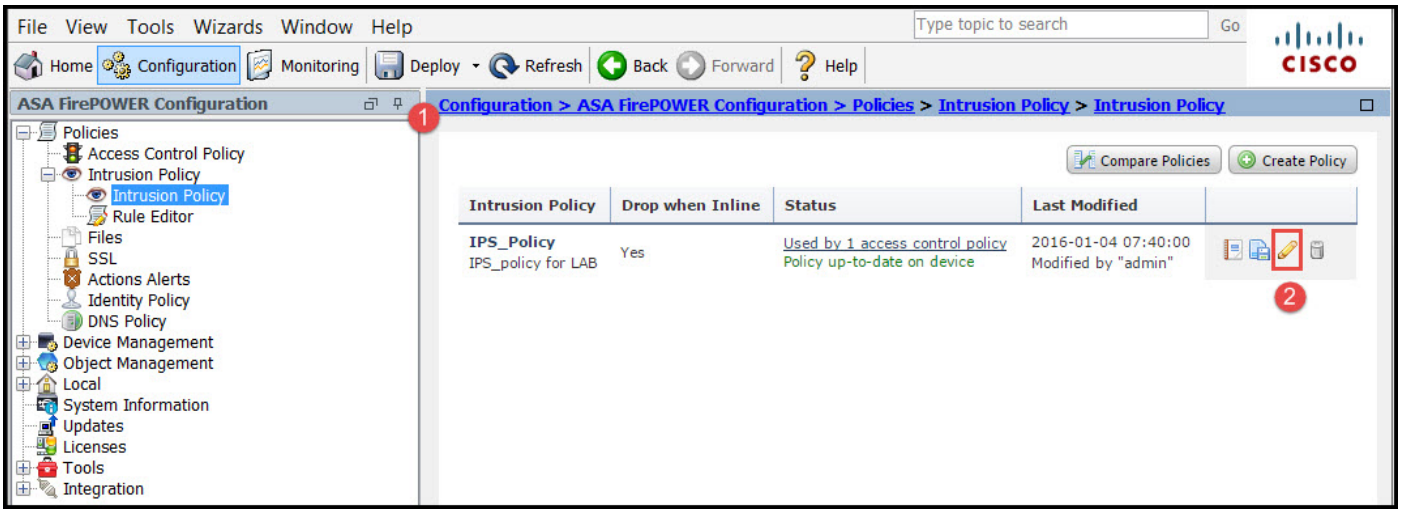
Paso 7. El tecleo **crea la directiva** para completar la creación de la directiva de la intrusión.

> **Tip**: Caiga cuando la opción en línea es crucial en ciertos escenarios cuando el sensor se configura en el modo en línea y se requiere para no caer el tráfico aunque hace juego una firma que tenga una acción de descarte.

Usted puede notar que la directiva está configurada, sin embargo, no está aplicada a ningún dispositivo.

Paso 1.2. Modifique la directiva de la intrusión

Para modificar la directiva de la intrusión, navegar a la **configuración > a la configuración ASA FirePOWER > a las directivas > a la directiva de la intrusión > a la directiva de la intrusión** y a selecto **edite la** opción.



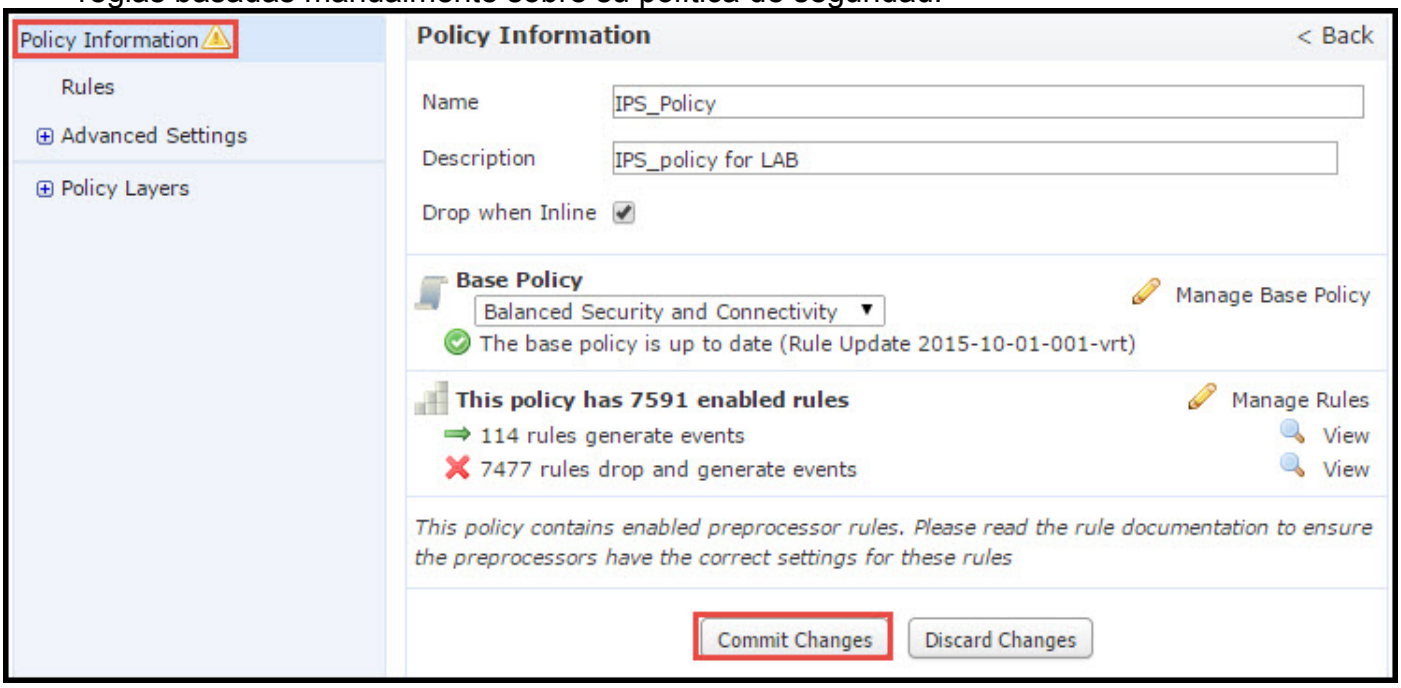
Paso 1.3. Modifique la directiva baja

La página de la Administración de políticas de la intrusión da la opción para cambiar el descenso bajo de la directiva cuando en línea opción de la salvaguardia y del descarte.

La directiva baja contiene alguno sistema-proporcionó a las directivas, que son directivas incorporadas.

1. Seguridad y Conectividad equilibradas: Es una directiva óptima en términos de Seguridad y Conectividad. Esta directiva tiene alrededor 7500 reglas habilitadas, algunas de ellas generan solamente los eventos mientras que otras generan los eventos así como caen el tráfico.
2. Seguridad sobre la Conectividad: Si su preferencia es Seguridad entonces usted puede elegir la Seguridad sobre la política de conectividad, que aumenta el número de reglas habilitadas.

3. Conectividad sobre la Seguridad: Si su preferencia es Conectividad bastante que Seguridad entonces usted puede elegir la Conectividad sobre la política de seguridad que reducirá el número de reglas habilitadas.
4. Detección máxima - Seleccione esta directiva para conseguir la detección máxima.
5. Ningún Active de la regla - Esta opción inhabilita todas las reglas. Usted necesita habilitar las reglas basadas manualmente sobre su política de seguridad.



Paso 1.4. Firma que filtra con la opción de la barra del filtro

Navegue a la opción de las **reglas** en el panel navegacional y la página de la Administración de la regla aparece. Hay millares de la regla en la base de datos de la regla. La barra del filtro proporciona una buena opción del motor de búsqueda para buscar la regla con eficacia.

Usted puede insertar cualquier palabra clave en la barra del filtro y el sistema ase los resultados para usted. Si hay un requisito de encontrar que la firma para Secure Sockets Layer (SSL) heartbleed la vulnerabilidad, usted puede buscar la palabra clave heartbleed en la barra del filtro y traerá la firma para la vulnerabilidad heartbleed.

> **Tip**: Si las palabras claves múltiples se utilizan en la barra del filtro entonces el sistema las combina que usan Y la lógica para crear un compuesto busca.

Usted puede también buscar las reglas usando el ID de la firma (SID), el generador ID (GID), categoría: DOS etc.

Las reglas se dividen con eficacia en las diferentes formas tales como basado en las vulnerabilidades de Microsoft de las clasificaciones de la categoría/el específico de la plataforma de los gusanos de Microsoft. Tal asociación de las reglas ayuda al cliente a conseguir la firma derecha en una forma sencilla y a ayudar al cliente a ajustar con eficacia las firmas.

Usted puede también buscar con CVE el número para encontrar las reglas que las cubren. Usted puede utilizar el sintaxis **CVE: <cve-number>.**

Paso 1.5. Configure el estado de la regla

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

1. **Genere los eventos: Esta opción genera los eventos cuando la regla hace juego el tráfico.**

2. **Caiga y genere los eventos: Esta opción genera los eventos y el tráfico del descenso cuando la regla hace juego el tráfico.**

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

Paso 1.6. Configuración del filtro del evento

La importancia de un evento de la intrusión se puede basar en la frecuencia de evento, o en la fuente o el IP Address de destino. En algunos casos, usted no puede cuidar sobre un evento hasta que haya ocurrido algunas veces. Por ejemplo, usted puede ser que no sea referido si alguien intenta iniciar sesión a un servidor hasta que fallen algunas veces. En otros casos, usted puede ser que necesite solamente ver algunos acontecimientos del golpe de la regla para marcar si hay un problema extenso.

Hay dos maneras por las cuales usted puede alcanzar esto:

1. Umbral del evento.

2. Supresión del evento.

Umbral del evento

Usted puede fijar los umbrales que dictan cuantas veces se visualiza un evento, sobre la base del número de acontecimientos. Usted puede configurar la formación de umbrales por el evento y por la directiva.

Pasos para configurar el umbral del evento:

Paso 1. Seleccione las **reglas** para las cuales usted quiere configurar el umbral del evento.

Paso 2. Haga clic el **filtrado de eventos**.

Paso 3. Haga clic el **umbral**.

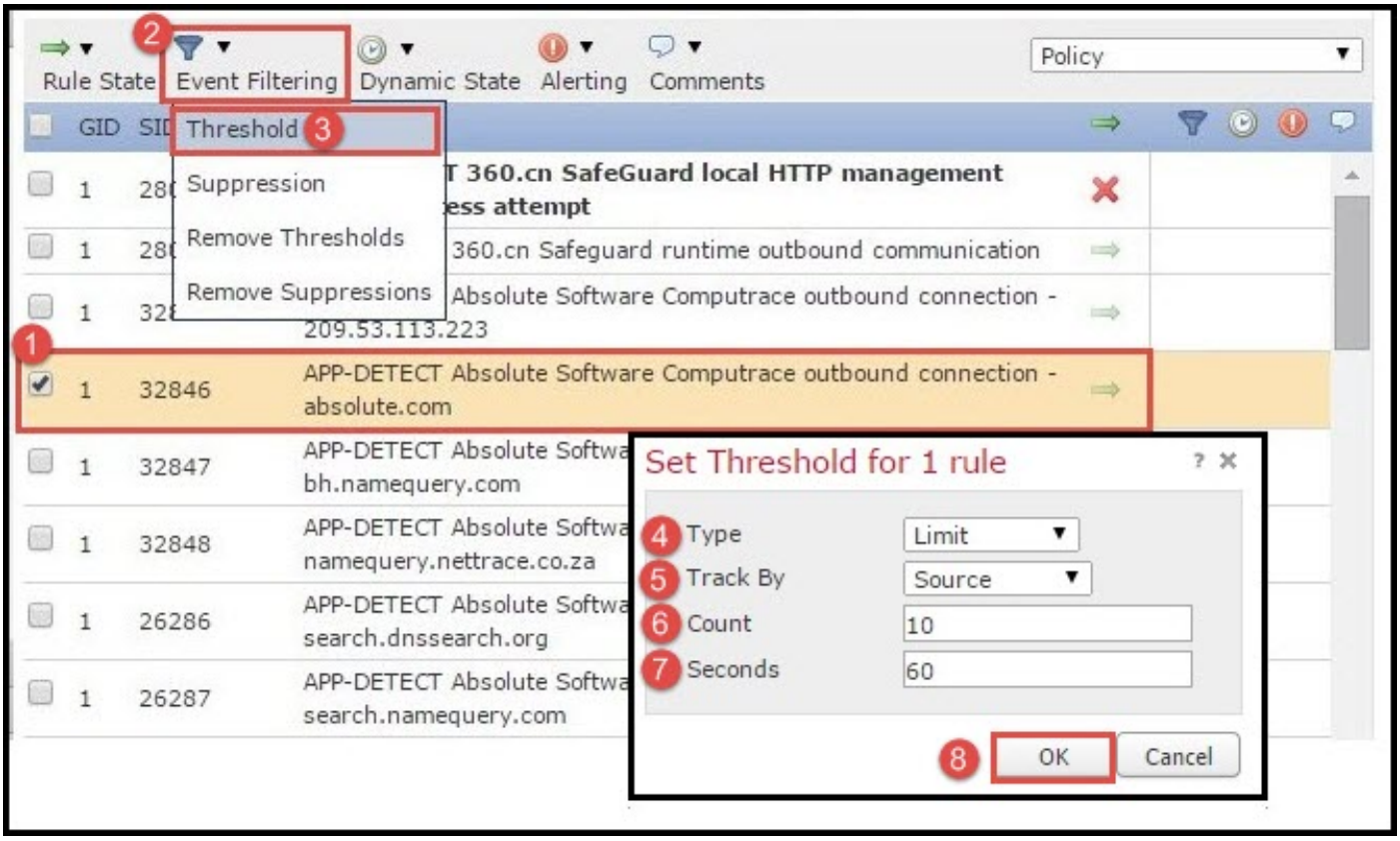
Paso 4. Seleccione el **tipo del** menú desplegable. (Límite o umbral o ambos).

Paso 5. Seleccione cómo usted quiere seguir de la **pista por el** cuadro del descenso. (Fuente o destino).

Paso 6. Ingrese la **cuenta de los** eventos para resolver el umbral.

Paso 7. Ingrese los **segundos** para transcurrir antes de las restauraciones de la cuenta.

Paso 8. Haga Click en OK a completar.



Después de que un filtro del evento se agregue a una regla, usted debe poder ver un icono del filtro al lado de la indicación de la regla, que muestra que hay un filtrado de eventos habilitado para esta regla.

Supresión del evento

Las notificaciones especificadas de los eventos se pueden suprimir en base del IP Address de destino de la fuente o por la regla.

Note: Cuando usted agrega la supresión del evento para una regla. El examen de la firma trabaja como normalmente pero el sistema no genera los eventos si el tráfico hace juego la firma. Si usted especifica una fuente/un destino específicos entonces los eventos no aparecen solamente para la fuente/el destino específicos para esta regla. Si usted elige suprimir la regla completa entonces el sistema no genera ningún evento para esta regla.

Pasos para configurar el umbral del evento:

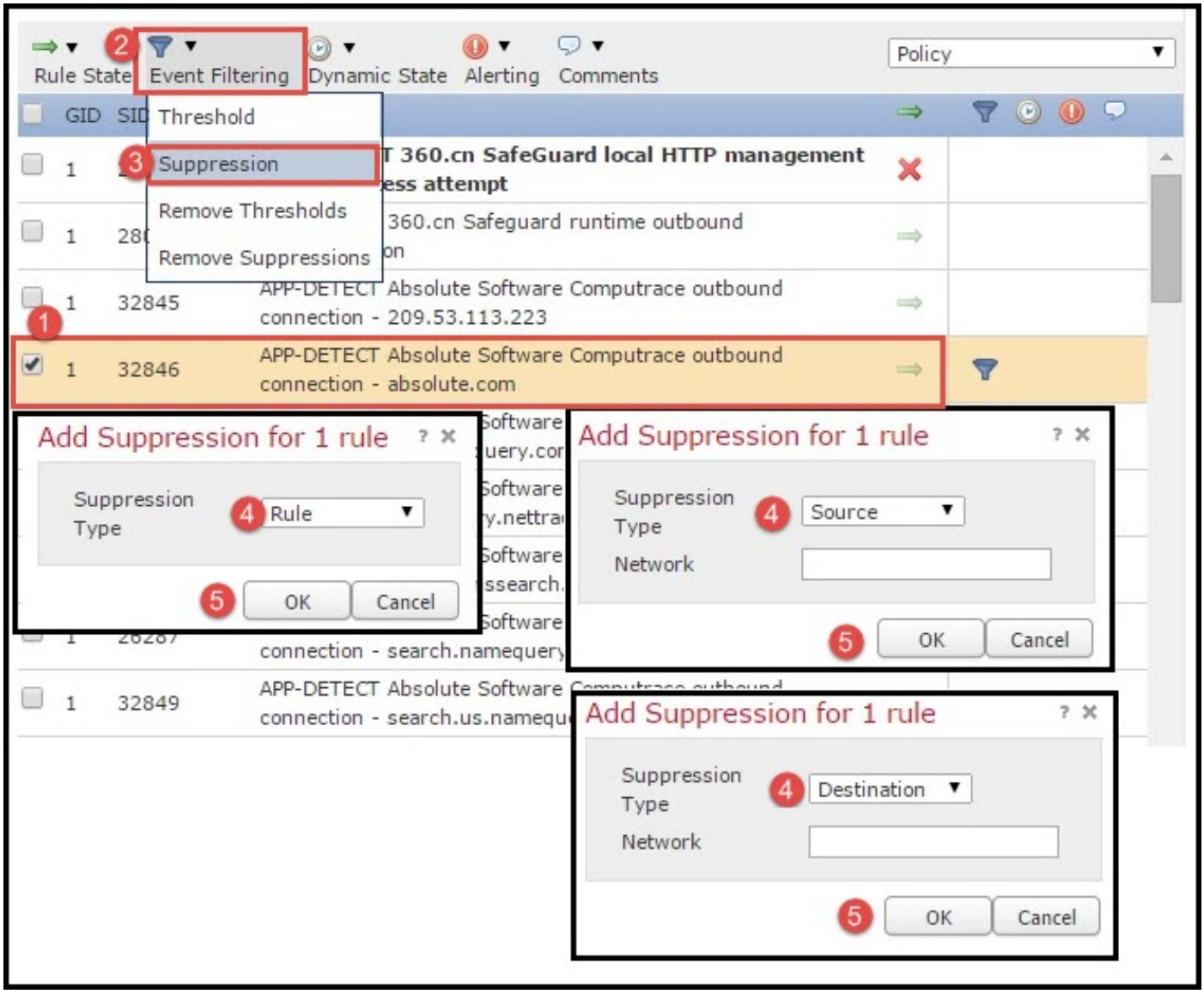
Paso 1. Seleccione las **reglas** para las cuales usted quiere configurar el umbral del evento.

Paso 2. **Filtración del** evento click.

Paso 3. **Supresión del** tecleo**.**

Tipo de la supresión del paso 4.Select del menú desplegable**.** (Regla o fuente o destino).

Paso 5. Haga Click en OK a completar.



Después de que el filtro del evento se agregue a esta regla, usted debe poder ver un icono del filtro con la cuenta dos al lado de la indicación de la regla, que muestra que hay dos filtros del evento habilitados para esta regla.

Paso 1.7. Estado dinámico de la configuración

Es una característica en donde podemos cambiar el estado de una regla si la condición especificada hace juego.

Suponga un escenario del ataque de fuerza bruta para quebrar la contraseña. Si una firma detecta la tentativa del fall de la contraseña y la acción de la regla es generar un evento. El sistema guarda en la generación de la alerta para la tentativa del fall de la contraseña. Para esta situación, usted puede utilizar el **estado dinámico** donde una acción de los **eventos Generate** se puede cambiar **para caer y para generar los eventos** para bloquear el ataque de fuerza bruta.

Navegue a la opción de las **reglas** en el panel navegacional y la página de la Administración de la regla aparece. Seleccione la regla para la cual usted quiere habilitar el estado dinámico y elegir el **estado dinámico de las** opciones **> Add un estado de la regla de la Tarifa-base.**

Para configurar el estado de la regla de la tarifa basada:

1. Seleccione las **reglas** para las cuales usted quiere configurar el umbral del evento.

2. Haga clic el **estado dinámico**.
3. Haga clic el **estado de la regla de la tarifa basada del agregar**.
4. Seleccione cómo usted quiere seguir el estado de la regla de la **pista por el** cuadro del descenso. (**Regla o fuente o destino**).
5. Ingrese la **red**. Usted puede especificar una sola dirección IP, el bloqueo de dirección, la variable, o una lista separada - de la coma que se comprenda de cualquier combinación de éstos.
6. Ingrese la **cuenta de los** eventos y el grupo fecha/hora en los segundos.
7. Seleccione el **nuevo estado,** usted quieren definir para la regla.
8. Ingrese el **descanso** después de lo cual se invierte el estado de la regla.
9. Haga Click en OK a completar.

Paso 2. Configure la directiva de la Análisis de red (SIESTA) y a los conjuntos variables (opcionales)

Configure la directiva de la Análisis de red

La directiva de acceso a la red también se conoce como preprocesadores. El preprocesador hace el nuevo ensamble del paquete y normaliza el tráfico. Ayuda a identificar las anomalías de la capa de red y del protocolo de capa de transporte en la identificación de las opciones inadecuadas de la encabezado.

La SIESTA hace el defragmentation de los datagramas IP, proporciona la inspección con estado TCP y el nuevo ensamble de la secuencia y las sumas de comprobación el validar. El preprocesador normaliza el tráfico, valida y verifica el estándar del protocolo.

Cada preprocesador tiene sus los propio GID número. Representa qué preprocesador ha sido accionado por el paquete.

Para configurar la directiva de la Análisis de red, navegue a la **configuración > a la configuración ASA FirePOWER > a las directivas > a la directiva del control de acceso > avanzó > Análisis de red y directiva de la intrusión**

La directiva del análisis de red predeterminada es Seguridad y la Conectividad equilibradas que es política recomendada óptima. Hay otras tres más directivas proporcionadas sistema de la SIESTA que se pueden seleccionar de la lista desplegable.

Lista selecta de la **directiva de la Análisis de red de la** opción para crear la directiva de encargo de la SIESTA.

Conjuntos variables de la configuración

Utilizan a los conjuntos variables en las reglas de la intrusión para identificar las direcciones de origen y de destino y los puertos. Las reglas son más eficaces cuando las variables reflejan su entorno de red más exactamente. La variable desempeña un papel importante en el ajuste del rendimiento.

Han configurado a los conjuntos variables ya con la opción predeterminada (/port de la red). Agregue a los nuevos conjuntos variables si usted quiere cambiar la configuración predeterminada.

Para configurar a los conjuntos variables, navegue a la **configuración > a la configuración ASA FirePOWER > a la Administración > al conjunto variable del objeto**. La opción selecta **agrega al conjunto variable** para agregar a los nuevos conjuntos variables. Ingrese el **nombre de los** conjuntos variables y especifique la **descripción.**

Si cualquier aplicación de encargo trabaja en un puerto específico después defina el número del puerto en el campo de número del puerto. Configure el parámetro de red.

$Home_NET especifican la red interna.

$External_NET especifican la red externa.

Paso 3: Configure el control de acceso para incluir a los conjuntos variables de la SIESTA de la directiva de la intrusión

Navegue a la **configuración > a la configuración ASA FirePOWER > a las directivas > a la directiva del control de acceso.** Usted necesita completar estos pasos:

1. Edite la regla de la política de acceso donde usted quiere asignar la directiva de la intrusión.
2. Elija la lengueta del **examen**.
3. Elija la **directiva de la intrusión del** menú desplegable y elija a los **conjuntos variables del** menú desplegable
4. Haga clic en Save (Guardar).

Puesto que una directiva de la intrusión se agrega a esta regla de la política de acceso. Usted puede ver el icono del blindaje en el color de oro que indica que la directiva de la intrusión está habilitada.

El almacén ASA FirePOWER del tecleo **cambia** para salvar los cambios.

Paso 4. Despliegue la directiva del control de acceso

Ahora, usted debe desplegar la directiva del control de acceso. Antes de que usted aplique la directiva, usted verá una directiva del control de acceso de la indicación anticuada en el dispositivo. Para desplegar los cambios al sensor:

1. El tecleo **despliega**.
2. El tecleo **despliega los cambios de FirePOWER**.
3. El tecleo **despliega** en la ventana emergente.

> **Note**: En la versión 5.4.x, aplicar la política de acceso al sensor, usted necesita hacer clic aplica los cambios ASA FirePOWER

> **Note**: Navegue a **monitorear > ASA FirePOWER que monitorea > estatus de la tarea.** Asegúrese de que la tarea deba completar para aplicar el cambio de configuración.

Paso 5. Eventos de la intrusión del monitor

Para ver los eventos de la intrusión generados por el módulo de FirePOWER, navegue a

monitorear > ASA FirePOWER que monitorea > Eventing en tiempo real.

Verificación

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

Troubleshooting

Paso 1. Asegúrese de que el estado de la regla de las reglas esté configurado apropiadamente.

Paso 2. Asegúrese de que la directiva correcta IPS se haya incluido en las reglas de acceso.

Paso 3. Asegúrese de que los conjuntos de las variables estén configurados correctamente. Si no configuran a los conjuntos variables correctamente entonces las firmas no harán juego el tráfico.

Paso 4. Asegúrese de que la implementación de política del control de acceso complete con éxito.

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

Información Relacionada

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