Opciones para reducir las intrusiones del falso positivo

Contenido

Introducción

Un sistema de prevención de intrusiones puede generar las alertas excesivas en cierta regla del Snort. Las alertas podían ser positivo o falso positivo verdadero. Si usted está recibiendo muchas alertas del falso positivo, hay varias opciones disponibles para que usted las reduzca. Este artículo proporciona un resumen de las ventajas y desventajas de cada opción.

Opciones para reducir las alertas del falso positivo

> **Note**: Estas opciones no son generalmente la mejor opción, ellas pueden ser la única solución bajo circunstancias específicas.

1. Señale al Soporte técnico de Cisco

Si usted encuentra una regla del Snort que accione las alertas en el tráfico benigno, señálelo por favor al Soporte técnico de Cisco. Una vez que está señalado, un ingeniero de asistencia técnica al cliente extiende el problema al equipo de investigación de la vulnerabilidad (VRT). VRT investiga las mejoras posibles a la regla. Las reglas mejoradas están típicamente disponibles para el reportero tan pronto como estén disponibles, y también se agregan a la actualización oficial siguiente de la regla.

2. Confíe en o permita la regla

La mejor opción para permitir que el tráfico de confianza pase a través de un dispositivo de Sourcefire sin el examen está habilitando la **confianza** o **permita la** acción sin una directiva asociada de la intrusión. Para configurar una confianza o permitir la regla, navegue a las **directivas > a la regla del control de acceso > Add**.

Note: Trafique la confianza que corresponde con o permita las reglas que no se configuran para hacer juego a los usuarios, las aplicaciones, o los URL tendrán efecto mínimo en el rendimiento general de un dispositivo de Sourcefire porque tales reglas se pueden procesar en el hardware de FirePOWER.

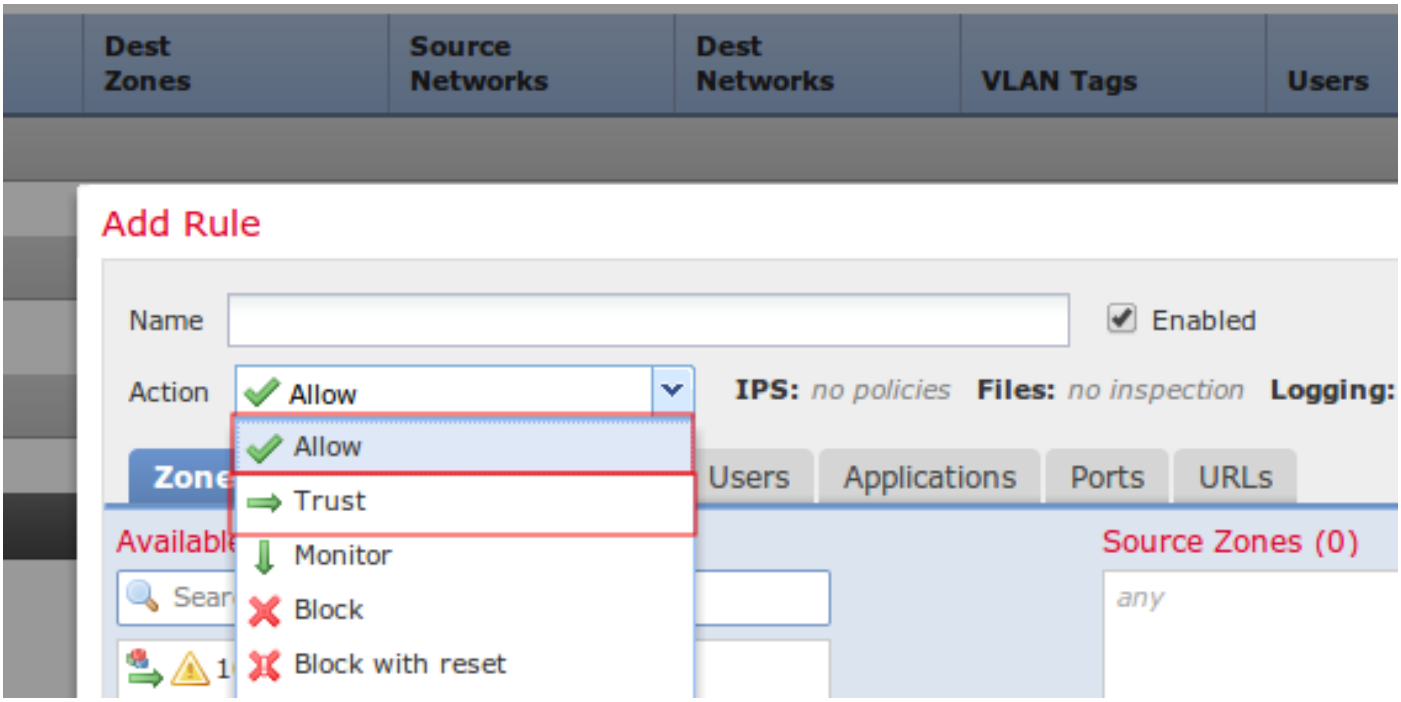

Figura: Configuración de una regla de la confianza

3. Reglas innecesarias de la neutralización

Usted puede inhabilitar las reglas del Snort que apuntan las viejas y parcheadas vulnerabilidades. Mejora el funcionamiento y reduce los falsos positivos. Usando FireSIGHT las recomendaciones pueden ayudar con esta tarea. Además, las reglas que generan con frecuencia las alertas de la prioridad baja o las alertas que no son procesables pueden ser buenos candidatos al retiro de una directiva de la intrusión.

4. Umbral

Usted puede utilizar el **umbral** para reducir el número de eventos de la intrusión. Esto es una buena opción a configurar cuando se espera que una regla accione regularmente un número limitado de eventos en el tráfico normal, pero podría ser una indicación de un problema si más que algunos paquetes hacen juego la regla. Usted puede utilizar esta opción para reducir el número de eventos accionados por las reglas ruidosas.

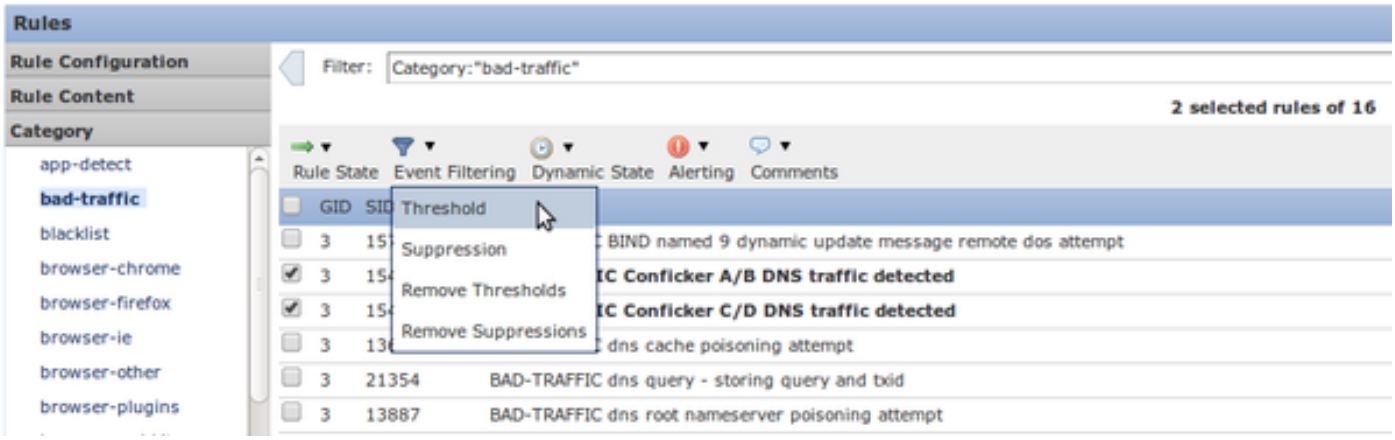

Figura: Configuración del umbral

5. Supresión

Usted puede utilizar la **supresión** para eliminar totalmente la notificación de los eventos. Es similar configurado a la opción del **umbral**.

> **Caution**: La supresión puede llevar los problemas de rendimiento, porque mientras que no se genera ningunos eventos, el Snort todavía tiene que procesar el tráfico.

> **Note**: La supresión no previene las reglas del descenso del tráfico de caída, así que el tráfico puede ser caído silenciosamente cuando hace juego con la regla del descenso.

6. Reglas del trayecto rápido

Similar para confiar en y permitir las reglas de una directiva del control de acceso, las reglas del trayecto rápido pueden también el examen de puentes. El Soporte técnico de Cisco no recomienda el usar de las reglas del trayecto rápido porque se configuran en la ventana **avanzada de la** página del **dispositivo** y puede generalmente ser pasado por alto fácilmente mientras que las reglas del control de acceso son casi siempre suficientes.

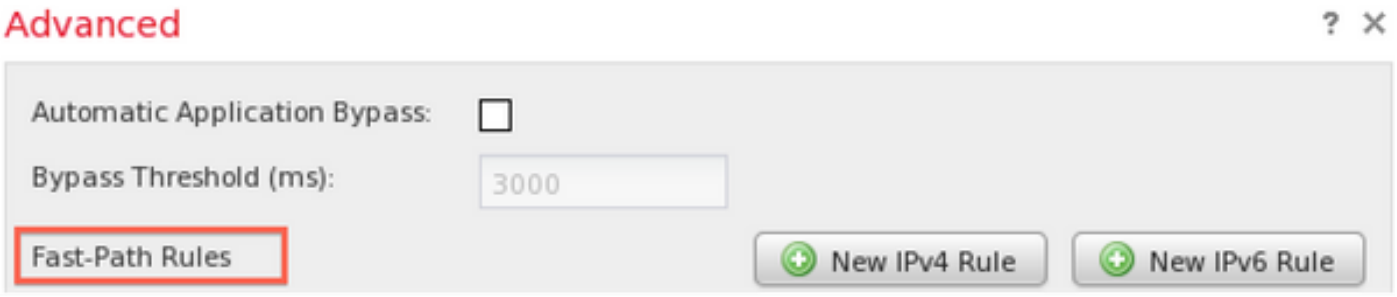

Figura: El trayecto rápido gobierna la opción en la ventana avanzada.

La única ventaja a usar las reglas del trayecto rápido es que pueden manejar un mayor volumen de tráfico máximo. Las reglas del trayecto rápido procesan el tráfico en el nivel del hardware (conocido como NMSB) y pueden dirigir teóricamente hasta el 200 Gbps del tráfico. En cambio, las reglas con la **confianza** y **permiten las** acciones se promueven al motor del flujo de red (NFE) y pueden manejar un máximo del 40 Gbps del tráfico.

Note: Las reglas del trayecto rápido están solamente disponibles en los dispositivos de las 8000 Series y el 3D9900.

7. Pase las reglas

Para prevenir una regla específica de accionar en el tráfico de cierto host (mientras que el otro tráfico de ese host necesita ser examinado), utilice una regla del Snort del tipo del *paso*. De hecho, ésta es la única forma de lograrla. Mientras que las reglas del paso son eficaces, pueden ser muy difíciles de mantener porque las reglas del paso se escriben manualmente. Además, si las reglas originales de reglas del paso son modificadas por una actualización de la regla, todas las reglas relacionadas del paso necesitan ser puestas al día manualmente. Si no pueden llegar a ser ineficaces.

8. Variable SNORT_BPF

La variable de `Snort_BPF` en una directiva de la intrusión permite a cierto tráfico para desviar el examen. Mientras que esta variable era una de las primeras opciones en las versiones del software heredado, el Soporte técnico de Cisco recomienda utilizar una regla de la directiva del control de acceso para desviar el examen, porque es más granular, más visible, y mucho más fácil configurar.