Configuración de la Función Ignorar Lista de Flow Collector's

Contenido

Introducción

Este documento describe cómo configurar su colector de flujo SNA para rechazar el flujo de red entrante de un exportador determinado mediante Ignorar lista.

Antecedentes

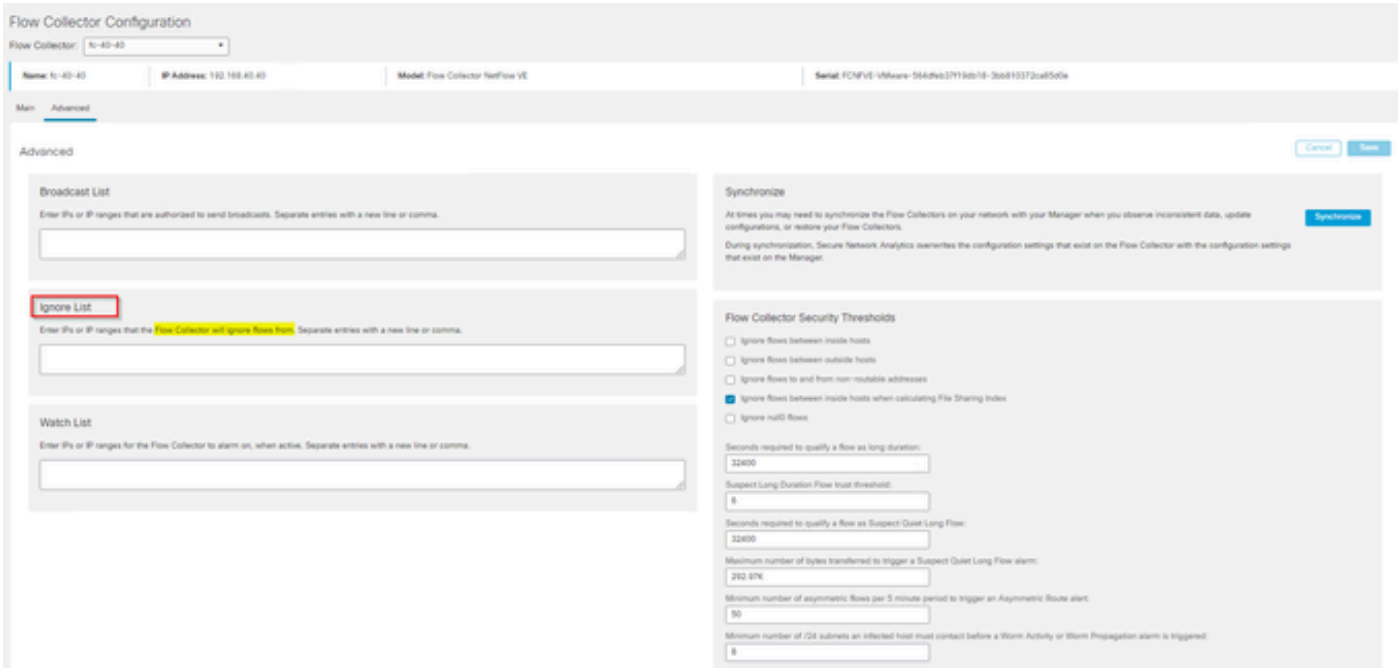
A menudo, se plantea la pregunta: "¿Hay alguna manera de decirle a mi colector de flujo SNA que rechace el flujo neto entrante de un exportador en particular?"

La respuesta es sí, esto se hace mediante el uso de los colectores de flujo "Ignorar lista" característica.

Configurar

La función ignorar lista es específica del colector de flujo. En una versión posterior de SNA 7.x, esta función está disponible dentro de la página de configuración del colector de flujo en la interfaz de usuario web de SNA Manager.

Utilice esta página para especificar un número ilimitado de hosts o subredes para los que elFlow Collector ignorará completamente el tráfico. Si el Flow Collector ve cualquier tráfico atribuible a estas direcciones IP, excluye ese tráfico de cualquier gráfico o tabla. Asegúrese de que puede confiar en todo el tráfico que viaja hacia o desde los hosts que se ignorarán.Secure Network Analytics no analiza este tráfico ni ninguno que se falsifique para incluir cualquiera de estos hosts. Si se lanza un ataque en su red que involucre a uno de estos hosts/subredes, el Flow Collector no puede informarlo.



Preguntas más Frecuentes

¿Cuál es el efecto de ignorar la lista en los cálculos de flujos por segundo (FPS) para Smart Licensing?

Respuesta: Agregar direcciones o rangos de IP de host a la lista de ignorados evita de manera efectiva que cualquiera de estos flujos cuente contra la velocidad de FPS calculada enviada hasta el SMC y utilizada para los informes de Smart License. Los flujos YA NO se muestran/cuentan en el gráfico de tendencias de flujo que se muestra en el tablero de mandos de SMC.

¿Cómo se utiliza la función de omitir lista al procesar el flujo de NVM cuando el cliente está en modo de túnel dividido?

Un cliente podría configurar AnyConnect para que nos envíe tráfico dentro y fuera de la red (también conocido como túnel dividido). El tráfico fuera de la red utiliza la dirección IP local del terminal que probablemente contenga IP superpuestas. SNA no admite IP superpuestas, tPor lo tanto, se ha sugerido que se utilice la función Ignorar lista para evitar el problema del túnel dividido, preservando así la ventaja de los flujos basados en NVM para las detecciones.

En este caso práctico, configuramos la "lista de ignorados" para evitar que los flujos de NVM fuera de la red provengan de la caché de flujo → flow_stats, Flow Search, eventos de seguridad personalizados

1. Agregue la dirección IP y la máscara de red (p. ej., agregue 192.168.1.0/24, 127.0.0.1/24) a la lista Ignorar
2. Verifique que nvm_flows aún se rellenan con los flujos NVM
3. Verifique que flow_stats no tenga los flujos NVM si src o dst IP está en la Lista de Ignorar

¿Puedo usar una lista de ignorados para ignorar los flujos de un exportador completo? No, dado que la lista de omisión se basa en datos de flujo y no en datos del exportador, la adición de una

dirección IP del exportador a la lista de omisión ignoraría de forma efectiva los datos de flujo en los que la IP del exportador figuraba como origen o destino del flujo, en lugar de ignorar todos los registros de flujo de ese exportador concreto

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).