Configurar o recurso Ignorar lista do coletor de fluxos

Contents

Introdução

Este documento descreve como configurar seu coletor de fluxo SNA para rejeitar o fluxo de rede de entrada de um exportador específico usando Ignorar lista.

Informações de Apoio

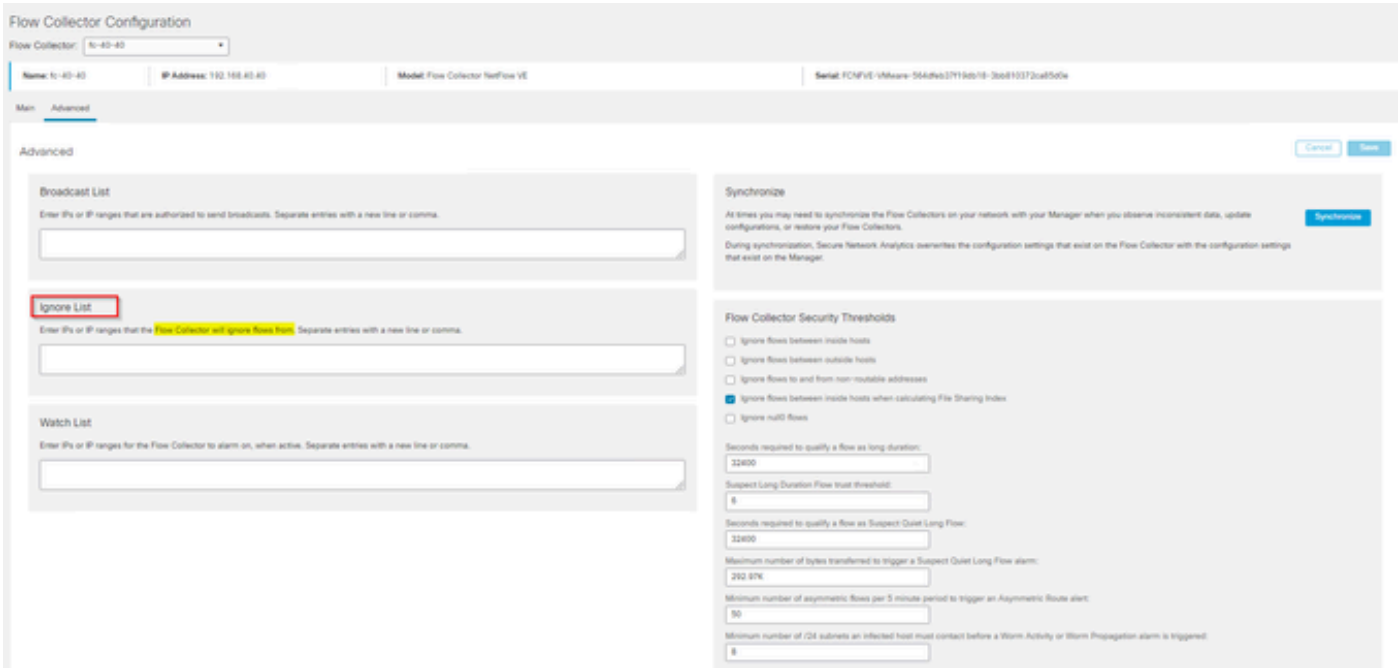
Muitas vezes, é feita a pergunta: "Há alguma maneira de dizer ao meu coletor de fluxo SNA para rejeitar o fluxo de rede de entrada de um exportador em particular?"

A resposta é sim, isso é feito com o uso do recurso "Ignorar lista" dos coletores de fluxo.

Configurar

O recurso ignorar lista é específico do coletor de fluxo. Na versão mais recente do SNA 7.x, esse recurso está disponível dentro da página de configuração do coletor de fluxo na interface de usuário da Web do SNA Manager.

Use esta página para especificar um número ilimitado de hosts ou sub-redes para os quais o coletor de fluxo ignora completamente o tráfego. Se o coletor de fluxo visualizar qualquer tráfego atribuível a esses endereços IP, ele excluirá esse tráfego de qualquer gráfico ou tabela. Certifique-se de que você pode confiar em todo o tráfego que viaja de ou para os hosts para ser ignorado.Secure Network Analytics não analisa esse tráfego nem qualquer tráfego que seja falsificado para incluir qualquer um desses hosts. Se um ataque for iniciado em sua rede envolvendo um desses hosts/sub-redes, oFlow Collector não poderá relatá-lo.



Perguntas freqüentes

Qual é o efeito dos cálculos de Ignore List on Flows Per Second (FPS) (Ignorar lista em fluxos por segundo) do Smart Licensing?

Resposta: Adicionar endereços IP de host ou intervalos à lista de ignorados impede efetivamente que qualquer um desses fluxos seja contado em relação à taxa de FPS calculada enviada para o SMC e usada para relatórios de Licença inteligente. Os fluxos NÃO são mais exibidos/contados no gráfico de tendência de fluxo exibido no painel SMC.

Como o recurso ignorar lista é usado ao processar o fluxo NVM quando o cliente está no modo de túnel dividido?

Um cliente pode configurar o AnyConnect para nos enviar tráfego dentro e fora da rede (ou seja, túnel dividido). O tráfego fora da rede usa o endereço IP local do ponto final que provavelmente contém IPs sobrepostos. SNA não suporta IPs sobrepostos, tAssim, foi sugerido o uso do recurso Ignorar lista para contornar o problema de divisão de túnel, preservando assim o benefício dos fluxos baseados em NVM para detecções.

Neste caso de uso, configuramos "Ignorar lista" para impedir que os fluxos NVM fora da rede fluam do cache → flow_stats, Pesquisa de fluxo, Eventos de segurança personalizados

1. Adicione o endereço IP e a máscara de rede (por exemplo, add 192.168.1.0/24, 127.0.0.1/24) na lista Ignorar
2. Verifique se nvm_flows ainda estão preenchidos com os fluxos NVM
3. Verifique se flow_stats não tem os fluxos de NVM se src ou dst IP estiver na lista Ignorar

Posso usar uma lista para ignorar fluxos de um exportador inteiro? Não, como a lista ignorar é baseada em dados de fluxo e não em dados do exportador, adicionar um endereço IP do exportador à lista ignorar efetivamente ignoraria os dados de fluxo em que o IP do exportador

estava listado como origem ou destino do fluxo, em vez de ignorar todos os registros de fluxo desse exportador específico

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.