De functie Lijst negeren van Flow Collector configureren

Inhoud

Inleiding

Dit document beschrijft hoe u uw SNA-stroomverzamelaar moet configureren om inkomende netwerkstroom van een bepaalde exporteur te weigeren door gebruik te maken van Lijst negeren.

Achtergrondinformatie

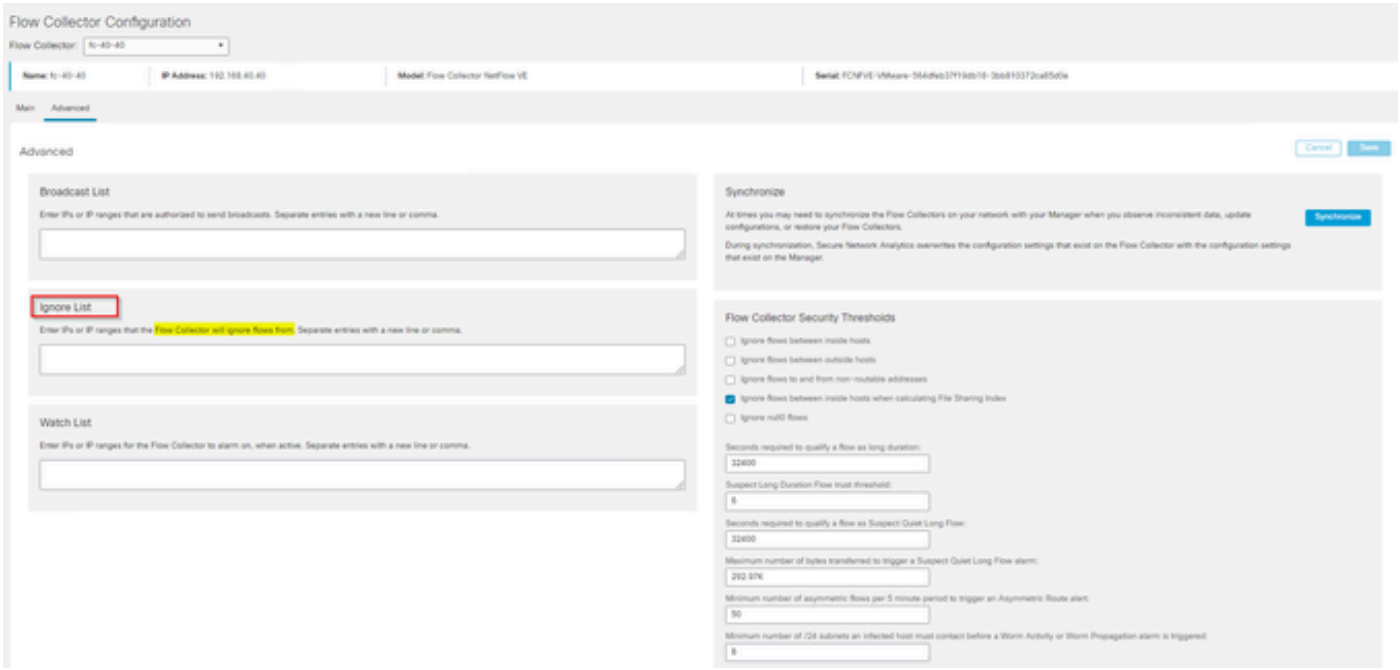
Vaak wordt de vraag gesteld, "Is er een manier om mijn SNA stroomverzamelaar te vertellen om inkomende netflow van een bepaalde exporteur af te wijzen?"

Het antwoord is ja, dit wordt gedaan door het gebruik van de Flow Collectors "Ignore List" functie.

Configureren

De negeer lijsteigenschap is specifieke stroomverzamelaar. In latere versie van SNA 7.x, is deze functie beschikbaar binnen de configuratiepagina van de stroomverzamelaar op de SNA Manager Web UI.

Gebruik deze pagina om een onbeperkt aantal hosts of subnetten op te geven waarvoor het Flow Collectorvolledig neutraal verkeer is. Als de Flow Collectors verkeer ziet dat kan worden toegeschreven aan deze IP-adressen, sluit het dat verkeer uit van elke grafiek of tabel. Zeker ben dat u op al verkeer kunt vertrouwen dat naar of van de hosts reist om te worden genegeerd.Secure Network Analytics analyseert dit verkeer noch op enige die wordt gespoofd om een van deze hosts te omvatten. Als een aanval wordt gelanceerd op uw netwerk met een van deze hosts/subnetten, kan de Flow Collector deze niet rapporteren.



Veelgestelde vragen

Wat is het effect van het negeren van de lijst op stromen per seconde (FPS) berekeningen voor slimme licenties?

Antwoord: Het toevoegen van host IP-adressen of -bereiken aan de negeerlijst voorkomt effectief dat een van deze stromen kan worden afgerekend tegen het berekende FPS-tarief dat naar de SCM wordt gestuurd en wordt gebruikt voor Smart License rapportage. De stromen worden NIET meer weergegeven/geteld in de stroomtrendgrafiek op het SMC-dashboard.

Hoe wordt de functie Lijst negeren gebruikt bij het verwerken van NVM-stroom als client in gesplitste tunnelmodus staat?

Een klant kan AnyConnect configureren om ons on-netwerk- en off-network verkeer te sturen (ook wel gesplitste tunnel genoemd). Het verkeer buiten het netwerk gebruikt het lokale IP-adres van het eindpunt dat waarschijnlijk overlappende IP's bevat. SNA ondersteunt geen overlappende IP's, tEr is dan ook gesuggereerd om de functie Lijst negeren te gebruiken om de gesplitste tunnelkwestie te omzeilen, waardoor het voordeel van de op NVM gebaseerde stromen voor detecties behouden blijft.

In dit gebruiksgeval, configureren we de "Ignore List" om te voorkomen dat de NVM-stromen buiten het netwerk stromen uit flow cache → flow_stats, Flow Search, Custom Security Events

1. Voeg het IP-adres en het netwerkmasker (bijvoorbeeld 192.168.1.0/24, 127.0.0.1/24) toe aan de lijst met negeren
2. Controleer of de nvm_flows nog steeds gevuld zijn met de NVM-stromen
3. Controleer of de flow_stats niet de NVM-stromen heeft als src of dst IP in de lijst Negeren staat

Kan ik een negelijst gebruiken om stromen van een hele exporteur te negeren? Neen, omdat de

negerlijst is gebaseerd op stroomgegevens en niet op uitvoergegevens, zou het toevoegen van een IP-adres van de exporteur aan de negerlijst in feite stromingsgegevens negeren wanneer het IP van de exporteur als bron of als bestemming van de stroom werd vermeld, in plaats van alle stroomgegevens van die specifieke exporteur te negeren

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.