Konfigurieren der Ignorierlistenfunktion von FlowCollector

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den SNA Flow Collector so konfigurieren, dass eingehender NetFlow von einem bestimmten Exporteur mithilfe der Ignore List abgelehnt wird.

Hintergrundinformationen

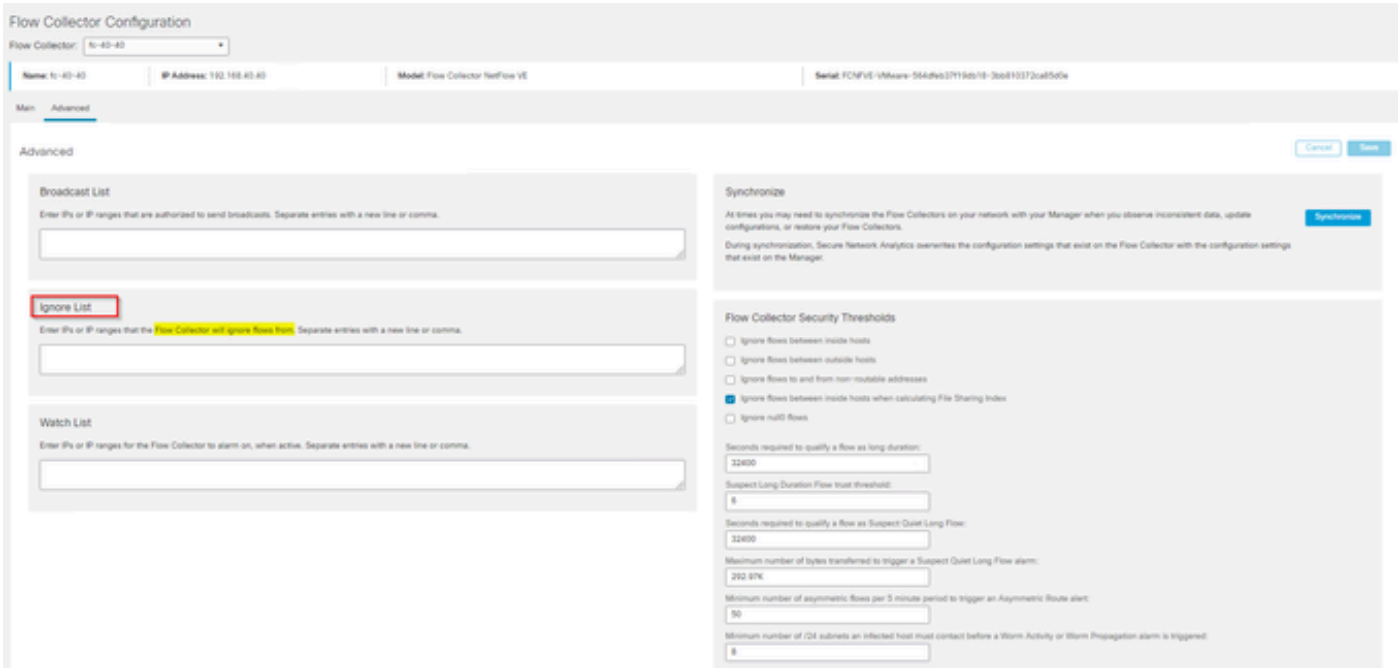
Oft stellt sich die Frage: "Gibt es eine Möglichkeit, meinem SNA Flow Collector mitzuteilen, dass er eingehenden NetFlow von einem bestimmten Exporteur ablehnt?"

Die Antwort ist ja, dies geschieht durch die Verwendung der Flow Collectors "Ignore List" Funktion.

Konfigurieren

Die Ignorierlisten-Funktion ist Flow Collector-spezifisch. In einer neueren Version von SNA 7.x ist diese Funktion auf der Flow Collector-Konfigurationsseite der SNA Manager-Webbenutzeroberfläche verfügbar.

Verwenden Sie diese Seite, um eine unbegrenzte Anzahl von Hosts oder Subnetzen anzugeben, für die der FlowCollectorDatenverkehr völlig ignoriert. Wenn der FlowCollector Datenverkehr erkennt, der auf diese IP-Adressen zurückgeführt werden kann, wird dieser Datenverkehr aus einem Diagramm oder einer Tabelle ausgeschlossen. Vergewissern Sie sich, dass der gesamte Datenverkehr, der zu oder von den Hosts läuft, ignoriert werden kann.Secure Network Analytics analysiert weder diesen Datenverkehr noch den Datenverkehr, der gefälscht wird, um einen dieser Hosts einzuschließen. Wenn ein Angriff auf Ihr Netzwerk gestartet wird, der einen dieser Hosts/Subnetze betrifft, kann der FlowCollector ihn nicht melden.



Häufig gestellte Fragen

Wie wirkt sich die Ignore List-Funktion auf FPS-Berechnungen (Flows Per Second) für Smart Licensing aus?

Die Antwort: Das Hinzufügen von Host-IP-Adressen oder -Bereichen zur Ignorierliste verhindert effektiv, dass diese Flows bei der Berechnung der FPS-Rate berücksichtigt werden, die an den SMC gesendet und für Smart License-Berichte verwendet wird. Die Datenflüsse werden NICHT mehr in dem im SMC-Dashboard angezeigten Diagramm für den Datenfluss angezeigt/gezählt.

Wie wird die Ignore-Listenfunktion verwendet, wenn der NVM-Fluss verarbeitet wird, wenn sich der Client im Split-Tunnel-Modus befindet?

Ein Kunde könnte AnyConnect so konfigurieren, dass uns netzwerkinterner und netzwerkexterner Datenverkehr (auch Split-Tunnel genannt) gesendet wird. Für den Verkehr außerhalb des Netzwerks wird die lokale IP-Adresse des Endpunkts verwendet, die höchstwahrscheinlich sich überschneidende IPs enthält. SNA unterstützt keine sich überschneidenden IPs. tDaher wird empfohlen, die Funktion "Ignore list" (Liste ignorieren) zu verwenden, um das Split-Tunnel-Problem zu umgehen. Auf diese Weise bleiben die Vorteile der NVM-basierten Flows für die Erkennung erhalten.

In diesem Anwendungsfall konfigurieren wir die "Ignore List" (Ignorierliste), um zu verhindern, dass die netzwerkexternen NVM-Flows aus dem Flow-Cache stammen → flow_stats, Flow Search, Custom Security Events

1. Fügen Sie die IP-Adresse und die Netzwerkmaske (z. B. 192.168.1.0/24, 127.0.0.1/24) zur Ignorierliste hinzu.
2. Vergewissern Sie sich, dass die NVM-Flows weiterhin in "nvm_flows" enthalten sind.
3. Vergewissern Sie sich, dass flow_stats nicht über die NVM-Flows verfügt, wenn sich src oder dst IP in der Ignore-Liste befindet.

Kann ich eine Ignorierliste verwenden, um Flüsse eines gesamten Exporteurs zu ignorieren? Nein, da die Ignorierliste auf Flow-Daten basiert und nicht auf Exporterdaten, würde das Hinzufügen einer Exporter-IP-Adresse zur Ignorierliste Flow-Daten ignorieren, bei denen die Exporter-IP entweder als Quelle oder als Ziel des Flow aufgeführt war, anstatt alle Flow-Datensätze dieses bestimmten Exporteurs zu ignorieren

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.