Secure Network Analytics Virtual Appliance Einschränkungen bei der Konfiguration der Netzwerkschnittstelle

Inhalt

Problem

Für Secure Network Analytics (SNA) mit Non Data Store wurde ein Bereitstellungsszenario ausgewertet, bei dem Flow Collector über eine Virtualisierungsplattform mehrere Netzwerkschnittstellen zugewiesen haben.

Es stellten sich folgende Fragen:

- Legt fest, ob der virtuelle Flow Collector mit zwei NICs betrieben werden kann - eine für die interne SNA-Kommunikation und eine andere für den NetFlow-Empfang.
- Legt fest, ob die virtuelle Manager-Appliance mit mehreren NICs konfiguriert werden kann, um Bedrohungs-Feeds abzurufen, wenn das interne Kommunikationssegment nicht auf das Internet zugreifen kann.

Umwelt

- Secure Network Analytics (StealthWatch) Version bis 7.6.0
- Versionen aller SNA-Komponenten für virtuelle Appliances (Manager, FlowCollector)
- Netzwerkarchitektur mit separater interner Kommunikation und NetFlow-Empfangssegmenten

Auflösung

FlowCollector von Cisco Secure Network Analytics (SNA) kann mit zwei NIC-Schnittstellen bereitgestellt werden. Dieses Verhalten wurde in einer Laborumgebung validiert:

1. Zwei Schnittstellen - Verwaltungszugriff und NetFlow-Empfang

- FlowCollector kann mit einer Schnittstelle für den Managementzugriff und einer zweiten Schnittstelle für den Empfang von NetFlow konfiguriert werden.
- Der Managementzugriff bleibt jedoch über beide Schnittstellen (Management oder NetFlow) erreichbar. Es gibt derzeit keine Möglichkeit, eine Schnittstelle strikt auf ihren beabsichtigten Zweck zu beschränken.

2. Zwei Schnittstellen - NetFlow-Empfang und Threat-Feed-Empfang

- Aktualisierungen von Bedrohungs-Feeds werden über den Internetzugriff von FlowCollector abgerufen.
- Wenn die IP-Adresse der Verwaltungsschnittstelle keinen direkten Internetzugriff hat, kann die auf Flow Collector verfügbare Proxyoption konfiguriert werden, um diese Anforderung zu erfüllen, während die zweite Schnittstelle weiterhin NetFlow empfängt.

Wichtiger Hinweis zum Geltungsbereich
Beide Szenarien wurden in einer Laborumgebung verifiziert und sind im SNA Designleitfaden nicht dokumentiert. Sie sind daher als beobachtetes Verhalten zu behandeln und nicht als offiziell veröffentlichte Entwurfsempfehlung. Kunden, die eine solche Bereitstellung planen, sollten diese zunächst in ihrer eigenen Testumgebung validieren.

Ursache

Dieses Verhalten ist in der Architektur der Secure Network Analytics Flow Collector Appliance festgelegt. Die Appliance unterstützt die Zuweisung einer zusätzlichen Netzwerkkarte. An dieser sekundären Schnittstelle kann Telemetrie (NetFlow) empfangen werden, während die primäre Schnittstelle für das Management verwendet wird. Die Appliance-Software führt jedoch ihre Management-Services (Appliance-Admin-UI, SSH und SNA-Kommunikation zwischen den Appliances) an alle konfigurierten und adressierten Schnittstellen gebunden aus und macht keine schnittstellenspezifische Dienstbindung oder Zugriffssteuerungsoption verfügbar. Der Managementzugriff bleibt daher von beiden NICs aus erreichbar und kann nicht auf die für diesen Zweck festgelegte Schnittstelle beschränkt werden.

Ebenso ist der Abruf von Bedrohungs-Feeds nicht an eine bestimmte Netzwerkkarte gebunden.

Der Aktualisierungsprozess initiiert lediglich eine ausgehende Verbindung auf Basis der Routing-Tabelle der Appliance, sodass jede Schnittstelle mit einem gültigen Pfad zu den Internetdiensten die Anforderung sendet. Wenn die Verwaltungsschnittstelle nicht direkt über das Internet erreichbar ist, leitet die Proxy-Konfigurationsoption in Appliance Admin die ausgehende Anforderung über einen genehmigten Proxy-Server weiter, sodass der Threat-Feed erfolgreich aktualisiert werden kann, ohne die Schnittstellenrollen zu ändern.

Da Bereitstellungen mit FlowCollector für mehrere NICs und die Trennung von Schnittstellen-Rollen nicht im Secure Network Analytics-Designleitfaden behandelt werden, ist dieses Verhalten nicht dokumentiert, sondern wird nicht unterstützt, und die Ergebnisse basieren ausschließlich auf Labortests.

Verwandte Inhalte

- Secure Network Analytics Virtual Edition Appliance - Installationshandbuch

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.