Beperkingen voor de configuratie van de Secure Network Analytics Virtual Appliance Network Interface

Inhoud

uitgifte

Er werd een implementatiescenario geëvalueerd voor Secure Network Analytics (SNA) met Non Data Store waarbij de Flow Collector meerdere netwerkinterfaces toegewezen heeft gekregen via een virtualisatieplatform.

De specifieke vragen die naar voren kwamen waren:

- Of de virtuele Flow Collector met twee NIC's kan werken - een voor interne communicatie van SNA en een andere voor NetFlow-ontvangst
- Of het virtuele beheertoestel kan worden geconfigureerd met meerdere NIC's om bedreigingsfeeds te verkrijgen wanneer het interne communicatiesegment geen toegang heeft tot internet

milieu

- Secure Network Analytics (Stealthwatch) versie tot 7.6.0
- Virtuele toestelversies van alle SNA-componenten (Manager, Flow Collector)
- Netwerkarchitectuur met gescheiden interne communicatie en NetFlow-ontvangstsegmenten

resolutie

Cisco Secure Network Analytics (SNA) Flow Collector kan worden geïmplementeerd met twee NIC-interfaces en dit gedrag is gevalideerd in een laboratoriumomgeving:

1. Twee interfaces — beheerstoegang en NetFlow-ontvangst

- De Flow Collector kan worden geconfigureerd met één interface voor beheertoegang en een tweede interface voor het ontvangen van NetFlow.
- De beheertoegang blijft echter bereikbaar via ofwel interfacebeheer (ofwel NetFlow). Er is momenteel geen optie om een interface te beperken tot het beoogde doel.

2. Twee interfaces — NetFlow-ontvangst en ontvangst van dreigingsfeed

- Updates van de bedreigingsfeed worden opgehaald met behulp van internettoegang van de Flow Collector.
- Als de IP-beheerinterface geen directe internettoegang heeft, kan de proxyoptie die beschikbaar is op de stroomcollector worden geconfigureerd om aan deze vereiste te voldoen, terwijl de tweede interface NetFlow blijft ontvangen.

Belangrijke opmerking over de reikwijdte
Beide scenario's werden uitsluitend in een laboratoriumopstelling geverifieerd en zijn niet gedocumenteerd in de SNA Design Guide. Ze moeten daarom worden behandeld als waargenomen gedrag in plaats van als een officieel gepubliceerde ontwerpaanbeveling. Klanten die een dergelijke implementatie plannen, worden aangemoedigd om deze eerst in hun eigen testomgeving te valideren.

Oorzaak

Dit gedrag wordt door ontwerp beschreven in de architectuur van het Secure Network Analytics Flow Collector-apparaat. Het toestel ondersteunt de toewijzing van een extra NIC, en telemetrie (NetFlow) kan worden ontvangen op die secundaire interface terwijl de primaire interface wordt gebruikt voor het beheer. De toestelsoftware voert echter zijn beheerservices uit — communicatie tussen toestelbeheerders (Appliance Admin UI, SSH en SNA) — die zijn gekoppeld aan alle geconfigureerde en geadresseerde interfaces, en biedt geen service-binding per interface of toegangsbeheeroptie. Als gevolg daarvan blijft de beheertoegang bereikbaar via een van beide NIC's en kan deze niet worden beperkt tot de interface die voor dat doel is aangewezen.

Op dezelfde manier is het ophalen van bedreigingsfeed niet gekoppeld aan een specifieke NIC. Het updateproces initieert eenvoudigweg een uitgaande verbinding op basis van de

toestelrouteringstabel, dus elke interface met een geldig pad naar de internetservices ondersteunt het verzoek. Wanneer de beheerinterface geen directe internetbereikbaarheid heeft, geeft de proxyconfiguratieoptie binnen Toestelbeheer het uitgaande verzoek door via een goedgekeurde proxyserver, zodat de bedreigingsfeed met succes kan worden bijgewerkt zonder de interfacerollen te wijzigen.

Omdat multi-NIC Flow Collector-implementaties en scheiding van interfacerollen niet worden behandeld in de Secure Network Analytics Design Guide, is dit gedrag niet gedocumenteerd in plaats van niet ondersteund en zijn de bevindingen uitsluitend gebaseerd op laboratoriumvalidatie.

Gerelateerde inhoud

- Installatiehandleiding voor Secure Network Analytics Virtual Edition-apparaten

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.