Secure Network Analytics Virtual Appliance Network Interface Configuration Limitations

Contents

Issue

A deployment scenario was being evaluated for Secure Network Analytics (SNA) with Non Data Store where the Flow Collector have multiple network interfaces assigned via virtualisation platform.

The specific questions that arose were:

- Whether the virtual Flow Collector can operate with two NICs - one for SNA internal communication and another for NetFlow reception
- Whether the virtual Manager appliance can be configured with multiple NICs to obtain threat feeds when the internal communication segment cannot access the internet

Environment

- Secure Network Analytics (Stealthwatch) version upto 7.6.0
- Virtual appliance versions of all SNA components (Manager, Flow Collector)
- Network architecture with separated internal communication and NetFlow receiving segments

Resolution

Cisco Secure Network Analytics (SNA) Flow Collector can be deployed with two NIC interfaces, and this behavior was validated in a lab environment:

1. Two interfaces — management access and NetFlow reception

- The Flow Collector can be configured with one interface for management access and a second

interface dedicated to receiving NetFlow.

- However, management access remains reachable through **either** interface (management or NetFlow). There is currently no option to restrict an interface strictly to its intended purpose.

2. Two interfaces — NetFlow reception and threat feed reception

- Threat feed updates are retrieved using internet access from the Flow Collector.
- If the management interface IP does not have direct internet access, the **proxy option** available on the Flow Collector can be configured to fulfil this requirement, while the second interface continues to receive NetFlow.

Important note on scope
Both scenarios were verified purely in a lab setup and are **not documented in the SNA Design Guide**. They must therefore be treated as observed behavior rather than an officially published design recommendation. Customers planning such a deployment are encouraged to validate it in their own test environment first.

Cause

This behavior is by design in the Secure Network Analytics Flow Collector appliance architecture. The appliance supports the assignment of an additional NIC, and telemetry (NetFlow) can be received on that secondary interface while the primary interface is used for management. However, the appliance software runs its management services — Appliance Admin UI, SSH, and SNA inter-appliance communication — bound to all configured and addressed interfaces, and it does not expose any per-interface service binding or access-control option. As a result, management access remains reachable from either NIC and cannot be restricted to the interface designated for that purpose.

Similarly, threat feed retrieval is not tied to a specific NIC. The update process simply initiates an outbound connection based on the appliance routing table, so any interface with a valid path to the internet services the request. Where the management interface has no direct internet reachability, the proxy configuration option within Appliance Admin relays the outbound request through an approved proxy server, allowing the threat feed to update successfully without altering the interface roles.

Because multi-NIC Flow Collector deployments and interface-role separation are not covered in the Secure Network Analytics Design Guide, this behavior is undocumented rather than unsupported, and the findings are based solely on lab validation.

Related Content

- Secure Network Analytics Virtual Edition Appliance Installation Guide