Limitaciones de Secure Network Analytics Virtual Appliance Network Interface Configuration

Contenido

Problema

Se estaba evaluando un escenario de implementación para Secure Network Analytics (SNA) con almacenamiento que no es de datos, donde el Flow Collector tiene varias interfaces de red asignadas a través de la plataforma de virtualización.

Las preguntas específicas que surgieron fueron:

- Si el Flow Collector virtual puede funcionar con dos NIC: una para la comunicación interna SNA y otra para la recepción de NetFlow
- Si el dispositivo de Virtual Manager se puede configurar con varias NIC para obtener fuentes de amenazas cuando el segmento de comunicación interna no puede acceder a Internet

Entorno

- Secure Network Analytics (StealthWatch) versión hasta 7.6.0
- Versiones de dispositivos virtuales de todos los componentes SNA (administrador, recopilador de flujos)
- Arquitectura de red con comunicación interna separada y segmentos receptores de NetFlow

Resolución

El Flow Collector de Cisco Secure Network Analytics (SNA) se puede implementar con dos

interfaces NIC y este comportamiento se validó en un entorno de laboratorio:

1. Dos interfaces: acceso a la gestión y recepción de NetFlow

- El Flow Collector se puede configurar con una interfaz para el acceso a la administración y una segunda interfaz dedicada a recibir NetFlow.
- Sin embargo, el acceso a la gestión sigue siendo accesible a través de cualquiera de las interfaces (gestión o NetFlow). Actualmente no existe la opción de restringir una interfaz estrictamente a su propósito previsto.

2. Dos interfaces: recepción de NetFlow y recepción de información sobre amenazas

- Las actualizaciones de la fuente de amenazas se recuperan mediante el acceso a Internet desde Flow Collector.
- Si la IP de la interfaz de administración no tiene acceso directo a Internet, la opción de proxy disponible en el Flow Collector se puede configurar para cumplir este requisito, mientras que la segunda interfaz continúa recibiendo NetFlow.

Nota importante sobre el alcance
Ambos escenarios se verificaron únicamente en una configuración de laboratorio y no se documentan en la Guía de diseño de SNA. Por consiguiente, deben tratarse como comportamiento observado y no como una recomendación de diseño publicada oficialmente. Se anima a los clientes que estén planificando una implementación de este tipo a validarla en primer lugar en su propio entorno de prueba.

Causa

Este comportamiento se define por diseño en la arquitectura del appliance Secure Network Analytics Flow Collector. El dispositivo admite la asignación de una NIC adicional y se puede recibir telemetría (NetFlow) en esa interfaz secundaria mientras se utiliza la interfaz principal para la gestión. Sin embargo, el software del dispositivo ejecuta sus servicios de gestión (interfaz de usuario de administración del dispositivo, SSH y comunicación entre dispositivos SNA) enlazados a todas las interfaces configuradas y dirigidas, y no expone ninguna opción de enlace de servicio o control de acceso por interfaz. Como resultado, el acceso a la administración sigue siendo accesible desde cualquier NIC y no puede restringirse a la interfaz designada para ese propósito.

Del mismo modo, la recuperación de fuentes de amenazas no está vinculada a una NIC específica. El proceso de actualización simplemente inicia una conexión saliente basada en la

tabla de ruteo de dispositivos, de modo que cualquier interfaz con una ruta válida a los servicios de Internet envía la solicitud. Cuando la interfaz de gestión no tiene acceso directo a Internet, la opción de configuración de proxy del administrador de dispositivos retransmite la solicitud saliente a través de un servidor proxy aprobado, lo que permite que la fuente de amenazas se actualice correctamente sin alterar los roles de la interfaz.

Debido a que las implementaciones de Flow Collector de NIC múltiples y la separación de funciones de interfaz no se tratan en la Guía de diseño de Secure Network Analytics, este comportamiento no está documentado en lugar de no ser compatible, y las conclusiones se basan únicamente en la validación de laboratorio.

Contenido relacionado

- Guía de instalación del dispositivo Secure Network Analytics Virtual Edition

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).