Limitazioni alla configurazione dell'interfaccia di rete dell'appliance virtuale Secure Network Analytics

Sommario

Problema

È in corso la valutazione di uno scenario di distribuzione per SNA (Secure Network Analytics) con archivio non di dati in cui il Flow Collector dispone di più interfacce di rete assegnate tramite la piattaforma di virtualizzazione.

Le domande specifiche che sono emerse sono le seguenti:

- Se il virtual Flow Collector può funzionare con due NIC - una per la comunicazione interna SNA e un'altra per la ricezione NetFlow
- Se è possibile configurare l'appliance Virtual Manager con più schede NIC per ottenere feed di minacce quando il segmento di comunicazione interno non è in grado di accedere a Internet

Ambiente

- Secure Network Analytics (Stealthwatch) versione fino a 7.6.0
- Versioni dell'appliance virtuale di tutti i componenti SNA (Manager, Flow Collector)
- Architettura di rete con comunicazioni interne separate e segmenti di ricezione NetFlow

Risoluzione

È possibile distribuire Cisco Secure Network Analytics (SNA) Flow Collector con due interfacce NIC e questo comportamento è stato convalidato in un ambiente lab:

1. Due interfacce: accesso alla gestione e ricezione NetFlow

- Flow Collector può essere configurato con un'interfaccia per l'accesso alla gestione e una seconda interfaccia dedicata alla ricezione di NetFlow.
- Tuttavia, l'accesso alla gestione rimane raggiungibile tramite entrambe le interfacce (gestione o NetFlow). Attualmente non vi è alcuna opzione per limitare un'interfaccia esclusivamente allo scopo per cui è stata progettata.

2. Due interfacce: ricezione NetFlow e ricezione di alimentazione di minaccia

- Gli aggiornamenti del feed delle minacce vengono recuperati tramite l'accesso a Internet da Flow Collector.
- Se l'IP dell'interfaccia di gestione non dispone di accesso diretto a Internet, l'opzione proxy disponibile sul Flow Collector può essere configurata in modo da soddisfare questo requisito, mentre la seconda interfaccia continua a ricevere NetFlow.

Nota importante sull'ambito
Entrambi gli scenari sono stati verificati esclusivamente in una configurazione di laboratorio e non sono documentati nella SNA Design Guide. Devono pertanto essere trattati come un comportamento osservato piuttosto che come una raccomandazione di progettazione pubblicata ufficialmente. I clienti che pianificano un'installazione di questo tipo sono invitati a convalidarla prima nel proprio ambiente di test.

Causa

Questo comportamento è previsto dall'architettura dell'appliance Secure Network Analytics Flow Collector. L'accessorio supporta l'assegnazione di una scheda NIC aggiuntiva e la telemetria (NetFlow) può essere ricevuta sull'interfaccia secondaria, mentre l'interfaccia principale viene utilizzata per la gestione. Tuttavia, il software dell'accessorio esegue i servizi di gestione (interfaccia utente di amministrazione dell'accessorio, SSH e comunicazione tra appliance SNA) associati a tutte le interfacce configurate e indirizzate e non espone alcuna opzione di associazione al servizio o di controllo dell'accesso per interfaccia. Di conseguenza, l'accesso alla gestione rimane raggiungibile da entrambe le schede NIC e non può essere limitato all'interfaccia designata a tale scopo.

Analogamente, il recupero del feed delle minacce non è legato a una scheda NIC specifica. Il processo di aggiornamento avvia semplicemente una connessione in uscita in base alla tabella di routing dell'accessorio, in modo che qualsiasi interfaccia con un percorso valido ai servizi Internet della richiesta. Se l'interfaccia di gestione non è raggiungibile direttamente da Internet, l'opzione di configurazione proxy in Appliance Admin inoltra la richiesta in uscita tramite un server proxy approvato, consentendo al feed delle minacce di eseguire l'aggiornamento senza modificare i ruoli dell'interfaccia.

Poiché le distribuzioni di Flow Collector multi-NIC e la separazione dei ruoli dell'interfaccia non sono trattate nella Guida alla progettazione di Secure Network Analytics, questo comportamento non è documentato anziché non supportato e i risultati sono basati esclusivamente sulla convalida in laboratorio.

Contenuto correlato

- Guida all'installazione dell'appliance Secure Network Analytics Virtual Edition

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).