قيود تكوين واجهة شبكة Secure Network Analytics Virtual Appliance

المحتويات

مسألة

كان يتم تقييم سيناريو نشر لتحليلات الشبكة الآمنة (SNA) باستخدام مخزن غير للبيانات حيث يحتوي مجمع التدفق على واجهات شبكة متعددة تم تعيينها عبر النظام الأساسي للمحاكاة الافتراضية.

والأسئلة المحددة التي أثيرت هي:

- (NIC) - ما إذا كان مجمع التدفق الظاهري يمكن أن يعمل باستخدام بطاقتي واجهة شبكة واحدة للاتصال الداخلي لـ SNA وأخرى لاستقبال NetFlow
- (NICs) ما إذا كان يمكن تكوين جهاز Virtual Manager باستخدام بطاقات واجهة شبكة متعددة للحصول على موجز ويب تهديدات عندما لا يتمكن مقطع الاتصال الداخلي من الوصول إلى الإنترنت

البيئة

- إصدار تحليلات الشبكة الآمنة (Stealthwatch) 7.6.0 يصل إلى
- إصدارات الجهاز الظاهري لجميع مكونات SNA (Manager، مجمع التدفق)
- بنية الشبكة مع قطع الاتصال الداخلي المنفصلة وقطاعات إستقبال NetFlow

قرار

يمكن نشر مجمع تدفق تحليلات الشبكة الآمنة (SNA) من Cisco باستخدام واجهتي بطاقة

واجهة الشبكة (NIC)، وتم التحقق من هذه السلوك في بيئة معملية:

1. واجهتان - الوصول إلى الإدارة واستقبال NetFlow

- يمكن تكوين مجمع التدفق باستخدام واجهة واحدة للوصول إلى الإدارة وواجهة ثانية مخصصة لتلقي NetFlow.
- وأ الإدارة) واجهة أي خالل من إليه الوصول إلى الإدارة قابل للوصول إلى الوصول يظل ،ذلك ومع .(NetFlow ال يوجد حاليا خيار لتقييد واجهة بشكل صارم للغرض المقصود منها.

2 - واجهتان - إستقبال NetFlow واستقبال التلقيمات بالتهديد

- يتم إسترداد تحديثات موجز ويب التهديد باستخدام الوصول إلى الإنترنت من مجمع التدفق.
- إذا لم يكن لواجهة الإدارة IP وصول مباشر إلى الإنترنت، يمكن تكوين خيار الوكيل للوصول إلى الإنترنت من خالل واجهة التدفق المتوفر على مجمع التدفق للوفاء بهذا المتطلب، بينما تستمر الواجهة الثانية في تلقي NetFlow.

ملاحظة هامة بشأن النطاق
تم التحقق من كل السيناريوهين في إعداد مختبر فقط ولم يتم توثيقهما في دليل تصميم SNA. ولذلك يجب أن تعامل على أنها سلوك الملاحظ بدل من أن تكون توصية تصميمية منشورة رسمية. ويتم تشجيع العمالء الذين يخططون لمثل هذا النشر على التحقق من صحته في بيئة االختبار الخاصة بهم أو.

السبب

هذا السلوك يتم من خالل التصميم في بنية جهاز مجمع تدفق تحليالت الشبكة المؤمنة. يدعم الجهاز تعيين بطاقة واجهة شبكة (NIC) إضافية، ويمكن تلقي القياس عن بعد (NetFlow) على تلك الواجهة الثانوية ألغراض إدارة. ومع ذلك، يتشغيل خدمات الإدارة الخاصة به - االتصال بين أجهزة Appliance Admin وقوم برنامج الجهاز بتعطيل أي عرض الو، طبر المرتبطة بجميع الواجهات التي تم تكوينها ومعالجتها - SNA و SSH و UI على مستوى نظام التشغيل. ونتيجة لذلك، يظل الوصول إلى الإدارة قابل للوصول من خالل أي واجهة لكن الوصول إلى الواجهة المحددة لهذا الغرض يمكن تقييده إلى الواجهة الوحيدة (NIC) بطاقة واجهة الشبكة المعينة. تقوم طبر التي يتم إسترداد موجز ويب التهديد بطاقة واجهة شبكة (NIC) المعينة. وبالمثل، إذن فإن عملية التحديث بسلطة بتهيئة اتصال صادر استنادا إلى جدول توجيه الجهاز، عن طريق واجهة مع مسار صالح لخدمات الإنترنت المطلوب. في الحاالت التي ال تتوفر فيها واجهة أي مزود خيار تكوين الوكيل داخل مسؤول الإدارة إمكانية الوصول المباشر إلى الإنترنت، يقوم

Appliance بإبلاغ الطلب الصادر من خلال خادم وكيل معتمد، مما يسمح بتحديث موجز ويب التهديد بنجاح دون تغيير أدوار الواجهة.

نظرا لأن عمليات نشر مجمع تدفق بطاقة واجهة الشبكة (NIC) المتعددة وفصل دور الواجهة غير مغطاة في دليل تصميم تحليلات الشبكة الآمنة، فإن هذا السلوك غير موثق بدلا من كونه غير مدعوم، وتعتمد النتائج فقط على التحقق من الصحة في المختبر.

المحتوى ذي الصلة

- دليل تثبيت الجهاز الظاهري Secure Network Analytics Virtual Edition

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).