安全网络分析虚拟设备网络接口配置限制

目录

问题

正在评估具有非数据存储的安全网络分析(SNA)的部署方案，其中流量收集器通过虚拟化平台分配了多个网络接口。

产生的具体问题是：

- 虚拟流量收集器是否可以与两个NIC一起运行 — 一个用于SNA内部通信，另一个用于NetFlow接收
- 当内部通信网段无法访问互联网时，是否可以使用多个NIC配置Virtual Manager设备以获取威胁源

环境

- Secure Network Analytics(Stealthwatch)版本7.6.0
- 所有SNA组件的虚拟设备版本（管理器、流量收集器）
- 具有分离的内部通信和NetFlow接收段的网络架构

分辨率

思科安全网络分析(SNA)流量收集器可以部署为两个NIC接口，并在实验室环境中验证此行为：

1.两个接口 — 管理访问和NetFlow接收

- 流量收集器可以配置一个用于管理访问的接口和一个专用于接收NetFlow的接口。
- 但是，管理访问仍可通过接口（管理或NetFlow）进行访问。 目前没有选项严格限制接口用于其预期目的。

2.两个接口 — NetFlow接收和威胁源接收

- 使用从流量收集器的Internet访问检索威胁源更新。
- 如果管理接口IP没有直接互联网访问，则可以配置流量收集器上可用的proxy选项以满足此要求，而第二个接口继续接收NetFlow。

关于范围的重要说明
这两种方案都仅在实验设置中进行了验证，未在SNA设计指南中记录。因此，它们必须被视为观察到的行为，而不是正式发布的设计建议。我们鼓励计划进行此类部署的客户首先在自己的测试环境中进行验证。

原因

此行为是设计在安全网络分析流量收集器设备架构中的。设备支持分配额外的NIC，并且可以在辅助接口上接收遥测(NetFlow)，同时主接口用于管理。但是，设备软件运行其管理服务（设备管理UI、SSH和SNA设备间通信）绑定到所有已配置和寻址的接口，并且不公开任何每个接口的服务绑定或访问控制选项。因此，管理访问仍然可以从任一网卡访问，并且不能限制到为此指定的接口。

同样，威胁源检索不与特定网卡关联。更新过程仅根据设备路由表启动出站连接，因此具有通往Internet的有效路径的任何接口都会为请求提供服务。当管理接口无法直接访问互联网时，设备管理中的代理配置选项通过已批准的代理服务器中继出站请求，从而允许威胁源在不更改接口角色的情况下成功更新。

由于多NIC流量收集器部署和接口角色分离未在《安全网络分析设计指南》中介绍，因此此行为未记录而非不受支持，并且调查结果仅基于实验室验证。

相关内容

- Secure Network Analytics Virtual Edition设备安装指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。