Limitações de configuração da interface de rede do Secure Network Analytics Virtual Appliance

Contents

Problema

Um cenário de implantação estava sendo avaliado para o Secure Network Analytics (SNA) com Armazenamento de Dados Não Pertencente ao qual o Flow Collector tem várias interfaces de rede atribuídas por meio da plataforma de virtualização.

As questões específicas que surgiram foram:

- Se o Flow Collector virtual pode operar com duas NICs - uma para comunicação interna SNA e outra para recepção NetFlow
- Se o dispositivo virtual Manager pode ser configurado com várias NICs para obter feeds de ameaças quando o segmento de comunicação interna não puder acessar a Internet

Ambiente

- Secure Network Analytics (Stealthwatch) versão até 7.6.0
- Versões de dispositivos virtuais de todos os componentes SNA (Manager, Flow Collector)
- Arquitetura de rede com comunicação interna separada e segmentos de recebimento NetFlow

Resolução

O Cisco Secure Network Analytics (SNA) Flow Collector pode ser implantado com duas interfaces

de NIC, e esse comportamento foi validado em um ambiente de laboratório:

1. Duas interfaces — acesso de gerenciamento e recepção NetFlow

- O Flow Collector pode ser configurado com uma interface para acesso de gerenciamento e uma segunda interface dedicada ao recebimento do NetFlow.
- No entanto, o acesso de gerenciamento permanece acessível através de qualquer interface (gerenciamento ou NetFlow). No momento, não há opção de restringir uma interface estritamente à finalidade pretendida.

2. Duas interfaces — recepção NetFlow e recepção de feed de ameaças

- As atualizações do feed de ameaças são recuperadas usando o acesso à Internet do Flow Collector.
- Se o IP da interface de gerenciamento não tiver acesso direto à Internet, a opção de proxy disponível no Flow Collector poderá ser configurada para atender a esse requisito, enquanto a segunda interface continua a receber o NetFlow.

Observação importante sobre o escopo
Ambos os cenários foram verificados apenas em uma configuração de laboratório e não estão documentados no Guia de design do SNA. Por conseguinte, devem ser tratados como um comportamento observado e não como uma recomendação de concepção oficialmente publicada. Os clientes que planejam essa implantação são encorajados a validá-la primeiro em seu próprio ambiente de teste.

Causa

Esse comportamento é definido na arquitetura do dispositivo Secure Network Analytics Flow Collector. O dispositivo oferece suporte à atribuição de uma NIC adicional e a telemetria (NetFlow) pode ser recebida nessa interface secundária enquanto a interface principal é usada para gerenciamento. No entanto, o software do dispositivo executa seus serviços de gerenciamento — UI de administração do dispositivo, SSH e comunicação entre dispositivos SNA — vinculados a todas as interfaces configuradas e endereçadas, e não expõe nenhuma opção de vinculação de serviço ou controle de acesso por interface. Como resultado, o acesso de gerenciamento permanece acessível de qualquer placa de rede e não pode ser restrito à interface designada para essa finalidade.

Da mesma forma, a recuperação do feed de ameaças não está vinculada a uma NIC específica.

O processo de atualização simplesmente inicia uma conexão de saída com base na tabela de roteamento do equipamento, de modo que qualquer interface com um caminho válido para os serviços de Internet atendem à solicitação. Quando a interface de gerenciamento não tem acesso direto à Internet, a opção de configuração de proxy no administrador do equipamento retransmite a solicitação de saída por meio de um servidor proxy aprovado, permitindo que o feed de ameaças seja atualizado com êxito sem alterar as funções da interface.

Como as implantações do coletor de fluxo de várias NICs e a separação de funções de interface não são abordadas no Guia de design analítico de rede segura, esse comportamento não é documentado, e não é suportado, e as descobertas são baseadas unicamente na validação do laboratório.

Conteúdo relacionado

- Guia de instalação do dispositivo Secure Network Analytics Virtual Edition

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.