O FireSIGHT pode identificar um host incorretamente ou marcar um evento como pendente ou desconhecido

Contents

Introduction

Um sistema FireSIGHT gera eventos quando detecta um novo host no segmento de rede monitorado. Ele pode detectar um sistema operacional ou serviço incorretamente ou com menos confiança. Se um evento for marcado como *Desconhecido*, significa que o tráfego é analisado, mas os sistemas operacionais não correspondem a nenhuma das impressões digitais conhecidas. Este documento fornece uma lista de verificação e recomendações para minimizar os eventos *Desconhecidos*.

Prerequisites

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Sistema FireSIGHT, dispositivos FirePOWER e dispositivos virtuais NGIPS
- Versão do software 5.2 ou posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Troubleshooting de Listas de Verificação

Se o seu sistema FireSIGHT estiver gerando eventos que estão em estado pendente ou desconhecido, você poderá seguir as etapas abaixo para começar a solucionar esse problema:

Observação: *Hosts não identificados* não são os mesmos que *Desconhecidos*. Hosts *não identificados* são hosts sobre os quais um sistema ainda não reuniu informações suficientes para identificar seus sistemas operacionais.

Lista de verificação de solução de problemas	Recomendações
1. Que versão do VDB está instalada no FireSIGHT Management Center?	A versão mais recente do VDB tem mais informações de impressão digital. É sempre recomendável ter a versão mais recente instalada no FireSIGHT Management Center.
2. Qual é o limite de hosts da sua licença do FireSIGHT? Quantos hosts foram detectados pelo FireSIGHT?	Se o limite de hosts for excedido, um sistema FireSIGHT corta os dados mais antigos à medida que os novos dados entram. Você pode configurar a Política do sistema para eliminar novos hosts quando o limite de hosts for atingido.
3. Quantos saltos distam os hosts do dispositivo gerenciado FireSIGHT?	Quanto maior a contagem de saltos entre os hosts e um dispositivo gerenciado, mais distante o host fica do dispositivo e, portanto, maior a probabilidade de que o tráfego tenha sido modificado e não permita uma identificação precisa.
4. Há algum dispositivo em linha entre os hosts e o dispositivo gerenciado?	A presença de qualquer dispositivo em linha, como firewall, dispositivo NAT, balanceador de carga e servidor proxy, pode modificar as informações originais do cabeçalho TCP ou IP que também podem ser as causas de coleta de informações não identificadas ou não identificadas dos hosts.
5. Os dispositivos gerenciados estão monitorando o tráfego em qualquer rede de roteamento assíncrono?	Se um sistema FireSIGHT monitorar o tráfego de roteamento assíncrono, talvez ele não consiga ver a sessão completa.
6. Há alguma porta fora do padrão usada para algum serviço? Há algum decodificador personalizado configurado para endereçar as portas fora do padrão?	Um decodificador personalizado configurado incorretamente pode entrar em conflito com os decodificadores padrão.

Dados adicionais

Se todas as recomendações acima forem seguidas, mas ainda assim forem encontrados hosts desconhecidos, pendentes ou não identificados, será necessário analisar os seguintes dados e dois-pontos:

1. Tráfego de sessão completo

Tráfego de sessão completo dos hosts identificados incorretamente ou marcados como desconhecidos ou pendentes.

2. Solução de problemas de arquivos

Solução de problemas de arquivos do FireSIGHT Management Center e do dispositivo gerenciado. O mapa de rede ou a topologia que mostra a localização do dispositivo gerenciado seria útil.

3. Captura de Pacotes (PCAP)

Os pacotes recebidos pelo dispositivo gerenciado podem ser diferentes dos pacotes originados nos hosts. Isso acontece se qualquer cabeçalho que modifique um dispositivo em linha existir entre os hosts e o dispositivo gerenciado. Portanto, é melhor capturar o PCAP de ambas as extremidades - hosts e dispositivos gerenciados, o que permite comparar os cabeçalhos dos dois PCAPs. Qualquer incompatibilidade entre os pacotes pode causar identificação incorreta de serviços ou hosts.

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.