使用Wireshark捕获和分析网络流量以进行诊断

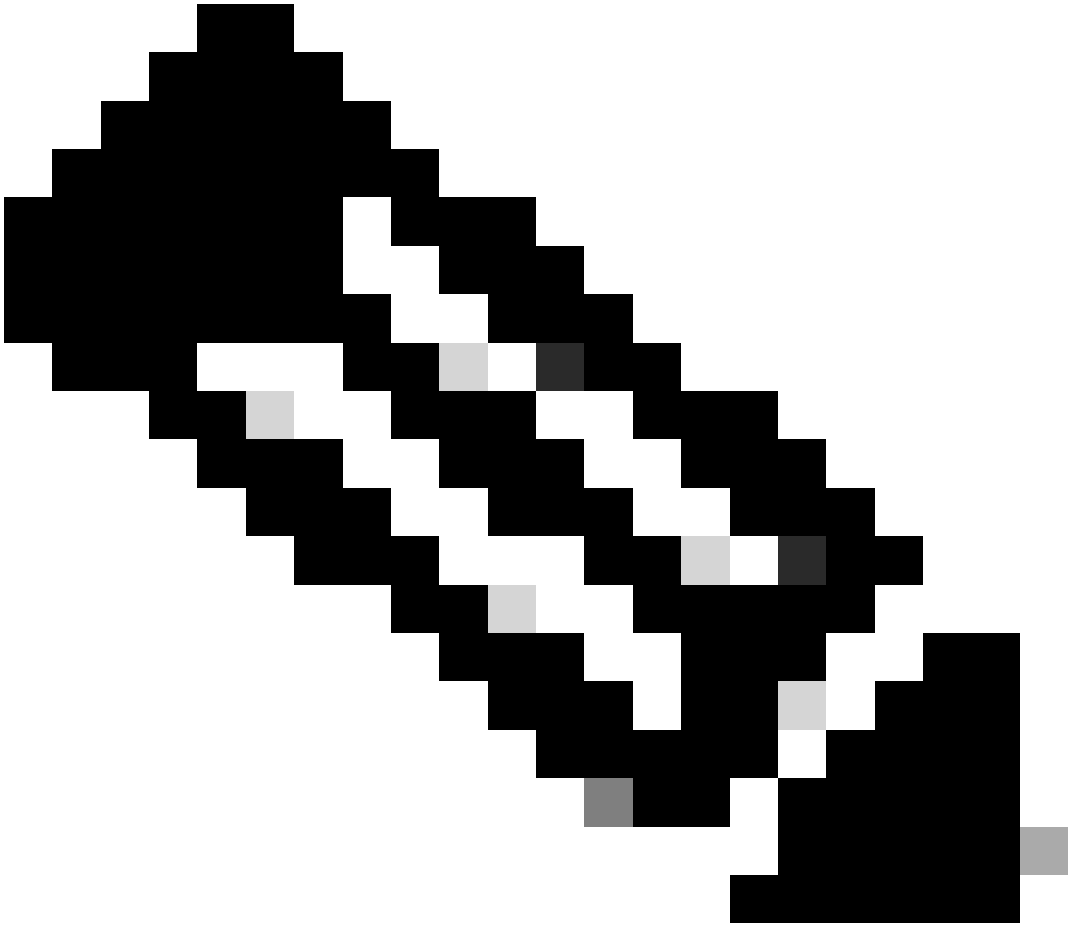
目录

简介

本文档介绍如何使用Wireshark捕获和分析用于诊断的网络流量。

概述

Wireshark是免费的应用程序，可用于读取和分析数据包捕获（也称为“TCP转储”）。 数据包捕获在数据包级别显示通过网络适配器进行的所有通信，因此可以查看DNS、HTTP、ping和其他流量类型。数据包捕获作为深度故障排除的诊断步骤尤其重要，随着SIG的引入，数据包捕获现在已经成为诊断过程的基本部分。



注意：Wireshark捕获选定适配器上的所有流量。由于数据包捕获通常包含个人身份信息(PII)，因此请始终使用安全方法（如Box链接）与支持人员共享捕获文件。

获取Wireshark

您可以在以下位置下载适用于Windows、macOS或Linux的Wireshark:https://www.wireshark.org/

收集数据包捕获

1. 选择连接到Internet的网络适配器，然后在Wireshark中开始捕获。
2. 捕获时，重现要诊断的问题。
3. 完成后停止捕获并将文件另存为`.pcap`。

基本端口和协议

- 大多数数据包在传输层协议TCP或UDP上通信
  - 例如，默认情况下，“DNS”在UDP的“顶部”运行。如果TCP失败，它会切换到UDP。
- HTTP和DNS是在传输协议+端口的组合上运行的常见协议。

传输层协议	端口	协议名称	使用率
TCP	22	SSH	远程VA访问
TCP	25	SMTP	VA监控
IP	50	ESP（封装安全负载）	机密性、数据完整性、源身份验证
IP	51	AH（身份验证报头）	数据完整性、源身份验证
UDP	53	DNS	DNS默认值
TCP	53	DNS	DNS故障转移
TCP	80	HTTP	Web流量（未加密）、API
UDP	123	NTP	VA时间同步
TCP	443	HTTPS	加密网络流量、API、AD连接器至VA
UDP	443	HTTPS	RC加密DNS查询
UDP	500	IKE	IPsec隧道协商
UDP	4500	NAT-T	IPsec隧道的NAT穿越
TCP	8080	HTTP	AD连接器与VA通信

了解协议名称、端口及其用途有助于您识别和分析Wireshark中的相关流量。

基本运算符

在Wireshark中构建过滤器字符串时，请使用以下运算符：

- `==`:等于(示例:`ip.dst==1.2.3.4`)
- `!=`:不等于(示例:`ip.dst!=1.2.3.4`)
- `&`:和(示例:`ip.dst==1.2.3.4 && ip.src==208.67.222.222`)
- `||`:或(示例:`ip.dst==1.2.3.4) || ip.dst==1.2.3.5`)

有关高级过滤器选项，请参阅Wireshark文档：6.4.构建显示过滤器表达式

过滤器

数据包捕获可能包含数千个数据包。过滤器可帮助您关注特定流量类型：

- 按协议：
  - `dns` — 仅显示DNS流量
  - `http || dns` -显示HTTP或DNS流量
- 按IP地址：
  - `ip.addr==<IP>`

— 所有来往流量<IP>
    - ip.src==<IP> -来自<IP>的所有流量
    - ip.dst==<IP> -发往<IP>的所有流量

- 其他：
    - tcp.flags.reset.1==检查TCP重置（超时）
    - dns.qry.name包含“[domain]” – 与域匹配的DNS查询
    - tcp.port==80 || udp.port==80 -端口80上的TCP或UDP流量

查看和分析数据包

找到数据包后，展开Wireshark中的数据段以分析详细信息。熟悉协议结构有助于解释这些详细信息，甚至可在需要时重新构建数据。

跟随数据流

使用数据包列表查找请求和响应对。右键单击数据包，然后选择Follow > TCP Stream、UDP Stream、TLS Stream或HTTP Stream以查看相关请求和响应序列。

- 对于具有多个交换的协议（例如HTTP），这比对于单请求协议（例如DNS）更有用。

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）。