HongKe 虹科

PROFITAP

白皮书

# NetFlow vs 元数据 vs 数据包检测

*它们有什么区别？*

我需要哪一种？

它们各自的优缺点是什么？

# 概览

随着时间的推移，IT工程师们正面临着如何在网络监控方面保持领先的难题。速度和馈送增加了，而接口成本却大大降低了。40Gbps的连接曾经是我们梦寐以求的东西--现在突然就在这里了。伴随着这一趋势，攻击、漏洞和入侵也在不断上升。大多数IT人员都意识到，如果他们还没有采取监控方法，现在是时候部署到位了。但是，怎么做呢？

有三种常见的方法来收集和报告遍历网络的数据：NetFlow（或任何基于流的监控方式）、数据包数据和元数据。但哪种方法适合您和您所负责的故障排除和保护的环境呢？

本文将对每种方法的监控方式进行分解，讨论其优缺点，并提供最佳实践，以确定使用的合适时机。

我们先从一些人认为是分析的黄金标准--数据包数据说起。

# 深度数据包检测

数据包是目前最详细的监控方法。事实上，其他两种方法大多使用数据包数据来创建它们产生的统计数据。通过数据包数据，我们可以测量数据包间的时序、服务器的响应时间，甚至可以解密流来查看应用的有效负载。

## *优点：详细信息，详细信息，详细信息*

一切都在数据包中。每一个位、字节和报头值都可以用于全面了解问题发生时的真实情况。有些问题只能在原始数据包数据中看到，这样才能真正分析出全貌。例如，如果一个问题是由TCP连接中的MSS值过低造成的，数据包数据使分析人员不仅可以在TCP对话中看到这个问题，而且可以将其与网络中预期的ICMP消息相关联。

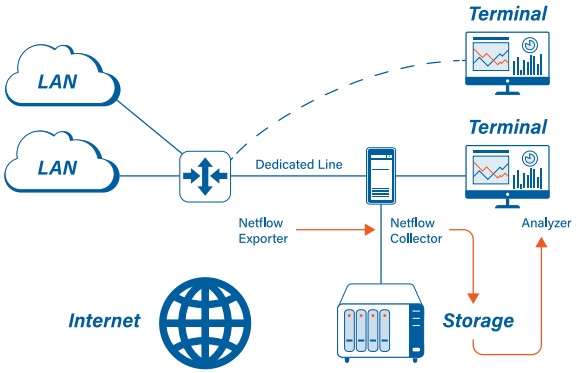
## *缺点：数据过载！*

在数据包中很容易大海捞针。特别是在高速、高容量链路上捕获时，数据包数据会很快变得不堪重负。考虑一下——在只有50%利用率的10Gbps链路上捕获5分钟，将导致近200GB的数据包捕获量！这使得回溯时间的故障排除变得困难。因为很难存储足够的数据来查看过去几个小时或几天的情况。

挖掘数据包需要技巧、经验和耐心。虽然这是最详细的方法，但需要根据分析的目标进行权衡。

# NetFlow

## (或其他基于流的方法)




分析网络流量并不需要在每一个案例中都去挖掘数据包。有时，高级别的统计数据足以帮助我们实现目标。这只是取决于我们在寻找什么。NetFlow是对网络基础设施设备产生的IP流量进行汇总，然后将其发送给采集器，生成漂亮的流量数据图表。

### 优点：长期监控，简单易读

流量提供了适当数量的统计信息，这些统计信息可用于查找网络入侵，并确定高层对话者和高利用率的原因。为此，我们并不需要流中每个数据包的详细信息。大多数流解决方案提供了IP地址、TCP或UDP端口号、DifSrv值、流时间、流长度和流中的数据量。许多这样的监控系统允许分析人员查看过去几天、几周甚至几个月的流量。

### 缺点：没有数据包有效负载，网络RTT或服务器响应时间

由于NetFlow将一个方向上的数据包流看作是一个单一的统计数字，因此它不提供时序详细信息以允许测量网络往返时间或数据包间的延迟。没有收集TCP标志、窗口大小和握手选项等报头详细信息，而这些详细信息在排除复杂问题时至关重要。

简而言之，如果监控流量的目标是为了取证和安全而长期监视网络，NetFlow是理想的工具。

# 元数据

这种方法提供了其他两种选择之间的最佳点。数据包数据由分析器收集，并在那里进行分类、解析、索引甚至存储（在某些情况下）。这允许生成并长期存储有关网络流量、使用情况、带宽、甚至应用性能的图表和统计数据。它为大多数常见的故障排除活动提供了数据包级别的细节，而不需要在庞大的pcap中进行复杂的挖掘。

### 优点：在NetFlow上有更多细节，没有数据包复杂性，可以长期索引。

iRTT、应用程序响应、TCP重传和DNS响应代码之类等统计信息可以随时间进行监控和绘制，使分析师能够测量它们并发现痛点。如果出于任何原因需要比元数据提供的更多细节，例如流量解密，则可以过滤和导出数据包，以便进行更集中的深入研究。

### 缺点：硬件资源，数据丢失

该工具需要大量的资源来进行线速分析，而线速分析通常非常昂贵。由于在将数据包转化为长期元数据的过程中发生了太多的事情，所以进行压缩的机器需要一些强大的处理能力。此外，还存在明显的数据丢失或过度配置的风险，特别是在高速链路上。

# 将2和2放在一起

IOTA采用了这三种分析方法的优点，并将它们整合到一个紧凑、便携和具有成本效益的工具中。它能够通过将数据流传输到1TB加密硬盘（可扩展到外部存储）来利用数据包收集的力量，同时对入口数据进行线速分析。

可以使用内置的仪表盘访问和分析关键性能和取证数据。带宽利用率、DNS性能、TCP指标、应用延迟、用户体验等都可以在自定义屏幕上进行监控，这些屏幕是根据发现问题所需的确切数据建立的。这使得各种经验水平的IT人员都能主动和积极地解决网络问题。

对于取证分析，在搜索入侵或漏洞时，可以通过对话流、GeoIP位置或带宽消耗来查看流量。在排除性能缓慢的问题时，数据包级别的统计数据，如网络延迟、TCP指标和服务器响应时间可以指出根本原因。如果有必要对数据包进行更深层次的挖掘，只需点击一下就可以得到一个经过过滤的、可导出的跟踪文件。

使用IOTA，可以在一个单一的窗口上利用数据包的细节，NetFlow的简单性和元数据的强大功能-所有这些都无需花钱！