选择用于回溯式分析的网络记录仪以解决间歇性问题和意外事件

通常，获得网络上发生的不受欢迎或间歇性事件的根源的唯一方法是使用网络记录仪。网络记录仪是可按全线速捕获和存储数据包且不会丢包，也不用进行数据包切片的设备。

在本白皮书中，您将了解何时使用网络记录仪，以及选择用于回溯式取证分析的网络记录仪的重要注意事项。

目录

FLUKE networks

简介

网络经理通常依靠基本协议分析仪（如 Wireshark）或监控设备（如 RMON 探测器）跟踪网络情况。但是，尽管精密的分析仪和探测器很有用，但它们也只不过是提供统计 KPI 的流量采样设备。此类设备有时可以指明长期存在的问题，但是它们无法全面地回顾和调查问题，因为它们未捕获和存储所有与问题相关的数据包。问题根源仍难以捉摸，进而导致相互指责的情况和工作效率的持续降低。

传统协议分析仪的缺点

当今市场上的协议分析仪通常基于软件，可安装在普通 PC 上。它们通常具有以下一项或多项限制：

- 捕获缓冲区较小，这意味着只能捕获少量数据包，已满时就必须停止捕获，否则必须循环使用缓冲区，而这通常会丢失重要数据。
- 如果将切片用于增加缓冲区可保存的数据包数量，将影响有效负载数据的可视性。这通常就难以分析安全问题、合规问题和某些类型的应用程序问题。
- 同时监控多个位置和关联数据的功能通常受到很多限制。存在冗余路径、负载平衡或非对称流量时，很难获得完整视图。
- 远程位置通常缺少足够分析功能。操作员可能需要将整个缓冲区的内容传送到网络上，才能进行分析。
- 协议分析仪可能无法打开较大的跟踪文件，或在尝试打开一个跟踪文件时会运行很慢。

何时需要使用网络记录仪?

拥有包括数据包有效负载的完整视图现在更加重要，因为只有这样才能解决问题。以下是一些特别需要借助良好网络记录仪的情况：

- 数据中心整合或虚拟化期间。较少的服务器或数据中心需要处理较多的流量。更多的流量进入较少的网段，运行速率高达 10 Gbps，而且利用率也较高。来自此类网段的流量将快速超过传统分析仪的捕获缓冲区的容量，只能保留非常少的流量供将来深入分析。
- 网络更稳定，但出现更多的间歇性问题和随机问题。确定可以找到问题数据包的唯一方法是捕获并存储所有数据包。
- 部署新应用程序时，因不同应用程序层出现互操作性问题或网络互连设备配置不兼容而出现意外行为：数据包由网关分区，层之间的延时预期，以及 IP 端口被防火墙阻止。这些问题的根源分析不仅需要响应时间测量值，还需要有效负载的详细分析。
- 尝试获取未经授权的网络访问。即使是最好的 IDS/IPS，也会丢失某些入侵。这些问题通常在正常工作时间外发生，只有捕获和存储所有数据包才会被发现。网络安全和运营团队需要通过查看流量有效负载来了解入侵者使用的方法，从而采取相应措施来禁止将来未经授权的访问。
- 其他会启动广播风暴和造成应用程序和网络瘫痪的意外事件，例如由在 VM 中移动资产导致的应用程序性能问题。

- 某些员工不当使用网络，如下载和观看视频流。您需要评估这种额外带宽占用是否会影响工作效率或给网络带来无法承受的负担。能够重建实际视频内容将有助于提供影响答案并提供有关纠正措施的证据。

简单类比

只是知道存在问题和真正找到问题根源是不同的。请考虑这种情况。您将车停在购物中心的停车场，然后走进购物中心进行购物。您回到车旁时，发现其中一个车门严重凹陷，但无任何便条留下。您知道遇到问题，但您知道的仅此而已。现在考虑如果该区域存在一个或多个摄像头，情况将有何不同。通过回放安全摄像头拍摄的视频，可以发现一辆卡车撞到车门，而且可以看到卡车的车牌号。现在，您就具有足够信息可提交给保险公司，而保险公司可找到司机并制定解决方法。这种情况下的安全摄像头与网络上的网络记录仪类似。

没有适当网络记录仪的风险

如果没有网络记录仪，或网络记录仪缺乏某些重要功能，会导致以下问题：

- **误报 –** 这些表面上是问题，但如果只能详细重建完整的事务，则将证明为良性问题。
- **漏报 –** 由于丢失部分证据，未检测到某个问题。
- 职能团队将互相指责（***“这不是我们的问题，是他们的问题”***），因为没有足够证据可正确指出问题原因。
- **间歇性问题 –** 检测到问题，但是当把便携式分析仪拿到问题网段进行测试时，未发现问题。
- **无用户友好分析功能 –** 存储的数据包足够，但无法找到所需信息，因为网络记录仪未提供快速简便的方法来从大量存储的数据包中检索所需信息。

选择网络记录仪时的重要注意事项

可视性	一部记录仪可连接至多少条链路，可链接至哪种类型的拓扑结构？
性能	线速为 64 字节/秒帧且无丢包时，数据进入磁盘（不是内存）的吞吐量为多少？ 打开实时监控或数据分析对吞吐量的影响如何？
容量	是根据初始存储容量还是实际可用数据存储容量指定存储容量？ 是否存在一种对流量进行过滤或切片，从而仅存储相关数据的方法？
冗余	是否使用 RAID 5 或 10？如果没有，则在硬盘出现故障时将会发生哪种情况？数据会不会丢失？要恢复系统和/或数据需要多少工作量？
易用性	分析捕获的数据有何难度？ 是否可以轻松对从网络各部分收集的数据进行汇聚、分段和分析，以便获得根源？

如何降低风险

通过安装一个或多个网络记录仪，可降低这些风险。但是，务必审查网络记录仪规格，确保购买的网络记录仪可满足需求。以下是需要提问的部分重要问题：

- 根据不良性能会给业务带来严重负面影响的判断标准，可将网络上的多少个点视为关键任务？考虑安装足够的网络记录仪来捕获每个此类点的流量。
- 每个点的带宽是多少？确保该处安装的网络记录仪可按全线速捕获并存储数据包，且不会丢包。
- 需要捕获多长时间的数据包，才能完好地展示所有可能发生的事件？将此时间乘以网络利用率的足够估计值。接着确保网络记录仪至少具有该存储容量。务必考虑可用于存储数据包的实际容量。部分网络记录仪将 30% 的初始磁盘空间用于长时间运行的系统和其他开销。
- 是否存在保留重要数据的方法，以便在捕获磁盘循环使用时不会覆盖这些数据？网络记录仪中的数据通常按“记录”（按开始时间和结束时间定义的数据块）整理。网络记录仪是否可锁定单条记录，以便不会覆盖它们？
- 捕获性能是否易于与实时监控或其他功能冲突？确保监控和捕获功能之间不存在令人不满意的平衡。这将让使用网络记录仪的主要目的落空。
- 硬盘系统中的冗余是否足以保证在发生硬盘故障时实现整体捕获？例如，RAID 5/10 磁盘系统比 RAID 0 磁盘系统更加可靠。各个硬盘是可轻松更换还是需要维修技术人员才能更换？这可能意味着面临泄露敏感数据的风险。
- 是否存在有效的硬件过滤器功能，从而只捕获您要观察的特定类型的数据包？测试仪通过 SPAN 端口监控网络时，有时某个数据包可显示多次，因为它出入交换机。测试仪是否具有在捕获期间取消重复帧的机制，从而节省容量和避免混淆？
- 是否存在可应用于捕获后分析的显示过滤器，使屏幕不会显示无关数据，让您方便地查看特定感兴趣的区域？例如，是否存在针对特定类型的 VoIP 流量、基于 ID 的特定主叫方和被叫方和/或 VoIP 特定问题的过滤器？是否存在模式匹配功能，从而对包含其中一个数据包模式的流量进行隔离？
- 是否提供便于在显示屏中查看结果的用户友好分析功能？这很重要，因为这可保证无需网络专家也可使用网络记录仪。
- 是否可从一个或多个远程位置访问和控制多个网络记录仪？在问题涉及多个网段时，这有助于获取完整视图。
- 是否可合并和关联从多个网段收集的信息？查找高级的多网段功能。确保存储的数据包具有精确（纳秒）的计时信息，以便可以正确同步不同网段中的数据。
- 是否同时提供机架式和便携式版本？通常应该在关键任务网段中安装机架式网络记录仪，而便携式网络记录仪可用于连接至其他网段（这些网段与调查相关时）。

总结

存在会让网络面临重大风险的严重问题，但这些问题极少发生或间歇性发生。网络记录仪是用于检测和分析此类问题的最重要工具。但是，在购买一台或多台网络记录仪前，务必仔细审查规格。编写本白皮书的目的就是帮助您选择用于回溯式分析的正确网络记录仪，以便确定意外事件并解决网络上的间歇性问题。

福禄克网络公司提供 Network Time Machine™ — 海量在线应用分析系统产品，即具有各种捕获速度和存储容量的网络记录仪。机架式和便携式版本均提供。

有关详细信息，请访问 **www.flukenetworks.com/ntm**

福禄克网络公司的以应用程序为中心的回溯式取证分析

通过独特的以应用程序为中心的网络取证功能，福禄克网络公司的海量在线应用分析系统 (NTM) 和 ClearSight™ 分析仪 (CSA) 可简化并加速问题根源的确定。海量在线应用分析系统 (NTM) 是一种最佳的导入磁盘式产品，它可以记录网络流量，然后生成数据的索引并加以分类。NTM Atlas 软件允许您倒带和查看事件与背景信息，以便提取 ClearSight 分析仪所需的数据*。ClearSight 分析仪与海量在线应用分析系统集成，可为无与伦比的以应用程序为中心的分析功能提供直观且易于使用的界面，便于快速提供答案。

凭借 NTM 和 CSA，您可以记录、识别和分析当前网络流量和以前网络流量，以便快速查看当前发生的或者过去数天或数周发生的活动：

- 在不查看数据包的情况下解决应用程序性能问题
- 间歇性应用程序事件的问题根源的回溯式隔离
- 提供证据来跟踪导致重要性能事件和安全或合规问题的事件序列
- 排查从应用程序级别到数据包级别之间的任意位置发生的问题
- 在部署新解决方案之前调试设备和应用程序性能

如面了解回溯式网络取证分析的详细信息，请访问：**www.flukenetworks.com/networkforensics**

*CSA 软件可集成在 NTM 中，也可单独提供，以便在 PC 上安装协议分析功能。

联系福禄克网络公司：电话 **800-283-5853**（美国/加拿大）或 **425-446-4519**（其他地区）。电子邮件：**info@flukenetworks.com**

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

福禄克网络公司的业务遍及全球 50 多个国家/地区。有关当地办事处的详细联络信息，请访问 **www.flukenetworks.com/contact**