WHITE PAPER

无损的网络可见性的重要性

无损的可见性的重要性

IT安全和分析工具的好坏取决于他们看到的数据。IT部门根本挑战是确保这些工具背后的基础设施提供可靠、快速和安全的应用程序。这意味着IT需要全面了解网络。鉴于当前的网络安全威胁级别以及企业对数据网络的完全依赖，您无法承受部分网络可见性。您需要无损的可见性。

根据Ponemon Institute进行的2016年数据中心中断成本研究，网络中断的平均成本为每分钟7793美元。当网络出现故障或受损时，时间很重要。这一点尤为重要，因为根据思科视觉网络指数、预测和方法：2015年至2020年，全球IP流量水平将从2015年的每月72.5EB增加到2020年的每月194.4 EB，是2015年的三倍。更好的网络可见性可以帮助精确定位问题，从而缩短平均修复时间。

可见性架构通过将监视策略与安全架构和问题解决流程进行组织和集成，有助于消除这些担忧。但是，创建可见性体系结构时要考虑三个基本项目：

- 当您试图控制成本时，性能很重要
- 数据丢失是不必要的安全风险
- 数据丢失导致故障排除工作时间更长、成本更高

那么，如何消除这些问题呢？

根据思科视觉网络指数、预测和方法：2015年至2020年，研究表明全球IP流量水平将从2015年的每月72.5EB(或72.5x1018)增加两倍，到2020年达到每月194.4 EB。

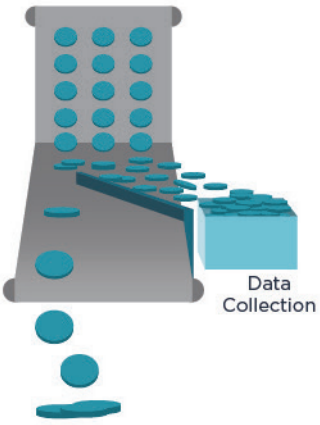
根据2016年ZK Research的一项调查，有45%的受访者承认为了提高性能，他们关闭了安全设备中的功能。

监控组件性能影响网络可见性

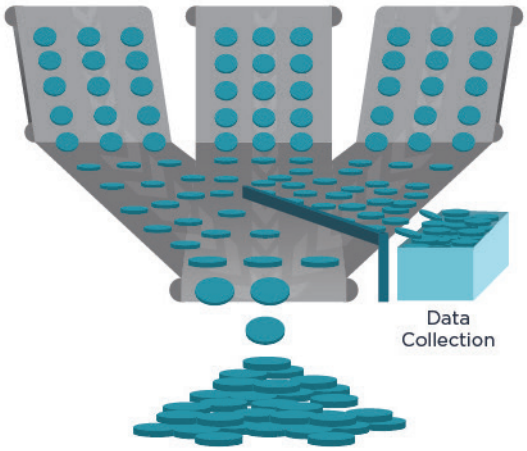
简而言之，性能很重要。出色的战略执行不力不会使您在竞争激烈的市场中走得太远。但是，企业数据网络的积极表现可能对已完成的交易和销售订单的履行产生深远的影响。

企业的监控解决方案需要在高性能水平上运行。这包括能够以线速处理数据，从而不会丢失任何数据包。随着核心网络速度从10 GE上升到40 GE和100 GE，甚至400GE，此性能水平变得越来越重要。监控解决方案需要本机全速支持这些速度。这意味着数据访问，网络数据包代理（NPB）和监视工具都需要能够以最高性能运行。

您的监控设备需要能够处理流量负载每周，每日和每小时波动，以便您可以捕获适正确的数据。否则，您可能会错过关键数据。如下图所示，监视设备在稳定状态下运行是一回事，而在随时间变化的负载条件下运行则是另一回事。



低速监控数据收集一些解决方案会丢失数据包。



高速监控数据收集小数据丢失可能会变得非常严重。

不幸的是，IT部门经常被迫做出可能不明智的权衡。根据2016年ZK Research的一项调查，有45%的受访者承认为了提高性能，他们关闭了安全设备中的功能。其中一个原因是，尽管一个安全工具可能能够像“ 瑞士军刀” 那样处理多个任务（入侵防御，防火墙，恶意软件检测，DDoS，解密等），但单个设备中的处理器却无法满载地处理任务。 在其他情况下，安全工具被迫执行非核心任务（如重复数据删除，数据屏蔽等），这会使该工具的CPU过载并使其运行缓慢。

虽然性能绝对是当务之急，但它真的比网络安全更重要吗？ 为什么要要求IT部门做出这种权衡呢？答案是您不应该，也不必如此。您只需要了解问题，然后就可以优化监控解决方案。

另一个性能需求涉及创建非阻塞架构。当打开多个功能时，某些数据包代理无法支持线路速率（例如，单个模块中的重复数据删除加NetFlow或SSL解密）。基于软件的NPB系统尤其如此。使用CPU和基于软件的处理会导致解决方案功能受CPU功能的限制。这种缺陷在超定用时更加明显，其中多个标准端口共享单个端口的资源以进行高级数据包处理。

有许多高级监控解决方案可满足不丢失数据包，无需关闭功能以及无阻塞架构的要求。例如，有一些基于现场可编程门阵列（FPGA）的NPB系统，它们能够以最小的延迟和不丢失数据包的速率支持线路速率。这是因为基于FPGA的数据包代理可以专门用于处理监视功能（如重复数据删除，数据包切片，协议标头剥离等），并且仍以线路速率运行。这样就无需进行性能折衷和权衡。

关注我们

数据丢失可能会导致错过安全威胁

暂时不考虑性能问题，您的体系结构是否捕获了所需的所有必要信息，或者是否缺少捕获安全相关事件所需的关键信息？根据EMA 2016年的一项研究调查，78%的受访者表示，他们的监控工具收到所有需要的数据包非常重要。与此同时，29%的人表示，他们对自己的工具正在接收所有数据并不完全有信心。这种怀疑是出于善意。Tolly Group对两个网络数据包代理进行了比较，发现其中一个数据包代理确实丢弃了数据包数据而没有报告。根据2016年的报告1，有问题的供应商“展示了每种数据大小的数据包丢失情况。256字节及以下时，丢失范围从20%到近75%。唯一比丢失数据更糟糕的是不知道您从一开始就丢失了数据。

唯一比丢失数据更糟糕的是不知道您从一开始就丢失了数据。

这些丢失的数据是一个极其重要的问题，因为数据丢失意味着您可能会遇到误报和/或错过入侵的真正积极指标。根据2016年Verizon数据泄露调查报告，大多数受害公司并不是自己发现安全漏洞的。大约75%必须由执法部门和第三方(客户、供应商、业务合作伙伴等)通知他们已经被入侵了-他们并不知道入侵已经发生。要打败现代网络安全威胁已经够难的了，你可不想从有限的网络可见性出发，在黑暗中摸索着找出缺失的是什么。

例如，许多安全工具需要“ 会话粘性” 。这使他们能够关联会话的所有组件，以评估风险并分析数据中的安全威胁。当数据丢失时会发生什么？通常会有两种结果--这两种结果都非常糟糕。结果1是设备、入侵防御系统(IPS)或某些其他内联安全分析工具没有检测到会话已关闭。如果打开的会话过多，该工具的内存将无法跟踪更多会话。在某些情况下，安全工具将从“ 内联阻止模式” 状态转换到“ 带外检测模式” 状态。然后，它发送故障警报，但忽略其他会话，允许它们在不进行检查的情况下向下游传递。这意味着设备没有主动分析这些潜在的安全威胁。IT工程师也可以手动发出命令将工具移回在线状态。然后，工程师需要执行某种类型的分析，以查看是什么触发了事件，这需要花费更多的时间和精力。

根据2016年Verizon数据泄露调查报告，大多数受害公司并不是自己发现安全漏洞的。大约75%必须由执法部门和第三方(客户、供应商、业务合作伙伴等)通知他们已经被入侵了。

结果2是安全工具，如Web应用程序防火墙(WAF)，在会话未结束时简单地忽略数据。这意味着它可以让可能是恶意软件或其他安全威胁的数据直接通过而不发出警告。此外，证据(数据包数据和丢失数据信息)被设备无意中丢弃了，因此现在工程师甚至不知道问题，也不知道如何调试情况。

在第二类示例中，数据丢失实际上可以帮助黑客隐藏自己。例如，黑客会从DDoS攻击开始。当目标网络设备被下载时，安全工具和监控设备也将被下载。如果NPB开始丢弃它应该发送到安全工具的数据包，那么在黑客开始探测弱点时，数据包的丢失可能会为黑客提供一种烟幕掩护。

数据丢失实际上可以帮助黑客隐藏自己。例如，黑客会从DDoS攻击开始。当目标网络设备被下载时，安全工具和监控设备也将被下载。如果NPB开始丢弃它应该发送到安全工具的数据包，那么在黑客开始探测弱点时，数据包的丢失可能会为黑客提供一种烟幕掩护。

第三个示例可能是带外入侵检测系统(IDS)，它正监视来自交换端口分析器(SPAN)端口的数据的。SPAN端口是众所周知的转发汇总数据的实体，而不是所有数据的完整副本。SPAN丢弃错误和丢失的数据。这使得攻击者能够将威胁(如数据包负载中的嵌入式恶意软件)隐藏在SPAN端口未受监视的间隙内。相反，分路器将转发所有数据包的完整内容，这可能表明存在应该分析的数据间隙。

这三组示例说明了丢失的数据如何帮助隐藏/加剧安全威胁。

完整的可见性意味着更快的故障排除

所有监控数据的完整副本还允许您更快地进行根本原因分析。某些解决方案，如SPAN端口和基于命令行界面(CLI)的数据包代理，可以裁剪数据或仅提供汇总版本。裁剪的数据显然是不好的，因为您不知道丢失了什么，除非您执行广泛的评估。汇总的数据也同样糟糕。这意味着数据被认为是相关的(格式错误的数据包、校验和损坏的数据包等)。它实际上对故障排除非常有用，从来不会被传播。直接影响是未知的数据丢失，由于丢失/误导信息以及丢失的安全威胁，在解决网络问题时通常会导致延迟和误诊。

丢失的数据可能会导致更长时间和更高成本的故障排除工作。具体地说，它可能导致错误的结论、更长的解决时间、更差的用户体验质量和更低的客户满意度。

这些丢失的数据可能会导致更长时间和更高成本的故障排除工作。具体地说，它可能导致错误的结论、更长的解决时间、更差的用户体验质量和更低的客户满意度。例如，丢失的数据看起来与通过网络丢弃的数据包相同。这通常会产生一种“ 假阳性” 的结果，IT管理员或网络运营中心(NOC)可能最终会通过故障排除工作流程来解决一些根本问题，然后立即得出结论认为网络正在丢弃数据包。这是有问题的，原因有两个。首先，他们可能会宣布“ 成功” ，而实际上并没有在实际网络上发现任何问题。其次，组织可能会花费大量的时间、精力和金钱尝试“ 修复” 数据包丢失问题，因为他们认为这是一个网络问题。例如，第一个补救措施可能是增加观察到的链路上的带宽。经过一定的时间和努力，他们会发现这个行动并没有解决任何问题。错误的结论实际上将一个问题变成了两个问题，他们的平均修复时间(和可能的客户满意度)得分受到了影响，因为他们仍然没有解决最初的问题。此外，由于误报，IT管理员和团队将开始经历很多挫折，并对监控解决方案产生怀疑。

在第二个示例中，丢失的数据使监控工具更难执行其工作。例如，以性能分析工具为例，在一定的数据包丢失量时，该工具监视数据的能力将开始失效。这是因为由于“ 结束会话” 数据从未通过，从而需要大量的内存来监控未完成的对话。因此，当内存缓冲区达到其最大阈值并且性能数据变得毫无价值或效用极低时，该工具的效率就会降低。

另一个例子是，也许有些数据最终确实到达了工具。但是，数据是乱序的，因为缓冲器对数据包进行了重新排序。这也可能导致损失。即使探针可以弥补丢失/排序错误的数据，它也会给工具带来更高的负载，并有损于工具分析数据的核心目的。工具CPU和内存资源被浪费在尝试更正设计不佳的网络数据包代理或设计不佳的可见性体系结构引入的错误上。

如何实现无懈可击的可见性

如果您不能最大限度地利用您的监控设备，那么为什么要使用它呢？有几种方法可以防止网络上的监控数据丢失。首先，使用负载流量生成器(即以20到40 Gbps的速度)验证现有和未来的NPB解决方案。这就是橡胶与道路相遇的地方。

事实是，某些网络数据包代理制造商无法支持同时运行所有功能，更不用说以全线速运行了。在60%或更高的负载下测试您的解决方案以了解真相。为什么购买监控解决方案只是为了让它以半速运行呢？

您不能查看图形用户界面(GUI)中列出的统计数据。你需要公正的验证。事实是，某些网络数据包代理制造商无法支持同时运行所有功能，更不用说以全线速运行了。在60%或更高的负载下测试您的解决方案以了解真相。为什么购买监控解决方案只是为了让它以半速运行呢？你的内部和外部客户不会满足于借口。

第二个考虑因素是寻找使用FPGA组件的解决方案。您希望以线速运行所有NPB功能，对吗？FPGA是专门构建的微处理器，可以编程以专注于专门的活动。这使它们比CPU具有性能优势，特别是在数据包重复数据删除、协议报头剥离、数据包裁剪、数据屏蔽和时间戳等高级功能处理功能方面。执行这些功能的CPU和软件方法存在固有问题，因为每行代码都会窃取周期，从而使CPU加软件方法变慢。越快越好。

第三个考虑因素是确保您的监视解决方案具有直观易用的GUI。 ZK Research的数据显示，创建的CLI筛选器中20%存在错误。许多自我造成的性能，安全性和故障排除错误可以避免。使用点击式和拖放技术的GUI消除了此错误源。为什么要增加工作量的复杂性和工作量？ GUI界面使生活更加轻松，并且不易出错。

方案咨询

结论

并不是所有的网络数据包代理都是平等的。随着网络和安全性需求的增加，NPB技术继续快速发展。要最大化任何解决方案的性能，请考虑评估当前和未来NPB的实际性能(负载为60%或更高)。您还应该考虑调查数据包代理是否为零丢失解决方案，以及它是否将GUI界面用于所有管理功能。

Cubro架构使用FPGA来处理数据(而不是运行软件的CPU)，并且具有完全集成的GUI。这使得我们的客户可以不受任何限制地进行线速操作。他们可以全速监控其网络，从而使业务具有竞争优势。