itbigtec
艾体宝

IOTA
应用程序延迟分析

问题描述

越来越多的应用程序由云提供商作为SaaS从全球分布的数据中心提供。通常，这提供了简单的应用程序部署。然而，它也带来了新的错误源，可能会影响应用程序的性能。例如，延迟问题可能导致应用程序迟缓，甚至导致这些应用程序超时。对于数据包丢失，会发生类似的行为，并且可以看到重新传输。

实时应用程序，特别是通过Microsoft Teams或WebEx进行的视频会议，对此类错误模式的反应非常敏感。在WAN链路上具有直接顺序数据库查询的遗留应用程序中，高延迟也会对应用程序性能产生负面影响。

如果应用程序堵塞住，在许多情况下这是由于TCP Zero Windows造成的。当这种情况发生时，网络已经正确地传输了用户数据，但由于本地性能限制，服务器或客户端无法进一步处理。

此外，越来越多地使用具有不同带宽、数据包丢失和延迟特性的WAN链路组合的SD-WAN解决方案。尽管相关的管理解决方案中有积极的表现，但如果应用程序性能不令人满意，那么熟悉的画面很快就会呈现：在负责应用程序、客户端、服务器和网络的人之间寻找问题。

Profitap IOTA希望通过直观的仪表板和可靠的流量捕获。

工作流疑难解答

以下示例逐步概述了如何使用Profitap IOTA对降低的应用程序性能进行分析。所使用的示例是一个缓慢且卡顿的Office 365应用程序。

作为第一步，我们需要配置物理接口。为此，我们导航到左侧菜单树中的"捕获"菜单，然后导航到"接口配置"页面。

在所示的配置中，接口配置为具有10/100/1000 Mbit/s自动协商的SPAN模式，因此两个物理接口都可以从SPAN端口或TAP接收要分析的流量。

如果IOTA要内联集成到数据流中，则必须选中内联模式旁边的框，然后单击保存按钮。

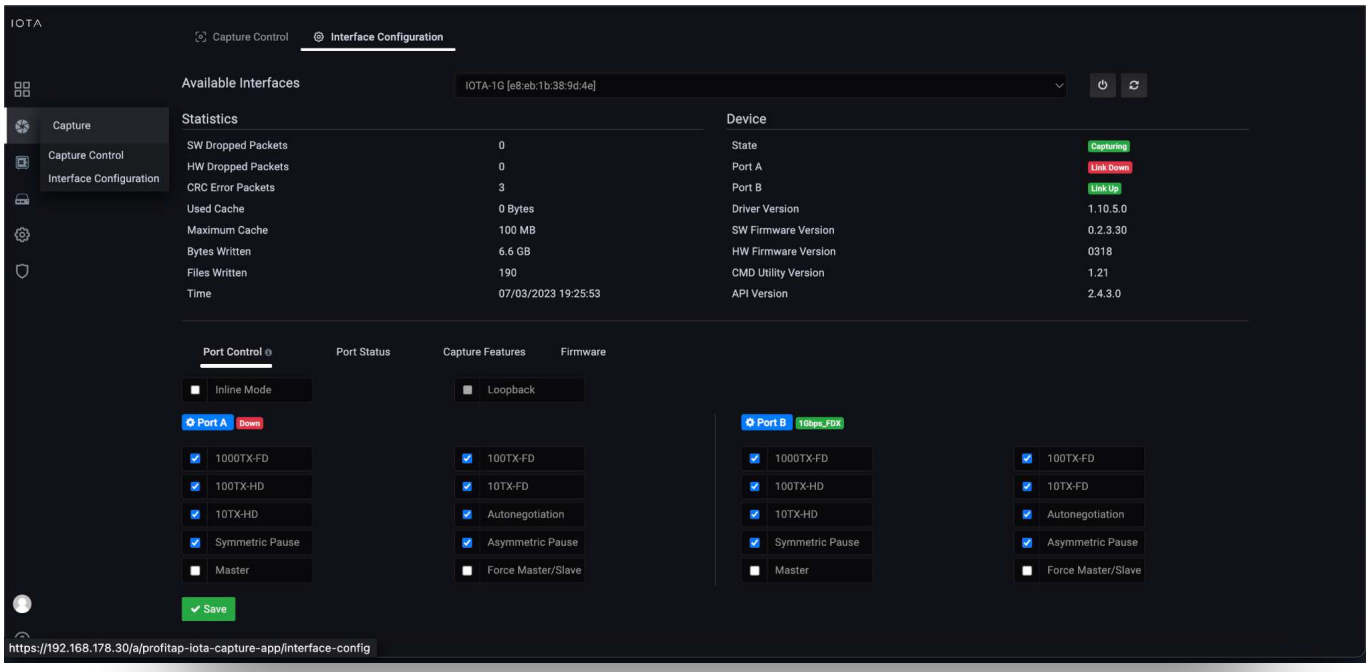

图1：物理接口的配置。在这种情况下，在SPAN模式下的10/100/1000 Mbit/s自动协商。

在我们准备好物理接口后，我们连接相应的电缆，并通过单击"开始捕获"按钮在"捕获控制"页面上开始捕获过程。

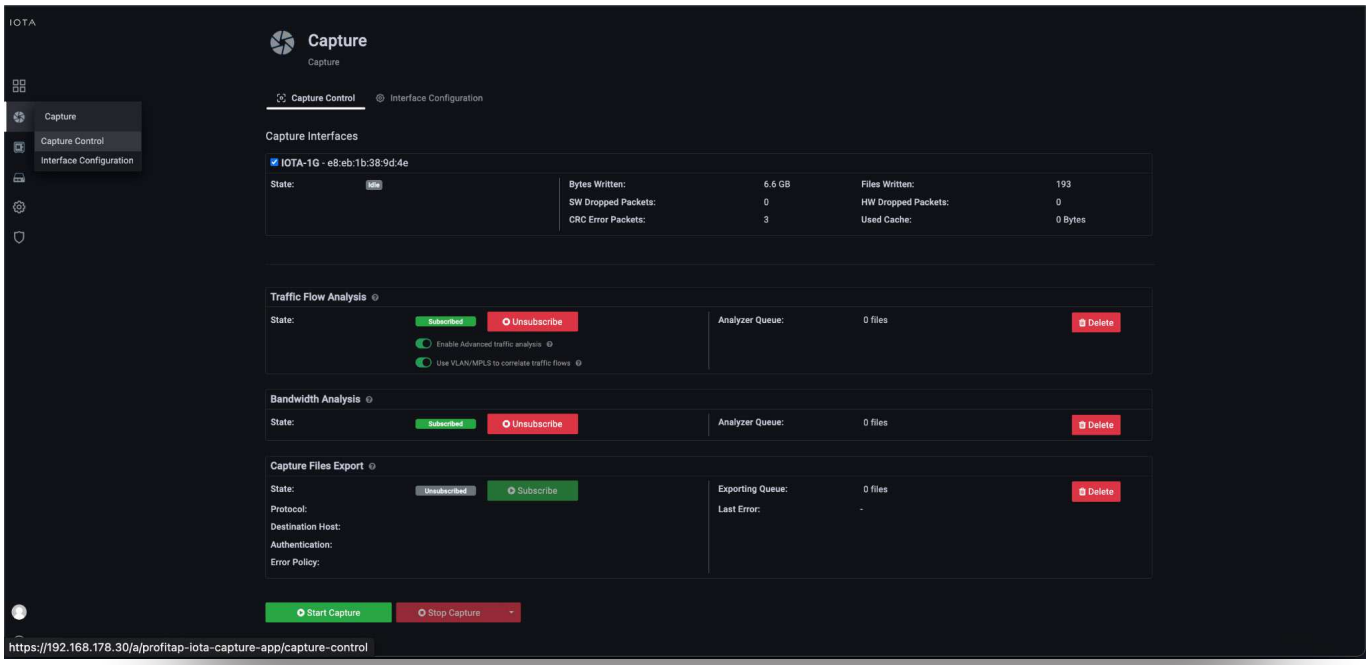

图2：通过"捕获控制"页面上的"开始捕获"按钮启动捕获

首先，我们在Overview面板上为Office 365应用程序和受影响客户端的源IP地址设置了一个筛选器。这使我们能够迅速缩小受影响的沟通关系

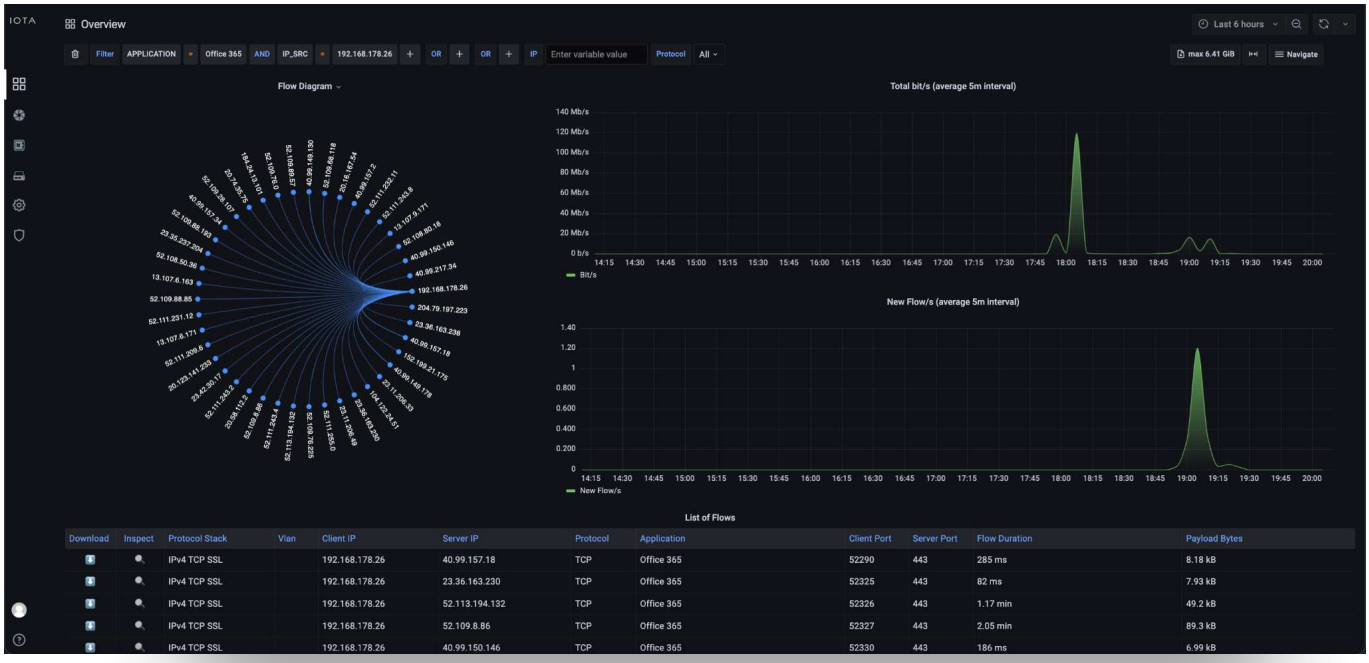

图3：过滤Office 365和客户端的源IP地址；在这种情况下为192.168.178.26

由于Office 365在端口443（HTTPS）上建立与相应目标服务器的TCP通信，因此我们将重点关注这种通信模式。为此，我们通过屏幕右上角的"导航"菜单切换到"TCP分析"面板。

在TCP分析仪表板中，我们使用递减iRTT排序立即识别到服务器"52.111.232.11"和服务器主机名"messaging.engagement.office.com"的初始往返时间的强峰值。

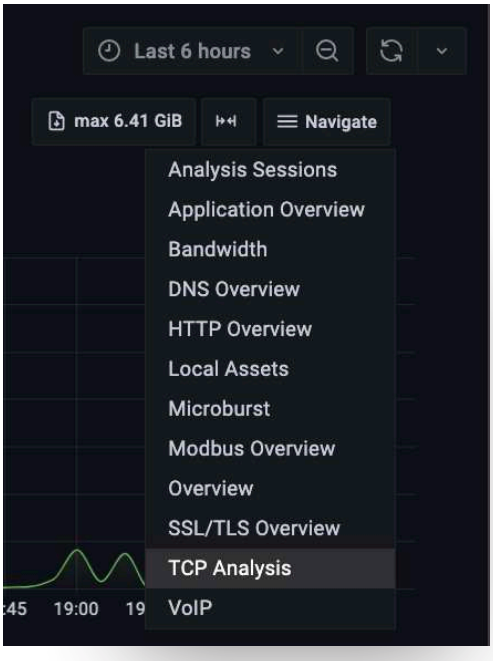

图4：切换到TCP分析.

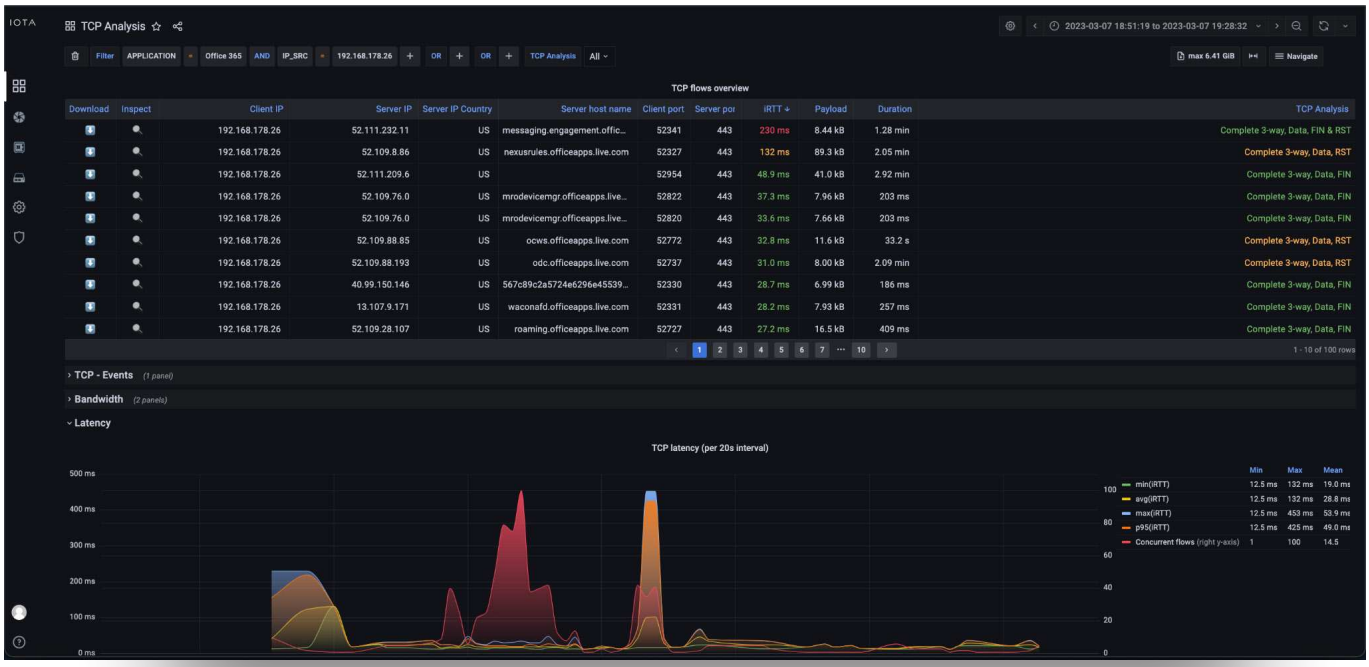

图5："TCP分析"面板

为了识别可能的带宽瓶颈，TCP分析面板中提供了带宽图。这些显示用于间隔记录的数据中的总TCP带宽，以及每个应用程序的显示和列表。

例如，低带宽使用率可能是由于TCP报头中缺少窗口缩放标志造成的，或者仅仅是由于在同一连接上并行传输并共享可用带宽的其他传输造成的。

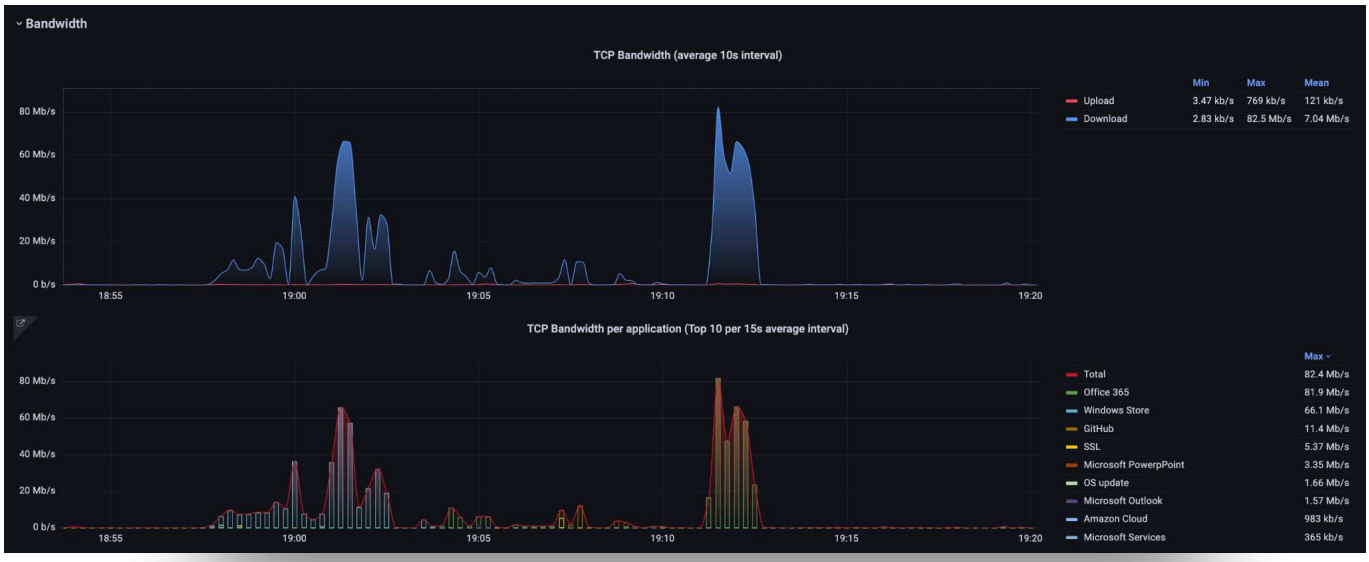

图6："TCP分析"面板的带宽图。上图显示了总带宽，低于每个应用程序的带宽

图7:TCP流详细信息面板

由于，根据TCP分析仪表板中iRTT的降序列表，只有这一台服务器在指定的时间窗口中具有如此高的初始往返时间，而微软同一自治系统中的其他目标服务器则要低得多，可以假设在与Microsoft网络中的服务器的网络连接中存在性能问题瓶颈或者在服务器本身上存在瓶颈。然而，根据Flow Detail仪表板中的信息，由于服务器延迟与iRTT大致在相同的范围内，因此可以假设在Microsoft连接此服务器时存在高延迟。这是因为当服务器出现性能瓶颈时，iRTT通常在正常范围内，但服务器延迟非常高。显示的行为导致应用程序运行缓慢。

然而，缓慢的应用程序也可能由于数据包丢失或服务器或客户端缓慢而导致TCP重传。为了评估这些，我们返回到TCP分析面板。

在这个仪表板中，我们现在根据服务器的目标IP地址进行过滤，方法是将鼠标悬停在目标IP地址上，然后单击+图标来激活过滤器。

图8：通过单击IP地址旁边的+符号，在服务器IP地址52.111.232.11上创建一个筛选器

设置好过滤器后，我们会看到仪表板底部的TCP重新传输图。在这里，我们可以看到在同一时间段内有客户端重传。这意味着客户端要么没有接收到请求的数据或确认消息（ACK），要么接收得晚，因此开始重新传输。在通信路径的其他点处的分析必须提供关于错误起源的精确信息。

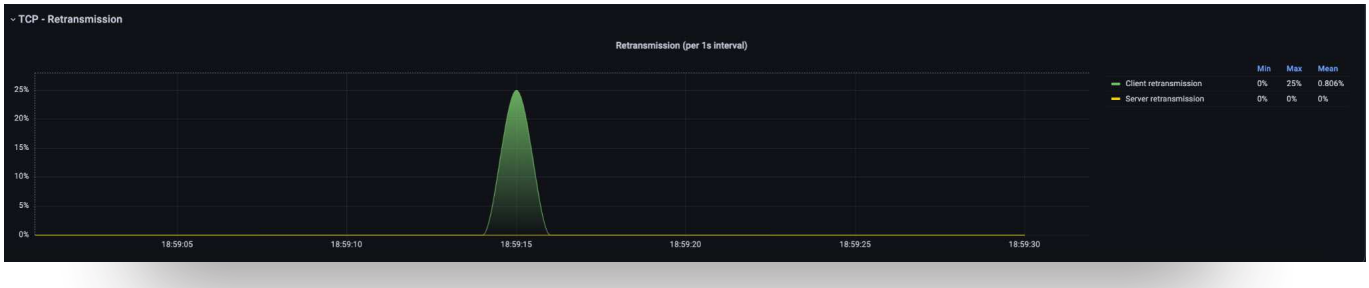

图9：过滤连接的TCP重传图

“应用程序概述”面板还可以进一步指示应用程序运行缓慢。在此仪表板中，可以根据饼图筛选不同的应用程序，例如所示示例中的Microsoft Teams，并在不同的图表中显示带宽和延迟。

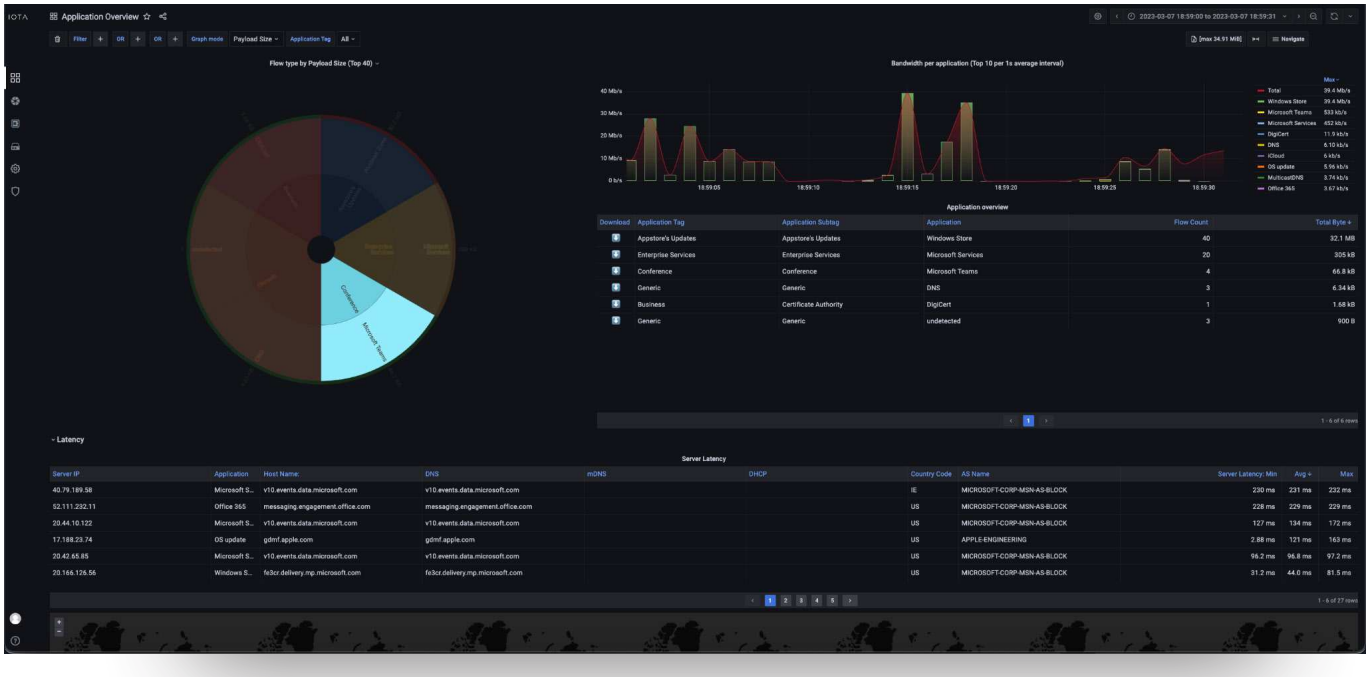

图10：应用程序概述面板，包含带宽图、基于饼图的过滤选项和表格延迟概述

另一种错误模式是应用程序间歇性“冻结”。“冻结”应用程序的一个可能原因可能是TCP Zero Windows。这意味着数据包是在网络端传递的，但应用程序无法从操作系统的TCP/IP堆栈中检索到。因此，TCP/IP堆栈将此信号发送给远程对等方。这种行为的原因是Zero Windows的发送方存在性能瓶颈。然后，我们可以向下搜索以缩小Zero Window消息的范围，然后过滤流。在下面的“零窗口”图中，我们可以看到这些情况发生的时间。

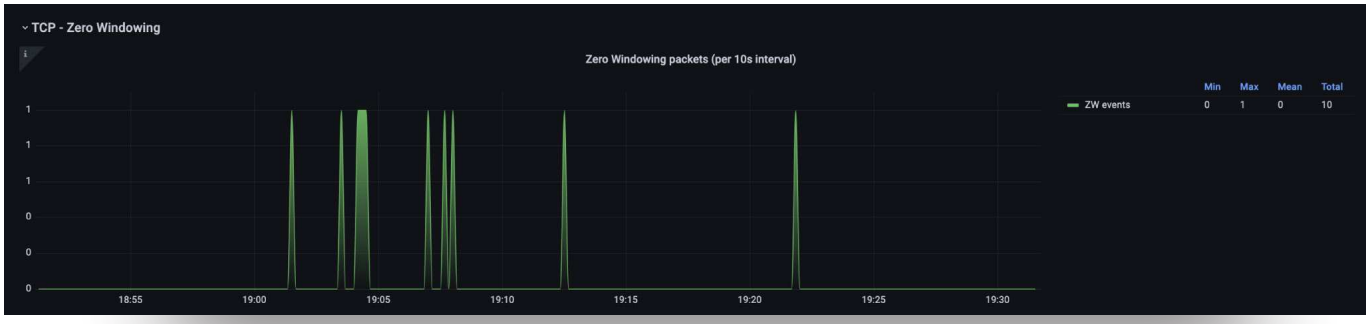

图11:TCP零窗口消息的表示

为了检测是谁发送了Zero Window消息，可以通过下图左侧的箭头按钮下载PCAPNG。

使用Wireshark中的显示过滤器"tcp.analysis.zero_window"，很容易确定零窗口的发送方。

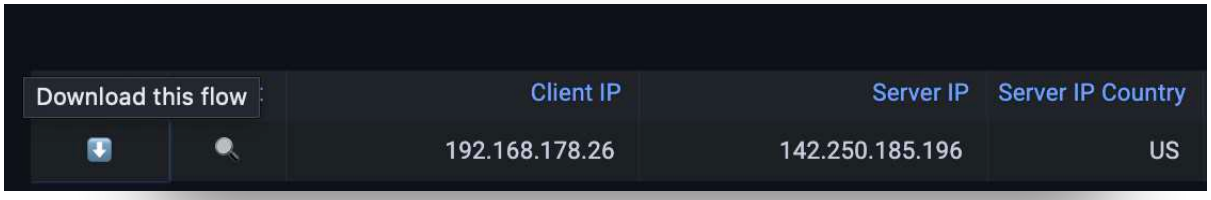

图12：下载PCAPNG文件以在Wireshark中进行分析

*关于 **IOTA** 解决方案*

IOTA为网络提供了一个集成的记录和分析平台。基于直观的仪表盘，可以应用高性能和多样化的过滤器来确定故障通信关系的根本原因，从而缩短平均修复时间。应用程序智能还有助于根据所使用的应用程序对数据流进行预过滤。

IOTA 设备型号

IOTA 1G

关键捕获点/远程办公室

2 x RJ45
1 TB SSD

IOTA 1G+

关键捕获点/远程办公室

2 x RJ45
1 TB or 2 TB Removable SSD GPS/PPS timing ports

IOTA 10G

大型分支机构/WAN边缘

2 x SFP / SFP+ 1 TB SSD

IOTA 10G+

大型分支机构/WAN边缘

2 x SFP / SFP+
1 TB or 2 TB Removable SSD GPS/PPS timing ports

itbigtec 艾体宝

艾体宝科技有限公司

www.itbigtec.com
sales@itbigtec.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼

T (+86)400-999-3848

各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 | 台湾 | 香港 | 日本 | 韩国 | 新加坡 | 美国硅谷

版本：V1.0 - 22/11/14

网络安全与监控方向
(T: 135 3349 1614)

网络安全交流2群

获取更多资料

itbigtec.com