itbigtec
艾体宝

IOTA
DNS疑难解答

问题描述

有句话说："这不是DNS；不可能是DNS；这是DNS"。这清楚地表明，DNS是IT基础设施服务的一个组成部分，并且可以表现出各种各样的错误模式。例如，DNS可能导致应用程序无法启动或启动延迟。有时，这是由于错误存储的DNS记录或DNS服务器上的性能瓶颈造成的。然而，由于一些系统集成商只支持UDP上的DNS，因此在某些情况下，过于严格的防火墙会导致问题。然而，对于大量响应，DNS会切换到TCP。浏览器中的证书错误也可能表明DNS条目不正确。

工作流疑难解答

以下示例提供了如何使用Profitap IOTA进行DNS流量分析的分步指南概述。为此使用了不同的错误模式。

启动捕获

在第一步中，我们必须配置物理接口。为此，我们从左侧菜单导航到"捕获">"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。

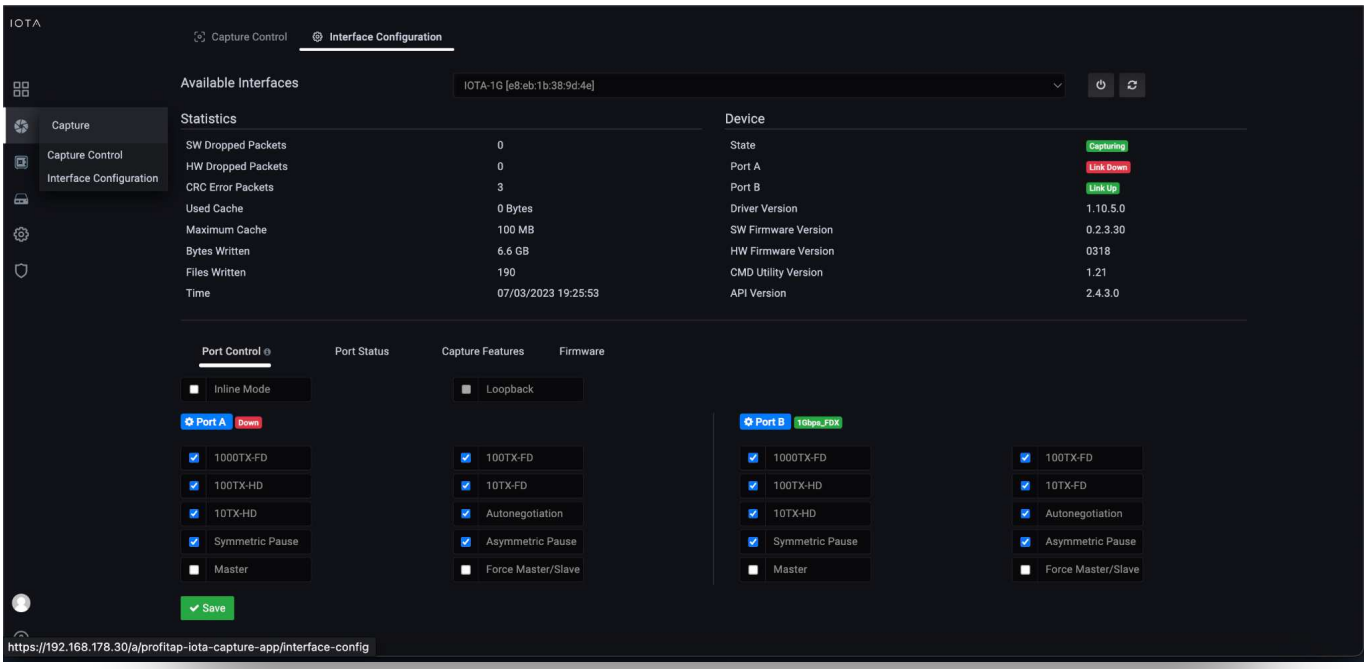

图1：物理接口的配置。在这种情况下，在SPAN模式下的10/100/1000 Mbit/s自动协商.

准备好物理接口后，我们连接适当的电缆，并通过单击“开始捕获”按钮在“捕获控制”页面上启动捕获过程。

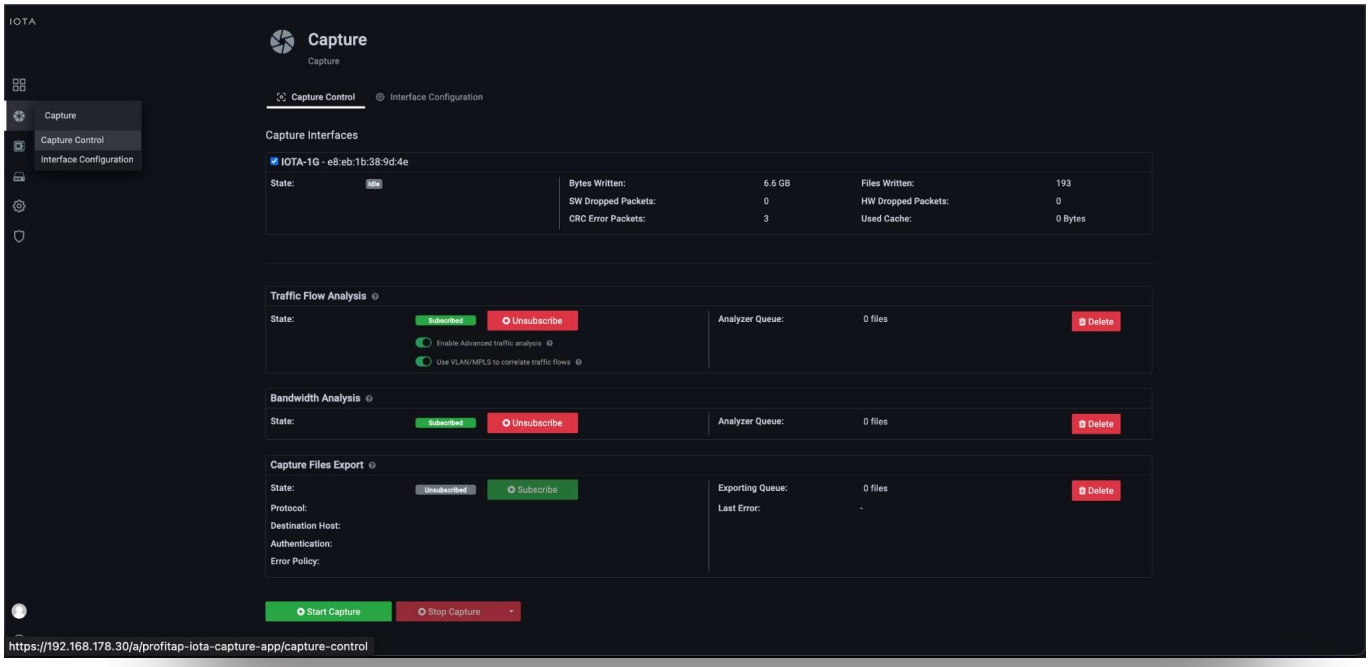

图2：通过“捕获控制”页面上的“开始捕获”按钮启动捕获

大量请求/ DNS服务器性能问题

在问题描述中，DNS服务器的性能非常差。客户端的响应只是延迟了一段时间。这就是为什么我们首先要检查是否存在服务器问题或异常大量的DNS查询，如果是，这些查询是从哪些客户端触发的，这样我们就可以将其与网络隔离开来。

为此，我们通过屏幕右上角的导航菜单从初始的概览面板切换到DNS概览面板。

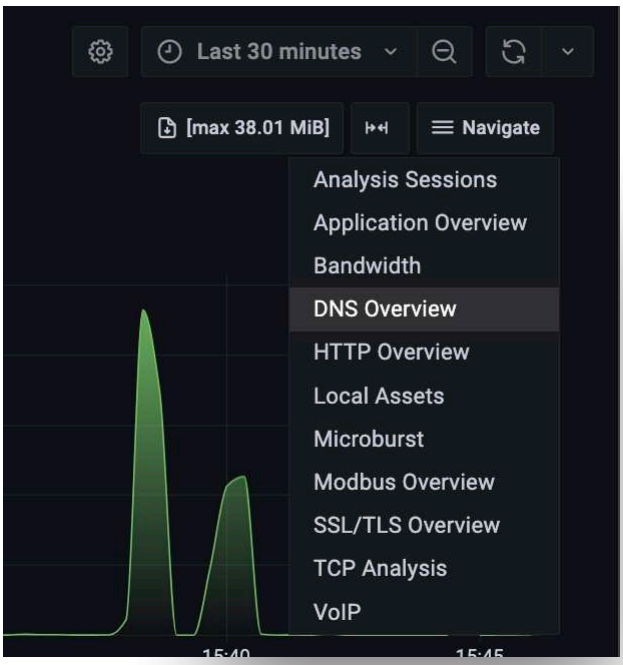

图3：通过"导航"菜单从"概览"切换到"DNS概览"面板

在DNS概览面板中，我们可以看到特定时间间隔内的DNS请求总数，以及按目标DNS服务器和目标域划分的细分。

图4:DNS概览仪表板，其中包含一个域的大量DNS请求

图4：切换到TCP分析

根据这些信息，我们可以直接看到，在最后一个小时的时间间隔内，有时会发送多达600个DNS请求，这在小型网络中是不寻常的。向DNS服务器192.168.178.1发出了14000个请求，向域名“heise.de”发出了12300个请求

在下文中，我们可以使用搜索DNS功能并过滤域名“heise.de”的请求

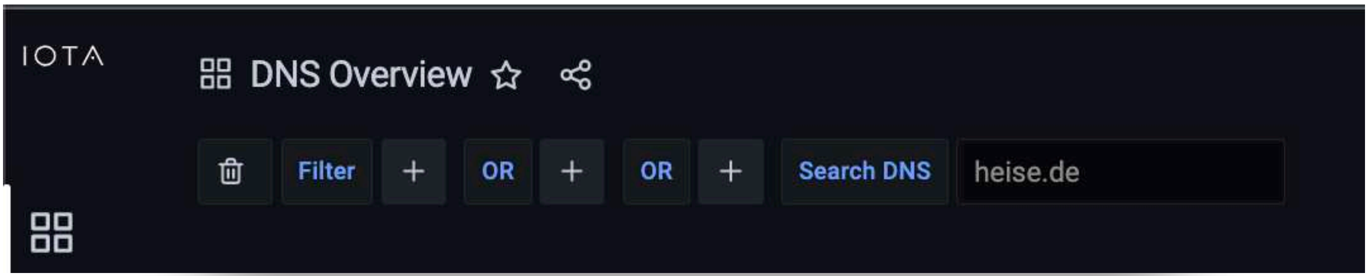

图5：基于域名'heise.de'通过“搜索DNS”功能进行过滤

然后，我们可以向下滚动到DNS概览面板中的流表（图6）。该流程表显示，从第四行开始，客户端192.168.178.22每秒多次对目标域“heise.de”进行DNS请求，但没有建立后续连接。列表顶部的三个流显示TCP和TLS连接是基于DNS响应建立的。

Flows

DNS query/response with associated flows (Latest 20)

Download	DNS query/response date ↓	Client IP	DNS Server IP	Query	Response		Protocols	Applications	Flows
	08.03.2023, 15:53:33	192.168.178.28	192.168.178.1	reichweite.heise.de	193.99.144.85	⇨	TCP	SSL	1
	08.03.2023, 15:53:31	192.168.178.28	192.168.178.1	www.heise.de	193.99.144.85	⇨	TCP	SSL	2
	08.03.2023, 15:53:31	192.168.178.28	192.168.178.1	prophet.heise.de	185.54.150.27	⇨	TCP	SSL	2
	08.03.2023, 15:31:32	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0
	08.03.2023, 15:31:32	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0
	08.03.2023, 15:31:32	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0
	08.03.2023, 15:31:32	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0
	08.03.2023, 15:31:32	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0
	08.03.2023, 15:31:32	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0
	08.03.2023, 15:31:32	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0
	08.03.2023, 15:31:30	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0
	08.03.2023, 15:31:30	192.168.178.22	192.168.178.1	heise.de	193.99.144.80	⇨			0

‹ 1 2 › 1 - 12 of 20 rows

图6:DNS FLOW表

客户端192.168.178.22的行为表示客户端错误，必须在主机192.168.178.22.上进行分析。在修复之前，客户端可以与网络隔离。在本例中，中的DNS请求循环客户端上的应用程序是原因。

DNS响应时间慢

要分析缓慢的应用程序启动，对DNS响应时间的分析在许多情况下都有帮助。PCAPNG下载单个DNS请求/应答和相关的TCP，以及TLS流（如果适用）可能会有所帮助。

与前面的示例一样，我们使用Search　DNS功能进行过滤，然后滚动到FLOW表。在左侧边缘，如图6所示，单击相应FLOW旁边的箭头按钮，即可开始以PCAPNG格式下载该FLOW。这提供了DNS请求、响应和相关的TCP，可能还有TLS FLOW供下载。

我们可以使用显示筛选器"DNS"和一列与前一个数据包的delta时间来快速确定DNS响应时间。
在本例中，这是12.5毫秒，这是一个正常值。

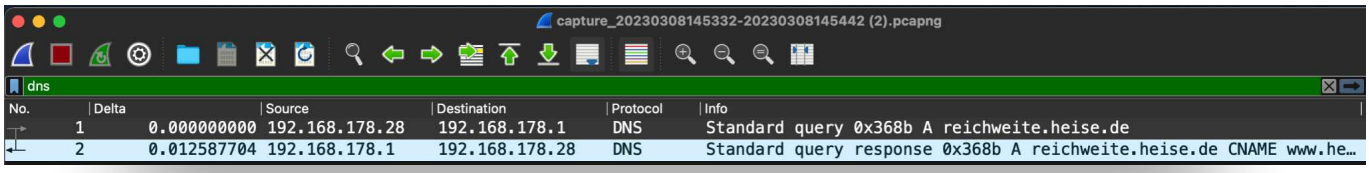

图7:Wireshark中显示的PCAPNG

浏览器中的证书错误

如果用户在浏览器或其他应用程序中收到证书错误，这也可能表明DNS中有错误。为了分析客户端从DNS服务器接收到的响应DNS-记录查询的IP地址，我们再次使用DNS概览面板。我们通过应用"SERVER_HOST_name_DNS=profitap.com"筛选器来筛选所需的域名。

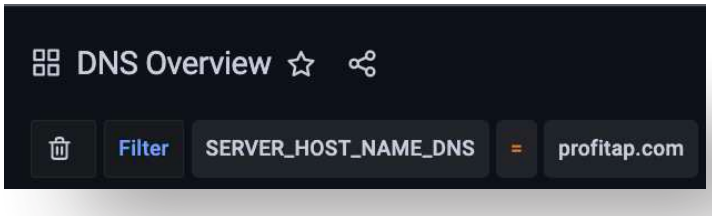

图8：在DNS请求面板中过滤服务器名称"profitap.com"

因此，我们可以在过滤FLOW表中看到DNS查询请求和响应。在下面的示例中，IP地址217.160.0.226被传递用于profilap.com A记录的DNS查询。基于这些数据，我们可以通过openssl s_client等工具比较预期的目标IP地址和目标服务器，或者检查TLS握手和交付的证书。

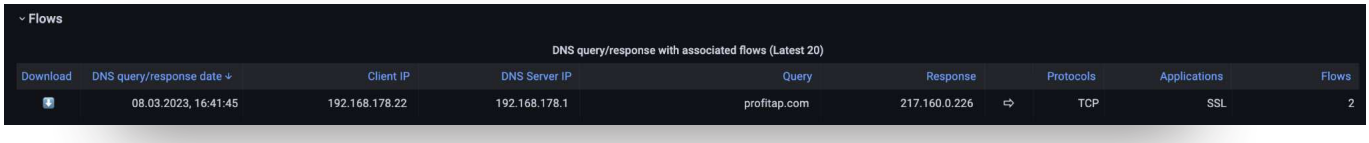

图9：A-record profilap.com上的DNS查询流程。我们将IP地址217.160.0.226识别为响应

IOTA 优势

除了简单快捷的过滤器外，Profitap IOTA还提供了广泛的DNS分析选项。DNS概览仪表板提供有关所使用的DNS服务器和目标域的定量图形评估和数据。例如，很容易检测到请求错误DNS服务器的配置错误的客户端。上面提到的仪表板中的FLOW表是应用程序分析的一个特别有用的工具，可以在必要时检测和下载DNS和后续TCP套接字以及TLS握手之间的相关性。

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