如何使用二三层仪表模拟无状态的 DDOS 攻击测试

关于网络安全现状，在前面的文章中已有介绍，感兴趣的小伙伴可以翻看往期的文章（信而泰测试方案，助力客户打造网络安全防护“金钟罩”），今天要和大家聊一聊众多网络攻击其中最常见的一种：DDOS 攻击，以及如何使用二三层仪表模拟无状态的 DDOS 攻击测试。

什么是 DDOS 攻击

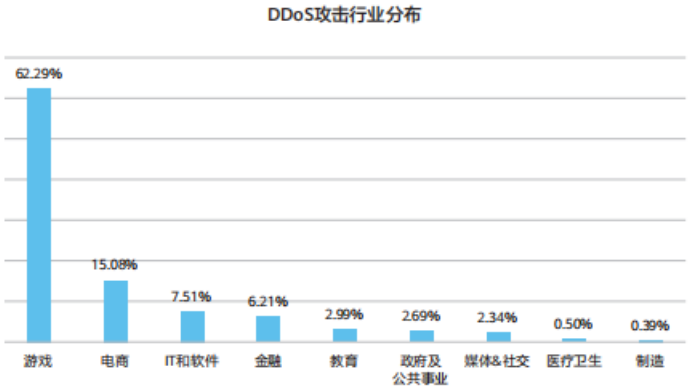
分布式拒绝服务攻击(Distributed Denial of Service，简称 DDoS)是指通过大规模互联网流量淹没目标服务器或其周边基础设施，以破坏目标服务器、服务或网络正常流量的恶意行为。大量虚假的用户占用网络资源，把资源耗尽，导致正常用户无法使用，好比高速公路全部被大量的恶意车辆占用，产生拥堵，妨碍常规车辆抵达预定目的地。

DDOS 攻击的类型

DDOS 攻击有多种类型，如：SYN Flood、UDP Reflection、TCP Reflection、UDP Flood、UDP Fragment Flood、ACK Flood 、FIN/RST Flood 、UDP Replay 、ICMP Flood 、UDP Malformed 、TCP Fragment Flood 、TCP Connection Flood 、HTTP Flood、HTTP 异常会话、HTTPS Flood、other。SYN Flood、UDP 反射是网络层攻击的主要方式，其次就是应用层的泛洪攻击。何为无状态的 DDOS 攻击，不需要与被攻击方进行 TCP 三次握手等动态交互，只需发送固定字段的请求，把被攻击方的资源耗尽。

DDOS 攻击态势

现如今大流量攻击已成常态化，在 2022 年监测到超 800Gbps 攻击达 7 次之多，均发生在 6 月份，攻击次数是 2021 年的 4 倍，而在对被攻击的行业统计中，游戏依然是受攻击最严重的行业，游戏行业内部激烈竞争导致针对游戏的攻击频率猛增。



注：数据摘自全球 DDos 现状与趋势分析

检测设备抗 DDOS 攻击能力

在面对 DDOS 攻击时，运营商有着相应的云清洗服务，即使这样企业在采用网络基础设备时，还是要检测设备的抗 DDOS 攻击能力，通过软硬结合的方式来进行防护。专业硬件提供高效“硬防”抵御大流量网络层攻击；CPU 提供 AI 加持的多层级“软防”，精细化过滤小流量应用层攻击，且“软防”需提供实时分析和提取攻击特征、智能调度“硬防”的能力，从而快速阻断混合攻击，有效提升防御效率。所以在对设备做测试的时候，不止要测设备的性能，还要测试设备的抗攻击能力。

仪表模拟 DDOS 攻击流量

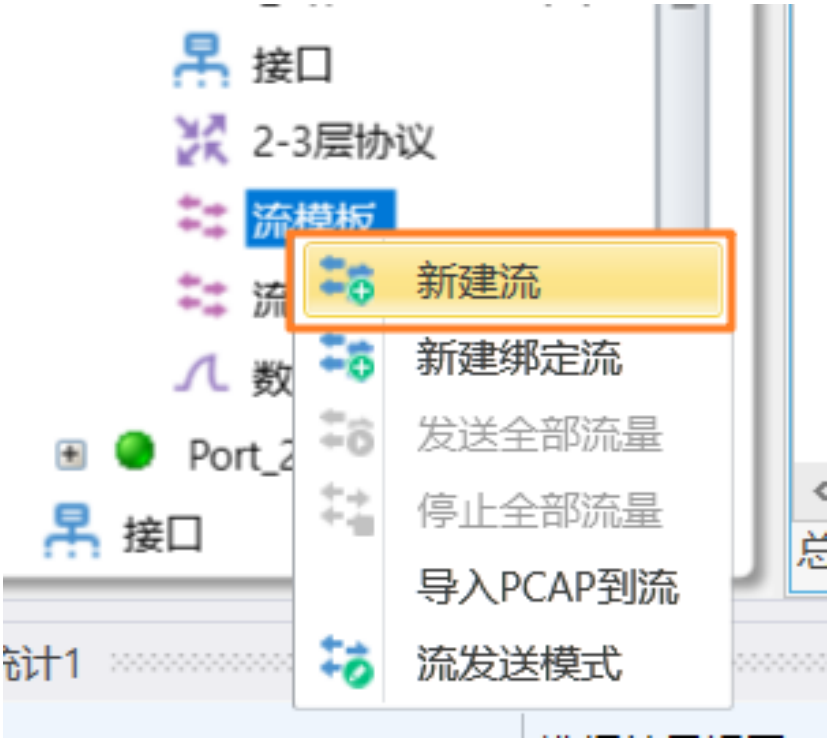
网络测试仪表可以构造 DDOS 复杂大流量攻击，来检验设备的 DDOS 攻击能力。本期我们要说的就是如何使用 2-3 层仪表模拟无状态的 DDOS 流量攻击。

信而泰 BigTao 系列、DarYu 系列及 Darpeng 系列网络测试仪表，均可模拟 DDOS 攻击测试

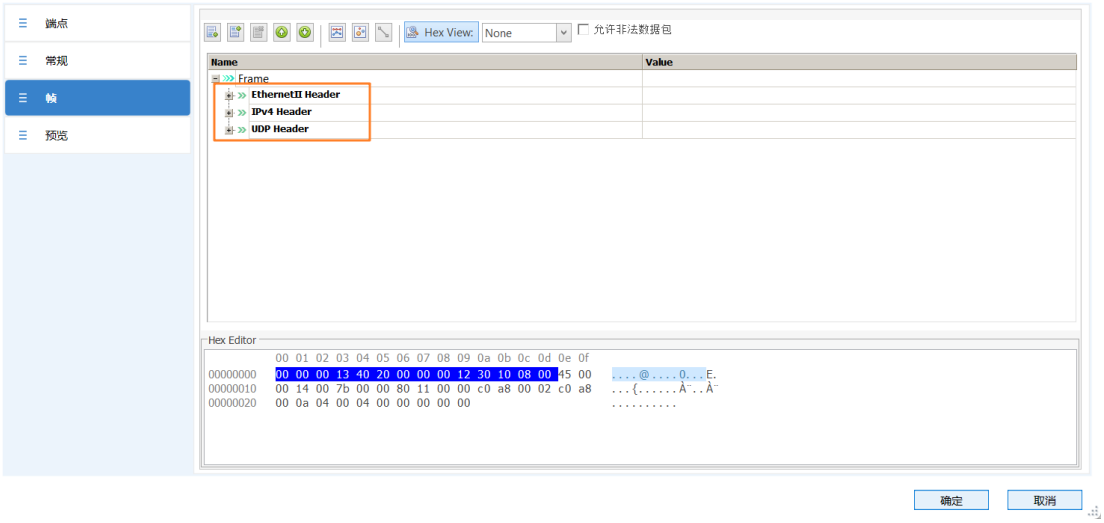
抗 DDOS 攻击测试拓扑

构造网络层及传输层 DDOS 攻击流量

1、仪表在测试的端口上增加 raw 流来构造攻击流量；

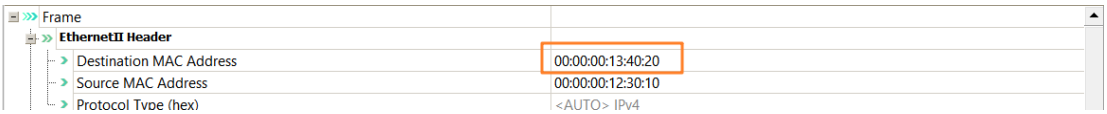


2、根据攻击类型选择相应的报头封装，以 UDP Flood 为例，即选择以太帧+IPv4 帧+UDP 报头；

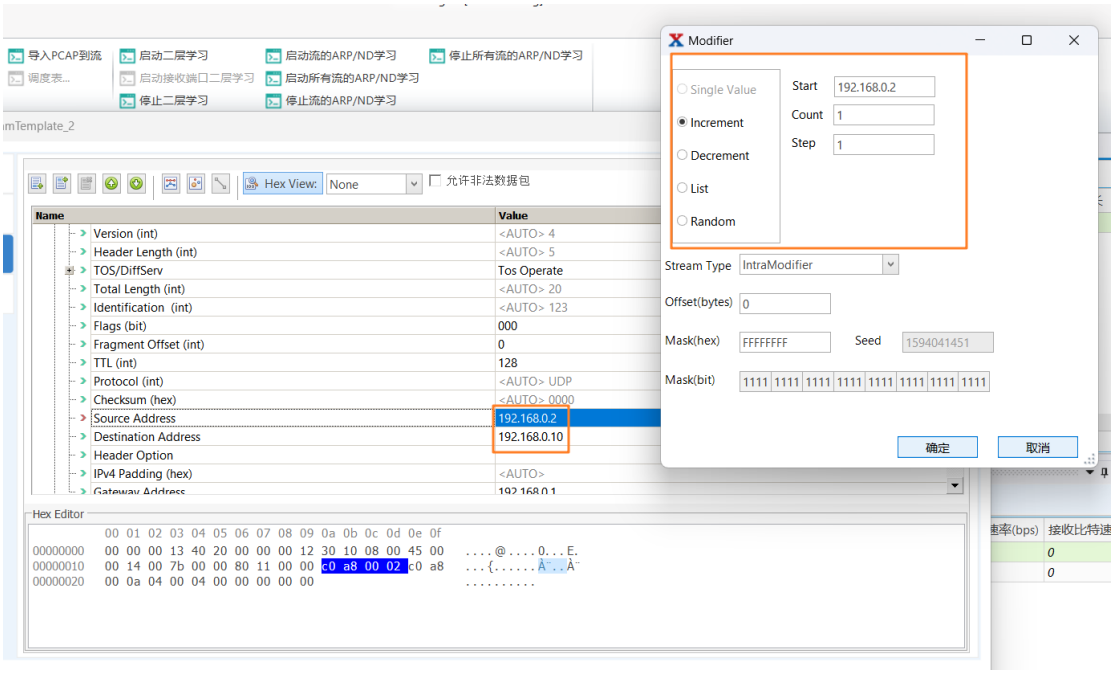


3、接着修改流量里面的内容，来达到攻击的目的。

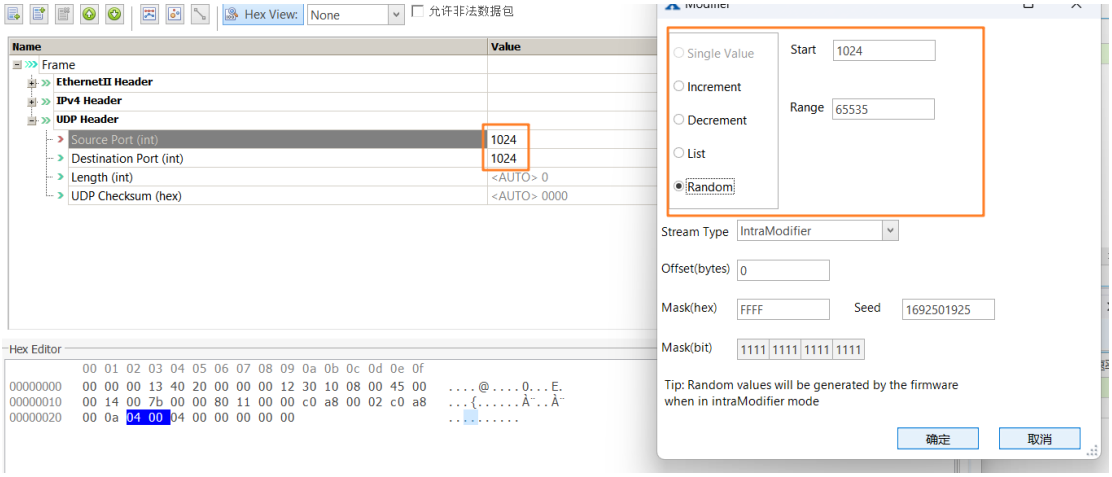
（1）目的 MAC 需要填充仪表该接口直连接口的 mac 地址；



（2）源 IP 可根据需要进行递增递减或随机的方式来进行跳变，从而达到模拟大量源 IP 不同用户的场景，目的 IP 则填充被攻击设备的 IP；



（3）UDP 源目端口选择随机跳变，来模拟真实 UDP Flood 的场景；

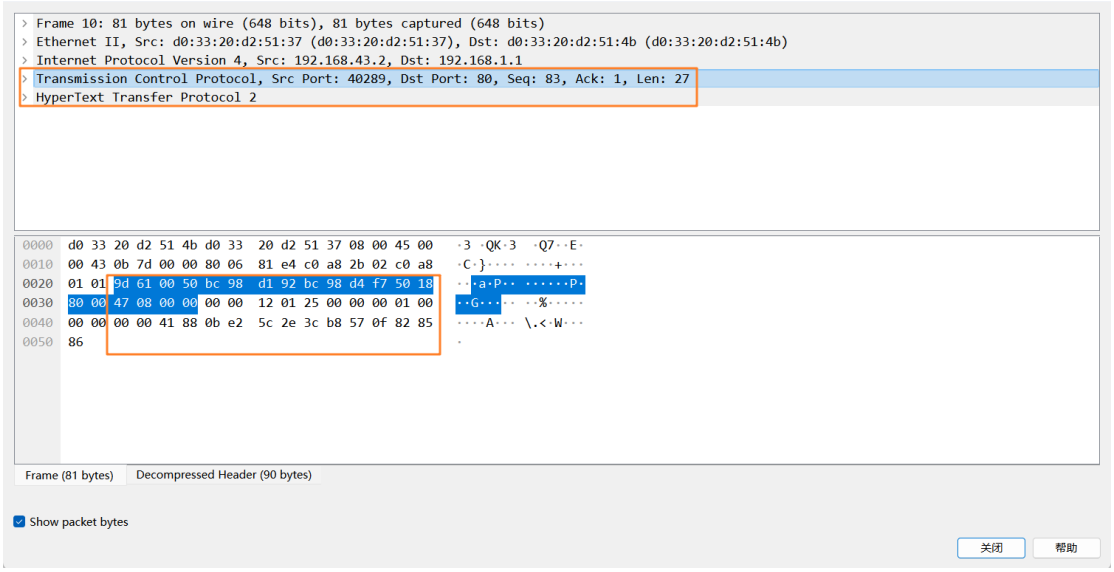


4、一个模拟 UDP Flood 的攻击流量就创建好了，设置好需要发送带宽的大小后，即可测试设备的抗 DDOS 能力；其他的网络层及传输层的 DDOS，同理，根据每种攻击的特性不同，将报文里的相应字段置位来达到攻击的目的，如 SYN Flood，需要将 TCP 报头里的 syn 置 1。

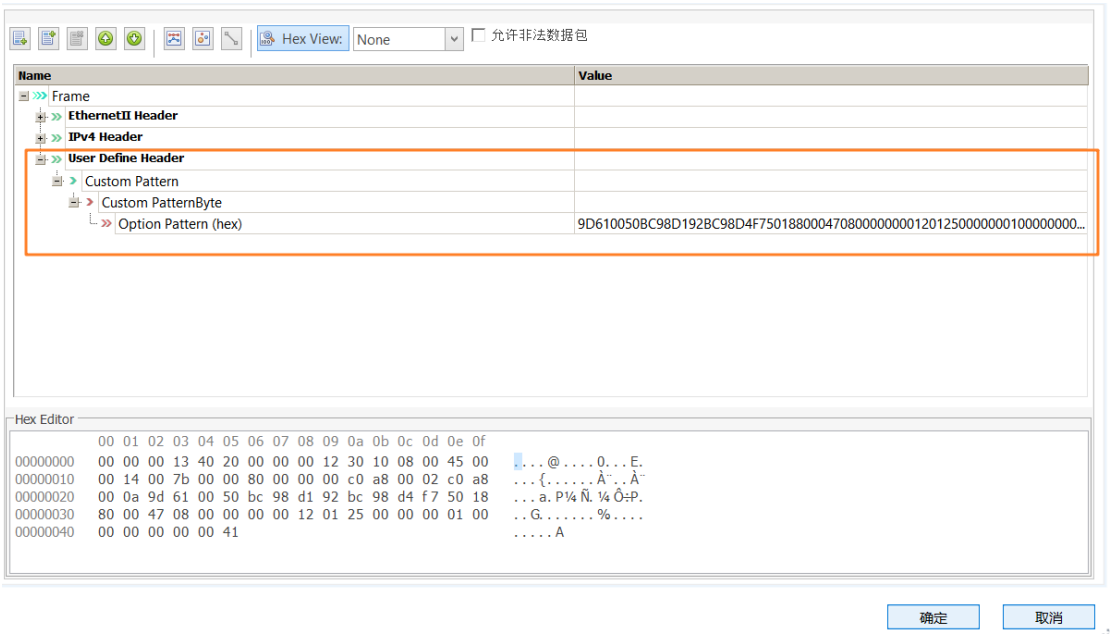
模拟应用层 DDOS 攻击流量

关于应用层的攻击，相应的应用层报头在二三层仪表上无法添加，可以通过导入 Custom 来实现，具体方式如下：

1、将需要模拟应用层报文抓出来，通过 wireshark 打开，把传输层及应用层报头对应的二进制导出来；



2、仪表创建 raw 流，增加以太帧+IPv4 头，以及再添加一个 custom 自定义报头，以太帧和 IPv4 头的跳变设置同上，在 custom 里把刚刚导出的二进制数导入，这样就完成了一个应用层报文构造



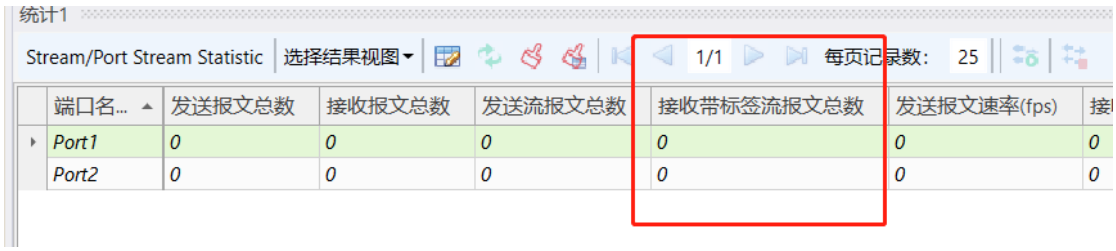
查看设备抗 DDOS 测试结果

1、仪表向被测设备发送 DDOS 攻击，若被测设备无法识别 DDOS 攻击，并处理了相应的攻击流量，如 ARP 攻击，则被测设备会将 ARP 攻击报文上送 CPU 处理，大量上送 CPU 处理的报文将会使得被测设备的 CPU 利用率高达 100%，可通过查看被测设备的 CPU 利用率来判断。

```
[DUT]display cpu-usage
CPU   Usage Stat. Cycle: 10 (Second)
CPU   Usage Stat. Time : 2023-04-19  14:55:04
Control Plane
    CPU Usage:  7.4%   Max: 31.0%
    User:  3.5%   System:  3.8%   SoftIrq:  0.0%   HardIrq:  0.0%   Idle: 92.6%
    CPU utilization for ten seconds:  7.4%  one minute:   7.0%  five minutes:   7.0% .
Data    Plane
    CPU Usage:  0.0%   Max:  7.3%
    CPU utilization for ten seconds:  0.0%  one minute:   0.0%  five minutes:   0.0% .

PID   ProcessName         CPU%     CoreIndex      Runtime     State
2370  cap                 0.0%      CPU1           6201076913  S
2370  cap                 0.0%      CPU2           6201076913  S
2370  cap                 0.0%      CPU3           6201076913  S
2370  cap                 0.0%      CPU4           6201076913  S
2370  cap                 0.0%      CPU5           6201076913  S
2370  cap                 0.0%      CPU6           6201076913  S
2370  cap                 0.0%      CPU7           6201076913  S
2370  cap                 0.0%      CPU8           6201076913  S
2370  cap                 0.0%      CPU9           6201076913  S
2370  cap                 0.0%      CPU10          6201076913  S
2370  cap                 0.0%      CPU11          6201076913  S
2370  cap                 0.0%      CPU12          6201076913  S
2370  cap                 0.0%      CPU13          6201076913  S
2370  cap                 0.0%      CPU14          6201076913  S
```

2、仪表与被测设备连接观察端口，通过在仪表端口统计视图上查看观察端口的接收带标签报文数量来判断被测设备抗 DDOS 攻击效果。


统计1
Stream/Port Stream Statistic
选择结果视图
1/1
每页记录数:
25
端口名...
发送报文总数
接收报文总数
发送流报文总数
接收带标签流报文总数
发送报文速率(fps)
Port1
0
0
0
0
0
0
Port2
0
0
0
0
0
0